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 .

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**.

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.

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.

Andr/Dropr-FH is also known as:

- GhostCtrl

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.

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.

Table 4. Table References

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

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.

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.

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.

Svpeng is also known as:

- Invisble Man

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.

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.

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.

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.

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.

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.

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.

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.

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.

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

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.

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).

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.

GM Bot is also known as:

- Acecard
- SlemBunk
- Bankosy

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.

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.

Adwind is also known as:

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

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.

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

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

Table 209. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-032606-5519-99

ImAdPush

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

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

Table 414. Table References

Links
https://securelist.com/sms-trojan-bypasses-captcha/69169//

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

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.

Zeus is also known as:

- Zbot

Table 415. 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.

Vawtrak is also known as:

- Neverquest

Table 416. 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.
```

Dridex is also known as:

- Feodo Version D

Table 417. 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

Gozi is also known as:

- Ursnif
- CRM
- Snifula
- Papras

Table 418. 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.

Goziv2 is also known as:

- Prinimalka

Table 419. 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.

Table 420. 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.

Table 421. 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

Table 422. 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.

Table 423. 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.

Zloader Zeus is also known as:

- Zeus Terdot

Table 424. 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.

Zeus VM is also known as:

- VM Zeus

Table 425. 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.

Table 426. 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.

Panda Banker is also known as:

- Zeus Panda

Table 427. 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

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.

Zeus KINS is also known as:

- Kasper Internet Non-Security
- Maple

Table 428. 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.

Table 429. 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

Trickbot is also known as:

- Trickster
- Trickloader

Table 430. 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/

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.

Dyre is also known as:

- Dyreza

Table 431. 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.

Tinba is also known as:

- Zusy
- TinyBanker
- illi

Table 432. 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.

Geodo is also known as:

- Feodo Version C
- Emotet

Table 433. Table References

Links
https://feodotracker.abuse.ch/
http://blog.trendmicro.com/trendlabs-security-intelligence/new-banking-malware-uses-network-sniffing-for-data-theft/

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.

Feodo is also known as:

- Bugat
- Cridex

Table 434. 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.

Ramnit is also known as:

- Nimnul

Table 435. 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.

Qakbot is also known as:

- Qbot
- Pinkslipbot

Table 436. 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.

Table 437. 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.

TinyNuke is also known as:

- NukeBot
- Nuclear Bot
- MicroBankingTrojan
- Xbot

Table 438. 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.

Retefe is also known as:

- Tsukuba
- Werdlod

Table 439. 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.

Table 440. 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.

Table 441. 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.

Table 442. 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.

Table 443. 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.

Table 444. 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.

Table 445. 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.

Table 446. 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.

Table 447. 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

Licat is also known as:

- Murofet

Table 448. 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.

Table 449. 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.

Table 450. 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/

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.

Table 451. 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.

Table 452. 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.

Table 453. 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.

Smominru is also known as:

- Ismo
- lsmo

Table 454. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/smominru-monero-mining-botnet-making-millions-operators

Branded Vulnerability

List of known vulnerabilities and attacks with a branding.

Branded Vulnerability is a cluster galaxy available in JSON format at https://github.com/MISP/misp-galaxy/blob/master/clusters/branded vulnerability.json[**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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

ImageTragick

Cert EU GovSector

Cert EU GovSector.

Cert EU GovSector is a cluster galaxy available in JSON format at https://github.com/MISP/misp-galaxy/blob/master/clusters/cert eu govsector.json[**this location**] The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Various

Constituency

EU-Centric

EU-nearby

World-class

Unknown

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

Astrum is also known as:

- Stegano EK

Table 455. 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/

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

Terror EK

Terror EK is built on Hunter, Sundown and RIG EK code

Terror EK is also known as:

- Blaze EK
- Neptune EK

Table 456. 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.

DealersChoice is also known as:

- Sednit RTF EK

Table 457. 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

DNSChanger is also known as:

- RouterEK

Table 458. 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

Table 459. 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

Kaixin is also known as:

- CK vip

Table 460. 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

Magnitude is also known as:

- Popads EK
- TopExp

Table 461. 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

Table 462. 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

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.

RIG is also known as:

- RIG 3
- RIG-v
- RIG 4
- Meadgive

Table 463. 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

Sednit EK is also known as:

- SedKit

Table 464. 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

Sundown-P is also known as:

- Sundown-Pirate
- CaptainBlack

Table 465. 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

Bizarro Sundown is also known as:

- Sundown-b

Table 466. 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

Hunter is also known as:

- 3ROS Exploit Kit

Table 467. 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

GreenFlash Sundown is also known as:

- Sundown-GF

Table 468. 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

Angler is also known as:

- XXX
- AEK
- Axpergle

Table 469. 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

Table 470. 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)

BlackHole is also known as:

- BHEK

Table 471. 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

Bleeding Life is also known as:

- BL
- BL2

Table 472. 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

Cool is also known as:

- CEK
- Styxy Cool

Table 473. 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

Fiesta is also known as:

- NeoSploit
- Fiexp

Table 474. 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

Empire is also known as:

- RIG-E

Table 475. 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

FlashPack is also known as:

- FlashEK
- SafePack
- CritXPack
- Vintage Pack

Table 476. 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

GrandSoft

GrandSoft Exploit Kit was a quite common exploit kit used in 2012/2013. Disappeared between march 2014 and September 2017

GrandSoft is also known as:

- StampEK
- SofosFO

Table 477. 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

Table 478. 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

Himan is also known as:

- High Load

Table 479. Table References

Links
http://malware.dontneedcoffee.com/2013/10/HiMan.html

Impact

Impact EK

Table 480. Table References

Links
http://malware.dontneedcoffee.com/2012/12/inside-impact-exploit-kit-back-on-track.html

Infinity

Infinity is an evolution of Redkit

Infinity is also known as:

- Redkit v2.0
- Goon

Table 481. 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

Table 482. 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

Table 483. 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.

Neutrino is also known as:

- Job314
- Neutrino Rebooted
- Neutrino-v

Table 484. 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.

Niteris is also known as:

- CottonCastle

Table 485. 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

Nuclear is also known as:

- NEK
- Nuclear Pack
- Spartan
- Neclu

Table 486. Table References

Links
http://blog.checkpoint.com/2016/05/17/inside-nuclears-core-unraveling-a-ransomware-as-a-service-infrastructure/

Phoenix

Phoenix Exploit Kit

Phoenix is also known as:

- PEK

Table 487. 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

Private Exploit Pack is also known as:

- PEP

Table 488. 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

Table 489. 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

Table 490. 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

SPL is also known as:

- SPL_Data
- SPLNet
- SPL2

Table 491. 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

Sundown is also known as:

- Beps
- Xer
- Beta

Table 492. 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

Sweet-Orange is also known as:

- SWO
- Anogre

Table 493. Table References

Links
http://malware.dontneedcoffee.com/2012/12/juice-sweet-orange-2012-12.html

Styx

Styx Exploit Kit

Table 494. 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

Table 495. 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.

Table 496. Table References

Links
https://twitter.com/kafeine
https://twitter.com/node5
https://twitter.com/kahusecurity

Microsoft Activity Group actor

Activity groups as described by Microsoft.

Microsoft Activity Group actor is a cluster galaxy available in JSON format at https://github.com/MISP/misp-galaxy/blob/master/clusters/microsoft activity group actor.json[**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.

Table 497. 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.

Table 498. 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.

Table 499. 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.

STRONTIUM is also known as:

- APT 28
- APT28
- Pawn Storm
- Fancy Bear

- Sednit
- TsarTeam
- TG-4127
- Group-4127
- Sofacy
- Grey-Cloud

Table 500. 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/

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.

DUBNIUM is also known as:

- darkhotel

Table 501. 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.

Table 502. 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.

Table 503. 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.

Table 504. 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.

Table 505. Table References

Links
https://blogs.technet.microsoft.com/mmpc/2017/03/27/detecting-and-mitigating-elevation-of-privilege-exploit-for-cve-2017-0005/

Attack Pattern

ATT&CK tactic.

Attack Pattern is a cluster galaxy available in JSON format at https://github.com/MISP/misp-galaxy/blob/master/clusters/attack pattern.json[**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

Table 506. 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

Table 507. 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

Table 508. 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

Table 509. 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

Table 510. 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

Table 511. 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

Table 512. 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

Table 513. 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

Table 514. 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

Table 515. 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

Table 516. 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

Table 517. 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

Table 518. 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

Table 519. 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

Table 520. 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

Table 521. 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

Table 522. 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

Table 523. 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

Table 524. 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

Table 525. 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

Table 526. 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

Table 527. 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

Table 528. 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

Table 529. 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

Table 530. 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

Table 531. 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

Table 532. 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

Table 533. 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

Table 534. 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

Table 535. 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

Table 536. 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

Table 537. 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

Table 538. 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

Table 539. 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

Table 540. 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

Table 541. 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

Table 542. 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

Table 543. 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

Table 544. 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

Table 545. 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

Table 546. 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

Table 547. 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

Table 548. 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

Table 549. 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

Table 550. 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

Table 551. 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

Table 552. 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

Table 553. 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

Table 554. 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

Table 555. 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

Table 556. 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

Table 557. 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

Table 558. 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

Table 559. 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

Table 560. 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

Table 561. 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

Table 562. 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

Table 563. 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

Table 564. 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

Table 565. 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

Table 566. 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

Table 567. 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

Table 568. 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

Table 569. 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

Table 570. 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

Table 571. 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

Table 572. 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

Table 573. 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

Table 574. 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

Table 575. 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

Table 576. 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

Table 577. 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

Table 578. 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

Table 579. 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

Table 580. 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

Table 581. 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

Table 582. 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

Table 583. 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

Table 584. 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

Table 585. 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

Table 586. 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

Table 587. 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

Table 588. 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

Table 589. 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

Table 590. 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

Table 591. 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

Table 592. 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

Table 593. 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

Table 594. 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

Table 595. 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

Table 596. 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

Table 597. 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

Table 598. 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

Table 599. 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

Table 600. 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

Table 601. 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

Table 602. 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

Table 603. 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

Table 604. 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

Table 605. 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

Table 606. 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

Table 607. 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

Table 608. 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

Table 609. 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

Table 610. 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

Table 611. 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

Table 612. 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

Table 613. 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

Table 614. 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

Table 615. 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

Table 616. 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

Table 617. 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

Table 618. 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

Table 619. 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

Table 620. 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

Table 621. 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

Table 622. 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

Table 623. 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

Table 624. 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

Table 625. 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

Table 626. 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

Table 627. 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

Table 628. 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

Table 629. 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

Table 630. 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

Table 631. 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

Table 632. 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

Table 633. 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

Table 634. 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

Table 635. 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

Table 636. 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

Table 637. 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

Table 638. 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

Table 639. 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

Table 640. 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

Table 641. 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

Table 642. 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

Table 643. 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

Table 644. 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

Table 645. 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

Table 646. 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

Table 647. 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

Table 648. 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

Table 649. 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

Table 650. 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

Table 651. 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

Table 652. 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

Table 653. 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

Table 654. 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

Table 655. 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

Table 656. 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

Table 657. 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

Table 658. 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

Table 659. 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

Table 660. 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

Table 661. 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

Table 662. 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

Table 663. 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

Table 664. 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

Table 665. 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

Table 666. 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

Table 667. 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

Table 668. 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

Table 669. 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

Table 670. 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

Table 671. 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

Table 672. 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

Table 673. 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

Table 674. 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 https://github.com/MISP/misp-galaxy/blob/master/clusters/course of action.json[**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]].

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]]

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]]

.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.

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]]

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]]

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]]

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.

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]]

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.

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.

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]]

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]]

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.

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]]

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]]

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]]

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]]

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]]

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]]

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.

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]]

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]]

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]]

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.

AppleScript Mitigation

Require that all AppleScript be signed by a trusted developer ID before being executed - this will prevent random AppleScript code from executing.

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.

Input Prompt Mitigation

Users need to be trained to know which programs ask for permission and why. Follow mitigation recommendations for [[Technique/T1155|AppleScript]].

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]]

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.

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]]

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]]

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]]

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.

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]]

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.

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]]

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]].

Source Mitigation

Due to potential legitimate uses of source commands, it's may be difficult to mitigate use of this technique.

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".

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.

LC_MAIN Hijacking Mitigation

Enforce valid digital signatures for signed code on all applications and only trust applications with signatures from trusted parties.

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.

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]]

Trap Mitigation

Due to potential legitimate uses of trap commands, it's may be difficult to mitigate use of this technique.

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]]

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]]

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]]

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]]

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]]

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]]

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.

Rc.common Mitigation

Limit privileges of user accounts so only authorized users can edit the rc.common file.

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]]

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]]

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]]

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]]

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]]

Scripting Mitigation

Turn off unused features or restrict access to scripting engines such as VBScript or scriptable administration frameworks such as PowerShell.

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]]

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]]

Hidden Window Mitigation

Whitelist programs that are allowed to have this plist tag. All other programs should be considered suspicious.

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]]

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.

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.

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]]

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]]

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.

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.

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]]

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]]

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]]

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]]

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]]

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]]

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]]

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]]

Launch Agent Mitigation

Restrict user's abilities to create Launch Agents with group policy.

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.

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]]

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.

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.

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]]

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.

Launch Daemon Mitigation

Limit privileges of user accounts and remediate Privilege Escalation vectors so only authorized administrators can create new Launch Daemons.

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.

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]]

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]]

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.

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]]

Disabling Security Tools Mitigation

Ensure proper process, registry, and file permissions are in place to prevent adversaries from disabling or interfering with security services.

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]]

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]]

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]]

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]]

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]]

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]]

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]]

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]]

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]]

Plist Modification Mitigation

Prevent plist files from being modified by users by making them read-only.

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.

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]]

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]]

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.

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.

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]]

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]]

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]]

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]]

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]]

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]]

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.

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]].

Launchctl Mitigation

Prevent users from installing their own launch agents or launch daemons and instead require them to be pushed out by group policy.

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]]

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]]

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]]

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]]

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]]

Hypervisor Mitigation

Prevent adversary access to privileged accounts necessary to install a hypervisor.

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]]

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]]

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]]

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.

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]]

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]]

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]]

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]]

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]]

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.

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]].

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]]

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]]

Space after Filename Mitigation

Prevent files from having a trailing space after the extension.

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.

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.

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]]

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]]

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]]

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]]

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]]

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]]

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]]

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]]

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]]

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]]

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.

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]]

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]]

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]]

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.

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.

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]]

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>.

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]]

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.

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]]

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.

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]]

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]]

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]]

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]]

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]]

intrusion Set

Name of ATT&CK Group.

intrusion Set is a cluster galaxy available in JSON format at https://github.com/MISP/misp-galaxy/blob/master/clusters/intrusion set.json[**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]]

Poseidon Group is also known as:

- Poseidon Group

Table 675. 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]]

Group5 is also known as:

- Group5

Table 676. 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]]

PittyTiger is also known as:

- PittyTiger

Table 677. 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]]

admin@338 is also known as:

- admin@338

Table 678. 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]]

RTM is also known as:

- RTM

Table 679. 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]]

APT16 is also known as:

- APT16

Table 680. 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]]

APT28 is also known as:

- APT28
- Sednit
- Sofacy
- Pawn Storm
- Fancy Bear
- STRONTIUM
- Tsar Team
- Threat Group-4127
- TG-4127

Table 681. 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]]

Winnti Group is also known as:

- Winnti Group
- Blackfly

Table 682. 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]]

Deep Panda is also known as:

- Deep Panda
- Shell Crew
- WebMasters
- KungFu Kittens

- PinkPanther
- Black Vine

Table 683. 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]]

Molerats is also known as:

- Molerats
- Gaza cybergang
- Operation Molerats

Table 684. 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]]

Strider is also known as:

- Strider
- ProjectSauron

Table 685. 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]]

Sandworm Team is also known as:

- Sandworm Team
- Quedagh

Table 686. 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]]

FIN6 is also known as:

- FIN6

Table 687. 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]]

Dust Storm is also known as:

- Dust Storm

Table 688. 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]]

Cleaver is also known as:

- Cleaver
- Threat Group 2889
- TG-2889

Table 689. 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]]

APT12 is also known as:

- APT12
- IXESHE
- DynCalc
- Numbered Panda

Table 690. 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]]

Moafee is also known as:

- Moafee

Table 691. 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]]

Threat Group-3390 is also known as:

- Threat Group-3390
- TG-3390
- Emissary Panda
- BRONZE UNION

Table 692. 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]]

DragonOK is also known as:

- DragonOK

Table 693. 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]]

APT1 is also known as:

- APT1
- Comment Crew
- Comment Group
- Comment Panda

Table 694. 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]]

Taidoor is also known as:

- Taidoor

Table 695. 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]]

Night Dragon is also known as:

- Night Dragon

Table 696. 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]]

Naikon is also known as:

- Naikon

Table 697. 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]]

Ke3chang is also known as:

- Ke3chang

Table 698. 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]]

Patchwork is also known as:

- Patchwork
- Dropping Elephant
- Chinastrats

Table 699. 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]]

APT30 is also known as:

- APT30

Table 700. 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]]

MONSOON is also known as:

- MONSOON
- Operation Hangover

Table 701. 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]]

APT17 is also known as:

- APT17
- Deputy Dog

Table 702. Table References

Links
https://attack.mitre.org/wiki/Group/G0025
https://www2.fireeye.com/rs/fireye/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]]

FIN7 is also known as:

- FIN7

Table 703. 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]]

APT3 is also known as:

- APT3
- Gothic Panda
- Pirpi
- UPS Team
- Buckeye
- Threat Group-0110
- TG-0110

Table 704. 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]]

GCMAN is also known as:

- GCMAN

Table 705. 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]]

Lazarus Group is also known as:

- Lazarus Group
- HIDDEN COBRA
- Guardians of Peace

Table 706. 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]]

Lotus Blossom is also known as:

- Lotus Blossom
- Spring Dragon

Table 707. 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]]

Equation is also known as:

- Equation

Table 708. 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]]

Darkhotel is also known as:

- Darkhotel

Table 709. 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]]

OilRig is also known as:

- OilRig

Table 710. 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]]

Dragonfly is also known as:

- Dragonfly
- Energetic Bear

Table 711. 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]]

Suckfly is also known as:

- Suckfly

Table 712. 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]]

Stealth Falcon is also known as:

- Stealth Falcon

Table 713. 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]]

Scarlet Mimic is also known as:

- Scarlet Mimic

Table 714. 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]]

Threat Group-1314 is also known as:

- Threat Group-1314
- TG-1314

Table 715. 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]]

Turla is also known as:

- Turla
- Waterbug

Table 716. 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]]

APT29 is also known as:

- APT29
- The Dukes
- Cozy Bear

Table 717. 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]]

FIN10 is also known as:

- FIN10

Table 718. 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]]

menuPass is also known as:

- menuPass
- Stone Panda
- APT10
- Red Apollo
- CVNX

Table 719. 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]]

Putter Panda is also known as:

- Putter Panda
- APT2
- MSUpdater

Table 720. 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]]

Axiom is also known as:

- Axiom
- Group 72

Table 721. 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]]

Carbanak is also known as:

- Carbanak
- Anunak

Table 722. 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]]

APT18 is also known as:

- APT18
- TG-0416
- Dynamite Panda
- Threat Group-0416

Table 723. 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]]

APT32 is also known as:

- APT32
- OceanLotus Group

Table 724. 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]]

Gamaredon Group is also known as:

- Gamaredon Group

Table 725. 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

OLDBAIT is also known as:

- OLDBAIT
- Sasfis

Table 726. 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]]

Table 727. 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

CosmicDuke is also known as:

- CosmicDuke
- TinyBaron
- BotgenStudios
- NemesisGemina

Table 728. 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]]

Table 729. 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]]

Table 730. Table References

Links
https://attack.mitre.org/wiki/Software/S0035
https://www2.fireeye.com/rs/fireye/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]]

Table 731. 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

TEXTMATE is also known as:

- TEXTMATE
- DNSMessenger

Table 732. 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

Net Crawler is also known as:

- Net Crawler
- NetC

Table 733. 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

BlackEnergy is also known as:

- BlackEnergy
- Black Energy

Table 734. 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]]

Table 735. 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]]

Table 736. 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

Backdoor.Oldrea is also known as:

- Backdoor.Oldrea
- Havex

Table 737. 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

ChChes is also known as:

- ChChes
- Scorpion
- HAYMAKER

Table 738. 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]]

Table 739. 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]]

Table 740. 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]]

Table 741. 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

Downdelph is also known as:

- Downdelph
- Delphacy

Table 742. 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]]

Table 743. 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]]

Table 744. 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

HDoor is also known as:

- HDoor
- Custom HDoor

Table 745. 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]].

Table 746. 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]]

Table 747. 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

BACKSPACE is also known as:

- BACKSPACE
- Lecna

Table 748. 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]]

Table 749. 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

CloudDuke is also known as:

- CloudDuke
- MiniDionis
- CloudLook

Table 750. 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]]

Table 751. 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]]

Table 752. 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]]

Table 753. 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]]

Table 754. 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]]

Table 755. 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]]

Table 756. 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]]

Table 757. 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]]

Table 758. 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]]

Table 759. 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]]

Table 760. 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

PlugX is also known as:

- PlugX
- Sogu
- Kaba

Table 761. 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]]

Table 762. 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]]

Table 763. 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]]

Table 764. 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]]

Table 765. 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

Crimson is also known as:

- Crimson
- MSIL/Crimson

Table 766. 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]]

Table 767. 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]]

Table 768. 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]]

Table 769. 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

HTTPBrowser is also known as:

- HTTPBrowser
- Token Control
- HttpDump

Table 770. 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

HAMMERTOSS is also known as:

- HAMMERTOSS
- HammerDuke
- NetDuke

Table 771. 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

PoisonIvy is also known as:

- PoisonIvy
- Poison Ivy

Table 772. 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

Carbanak is also known as:

- Carbanak
- Anunak

Table 773. 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]]

Table 774. 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]]

Table 775. 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

Flame is also known as:

- Flame
- Flamer
- sKyWIper

Table 776. 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]]

Table 777. 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

CozyCar is also known as:

- CozyCar
- CozyDuke
- CozyBear
- Cozer
- EuroAPT

Table 778. 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]]

Table 779. 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]]

Table 780. 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

XTunnel is also known as:

- XTunnel
- X-Tunnel
- XAPS

Table 781. 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]]

Table 782. 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

Sakula is also known as:

- Sakula
- Sakurel
- VIPER

Table 783. 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]]

Table 784. 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]]

Table 785. 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]]

Table 786. 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

USBStealer is also known as:

- USBStealer
- USB Stealer
- Win32/USBStealer

Table 787. 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]]

Table 788. 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]]

Table 789. 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]]

Table 790. 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]]

Table 791. 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]]

Table 792. 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]]

Table 793. 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

SHOTPUT is also known as:

- SHOTPUT
- Backdoor.APT.CookieCutter
- Pirpi

Table 794. 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]]

Table 795. 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]]

Table 796. 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

CHOPSTICK is also known as:

- CHOPSTICK
- SPLM
- Xagent
- X-Agent
- webhp

Table 797. 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]]

Table 798. 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]]

Table 799. 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

Elise is also known as:

- Elise
- BKDR_ESILE
- Page

Table 800. 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]]

Table 801. 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]]

Table 802. 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

POWERSOURCE is also known as:

- POWERSOURCE
- DNSMessenger

Table 803. 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]]

Table 804. 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

Zeroaccess is also known as:

- Zeroaccess
- Trojan.Zeroaccess

Table 805. 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.

Table 806. 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

Shamoon is also known as:

- Shamoon
- Disttrack

Table 807. 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]]

Table 808. 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]]

Table 809. 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]]

Table 810. 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]]

Table 811. 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]]

Table 812. 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]]

Table 813. 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

CORESHELL is also known as:

- CORESHELL
- SOURFACE

Table 814. 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

Remsec is also known as:

- Remsec
- Backdoor.Remsec

- ProjectSauron

Table 815. 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]]

Table 816. 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]]

Table 817. 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

SeaDuke is also known as:

- SeaDuke
- SeaDaddy
- SeaDesk

Table 818. 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]]

Table 819. 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

ADVSTORESHELL is also known as:

- ADVSTORESHELL
- NETUI
- EVILTOSS
- AZZY
- Sedreco

Table 820. 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]]

Table 821. 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]]

Table 822. 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]]

Table 823. 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

P2P ZeuS is also known as:

- P2P ZeuS
- Peer-to-Peer ZeuS
- Gameover ZeuS

Table 824. 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]]

Table 825. 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]]

Table 826. 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

RedLeaves is also known as:

- RedLeaves
- BUGJUICE

Table 827. 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]]

Table 828. 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]]

Table 829. 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]]

Table 830. 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]]

Table 831. 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]]

Table 832. 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]]

Table 833. 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

ASPXSpy is also known as:

- ASPXSpy
- ASPXTool

Table 834. 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]]

Table 835. 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

GLOOXMAIL is also known as:

- GLOOXMAIL
- Trojan.GTALK

Table 836. 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]]

Table 837. 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

Miner-C is also known as:

- Miner-C
- Mal/Miner-C
- PhotoMiner

Table 838. 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]]

Table 839. 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

DustySky is also known as:

- DustySky
- NeD Worm

Table 840. 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

BUBBLEWRAP is also known as:

- BUBBLEWRAP
- Backdoor.APT.FakeWinHTTPHelper

Table 841. 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]]

Table 842. 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]]

Table 843. 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

Nidiran is also known as:

- Nidiran
- Backdoor.Nidiran

Table 844. 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]]

Table 845. 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]]

Table 846. 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]]

Table 847. 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]]

Table 848. 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]]

Table 849. 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]]

Table 850. 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]]

Table 851. Table References

Links
https://attack.mitre.org/wiki/Software/S0069
https://www2.fireeye.com/rs/fireye/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]]

Table 852. 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

Epic is also known as:

- Epic
- Tavdig
- Wipbot
- WorldCupSec
- TadjMakhal

Table 853. 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

Lurid is also known as:

- Lurid
- Enfal

Table 854. 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]]

Table 855. 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

JHUHUGIT is also known as:

- JHUHUGIT
- Seduploader
- JKEYSKW
- Sednit
- GAMEFISH

Table 856. 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]]

Table 857. 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

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

at is also known as:

- at
- at.exe

Table 858. 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

route is also known as:

- route
- route.exe

Table 859. 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]]

Table 860. 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

Windows Credential Editor is also known as:

- Windows Credential Editor
- WCE

Table 861. 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

schtasks is also known as:

- schtasks

- schtasks.exe

Table 862. 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]]

Table 863. 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]]

Table 864. 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]]

Table 865. 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]]

Table 866. 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

Systeminfo is also known as:

- systeminfo.exe
- Systeminfo

Table 867. 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

netsh is also known as:

- netsh
- netsh.exe

Table 868. 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

dsquery is also known as:

- dsquery
- dsquery.exe

Table 869. 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]]

Table 870. 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

Ping is also known as:

- ping.exe
- Ping

Table 871. 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]]

Table 872. 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]]

Table 873. 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]]

Table 874. 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

FTP is also known as:

- FTP
- ftp.exe

Table 875. 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

ipconfig is also known as:

- ipconfig
- ipconfig.exe

Table 876. 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

certutil is also known as:

- certutil
- certutil.exe

Table 877. 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

nbtstat is also known as:

- nbtstat
- nbtstat.exe

Table 878. 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

HTRAN is also known as:

- HTRAN
- HUC Packet Transmit Tool

Table 879. 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

netstat is also known as:

- netstat
- netstat.exe

Table 880. 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]]

Table 881. 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]]

Table 882. 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

Net is also known as:

- Net
- net.exe

Table 883. 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]]

Table 884. 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

Arp is also known as:

- Arp
- arp.exe

Table 885. 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

cmd is also known as:

- cmd
- cmd.exe

Table 886. 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.

Table 887. 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

Reg is also known as:

- Reg
- reg.exe

Table 888. 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 https://github.com/MISP/misp-galaxy/blob/master/clusters/preventive measure.json[**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

Table 889. 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

Table 890. 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

Table 891. 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

Filter Attachments Level 2

Filter the following attachments on your mail gateway: (Filter expression of Level 1 plus) .doc, .xls, .rtf, .docm, .xlsm, .pptm

Restrict program execution

Block all program executions from the %LocalAppData% and %AppData% folder

Table 892. 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")

Table 893. 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

Table 894. 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.

Restrict Workstation Communication

Activate the Windows Firewall to restrict workstation to workstation communication

Sandboxing Email Input

Using sandbox that opens email attachments and removes attachments based on behavior analysis

Execution Prevention

Software that allows to control the execution of processes - sometimes integrated in Antivirus software Free: AntiHook, ProcessGuard, System Safety Monitor

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

Table 895. 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

Table 896. 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)

Table 897. 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

Table 898. 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

Table 899. Table References

Links
https://twitter.com/JohnLaTwC/status/799792296883388416

Blacklist-phone-numbers

Filter the numbers at phone routing level including PABX

Table 900. 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..

Table 901. 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..

Table 902. 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..

Table 903. 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..

Table 904. 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..

Table 905. 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..

Vortex Ransomware is also known as:

- Ŧl ter r rɛ

Table 906. 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..

Table 907. 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..

Table 908. 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..

Table 909. 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

Table 910. 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..

Table 911. 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..

Table 912. 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

Table 913. 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

Table 914. 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..

Turkish FileEncryptor Ransomware is also known as:

- Fake CTB-Locker

Table 915. 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

Table 916. 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..

Table 917. 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

Table 918. 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..

Table 919. 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..

Table 920. 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

Table 921. 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..

Table 922. 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..

Table 923. 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..

Table 924. 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..

Table 925. 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

Table 926. 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..

Table 927. 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..

Table 928. 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

Table 929. 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

Table 930. 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..

Table 931. 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

Table 932. 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

Table 933. 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

Table 934. 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..

Table 935. 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..

Table 936. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/cryptconsole-2-ransomware.html

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

BarRax Ransomware is also known as:

- BarRaxCrypt Ransomware

Table 937. 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..

Table 938. 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..

UserFilesLocker Ransomware is also known as:

- CzechoSlovak Ransomware

Table 939. 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!!!!

Table 940. 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..

Table 941. 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..

PleaseRead Ransomware is also known as:

- VHDLocker Ransomware

Table 942. 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..

Table 943. 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..

Fake Locky Ransomware is also known as:

- Locky Impersonator Ransomware

Table 944. 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.

Table 945. 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"

Table 946. 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..

Table 947. 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..

Table 948. 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..

Table 949. 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..

Table 950. 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.

Table 951. 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)

Table 952. 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

Table 953. 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.

Table 954. 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.

Table 955. 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.

Table 956. 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

Table 957. 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

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

Table 958. 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

Table 959. 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.

Table 960. 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.

Table 961. 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

Table 962. 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

Table 963. 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!!!!

DN is also known as:

- Fake

Table 964. 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..

Table 965. 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

Table 966. 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..

Havoc is also known as:

- HavocCrypt Ransomware

Table 967. 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.

Table 968. 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

Kaandsona Ransomware is also known as:

- RansomTroll Ransomware
- Käändsõna Ransomware

Table 969. 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

Table 970. 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..

NMoreia 2.0 Ransomware is also known as:

- HakunaMatataRansomware

Table 971. 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)

Table 972. 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

Table 973. 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.

Table 974. 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..

Table 975. 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.

Table 976. 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.

Table 977. 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..

Table 978. 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..

DynA-Crypt Ransomware is also known as:

- DynA CryptoLocker Ransomware

Table 979. 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..

Serpent 2017 Ransomware is also known as:

- Serpent Danish Ransomware

Table 980. 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..

Table 981. 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..

Cyber Drill Exercise is also known as:

- Ransomuhahawhere

Table 982. 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.

Table 983. 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.

Table 984. 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.

Table 985. 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

Evil Ransomware is also known as:

- File0Locked KZ Ransomware

Table 986. 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.

Ocelot Ransomware (FAKE RANSOMWARE) is also known as:

- Ocelot Locker Ransomware

Table 987. 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

SkyName Ransomware is also known as:

- Blablabla Ransomware

Table 988. 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

MafiaWare Ransomware is also known as:

- Depsex Ransomware

Table 989. 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.

Globe3 Ransomware is also known as:

- Purge Ransomware

Table 990. 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

BleedGreen Ransomware is also known as:

- FireCrypt Ransomware

Table 991. 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)

Table 992. 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.

Table 993. 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..

Table 994. 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.

Table 995. 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

Table 996. 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..

Table 997. 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.

Table 998. 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..

Table 999. 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.

Table 1000. 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.

Table 1001. 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.

Table 1002. 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.

Merry Christmas is also known as:

- Merry X-Mas
- MRCR

Table 1003. 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.

Table 1004. 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.

Table 1005. 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.

Table 1006. 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..

Table 1007. 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.

Table 1008. 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.

Table 1009. 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

KoKoKrypt Ransomware is also known as:

- KokoLocker Ransomware

Table 1010. 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

Table 1011. 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..

PClock4 Ransomware is also known as:

- PClock SysGop Ransomware

Table 1012. 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.

Table 1013. 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

Table 1014. 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.

CryptoLocker3 Ransomware is also known as:

- Fake CryptoLocker

Table 1015. 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.

Table 1016. 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.

Table 1017. 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

EnkripsiPC Ransomware is also known as:

- IDRANSOMv3
- Manifestus

Table 1018. 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.

Table 1019. 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.

Table 1020. 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

Table 1021. 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..

Table 1022. 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

Table 1023. 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.

Fake Globe Ransomware is also known as:

- Globe Imposter

- GlobeImposter

Table 1024. 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

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…

Table 1025. 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.

Table 1026. 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).

Table 1027. 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

Table 1028. 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.

Table 1029. 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.

Table 1030. 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.

Table 1031. 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

Table 1032. 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.

Table 1033. 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!!!!!!!

Table 1034. 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

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

Table 1035. 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…

Table 1036. 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..

Table 1037. 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..

Table 1038. 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

Table 1039. 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.

Table 1040. 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...

Table 1041. 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...

Table 1042. 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.

SQ_ Ransomware is also known as:

- VO_ Ransomware

Table 1043. 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...

Matrix is also known as:

- Malta Ransomware

Table 1044. 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

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..

Table 1045. 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

Table 1046. 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

Table 1047. 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..

Table 1048. 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]

Table 1049. 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..

Table 1050. 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..

Table 1051. 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

Table 1052. 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

Table 1053. 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..

Crypute Ransomware is also known as:

- m0on Ransomware

Table 1054. 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..

NMoreira Ransomware is also known as:

- Fake Maktub Ransomware

Table 1055. 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.

Table 1056. 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

Table 1057. 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

Nagini Ransomware is also known as:

- Voldemort Ransomware

Table 1058. 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..

Table 1059. 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..

Chip Ransomware is also known as:

- ChipLocker Ransomware

Table 1060. 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

Table 1061. 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/

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..

Table 1062. 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..

CryptoLuck Ransomware is also known as:

- YafunnLocker

Table 1063. 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..

Crypton Ransomware is also known as:

- Nemesis
- X3M

Table 1064. 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

Table 1065. 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..

Table 1066. 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

PClock3 Ransomware is also known as:

- PClock SuppTeam Ransomware
- WinPlock
- CryptoLocker clone

Table 1067. 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..

Kolobo Ransomware is also known as:

- Kolobocheg Ransomware

Table 1068. 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..

PaySafeGen (German) Ransomware is also known as:

- Paysafecard Generator 2016

Table 1069. 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.

Table 1070. 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..

Table 1071. 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

Table 1072. 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

PayDOS Ransomware is also known as:

- Serpent Ransomware

Table 1073. 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..

Table 1074. 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..

Table 1075. 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..

Table 1076. 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..

BTCLocker Ransomware is also known as:

- BTC Ransomware

Table 1077. 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

Table 1078. 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..

Table 1079. 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..

Encryptss77 Ransomware is also known as:

- SFX Monster Ransomware

Table 1080. 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..

Table 1081. 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..

Table 1082. 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..

Table 1083. 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..

Table 1084. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/rotorcrypt-ransomware.html

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.

Table 1085. 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..

Table 1086. 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..

JackPot Ransomware is also known as:

- Jack.Pot Ransomware

Table 1087. 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

Table 1088. 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..

Table 1089. 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..

Table 1090. 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..

Table 1091. 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..

Table 1092. 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

Table 1093. 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..

Table 1094. 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

Hucky Ransomware is also known as:

- Hungarian Locky Ransomware

Table 1095. 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..

Table 1096. 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

Table 1097. 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..

Table 1098. 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..

Table 1099. 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

Table 1100. 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..

Table 1101. 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

JapanLocker Ransomware is also known as:

- SHC Ransomware

- SHCLocker
- SyNcryption

Table 1102. 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

Table 1103. 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..

Table 1104. 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

Table 1105. 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

Table 1106. 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..

Windows_Security Ransonware is also known as:

- WS Go Ransonware
- Trojan.Encoder.6491

Table 1107. 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..

Table 1108. 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

Table 1109. 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..

Table 1110. 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...

Deadly Ransomware is also known as:

- Deadly for a Good Purpose Ransomware

Table 1111. 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..

Table 1112. 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..

Globe2 Ransomware is also known as:

- Purge Ransomware

Table 1113. 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..

Table 1114. 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..

Table 1115. 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

Table 1116. 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.

WannaCry is also known as:

- WannaCrypt
- WannaCry
- WanaCrypt0r
- WCrypt
- WCRY

Table 1117. Table References

Links
https://gist.github.com/rain-1/989428fa5504f378b993ee6efbc0b168

.CryptoHasYou.

Ransomware

Table 1118. Table References

Links
http://www.nyxbone.com/malware/CryptoHasYou.html

777

Ransomware

777 is also known as:

- Sevleg

Table 1119. Table References

Links
https://decrypter.emsisoft.com/777

7ev3n

Ransomware

7ev3n is also known as:

- 7ev3n-HONE$T

Table 1120. 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

Table 1121. Table References

Links
http://www.bleepingcomputer.com/forums/t/614025/8lock8-help-support-topic-8lock8-read-ittxt/

AiraCrop

Ransomware related to TeamXRat

Table 1122. Table References

Links

https://twitter.com/PolarToffee/status/796079699478900736

Al-Namrood

Ransomware

Table 1123. Table References

Links
https://decrypter.emsisoft.com/al-namrood

ALFA Ransomware

Ransomware Made by creators of Cerber

Table 1124. Table References

Links
http://www.bleepingcomputer.com/news/security/new-alfa-or-alpha-ransomware-from-the-same-devs-as-cerber/

Alma Ransomware

Ransomware

Table 1125. Table References

Links

https://cta-service-cms2.hubspot.com/ctas/v2/public/cs/c/?cta_guid=d4173312-989b-4721-ad00-8308fff353b3&placement_guid=22f2fe97-c748-4d6a-9e1e-ba3fb1060abe&portal_id=326665&redirect_url=APefjpGnqFjmP_xzeUZ1Y55ovglY1y1ch7CgMDLit5GTHcW9N0ztpnIE-ZReqqv8MDj687_4Joou7Cd2rSx8-De8uhFQAD_Len9QpT7Xvu8neW5drkdtTPV7hAaou0osAi2O61dizFXibewmpO60UUCd5OazCGz1V6yT_3UFMgL0x9S1VeOvoL_ucuER8g2H3f1EfbtYBw5QFWeUmrjk-9dGzOGspyn303k9XagBtF3SSX4YWSyuEs03Vq7Fxb04KkyKc4GJx-igK98Qta8iMafUam8ikg8XKPkob0FK6Pe-wRZ0QVWIIkM&hsutk=34612af1cd87864cf7162095872571d1&utm_referrer=https%3A%2F%2Finfo.phishlabs.com%2Fblog%2Falma-ransomware-analysis-of-a-new-ransomware-threat-and-a-decrypter&canon=https%3A%2F%2Finfo.phishlabs.com%2Fblog%2Falma-ransomware-analysis-of-a-new-ransomware-threat-and-a-decrypter&amp;hstc=61627571.34612af1cd87864cf7162095872571d1.1472135921345.1472140656779.1472593507113.3&hssc=61627571.1.1472593507113&hsfp=1114323283[<a href="https://cta-service-cms2.hubspot.com/ctas/v2/public/cs/c/?cta_guid=d4173312-989b-4721-ad00-8308fff353b3&placement_guid=22f2fe97-c748-4d6a-9e1e-ba3fb1060abe&portal_id=326665&redirect_url=APefjpGnqFjmP_xzeUZ1Y55ovglY1y1ch7CgMDLit5GTHcW9N0ztpnIE-ZReqqv8MDj687_4Joou7Cd2rSx8-De8uhFQAD_Len9QpT7Xvu8neW5drkdtTPV7hAaou0osAi2O61dizFXibewmpO60UUCd5OazCGz1V6yT_3UFMgL0x9S1VeOvoL_ucuER8g2H3f1EfbtYBw5QFWeUmrjk-9dGzOGspyn303k9XagBtF3SSX4YWSyuEs03Vq7Fxb04KkyKc4GJx-igK98Qta8iMafUam8ikg8XKPkob0FK6Pe-wRZ0QVWIIkM&hsutk=34612af1cd87864cf7162095872571d1&utm_referrer=https%3A%2F%2Finfo.phishlabs.com%2Fblog%2Falma-ransomware-analysis-of-a-new-ransomware-threat-and-a-decrypter&canon=https%3A%2F%2Finfo.phishlabs.com%2Fblog%2Falma-ransomware-analysis-of-a-new-ransomware-threat-and-a-decrypter&" class="bare">https://cta-service-cms2.hubspot.com/ctas/v2/public/cs/c/?cta_guid=d4173312-989b-4721-ad00-8308fff353b3&placement_guid=22f2fe97-c748-4d6a-9e1e-ba3fb1060abe&portal_id=326665&redirect_url=APefjpGnqFjmP_xzeUZ1Y55ovglY1y1ch7CgMDLit5GTHcW9N0ztpnIE-ZReqqv8MDj687_4Joou7Cd2rSx8-De8uhFQAD_Len9QpT7Xvu8neW5drkdtTPV7hAaou0osAi2O61dizFXibewmpO60UUCd5OazCGz1V6yT_3UFMgL0x9S1VeOvoL_ucuER8g2H3f1EfbtYBw5QFWeUmrjk-9dGzOGspyn303k9XagBtF3SSX4YWSyuEs03Vq7Fxb04KkyKc4GJx-igK98Qta8iMafUam8ikg8XKPkob0FK6Pe-wRZ0QVWIIkM&hsutk=34612af1cd87864cf7162095872571d1&utm_referrer=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

Alpha Ransomware is also known as:

- AlphaLocker

Table 1126. 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

Table 1127. Table References

Links
https://twitter.com/benkow_/status/747813034006020096

AngleWare

Ransomware

Table 1128. Table References

Links
https://twitter.com/BleepinComputer/status/844531418474708993

Anony

Ransomware Based on HiddenTear

Anony is also known as:

- ngocanh

Table 1129. 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

Apocalypse is also known as:

- Fabiansomeware

Table 1130. 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

Table 1131. Table References

Links
http://decrypter.emsisoft.com/download/apocalypsevm

AutoLocky

Ransomware

Table 1132. Table References

Links
https://decrypter.emsisoft.com/autolocky

Aw3s0m3Sc0t7

Ransomware

Table 1133. Table References

Links
https://twitter.com/struppigel/status/828902907668000770

BadBlock

Ransomware

Table 1134. 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

Table 1135. 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

Bandarchor is also known as:

- Rakhni

Table 1136. 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

Bart is also known as:

- BaCrypt

Table 1137. 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.

Table 1138. Table References

Links
https://noransom.kaspersky.com/

BitStak

Ransomware

Table 1139. Table References

Links
https://download.bleepingcomputer.com/demonslay335/BitStakDecrypter.zip

BlackShades Crypter

Ransomware

BlackShades Crypter is also known as:

- SilentShade

Table 1140. Table References

Links
http://nyxbone.com/malware/BlackShades.html

Blocatto

Ransomware Based on HiddenTear

Table 1141. 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

Booyah is also known as:

- Salami

Brazilian

Ransomware Based on EDA2

Table 1142. Table References

Links
http://www.nyxbone.com/malware/brazilianRansom.html
http://www.nyxbone.com/images/articulos/malware/brazilianRansom/0.png

Brazilian Globe

Ransomware

Table 1143. Table References

Links
https://twitter.com/JakubKroustek/status/821831437884211201

BrLock

Ransomware

Table 1144. 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

BTCWare Related to / new version of CryptXXX

Ransomware

Table 1145. Table References

Links
https://twitter.com/malwrhunterteam/status/845199679340011520

Bucbi

Ransomware no file name change, no extension

Table 1146. 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

Central Security Treatment Organization

Ransomware

Table 1147. Table References

Links
http://www.bleepingcomputer.com/forums/t/625820/central-security-treatment-organization-ransomware-help-topic-cry-extension/

Cerber

Ransomware

Cerber is also known as:

- CRBR ENCRYPTOR

Table 1148. 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

Table 1149. 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

Table 1150. Table References

Links
https://twitter.com/JakubKroustek/status/794956809866018816

CoinVault

Ransomware CryptoGraphic Locker family. Has a GUI. Do not confuse with CrypVault!

Table 1151. Table References

Links
https://noransom.kaspersky.com/

Coverton

Ransomware

Table 1152. Table References

Links
http://www.bleepingcomputer.com/news/security/paying-the-coverton-ransomware-may-not-get-your-data-back/

Cryaki

Ransomware

Table 1153. Table References

Links
https://support.kaspersky.com/viruses/disinfection/8547

Crybola

Ransomware

Table 1154. Table References

Links
https://support.kaspersky.com/viruses/disinfection/8547

CryFile

Ransomware

Table 1155. Table References

Links
SHTODELATVAM.txt[SHTODELATVAM.txt]
Instructionaga.txt[Instructionaga.txt]

CryLocker

Ransomware Identifies victim locations w/Google Maps API

CryLocker is also known as:

- Cry
- CSTO
- Central Security Treatment Organization

Table 1156. 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

Table 1157. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/crypmic-ransomware-wants-to-follow-cryptxxx/

Crypren

Ransomware

Table 1158. 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

Table 1159. 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

Table 1160. Table References

Links
https://twitter.com/jiriatvirlab/status/802554159564062722

CryptFIle2

Ransomware

Table 1161. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/ransomware-explosion-continues-cryptflle2-brlock-mm-locker-discovered

CryptInfinite

Ransomware

Table 1162. Table References

Links
https://decrypter.emsisoft.com/

CryptoBit

Ransomware sekretzbel0ngt0us.KEY - do not confuse with CryptorBit.

Table 1163. 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

Table 1164. Table References

Links
https://decrypter.emsisoft.com/

CryptoFinancial

Ransomware

CryptoFinancial is also known as:

- Ranscam

Table 1165. 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

CryptoGraphic Locker

Ransomware Has a GUI. Subvariants: CoinVault BitCryptor

CryptoHost

Ransomware RAR's victim's files has a GUI

CryptoHost is also known as:

- Manamecrypt
- Telograph
- ROI Locker

Table 1166. Table References

Links
http://www.bleepingcomputer.com/news/security/cryptohost-decrypted-locks-files-in-a-password-protected-rar-file/

CryptoJoker

Ransomware

CryptoLocker

Ransomware no longer relevant

Table 1167. 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

Table 1168. Table References

Links
https://twitter.com/malwrhunterteam/status/839747940122001408

CryptoLocker 5.1

Ransomware

Table 1169. Table References

Links
https://twitter.com/malwrhunterteam/status/782890104947867649

CryptoMix

Ransomware

CryptoMix is also known as:

- Zeta

Table 1170. 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/

CryptoRansomeware

Ransomware

Table 1171. Table References

Links
https://twitter.com/malwrhunterteam/status/817672617658347521

CryptoRoger

Ransomware

Table 1172. Table References

Links
http://www.bleepingcomputer.com/news/security/new-ransomware-called-cryptoroger-that-appends-crptrgr-to-encrypted-files/

CryptoShadow

Ransomware

Table 1173. Table References

Links
https://twitter.com/struppigel/status/821992610164277248

CryptoShocker

Ransomware

Table 1174. Table References

Links

http://www.bleepingcomputer.com/forums/t/617601/cryptoshocker-ransomware-help-and-support-topic-locked-attentionurl/

CryptoTorLocker2015

Ransomware

Table 1175. Table References

Links
http://www.bleepingcomputer.com/forums/t/565020/new-cryptotorlocker2015-ransomware-discovered-and-easily-decrypted/

CryptoTrooper

Ransomware

Table 1176. Table References

Links
http://news.softpedia.com/news/new-open-source-linux-ransomware-shows-infosec-community-divide-508669.shtml

CryptoWall 1

Ransomware

CryptoWall 2

Ransomware

CryptoWall 3

Ransomware

Table 1177. 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

CryptXXX

Ransomware Comes with Bedep

CryptXXX is also known as:

- CryptProjectXXX

Table 1178. 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.

CryptXXX 2.0 is also known as:

- CryptProjectXXX

Table 1179. 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

CryptXXX 3.0 is also known as:

- UltraDeCrypter
- UltraCrypter

Table 1180. 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

Table 1181. 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

Table 1182. Table References

Links
http://www.bleepingcomputer.com/news/security/ctb-faker-ransomware-does-a-poor-job-imitating-ctb-locker/

CTB-Faker

Ransomware

CTB-Faker is also known as:

- Citroni

CTB-Locker WEB

Ransomware websites only

Table 1183. 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

CuteRansomware is also known as:

- my-Little-Ransomware

Table 1184. 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

Cyber SpLiTTer Vbs is also known as:

- CyberSplitter

Table 1185. Table References

Links
https://twitter.com/struppigel/status/778871886616862720
https://twitter.com/struppigel/status/806758133720698881

Death Bitches

Ransomware

Table 1186. Table References

Links
https://twitter.com/JaromirHorejsi/status/815555258478981121

DeCrypt Protect

Ransomware

Table 1187. Table References

Links
http://www.malwareremovalguides.info/decrypt-files-with-decrypt_mblblock-exe-decrypt-protect/

DEDCryptor

Ransomware Based on EDA2

Table 1188. 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

Table 1189. Table References

Links
https://twitter.com/struppigel/status/798573300779745281

DetoxCrypto

Ransomware - Based on Detox: Calipso, We are all Pokemons, Nullbyte

Table 1190. 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

Table 1191. Table References

Links
https://twitter.com/PolarToffee/status/829727052316160000

DirtyDecrypt

Ransomware

Table 1192. 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

Table 1193. 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

Table 1194. 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

Table 1195. Table References

Links
https://twitter.com/BleepinComputer/status/822500056511213568

Domino

Ransomware Based on Hidden Tear

Table 1196. 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

Table 1197. Table References

Links
https://www.bleepingcomputer.com/forums/t/643330/donotchange-ransomware-id-7es642406cry-do-not-change-the-file-namecryp/

DummyLocker

Ransomware

Table 1198. Table References

Links
https://twitter.com/struppigel/status/794108322932785158

DXXD

Ransomware

Table 1199. 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#

HiddenTear is also known as:

- Cryptear
- EDA2

Table 1200. Table References

Links
http://www.utkusen.com/blog/dealing-with-script-kiddies-cryptear-b-incident.html

EduCrypt

Ransomware Based on Hidden Tear

EduCrypt is also known as:

- EduCrypter

Table 1201. Table References

Links
http://www.filedropper.com/decrypter_1
https://twitter.com/JakubKroustek/status/747031171347910656

EiTest

Ransomware

Table 1202. Table References

Links
https://twitter.com/BroadAnalysis/status/845688819533930497
https://twitter.com/malwrhunterteam/status/845652520202616832

El-Polocker

Ransomware Has a GUI

El-Polocker is also known as:

- Los Pollos Hermanos

Encoder.xxxx

Ransomware Coded in GO

Encoder.xxxx is also known as:

- Trojan.Encoder.6491

Table 1203. 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

Enigma

Ransomware

Table 1204. Table References

Links
http://www.bleepingcomputer.com/news/security/the-enigma-ransomware-targets-russian-speaking-users/

Enjey

Ransomware Based on RemindMe

Table 1205. Table References

Links

https://twitter.com/malwrhunterteam/status/839022018230112256

Fairware

Ransomware Target Linux O.S.

Table 1206. Table References

Links
http://www.bleepingcomputer.com/news/security/new-fairware-ransomware-targeting-linux-computers/

Fakben

Ransomware Based on Hidden Tear

Table 1207. Table References

Links
https://blog.fortinet.com/post/fakben-team-ransomware-uses-open-source-hidden-tear-code

FakeCryptoLocker

Ransomware

Table 1208. Table References

Links
https://twitter.com/PolarToffee/status/812312402779836416

Fantom

Ransomware Based on EDA2

Fantom is also known as:

- Comrad Circle

Table 1209. Table References

Links
http://www.bleepingcomputer.com/news/security/fantom-ransomware-encrypts-your-files-while-pretending-to-be-windows-update/

FenixLocker

Ransomware

Table 1210. Table References

Links
https://decrypter.emsisoft.com/fenixlocker
https://twitter.com/fwosar/status/777197255057084416

FILE FROZR

Ransomware RaaS

Table 1211. Table References

Links
https://twitter.com/rommeljoven17/status/846973265650335744

FileLocker

Ransomware

Table 1212. Table References

Links
https://twitter.com/jiriatvirlab/status/836616468775251968

FireCrypt

Ransomware

Table 1213. Table References

Links
https://www.bleepingcomputer.com/news/security/firecrypt-ransomware-comes-with-a-ddos-component/

Flyper

Ransomware Based on EDA2 / HiddenTear

Table 1214. Table References

Links
https://twitter.com/malwrhunterteam/status/773771485643149312

Fonco

Ransomware contact email safefiles32@mail.ru also as prefix in encrypted file contents

FortuneCookie

Ransomware

Table 1215. Table References

Links
https://twitter.com/struppigel/status/842302481774321664

Free-Freedom

Ransomware Unlock code is: adam or adamdude9

Free-Freedom is also known as:

- Roga

Table 1216. Table References

Links
https://twitter.com/BleepinComputer/status/812135608374226944

FSociety

Ransomware Based on EDA2 and RemindMe

Table 1217. 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

Table 1218. Table References

Links
https://support.kaspersky.com/viruses/disinfection/8547

GhostCrypt

Ransomware Based on Hidden Tear

Table 1219. 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

Table 1220. Table References

Links
https://twitter.com/ni_fi_70/status/796353782699425792

Globe v1

Ransomware

Globe v1 is also known as:

- Purge

Table 1221. 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

Table 1222. Table References

Links
http://www.bleepingcomputer.com/forums/t/611342/gnl-locker-support-and-help-topic-locked-and-unlock-files-instructionshtml/

Gomasom

Ransomware

Table 1223. Table References

Links

https://decrypter.emsisoft.com/

Goopic

Ransomware

Table 1224. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/angler-shift-ek-landscape-new-crytpo-ransomware-activity/

Gopher

Ransomware OS X ransomware (PoC)

Hacked

Ransomware Jigsaw Ransomware variant

Table 1225. Table References

Links
https://twitter.com/demonslay335/status/806878803507101696

HappyDayzz

Ransomware

Table 1226. Table References

Links
https://twitter.com/malwrhunterteam/status/847114064224497666

Harasom

Ransomware

Table 1227. Table References

Links
https://decrypter.emsisoft.com/

HDDCryptor

Ransomware Uses https://diskcryptor.net for full disk encryption

HDDCryptor is also known as:

- Mamba

Table 1228. 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---"

Table 1229. Table References

Links
https://www.bleepingcomputer.com/news/security/heimdall-open-source-php-ransomware-targets-web-servers/

Help_dcfile

Ransomware

Herbst

Ransomware

Table 1230. Table References

Links
https://blog.fortinet.com/2016/06/03/cooking-up-autumn-herbst-ransomware

Hi Buddy!

Ransomware Based on HiddenTear

Table 1231. Table References

Links
http://www.nyxbone.com/malware/hibuddy.html

Hitler

Ransomware Deletes files

Table 1232. Table References

Links
http://www.bleepingcomputer.com/news/security/development-version-of-the-hitler-ransomware-discovered/
https://twitter.com/jiriatvirlab/status/825310545800740864

HolyCrypt

Ransomware

Table 1233. 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

Table 1234. Table References

Links
https://twitter.com/BleepinComputer/status/803288396814839808

HydraCrypt

Ransomware CrypBoss Family

Table 1235. Table References

Links
https://decrypter.emsisoft.com/
http://www.malware-traffic-analysis.net/2016/02/03/index2.html

iLock

Ransomware

Table 1236. Table References

Links
https://twitter.com/BleepinComputer/status/817085367144873985

iLockLight

Ransomware

International Police Association

Ransomware CryptoTorLocker2015 variant

Table 1237. Table References

Links
http://download.bleepingcomputer.com/Nathan/StopPirates_Decrypter.exe

iRansom

Ransomware

Table 1238. Table References

Links
https://twitter.com/demonslay335/status/796134264744083460

JagerDecryptor

Ransomware Prepends filenames

Table 1239. Table References

Links
https://twitter.com/JakubKroustek/status/757873976047697920

Jeiphoos

Ransomware Windows, Linux. Campaign stopped. Actor claimed he deleted the master key.

Jeiphoos is also known as:

- Encryptor RaaS
- Sarento

Table 1240. 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

Table 1241. Table References

Links
https://download.bleepingcomputer.com/demonslay335/DoNotOpenDecrypter.zip
https://twitter.com/BleepinComputer/status/822509105487245317

Jigsaw

Ransomware Has a GUI

Jigsaw is also known as:

- CryptoHitMan

Table 1242. 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

Table 1243. 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

KawaiiLocker

Ransomware

Table 1244. Table References

Links
https://safezone.cc/resources/kawaii-decryptor.195/

KeRanger

Ransomware OS X Ransomware

Table 1245. 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

Table 1246. Table References

Links
https://decrypter.emsisoft.com/

KEYHolder

Ransomware via remote attacker. tuyuljahat@hotmail.com contact address

Table 1247. Table References

Links
http://www.bleepingcomputer.com/forums/t/559463/keyholder-ransomware-support-and-help-topic-how-decryptgifhow-decrypthtml

KillerLocker

Ransomware Possibly Portuguese dev

Table 1248. Table References

Links
https://twitter.com/malwrhunterteam/status/782232299840634881

KimcilWare

Ransomware websites only

Table 1249. 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

Table 1250. 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

Kozy.Jozy is also known as:

- QC

Table 1251. 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

Table 1252. Table References

Links
https://twitter.com/demonslay335/status/746090483722686465

KryptoLocker

Ransomware Based on HiddenTear

LanRan

Ransomware Variant of open-source MyLittleRansomware

Table 1253. Table References

Links
https://twitter.com/struppigel/status/847689644854595584

LeChiffre

Ransomware Encrypts first 0x2000 and last 0x2000 bytes. Via remote attacker

Table 1254. 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

Table 1255. Table References

Links
https://twitter.com/JakubKroustek/status/842404866614038529

Linux.Encoder

Ransomware Linux Ransomware

Linux.Encoder is also known as:

- Linux.Encoder.{0,3}

Table 1256. Table References

Links
https://labs.bitdefender.com/2015/11/linux-ransomware-debut-fails-on-predictable-encryption-key/

LK Encryption

Ransomware Based on HiddenTear

Table 1257. Table References

Links
https://twitter.com/malwrhunterteam/status/845183290873044994

LLTP Locker

Ransomware Targeting Spanish speaking victims

Table 1258. Table References

Links
https://www.bleepingcomputer.com/news/security/new-lltp-ransomware-appears-to-be-a-rewritten-venus-locker/

Locker

Ransomware has GUI

Table 1259. Table References

Links
http://www.bleepingcomputer.com/forums/t/577246/locker-ransomware-support-and-help-topic/page-32#entry3721545

LockLock

Ransomware

Table 1260. Table References

Links
https://www.bleepingcomputer.com/forums/t/626750/locklock-ransomware-locklock-help-support/

Locky

Ransomware Affiliations with Dridex and Necurs botnets

Table 1261. 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

LowLevel04

Ransomware Prepends filenames

M4N1F3STO

Ransomware Does not encrypt Unlock code=suckmydicknigga

Table 1262. Table References

Links
https://twitter.com/jiriatvirlab/status/808015275367002113

Mabouia

Ransomware OS X ransomware (PoC)

MacAndChess

Ransomware Based on HiddenTear

Magic

Ransomware Based on EDA2

MaktubLocker

Ransomware

Table 1263. Table References

Links
https://blog.malwarebytes.org/threat-analysis/2016/03/maktub-locker-beautiful-and-dangerous/

MarsJoke

Ransomware

Table 1264. 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

Table 1265. Table References

Links
https://twitter.com/siri_urz/status/840913419024945152

Meteoritan

Ransomware

Table 1266. Table References

Links
https://twitter.com/malwrhunterteam/status/844614889620561924

MIRCOP

Ransomware Prepends files Demands 48.48 BTC

MIRCOP is also known as:

- Crypt888

Table 1267. 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

Mischa

Ransomware Packaged with Petya PDFBewerbungsmappe.exe

Mischa is also known as:

- "Petya’s little brother"

Table 1268. 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

MM Locker is also known as:

- Booyah

Table 1269. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/ransomware-explosion-continues-cryptflle2-brlock-mm-locker-discovered

Mobef

Ransomware

Mobef is also known as:

- Yakes
- CryptoBit

Table 1270. 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

Table 1271. Table References

Links
https://twitter.com/malwrhunterteam/status/844826339186135040

N-Splitter

Ransomware Russian Koolova Variant

Table 1272. 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"

Table 1273. Table References

Links
https://twitter.com/demonslay335/status/790608484303712256
https://twitter.com/demonslay335/status/831891344897482754

NanoLocker

Ransomware no extension change, has a GUI

Table 1274. Table References

Links
http://github.com/Cyberclues/nanolocker-decryptor

Nemucod

Ransomware 7zip (a0.exe) variant cannot be decrypted Encrypts the first 2048 Bytes

Table 1275. 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

Netix is also known as:

- RANSOM_NETIX.A

Table 1276. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/netflix-scam-delivers-ransomware/

Nhtnwcuf

Ransomware Does not encrypt the files / Files are destroyed

Table 1277. Table References

Links
https://twitter.com/demonslay335/status/839221457360195589

NMoreira

Ransomware

NMoreira is also known as:

- XRatTeam
- XPan

Table 1278. Table References

Links
https://decrypter.emsisoft.com/nmoreira
https://twitter.com/fwosar/status/803682662481174528

NoobCrypt

Ransomware

Table 1279. 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

Nullbyte

Ransomware

Table 1280. 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

Table 1281. 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

Offline ransomware is also known as:

- Vipasana
- Cryakl

Table 1282. 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

OMG! Ransomware is also known as:

- GPCode

Operation Global III

Ransomware Is a file infector (virus)

Table 1283. Table References

Links
http://news.thewindowsclub.com/operation-global-iii-ransomware-decryption-tool-released-70341/

Owl

Ransomware

Owl is also known as:

- CryptoWire

Table 1284. Table References

Links
https://twitter.com/JakubKroustek/status/842342996775448576

PadCrypt

Ransomware has a live support chat

Table 1285. 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

Table 1286. Table References

Links
https://twitter.com/BleepinComputer/status/811635075158839296

Patcher

Ransomware Targeting macOS users

Table 1287. 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

Petya is also known as:

- Goldeneye

Table 1288. 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"

Table 1289. 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

Table 1290. Table References

Links
http://download.bleepingcomputer.com/BloodDolly/JuicyLemonDecoder.zip

PokemonGO

Ransomware Based on Hidden Tear

Table 1291. 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

Table 1292. Table References

Links
https://support.kaspersky.com/8547
https://securelist.com/blog/research/76182/polyglot-the-fake-ctb-locker/

PowerWare

Ransomware Open-sourced PowerShell

PowerWare is also known as:

- PoshCoder

Table 1293. 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

Princess Locker

Ransomware

Table 1294. 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

Table 1295. Table References

Links
http://www.enigmasoftware.com/prismyourcomputerhasbeenlockedransomware-removal/

Ps2exe

Ransomware

Table 1296. Table References

Links
https://twitter.com/jiriatvirlab/status/803297700175286273

R

Ransomware

Table 1297. Table References

Links
https://twitter.com/malwrhunterteam/status/846705481741733892

R980

Ransomware

Table 1298. Table References

Links
https://otx.alienvault.com/pulse/57976b52b900fe01376feb01/

RAA encryptor

Ransomware Possible affiliation with Pony

RAA encryptor is also known as:

- RAA

Table 1299. 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

Table 1300. Table References

Links
https://twitter.com/CryptoInsane/status/846181140025282561

Radamant

Ransomware

Table 1301. 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

Rakhni is also known as:

- Agent.iih
- Aura
- Autoit
- Pletor
- Rotor
- Lamer
- Isda
- Cryptokluchen
- Bandarchor

Table 1302. Table References

Links
https://support.kaspersky.com/us/viruses/disinfection/10556

Ramsomeer

Ransomware Based on the DUMB ransomware

Rannoh

Ransomware

Table 1303. Table References

Links
https://support.kaspersky.com/viruses/disinfection/8547

RanRan

Ransomware

Table 1304. 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

Table 1305. 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

RansomLock

Ransomware Locks the desktop

Table 1306. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2009-041513-1400-99&tabid=2

RarVault

Ransomware

Razy

Ransomware

Table 1307. Table References

Links
http://www.nyxbone.com/malware/Razy(German).html
http://nyxbone.com/malware/Razy.html

Rector

Ransomware

Table 1308. Table References

Links
https://support.kaspersky.com/viruses/disinfection/4264

RektLocker

Ransomware

Table 1309. Table References

Links
https://support.kaspersky.com/viruses/disinfection/4264

RemindMe

Ransomware

Table 1310. Table References

Links

http://www.nyxbone.com/malware/RemindMe.html
http://i.imgur.com/gV6i5SN.jpg

Rokku

Ransomware possibly related with Chimera

Table 1311. Table References

Links
https://blog.malwarebytes.org/threat-analysis/2016/04/rokku-ransomware/

RoshaLock

Ransomware Stores your files in a password protected RAR file

Table 1312. Table References

Links
https://twitter.com/siri_urz/status/842452104279134209

Runsomewere

Ransomware Based on HT/EDA2 Utilizes the Jigsaw Ransomware background

Table 1313. Table References

Links
https://twitter.com/struppigel/status/801812325657440256

RussianRoulette

Ransomware Variant of the Philadelphia ransomware

Table 1314. Table References

Links
https://twitter.com/struppigel/status/823925410392080385

SADStory

Ransomware Variant of CryPy

Table 1315. 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.

Table 1316. 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

Samas-Samsam is also known as:

- samsam.exe
- MIKOPONI.exe
- RikiRafael.exe
- showmehowto.exe

Table 1317. 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

Sanction

Ransomware Based on HiddenTear, but heavily modified keygen

Sanctions

Ransomware

Table 1318. Table References

Links
https://www.bleepingcomputer.com/news/security/sanctions-ransomware-makes-fun-of-usa-sanctions-against-russia/

Sardoninir

Ransomware

Table 1319. Table References

Links
https://twitter.com/BleepinComputer/status/835955409953357825

Satana

Ransomware

Table 1320. Table References

Links
https://blog.malwarebytes.com/threat-analysis/2016/06/satana-ransomware/
https://blog.kaspersky.com/satana-ransomware/12558/

Scraper

Ransomware

Table 1321. Table References

Links
http://securelist.com/blog/research/69481/a-flawed-ransomware-encryptor/

Serpico

Ransomware DetoxCrypto Variant

Table 1322. Table References

Links
http://www.nyxbone.com/malware/Serpico.html

Shark

Ransomware

Shark is also known as:

- Atom

Table 1323. 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

Table 1324. Table References

Links
https://twitter.com/JakubKroustek/status/760560147131408384
http://www.bleepingcomputer.com/news/security/new-educational-shinolocker-ransomware-project-released/

Shujin

Ransomware

Shujin is also known as:

- KinCrypt

Table 1325. 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

Table 1326. 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

SkidLocker is also known as:

- Pompous

Table 1327. 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

Table 1328. Table References

Links
https://www.bleepingcomputer.com/news/security/smash-ransomware-is-cute-rather-than-dangerous/

Smrss32

Ransomware

SNSLocker

Ransomware Based on EDA2

Table 1329. Table References

Links
http://nyxbone.com/malware/SNSLocker.html
http://nyxbone.com/images/articulos/malware/snslocker/16.png

Sport

Ransomware

Stampado

Ransomware Coded by "The_Rainmaker" Randomly deletes a file every 6hrs up to 96hrs then deletes decryption key

Table 1330. 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

Table 1331. Table References

Links
http://www.nyxbone.com/malware/Strictor.html

Surprise

Ransomware Based on EDA2

Survey

Ransomware Still in development, shows FileIce survey

Table 1332. 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

SZFLocker

Ransomware

Table 1333. Table References

Links
http://now.avg.com/dont-pay-the-ransom-avg-releases-six-free-decryption-tools-to-retrieve-your-files/

TeamXrat

Ransomware

Table 1334. Table References

Links

https://securelist.com/blog/research/76153/teamxrat-brazilian-cybercrime-meets-ransomware/

TeslaCrypt 0.x - 2.2.0

Ransomware Factorization

TeslaCrypt 0.x - 2.2.0 is also known as:

- AlphaCrypt

Table 1335. 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

Table 1336. 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

Table 1337. 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

Table 1338. 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

TorrentLocker

Ransomware Newer variants not decryptable. Only first 2 MB are encrypted

TorrentLocker is also known as:

- Crypt0L0cker
- CryptoFortress
- Teerac

Table 1339. 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

Table 1340. Table References

Links
http://www.bleepingcomputer.com/forums/t/618055/towerweb-ransomware-help-support-topic-payment-instructionsjpg/

Toxcrypt

Ransomware

Trojan

Ransomware

Trojan is also known as:

- BrainCrypt

Table 1341. 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

Table 1342. 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

Table 1343. Table References

Links
http://www.bleepingcomputer.com/news/security/truecrypter-ransomware-accepts-payment-in-bitcoins-or-amazon-gift-card/

Turkish

Ransomware

Table 1344. Table References

Links
https://twitter.com/struppigel/status/821991600637313024

Turkish Ransom

Ransomware

Table 1345. Table References

Links
http://www.nyxbone.com/malware/turkishRansom.html

UmbreCrypt

Ransomware CrypBoss Family

Table 1346. Table References

Links
http://www.thewindowsclub.com/emsisoft-decrypter-hydracrypt-umbrecrypt-ransomware

UnblockUPC

Ransomware

Table 1347. 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

Unlock92

Ransomware

Table 1348. Table References

Links
https://twitter.com/malwrhunterteam/status/839038399944224768

VapeLauncher

Ransomware CryptoWire variant

Table 1349. Table References

Links
https://twitter.com/struppigel/status/839771195830648833

VaultCrypt

Ransomware

VaultCrypt is also known as:

- CrypVault
- Zlader

Table 1350. Table References

Links
http://www.nyxbone.com/malware/russianRansom.html

VBRANSOM 7

Ransomware

Table 1351. Table References

Links
https://twitter.com/BleepinComputer/status/817851339078336513

VenusLocker

Ransomware Based on EDA2

Table 1352. 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

Table 1353. 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

Virus-Encoder is also known as:

- CrySiS

Table 1354. 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

WildFire Locker is also known as:

- Hades Locker

Table 1355. 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

Table 1356. Table References

Links
https://support.kaspersky.com/viruses/disinfection/2911
https://decrypter.emsisoft.com/xorist

XRTN

Ransomware VaultCrypt family

You Have Been Hacked!!!

Ransomware Attempt to steal passwords

Table 1357. Table References

Links
https://twitter.com/malwrhunterteam/status/808280549802418181

Zcrypt

Ransomware

Zcrypt is also known as:

- Zcryptor

Table 1358. Table References

Links
https://blogs.technet.microsoft.com/mmpc/2016/05/26/link-lnk-to-ransom/

Zimbra

Ransomware mpritsken@priest.com

Table 1359. 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

Zlader is also known as:

- Russian
- VaultCrypt
- CrypVault

Table 1360. Table References

Links
http://www.nyxbone.com/malware/russianRansom.html

Zorro

Ransomware

Table 1361. Table References

Links
https://twitter.com/BleepinComputer/status/844538370323812353

Zyklon

Ransomware Hidden Tear family, GNL Locker variant

Zyklon is also known as:

- GNL Locker

vxLock

Ransomware

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.

Table 1362. 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

Table 1363. Table References

Links
https://www.bleepingcomputer.com/news/security/uiwix-ransomware-using-eternalblue-smb-exploit-to-infect-victims/

SOREBRECT

Fileless, Code-injecting Ransomware

Table 1364. 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

Table 1365. Table References

Links
https://twitter.com/struppigel/status/899524853426008064

Kappa

Made with OXAR builder; decryptable

Table 1366. Table References

Links
https://twitter.com/struppigel/status/899528477824700416

Trojan Dz

CyberSplitter variant

Table 1367. Table References

Links
https://twitter.com/struppigel/status/899537940539478016

Xolzsec

ransomware written by self proclaimed script kiddies that should really be considered trollware

Table 1368. Table References

Links
https://twitter.com/struppigel/status/899916577252028416

FlatChestWare

HiddenTear variant; decryptable

Table 1369. 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.

SynAck is also known as:

- Syn Ack

Table 1370. Table References

Links
https://www.bleepingcomputer.com/news/security/synack-ransomware-sees-huge-spike-in-activity/

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.

Table 1371. 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.

Bad Rabbit is also known as:

- BadRabbit
- Bad-Rabbit

Table 1372. 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.

Table 1373. 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.

Table 1374. 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.

Table 1375. Table References

Links
https://www.bleepingcomputer.com/news/security/hc7-gotya-ransomware-installed-via-remote-desktop-services-spread-with-psexec/

HC6

Predecessor of HC7

Table 1376. 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.

Table 1377. 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.

Table 1378. 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/

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.

Table 1379. 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.

FileCoder is also known as:

- FindZip
- Patcher

Table 1380. 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.

Table 1381. Table References

Links
https://objective-see.com/blog/blog_0x25.html

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

TeamViewer

TeamViewer is a proprietary computer software package for remote control, desktop sharing, online meetings, web conferencing and file transfer between computers.

Table 1382. 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.

Table 1383. Table References

Links
https://blog.lookout.com/mobile-threat-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.

Back Orifice is also known as:

- BO

Table 1384. 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.

Netbus is also known as:

- NetBus

Table 1385. 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.

PoisonIvy is also known as:

- Poison Ivy
- Backdoor.Win32.PoisonIvy
- Gen:Trojan.Heur.PT

Table 1386. 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.

Sub7 is also known as:

- SubSeven
- Sub7Server

Table 1387. 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.

Table 1388. 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).

Table 1389. 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.

Table 1390. 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.

DarkComet is also known as:

- Dark Comet

Table 1391. 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.

Table 1392. 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.

Table 1393. 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

Table 1394. 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.

Back Orifice 2000 is also known as:

- BO2k

Table 1395. 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

RealVNC is also known as:

- VNC Connect
- VNC Viewer

Table 1396. 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.

Adwind RAT is also known as:

- UNRECOM
- UNiversal REmote COntrol Multi-Platform
- Frutas
- AlienSpy
- Unrecom
- Jsocket
- JBifrost

Table 1397. 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

Albertino Advanced RAT

Table 1398. 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.

Table 1399. 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.

Table 1400. 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

Table 1401. 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.

Table 1402. 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.

Table 1403. 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.

Table 1404. 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

Table 1405. 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.

DarkRat is also known as:

- DarkRAT

Table 1406. Table References

Links
https://www.infosecurity-magazine.com/blogs/the-dark-rat/
http://darkratphp.blogspot.lu/

Greame

Table 1407. 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.

Table 1408. Table References

Links
http://securityaffairs.co/wordpress/54837/hacking/one-stop-shop-hacking.html

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.

jRAT is also known as:

- JacksBot

Table 1409. Table References

Links
https://www.rekings.com/shop/jrat/

jSpy

jSpy is a Java RAT.

Table 1410. 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.

Table 1411. 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.

NJRat is also known as:

- Njw0rm

Table 1412. 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.

Table 1413. 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.

Predator Pain is also known as:

- PredatorPain

Table 1414. 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

Table 1415. 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.

Table 1416. 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

Small-Net is also known as:

- SmallNet

Table 1417. Table References

Links
http://small-net-rat.blogspot.lu/

Vantom

Vantom is a free RAT with good option and very stable.

Table 1418. 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.

Table 1419. 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.

Table 1420. 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.

Table 1421. 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. .

Table 1422. 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.

Table 1423. 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)

Table 1424. Table References

Links
https://www.rekings.com/babylon-rat/

Imminent Monitor

RAT

Table 1425. 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.

Table 1426. 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

Table 1427. Table References

Links
https://github.com/quasar/QuasarRAT

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.

Table 1428. Table References

Links
https://github.com/qqshow/dendroid
https://github.com/nyx0/Dendroid

Ratty

A Java R.A.T. program

Table 1429. Table References

Links
https://github.com/shotskeber/Ratty

RaTRon

Java RAT

Table 1430. Table References

Links

http://level23hacktools.com/forum/showthread.php?t=27971
https://leakforums.net/thread-405562?tid=405562&&pq=1

Arabian-Attacker RAT

Table 1431. 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.

Table 1432. Table References

Links
https://latesthackingnews.com/2015/05/31/how-to-hack-android-phones-with-androrat/
https://github.com/wszf/androrat

Adzok

Remote Administrator

Table 1433. Table References

Links
http://adzok.com/

Schwarze-Sonne-RAT

Schwarze-Sonne-RAT is also known as:

- SS-RAT
- Schwarze Sonne

Table 1434. Table References

Links
https://github.com/mwsrc/Schwarze-Sonne-RAT

Cyber Eye RAT

Table 1435. Table References

Links

https://www.indetectables.net/viewtopic.php?t=24245

Batch NET

RWX RAT

Table 1436. 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

Table 1437. Table References

Links
http://spynet-rat-officiel.blogspot.lu/

CTOS

Table 1438. Table References

Links
https://leakforums.net/thread-559871

Virus RAT

Table 1439. Table References

Links
https://github.com/mwsrc/Virus-RAT-v8.0-Beta

Atelier Web Remote Commander

Table 1440. 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

Table 1441. Table References

Links
https://github.com/chrismattmann/drat

MoSucker

MoSucker is a powerful backdoor - hacker's remote access tool.

Table 1442. Table References

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

Theef

Table 1443. 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).

Table 1444. Table References

Links
http://prorat.software.informer.com/
http://malware.wikia.com/wiki/ProRat

Setro

Table 1445. Table References

Links
https://sites.google.com/site/greymecompany/setro-rat-project

Indetectables RAT

Table 1446. Table References

Links
http://www.connect-trojan.net/2015/03/indetectables-rat-v.0.5-beta.html

Luminosity Link

Table 1447. Table References

Links
https://luminosity.link/

Orcus

Table 1448. Table References

Links
https://orcustechnologies.com/

Blizzard

Table 1449. Table References

Links
http://www.connect-trojan.net/2014/10/blizzard-rat-lite-v1.3.1.html

Kazybot

Table 1450. Table References

Links
https://www.rekings.com/kazybot-lite-php-rat/
http://telussecuritylabs.com/threats/show/TSL20150122-06

BX

Table 1451. Table References

Links
http://www.connect-trojan.net/2015/01/bx-rat-v1.0.html

death

Sky Wyder

Table 1452. Table References

Links
https://rubear.me/threads/sky-wyder-2016-cracked.127/

DarkTrack

Table 1453. 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).

Table 1454. Table References

Links
https://github.com/c4bbage/xRAT

Biodox

Table 1455. 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.

Table 1456. Table References

Links
https://leakforums.net/thread-31386?tid=31386&&pq=1

Apocalypse

Table 1457. Table References

Links

https://leakforums.net/thread-36962

JCage

Table 1458. 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).

Table 1459. 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

Table 1460. Table References

Links
http://ozonercp.com/

Xanity

Table 1461. Table References

Links
https://github.com/alienwithin/xanity-php-rat

DarkMoon

DarkMoon is also known as:

- Dark Moon

Xpert

Table 1462. 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.

Kiler RAT is also known as:

- Njw0rm

Table 1463. Table References

Links
https://www.alienvault.com/blogs/labs-research/kilerrat-taking-over-where-njrat-remote-access-trojan-left-off

Brat

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.

Lost Door is also known as:

- LostDoor

Table 1464. 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.

Table 1465. Table References

Links
https://www.rekings.com/loki-rat-php-rat/

MLRat

Table 1466. Table References

Links
https://github.com/BahNahNah/MLRat

SpyCronic

Table 1467. 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

Table 1468. Table References

Links
https://github.com/n1nj4sec/pupy

Nova

Nova is a proof of concept demonstrating screen sharing over UDP hole punching.

Table 1469. Table References

Links
http://novarat.sourceforge.net/

BD Y3K RAT

BD Y3K RAT is also known as:

- Back Door Y3K RAT
- Y3k

Table 1470. 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.

Table 1471. 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.

Table 1472. 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.

SharK is also known as:

- SHARK
- Shark

Table 1473. 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.

Snowdoor is also known as:

- Backdoor.Blizzard
- Backdoor.Fxdoor
- Backdoor.Snowdoor
- Backdoor:Win32/Snowdoor

Table 1474. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2003-022018-5040-99

Paradox

Table 1475. Table References

Links
https://www.nulled.to/topic/155464-paradox-rat/

SpyNote

Android RAT

Table 1476. Table References

Links
https://www.rekings.com/spynote-v4-android-rat/

ZOMBIE SLAYER

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.

Table 1477. Table References

Links
https://networklookout.com/help/

DameWare Mini Remote Control

Affordable remote control software for all your customer support and help desk needs.

DameWare Mini Remote Control is also known as:

- dameware

Table 1478. 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.

Table 1479. 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.

Ammyy Admin is also known as:

- Ammyy

Table 1480. 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.

Table 1481. 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.

Table 1482. 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.

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.

Table 1483. 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.

Seecreen is also known as:

- Firnass

Table 1484. 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.

Table 1485. 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.

Table 1486. 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.

Table 1487. 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.

Table 1488. 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.

Table 1489. 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.

Table 1490. 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.

Table 1491. 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.

Table 1492. Table References

Links
http://www.beamyourscreen.com/

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

Table 1493. 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

Table 1494. Table References

Links
http://www.hacktohell.org/2011/05/setting-up-cerberus-ratremote.html

Syndrome RAT

Snoopy

Snoopy is a Remote Administration Tool. Software for controlling user computer remotely from other computer on local network or Internet.

Table 1495. Table References

Links
http://www.spy-emergency.com/research/S/Snoopy.html

5p00f3r.N$ RAT

P. Storrie RAT

A. Storrie RAT is also known as:

   - P.Storrie RAT

xHacker Pro RAT

NetDevil

Backdoor.NetDevil allows a hacker to remotely control an infected computer.

Table 1496. 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.

Table 1497. 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

Table 1498. 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.

Table 1499. Table References

Links
http://www.netsupportmanager.com/index.asp

Vortex

Assassin

Net Devil

Net Devil is also known as:

- NetDevil

Table 1500. Table References

Links
https://www.symantec.com/security_response/attacksignatures/detail.jsp?asid=20702

A4Zeta

Table 1501. Table References

Links
http://www.megasecurity.org/trojans/a/a4zeta/A4zeta_b2.html

Greek Hackers RAT

Table 1502. Table References

Links
http://www.connect-trojan.net/2013/04/greek-hackers-rat-1.0.html?m=0

MRA RAT

Table 1503. Table References

Links
http://www.connect-trojan.net/2013/04/greek-hackers-rat-1.0.html?m=0

Sparta RAT

Table 1504. Table References

Links
http://www.connect-trojan.net/2015/09/sparta-rat-1.2-by-azooz-ejram.html

LokiTech

MadRAT

Tequila Bandita

Table 1505. Table References

Links
http://www.connect-trojan.net/2013/07/tequila-bandita-1.3b2.html

Toquito Bandito

Table 1506. Table References

Links
http://www.megasecurity.org/trojans/t/toquitobandito/Toquitobandito_all.html

MofoTro

MofoTro is a new rat coded by Cool_mofo_2.

Table 1507. 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

Table 1508. 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.

Table 1509. 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.

Table 1510. Table References

Links
https://attack.mitre.org/wiki/Software/S0065

Darknet RAT

Darknet RAT is also known as:

- Dark NET RAT

Table 1511. Table References

Links
http://www.connect-trojan.net/2015/06/dark-net-rat-v.0.3.9.0.html

CIA RAT

Minimo

miniRAT

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.

PlugX is also known as:

- Korplug

Table 1512. 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.

Table 1513. 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

Table 1514. Table References

Links
http://www.megasecurity.org/trojans/m/mega/Megatrojan1.0.html

Venomous Ivy

Xploit

Arctic R.A.T.

Arctic R.A.T. is also known as:

- Artic

Table 1515. Table References

Links
http://anti-virus-soft.com/threats/artic

GOlden Phoenix

Table 1516. Table References

Links
http://www.connect-trojan.net/2014/02/golden-phoenix-rat-0.2.html

GraphicBooting

Table 1517. Table References

Links
http://www.connect-trojan.net/2014/10/graphicbooting-rat-v0.1-beta.html?m=0

Pocket RAT

Erebus

SharpEye

Table 1518. 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

Archelaus Beta

Table 1519. Table References

Links
http://www.connect-trojan.net/2014/02/archelaus-rat-beta.html

BlackHole

C# RAT (Remote Adminitration Tool) - Educational purposes only

Table 1520. Table References

Links
https://github.com/hussein-aitlahcen/BlackHole

Vanguard

Table 1521. Table References

Links
http://ktwox7.blogspot.lu/2010/12/vanguard-remote-administration.html

Ahtapod

Table 1522. 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.

Table 1523. 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.

Table 1524. Table References

Links
http://www.nuclearwintercrew.com/Products-View/25/Seed_1.1/

SharpBot

TorCT PHP RAT

Table 1525. Table References

Links
https://github.com/alienwithin/torCT-PHP-RAT

A32s RAT

Char0n

Nytro

Syla

Table 1526. 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.

Table 1527. 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.

Sakula is also known as:

- Sakurel
- VIPER

Table 1528. 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.

Table 1529. Table References

Links
https://attack.mitre.org/wiki/Software/S0071

Crimson

Table 1530. Table References

Links
http://www.connect-trojan.net/2015/01/crimson-rat-3.0.0.html

KjW0rm

Table 1531. Table References

Links
http://hack-defender.blogspot.fr/2015/12/kjw0rm-v05x.html

Ghost

Ghost is also known as:

- Ucul

Table 1532. Table References

Links
https://www.youtube.com/watch?v=xXZW4ajVYkI

9002

Sandro RAT

Mega

WiRAT

3PARA RAT

Table 1533. Table References

Links
https://books.google.fr/books?isbn=2212290136

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.

Konni is also known as:

- KONNI

Table 1534. 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

Felismus RAT

Used by Sowbug

Table 1535. 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.

Xsser is also known as:

- mRAT

Table 1536. 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.

Table 1537. 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

Table 1538. Table References

Links
https://www.youtube.com/watch?v=jUg5—68Iqs

Killer RAT

Hi-Zor

Table 1539. 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.

Quaverse is also known as:

- QRAT

Table 1540. Table References

Links
https://www.trustwave.com/Resources/SpiderLabs-Blog/Quaverse-RAT—Remote-Access-as-a-Service/

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.

Table 1541. 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!

Table 1542. Table References

Links
https://omnirat.eu/en/

Jfect

Table 1543. 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.

Table 1544. 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.

Table 1545. 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.

Table 1546. 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

Table 1547. 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.

Table 1548. Table References

Links
http://www.securitynewspaper.com/2016/08/31/unsophisticated-revenge-rat-released-online-free-exclusive/

vjw0rm 0.1

Table 1549. 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.

rokrat is also known as:

- ROKRAT

Table 1550. 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").

Qarallax is also known as:

- qrat

Table 1551. 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.

Table 1552. 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.

Table 1553. Table References

Links
https://blog.fortinet.com/2017/02/14/remcos-a-new-rat-in-the-wild-2

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.

Table 1554. 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…

Table 1555. 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.

Table 1556. 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.

Table 1557. 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.

Table 1558. 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.

Table 1559. Table References

Links
https://researchcenter.paloaltonetworks.com/2017/08/unit42-updated-khrat-malware-used-in-cambodia-attacks/

RevCode

Table 1560. Table References

Links
https://revcode.eu/

AhNyth Android

Android Remote Administration Tool

Table 1561. 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'

Table 1562. Table References

Links
https://www.virusbulletin.com/uploads/pdf/magazine/1999/199908.pdf

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.

Table 1563. 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.

Table 1564. Table References

Links
http://blog.talosintelligence.com/2017/03/dnsmessenger.html

PentagonRAT

Table 1565. 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.

Table 1566. 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

Xyligan

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.

Table 1567. 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.

Table 1568. Table References

Links

https://www.us-cert.gov/ncas/alerts/TA17-318A

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.

Table 1569. 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.”

Table 1570. Table References

Links
https://digitasecurity.com/blog/2018/01/23/crossrat/

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

Other

Academia - University

Activists

Aerospace

Agriculture

Arts

Bank

Chemical

Citizens

Civil Aviation

Country

Culture

Data Broker

Defense

Development

Diplomacy

Education

Electric

Electronic

Employment

Energy

Entertainment

Environment

Finance

Food

Game

Gas

Government, Administration

Health

Higher education

Hotels

Infrastructure

Intelligence

IT

IT - Hacker

IT - ISP

IT - Security

Justice

Manufacturing

Maritime

Military

Multi-sector

News - Media

NGO

Oil

Payment

Pharmacy

Police - Law enforcement

Research - Innovation

Satellite navigation

Security systems

Social networks

Space

Steel

Telecoms

Think Tanks

Trade

Transport

Travel

Turbine

Tourism

Life science

Biomedical

High tech

Opposition

Political party

Hospitality

Automotive

Metal

Railway

Water

Smart meter

Retai

Retail

Technology

engineering

Mining

Sport

Restaurant

Semi-conductors

Insurance

Legal

Shipping

Logistic

Construction

Industrial

Communication equipment

Security Service

Tax firm

Television broadcast

Separatists

Dissidents

Digital services

Digital infrastructure

Security actors

eCommerce

Islamic forums

Journalist

Streaming service

Puplishing industry

Publishing industry

Islamic organisation

Casino

Consulting

Online marketplace

DNS service provider

Veterinary

Marketing

Video Sharing

Advertising

Investment

Accounting

Programming

Managed Services Provider

Lawyers

Civil society

Petrochemical

Immigration

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

Table 1571. Table References

Links
https://keitarotds.com/

BlackTDS

BlackTDS is mutualised TDS advertised underground since end of December 2017

Table 1572. 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

Sutra

Sutra TDS was dominant from 2012 till 2015

Table 1573. Table References

Links
http://kytoon.com/sutra-tds.html

SimpleTDS

SimpleTDS is a basic open source TDS

SimpleTDS is also known as:

- Stds

Table 1574. Table References

Links
https://sourceforge.net/projects/simpletds/

BossTDS

BossTDS

Table 1575. Table References

Links
http://bosstds.com/

BlackHat TDS

BlackHat TDS is sold underground.

Table 1576. 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

Orchid TDS

Orchid TDS was sold underground. Rare usage

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 https://github.com/MISP/misp-galaxy/blob/master/clusters/threat actor.json[**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

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

Table 1577. Table References

Links
https://en.wikipedia.org/wiki/PLA_Unit_61398
http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

Stalker Panda

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.

Nitro is also known as:

- Covert Grove

Table 1578. 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.'

Codoso is also known as:

- C0d0so
- APT19
- APT 19
- Sunshop Group

Table 1579. 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

Dust Storm

Table 1580. 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.

Table 1581. 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

Keyhole Panda is also known as:

- temp.bottle

Wet Panda

Table 1582. Table References

Links
http://go.crowdstrike.com/rs/281-OBQ-266/images/ReportGlobalThreatIntelligence.pdf

Foxy Panda

Adversary group targeting telecommunication and technology organizations.

Table 1583. 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

Table 1584. Table References

Links
http://go.crowdstrike.com/rs/281-OBQ-266/images/ReportGlobalThreatIntelligence.pdf

Union Panda

Table 1585. 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

Table 1586. Table References

Links
http://go.crowdstrike.com/rs/281-OBQ-266/images/ReportGlobalThreatIntelligence.pdf

Eloquent Panda

Table 1587. 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

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.'

Putter Panda is also known as:

- PLA Unit 61486
- APT 2
- Group 36
- APT-2
- MSUpdater
- 4HCrew
- SULPHUR

- TG-6952

Table 1588. Table References

Links
http://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf

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.'

UPS is also known as:

- Gothic Panda
- TG-0110
- APT 3
- Group 6
- UPS Team
- APT3
- Buckeye

Table 1589. 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

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.'

DarkHotel is also known as:

- DUBNIUM
- Fallout Team
- Karba

- Luder
- Nemim
- Tapaoux

Table 1590. 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/

IXESHE

A group of China-based attackers, who conducted a number of spear phishing attacks in 2013.

IXESHE is also known as:

- Numbered Panda
- TG-2754
- BeeBus
- Group 22
- DynCalc
- Calc Team
- DNSCalc
- Crimson Iron
- APT12
- APT 12

Table 1591. Table References

Links
http://www.crowdstrike.com/blog/whois-numbered-panda/

APT 16

Table 1592. Table References

Links
https://www.fireeye.com/blog/threat-research/2015/12/the_eps_awakens.html

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.'

Aurora Panda is also known as:

- APT 17
- Deputy Dog
- Group 8
- APT17
- Hidden Lynx
- Tailgater Team

Table 1593. 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

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.'

Wekby is also known as:

- Dynamite Panda
- TG-0416
- APT 18
- SCANDIUM
- PLA Navy
- APT18

Table 1594. Table References

Links

https://threatpost.com/apt-gang-branches-out-to-medical-espionage-in-community-health-breach/107828

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.'

Tropic Trooper is also known as:

- Operation Tropic Trooper

Table 1595. 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.'

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

Table 1596. 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

Shell Crew

Adversary group targeting financial, technology, non-profit organisations.

Shell Crew is also known as:

- Deep Panda
- WebMasters
- APT 19
- KungFu Kittens
- Black Vine
- Group 13
- PinkPanther
- Sh3llCr3w

Table 1597. 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

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.'

Naikon is also known as:

- PLA Unit 78020
- APT 30
- APT30
- Override Panda
- Camerashy
- APT.Naikon

Table 1598. 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

Lotus Blossom

Lotus Blossom is also known as:

- Spring Dragon
- ST Group

Table 1599. Table References

Links
https://securelist.com/blog/research/70726/the-spring-dragon-apt/
https://securelist.com/spring-dragon-updated-activity/79067/

Lotus Panda

Lotus Panda is also known as:

- Elise

Table 1600. Table References

Links
http://www.crowdstrike.com/blog/rhetoric-foreshadows-cyber-activity-in-the-south-china-sea/

Hurricane Panda

Hurricane Panda is also known as:

- Black Vine
- TEMP.Avengers

Table 1601. 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.

Emissary Panda is also known as:

- TG-3390
- APT 27
- TEMP.Hippo
- Group 35
- Bronze Union
- ZipToken
- HIPPOTeam
- APT27
- Operation Iron Tiger

Table 1602. 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/

Stone Panda

Stone Panda is also known as:

- APT10
- APT 10
- menuPass
- happyyongzi
- POTASSIUM
- DustStorm
- Red Apollo
- CVNX

Table 1603. Table References

Links
http://researchcenter.paloaltonetworks.com/2017/02/unit42-menupass-returns-new-malware-new-attacks-japanese-academics-organizations/

Nightshade Panda

Nightshade Panda is also known as:

- APT 9
- Flowerlady/Flowershow
- Flowerlady
- Flowershow

Table 1604. Table References

Links
https://otx.alienvault.com/pulse/55bbc68e67db8c2d547ae393/

Hellsing

Hellsing is also known as:

- Goblin Panda
- Cycldek

Table 1605. Table References

Links
https://securelist.com/analysis/publications/69567/the-chronicles-of-the-hellsing-apt-the-empire-strikes-back/

Night Dragon

Table 1606. Table References

Links
https://kc.mcafee.com/corporate/index?page=content&id=KB71150

Mirage

Mirage is also known as:

- Vixen Panda
- Ke3Chang

- GREF
- Playful Dragon
- APT 15
- Metushy
- Lurid
- Social Network Team

Table 1607. 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/

Anchor Panda

PLA Navy

Anchor Panda is also known as:

- APT14
- APT 14
- QAZTeam
- ALUMINUM

Table 1608. Table References

Links
http://www.crowdstrike.com/blog/whois-anchor-panda/

NetTraveler

NetTraveler is also known as:

- APT 21

Table 1609. Table References

Links
https://securelist.com/blog/research/35936/nettraveler-is-running-red-star-apt-attacks-compromise-high-profile-victims/

Ice Fog

Operate since at least 2011, from several locations in China, with members in Korea and Japan as

well.

Ice Fog is also known as:

- IceFog
- Dagger Panda

Table 1610. 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/

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

Pitty Panda is also known as:

- PittyTiger
- MANGANESE

Table 1611. Table References

Links
http://blog.airbuscybersecurity.com/post/2014/07/The-Eye-of-the-Tiger2

Roaming Tiger

Table 1612. Table References

Links
http://researchcenter.paloaltonetworks.com/2015/12/bbsrat-attacks-targeting-russian-organizations-linked-to-roaming-tiger/

Beijing Group

Beijing Group is also known as:

- Sneaky Panda

Radio Panda

Radio Panda is also known as:

- Shrouded Crossbow

APT.3102

Table 1613. Table References

Links
http://researchcenter.paloaltonetworks.com/2015/09/chinese-actors-use-3102-malware-in-attacks-on-us-government-and-eu-media/

Samurai Panda

Samurai Panda is also known as:

- PLA Navy
- APT4
- APT 4
- Wisp Team
- Getkys
- SykipotGroup
- Wkysol

Table 1614. Table References

Links
http://www.crowdstrike.com/blog/whois-samurai-panda/

Impersonating Panda

Violin Panda

Violin Panda is also known as:

- APT20
- APT 20
- APT8
- APT 8
- TH3Bug

Table 1615. 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.

Table 1616. 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.

Temper Panda is also known as:

- Admin338
- Team338
- MAGNESIUM
- admin@338

Table 1617. 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

Pirate Panda

Pirate Panda is also known as:

- APT23
- KeyBoy

Table 1618. 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.

Flying Kitten is also known as:

- SaffronRose
- Saffron Rose
- AjaxSecurityTeam
- Ajax Security Team
- Group 26

Table 1619. 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/

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.

Cutting Kitten is also known as:

- ITSecTeam
- Threat Group 2889
- TG-2889
- Ghambar

Table 1620. Table References

Links
http://www.secureworks.com/cyber-threat-intelligence/threats/suspected-iran-based-hacker-group-creates-network-of-fake-linkedin-profiles/

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.

Charming Kitten is also known as:

- Newscaster
- Parastoo
- iKittens
- Group 83
- Newsbeef

Table 1621. 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

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.

APT33 is also known as:

Table 1622. 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.

Magic Kitten is also known as:

- Group 42

Table 1623. 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.

Rocket Kitten is also known as:

- TEMP.Beanie
- Operation Woolen Goldfish
- Thamar Reservoir
- Timberworm

Table 1624. 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

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.

Cleaver is also known as:

- Operation Cleaver

- Tarh Andishan
- Alibaba
- 2889
- TG-2889
- Cobalt Gypsy
- Ghambar
- Cutting Kitten

Table 1625. 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/

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.

Rebel Jackal is also known as:

- FallagaTeam

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.

Sofacy is also known as:

- APT 28
- APT28
- Pawn Storm
- Fancy Bear
- Sednit
- TsarTeam
- TG-4127
- Group-4127
- STRONTIUM
- TAG_0700
- Swallowtail
- IRON TWILIGHT
- Group 74

Table 1626. 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/

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 '

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

Table 1627. 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

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.'

Turla Group is also known as:

- Turla
- Snake
- Venomous Bear
- Group 88
- Waterbug
- WRAITH
- Turla Team
- Uroburos
- Pfinet
- TAG_0530
- KRYPTON
- Hippo Team

Table 1628. 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/

Energetic Bear

A Russian group that collects intelligence on the energy industry.

Energetic Bear is also known as:

- Dragonfly
- Crouching Yeti
- Group 24
- Havex
- CrouchingYeti
- Koala Team

Table 1629. 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/

Sandworm

Sandworm is also known as:

- Sandworm Team
- Black Energy
- BlackEnergy
- Quedagh
- Voodoo Bear
- TEMP.Noble

Table 1630. 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

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.

TeleBots is also known as:

- Sandworm

Table 1631. 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.

Anunak is also known as:

- Carbanak
- Carbon Spider
- FIN7

Table 1632. 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

TeamSpy Crew

TeamSpy Crew is also known as:

- TeamSpy
- Team Bear
- Berserk Bear

- Anger Bear

Table 1633. Table References

Links
https://securelist.com/blog/incidents/35520/the-teamspy-crew-attacks-abusing-teamviewer-for-cyberespionage-8/

BuhTrap

Table 1634. Table References

Links
http://www.welivesecurity.com/2015/11/11/operathion-buhtrap-malware-distributed-via-ammyy-com/

Berserk Bear

Wolf Spider

Wolf Spider is also known as:

- FIN4

Boulder Bear

First observed activity in December 2013.

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.

Union Spider

Adversary targeting manufacturing and industrial organizations.

Table 1635. 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

Silent Chollima is also known as:

- OperationTroy
- Guardian of Peace
- GOP
- WHOis Team

Table 1636. 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.

Lazarus Group is also known as:

- Operation DarkSeoul
- Dark Seoul
- Hidden Cobra
- Hastati Group
- Andariel
- Unit 121
- Bureau 121
- NewRomanic Cyber Army Team
- Bluenoroff

Table 1637. 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

Viceroy Tiger

Viceroy Tiger is also known as:

- Appin
- OperationHangover

Table 1638. Table References

Links
http://enterprise-manage.norman.c.bitbit.net/resources/files/Unveiling_an_Indian_Cyberattack_Infrastructure.pdf

Pizzo Spider

Pizzo Spider is also known as:

- DD4BC
- Ambiorx

Corsair Jackal

Corsair Jackal is also known as:

- TunisianCyberArmy

Table 1639. 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.

SNOWGLOBE is also known as:

- Animal Farm

Table 1640. 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

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

Deadeye Jackal is also known as:

- SyrianElectronicArmy
- SEA

Table 1641. Table References

Links
https://en.wikipedia.org/wiki/Syrian_Electronic_Army

Operation C-Major

Group targeting Indian Army or related assets in India. Attribution to a Pakistani connection has been made by TrendMicro.

Operation C-Major is also known as:

- C-Major

Table 1642. Table References

Links
http://documents.trendmicro.com/assets/pdf/Indian-military-personnel-targeted-by-information-theft-campaign-cmajor.pdf

Stealth Falcon

Group targeting Emirati journalists, activists, and dissidents.

Stealth Falcon is also known as:

- FruityArmor

Table 1643. Table References

Links
https://citizenlab.org/2016/05/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.

ScarCruft is also known as:

- Operation Daybreak
- Operation Erebus

Table 1644. 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.

Pacifier APT is also known as:

- Skipper
- Popeye

Table 1645. 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

Table 1646. 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.

Dropping Elephant is also known as:

- Chinastrats
- Patchwork
- Monsoon
- Sarit

Table 1647. 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/

Operation Transparent Tribe

Proofpoint researchers recently uncovered evidence of an advanced persistent threat (APT) against Indian diplomatic and military resources. Our investigation began with malicious emails sent to Indian embassies in Saudi Arabia and Kazakstan but turned up connections to watering hole sites focused on Indian military personnel and designed to drop a remote access Trojan (RAT) with a variety of data exfiltration functions.

Table 1648. Table References

Links
https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf

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.

Table 1649. 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.

Table 1650. 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.

DragonOK is also known as:

- Moafee

Table 1651. 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

Threat Group-3390

Chinese threat group that has extensively used strategic Web compromises to target victims.

Threat Group-3390 is also known as:

- TG-3390
- Emissary Panda

Table 1652. Table References

Links
http://www.secureworks.com/cyber-threat-intelligence/threats/threat-group-3390-targets-organizations-for-cyberespionage/
https://attack.mitre.org

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.

ProjectSauron is also known as:

- Strider
- Sauron

Table 1653. Table References

Links
https://securelist.com/analysis/publications/75533/faq-the-projectsauron-apt/

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.

APT 30 is also known as:

- APT30

Table 1654. Table References

Links
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf
https://attack.mitre.org/wiki/Group/G0013

TA530

TA530, who we previously examined in relation to large-scale personalized phishing campaigns

GCMAN

GCMAN is a threat group that focuses on targeting banks for the purpose of transferring money to e-currency services.

Table 1655. 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

Table 1656. 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.

Table 1657. 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.

TeamXRat

TeamXRat is also known as:

- CorporacaoXRat
- CorporationXRat

Table 1658. 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.

OilRig is also known as:

- Twisted Kitten
- Cobalt Gypsy

Table 1659. 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

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 .

Table 1660. 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.

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.

Table 1661. 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.”

Molerats is also known as:

- Gaza Hackers Team
- Gaza cybergang
- Operation Molerats
- Extreme Jackal
- Moonlight

Table 1662. 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.

PROMETHIUM is also known as:

- StrongPity

Table 1663. 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.

Table 1664. 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.

Table 1665. 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.

Table 1666. 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.

Table 1667. 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.

Table 1668. 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.

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

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.

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.

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

Equation Group is also known as:

- Tilded Team
- Lamberts
- EQGRP

Table 1669. Table References

Links
https://en.wikipedia.org/wiki/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.

Table 1670. 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.

Table 1671. 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.

Hammer Panda is also known as:

- Zhenbao
- TEMP.Zhenbao

Table 1672. 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.

Infy is also known as:

- Operation Mermaid

Table 1673. 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/

Sima

Sima is a group of suspected Iranian origin targeting Iranians in diaspora.

Table 1674. 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.

Blue Termite is also known as:

- Cloudy Omega

Table 1675. 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

Groundbait

Groundbait is a group targeting anti-government separatists in the self-declared Donetsk and

Luhansk People's Republics.

Table 1676. 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.

Table 1677. 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/

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.

Table 1678. 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.

APT32 is also known as:

- OceanLotus Group
- Ocean Lotus
- Cobalt Kitty
- APT-C-00
- SeaLotus
- APT-32
- APT 32

Table 1679. 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

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.

Table 1680. 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.

WildNeutron is also known as:

- Butterfly
- Morpho
- Sphinx Moth

Table 1681. 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.

PLATINUM is also known as:

- TwoForOne

Table 1682. 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

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.

ELECTRUM is also known as:

- Sandworm

Table 1683. Table References

Links
https://dragos.com/blog/crashoverride/CrashOverride-01.pdf
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf

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.

Table 1684. 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.

Table 1685. 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

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.

Cobalt is also known as:

- Cobalt group
- Cobalt gang

Table 1686. Table References

Links
https://www.helpnetsecurity.com/2016/11/22/cobalt-hackers-synchronized-atm-heists/

TA459

Table 1687. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/apt-targets-financial-analysts#.WS3IBVFV4no.twitter

Cyber Berkut

Table 1688. Table References

Links
https://www.threatconnect.com/blog/russia-hacks-bellingcat-mh17-investigation/.V-wnrubaeEU.twitter

Tonto Team

Table 1689. 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

Table 1690. Table References

Links
https://securelist.com/analysis/publications/74828/cve-2015-2545-overview-of-current-threats/

APT5

Table 1691. Table References

Links
https://www.fireeye.com/current-threats/apt-groups.html

APT 22

APT 22 is also known as:

- APT22

Table 1692. Table References

Links
http://www.slideshare.net/CTruncer/ever-present-persistence-established-footholds-seen-in-the-wild

Tick

Tick is also known as:

- Bronze Butler

Table 1693. 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

APT 26

APT 26 is also known as:

- APT26
- Hippo Team
- JerseyMikes

Sabre Panda

Table 1694. Table References

Links
http://go.crowdstrike.com/rs/281-OBQ-266/images/ReportGlobalThreatIntelligence.pdf

Big Panda

Table 1695. Table References

Links

http://www.darkreading.com/attacks-and-breaches/crowdstrike-falcon-traces-attacks-back-to-hackers/d/d-id/1110402?

Poisonous Panda

Table 1696. 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

Table 1697. 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

Table 1698. Table References

Links
https://www.isightpartners.com/2016/02/threatscape-media-highlights-update-week-of-february-17th/

Mofang

Mofang is also known as:

- Superman

Table 1699. 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/

CopyKittens

CopyKittens is also known as:

- Slayer Kitten

Table 1700. 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/

EvilPost

Table 1701. 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

Table 1702. Table References

Links
https://securelist.com/analysis/publications/74828/cve-2015-2545-overview-of-current-threats/

Test Panda

Table 1703. Table References

Links
http://www.slideshare.net/CrowdStrike/crowd-casts-monthly-you-have-an-adversary-problem

Madi

Table 1704. 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/

Electric Panda

Table 1705. Table References

Links
http://www.slideshare.net/CrowdStrike/crowd-casts-monthly-you-have-an-adversary-problem

Maverick Panda

Maverick Panda is also known as:

- PLA Navy
- Sykipot

Table 1706. 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

Kimsuki

Table 1707. Table References

Links
http://securelist.com/analysis/57915/the-kimsuky-operation-a-north-korean-apt/

Snake Wine

Table 1708. Table References

Links
https://www.cylance.com/en_us/blog/the-deception-project-a-new-japanese-centric-threat.html

Careto

Careto is also known as:

- The Mask

Table 1709. Table References

Links
https://securelist.com/blog/research/58254/the-caretomask-apt-frequently-asked-questions/

Gibberish Panda

Table 1710. Table References

Links
http://www.slideshare.net/CrowdStrike/crowd-casts-monthly-you-have-an-adversary-problem

OnionDog

Table 1711. Table References

Links
http://news.softpedia.com/news/korean-energy-and-transportation-targets-attacked-by-oniondog-apt-501534.shtml

Clever Kitten

Clever Kitten is also known as:

- Group 41

Table 1712. Table References

Links
http://www.crowdstrike.com/blog/whois-clever-kitten/

Andromeda Spider

Table 1713. 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

Cyber Caliphate Army is also known as:

- Islamic State Hacking Division
- CCA
- United Cyber Caliphate
- UUC

Table 1714. 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

Table 1715. Table References

Links
http://go.crowdstrike.com/rs/281-OBQ-266/images/ReportGlobalThreatIntelligence.pdf

Group 27

Table 1716. 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

Table 1717. 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

Cyber fighters of Izz Ad-Din Al Qassam is also known as:

- Fraternal Jackal

Table 1718. Table References

Links
http://pastebin.com/u/QassamCyberFighters
http://ddanchev.blogspot.com.es/2012/09/dissecting-operation-ababil-osint.html

APT 6

APT 6 is also known as:

- 1.php Group
- APT6

AridViper

AridViper is also known as:

- Desert Falcon
- Arid Viper
- APT-C-23

Table 1719. 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

Table 1720. 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

Unit 8200 is also known as:

- Duqu Group

Table 1721. 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

White Bear

White Bear is also known as:

- Skipper Turla

Table 1722. Table References

Links
https://securelist.com/introducing-whitebear/81638/

Pale Panda

Table 1723. Table References

Links
http://go.crowdstrike.com/rs/281-OBQ-266/images/ReportGlobalThreatIntelligence.pdf

Mana Team

Table 1724. 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.

Table 1725. Table References

Links
https://www.symantec.com/connect/blogs/sowbug-cyber-espionage-group-targets-south-american-and-southeast-asian-governments

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.

Table 1726. Table References

Links
https://researchcenter.paloaltonetworks.com/2017/11/unit42-muddying-the-water-targeted-attacks-in-the-middle-east/

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.

Table 1727. 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.

Table 1728. 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.

Table 1729. 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.

Table 1730. Table References

Links

https://blog.newskysecurity.com/masuta-satori-creators-second-botnet-weaponizes-a-new-router-exploit-2ddc51cc52a7

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

Tinba

Banking Malware

Tinba is also known as:

- Hunter
- Zusy
- TinyBanker

Table 1731. Table References

Links
https://thehackernews.com/search/label/Zusy%20Malware
http://blog.trendmicro.com/trendlabs-security-intelligence/the-tinbatinybanker-malware/

PlugX

Malware

PlugX is also known as:

- Backdoor.FSZO-5117
- Trojan.Heur.JP.juW@ayZZvMb
- Trojan.Inject1.6386
- Korplug
- Agent.dhwf

Table 1732. 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
```

Table 1733. Table References

Links
https://www.zscaler.com/pdf/whitepapers/msupdater_trojan_whitepaper.pdfx

Lazagne

A password sthealing tool regularly used by attackers

Table 1734. Table References

Links
https://github.com/AlessandroZ/LaZagne

Poison Ivy

Poison Ivy is a RAT which was freely available and first released in 2005.

Poison Ivy is also known as:

- Backdoor.Win32.PoisonIvy
- Gen:Trojan.Heur.PT

Table 1735. 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.

Table 1736. Table References

Links

http://researchcenter.paloaltonetworks.com/2016/04/unit42-new-poison-ivy-rat-variant-targets-hong-kong-pro-democracy-activists/

Torn RAT

Torn RAT is also known as:

- Anchor Panda

Table 1737. Table References

Links
https://www.crowdstrike.com/blog/whois-anchor-panda/

OzoneRAT

OzoneRAT is also known as:

- Ozone RAT
- ozonercp

Table 1738. 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.

ZeGhost is also known as:

- BackDoor-FBZT!52D84425CDF2
- Trojan.Win32.Staser.ytq
- Win32/Zegost.BW

Table 1739. 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

Elise Backdoor is also known as:

- Elise

Table 1740. 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.

Trojan.Laziok is also known as:

- Laziok

Table 1741. Table References

Links
http://www.symantec.com/connect/blogs/new-reconnaissance-threat-trojanlaziok-targets-energy-sector

Slempo

Android-based malware

Slempo is also known as:

- GM-Bot
- SlemBunk
- Bankosy
- Acecard

Table 1742. 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.

PWOBot is also known as:

- PWOLauncher

- PWOHTTPD
- PWOKeyLogger
- PWOMiner
- PWOPyExec
- PWOQuery

Table 1743. 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.

Lost Door RAT is also known as:

- LostDoor RAT
- BKDR_LODORAT

Table 1744. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/lost-door-rat-accessible-customizable-attack-tool/

njRAT

njRAT is also known as:

- Bladabindi
- Jorik

Table 1745. 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

NanoCoreRAT is also known as:

- NanoCore

- Nancrat
- Zurten
- Atros2.CKPN

Table 1746. Table References

Links
http://www.symantec.com/connect/blogs/nanocore-another-rat-tries-make-it-out-gutter
https://nanocore.io/

Sakula

Sakula is also known as:

- Sakurel

Table 1747. Table References

Links
https://www.secureworks.com/research/sakula-malware-family

Hi-ZOR

Table 1748. Table References

Links
http://www.threatgeek.com/2016/01/introducing-hi-zor-rat.html

Derusbi

Derusbi is also known as:

- TROJ_DLLSERV.BE

Table 1749. 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

EvilGrab is also known as:

- BKDR_HGDER
- BKDR_EVILOGE
- BKDR_NVICM

- Wmonder

Table 1750. 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

Trojan.Naid is also known as:

- Naid
- Mdmbot.E
- AGENT.GUNZ
- AGENT.AQUP.DROPPER
- AGENT.BMZA
- MCRAT.A
- AGENT.ABQMR

Table 1751. 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

Moudoor is also known as:

- SCAR
- KillProc.14145

Table 1752. 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.

NetTraveler is also known as:

- TravNet
- Netfile

Table 1753. 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.

Winnti is also known as:

- Etso
- SUQ
- Agent.ALQHI

Table 1754. 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.

Mimikatz is also known as:

- Mikatz

Table 1755. Table References

Links

https://github.com/gentilkiwi/mimikatz
https://researchcenter.paloaltonetworks.com/2017/07/unit42-twoface-webshell-persistent-access-point-lateral-movement/

WEBC2

Backdoor attribued to APT1

Table 1756. 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.

Pirpi is also known as:

- Badey
- EXL

Table 1757. 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.

Table 1758. 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).

Backspace is also known as:

- Lecna

Table 1759. 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

Table 1760. 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.

Neteagle is also known as:

- scout
- norton

Table 1761. 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.

Agent.BTZ is also known as:

- ComRat

Table 1762. 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).

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)

Wipbot is also known as:

- Tavdig
- Epic Turla
- WorldCupSec
- TadjMakhal

Table 1763. 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!

Turla is also known as:

- Snake
- Uroburos
- Urouros

Table 1764. 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

Dark Comet

RAT initialy identified in 2011 and still actively used.

Cadelspy

Cadelspy is also known as:

- WinSpy

CMStar

Table 1765. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/03/digital-quartermaster-scenario-demonstrated-in-attacks-against-the-mongolian-government/

DHS2015

DHS2015 is also known as:

- iRAT

Table 1766. 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.

Gh0st Rat is also known as:

- Gh0stRat, GhostRat

Table 1767. 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).

Fakem RAT is also known as:

- FAKEM

Table 1768. Table References

Links
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-fakem-rat.pdf

MFC Huner

MFC Huner is also known as:

- Hupigon
- BKDR_HUPIGON

Table 1769. 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.

Table 1770. 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

CHOPSTICK is also known as:

- webhp
- SPLM

- (.v2 fysbis)

Table 1771. 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.

EVILTOSS is also known as:

- Sedreco
- AZZY
- ADVSTORESHELL
- NETUI

Table 1772. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf

GAMEFISH

backdoor

GAMEFISH is also known as:

- Sednit
- Seduploader
- JHUHUGIT
- Sofacy

Table 1773. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf

SOURFACE

downloader - Older version of CORESHELL

SOURFACE is also known as:

- Sofacy

Table 1774. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf

OLDBAIT

credential harvester

OLDBAIT is also known as:

- Sasfis
- BackDoor-FDU
- IEChecker

Table 1775. 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

CORESHELL is also known as:

- Sofacy

Table 1776. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf

Havex RAT

Havex RAT is also known as:

- Havex

KjW0rm

RAT initially written in VB.

Table 1777. Table References

Links
https://www.sentinelone.com/blog/understanding-kjw0rm-malware-we-dive-in-to-the-tv5-cyber-attack/

TinyTyphon

Badnews

LURK

Oldrea

AmmyAdmin

Matryoshka

TinyZBot

GHOLE

CWoolger

FireMalv

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.

Regin is also known as:

- Prax
- WarriorPride

Table 1778. Table References

Links
https://en.wikipedia.org/wiki/Regin_(malware)

Duqu

Flame

Stuxnet

EquationLaser

EquationDrug

DoubleFantasy

TripleFantasy

Fanny

GrayFish

Babar

Bunny

Casper

NBot

Tafacalou

Tdrop

Troy

Tdrop2

ZXShell

ZXShell is also known as:

- Sensode

Table 1779. Table References

Links
http://www.fireeye.com/blog/uncategorized/2014/02/operation-snowman-deputydog-actor-compromises-us-veterans-of-foreign-wars-website.html

T9000

Table 1780. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/02/t9000-advanced-modular-backdoor-uses-complex-anti-analysis-techniques/

T5000

T5000 is also known as:

- Plat1

Table 1781. Table References

Links
http://www.cylance.com/techblog/Grand-Theft-Auto-Panda.shtml

Taidoor

Table 1782. Table References

Links
http://www.symantec.com/connect/blogs/trojantaidoor-takes-aim-policy-think-tanks

Swisyn

Table 1783. Table References

Links
http://labs.alienvault.com/labs/index.php/2013/latest-adobe-pdf-exploit-used-to-target-uyghur-and-tibetan-activists/

Rekaf

Table 1784. Table References

Links
https://www.proofpoint.com/us/exploring-bergard-old-malware-new-tricks

Scieron

SkeletonKey

Table 1785. Table References

Links
http://www.secureworks.com/cyber-threat-intelligence/threats/skeleton-key-malware-analysis/

Skyipot

Table 1786. Table References

Links
http://labs.alienvault.com/labs/index.php/2011/another-sykipot-sample-likely-targeting-us-federal-agencies/

Spindest

Table 1787. Table References

Links
http://www.threatconnect.com/news/threatconnect-enables-healthy-networking-biomed-life-sciences-industry/

Preshin

Oficla

PCClient RAT

Table 1788. Table References

Links
http://researchcenter.paloaltonetworks.com/2014/10/new-indicators-compromise-apt-group-nitro-uncovered/

Plexor

Mongall

Table 1789. Table References

Links
https://www.fireeye.com/blog/threat-research/2014/09/the-path-to-mass-producing-cyber-attacks.html

NeD Worm

Table 1790. Table References

Links
http://www.clearskysec.com/dustysky/

NewCT

Table 1791. Table References

Links
https://www.fireeye.com/blog/threat-research/2014/09/the-path-to-mass-producing-cyber-attacks.html

Nflog

Table 1792. Table References

Links
https://www.fireeye.com/blog/threat-research/2014/09/the-path-to-mass-producing-cyber-attacks.html

Janicab

Table 1793. Table References

Links
http://blog.avast.com/2013/07/22/multisystem-trojan-janicab-attacks-windows-and-macosx-via-scripts/

Jripbot

Jripbot is also known as:

- Jiripbot

Table 1794. Table References

Links
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/butterfly-corporate-spies-out-for-financial-gain.pdf

Jolob

Table 1795. Table References

Links
http://pwc.blogs.com/cyber_security_updates/2014/10/scanbox-framework-whos-affected-and-whos-using-it-1.html

IsSpace

Table 1796. Table References

Links
https://www.fireeye.com/blog/threat-research/2014/09/the-path-to-mass-producing-cyber-attacks.html

Emotet

Emotet is also known as:

- Geodo

Table 1797. Table References

Links
https://securelist.com/analysis/publications/69560/the-banking-trojan-emotet-detailed-analysis/

Hoardy

Hoardy is also known as:

- Hoarde
- Phindolp
- BS2005

Htran

Table 1798. Table References

Links
http://www.secureworks.com/research/threats/htran/

HTTPBrowser

HTTPBrowser is also known as:

- TokenControl

Table 1799. Table References

Links
https://www.threatstream.com/blog/evasive-maneuvers-the-wekby-group-attempts-to-evade-analysis-via-custom-rop

Disgufa

Elirks

Snifula

Snifula is also known as:

- Ursnif

Table 1800. Table References

Links
https://www.circl.lu/pub/tr-13/

Aumlib

Aumlib is also known as:

- Yayih
- mswab
- Graftor

Table 1801. Table References

Links
http://www.cybersquared.com/killing-with-a-borrowed-knife-chaining-core-cloud-service-profile-infrastructure-for-cyber-attacks

CTRat

Table 1802. Table References

Links
http://www.fireeye.com/blog/technical/threat-intelligence/2014/07/spy-of-the-tiger.html

Emdivi

Emdivi is also known as:

- Newsripper

Table 1803. Table References

Links
http://www.symantec.com/connect/blogs/operation-cloudyomega-ichitaro-zero-day-and-ongoing-cyberespionage-campaign-targeting-japan

Etumbot

Etumbot is also known as:

- Exploz
- Specfix
- RIPTIDE

Table 1804. 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

Fexel is also known as:

- Loneagent

Fysbis

Table 1805. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/02/a-look-into-fysbis-sofacys-linux-backdoor/

Hikit

Table 1806. Table References

Links
https://blog.bit9.com/2013/02/25/bit9-security-incident-update/

Hancitor

Hancitor is also known as:

- Tordal
- Chanitor
- Pony

Table 1807. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/hancitor-ruckguv-reappear

Ruckguv

Table 1808. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/hancitor-ruckguv-reappear

HerHer Trojan

Table 1809. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/05/the-oilrig-campaign-attacks-on-saudi-arabian-organizations-deliver-helminth-backdoor/

Helminth backdoor

Table 1810. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/05/the-oilrig-campaign-attacks-on-saudi-arabian-organizations-deliver-helminth-backdoor/

HDRoot

Table 1811. Table References

Links
http://williamshowalter.com/a-universal-windows-bootkit/

IRONGATE

Table 1812. Table References

Links
https://www.fireeye.com/blog/threat-research/2016/06/irongate_ics_malware.html

ShimRAT

Table 1813. 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.

X-Agent is also known as:

- XAgent

Table 1814. 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

X-Tunnel is also known as:

- XTunnel

Foozer

Table 1815. Table References

Links

https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

WinIDS

Table 1816. Table References

Links
https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

DownRange

Table 1817. Table References

Links
https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

Mad Max

Table 1818. 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

Table 1819. Table References

Links
https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.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.

Table 1820. 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.

Table 1821. 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.

Table 1822. 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.

Table 1823. 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.

Hworm is also known as:

- Houdini

Table 1824. 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.

Backdoor.Dripion is also known as:

- Dripion

Table 1825. 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.

Adwind is also known as:

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

Table 1826. Table References

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

Bedep

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.

Dridex is also known as:

- Cridex

Table 1827. Table References

Links
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/dridex-financial-trojan.pdf

Fareit

Gafgyt

Gamarue

Gamarue is also known as:

- Andromeda

Table 1828. 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.

Table 1829. Table References

Links
https://en.wikipedia.org/wiki/Necurs_botnet

Palevo

Akbot

Akbot is also known as:

- Qbot

- Qakbot
- PinkSlipBot

Table 1830. 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.

Vawtrak

Vawtrak is an information stealing malware family that is primarily used to gain unauthorised access to bank accounts through online banking websites.

Table 1831. 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

Table 1832. 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.

Table 1833. 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

Table 1834. 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…

Yahoyah is also known as:

- W32/Seeav

Table 1835. 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.

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.

Mirai is also known as:

- Linux/Mirai

Table 1836. Table References

Links

https://en.wikipedia.org/wiki/Mirai_(malware)

Masuta

IoT malware based on Mirai but slightly improved.

Masuta is also known as:

- PureMasuta

Table 1837. Table References

Links
https://blog.newskysecurity.com/masuta-satori-creators-second-botnet-weaponizes-a-new-router-exploit-2ddc51cc52a7

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.

Table 1838. 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.

Trojan.Seaduke is also known as:

- Seaduke

Table 1839. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-031915-4935-99

Backdoor.Tinybaron

Incognito RAT

DownRage

DownRage is also known as:

- Carberplike

Table 1840. Table References

Links
https://labsblog.f-secure.com/2015/09/08/sofacy-recycles-carberp-and-metasploit-code/
https://twitter.com/Timo_Steffens/status/814781584536719360

Chthonic

Table 1841. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/threat-actors-using-legitimate-paypal-accounts-to-distribute-chthonic-banking-trojan

GeminiDuke

GeminiDuke is malware that was used by APT29 from 2009 to 2012.

Table 1842. 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.

Zeus is also known as:

- Trojan.Zbot
- Zbot

Table 1843. 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.

Table 1844. 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.

Table 1845. 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.

MM Core is also known as:

- MM Core backdoor
- BigBoss
- SillyGoose
- BaneChant
- StrangeLove

Table 1846. 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]

Table 1847. Table References

Links
https://en.wikipedia.org/wiki/Shamoon

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.

Table 1848. 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.)

Table 1849. 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

Table 1850. 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.

Flokibot is also known as:

- Floki Bot
- Floki

Table 1851. 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.

Table 1852. 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.

Table 1853. Table References

Links
https://blog.cylance.com/shell-crew-variants-continue-to-fly-under-big-avs-radar

adzok

Remote Access Trojan

Table 1854. Table References

Links
https://github.com/kevthehermit/RATDecoders

albertino

Remote Access Trojan

Table 1855. Table References

Links
https://github.com/kevthehermit/RATDecoders

arcom

Remote Access Trojan

Table 1856. Table References

Links
https://github.com/kevthehermit/RATDecoders

blacknix

Remote Access Trojan

Table 1857. Table References

Links
https://github.com/kevthehermit/RATDecoders

bluebanana

Remote Access Trojan

Table 1858. Table References

Links
https://github.com/kevthehermit/RATDecoders

bozok

Remote Access Trojan

Table 1859. Table References

Links
https://github.com/kevthehermit/RATDecoders

clientmesh

Remote Access Trojan

Table 1860. Table References

Links
https://github.com/kevthehermit/RATDecoders

cybergate

Remote Access Trojan

Table 1861. Table References

Links
https://github.com/kevthehermit/RATDecoders

darkcomet

Remote Access Trojan

Table 1862. Table References

Links
https://github.com/kevthehermit/RATDecoders

darkrat

Remote Access Trojan

Table 1863. Table References

Links
https://github.com/kevthehermit/RATDecoders

gh0st

Remote Access Trojan

Table 1864. Table References

Links
https://github.com/kevthehermit/RATDecoders

greame

Remote Access Trojan

Table 1865. Table References

Links
https://github.com/kevthehermit/RATDecoders

hawkeye

Remote Access Trojan

Table 1866. Table References

Links
https://github.com/kevthehermit/RATDecoders

javadropper

Remote Access Trojan

Table 1867. Table References

Links
https://github.com/kevthehermit/RATDecoders

lostdoor

Remote Access Trojan

Table 1868. Table References

Links
https://github.com/kevthehermit/RATDecoders

luxnet

Remote Access Trojan

Table 1869. Table References

Links
https://github.com/kevthehermit/RATDecoders

pandora

Remote Access Trojan

Table 1870. Table References

Links
https://github.com/kevthehermit/RATDecoders

poisonivy

Remote Access Trojan

Table 1871. Table References

Links
https://github.com/kevthehermit/RATDecoders

predatorpain

Remote Access Trojan

Table 1872. Table References

Links
https://github.com/kevthehermit/RATDecoders

punisher

Remote Access Trojan

Table 1873. Table References

Links
https://github.com/kevthehermit/RATDecoders

qrat

Remote Access Trojan

Table 1874. Table References

Links
https://github.com/kevthehermit/RATDecoders

shadowtech

Remote Access Trojan

Table 1875. Table References

Links
https://github.com/kevthehermit/RATDecoders

smallnet

Remote Access Trojan

Table 1876. Table References

Links
https://github.com/kevthehermit/RATDecoders

spygate

Remote Access Trojan

Table 1877. Table References

Links
https://github.com/kevthehermit/RATDecoders

template

Remote Access Trojan

Table 1878. Table References

Links
https://github.com/kevthehermit/RATDecoders

tapaoux

Remote Access Trojan

Table 1879. Table References

Links
https://github.com/kevthehermit/RATDecoders

vantom

Remote Access Trojan

Table 1880. Table References

Links
https://github.com/kevthehermit/RATDecoders

virusrat

Remote Access Trojan

Table 1881. Table References

Links
https://github.com/kevthehermit/RATDecoders

xena

Remote Access Trojan

Table 1882. Table References

Links
https://github.com/kevthehermit/RATDecoders

xtreme

Remote Access Trojan

Table 1883. Table References

Links
https://github.com/kevthehermit/RATDecoders

darkddoser

Remote Access Trojan

Table 1884. Table References

Links
https://github.com/kevthehermit/RATDecoders

jspy

Remote Access Trojan

Table 1885. Table References

Links
https://github.com/kevthehermit/RATDecoders

xrat

Remote Access Trojan

Table 1886. 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.

Table 1887. 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.

Table 1888. 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.

Table 1889. 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.

Table 1890. 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,

Table 1891. 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.

Chrysaor is also known as:

- Pegasus
- Pegasus spyware

Table 1892. 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.

Table 1893. 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.

Table 1894. 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.

Table 1895. 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).

Table 1896. 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.

Table 1897. 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.

Table 1898. 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.

Table 1899. 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.

COOKIEBAG is also known as:

- TROJAN.COOKIES

Table 1900. 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.

Table 1901. 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.

Table 1902. 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.

Table 1903. 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.

GLOOXMAIL is also known as:

- TROJAN.GTALK

Table 1904. 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.

GOGGLES is also known as:

- TROJAN.FOXY

Table 1905. 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.

Table 1906. 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.
```

Table 1907. 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.
```

Table 1908. 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.

Table 1909. 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.

Table 1910. 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.

Table 1911. 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.

Table 1912. 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.

Table 1913. 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).

Table 1914. 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.

Table 1915. 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.

Table 1916. 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.

Table 1917. 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.

Table 1918. 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.

Table 1919. 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.
```

TABMSGSQL is also known as:

- TROJAN LETSGO

Table 1920. 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.

Table 1921. 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.

Table 1922. 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.

Table 1923. 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.

Table 1924. 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.

Table 1925. 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.
```

Table 1926. 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.

Table 1927. 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.

Table 1928. 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.

Table 1929. 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.

Table 1930. 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.

Table 1931. 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.

Table 1932. 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.

Table 1933. 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.

Table 1934. 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.

Table 1935. 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.

Table 1936. 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.

Table 1937. 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.

Table 1938. 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.

Table 1939. 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.

Table 1940. 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.

Table 1941. 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.

Table 1942. 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.

Table 1943. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html

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.

da Vinci RCS is also known as:

- DaVinci

- Morcut

Table 1944. 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.

Table 1945. 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.

FINSPY is also known as:

- BlackOasis

Table 1946. 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

Table 1947. Table References

Links
https://www.f-secure.com/documents/996508/1030745/callisto-group

EARLYSHOVEL

RedHat 7.0 - 7.1 Sendmail 8.11.x exploit

EBBISLAND (EBBSHAVE)

root RCE via RPC XDR overflow in Solaris 6, 7, 8, 9 & 10 (possibly newer) both SPARC and x86

ECHOWRECKER

remote Samba 3.0.x Linux exploit

EASYBEE

appears to be an MDaemon email server vulnerability

EASYPI

an IBM Lotus Notes exploit that gets detected as Stuxnet

EWOKFRENZY

an exploit for IBM Lotus Domino 6.5.4 & 7.0.2

EXPLODINGCAN

an IIS 6.0 exploit that creates a remote backdoor

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)

EDUCATEDSCHOLAR

a SMB exploit (MS09-050)

EMERALDTHREAD

a SMB exploit for Windows XP and Server 2003 (MS10-061)

EMPHASISMINE

a remote IMAP exploit for IBM Lotus Domino 6.6.4 to 8.5.2

ENGLISHMANSDENTIST

Outlook Exchange WebAccess rules to trigger executable code on the client's side to send an email

to other users

EPICHERO

0-day exploit (RCE) for Avaya Call Server

ERRATICGOPHER

SMBv1 exploit targeting Windows XP and Server 2003

ETERNALSYNERGY

a SMBv3 remote code execution flaw for Windows 8 and Server 2012 SP0 (MS17-010)

ETERNALBLUE

SMBv2 exploit for Windows 7 SP1 (MS17-010)

ETERNALCHAMPION

a SMBv1 exploit

ESKIMOROLL

Kerberos exploit targeting 2000, 2003, 2008 and 2008 R2 domain controllers

ESTEEMAUDIT

RDP exploit and backdoor for Windows Server 2003

ECLIPSEDWING

RCE exploit for the Server service in Windows Server 2008 and later (MS08-067)

ETRE

exploit for IMail 8.10 to 8.22

FUZZBUNCH

an exploit framework, similar to MetaSploit

ODDJOB

implant builder and C&C server that can deliver exploits for Windows 2000 and later, also not detected by any AV vendors

PASSFREELY

utility which Bypasses authentication for Oracle servers

SMBTOUCH

check if the target is vulnerable to samba exploits like ETERNALSYNERGY, ETERNALBLUE, ETERNALROMANCE

ERRATICGOPHERTOUCH

Check if the target is running some RPC

IISTOUCH

check if the running IIS version is vulnerable

RPCOUTCH

get info about windows via RPC

DOPU

used to connect to machines exploited by ETERNALCHAMPIONS

FlexSpy

covert surveillance tools

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.

Table 1948. 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.

Table 1949. 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.

Table 1950. 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.

Table 1951. 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).

Trick Bot is also known as:

- TrickBot
- TrickLoader

Table 1952. 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/

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.

Table 1953. Table References

Links
https://resources.netskope.com/h/i/352356475-phishing-as-a-service-phishing-revamped

Moneygram Adwind

Table 1954. 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.
```

Table 1955. 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.

Smoke Loader is also known as:

- Dofoil

Table 1956. 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).

Table 1957. 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.

Fadok is also known as:

- Win32/Fadok

Table 1958. 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.

Table 1959. 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:

Table 1960. Table References

Links
http://blog.talosintelligence.com/2017/05/konni-malware-under-radar-for-years.html

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.

Table 1961. 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.

Table 1962. 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.

Svpeng is also known as:

- trojan-banker.androidos.svpeng.ae

Table 1963. 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.

Table 1964. 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

Table 1965. 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.

Table 1966. 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.

Table 1967. 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.

Table 1968. 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.

Table 1969. 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.

Table 1970. 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.

Table 1971. 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.

Table 1972. 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.

Table 1973. 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.

Table 1974. 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.

Table 1975. 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

Table 1976. 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

Table 1977. 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.

GootKit is also known as:

- Gootkit

Table 1978. 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).

Table 1979. Table References

Links
https://www.agenttesla.com/

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.

Ordinypt is also known as:

- HSDFSDCrypt

Table 1980. 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.

StrongPity2 is also known as:

- Win32/StrongPity2

Table 1981. 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.

Table 1982. 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

Table 1983. 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.

Table 1984. 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

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.

Table 1985. 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.

TRISIS is also known as:

- TRITON

Table 1986. 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

OSX.Pirrit is also known as:

- OSX/Pirrit

Table 1987. 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.

Table 1988. 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.

Table 1989. 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.

Table 1990. 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.

Satori is also known as:

- Okiru

Table 1991. 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.

Table 1992. 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.

Table 1993. 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.

Table 1994. 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.

Table 1995. 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.

Table 1996. Table References

Links
https://www.welivesecurity.com/2017/12/21/sednit-update-fancy-bear-spent-year/

CoinMiner

Monero-mining malware

Table 1997. 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

Table 1998. 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.

MacDownloader is also known as:

- iKitten

Table 1999. 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

Empyre is also known as:

- Empye

Table 2000. 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.

Table 2001. 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.

Table 2002. Table References

Links
https://objective-see.com/blog/blog_0x25.html

Pwnet

A macOS crypto-currency miner, distributed via a trojaned 'CS-GO' hack.

Table 2003. Table References

Links
https://objective-see.com/blog/blog_0x25.html

CpuMeaner

A macOS crypto-currency mining trojan.

Table 2004. 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.

Travle is also known as:

- PYLOT

Table 2005. 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.

Table 2006. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/digmine-cryptocurrency-miner-spreading-via-facebook-messenger/