

# MISP Galaxy Clusters

# MISP Galaxy Cluster

Exploit-Kit.....	1
Microsoft Activity Group actor.....	13
Preventive Measure.....	17
Ransomware.....	20
RAT.....	150
TDS.....	177
Threat actor.....	179
Tool.....	218



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.

## 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 1. Table References

Links
<a href="http://malware.dontneedcoffee.com/2014/09/astnum-ek.html">http://malware.dontneedcoffee.com/2014/09/astnum-ek.html</a>
<a href="http://www.welivesecurity.com/2016/12/06/readers-popular-websites-targeted-stealthy-stegano-exploit-kit-hiding-pixels-malicious-ads/">http://www.welivesecurity.com/2016/12/06/readers-popular-websites-targeted-stealthy-stegano-exploit-kit-hiding-pixels-malicious-ads/</a>

# Terror EK

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

Terror EK is also known as:

- Blaze EK
- Neptune EK

*Table 2. Table References*

Links
<a href="https://www.trustwave.com/Resources/SpiderLabs-Blog/Terror-Exploit-Kit—More-like-Error-Exploit-Kit/">https://www.trustwave.com/Resources/SpiderLabs-Blog/Terror-Exploit-Kit—More-like-Error-Exploit-Kit/</a>

# DealersChoice

DealersChoice is a Flash Player Exploit platform triggered by RTF

DealersChoice is also known as:

- Sednit RTF EK

*Table 3. Table References*

Links
<a href="http://researchcenter.paloaltonetworks.com/2016/10/unit42-dealerschoice-sofacys-flash-player-exploit-platform/">http://researchcenter.paloaltonetworks.com/2016/10/unit42-dealerschoice-sofacys-flash-player-exploit-platform/</a>
<a href="http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-ramps-up-spear-phishing-before-zero-days-get-patched/">http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-ramps-up-spear-phishing-before-zero-days-get-patched/</a>

# DNSChanger

DNSChanger Exploit Kit is an exploit kit targeting Routers via the browser

DNSChanger is also known as:

- RouterEK

*Table 4. Table References*

Links
<a href="http://malware.dontneedcoffee.com/2015/05/an-exploit-kit-dedicated-to-csrf.html">http://malware.dontneedcoffee.com/2015/05/an-exploit-kit-dedicated-to-csrf.html</a>
<a href="https://www.proofpoint.com/us/threat-insight/post/home-routers-under-attack-malvertising-windows-android-devices">https://www.proofpoint.com/us/threat-insight/post/home-routers-under-attack-malvertising-windows-android-devices</a>

# Hunter

Hunter EK is an evolution of 3Ros EK

Hunter is also known as:

- 3ROS Exploit Kit

Table 5. Table References

Links
<a href="https://www.proofpoint.com/us/threat-insight/post/Hunter-Exploit-Kit-Targets-Brazilian-Banking-Customers">https://www.proofpoint.com/us/threat-insight/post/Hunter-Exploit-Kit-Targets-Brazilian-Banking-Customers</a>

# Kaixin

Kaixin is an exploit kit mainly seen behind compromised website in Asia

Kaixin is also known as:

- CK vip

Table 6. Table References

Links
<a href="http://www.kahusecurity.com/2013/deobfuscating-the-ck-exploit-kit/">http://www.kahusecurity.com/2013/deobfuscating-the-ck-exploit-kit/</a>
<a href="http://www.kahusecurity.com/2012/new-chinese-exploit-pack/">http://www.kahusecurity.com/2012/new-chinese-exploit-pack/</a>

# Magnitude

Magnitude EK

Magnitude is also known as:

- Popads EK
- TopExp

Table 7. Table References

Links
<a href="http://malware.dontneedcoffee.com/2013/10/Magnitude.html">http://malware.dontneedcoffee.com/2013/10/Magnitude.html</a>
<a href="https://www.trustwave.com/Resources/SpiderLabs-Blog/A-Peek-Into-the-Lion-s-Den-%E2%80%93-The-Magnitude—aka-PopAds—Exploit-Kit/">https://www.trustwave.com/Resources/SpiderLabs-Blog/A-Peek-Into-the-Lion-s-Den-%E2%80%93-The-Magnitude—aka-PopAds—Exploit-Kit/</a>
<a href="http://malware.dontneedcoffee.com/2014/02/and-real-name-of-magnitude-is.html">http://malware.dontneedcoffee.com/2014/02/and-real-name-of-magnitude-is.html</a>
<a href="https://community.rsa.com/community/products/netwitness/blog/2017/02/09/magnitude-exploit-kit-under-the-hood">https://community.rsa.com/community/products/netwitness/blog/2017/02/09/magnitude-exploit-kit-under-the-hood</a>

# 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 8. Table References*

Links
<a href="https://www.fireeye.com/blog/threat-research/2015/04/a_new_word_document.html">https://www.fireeye.com/blog/threat-research/2015/04/a_new_word_document.html</a>
<a href="https://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/sophos-microsoft-word-intruder-revealed.pdf">https://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/sophos-microsoft-word-intruder-revealed.pdf</a>

# 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 9. Table References*

Links
<a href="http://malware.dontneedcoffee.com/2013/03/hello-neutrino-just-one-more-exploit-kit.html">http://malware.dontneedcoffee.com/2013/03/hello-neutrino-just-one-more-exploit-kit.html</a>
<a href="http://malware.dontneedcoffee.com/2014/11/neutrino-come-back.html">http://malware.dontneedcoffee.com/2014/11/neutrino-come-back.html</a>

# 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 10. 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

*Table 11. 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/>

## 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 12. 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/>

## GreenFlash Sundown

GreenFlash Sundown is a variation of Bizarro Sundown without landing

GreenFlash Sundown is also known as:

- Sundown-GF

*Table 13. 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 notably 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 14. Table References

Links
<a href="https://blogs.sophos.com/2015/07/21/a-closer-look-at-the-angler-exploit-kit/">https://blogs.sophos.com/2015/07/21/a-closer-look-at-the-angler-exploit-kit/</a>
<a href="http://malware.dontneedcoffee.com/2015/12/xxx-is-angler-ek.html">http://malware.dontneedcoffee.com/2015/12/xxx-is-angler-ek.html</a>
<a href="http://malware.dontneedcoffee.com/2016/06/is-it-end-of-angler.html">http://malware.dontneedcoffee.com/2016/06/is-it-end-of-angler.html</a>

# Archie

Archie EK

Table 15. Table References

Links
<a href="https://www.alienvault.com/blogs/labs-research/archie-just-another-exploit-kit">https://www.alienvault.com/blogs/labs-research/archie-just-another-exploit-kit</a>

# 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 16. Table References

Links
<a href="https://www.trustwave.com/Resources/SpiderLabs-Blog/Blackhole-Exploit-Kit-v2/">https://www.trustwave.com/Resources/SpiderLabs-Blog/Blackhole-Exploit-Kit-v2/</a>
<a href="https://nakedsecurity.sophos.com/exploring-the-blackhole-exploit-kit/">https://nakedsecurity.sophos.com/exploring-the-blackhole-exploit-kit/</a>

# 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 17. Table References

Links
<a href="http://www.kahusecurity.com/2011/flash-used-in-idol-malvertisement/">http://www.kahusecurity.com/2011/flash-used-in-idol-malvertisement/</a>
<a href="http://thehackernews.com/2011/10/bleeding-life-2-exploit-pack-released.html">http://thehackernews.com/2011/10/bleeding-life-2-exploit-pack-released.html</a>

## Cool

The Cool Exploit Kit was a kind of BlackHole VIP in 2012/2013

Cool is also known as:

- CEK
- Styxy Cool

Table 18. Table References

Links
<a href="http://malware.dontneedcoffee.com/2012/10/newcoolek.html">http://malware.dontneedcoffee.com/2012/10/newcoolek.html</a>
<a href="http://malware.dontneedcoffee.com/2013/07/a-styxy-cool-ek.html">http://malware.dontneedcoffee.com/2013/07/a-styxy-cool-ek.html</a>
<a href="http://blog.trendmicro.com/trendlabs-security-intelligence/styx-exploit-pack-how-it-works/">http://blog.trendmicro.com/trendlabs-security-intelligence/styx-exploit-pack-how-it-works/</a>

## Fiesta

Fiesta Exploit Kit

Fiesta is also known as:

- NeoSploit
- Fiexp

Table 19. Table References

Links
<a href="http://blog.0x3a.com/post/110052845124/an-in-depth-analysis-of-the-fiesta-exploit-kit-an">http://blog.0x3a.com/post/110052845124/an-in-depth-analysis-of-the-fiesta-exploit-kit-an</a>
<a href="http://www.kahusecurity.com/2011/neosploit-is-back/">http://www.kahusecurity.com/2011/neosploit-is-back/</a>

## 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 20. Table References

Links
<a href="http://malware.dontneedcoffee.com/2016/10/rig-evolves-neutrino-waves-goodbye.html">http://malware.dontneedcoffee.com/2016/10/rig-evolves-neutrino-waves-goodbye.html</a>

## 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 21. Table References

Links
<a href="http://malware.dontneedcoffee.com/2012/11/meet-critxpack-previously-vintage-pack.html">http://malware.dontneedcoffee.com/2012/11/meet-critxpack-previously-vintage-pack.html</a>
<a href="http://malware.dontneedcoffee.com/2013/04/meet-safe-pack-v20-again.html">http://malware.dontneedcoffee.com/2013/04/meet-safe-pack-v20-again.html</a>

## GrandSoft

GrandSoft Exploit Kit was a quite common exploit kit used in 2012/2013

GrandSoft is also known as:

- StampEK
- SofosFO

Table 22. Table References

Links
<a href="http://malware.dontneedcoffee.com/2013/09/FinallyGrandSoft.html">http://malware.dontneedcoffee.com/2013/09/FinallyGrandSoft.html</a>
<a href="http://malware.dontneedcoffee.com/2012/10/neosploit-now-showing-bh-ek-20-like.html">http://malware.dontneedcoffee.com/2012/10/neosploit-now-showing-bh-ek-20-like.html</a>
<a href="https://nakedsecurity.sophos.com/2012/08/24/sophos-sucks-malware/">https://nakedsecurity.sophos.com/2012/08/24/sophos-sucks-malware/</a>

## 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 23. 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 24. Table References*

## Links

<http://malware.dontneedcoffee.com/2013/10/HiMan.html>

## Impact

Impact EK

*Table 25. 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 26. 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 27. Table References

Links
<a href="http://blog.talosintel.com/2014/03/hello-new-exploit-kit.html">http://blog.talosintel.com/2014/03/hello-new-exploit-kit.html</a>
<a href="http://blog.talosintel.com/2014/05/continued-analysis-of-lightsout-exploit.html">http://blog.talosintel.com/2014/05/continued-analysis-of-lightsout-exploit.html</a>
<a href="http://malwageddon.blogspot.fr/2013/09/unknown-ek-by-way-how-much-is-fish.html">http://malwageddon.blogspot.fr/2013/09/unknown-ek-by-way-how-much-is-fish.html</a>

# Nebula

Nebula Exploit Kit has been built on Sundown source and features an internal TDS

Table 28. Table References

Links
<a href="http://malware.dontneedcoffee.com/2017/03/nebula-exploit-kit.html">http://malware.dontneedcoffee.com/2017/03/nebula-exploit-kit.html</a>

# Niteris

Niteris was used mainly to target Russian.

Niteris is also known as:

- CottonCastle

Table 29. Table References

Links
<a href="http://malware.dontneedcoffee.com/2014/06/cottoncastle.html">http://malware.dontneedcoffee.com/2014/06/cottoncastle.html</a>
<a href="http://malware.dontneedcoffee.com/2015/05/another-look-at-niteris-post.html">http://malware.dontneedcoffee.com/2015/05/another-look-at-niteris-post.html</a>

# 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 30. Table References

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

## Phoenix

Phoenix Exploit Kit

Phoenix is also known as:

- PEK

*Table 31. Table References*

Links
<a href="http://malwareint.blogspot.fr/2010/09/phoenix-exploits-kit-v21-inside.html">http://malwareint.blogspot.fr/2010/09/phoenix-exploits-kit-v21-inside.html</a>
<a href="http://blog.trendmicro.com/trendlabs-security-intelligence/now-exploiting-phoenix-exploit-kit-version-2-5/">http://blog.trendmicro.com/trendlabs-security-intelligence/now-exploiting-phoenix-exploit-kit-version-2-5/</a>

## Private Exploit Pack

Private Exploit Pack

Private Exploit Pack is also known as:

- PEP

*Table 32. Table References*

Links
<a href="http://malware.dontneedcoffee.com/2013/07/pep-new-bep.html">http://malware.dontneedcoffee.com/2013/07/pep-new-bep.html</a>
<a href="http://malwageddon.blogspot.fr/2013/07/unknown-ek-well-hey-hey-i-wanna-be.html">http://malwageddon.blogspot.fr/2013/07/unknown-ek-well-hey-hey-i-wanna-be.html</a>

## 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 33. Table References*

Links
<a href="https://www.trustwave.com/Resources/SpiderLabs-Blog/A-Wild-Exploit-Kit-Appears----Meet-RedKit/">https://www.trustwave.com/Resources/SpiderLabs-Blog/A-Wild-Exploit-Kit-Appears----Meet-RedKit/</a>
<a href="http://malware.dontneedcoffee.com/2012/05/inside-redkit.html">http://malware.dontneedcoffee.com/2012/05/inside-redkit.html</a>
<a href="https://nakedsecurity.sophos.com/2013/05/09/redkit-exploit-kit-part-2/">https://nakedsecurity.sophos.com/2013/05/09/redkit-exploit-kit-part-2/</a>

# Sakura

Description Here

Table 34. Table References

Links
<a href="http://www.xylibox.com/2012/01/sakura-exploit-pack-10.html">http://www.xylibox.com/2012/01/sakura-exploit-pack-10.html</a>

# Sundown

Sundown Exploit Kit is mainly built out of stolen code from other exploit kits

Sundown is also known as:

- Beps
- Xer
- Beta

Table 35. Table References

Links
<a href="http://malware.dontneedcoffee.com/2015/06/fast-look-at-sundown-ek.html">http://malware.dontneedcoffee.com/2015/06/fast-look-at-sundown-ek.html</a>
<a href="https://www.virusbulletin.com/virusbulletin/2015/06/beta-exploit-pack-one-more-piece-crimeware-infection-road">https://www.virusbulletin.com/virusbulletin/2015/06/beta-exploit-pack-one-more-piece-crimeware-infection-road</a>

# Sweet-Orange

Sweet Orange

Sweet-Orange is also known as:

- SWO
- Anogre

Table 36. Table References

Links
<a href="http://malware.dontneedcoffee.com/2012/12/juice-sweet-orange-2012-12.html">http://malware.dontneedcoffee.com/2012/12/juice-sweet-orange-2012-12.html</a>

# Styx

Styx Exploit Kit

Table 37. Table References

Links
<a href="http://malware.dontneedcoffee.com/2012/12/crossing-styx-styx-splloit-pack-20-cve.html">http://malware.dontneedcoffee.com/2012/12/crossing-styx-styx-splloit-pack-20-cve.html</a>

<https://krebsonsecurity.com/2013/07/styx-exploit-pack-domo-arigato-pc-roboto/>

<http://malware.dontneedcoffee.com/2013/05/inside-styx-2013-05.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 38. Table References

Links
<a href="https://twitter.com/kafeine">https://twitter.com/kafeine</a>
<a href="https://twitter.com/node5">https://twitter.com/node5</a>
<a href="https://twitter.com/kahusecurity">https://twitter.com/kahusecurity</a>

## 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 39. Table References

Links
<a href="https://blogs.technet.microsoft.com/mmpc/2016/12/14/twin-zero-day-attacks-promethium-and-neodymium-target-individuals-in-europe/">https://blogs.technet.microsoft.com/mmpc/2016/12/14/twin-zero-day-attacks-promethium-and-neodymium-target-individuals-in-europe/</a>

## 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 40. Table References

Links
<a href="https://blogs.technet.microsoft.com/mmpc/2016/12/14/twin-zero-day-attacks-promethium-and-neodymium-target-individuals-in-europe/">https://blogs.technet.microsoft.com/mmpc/2016/12/14/twin-zero-day-attacks-promethium-and-neodymium-target-individuals-in-europe/</a>

## 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 41. Table References

Links
<a href="https://blogs.technet.microsoft.com/mmpc/2016/12/09/windows-10-protection-detection-and-response-against-recent-attacks/">https://blogs.technet.microsoft.com/mmpc/2016/12/09/windows-10-protection-detection-and-response-against-recent-attacks/</a>

## 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 42. Table References

Links
<a href="https://blogs.technet.microsoft.com/mmpc/2016/11/01/our-commitment-to-our-customers-security/">https://blogs.technet.microsoft.com/mmpc/2016/11/01/our-commitment-to-our-customers-security/</a>
<a href="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">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</a>
<a href="https://blogs.technet.microsoft.com/mmpc/2015/11/16/microsoft-security-intelligence-report-strontium/">https://blogs.technet.microsoft.com/mmpc/2015/11/16/microsoft-security-intelligence-report-strontium/</a>

## 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 43. Table References

Links
<a href="https://securelist.com/blog/research/71713/darkhotels-attacks-in-2015/">https://securelist.com/blog/research/71713/darkhotels-attacks-in-2015/</a>
<a href="https://blogs.technet.microsoft.com/mmpc/2016/06/09/reverse-engineering-dubnium-2">https://blogs.technet.microsoft.com/mmpc/2016/06/09/reverse-engineering-dubnium-2</a>
<a href="https://blogs.technet.microsoft.com/mmpc/2016/06/20/reverse-engineering-dubnioms-flash-targeting-exploit/">https://blogs.technet.microsoft.com/mmpc/2016/06/20/reverse-engineering-dubnioms-flash-targeting-exploit/</a>
<a href="https://blogs.technet.microsoft.com/mmpc/2016/07/14/reverse-engineering-dubnium-stage-2-payload-analysis/">https://blogs.technet.microsoft.com/mmpc/2016/07/14/reverse-engineering-dubnium-stage-2-payload-analysis/</a>

## 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 44. Table References

Links
<a href="https://blogs.technet.microsoft.com/mmpc/2016/04/26/digging-deep-for-platinum/">https://blogs.technet.microsoft.com/mmpc/2016/04/26/digging-deep-for-platinum/</a>
<a href="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">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</a>

## 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 45. Table References

Links
<a href="https://blogs.technet.microsoft.com/mmpc/2017/01/25/detecting-threat-actors-in-recent-german-industrial-attacks-with-windows-defender-atp/">https://blogs.technet.microsoft.com/mmpc/2017/01/25/detecting-threat-actors-in-recent-german-industrial-attacks-with-windows-defender-atp/</a>

## 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 46. Table References

Links
<a href="https://blogs.technet.microsoft.com/mmpc/2017/01/25/detecting-threat-actors-in-recent-german-industrial-attacks-with-windows-defender-atp/">https://blogs.technet.microsoft.com/mmpc/2017/01/25/detecting-threat-actors-in-recent-german-industrial-attacks-with-windows-defender-atp/</a>

## 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 47. Table References

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

## Preventive Measure

Preventive measures based on the ransomware document overview as published in <https://docs.google.com/spreadsheets/d/1TWS238xacAto-fLK1n5uTsdijWdCEsGIM0Y0Hvmc5g/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](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 48. Table References

Links
<a href="http://windows.microsoft.com/en-us/windows/backup-restore-faq#1TC=windows-7">http://windows.microsoft.com/en-us/windows/backup-restore-faq#1TC=windows-7</a> .[ <a href="http://windows.microsoft.com/en-us/windows/backup-restore-faq#1TC=windows-7">http://windows.microsoft.com/en-us/windows/backup-restore-faq#1TC=windows-7.</a> ]

# 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 49. Table References

Links
<a href="https://support.office.com/en-us/article/Enable-or-disable-macros-in-Office-files-12b036fd-d140-4e74-b45e-16fed1a7e5c6?ui=en-US&amp;rs=en-US&amp;ad=US">https://support.office.com/en-us/article/Enable-or-disable-macros-in-Office-files-12b036fd-d140-4e74-b45e-16fed1a7e5c6?ui=en-US&amp;rs=en-US&amp;ad=US</a>
<a href="https://www.404techsupport.com/2016/04/office2016-macro-group-policy/?utm_source=dlvr.it&amp;utm_medium=twitter">https://www.404techsupport.com/2016/04/office2016-macro-group-policy/?utm_source=dlvr.it&amp;utm_medium=twitter</a>

# Disable WSH

Disable Windows Script Host

Table 50. Table References

Links
<a href="http://www.windowsnetworking.com/kbase/WindowsTips/WindowsXP/AdminTips/Customization/DisableWindowsScriptingHostWSH.html">http://www.windowsnetworking.com/kbase/WindowsTips/WindowsXP/AdminTips/Customization/DisableWindowsScriptingHostWSH.html</a>

# 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 51. Table References

Links
<a href="http://www.fatdex.net/php/2014/06/01/disable-exes-from-running-inside-any-user-appdata-directory-gpo/">http://www.fatdex.net/php/2014/06/01/disable-exes-from-running-inside-any-user-appdata-directory-gpo/</a>
<a href="http://www.thirdtier.net/ransomware-prevention-kit/">http://www.thirdtier.net/ransomware-prevention-kit/</a>

## 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 52. Table References*

Links
<a href="http://www.sevenforums.com/tutorials/10570-file-extensions-hide-show.htm">http://www.sevenforums.com/tutorials/10570-file-extensions-hide-show.htm</a>

## Enforce UAC Prompt

Enforce administrative users to confirm an action that requires elevated rights

*Table 53. Table References*

Links
<a href="https://technet.microsoft.com/en-us/library/dd835564(WS.10).aspx">https://technet.microsoft.com/en-us/library/dd835564(WS.10).aspx</a>

## 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 54. Table References*

Links
<a href="https://bluesoul.me/2016/05/12/use-gpo-to-change-the-default-behavior-of-potentially-malicious-file-extensions/">https://bluesoul.me/2016/05/12/use-gpo-to-change-the-default-behavior-of-potentially-malicious-file-extensions/</a>

# File Screening

Server-side file screening with the help of File Server Resource Manager

Table 55. Table References

Links
<a href="http://jpelectron.com/sample/Info%20and%20Documents/Stop%20crypto%20badware%20before%20it%20ruins%20your%20day/1-PreventCrypto-Readme.htm">http://jpelectron.com/sample/Info%20and%20Documents/Stop%20crypto%20badware%20before%20it%20ruins%20your%20day/1-PreventCrypto-Readme.htm</a>

## Restrict program execution #2

Block program executions (AppLocker)

Table 56. Table References

Links
<a href="https://technet.microsoft.com/en-us/library/dd759117%28v=ws.11%29.aspx">https://technet.microsoft.com/en-us/library/dd759117%28v=ws.11%29.aspx</a>
<a href="http://social.technet.microsoft.com/wiki/contents/articles/5211.how-to-configure-applocker-group-policy-to-prevent-software-from-running.aspx">http://social.technet.microsoft.com/wiki/contents/articles/5211.how-to-configure-applocker-group-policy-to-prevent-software-from-running.aspx</a>

## EMET

Detect and block exploitation techniques

Table 57. Table References

Links
<a href="http://www.microsoft.com/emet">www.microsoft.com/emet</a> [ <a href="http://www.microsoft.com/emet">www.microsoft.com/emet</a> ]
<a href="http://windowsitpro.com/security/control-emet-group-policy">http://windowsitpro.com/security/control-emet-group-policy</a>

## Sysmon

Detect Ransomware in an early stage with new Sysmon 5 File/Registry monitoring

Table 58. Table References

Links
<a href="https://twitter.com/JohnLaTwC/status/799792296883388416">https://twitter.com/JohnLaTwC/status/799792296883388416</a>

## Ransomware

Ransomware galaxy based on <https://docs.google.com/spreadsheets/d/1TWS238xacAto-fLK1n5uTsdijWdCEsGIM0Y0Hvmc5g/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 59. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/03/nhtnwcuf-ransomware.html">https://id-ransomware.blogspot.co.il/2017/03/nhtnwcuf-ransomware.html</a>

## 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 60. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/03/cryptojacky-ransomware.html">https://id-ransomware.blogspot.co.il/2017/03/cryptojacky-ransomware.html</a>
<a href="https://twitter.com/jiriatvirlab/status/838779371750031360">https://twitter.com/jiriatvirlab/status/838779371750031360</a>

## 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 61. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/03/kaenlupuf-ransomware.html">https://id-ransomware.blogspot.co.il/2017/03/kaenlupuf-ransomware.html</a>

## EnjoyCrypter 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 62. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/03/enjey-crypter-ransomware.html">https://id-ransomware.blogspot.co.il/2017/03/enjey-crypter-ransomware.html</a>
<a href="https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-march-10th-2017-spora-cerber-and-technical-writeups/">https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-march-10th-2017-spora-cerber-and-technical-writeups/</a>
<a href="https://www.bleepingcomputer.com/news/security/embittered-enjey-ransomware-developer-launches-ddos-attack-on-id-ransomware/">https://www.bleepingcomputer.com/news/security/embittered-enjey-ransomware-developer-launches-ddos-attack-on-id-ransomware/</a>

## 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 63. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/03/dangerous-ransomware.html">https://id-ransomware.blogspot.co.il/2017/03/dangerous-ransomware.html</a>

## 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:

- Fl ter r re

Table 64. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/03/vortex-ransomware.html">https://id-ransomware.blogspot.co.il/2017/03/vortex-ransomware.html</a>
<a href="https://twitter.com/struppigel/status/839778905091424260">https://twitter.com/struppigel/status/839778905091424260</a>

## 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 65. 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 66. Table References*

Links

<https://id-ransomware.blogspot.co.il/2017/03/rozalocker-ransomware.html>

<https://twitter.com/jiriavirlab/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 67. 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 68. 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 69. Table References*

Links
-------

<a href="https://id-ransomware.blogspot.co.il/2017/03/project34-ransomware.html">https://id-ransomware.blogspot.co.il/2017/03/project34-ransomware.html</a>
---

## 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 70. Table References

Links
-------

<a href="https://id-ransomware.blogspot.co.il/2017/03/petrwrap-ransomware.html">https://id-ransomware.blogspot.co.il/2017/03/petrwrap-ransomware.html</a>
---

<a href="https://www.bleepingcomputer.com/news/security/petrwrap-ransomware-is-a-petya-offspring-used-in-targeted-attacks/">https://www.bleepingcomputer.com/news/security/petrwrap-ransomware-is-a-petya-offspring-used-in-targeted-attacks/</a>
---

<a href="https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-march-17th-2017-revenge-petrwrap-and-captain-kirk/">https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-march-17th-2017-revenge-petrwrap-and-captain-kirk/</a>
---

<a href="https://securelist.com/blog/research/77762/petrwrap-the-new-petya-based-ransomware-used-in-targeted-attacks/">https://securelist.com/blog/research/77762/petrwrap-the-new-petya-based-ransomware-used-in-targeted-attacks/</a>
---

## 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 71. Table References

Links
-------

<a href="https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-march-17th-2017-revenge-petrwrap-and-captain-kirk/">https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-march-17th-2017-revenge-petrwrap-and-captain-kirk/</a>
---

<a href="https://id-ransomware.blogspot.co.il/2017/03/karmen-ransomware.html">https://id-ransomware.blogspot.co.il/2017/03/karmen-ransomware.html</a>
---

<a href="https://twitter.com/malwrhunterteam/status/841747002438361089">https://twitter.com/malwrhunterteam/status/841747002438361089</a>
---

## 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 72. 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

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..

Turkish FileEncryptor Ransomware is also known as:

- Fake CTB-Locker

Table 73. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/03/turkish-fileencryptor.html">https://id-ransomware.blogspot.co.il/2017/03/turkish-fileencryptor.html</a>
<a href="https://twitter.com/JakubKroustek/status/842034887397908480">https://twitter.com/JakubKroustek/status/842034887397908480</a>

## 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 74. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/03/kirkspock-ransomware.html">https://id-ransomware.blogspot.co.il/2017/03/kirkspock-ransomware.html</a>
<a href="https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-march-17th-2017-revenge-petrwrap-and-captain-kirk/">https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-march-17th-2017-revenge-petrwrap-and-captain-kirk/</a>
<a href="https://www.bleepingcomputer.com/forums/t/642239/kirk-ransomware-help-support-topic-kirk-extension-ransom-notetxt/">https://www.bleepingcomputer.com/forums/t/642239/kirk-ransomware-help-support-topic-kirk-extension-ransom-notetxt/</a>
<a href="http://www.networkworld.com/article/3182415/security/star-trek-themed-kirk-ransomware-has-spock-decryptor-demands-ransom-be-paid-in-monero.html">http://www.networkworld.com/article/3182415/security/star-trek-themed-kirk-ransomware-has-spock-decryptor-demands-ransom-be-paid-in-monero.html</a>
<a href="http://www.securityweek.com/star-trek-themed-kirk-ransomware-emerges">http://www.securityweek.com/star-trek-themed-kirk-ransomware-emerges</a>
<a href="https://www.grahamcluley.com/kirk-ransomware-sports-star-trek-themed-decryptor-little-known-crypto-currency/">https://www.grahamcluley.com/kirk-ransomware-sports-star-trek-themed-decryptor-little-known-crypto-currency/</a>
<a href="https://www.virustotal.com/en/file/39a2201a88f10d81b220c973737f0becedab2e73426ab9923880fb0fb990c5cc/analysis/">https://www.virustotal.com/en/file/39a2201a88f10d81b220c973737f0becedab2e73426ab9923880fb0fb990c5cc/analysis/</a>

## 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 75. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/03/zinocrypt-ransomware.html">https://id-ransomware.blogspot.co.il/2017/03/zinocrypt-ransomware.html</a>
<a href="https://twitter.com/demonslay335?lang=en">https://twitter.com/demonslay335?lang=en</a>
<a href="https://twitter.com/malwrhunterteam/status/842781575410597894">https://twitter.com/malwrhunterteam/status/842781575410597894</a>

## 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 76. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/03/crptxxx-ransomware.html">https://id-ransomware.blogspot.co.il/2017/03/crptxxx-ransomware.html</a>
<a href="https://www.bleepingcomputer.com/forums/t/609690/ultracrypter-cryptxxx-ultradecrypter-ransomware-help-topic-crypt-cryp1/page-84">https://www.bleepingcomputer.com/forums/t/609690/ultracrypter-cryptxxx-ultradecrypter-ransomware-help-topic-crypt-cryp1/page-84</a>
<a href="http://www.fixinfectedpc.com/uninstall-crptxxx-ransomware-from-pc">http://www.fixinfectedpc.com/uninstall-crptxxx-ransomware-from-pc</a>
<a href="https://twitter.com/malwrhunterteam/status/839467168760725508">https://twitter.com/malwrhunterteam/status/839467168760725508</a>

## 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 77. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/03/motd-ransomware.html">https://id-ransomware.blogspot.co.il/2017/03/motd-ransomware.html</a>
<a href="https://www.bleepingcomputer.com/forums/t/642409/motd-of-ransome-hostage/">https://www.bleepingcomputer.com/forums/t/642409/motd-of-ransome-hostage/</a>
<a href="https://www.bleepingcomputer.com/forums/t/642409/motd-ransomware-help-support-topics-motdtxt-and-enc-extension/">https://www.bleepingcomputer.com/forums/t/642409/motd-ransomware-help-support-topics-motdtxt-and-enc-extension/</a>

## 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 78. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/03/cryptodevil-ransomware.html">https://id-ransomware.blogspot.co.il/2017/03/cryptodevil-ransomware.html</a>
<a href="https://twitter.com/PolarToffee/status/843527738774507522">https://twitter.com/PolarToffee/status/843527738774507522</a>

## 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 79. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/03/fabsyscrypto-ransomware.html">https://id-ransomware.blogspot.co.il/2017/03/fabsyscrypto-ransomware.html</a>
<a href="https://twitter.com/struppigel/status/837565766073475072">https://twitter.com/struppigel/status/837565766073475072</a>

## 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 80. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/03/lock2017-ransomware.html">https://id-ransomware.blogspot.co.il/2017/03/lock2017-ransomware.html</a>

## 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 81. 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 82. 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 83. 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/AAAAAAAAAEDg/Zhy3eYf-ek8fY5uM0yHs7E0fEFg2AXG-gCLcB/s1600/failed-key.jpg>

Table 84. 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 85. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/02/dotransomware.html">https://id-ransomware.blogspot.co.il/2017/02/dotransomware.html</a>

## 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 86. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/02/unlock26-ransomware.html">https://id-ransomware.blogspot.co.il/2017/02/unlock26-ransomware.html</a>
<a href="https://www.bleepingcomputer.com/news/security/new-raas-portal-preparing-to-spread-unlock26-ransomware/">https://www.bleepingcomputer.com/news/security/new-raas-portal-preparing-to-spread-unlock26-ransomware/</a>

## 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 87. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/02/pickles-ransomware.html">https://id-ransomware.blogspot.co.il/2017/02/pickles-ransomware.html</a>
<a href="https://twitter.com/JakubKroustek/status/834821166116327425">https://twitter.com/JakubKroustek/status/834821166116327425</a>

## 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 88. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/02/vanguard-ransomware.html">https://id-ransomware.blogspot.co.il/2017/02/vanguard-ransomware.html</a>
<a href="https://twitter.com/JAMESWT_MHT/status/834783231476166657">https://twitter.com/JAMESWT_MHT/status/834783231476166657</a>

## 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 89. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/02/pyl33t-ransomware.html">https://id-ransomware.blogspot.co.il/2017/02/pyl33t-ransomware.html</a>
<a href="https://twitter.com/JanOfficial/status/834706668466405377">https://twitter.com/JanOfficial/status/834706668466405377</a>

## 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 disguise .To delete shadow files use the following commend: C:\Windows\system32\wbem\wmic.exe shadowcopy delete&exit [https://2.bp.blogspot.com/-8qliBHnE9yU/WK1mZn3LgwI/AAAAAAAAAD-M/ZKl7\\_Iwr1agYtlVO3HXaUrwitcowp5\\_NQCLcB/s1600/lock.jpg](https://2.bp.blogspot.com/-8qliBHnE9yU/WK1mZn3LgwI/AAAAAAAAAD-M/ZKl7_Iwr1agYtlVO3HXaUrwitcowp5_NQCLcB/s1600/lock.jpg)

Table 90. Table References

Links
<a href="https://www.bleepingcomputer.com/news/security/new-trump-locker-ransomware-is-a-fraud-just-venuslocker-in-disguise/">https://www.bleepingcomputer.com/news/security/new-trump-locker-ransomware-is-a-fraud-just-venuslocker-in-disguise/</a>
<a href="https://id-ransomware.blogspot.co.il/2017/02/trumplocker.html">https://id-ransomware.blogspot.co.il/2017/02/trumplocker.html</a>
<a href="https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-february-24th-2017-trump-locker-macos-rw-and-cryptomix/">https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-february-24th-2017-trump-locker-macos-rw-and-cryptomix/</a>

## 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 91. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/02/damage-ransomware.html">https://id-ransomware.blogspot.co.il/2017/02/damage-ransomware.html</a>
<a href="https://decrypter.emsisoft.com/damage">https://decrypter.emsisoft.com/damage</a>
<a href="https://twitter.com/demonslay335/status/835664067843014656">https://twitter.com/demonslay335/status/835664067843014656</a>



## 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 92. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/02/xyzware-ransomware.html">https://id-ransomware.blogspot.co.il/2017/02/xyzware-ransomware.html</a>
<a href="https://twitter.com/malwrhunterteam/status/833636006721122304">https://twitter.com/malwrhunterteam/status/833636006721122304</a>

## 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 93. Table References

Links
<a href="https://www.enigmasoftware.com/youarefuckedransomware-removal/">https://www.enigmasoftware.com/youarefuckedransomware-removal/</a>

## 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 94. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/02/cryptconsole-2-ransomware.html">https://id-ransomware.blogspot.co.il/2017/02/cryptconsole-2-ransomware.html</a>

## 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 95. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/02/barraxcrypt-ransomware.html">https://id-ransomware.blogspot.co.il/2017/02/barraxcrypt-ransomware.html</a>
<a href="https://twitter.com/demonslay335/status/83566854036777792">https://twitter.com/demonslay335/status/83566854036777792</a>

## 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 96. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/02/cryptolocker-by-ntk-ransomware.html">https://id-ransomware.blogspot.co.il/2017/02/cryptolocker-by-ntk-ransomware.html</a>

## 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 97. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/02/userfileslocker-ransomware.html">https://id-ransomware.blogspot.co.il/2017/02/userfileslocker-ransomware.html</a>

## 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 98. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017_03_01_archive.html">https://id-ransomware.blogspot.co.il/2017_03_01_archive.html</a>
<a href="https://id-ransomware.blogspot.co.il/2017/03/avastvirusinfo-ransomware.html">https://id-ransomware.blogspot.co.il/2017/03/avastvirusinfo-ransomware.html</a>

## 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..

Table 99. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/03/fabsyscrypto-ransomware.html">https://id-ransomware.blogspot.co.il/2017/03/fabsyscrypto-ransomware.html</a>

## 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 100. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/03/suchsecurity-ransomware.html">https://id-ransomware.blogspot.co.il/2017/03/suchsecurity-ransomware.html</a>

## 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 101. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/02/vhd-ransomware.html">https://id-ransomware.blogspot.co.il/2017/02/vhd-ransomware.html</a>

## 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 102. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/02/kasiski-ransomware.html">https://id-ransomware.blogspot.co.il/2017/02/kasiski-ransomware.html</a>

<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 103. 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 104. 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 105. 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 106. 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 107. 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 108. 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 109. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017_02_01_archive.html">https://id-ransomware.blogspot.co.il/2017_02_01_archive.html</a>
<a href="https://id-ransomware.blogspot.co.il/2017/02/x-files-ransomware.html">https://id-ransomware.blogspot.co.il/2017/02/x-files-ransomware.html</a>

## 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 110. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/02/polski-ransomware.html">https://id-ransomware.blogspot.co.il/2017/02/polski-ransomware.html</a>

## 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 111. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/02/yourransom-ransomware.html">https://id-ransomware.blogspot.co.il/2017/02/yourransom-ransomware.html</a>
<a href="https://www.bleepingcomputer.com/news/security/yourransom-is-the-latest-in-a-long-line-of-prank-and-educational-ransomware/">https://www.bleepingcomputer.com/news/security/yourransom-is-the-latest-in-a-long-line-of-prank-and-educational-ransomware/</a>
<a href="https://twitter.com/_ddoxer/status/827555507741274113">https://twitter.com/_ddoxer/status/827555507741274113</a>

## 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 112. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/02/ranion-raas.html">https://id-ransomware.blogspot.co.il/2017/02/ranion-raas.html</a>
<a href="https://www.bleepingcomputer.com/news/security/ranion-ransomware-as-a-service-available-on-the-dark-web-for-educational-purposes/">https://www.bleepingcomputer.com/news/security/ranion-ransomware-as-a-service-available-on-the-dark-web-for-educational-purposes/</a>

## Potato Ransomware

Wants a ransom to get the victim's files back . Originated in English. Spread worldwide.

Table 113. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/01/polato-ransomware.html">https://id-ransomware.blogspot.co.il/2017/01/polato-ransomware.html</a>

## 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 114. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/01/opentodecrypt-ransomware.html">https://id-ransomware.blogspot.co.il/2017/01/opentodecrypt-ransomware.html</a>

## 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 115. Table References

Links
<a href="http://www.2-spyware.com/remove-ransomplus-ransomware-virus.html">http://www.2-spyware.com/remove-ransomplus-ransomware-virus.html</a>
<a href="https://id-ransomware.blogspot.co.il/2017/01/ransomplus-ransomware.html">https://id-ransomware.blogspot.co.il/2017/01/ransomplus-ransomware.html</a>
<a href="https://twitter.com/jiriatvirlab/status/825411602535088129">https://twitter.com/jiriatvirlab/status/825411602535088129</a>

## 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 116. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/01/cryptconsole-ransomware.html">https://id-ransomware.blogspot.co.il/2017/01/cryptconsole-ransomware.html</a>
<a href="https://www.bleepingcomputer.com/forums/t/638344/cryptconsole-uncrypteoutlookcom-support-topic-how-decrypt-fileshta/">https://www.bleepingcomputer.com/forums/t/638344/cryptconsole-uncrypteoutlookcom-support-topic-how-decrypt-fileshta/</a>
<a href="https://twitter.com/PolarToffee/status/824705553201057794">https://twitter.com/PolarToffee/status/824705553201057794</a>

## ZXZ Ransomware

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 117. Table References

Links
<a href="https://www.bleepingcomputer.com/forums/t/638191/zxz-ransomware-support-help-topic-zxz/?hl=%2Bzxz#entry4168310">https://www.bleepingcomputer.com/forums/t/638191/zxz-ransomware-support-help-topic-zxz/?hl=%2Bzxz#entry4168310</a>
<a href="https://id-ransomware.blogspot.co.il/2017/01/zxz-ransomware.html">https://id-ransomware.blogspot.co.il/2017/01/zxz-ransomware.html</a>

## 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 118. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/01/vxlock-ransomware.html">https://id-ransomware.blogspot.co.il/2017/01/vxlock-ransomware.html</a>

## FunFact Ransomware

Funfact uses an open code for GNU Privacy Guard (GnuPG), then asks to email them to find out the amount 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 119. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/01/funfact.html">https://id-ransomware.blogspot.co.il/2017/01/funfact.html</a>
<a href="http://www.enigmasoftware.com/funfactransomware-removal/">http://www.enigmasoftware.com/funfactransomware-removal/</a>

## 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 120. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/06/zekwacrypt-ransomware.html">https://id-ransomware.blogspot.co.il/2016/06/zekwacrypt-ransomware.html</a>
<a href="http://www.2-spyware.com/remove-zekwacrypt-ransomware-virus.html">http://www.2-spyware.com/remove-zekwacrypt-ransomware-virus.html</a>



## 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 121. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/01/sage-2-ransomware.html">https://id-ransomware.blogspot.co.il/2017/01/sage-2-ransomware.html</a>
<a href="https://isc.sans.edu/forums/diary/Sage+20+Ransomware/21959/">https://isc.sans.edu/forums/diary/Sage+20+Ransomware/21959/</a>
<a href="http://www.securityweek.com/sage-20-ransomware-demands-2000-ransom">http://www.securityweek.com/sage-20-ransomware-demands-2000-ransom</a>
<a href="https://www.bleepingcomputer.com/news/security/sage-2-0-ransomware-gearing-up-for-possible-greater-distribution/">https://www.bleepingcomputer.com/news/security/sage-2-0-ransomware-gearing-up-for-possible-greater-distribution/</a>
<a href="https://www.govcert.admin.ch/blog/27/sage-2.0-comes-with-ip-generation-algorithm-ipga">https://www.govcert.admin.ch/blog/27/sage-2.0-comes-with-ip-generation-algorithm-ipga</a>

## 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 122. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/01/cloudsword.html">https://id-ransomware.blogspot.co.il/2017/01/cloudsword.html</a>
<a href="http://bestsecuritysearch.com/cloudsword-ransomware-virus-removal-steps-protection-updates/">http://bestsecuritysearch.com/cloudsword-ransomware-virus-removal-steps-protection-updates/</a>
<a href="https://twitter.com/BleepinComputer/status/822653335681593345">https://twitter.com/BleepinComputer/status/822653335681593345</a>

## 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 123. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/01/dn-donotopen.html">https://id-ransomware.blogspot.co.il/2017/01/dn-donotopen.html</a>

## 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 encrypts all your files, including: music, MS Office, Open Office, pictures etc..

Table 124. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/01/garryweber.html">https://id-ransomware.blogspot.co.il/2017/01/garryweber.html</a>

## 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 encrypts 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-ftpNjDgI/AAAAAAAAADPk/KVP\\_ji8lR0gENCMYhb324mfzIFFpiaOwACLcB/s1600/site-raas.gif](https://3.bp.blogspot.com/-7fwX40eYL18/WH-ftpNjDgI/AAAAAAAAADPk/KVP_ji8lR0gENCMYhb324mfzIFFpiaOwACLcB/s1600/site-raas.gif) RaaS

Table 125. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/01/satan-raas.html">https://id-ransomware.blogspot.co.il/2017/01/satan-raas.html</a>
<a href="https://www.bleepingcomputer.com/forums/t/637811/satan-ransomware-help-support-topic-stn-extension-help-decrypt-fileshtml/">https://www.bleepingcomputer.com/forums/t/637811/satan-ransomware-help-support-topic-stn-extension-help-decrypt-fileshtml/</a>
<a href="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/the-week-in-ransomware-january-20th-2017-satan-raas-spora-locky-and-more/</a>
<a href="https://www.bleepingcomputer.com/news/security/new-satan-ransomware-available-through-a-ransomware-as-a-service/">https://www.bleepingcomputer.com/news/security/new-satan-ransomware-available-through-a-ransomware-as-a-service/</a>
<a href="https://twitter.com/Xylit01/status/821757718885236740">https://twitter.com/Xylit01/status/821757718885236740</a>

## 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 126. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/01/havoc-ransomware.html">https://id-ransomware.blogspot.co.il/2017/01/havoc-ransomware.html</a>

## 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 127. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/01/cryptosweettooth.html">https://id-ransomware.blogspot.co.il/2017/01/cryptosweettooth.html</a>
<a href="http://sensorstechforum.com/remove-cryptosweettooth-ransomware-restore-locked-files/">http://sensorstechforum.com/remove-cryptosweettooth-ransomware-restore-locked-files/</a>

## 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 128. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/01/kaandsona-ransomtroll.html">https://id-ransomware.blogspot.co.il/2017/01/kaandsona-ransomtroll.html</a>
<a href="https://twitter.com/BleepinComputer/status/819927858437099520">https://twitter.com/BleepinComputer/status/819927858437099520</a>

## 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 129. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/01/lambdalocker.html">https://id-ransomware.blogspot.co.il/2017/01/lambdalocker.html</a>
<a href="http://cfoc.org/how-to-restore-files-affected-by-the-lambdalocker-ransomware/">http://cfoc.org/how-to-restore-files-affected-by-the-lambdalocker-ransomware/</a>

## 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 130. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/01/hakunamatata.html">https://id-ransomware.blogspot.co.il/2017/01/hakunamatata.html</a>
<a href="https://id-ransomware.blogspot.co.il/2016_03_01_archive.html">https://id-ransomware.blogspot.co.il/2016_03_01_archive.html</a>

## 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 131. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/01/marlboro.html">https://id-ransomware.blogspot.co.il/2017/01/marlboro.html</a>
<a href="https://decrypter.emsisoft.com/marlboro">https://decrypter.emsisoft.com/marlboro</a>
<a href="https://www.bleepingcomputer.com/news/security/marlboro-ransomware-defeated-in-one-day/">https://www.bleepingcomputer.com/news/security/marlboro-ransomware-defeated-in-one-day/</a>

## 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/AAAAAAAAADDg/F\\_bN796ndMYnzfUsgSWMXhRxFf3Ic-HtACLcB/s1600/spam-email.png](https://4.bp.blogspot.com/-KkJXiHG80S0/WHX4TBpkamI/AAAAAAAAADDg/F_bN796ndMYnzfUsgSWMXhRxFf3Ic-HtACLcB/s1600/spam-email.png)

Table 132. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/01/spora-ransomware.html">https://id-ransomware.blogspot.co.il/2017/01/spora-ransomware.html</a>
<a href="https://blog.gdatasoftware.com/2017/01/29442-spora-worm-and-ransomware">https://blog.gdatasoftware.com/2017/01/29442-spora-worm-and-ransomware</a>
<a href="http://blog.emsisoft.com/2017/01/10/from-darknet-with-love-meet-spora-ransomware/">http://blog.emsisoft.com/2017/01/10/from-darknet-with-love-meet-spora-ransomware/</a>

## 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 133. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/02/cryptokill-ransomware.html">https://id-ransomware.blogspot.co.il/2017/02/cryptokill-ransomware.html</a>

## 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 134. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/02/allyourdocuments-ransomware.html">https://id-ransomware.blogspot.co.il/2017/02/allyourdocuments-ransomware.html</a>

## 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 135. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/02/serbransom-2017.html">https://id-ransomware.blogspot.co.il/2017/02/serbransom-2017.html</a>
<a href="https://www.bleepingcomputer.com/news/security/ultranationalist-developer-behind-serbransom-ransomware/">https://www.bleepingcomputer.com/news/security/ultranationalist-developer-behind-serbransom-ransomware/</a>
<a href="https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-february-10th-2017-serpent-spora-id-ransomware/">https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-february-10th-2017-serpent-spora-id-ransomware/</a>
<a href="https://twitter.com/malwrhunterteam/status/830116190873849856">https://twitter.com/malwrhunterteam/status/830116190873849856</a>

## 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 136. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/02/fadesoft-ransomware.html">https://id-ransomware.blogspot.co.il/2017/02/fadesoft-ransomware.html</a>
<a href="https://twitter.com/malwrhunterteam/status/829768819031805953">https://twitter.com/malwrhunterteam/status/829768819031805953</a>

<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 137. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/02/hugeme-ransomware.html">https://id-ransomware.blogspot.co.il/2017/02/hugeme-ransomware.html</a>
<a href="https://www.ozbargain.com.au/node/228888?page=3">https://www.ozbargain.com.au/node/228888?page=3</a>
<a href="https://id-ransomware.blogspot.co.il/2016/04/magic-ransomware.html">https://id-ransomware.blogspot.co.il/2016/04/magic-ransomware.html</a>

## 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 138. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/02/dyna-crypt-ransomware.html">https://id-ransomware.blogspot.co.il/2017/02/dyna-crypt-ransomware.html</a>
<a href="https://www.bleepingcomputer.com/news/security/dyna-crypt-not-only-encrypts-your-files-but-also-steals-your-info/">https://www.bleepingcomputer.com/news/security/dyna-crypt-not-only-encrypts-your-files-but-also-steals-your-info/</a>

## 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 139. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/02/serpent-danish-ransomware.html">https://id-ransomware.blogspot.co.il/2017/02/serpent-danish-ransomware.html</a>

## 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 140. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/02/erebus-2017-ransomware.html">https://id-ransomware.blogspot.co.il/2017/02/erebus-2017-ransomware.html</a>
<a href="https://www.bleepingcomputer.com/news/security/erebus-ransomware-utilizes-a-uac-bypass-and-request-a-90-ransom-payment/">https://www.bleepingcomputer.com/news/security/erebus-ransomware-utilizes-a-uac-bypass-and-request-a-90-ransom-payment/</a>

## 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 141. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/02/ransomuhahawhere.html">https://id-ransomware.blogspot.co.il/2017/02/ransomuhahawhere.html</a>

## 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 142. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/02/cancer-ransomware.html">https://id-ransomware.blogspot.co.il/2017/02/cancer-ransomware.html</a>
<a href="https://www.bleepingcomputer.com/news/security/watch-your-computer-go-bonkers-with-cancer-trollware/">https://www.bleepingcomputer.com/news/security/watch-your-computer-go-bonkers-with-cancer-trollware/</a>

## 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 143. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/02/updatehost-ransomware.html">https://id-ransomware.blogspot.co.il/2017/02/updatehost-ransomware.html</a>
<a href="https://www.bleepingcomputer.com/startups/Windows_Update_Host-16362.html">https://www.bleepingcomputer.com/startups/Windows_Update_Host-16362.html</a>

## 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 144. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/01/nemesis-ransomware.html">https://id-ransomware.blogspot.co.il/2017/01/nemesis-ransomware.html</a>

## 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 145. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/01/evil-ransomware.html">https://id-ransomware.blogspot.co.il/2017/01/evil-ransomware.html</a>
<a href="http://www.enigmasoftware.com/evilransomware-removal/">http://www.enigmasoftware.com/evilransomware-removal/</a>
<a href="http://usproins.com/evil-ransomware-is-lurking/">http://usproins.com/evil-ransomware-is-lurking/</a>
<a href="https://twitter.com/jiriavirlab/status/818443491713884161">https://twitter.com/jiriavirlab/status/818443491713884161</a>
<a href="https://twitter.com/PolarToffee/status/826508611878793219">https://twitter.com/PolarToffee/status/826508611878793219</a>

## 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 146. Table References



Links
<a href="https://id-ransomware.blogspot.co.il/2017/01/ocelot-ransomware.html">https://id-ransomware.blogspot.co.il/2017/01/ocelot-ransomware.html</a>
<a href="https://twitter.com/malwrhunterteam/status/817648547231371264">https://twitter.com/malwrhunterteam/status/817648547231371264</a>

## 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 147. Table References*

Links
<a href="https://id-ransomware.blogspot.co.il/2017/01/skyname-ransomware.html">https://id-ransomware.blogspot.co.il/2017/01/skyname-ransomware.html</a>
<a href="https://twitter.com/malwrhunterteam/status/817079028725190656">https://twitter.com/malwrhunterteam/status/817079028725190656</a>

## 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 148. Table References*

Links
<a href="https://id-ransomware.blogspot.co.il/2017/01/mafiaaware.html">https://id-ransomware.blogspot.co.il/2017/01/mafiaaware.html</a>
<a href="https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-january-6th-2017-fsociety-mongodb-pseudo-darkleech-and-more/">https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-january-6th-2017-fsociety-mongodb-pseudo-darkleech-and-more/</a>
<a href="https://twitter.com/BleepinComputer/status/817069320937345024">https://twitter.com/BleepinComputer/status/817069320937345024</a>

## 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 149. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/01/globe3-ransomware.html">https://id-ransomware.blogspot.co.il/2017/01/globe3-ransomware.html</a>
<a href="https://www.bleepingcomputer.com/forums/t/624518/globe-ransomware-help-and-support-purge-extension-how-to-restore-fileshta/">https://www.bleepingcomputer.com/forums/t/624518/globe-ransomware-help-and-support-purge-extension-how-to-restore-fileshta/</a>
<a href="https://www.bleepingcomputer.com/news/security/the-globe-ransomware-wants-to-purge-your-files/">https://www.bleepingcomputer.com/news/security/the-globe-ransomware-wants-to-purge-your-files/</a>
<a href="https://decryptors.blogspot.co.il/2017/01/globe3-decrypter.html">https://decryptors.blogspot.co.il/2017/01/globe3-decrypter.html</a>
<a href="https://decrypter.emsisoft.com/globe3">https://decrypter.emsisoft.com/globe3</a>

## 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/AAAAAAAAAC-Q/KtKdQP6iLY4LHaHgudF5dKs6i1JHQOBmgCLcB/s1600/green1.jpg](https://4.bp.blogspot.com/-xrr6aoB_giw/WG1UrGpmZJI/AAAAAAAAAC-Q/KtKdQP6iLY4LHaHgudF5dKs6i1JHQOBmgCLcB/s1600/green1.jpg)

BleedGreen Ransomware is also known as:

- FireCrypt Ransomware

Table 150. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/01/bleedgreen-ransomware.html">https://id-ransomware.blogspot.co.il/2017/01/bleedgreen-ransomware.html</a>
<a href="https://www.bleepingcomputer.com/news/security/firecrypt-ransomware-comes-with-a-ddos-component/">https://www.bleepingcomputer.com/news/security/firecrypt-ransomware-comes-with-a-ddos-component/</a>

## 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 151. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/01/btcamant.html">https://id-ransomware.blogspot.co.il/2017/01/btcamant.html</a>

## 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 152. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/01/x3m-ransomware.html">https://id-ransomware.blogspot.co.il/2017/01/x3m-ransomware.html</a>

## 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 153. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/01/gog-ransomware.html">https://id-ransomware.blogspot.co.il/2017/01/gog-ransomware.html</a>
<a href="https://twitter.com/BleepinComputer/status/816112218815266816">https://twitter.com/BleepinComputer/status/816112218815266816</a>

## 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 154. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/01/edgelocker-ransomware.html">https://id-ransomware.blogspot.co.il/2017/01/edgelocker-ransomware.html</a>
<a href="https://twitter.com/BleepinComputer/status/815392891338194945">https://twitter.com/BleepinComputer/status/815392891338194945</a>

## 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 155. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/01/red-alert-ransomware.html">https://id-ransomware.blogspot.co.il/2017/01/red-alert-ransomware.html</a>
<a href="https://twitter.com/JaromirHorejsi/status/815557601312329728">https://twitter.com/JaromirHorejsi/status/815557601312329728</a>

## 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 156. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/01/first-ransomware.html">https://id-ransomware.blogspot.co.il/2017/01/first-ransomware.html</a>

## 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 157. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/01/xcrypt-ransomware.html">https://id-ransomware.blogspot.co.il/2017/01/xcrypt-ransomware.html</a>
<a href="https://twitter.com/JakubKroustek/status/825790584971472902">https://twitter.com/JakubKroustek/status/825790584971472902</a>

## 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 158. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/01/7zipper-ransomware.html">https://id-ransomware.blogspot.co.il/2017/01/7zipper-ransomware.html</a>
<a href="https://1.bp.blogspot.com/-ClM0LCPjQuk/WI-BgHTpdNI/AAAAAAAAADc8/JyEQ8-pcJmsXIntuP-MMdE-pohVncxTXQCLcB/s1600/7-zip-logo.png">https://1.bp.blogspot.com/-ClM0LCPjQuk/WI-BgHTpdNI/AAAAAAAAADc8/JyEQ8-pcJmsXIntuP-MMdE-pohVncxTXQCLcB/s1600/7-zip-logo.png</a>

## 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 159. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/01/zyka-ransomware.html">https://id-ransomware.blogspot.co.il/2017/01/zyka-ransomware.html</a>
<a href="https://www.pcrisk.com/removal-guides/10899-zyka-ransomware">https://www.pcrisk.com/removal-guides/10899-zyka-ransomware</a>
<a href="https://download.bleepingcomputer.com/demonslay335/StupidDecrypter.zip">https://download.bleepingcomputer.com/demonslay335/StupidDecrypter.zip</a>
<a href="https://twitter.com/GrujaRS/status/826153382557712385">https://twitter.com/GrujaRS/status/826153382557712385</a>

## SureRansom Ransomware (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 160. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/01/sureransom-ransomware.html">https://id-ransomware.blogspot.co.il/2017/01/sureransom-ransomware.html</a>
<a href="http://www.forbes.com/sites/leemathews/2017/01/27/fake-ransomware-is-tricking-people-into-paying/#777faed0381c">http://www.forbes.com/sites/leemathews/2017/01/27/fake-ransomware-is-tricking-people-into-paying/#777faed0381c</a>

## 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 161. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/01/netflix-ransomware.html">https://id-ransomware.blogspot.co.il/2017/01/netflix-ransomware.html</a>
<a href="http://blog.trendmicro.com/trendlabs-security-intelligence/netflix-scam-delivers-ransomware/">http://blog.trendmicro.com/trendlabs-security-intelligence/netflix-scam-delivers-ransomware/</a>
<a href="https://www.bleepingcomputer.com/news/security/rogue-netflix-app-spreads-netix-ransomware-that-targets-windows-7-and-10-users/">https://www.bleepingcomputer.com/news/security/rogue-netflix-app-spreads-netix-ransomware-that-targets-windows-7-and-10-users/</a>
<a href="http://www.darkreading.com/attacks-breaches/netflix-scam-spreads-ransomware/d/d-id/1328012">http://www.darkreading.com/attacks-breaches/netflix-scam-spreads-ransomware/d/d-id/1328012</a>
<a href="https://4.bp.blogspot.com/-bQQ4DTIClvA/WJCIh6Uq2nI/AAAAAAAAADfY/hB5HcjuGgh8rRJKelHoIRz3Ezth22-wCEw/s1600/form1.jpg">https://4.bp.blogspot.com/-bQQ4DTIClvA/WJCIh6Uq2nI/AAAAAAAAADfY/hB5HcjuGgh8rRJKelHoIRz3Ezth22-wCEw/s1600/form1.jpg</a> [ <a href="https://4.bp.blogspot.com/-bQQ4DTIClvA/WJCIh6Uq2nI/AAAAAAAAADfY/hB5HcjuGgh8rRJKelHoIRz3Ezth22-wCEw/s1600/form1.jpg">https://4.bp.blogspot.com/-bQQ4DTIClvA/WJCIh6Uq2nI/AAAAAAAAADfY/hB5HcjuGgh8rRJKelHoIRz3Ezth22-wCEw/s1600/form1.jpg</a> ]
<a href="https://4.bp.blogspot.com/-ZnWdPDprJOg/WJCPeCtP4HI/AAAAAAAAADfw/kR0if11naSwTAWsuOPiw8ZCPrOtSIz1CgCLcB/s1600/netflix-akk.png">https://4.bp.blogspot.com/-ZnWdPDprJOg/WJCPeCtP4HI/AAAAAAAAADfw/kR0if11naSwTAWsuOPiw8ZCPrOtSIz1CgCLcB/s1600/netflix-akk.png</a>

## 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 CryptoMixfamily.

Table 162. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2017/01/cryptoshield-ransomware.html">https://id-ransomware.blogspot.co.il/2017/01/cryptoshield-ransomware.html</a>
<a href="https://www.bleepingcomputer.com/news/security/cryptomix-variant-named-cryptoshield-1-0-ransomware-distributed-by-exploit-kits/">https://www.bleepingcomputer.com/news/security/cryptomix-variant-named-cryptoshield-1-0-ransomware-distributed-by-exploit-kits/</a>

## 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 163. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/12/mrcr1-ransomware.html">https://id-ransomware.blogspot.co.il/2016/12/mrcr1-ransomware.html</a>
<a href="https://www.bleepingcomputer.com/news/security/-merry-christmas-ransomware-now-steals-user-private-data-via-diamondfox-malware/">https://www.bleepingcomputer.com/news/security/-merry-christmas-ransomware-now-steals-user-private-data-via-diamondfox-malware/</a>
<a href="http://www.zdnet.com/article/not-such-a-merry-christmas-the-ransomware-that-also-steals-user-data/">http://www.zdnet.com/article/not-such-a-merry-christmas-the-ransomware-that-also-steals-user-data/</a>
<a href="https://www.bleepingcomputer.com/news/security/merry-christmas-ransomware-and-its-dev-comodosecurity-not-bringing-holiday-cheer/">https://www.bleepingcomputer.com/news/security/merry-christmas-ransomware-and-its-dev-comodosecurity-not-bringing-holiday-cheer/</a>
<a href="https://decrypter.emsisoft.com/mrcr">https://decrypter.emsisoft.com/mrcr</a>

## 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 164. 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 165. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/12/killdisk-ransomware.html">https://id-ransomware.blogspot.co.il/2016/12/killdisk-ransomware.html</a>
<a href="https://www.bleepingcomputer.com/news/security/killdisk-ransomware-now-targets-linux-prevents-boot-up-has-faulty-encryption/">https://www.bleepingcomputer.com/news/security/killdisk-ransomware-now-targets-linux-prevents-boot-up-has-faulty-encryption/</a>
<a href="https://www.bleepingcomputer.com/news/security/killdisk-disk-wiping-malware-adds-ransomware-component/">https://www.bleepingcomputer.com/news/security/killdisk-disk-wiping-malware-adds-ransomware-component/</a>
<a href="http://www.zdnet.com/article/247000-killdisk-ransomware-demands-a-fortune-forgets-to-unlock-files/">http://www.zdnet.com/article/247000-killdisk-ransomware-demands-a-fortune-forgets-to-unlock-files/</a>
<a href="http://www.securityweek.com/destructive-killdisk-malware-turns-ransomware">http://www.securityweek.com/destructive-killdisk-malware-turns-ransomware</a>
<a href="http://www.welivesecurity.com/2017/01/05/killdisk-now-targeting-linux-demands-250k-ransom-cant-decrypt/">http://www.welivesecurity.com/2017/01/05/killdisk-now-targeting-linux-demands-250k-ransom-cant-decrypt/</a>
<a href="https://cyberx-labs.com/en/blog/new-killdisk-malware-brings-ransomware-into-industrial-domain/">https://cyberx-labs.com/en/blog/new-killdisk-malware-brings-ransomware-into-industrial-domain/</a>

## 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 166. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/12/derialock-ransomware.html">https://id-ransomware.blogspot.co.il/2016/12/derialock-ransomware.html</a>
<a href="https://www.bleepingcomputer.com/news/security/new-derialock-ransomware-active-on-christmas-includes-an-unlock-all-command/">https://www.bleepingcomputer.com/news/security/new-derialock-ransomware-active-on-christmas-includes-an-unlock-all-command/</a>

## BadEncrypt 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 167. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/12/badencrypt-ransomware.html">https://id-ransomware.blogspot.co.il/2016/12/badencrypt-ransomware.html</a>
<a href="https://twitter.com/demonslay335/status/813064189719805952">https://twitter.com/demonslay335/status/813064189719805952</a>

## 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 168. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/12/adamlocker-ransomware.html">https://id-ransomware.blogspot.co.il/2016/12/adamlocker-ransomware.html</a>

## 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 169. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/12/alphabet-ransomware.html">https://id-ransomware.blogspot.co.il/2016/12/alphabet-ransomware.html</a>
<a href="https://twitter.com/PolarToffee/status/812331918633172992">https://twitter.com/PolarToffee/status/812331918633172992</a>

## 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 170. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/12/kokokrypt-ransomware.html">https://id-ransomware.blogspot.co.il/2016/12/kokokrypt-ransomware.html</a>
<a href="https://removevirusadware.com/tips-for-removeing-kokokrypt-ransomware/">https://removevirusadware.com/tips-for-removeing-kokokrypt-ransomware/</a>



## 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 171. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/12/l33taf-locker-ransomware.html">https://id-ransomware.blogspot.co.il/2016/12/l33taf-locker-ransomware.html</a>

## 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 172. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/12/pclock4-sysgop-ransomware.html">https://id-ransomware.blogspot.co.il/2016/12/pclock4-sysgop-ransomware.html</a>

## 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 173. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/12/guster-ransomware.html">https://id-ransomware.blogspot.co.il/2016/12/guster-ransomware.html</a>
<a href="https://twitter.com/BleepinComputer/status/812131324979007492">https://twitter.com/BleepinComputer/status/812131324979007492</a>

## 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/-CIUef8T55f4/WGKb8U4GeaI/AAAAAAAAACzg/UFD0X2sORHYTVRNBSoqd5q7TBrOblQHmgCLcB/s1600/site.png>

Table 174. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/12/roga-ransomware.html">https://id-ransomware.blogspot.co.il/2016/12/roga-ransomware.html</a>

## 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 175. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/12/cryptolocker3-ransomware.html">https://id-ransomware.blogspot.co.il/2016/12/cryptolocker3-ransomware.html</a>

## 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 176. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/12/proposalcrypt-ransomware.html">https://id-ransomware.blogspot.co.il/2016/12/proposalcrypt-ransomware.html</a>
<a href="https://www.archersecuritygroup.com/what-is-ransomware/">https://www.archersecuritygroup.com/what-is-ransomware/</a>
<a href="https://twitter.com/demonslay335/status/812002960083394560">https://twitter.com/demonslay335/status/812002960083394560</a>
<a href="https://twitter.com/malwrhunterteam/status/811613888705859586">https://twitter.com/malwrhunterteam/status/811613888705859586</a>

## 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 177. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/12/manifestus-ransomware.html">https://id-ransomware.blogspot.co.il/2016/12/manifestus-ransomware.html</a>
<a href="https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-december-23rd-2016-cryptxxx-koolova-cerber-and-more/">https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-december-23rd-2016-cryptxxx-koolova-cerber-and-more/</a>

<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 178. Table References*

Links
<a href="https://id-ransomware.blogspot.co.il/2016/12/enkripsipc-ransomware.html">https://id-ransomware.blogspot.co.il/2016/12/enkripsipc-ransomware.html</a>
<a href="https://twitter.com/demonslay335/status/811343914712100872">https://twitter.com/demonslay335/status/811343914712100872</a>
<a href="https://twitter.com/BleepinComputer/status/811264254481494016">https://twitter.com/BleepinComputer/status/811264254481494016</a>
<a href="https://twitter.com/struppigel/status/811587154983981056">https://twitter.com/struppigel/status/811587154983981056</a>

## 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 179. Table References*

Links
<a href="https://id-ransomware.blogspot.co.il/2016/12/braincrypt-ransomware.html">https://id-ransomware.blogspot.co.il/2016/12/braincrypt-ransomware.html</a>

## 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 180. Table References*

Links
<a href="https://id-ransomware.blogspot.co.il/2016/12/msn-cryptolocker-ransomware.html">https://id-ransomware.blogspot.co.il/2016/12/msn-cryptolocker-ransomware.html</a>
<a href="https://twitter.com/struppigel/status/810766686005719040">https://twitter.com/struppigel/status/810766686005719040</a>

## 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 181. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/12/cryptoblock-ransomware.html">https://id-ransomware.blogspot.co.il/2016/12/cryptoblock-ransomware.html</a>
<a href="https://twitter.com/drProct0r/status/810500976415281154">https://twitter.com/drProct0r/status/810500976415281154</a>

## 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 182. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/12/aes-ni-ransomware.html">https://id-ransomware.blogspot.co.il/2016/12/aes-ni-ransomware.html</a>

## 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 183. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/12/koolova-ransomware.html">https://id-ransomware.blogspot.co.il/2016/12/koolova-ransomware.html</a>
<a href="https://www.bleepingcomputer.com/news/security/koolova-ransomware-decrypts-for-free-if-you-read-two-articles-about-ransomware/">https://www.bleepingcomputer.com/news/security/koolova-ransomware-decrypts-for-free-if-you-read-two-articles-about-ransomware/</a>

## 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

Table 184. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/12/fake-globe-ransomware.html">https://id-ransomware.blogspot.co.il/2016/12/fake-globe-ransomware.html</a>
<a href="https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-december-30th-2016-infected-tvs-and-open-source-ransomware-sucks/">https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-december-30th-2016-infected-tvs-and-open-source-ransomware-sucks/</a>
<a href="https://twitter.com/fwosar/status/812421183245287424">https://twitter.com/fwosar/status/812421183245287424</a>
<a href="https://decrypter.emsisoft.com/globeimposter">https://decrypter.emsisoft.com/globeimposter</a>
<a href="https://twitter.com/malwrhunterteam/status/809795402421641216">https://twitter.com/malwrhunterteam/status/809795402421641216</a>

## 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 185. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/12/v8locker-ransomware.html">https://id-ransomware.blogspot.co.il/2016/12/v8locker-ransomware.html</a>

## 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 186. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/12/cryptorium-ransomware.html">https://id-ransomware.blogspot.co.il/2016/12/cryptorium-ransomware.html</a>

## Antihacker2017 Ransomware

It's directed to Russian speaking users, there fore is able to infect mostly 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 187. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/12/antihacker2017-ransomware.html">https://id-ransomware.blogspot.co.il/2016/12/antihacker2017-ransomware.html</a>

## 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/AAAAAAAAACm0/SO8SrwX2UIM3FPZcZI7W76oSDCsnq2vfgCPcB/s1600/code2.jpg>

Table 188. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/12/cia-special-agent-767-ransomware.html">https://id-ransomware.blogspot.co.il/2016/12/cia-special-agent-767-ransomware.html</a>
<a href="https://www.bleepingcomputer.com/virus-removal/remove-cia-special-agent-767-screen-locker">https://www.bleepingcomputer.com/virus-removal/remove-cia-special-agent-767-screen-locker</a>
<a href="https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-december-16th-2016-samas-no-more-ransom-screen-lockers-and-more/">https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-december-16th-2016-samas-no-more-ransom-screen-lockers-and-more/</a>
<a href="https://guides.yoosecurity.com/cia-special-agent-767-virus-locks-your-pc-screen-how-to-unlock/">https://guides.yoosecurity.com/cia-special-agent-767-virus-locks-your-pc-screen-how-to-unlock/</a>

## 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 189. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/12/loveserver-ransomware.html">https://id-ransomware.blogspot.co.il/2016/12/loveserver-ransomware.html</a>

## 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 190. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/12/kraken-ransomware.html">https://id-ransomware.blogspot.co.il/2016/12/kraken-ransomware.html</a>

## 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 191. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/12/antix-ransomware.html">https://id-ransomware.blogspot.co.il/2016/12/antix-ransomware.html</a>

## 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 192. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/12/payday-ransomware.html">https://id-ransomware.blogspot.co.il/2016/12/payday-ransomware.html</a>
<a href="https://twitter.com/BleepinComputer/status/808316635094380544">https://twitter.com/BleepinComputer/status/808316635094380544</a>

## 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 193. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/12/slimhem-ransomware.html">https://id-ransomware.blogspot.co.il/2016/12/slimhem-ransomware.html</a>

## 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 194. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/12/m4n1f3sto-ransomware.html">https://id-ransomware.blogspot.co.il/2016/12/m4n1f3sto-ransomware.html</a>

## 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 195. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/12/ultralocker-ransomware.html">https://id-ransomware.blogspot.co.il/2016/12/ultralocker-ransomware.html</a>
<a href="https://twitter.com/struppigel/status/807161652663742465">https://twitter.com/struppigel/status/807161652663742465</a>

## 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 196. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/12/aeskeygenassist-ransomware.html">https://id-ransomware.blogspot.co.il/2016/12/aeskeygenassist-ransomware.html</a>
<a href="https://id-ransomware.blogspot.co.il/2016/09/dxxd-ransomware.html">https://id-ransomware.blogspot.co.il/2016/09/dxxd-ransomware.html</a>
<a href="https://www.bleepingcomputer.com/forums/t/634258/aes-key-gen-assistprotonmailcom-help-support/">https://www.bleepingcomputer.com/forums/t/634258/aes-key-gen-assistprotonmailcom-help-support/</a>

## 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 197. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/12/code-virus-ransomware.html">https://id-ransomware.blogspot.co.il/2016/12/code-virus-ransomware.html</a>

## 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 198. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/12/flkr-ransomware.html">https://id-ransomware.blogspot.co.il/2016/12/flkr-ransomware.html</a>

## 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 below: <https://www.bleepstatic.com/images/news/ransomware/p/Popcorn-time/refer-a-friend.png>

Table 199. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/12/popcorn-time-ransomware.html">https://id-ransomware.blogspot.co.il/2016/12/popcorn-time-ransomware.html</a>
<a href="https://www.bleepingcomputer.com/news/security/new-scheme-spread-popcorn-time-ransomware-get-chance-of-free-decryption-key/">https://www.bleepingcomputer.com/news/security/new-scheme-spread-popcorn-time-ransomware-get-chance-of-free-decryption-key/</a>

## 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 200. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/12/hackedlocker-ransomware.html">https://id-ransomware.blogspot.co.il/2016/12/hackedlocker-ransomware.html</a>

## 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 201. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/12/goldeneye-ransomware.html">https://id-ransomware.blogspot.co.il/2016/12/goldeneye-ransomware.html</a>
<a href="https://www.bleepingcomputer.com/news/security/petya-ransomware-returns-with-goldeneye-version-continuing-james-bond-theme/">https://www.bleepingcomputer.com/news/security/petya-ransomware-returns-with-goldeneye-version-continuing-james-bond-theme/</a>

## 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 202. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/12/sage-ransomware.html">https://id-ransomware.blogspot.co.il/2016/12/sage-ransomware.html</a>
<a href="https://www.bleepingcomputer.com/forums/t/634978/sage-file-sample-extension-sage/">https://www.bleepingcomputer.com/forums/t/634978/sage-file-sample-extension-sage/</a>
<a href="https://www.bleepingcomputer.com/forums/t/634747/sage-20-ransomware-sage-support-help-topic/">https://www.bleepingcomputer.com/forums/t/634747/sage-20-ransomware-sage-support-help-topic/</a>

## 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 203. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/12/sq-vo-ransomware.html">https://id-ransomware.blogspot.co.il/2016/12/sq-vo-ransomware.html</a>

## 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 204. Table References

Links
<a href="https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-december-2nd-2016-screenlockers-kangaroo-the-sfmta-and-more/">https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-december-2nd-2016-screenlockers-kangaroo-the-sfmta-and-more/</a>
<a href="https://id-ransomware.blogspot.co.il/2016/12/matrix-ransomware.html">https://id-ransomware.blogspot.co.il/2016/12/matrix-ransomware.html</a>
<a href="https://twitter.com/rommeljoen17/status/804251901529231360">https://twitter.com/rommeljoen17/status/804251901529231360</a>

## 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 205. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/11/satan666-ransomware.html">https://id-ransomware.blogspot.co.il/2016/11/satan666-ransomware.html</a>

## 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 206. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/11/rip-ransomware.html">https://id-ransomware.blogspot.co.il/2016/11/rip-ransomware.html</a>
<a href="https://twitter.com/BleepinComputer/status/804810315456200704">https://twitter.com/BleepinComputer/status/804810315456200704</a>

## 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 207. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/11/novalid-ransomware.html">https://id-ransomware.blogspot.co.il/2016/11/novalid-ransomware.html</a>
<a href="https://www.bleepingcomputer.com/forums/t/634754/locked-in-ransomware-help-support-restore-corrupted-fileshtml/">https://www.bleepingcomputer.com/forums/t/634754/locked-in-ransomware-help-support-restore-corrupted-fileshtml/</a>
<a href="https://twitter.com/struppigel/status/807169774098796544">https://twitter.com/struppigel/status/807169774098796544</a>

## 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 208. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/11/chartwig-ransomware.html">https://id-ransomware.blogspot.co.il/2016/11/chartwig-ransomware.html</a>

## 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 209. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/11/renlocker-ransomware.html">https://id-ransomware.blogspot.co.il/2016/11/renlocker-ransomware.html</a>

## 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 210. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/11/thanksgiving-ransomware.html">https://id-ransomware.blogspot.co.il/2016/11/thanksgiving-ransomware.html</a>
<a href="https://id-ransomware.blogspot.co.il/2016/07/stampado-ransomware-1.html">https://id-ransomware.blogspot.co.il/2016/07/stampado-ransomware-1.html</a>
<a href="https://twitter.com/BleepinComputer/status/801486420368093184">https://twitter.com/BleepinComputer/status/801486420368093184</a>

## 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 211. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/11/cockblocker-ransomware.html">https://id-ransomware.blogspot.co.il/2016/11/cockblocker-ransomware.html</a>
<a href="https://twitter.com/jiriativrlab/status/801910919739674624">https://twitter.com/jiriativrlab/status/801910919739674624</a>

## 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 212. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/11/lomix-ransomware.html">https://id-ransomware.blogspot.co.il/2016/11/lomix-ransomware.html</a>

[https://twitter.com/siri\\_urz/status/801815087082274816](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/AAAAAAAAACQE/E63a4FnaOfACZ07s1xUiv\\_haxy8cp5YCACLcB/s1600/ozozalocker.png](https://3.bp.blogspot.com/--jubfYRaRmw/WDaOyZXkAaI/AAAAAAAAACQE/E63a4FnaOfACZ07s1xUiv_haxy8cp5YCACLcB/s1600/ozozalocker.png)

Table 213. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/11/ozozalocker-ransomware.html">https://id-ransomware.blogspot.co.il/2016/11/ozozalocker-ransomware.html</a>
<a href="https://decrypter.emsisoft.com/ozozalocker">https://decrypter.emsisoft.com/ozozalocker</a>
<a href="https://twitter.com/malwrhunterteam/status/801503401867673603">https://twitter.com/malwrhunterteam/status/801503401867673603</a>

## 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 214. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/11/crypute-ransomware-m0on.html">https://id-ransomware.blogspot.co.il/2016/11/crypute-ransomware-m0on.html</a>
<a href="https://www.bleepingcomputer.com/virus-removal/threat/ransomware/">https://www.bleepingcomputer.com/virus-removal/threat/ransomware/</a>

## 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 215. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/11/nmoreira-ransomware.html">https://id-ransomware.blogspot.co.il/2016/11/nmoreira-ransomware.html</a>
<a href="https://id-ransomware.blogspot.co.il/2016/10/airacrop-ransomware.html">https://id-ransomware.blogspot.co.il/2016/10/airacrop-ransomware.html</a>

## 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 216. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/11/windowslocker-ransomware.html">https://id-ransomware.blogspot.co.il/2016/11/windowslocker-ransomware.html</a>
<a href="https://malwarebytes.app.box.com/s/gdu18hr17mwqszej3hgw5m3sw84k8hlph">https://malwarebytes.app.box.com/s/gdu18hr17mwqszej3hgw5m3sw84k8hlph</a>
<a href="https://rol.in/VindowsUnlocker.zip">https://rol.in/VindowsUnlocker.zip</a>
<a href="https://twitter.com/JakubKroustek/status/800729944112427008">https://twitter.com/JakubKroustek/status/800729944112427008</a>
<a href="https://www.bleepingcomputer.com/news/security/windowslocker-ransomware-mimics-tech-support-scam-not-the-other-way-around/">https://www.bleepingcomputer.com/news/security/windowslocker-ransomware-mimics-tech-support-scam-not-the-other-way-around/</a>

## 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 217. Table References

Links
<a href="http://id-ransomware.blogspot.co.il/2016/09/donald-trump-ransomware.html">http://id-ransomware.blogspot.co.il/2016/09/donald-trump-ransomware.html</a>
<a href="https://www.bleepingcomputer.com/news/security/the-donald-trump-ransomware-tries-to-build-walls-around-your-files/">https://www.bleepingcomputer.com/news/security/the-donald-trump-ransomware-tries-to-build-walls-around-your-files/</a>

## 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 218. Table References

Links
<a href="http://id-ransomware.blogspot.co.il/2016/09/nagini-voldemort-ransomware.html">http://id-ransomware.blogspot.co.il/2016/09/nagini-voldemort-ransomware.html</a>
<a href="https://www.bleepingcomputer.com/news/security/the-nagini-ransomware-sics-voldemort-on-your-files/">https://www.bleepingcomputer.com/news/security/the-nagini-ransomware-sics-voldemort-on-your-files/</a>

## 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 219. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/11/shellocker-ransomware.html">https://id-ransomware.blogspot.co.il/2016/11/shellocker-ransomware.html</a>
<a href="https://twitter.com/JakubKroustek/status/799388289337671680">https://twitter.com/JakubKroustek/status/799388289337671680</a>

## 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 220. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/11/chip-ransomware.html">https://id-ransomware.blogspot.co.il/2016/11/chip-ransomware.html</a>
<a href="http://malware-traffic-analysis.net/2016/11/17/index.html">http://malware-traffic-analysis.net/2016/11/17/index.html</a>
<a href="https://www.bleepingcomputer.com/news/security/rig-e-exploit-kit-now-distributing-new-chip-ransomware/">https://www.bleepingcomputer.com/news/security/rig-e-exploit-kit-now-distributing-new-chip-ransomware/</a>

## 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](mailto:bitcoin143@india.com). CrySiS variant

Table 221. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/11/dharma-ransomware.html">https://id-ransomware.blogspot.co.il/2016/11/dharma-ransomware.html</a>
<a href="https://www.bleepingcomputer.com/news/security/kaspersky-releases-decryptor-for-the-dharma-ransomware/">https://www.bleepingcomputer.com/news/security/kaspersky-releases-decryptor-for-the-dharma-ransomware/</a>

## 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 222. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/11/angela-merkel-ransomware.html">https://id-ransomware.blogspot.co.il/2016/11/angela-merkel-ransomware.html</a>
<a href="https://twitter.com/malwrhunterteam/status/798268218364358656">https://twitter.com/malwrhunterteam/status/798268218364358656</a>

## 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 223. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/11/cryptoluck-ransomware.html">https://id-ransomware.blogspot.co.il/2016/11/cryptoluck-ransomware.html</a>
<a href="http://www.bleepingcomputer.com/news/security/cryptoluck-ransomware-being-malvertised-via-rig-e-exploit-kits/">http://www.bleepingcomputer.com/news/security/cryptoluck-ransomware-being-malvertised-via-rig-e-exploit-kits/</a>
<a href="https://twitter.com/malwareforme/status/798258032115322880">https://twitter.com/malwareforme/status/798258032115322880</a>

## 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 224. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/11/crypton-ransomware.html">https://id-ransomware.blogspot.co.il/2016/11/crypton-ransomware.html</a>
<a href="https://decrypter.emsisoft.com/crypton">https://decrypter.emsisoft.com/crypton</a>



<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 225. 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 226. 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 227. 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/supteam-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:

- Kolobocheq Ransomware

*Table 228. 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 229. 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 230. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/11/telecrypt-ransomware.html">https://id-ransomware.blogspot.co.il/2016/11/telecrypt-ransomware.html</a>
<a href="http://www.securityweek.com/telecrypt-ransomwares-encryption-cracked">http://www.securityweek.com/telecrypt-ransomwares-encryption-cracked</a>
<a href="https://malwarebytes.app.box.com/s/kkxwzgbpwe7oh59xqfwcz97uk0q05kp3">https://malwarebytes.app.box.com/s/kkxwzgbpwe7oh59xqfwcz97uk0q05kp3</a>
<a href="https://blog.malwarebytes.com/threat-analysis/2016/11/telecrypt-the-ransomware-abusing-telegram-api-defeated/">https://blog.malwarebytes.com/threat-analysis/2016/11/telecrypt-the-ransomware-abusing-telegram-api-defeated/</a>
<a href="https://securelist.com/blog/research/76558/the-first-cryptor-to-exploit-telegram/">https://securelist.com/blog/research/76558/the-first-cryptor-to-exploit-telegram/</a>

## 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 231. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/11/cerbertear-ransomware.html">https://id-ransomware.blogspot.co.il/2016/11/cerbertear-ransomware.html</a>
<a href="https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/november-2016-month-ransomware/">https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/november-2016-month-ransomware/</a>
<a href="https://twitter.com/struppigel/status/795630452128227333">https://twitter.com/struppigel/status/795630452128227333</a>

## 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 232. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/11/fucksociety-ransomware.html">https://id-ransomware.blogspot.co.il/2016/11/fucksociety-ransomware.html</a>

## 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 233. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/11/paydos-ransomware-serpent.html">https://id-ransomware.blogspot.co.il/2016/11/paydos-ransomware-serpent.html</a>
<a href="https://www.bleepingcomputer.com/news/security/ransomware-goes-retro-with-paydos-and-serpent-written-as-batch-files/">https://www.bleepingcomputer.com/news/security/ransomware-goes-retro-with-paydos-and-serpent-written-as-batch-files/</a>
<a href="https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-4th-2016-cerber-paydos-alcatraz-locker-and-more/">https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-4th-2016-cerber-paydos-alcatraz-locker-and-more/</a>
<a href="https://www.proofpoint.com/us/threat-insight/post/new-serpent-ransomware-targets-danish-speakers">https://www.proofpoint.com/us/threat-insight/post/new-serpent-ransomware-targets-danish-speakers</a>

## 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 234. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/11/zscreenlocker-ransomware.html">https://id-ransomware.blogspot.co.il/2016/11/zscreenlocker-ransomware.html</a>
<a href="https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/november-2016-month-ransomware/">https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/november-2016-month-ransomware/</a>
<a href="https://twitter.com/struppigel/status/794077145349967872">https://twitter.com/struppigel/status/794077145349967872</a>

## 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 235. 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 236. 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 237. 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 238. 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 239. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/11/dummyencrypter-ransomware.html">https://id-ransomware.blogspot.co.il/2016/11/dummyencrypter-ransomware.html</a>

## 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 240. Table References

Links
<a href="http://virusinfo.info/showthread.php?t=201710">http://virusinfo.info/showthread.php?t=201710</a>
<a href="https://id-ransomware.blogspot.co.il/2016/11/encryptss77-ransomware.html">https://id-ransomware.blogspot.co.il/2016/11/encryptss77-ransomware.html</a>

## 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 241. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/11/winrarer-ransomware.html">https://id-ransomware.blogspot.co.il/2016/11/winrarer-ransomware.html</a>

## 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 242. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/11/russian-globe-ransomware.html">https://id-ransomware.blogspot.co.il/2016/11/russian-globe-ransomware.html</a>

## 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 243. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/11/zerocrypt-ransomware.html">https://id-ransomware.blogspot.co.il/2016/11/zerocrypt-ransomware.html</a>

## 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 244. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/10/rotorcrypt-ransomware.html">https://id-ransomware.blogspot.co.il/2016/10/rotorcrypt-ransomware.html</a>

## 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 245. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/10/ishtar-ransomware.html">https://id-ransomware.blogspot.co.il/2016/10/ishtar-ransomware.html</a>

## 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 246. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/10/masterbuster-ransomware.html">https://id-ransomware.blogspot.co.il/2016/10/masterbuster-ransomware.html</a>
<a href="https://twitter.com/struppigel/status/791943837874651136">https://twitter.com/struppigel/status/791943837874651136</a>

## 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 247. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/10/jackpot-ransomware.html">https://id-ransomware.blogspot.co.il/2016/10/jackpot-ransomware.html</a>
<a href="https://twitter.com/struppigel/status/791639214152617985">https://twitter.com/struppigel/status/791639214152617985</a>
<a href="https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-28-2016-locky-angry-duck-and-more/">https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-28-2016-locky-angry-duck-and-more/</a>

## ONYX 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.. Georgian ransomware

Table 248. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/10/onyx-ransomware.html">https://id-ransomware.blogspot.co.il/2016/10/onyx-ransomware.html</a>
<a href="https://twitter.com/struppigel/status/791557636164558848">https://twitter.com/struppigel/status/791557636164558848</a>
<a href="https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-28-2016-locky-angry-duck-and-more/">https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-28-2016-locky-angry-duck-and-more/</a>

## 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 249. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/10/ifn643-ransomware.html">https://id-ransomware.blogspot.co.il/2016/10/ifn643-ransomware.html</a>
<a href="https://twitter.com/struppigel/status/791576159960072192">https://twitter.com/struppigel/status/791576159960072192</a>
<a href="https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-28-2016-locky-angry-duck-and-more/">https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-28-2016-locky-angry-duck-and-more/</a>

## 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 250. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/10/alcatraz-locker-ransomware.html">https://id-ransomware.blogspot.co.il/2016/10/alcatraz-locker-ransomware.html</a>
<a href="https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-4th-2016-cerber-paydos-alcatraz-locker-and-more/">https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-4th-2016-cerber-paydos-alcatraz-locker-and-more/</a>
<a href="https://twitter.com/PolarToffee/status/792796055020642304">https://twitter.com/PolarToffee/status/792796055020642304</a>

## 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 251. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/10/esmeralda-ransomware.html">https://id-ransomware.blogspot.co.il/2016/10/esmeralda-ransomware.html</a>
<a href="https://www.bleepingcomputer.com/forums/t/630835/esmeralda-ransomware/">https://www.bleepingcomputer.com/forums/t/630835/esmeralda-ransomware/</a>

## 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 252. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/10/encryptile-ransomware.html">https://id-ransomware.blogspot.co.il/2016/10/encryptile-ransomware.html</a>

## 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/AAAAAAAAABzA/i8V-Kg8Gstcn\\_7-YZK\\_PDC2VgafWcfDgCLcB/s1600/survey-screen.png](https://1.bp.blogspot.com/-72ECd1vsUdE/WBMSzPQEgZI/AAAAAAAAABzA/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/AAAAAAAAABzc/1KvAMeDmY2w9BN9vkqZO8LWkBu7T9mvDAcLcB/s1600/ThxForYurTyme.JPG](https://1.bp.blogspot.com/-2AlvtcvdyUY/WBMVptG_V5I/AAAAAAAAABzc/1KvAMeDmY2w9BN9vkqZO8LWkBu7T9mvDAcLcB/s1600/ThxForYurTyme.JPG)

Table 253. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/10/fileice-ransomware-survey.html">https://id-ransomware.blogspot.co.il/2016/10/fileice-ransomware-survey.html</a>
<a href="https://www.bleepingcomputer.com/news/security/in-dev-ransomware-forces-you-do-to-survey-before-unlocking-computer/">https://www.bleepingcomputer.com/news/security/in-dev-ransomware-forces-you-do-to-survey-before-unlocking-computer/</a>

## CryptoWire 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 254. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/10/cryptowire-ransomware.html">https://id-ransomware.blogspot.co.il/2016/10/cryptowire-ransomware.html</a>
<a href="https://twitter.com/struppigel/status/791554654664552448">https://twitter.com/struppigel/status/791554654664552448</a>
<a href="https://www.bleepingcomputer.com/news/security/-proof-of-concept-cryptowire-ransomware-spawns-lomix-and-ultralocker-families/">https://www.bleepingcomputer.com/news/security/-proof-of-concept-cryptowire-ransomware-spawns-lomix-and-ultralocker-families/</a>

## 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 255. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/10/hucky-ransomware-hungarian-locky.html">https://id-ransomware.blogspot.co.il/2016/10/hucky-ransomware-hungarian-locky.html</a>

<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 256. 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 257. 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 258. 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 259. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/10/asn1-encoder-ransomware.html">https://id-ransomware.blogspot.co.il/2016/10/asn1-encoder-ransomware.html</a>
<a href="https://malwarebreakdown.com/2017/03/02/rig-ek-at-92-53-105-43-drops-asn1-ransomware/">https://malwarebreakdown.com/2017/03/02/rig-ek-at-92-53-105-43-drops-asn1-ransomware/</a>

## 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/AAAAAAAAABxI/DO3vycRW-TozneSfRTdeKyXGNETjSMehgCLcB/s1600/all-images.gif>

Table 260. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/10/click-me-ransomware.html">https://id-ransomware.blogspot.co.il/2016/10/click-me-ransomware.html</a>
<a href="https://www.youtube.com/watch?v=Xe30kV4ip8w">https://www.youtube.com/watch?v=Xe30kV4ip8w</a>

## 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 261. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/10/airacrop-ransomware.html">https://id-ransomware.blogspot.co.il/2016/10/airacrop-ransomware.html</a>

## 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 262. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/10/japanlocker-ransomware.html">https://id-ransomware.blogspot.co.il/2016/10/japanlocker-ransomware.html</a>
<a href="https://www.cyber.nj.gov/threat-profiles/ransomware-variants/japanlocker">https://www.cyber.nj.gov/threat-profiles/ransomware-variants/japanlocker</a>
<a href="https://github.com/fortiguard-lion/schRansomwareDecryptor/blob/master/schRansomwarev1_decryptor.php">https://github.com/fortiguard-lion/schRansomwareDecryptor/blob/master/schRansomwarev1_decryptor.php</a>
<a href="https://blog.fortinet.com/2016/10/19/japanlocker-an-excavation-to-its-indonesian-roots">https://blog.fortinet.com/2016/10/19/japanlocker-an-excavation-to-its-indonesian-roots</a>

## 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 263. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/10/anubis-ransomware.html">https://id-ransomware.blogspot.co.il/2016/10/anubis-ransomware.html</a>
<a href="http://nyxbone.com/malware/Anubis.html">http://nyxbone.com/malware/Anubis.html</a>

## 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 264. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/10/xtplocker-ransomware.html">https://id-ransomware.blogspot.co.il/2016/10/xtplocker-ransomware.html</a>

## 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 265. 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 266. Table References*

Links

<https://id-ransomware.blogspot.co.il/2016/10/apt-ransomware-2.html>

## Windows\_Security 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..

Windows\_Security Ransomware is also known as:

- WS Go Ransomware
- Trojan.Encoder.6491

*Table 267. Table References*

Links

<https://id-ransomware.blogspot.co.il/2016/10/ws-go-ransomware.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 268. Table References*

Links
-------

<a href="https://id-ransomware.blogspot.co.il/2016/10/ncrypt-ransomware.html">https://id-ransomware.blogspot.co.il/2016/10/ncrypt-ransomware.html</a>
---

## 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](mailto:devVenisRansom@protonmail.com)

Table 269. Table References

Links
-------

<a href="https://id-ransomware.blogspot.co.il/2016/10/venis-ransomware.html">https://id-ransomware.blogspot.co.il/2016/10/venis-ransomware.html</a>
---

<a href="https://twitter.com/Antelox/status/785849412635521024">https://twitter.com/Antelox/status/785849412635521024</a>
---

<a href="http://pastebin.com/HuK99Xmj">http://pastebin.com/HuK99Xmj</a>
---

## 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 270. Table References

Links
-------

<a href="https://id-ransomware.blogspot.co.il/2016/10/enigma-2-ransomware.html">https://id-ransomware.blogspot.co.il/2016/10/enigma-2-ransomware.html</a>
---

## 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 271. Table References

Links
-------

<a href="https://id-ransomware.blogspot.co.il/2016/10/deadly-ransomware.html">https://id-ransomware.blogspot.co.il/2016/10/deadly-ransomware.html</a>
---

<a href="https://twitter.com/malwrhunterteam/status/785533373007728640">https://twitter.com/malwrhunterteam/status/785533373007728640</a>
---

## 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 272. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/10/comrade-circle-ransomware.html">https://id-ransomware.blogspot.co.il/2016/10/comrade-circle-ransomware.html</a>

## 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 273. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/10/globe2-ransomware.html">https://id-ransomware.blogspot.co.il/2016/10/globe2-ransomware.html</a>
<a href="https://success.trendmicro.com/portal_kb_articleDetail?solutionid=1114221">https://success.trendmicro.com/portal_kb_articleDetail?solutionid=1114221</a>

## 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 274. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/10/kostya-ransomware.html">https://id-ransomware.blogspot.co.il/2016/10/kostya-ransomware.html</a>
<a href="http://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-14-2016-exotic-lockydump-comrade-and-more/">http://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-14-2016-exotic-lockydump-comrade-and-more/</a>

## 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 275. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/10/fs0ciety-locker-ransomware.htm">https://id-ransomware.blogspot.co.il/2016/10/fs0ciety-locker-ransomware.htm</a>

## 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 276. Table References

Links
<a href="https://id-ransomware.blogspot.co.il/2016/09/erebus-ransomware.html">https://id-ransomware.blogspot.co.il/2016/09/erebus-ransomware.html</a>

## 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 277. Table References

Links
<a href="https://gist.github.com/rain-1/989428fa5504f378b993ee6efbc0b168">https://gist.github.com/rain-1/989428fa5504f378b993ee6efbc0b168</a>

## .CryptoHasYou.

Ransomware

Table 278. Table References

Links
<a href="http://www.nyxbone.com/malware/CryptoHasYou.html">http://www.nyxbone.com/malware/CryptoHasYou.html</a>

## 777

Ransomware

777 is also known as:

- Sevleg

Table 279. Table References

Links
<a href="https://decrypter.emsisoft.com/777">https://decrypter.emsisoft.com/777</a>

## 7ev3n

Ransomware

7ev3n is also known as:

- 7ev3n-HONE\$T

Table 280. Table References

Links
<a href="https://github.com/hasherezade/malware_analysis/tree/master/7ev3n">https://github.com/hasherezade/malware_analysis/tree/master/7ev3n</a>
<a href="https://www.youtube.com/watch?v=RDNbH5HDO1E&amp;feature=youtu.be">https://www.youtube.com/watch?v=RDNbH5HDO1E&amp;feature=youtu.be</a>
<a href="http://www.nyxbone.com/malware/7ev3n-HONE\$T.html">http://www.nyxbone.com/malware/7ev3n-HONE\$T.html</a>

## 8lock8

Ransomware Based on HiddenTear

Table 281. Table References

Links
<a href="http://www.bleepingcomputer.com/forums/t/614025/8lock8-help-support-topic-8lock8-read-ittxt/">http://www.bleepingcomputer.com/forums/t/614025/8lock8-help-support-topic-8lock8-read-ittxt/</a>

## AiraCrop

Ransomware related to TeamXRat

Table 282. Table References

Links
-------

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

## Al-Namrood

Ransomware

*Table 283. Table References*

Links

<https://decrypter.emsisoft.com/al-namrood>

## ALFA Ransomware

Ransomware Made by creators of Cerber

*Table 284. Table References*

Links

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

## Alma Ransomware

Ransomware

*Table 285. Table References*

Links

<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\_uacuER8g2H3f1EfbtYBw5QFWeUmrjk-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\_uacuER8g2H3f1EfbtYBw5QFWeUmrjk-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&em>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\_uacuER8g2H3f1EfbtYBw5QFWeUmrjk-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\_uacuER8g2H3f1EfbtYBw5QFWeUmrjk-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&

<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 286. 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](mailto:amba@riseup.net)

*Table 287. Table References*

Links

[https://twitter.com/benkow\\_/status/747813034006020096](https://twitter.com/benkow_/status/747813034006020096)

## AngleWare

Ransomware

*Table 288. Table References*

Links

<https://twitter.com/BleepinComputer/status/844531418474708993>

## Anony

Ransomware Based on HiddenTear

Anony is also known as:

- ngocanh

*Table 289. Table References*

Links
<a href="https://twitter.com/struppigel/status/842047409446387714">https://twitter.com/struppigel/status/842047409446387714</a>

## Apocalypse

Ransomware [decryption@mail.ru](mailto:decryption@mail.ru) [recoveryhelp@bk.ru](mailto:recoveryhelp@bk.ru) [ransomware.attack@list.ru](mailto:ransomware.attack@list.ru)  
[esmeraldaencryption@mail.ru](mailto:esmeraldaencryption@mail.ru) [dr.compress@bk.ru](mailto:dr.compress@bk.ru)

Apocalypse is also known as:

- Fabiansomeware

*Table 290. Table References*

Links
<a href="https://decrypter.emsisoft.com/apocalypse">https://decrypter.emsisoft.com/apocalypse</a>
<a href="http://blog.emsisoft.com/2016/06/29/apocalypse-ransomware-which-targets-companies-through-insecure-rdp/">http://blog.emsisoft.com/2016/06/29/apocalypse-ransomware-which-targets-companies-through-insecure-rdp/</a>

## ApocalypseVM

Ransomware Apocalypse ransomware version which uses VMprotect

*Table 291. Table References*

Links
<a href="http://decrypter.emsisoft.com/download/apocalypsevm">http://decrypter.emsisoft.com/download/apocalypsevm</a>

## AutoLocky

Ransomware

*Table 292. Table References*

Links
<a href="https://decrypter.emsisoft.com/autolocky">https://decrypter.emsisoft.com/autolocky</a>

## Aw3s0m3Sc0t7

Ransomware

*Table 293. Table References*

Links
<a href="https://twitter.com/struppigel/status/828902907668000770">https://twitter.com/struppigel/status/828902907668000770</a>

# BadBlock

Ransomware

Table 294. Table References

Links
<a href="https://decrypter.emsisoft.com/badblock">https://decrypter.emsisoft.com/badblock</a>
<a href="http://www.nyxbone.com/malware/BadBlock.html">http://www.nyxbone.com/malware/BadBlock.html</a>
<a href="http://www.nyxbone.com/images/articulos/malware/badblock/5.png">http://www.nyxbone.com/images/articulos/malware/badblock/5.png</a>

# BaksoCrypt

Ransomware Based on my-Little-Ransomware

Table 295. Table References

Links
<a href="https://twitter.com/JakubKroustek/status/760482299007922176">https://twitter.com/JakubKroustek/status/760482299007922176</a>
<a href="https://0xc1r3ng.wordpress.com/2016/06/24/bakso-crypt-simple-ransomware/">https://0xc1r3ng.wordpress.com/2016/06/24/bakso-crypt-simple-ransomware/</a>

# Bandarchor

Ransomware Files might be partially encrypted

Bandarchor is also known as:

- Rakhni

Table 296. Table References

Links
<a href="https://reaqta.com/2016/03/bandarchor-ransomware-still-active/">https://reaqta.com/2016/03/bandarchor-ransomware-still-active/</a>
<a href="https://www.bleepingcomputer.com/news/security/new-bandarchor-ransomware-variant-spreads-via-malvertising-on-adult-sites/">https://www.bleepingcomputer.com/news/security/new-bandarchor-ransomware-variant-spreads-via-malvertising-on-adult-sites/</a>

# Bart

Ransomware Possible affiliations with RockLoader, Locky and Dridex

Bart is also known as:

- BaCrypt

Table 297. Table References

Links
<a href="http://now.avg.com/barts-shenanigans-are-no-match-for-avg/">http://now.avg.com/barts-shenanigans-are-no-match-for-avg/</a>

<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 298. Table References*

Links

<https://noransom.kaspersky.com/>

## BitStak

Ransomware

*Table 299. Table References*

Links

<https://download.bleepingcomputer.com/demonslay335/BitStakDecrypter.zip>

## BlackShades Crypter

Ransomware

BlackShades Crypter is also known as:

- SilentShade

*Table 300. Table References*

Links

<http://nyxbone.com/malware/BlackShades.html>

## Blocatto

Ransomware Based on HiddenTear

*Table 301. Table References*

Links

<http://www.bleepingcomputer.com/forums/t/614456/blocatto-ransomware-blocatto-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 302. Table References

Links
<a href="http://www.nyxbone.com/malware/brazilianRansom.html">http://www.nyxbone.com/malware/brazilianRansom.html</a>
<a href="http://www.nyxbone.com/images/articulos/malware/brazilianRansom/0.png">http://www.nyxbone.com/images/articulos/malware/brazilianRansom/0.png</a>

## Brazilian Globe

Ransomware

Table 303. Table References

Links
<a href="https://twitter.com/JakubKroustek/status/821831437884211201">https://twitter.com/JakubKroustek/status/821831437884211201</a>

## BrLock

Ransomware

Table 304. Table References

Links
<a href="https://www.proofpoint.com/us/threat-insight/post/ransomware-explosion-continues-cryptfle2-brlock-mm-locker-discovered">https://www.proofpoint.com/us/threat-insight/post/ransomware-explosion-continues-cryptfle2-brlock-mm-locker-discovered</a>

## Browlock

Ransomware no local encryption, browser only

## BTCWare Related to / new version of CryptXXX

Ransomware

Table 305. Table References

Links
<a href="https://twitter.com/malwrhunterteam/status/845199679340011520">https://twitter.com/malwrhunterteam/status/845199679340011520</a>

## Bucbi

Ransomware no file name change, no extension

*Table 306. Table References*

Links
<a href="http://researchcenter.paloaltonetworks.com/2016/05/unit42-bucbi-ransomware-is-back-with-a-ukrainian-makeover/">http://researchcenter.paloaltonetworks.com/2016/05/unit42-bucbi-ransomware-is-back-with-a-ukrainian-makeover/</a>

## BuyUnlockCode

Ransomware Does not delete Shadow Copies

## Central Security Treatment Organization

Ransomware

*Table 307. Table References*

Links
<a href="http://www.bleepingcomputer.com/forums/t/625820/central-security-treatment-organization-ransomware-help-topic-cry-extension/">http://www.bleepingcomputer.com/forums/t/625820/central-security-treatment-organization-ransomware-help-topic-cry-extension/</a>

## Cerber

Ransomware

*Table 308. Table References*

Links
<a href="https://blog.malwarebytes.org/threat-analysis/2016/03/cerber-ransomware-new-but-mature/">https://blog.malwarebytes.org/threat-analysis/2016/03/cerber-ransomware-new-but-mature/</a>
<a href="https://community.rsa.com/community/products/netwitness/blog/2016/11/04/the-evolution-of-cerber-v410">https://community.rsa.com/community/products/netwitness/blog/2016/11/04/the-evolution-of-cerber-v410</a>

## Chimera

Ransomware

*Table 309. Table References*

Links
<a href="http://www.bleepingcomputer.com/news/security/chimera-ransomware-decryption-keys-released-by-petya-devs/">http://www.bleepingcomputer.com/news/security/chimera-ransomware-decryption-keys-released-by-petya-devs/</a>
<a href="https://blog.malwarebytes.org/threat-analysis/2015/12/inside-chimera-ransomware-the-first-doxingware-in-wild/">https://blog.malwarebytes.org/threat-analysis/2015/12/inside-chimera-ransomware-the-first-doxingware-in-wild/</a>

# Clock

Ransomware Does not encrypt anything

Table 310. Table References

Links
<a href="https://twitter.com/JakubKroustek/status/794956809866018816">https://twitter.com/JakubKroustek/status/794956809866018816</a>

# CoinVault

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

Table 311. Table References

Links
<a href="https://noransom.kaspersky.com/">https://noransom.kaspersky.com/</a>

# Covertion

Ransomware

Table 312. Table References

Links
<a href="http://www.bleepingcomputer.com/news/security/paying-the-covertion-ransomware-may-not-get-your-data-back/">http://www.bleepingcomputer.com/news/security/paying-the-covertion-ransomware-may-not-get-your-data-back/</a>

# Cryaki

Ransomware

Table 313. Table References

Links
<a href="https://support.kaspersky.com/viruses/disinfection/8547">https://support.kaspersky.com/viruses/disinfection/8547</a>

# Crybola

Ransomware

Table 314. Table References

Links
<a href="https://support.kaspersky.com/viruses/disinfection/8547">https://support.kaspersky.com/viruses/disinfection/8547</a>

# CryFile

Ransomware

Table 315. Table References

Links
<a href="#">SHTODELATVAM.txt[SHTODELATVAM.txt]</a>
<a href="#">Instructionaga.txt[Instructionaga.txt]</a>

# CryLocker

Ransomware Identifies victim locations w/Google Maps API

CryLocker is also known as:

- Cry
- CSTO
- Central Security Treatment Organization

Table 316. Table References

Links
<a href="http://www.bleepingcomputer.com/news/security/the-crylocker-ransomware-communicates-using-udp-and-stores-data-on-imgur-com/">http://www.bleepingcomputer.com/news/security/the-crylocker-ransomware-communicates-using-udp-and-stores-data-on-imgur-com/</a>

# CrypMIC

Ransomware CryptXXX clone/spinoff

Table 317. Table References

Links
<a href="http://blog.trendmicro.com/trendlabs-security-intelligence/crypmic-ransomware-wants-to-follow-cryptxxx/">http://blog.trendmicro.com/trendlabs-security-intelligence/crypmic-ransomware-wants-to-follow-cryptxxx/</a>

# Crypren

Ransomware

Table 318. Table References

Links
<a href="https://github.com/pekeinfo/DecryptCrypren">https://github.com/pekeinfo/DecryptCrypren</a>
<a href="http://www.nyxbone.com/malware/Crypren.html">http://www.nyxbone.com/malware/Crypren.html</a>
<a href="http://www.nyxbone.com/images/articulos/malware/crypren/0.png">http://www.nyxbone.com/images/articulos/malware/crypren/0.png</a>

# Crypt38

Ransomware

Table 319. Table References

Links
<a href="https://download.bleepingcomputer.com/demonslay335/Crypt38Keygen.zip">https://download.bleepingcomputer.com/demonslay335/Crypt38Keygen.zip</a>
<a href="https://blog.fortinet.com/2016/06/17/buggy-russian-ransomware-inadvertently-allows-free-decryption">https://blog.fortinet.com/2016/06/17/buggy-russian-ransomware-inadvertently-allows-free-decryption</a>

# Crypter

Ransomware Does not actually encrypt the files, but simply renames them

Table 320. Table References

Links
<a href="https://twitter.com/jiriatvirlab/status/802554159564062722">https://twitter.com/jiriatvirlab/status/802554159564062722</a>

# CryptFile2

Ransomware

Table 321. Table References

Links
<a href="https://www.proofpoint.com/us/threat-insight/post/ransomware-explosion-continues-cryptfile2-brlock-mm-locker-discovered">https://www.proofpoint.com/us/threat-insight/post/ransomware-explosion-continues-cryptfile2-brlock-mm-locker-discovered</a>

# CryptInfinite

Ransomware

Table 322. Table References

Links
<a href="https://decrypter.emsisoft.com/">https://decrypter.emsisoft.com/</a>

# CryptoBit

Ransomware sekretzbel0ngt0us.KEY - do not confuse with CryptorBit.

Table 323. Table References

Links
<a href="http://www.pandasecurity.com/mediacenter/panda-security/cryptobit/">http://www.pandasecurity.com/mediacenter/panda-security/cryptobit/</a>
<a href="http://news.softpedia.com/news/new-cryptobit-ransomware-could-be-decryptable-503239.shtml">http://news.softpedia.com/news/new-cryptobit-ransomware-could-be-decryptable-503239.shtml</a>

# CryptoDefense

Ransomware no extension change

Table 324. Table References

Links
<a href="https://decrypter.emsisoft.com/">https://decrypter.emsisoft.com/</a>

# CryptoFinancial

Ransomware

CryptoFinancial is also known as:

- Ranscam

Table 325. Table References

Links
<a href="http://blog.talosintel.com/2016/07/ranscam.html">http://blog.talosintel.com/2016/07/ranscam.html</a>
<a href="https://nakedsecurity.sophos.com/2016/07/13/ransomware-that-demands-money-and-gives-you-back-nothing/">https://nakedsecurity.sophos.com/2016/07/13/ransomware-that-demands-money-and-gives-you-back-nothing/</a>

# 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 326. Table References

Links
<a href="http://www.bleepingcomputer.com/news/security/crytohost-decrypts-files-in-a-password-protected-rar-file/">http://www.bleepingcomputer.com/news/security/crytohost-decrypts-files-in-a-password-protected-rar-file/</a>

# CryptoJoker

Ransomware

# CryptoLocker

Ransomware no longer relevant

Table 327. Table References

Links
<a href="https://www.fireeye.com/blog/executive-perspective/2014/08/your-locker-of-information-for-cryptolocker-decryption.html">https://www.fireeye.com/blog/executive-perspective/2014/08/your-locker-of-information-for-cryptolocker-decryption.html</a>
<a href="https://reaqta.com/2016/04/uncovering-ransomware-distribution-operation-part-2/">https://reaqta.com/2016/04/uncovering-ransomware-distribution-operation-part-2/</a>

# CryptoLocker 1.0.0

Ransomware

Table 328. Table References

Links
<a href="https://twitter.com/malwrhunterteam/status/839747940122001408">https://twitter.com/malwrhunterteam/status/839747940122001408</a>

# CryptoLocker 5.1

Ransomware

Table 329. Table References

Links
<a href="https://twitter.com/malwrhunterteam/status/782890104947867649">https://twitter.com/malwrhunterteam/status/782890104947867649</a>

# CryptoMix

Ransomware

CryptoMix is also known as:

- Zeta

Table 330. Table References

Links
<a href="http://www.nyxbone.com/malware/CryptoMix.html">http://www.nyxbone.com/malware/CryptoMix.html</a>
<a href="https://www.cert.pl/en/news/single/technical-analysis-of-cryptomixcryptfile2-ransomware/">https://www.cert.pl/en/news/single/technical-analysis-of-cryptomixcryptfile2-ransomware/</a>

# CryptoRansomware

Ransomware

Table 331. Table References

Links
<a href="https://twitter.com/malwrhunterteam/status/817672617658347521">https://twitter.com/malwrhunterteam/status/817672617658347521</a>

# CryptoRoger

Ransomware

Table 332. Table References

Links
<a href="http://www.bleepingcomputer.com/news/security/new-ransomware-called-cryptoroger-that-appends-crptrgr-to-encrypted-files/">http://www.bleepingcomputer.com/news/security/new-ransomware-called-cryptoroger-that-appends-crptrgr-to-encrypted-files/</a>

# CryptoShadow

Ransomware

Table 333. Table References

Links
<a href="https://twitter.com/struppigel/status/821992610164277248">https://twitter.com/struppigel/status/821992610164277248</a>

# CryptoShocker

Ransomware

Table 334. Table References

Links
<a href="http://www.bleepingcomputer.com/forums/t/617601/cryptoshocker-ransomware-help-and-support-topic-locked-attentionurl/">http://www.bleepingcomputer.com/forums/t/617601/cryptoshocker-ransomware-help-and-support-topic-locked-attentionurl/</a>

# CryptoTorLocker2015

Ransomware

Table 335. Table References

Links
<a href="http://www.bleepingcomputer.com/forums/t/565020/new-cryptotorlocker2015-ransomware-discovered-and-easily-decrypted/">http://www.bleepingcomputer.com/forums/t/565020/new-cryptotorlocker2015-ransomware-discovered-and-easily-decrypted/</a>



# CryptoTrooper

Ransomware

*Table 336. 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 337. 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 338. 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 339. Table References

Links
<a href="https://support.kaspersky.com/viruses/disinfection/8547">https://support.kaspersky.com/viruses/disinfection/8547</a>
<a href="https://www.proofpoint.com/us/threat-insight/post/cryptxxx2-ransomware-authors-strike-back-against-free-decryption-tool">https://www.proofpoint.com/us/threat-insight/post/cryptxxx2-ransomware-authors-strike-back-against-free-decryption-tool</a>
<a href="http://blogs.cisco.com/security/cryptxxx-technical-deep-dive">http://blogs.cisco.com/security/cryptxxx-technical-deep-dive</a>

## CryptXXX 3.0

Ransomware Comes with Bedep

CryptXXX 3.0 is also known as:

- UltraDeCrypter
- UltraCrypter

Table 340. Table References

Links
<a href="https://support.kaspersky.com/viruses/disinfection/8547">https://support.kaspersky.com/viruses/disinfection/8547</a>
<a href="http://www.bleepingcomputer.com/news/security/cryptxxx-updated-to-version-3-0-decryptors-no-longer-work/">http://www.bleepingcomputer.com/news/security/cryptxxx-updated-to-version-3-0-decryptors-no-longer-work/</a>
<a href="http://blogs.cisco.com/security/cryptxxx-technical-deep-dive">http://blogs.cisco.com/security/cryptxxx-technical-deep-dive</a>

## CryptXXX 3.1

Ransomware StilerX credential stealing

Table 341. Table References

Links
<a href="https://support.kaspersky.com/viruses/disinfection/8547">https://support.kaspersky.com/viruses/disinfection/8547</a>
<a href="https://www.proofpoint.com/us/threat-insight/post/cryptxxx-ransomware-learns-samba-other-new-tricks-with-version3100">https://www.proofpoint.com/us/threat-insight/post/cryptxxx-ransomware-learns-samba-other-new-tricks-with-version3100</a>

## CryPy

Ransomware

Table 342. Table References

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

## CTB-Faker

Ransomware

CTB-Faker is also known as:

- Citroni

## CTB-Locker WEB

Ransomware websites only

Table 343. Table References

Links
<a href="https://thisissecurity.net/2016/02/26/a-lockpicking-exercise/">https://thisissecurity.net/2016/02/26/a-lockpicking-exercise/</a>
<a href="https://github.com/eyecatchup/Critroni-php">https://github.com/eyecatchup/Critroni-php</a>

## CuteRansomware

Ransomware Based on my-Little-Ransomware

CuteRansomware is also known as:

- my-Little-Ransomware

Table 344. Table References

Links
<a href="https://github.com/aaaddress1/my-Little-Ransomware/tree/master/decryptoTool">https://github.com/aaaddress1/my-Little-Ransomware/tree/master/decryptoTool</a>
<a href="https://github.com/aaaddress1/my-Little-Ransomware">https://github.com/aaaddress1/my-Little-Ransomware</a>

## Cyber SpLiTTER Vbs

Ransomware Based on HiddenTear

Cyber SpLiTTER Vbs is also known as:

- CyberSplitter

Table 345. Table References

Links
-------

<https://twitter.com/struppigel/status/778871886616862720>

<https://twitter.com/struppigel/status/806758133720698881>

## Death Bitches

Ransomware

*Table 346. Table References*

Links

<https://twitter.com/JaromirHorejsi/status/815555258478981121>

## DeCrypt Protect

Ransomware

*Table 347. Table References*

Links

[http://www.malwareremovalguides.info/decrypt-files-with-decrypt\\_mblblock-exe-decrypt-protect/](http://www.malwareremovalguides.info/decrypt-files-with-decrypt_mblblock-exe-decrypt-protect/)

## DEDCryptor

Ransomware Based on EDA2

*Table 348. 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 349. Table References*

Links

<https://twitter.com/struppigel/status/798573300779745281>

## DetoxCrypto

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

*Table 350. 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 351. Table References*

Links

<https://twitter.com/PolarToffee/status/829727052316160000>

## DirtyDecrypt

Ransomware

*Table 352. 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 353. Table References*

Links

<https://decrypter.emsisoft.com/>

[https://github.com/hasherezade/dma\\_unlocker](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 354. Table References*

Links

<https://drive.google.com/drive/folders/0Bzb5kQFOXkiSMm94QzdyM3hCdDg>

<https://blog.malwarebytes.org/threat-analysis/2016/02/dma-locker-strikes-back/>

# DN Ransomware

Ransomware Code to decrypt: 83KYG9NW-3K39V-2T3HJ-93F3Q-GT

Table 355. Table References

Links
<a href="https://twitter.com/BleepinComputer/status/822500056511213568">https://twitter.com/BleepinComputer/status/822500056511213568</a>

# Domino

Ransomware Based on Hidden Tear

Table 356. Table References

Links
<a href="http://www.nyxbone.com/malware/Domino.html">http://www.nyxbone.com/malware/Domino.html</a>
<a href="http://www.bleepingcomputer.com/news/security/the-curious-case-of-the-domino-ransomware-a-windows-crack-and-a-cow/">http://www.bleepingcomputer.com/news/security/the-curious-case-of-the-domino-ransomware-a-windows-crack-and-a-cow/</a>

# DoNotChange

Ransomware

Table 357. Table References

Links
<a href="https://www.bleepingcomputer.com/forums/t/643330/donotchange-ransomware-id-7es642406cry-do-not-change-the-file-namecryp/">https://www.bleepingcomputer.com/forums/t/643330/donotchange-ransomware-id-7es642406cry-do-not-change-the-file-namecryp/</a>

# DummyLocker

Ransomware

Table 358. Table References

Links
<a href="https://twitter.com/struppigel/status/794108322932785158">https://twitter.com/struppigel/status/794108322932785158</a>

# DXXD

Ransomware

Table 359. Table References

Links
<a href="https://www.bleepingcomputer.com/forums/t/627831/dxxd-ransomware-dxxd-help-support-readmetxt/">https://www.bleepingcomputer.com/forums/t/627831/dxxd-ransomware-dxxd-help-support-readmetxt/</a>

<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 360. 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 361. Table References*

Links

[http://www.filedropper.com/decrypter\\_1](http://www.filedropper.com/decrypter_1)

<https://twitter.com/JakubKroustek/status/747031171347910656>

## EiTest

Ransomware

*Table 362. 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 363. Table References

Links
<a href="http://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-14-2016-exotic-lockydump-comrade-and-more/">http://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-14-2016-exotic-lockydump-comrade-and-more/</a>
<a href="http://vms.drweb.ru/virus/?_is=1&amp;i=8747343">http://vms.drweb.ru/virus/?_is=1&amp;i=8747343</a>

# encryptoJJS

Ransomware

# Enigma

Ransomware

Table 364. Table References

Links
<a href="http://www.bleepingcomputer.com/news/security/the-enigma-ransomware-targets-russian-speaking-users/">http://www.bleepingcomputer.com/news/security/the-enigma-ransomware-targets-russian-speaking-users/</a>

# Enjey

Ransomware Based on RemindMe

Table 365. Table References

Links
<a href="https://twitter.com/malwrhunterteam/status/839022018230112256">https://twitter.com/malwrhunterteam/status/839022018230112256</a>

# Fairware

Ransomware Target Linux O.S.

Table 366. Table References

Links
<a href="http://www.bleepingcomputer.com/news/security/new-fairware-ransomware-targeting-linux-computers/">http://www.bleepingcomputer.com/news/security/new-fairware-ransomware-targeting-linux-computers/</a>



# Fakben

Ransomware Based on Hidden Tear

Table 367. Table References

Links
<a href="https://blog.fortinet.com/post/fakben-team-ransomware-uses-open-source-hidden-tear-code">https://blog.fortinet.com/post/fakben-team-ransomware-uses-open-source-hidden-tear-code</a>

# FakeCryptoLocker

Ransomware

Table 368. Table References

Links
<a href="https://twitter.com/PolarToffee/status/812312402779836416">https://twitter.com/PolarToffee/status/812312402779836416</a>

# Fantom

Ransomware Based on EDA2

Fantom is also known as:

- Comrad Circle

Table 369. Table References

Links
<a href="http://www.bleepingcomputer.com/news/security/fantom-ransomware-encrypts-your-files-while-pretending-to-be-windows-update/">http://www.bleepingcomputer.com/news/security/fantom-ransomware-encrypts-your-files-while-pretending-to-be-windows-update/</a>

# FenixLocker

Ransomware

Table 370. Table References

Links
<a href="https://decrypter.emsisoft.com/fenixlocker">https://decrypter.emsisoft.com/fenixlocker</a>
<a href="https://twitter.com/fwosar/status/777197255057084416">https://twitter.com/fwosar/status/777197255057084416</a>

# FILE FROZR

Ransomware RaaS

Table 371. Table References

Links
-------

<https://twitter.com/rommeljovent17/status/846973265650335744>

## FileLocker

Ransomware

*Table 372. Table References*

Links

<https://twitter.com/jiriavirlab/status/836616468775251968>

## FireCrypt

Ransomware

*Table 373. Table References*

Links

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

## Flyper

Ransomware Based on EDA2 / HiddenTear

*Table 374. Table References*

Links

<https://twitter.com/malwrhunterteam/status/773771485643149312>

## Fonco

Ransomware contact email [safefiles32@mail.ru](mailto:safefiles32@mail.ru) also as prefix in encrypted file contents

## FortuneCookie

Ransomware

*Table 375. 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 376. Table References

Links
<a href="https://twitter.com/BleepinComputer/status/812135608374226944">https://twitter.com/BleepinComputer/status/812135608374226944</a>

## FSociety

Ransomware Based on EDA2 and RemindMe

Table 377. Table References

Links
<a href="https://www.bleepingcomputer.com/forums/t/628199/fsociety-locker-ransomware-help-support-fsocietyhtml/">https://www.bleepingcomputer.com/forums/t/628199/fsociety-locker-ransomware-help-support-fsocietyhtml/</a>
<a href="http://www.bleepingcomputer.com/news/security/new-fsociety-ransomware-pays-homage-to-mr-robot/">http://www.bleepingcomputer.com/news/security/new-fsociety-ransomware-pays-homage-to-mr-robot/</a>
<a href="https://twitter.com/siri_urz/status/795969998707720193">https://twitter.com/siri_urz/status/795969998707720193</a>

## Fury

Ransomware

Table 378. Table References

Links
<a href="https://support.kaspersky.com/viruses/disinfection/8547">https://support.kaspersky.com/viruses/disinfection/8547</a>

## GhostCrypt

Ransomware Based on Hidden Tear

Table 379. Table References

Links
<a href="https://download.bleepingcomputer.com/demonslay335/GhostCryptDecrypter.zip">https://download.bleepingcomputer.com/demonslay335/GhostCryptDecrypter.zip</a>
<a href="http://www.bleepingcomputer.com/forums/t/614197/ghostcrypt-z81928819-help-support-topic-read-this-filetxt/">http://www.bleepingcomputer.com/forums/t/614197/ghostcrypt-z81928819-help-support-topic-read-this-filetxt/</a>

## Gingerbread

Ransomware

Table 380. Table References

Links
<a href="https://twitter.com/ni_fi_70/status/796353782699425792">https://twitter.com/ni_fi_70/status/796353782699425792</a>

# Globe v1

Ransomware

Globe v1 is also known as:

- Purge

Table 381. Table References

Links
<a href="https://success.trendmicro.com/portal_kb_articledetail?solutionid=1114221">https://success.trendmicro.com/portal_kb_articledetail?solutionid=1114221</a>
<a href="http://www.bleepingcomputer.com/news/security/the-globe-ransomware-wants-to-purge-your-files/">http://www.bleepingcomputer.com/news/security/the-globe-ransomware-wants-to-purge-your-files/</a>

# GNL Locker

Ransomware Only encrypts DE or NL country. Variants, from old to latest: Zyklon Locker, WildFire locker, Hades Locker

Table 382. Table References

Links
<a href="http://www.bleepingcomputer.com/forums/t/611342/gnl-locker-support-and-help-topic-locked-and-unlock-files-instructionshtml/">http://www.bleepingcomputer.com/forums/t/611342/gnl-locker-support-and-help-topic-locked-and-unlock-files-instructionshtml/</a>

# Gomasom

Ransomware

Table 383. Table References

Links
<a href="https://decrypter.emsisoft.com/">https://decrypter.emsisoft.com/</a>

# Goopic

Ransomware

Table 384. Table References

Links
<a href="http://blog.trendmicro.com/trendlabs-security-intelligence/angler-shift-ek-landscape-new-crypto-ransomware-activity/">http://blog.trendmicro.com/trendlabs-security-intelligence/angler-shift-ek-landscape-new-crypto-ransomware-activity/</a>

# Gopher

Ransomware OS X ransomware (PoC)

# Hacked

Ransomware Jigsaw Ransomware variant

Table 385. Table References

Links
<a href="https://twitter.com/demonslay335/status/806878803507101696">https://twitter.com/demonslay335/status/806878803507101696</a>

# HappyDayzz

Ransomware

Table 386. Table References

Links
<a href="https://twitter.com/malwrhunterteam/status/847114064224497666">https://twitter.com/malwrhunterteam/status/847114064224497666</a>

# Harasom

Ransomware

Table 387. Table References

Links
<a href="https://decrypter.emsisoft.com/">https://decrypter.emsisoft.com/</a>

# HDDCryptor

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

HDDCryptor is also known as:

- Mamba

Table 388. Table References

Links
<a href="https://www.linkedin.com/pulse/mamba-new-full-disk-encryption-ransomware-family-member-marinho">https://www.linkedin.com/pulse/mamba-new-full-disk-encryption-ransomware-family-member-marinho</a>
<a href="https://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/</a>

# Heimdall

Ransomware File marker: "Heimdall---"

Table 389. Table References

Links

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

## Help\_dcfile

Ransomware

## Herbst

Ransomware

Table 390. Table References

Links

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

## Hi Buddy!

Ransomware Based on HiddenTear

Table 391. Table References

Links

<http://www.nyxbone.com/malware/hibuddy.html>

## Hitler

Ransomware Deletes files

Table 392. 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 393. 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 394. Table References

Links
<a href="https://twitter.com/BleepinComputer/status/803288396814839808">https://twitter.com/BleepinComputer/status/803288396814839808</a>

# HydraCrypt

Ransomware CrypBoss Family

Table 395. Table References

Links
<a href="https://decrypter.emsisoft.com/">https://decrypter.emsisoft.com/</a>
<a href="http://www.malware-traffic-analysis.net/2016/02/03/index2.html">http://www.malware-traffic-analysis.net/2016/02/03/index2.html</a>

# iLock

Ransomware

Table 396. Table References

Links
<a href="https://twitter.com/BleepinComputer/status/817085367144873985">https://twitter.com/BleepinComputer/status/817085367144873985</a>

# iLockLight

Ransomware

# International Police Association

Ransomware CryptoTorLocker2015 variant

Table 397. Table References

Links
<a href="http://download.bleepingcomputer.com/Nathan/StopPirates_Decrypter.exe">http://download.bleepingcomputer.com/Nathan/StopPirates_Decrypter.exe</a>

# iRansom

Ransomware

Table 398. Table References

Links
-------

<a href="https://twitter.com/demonslay335/status/796134264744083460">https://twitter.com/demonslay335/status/796134264744083460</a>
---

## JagerDecryptor

Ransomware Prepends filenames

*Table 399. Table References*

Links
-------

<a href="https://twitter.com/JakubKroustek/status/757873976047697920">https://twitter.com/JakubKroustek/status/757873976047697920</a>
---

## Jeiphoos

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

Jeiphoos is also known as:

- Encryptor RaaS
- Sarento

*Table 400. Table References*

Links
-------

<a href="http://www.nyxbone.com/malware/RaaS.html">http://www.nyxbone.com/malware/RaaS.html</a>
---

<a href="http://blog.trendmicro.com/trendlabs-security-intelligence/the-rise-and-fall-of-encryptor-raas/">http://blog.trendmicro.com/trendlabs-security-intelligence/the-rise-and-fall-of-encryptor-raas/</a>
---

## Jhon Woddy

Ransomware Same codebase as DNRansomware Lock screen password is M3VZ>5BwGGVH

*Table 401. Table References*

Links
-------

<a href="https://download.bleepingcomputer.com/demonslay335/DoNotOpenDecrypter.zip">https://download.bleepingcomputer.com/demonslay335/DoNotOpenDecrypter.zip</a>
---

<a href="https://twitter.com/BleepinComputer/status/822509105487245317">https://twitter.com/BleepinComputer/status/822509105487245317</a>
---

## Jigsaw

Ransomware Has a GUI

Jigsaw is also known as:

- CryptoHitMan

*Table 402. Table References*

Links
-------



<http://www.bleepingcomputer.com/news/security/jigsaw-ransomware-decrypt-ed-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 403. 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>

## JohnnyCryptor

Ransomware

## KawaiiLocker

Ransomware

*Table 404. Table References*

Links

<https://safezone.cc/resources/kawaii-decryptor.195/>

## KeRanger

Ransomware OS X Ransomware

*Table 405. 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 406. Table References*

Links

<https://decrypter.emsisoft.com/>

## KEYHolder

Ransomware via remote attacker. [tuyuljahat@hotmail.com](mailto:tuyuljahat@hotmail.com) contact address

*Table 407. 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 408. Table References*

Links

<https://twitter.com/malwrhunterteam/status/782232299840634881>

## KimcilWare

Ransomware websites only

*Table 409. 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 410. Table References*

Links

<http://www.nyxbone.com/malware/koreanRansom.html>

## Kozy.Jozy

Ransomware      Potential      Kit      [selectedkozy.jozy@yahoo.com](mailto:selectedkozy.jozy@yahoo.com)      [kozy.jozy@yahoo.com](mailto:kozy.jozy@yahoo.com)  
[unlock92@india.com](mailto:unlock92@india.com)

Kozy.Jozy is also known as:

- QC

Table 411. Table References

Links
<a href="http://www.nyxbone.com/malware/KozyJozy.html">http://www.nyxbone.com/malware/KozyJozy.html</a>
<a href="http://www.bleepingcomputer.com/forums/t/617802/kozyjozy-ransomware-help-support-wjpg-31392e30362e32303136-num-lsbj1/">http://www.bleepingcomputer.com/forums/t/617802/kozyjozy-ransomware-help-support-wjpg-31392e30362e32303136-num-lsbj1/</a>

## KratosCrypt

Ransomware [kratosdimetrici@gmail.com](mailto:kratosdimetrici@gmail.com)

Table 412. Table References

Links
<a href="https://twitter.com/demonslay335/status/746090483722686465">https://twitter.com/demonslay335/status/746090483722686465</a>

## KryptoLocker

Ransomware Based on HiddenTear

## LanRan

Ransomware Variant of open-source MyLittleRansomware

Table 413. Table References

Links
<a href="https://twitter.com/struppigel/status/847689644854595584">https://twitter.com/struppigel/status/847689644854595584</a>

## LeChiffre

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

Table 414. Table References

Links
<a href="https://decrypter.emsisoft.com/lechiffre">https://decrypter.emsisoft.com/lechiffre</a>
<a href="https://blog.malwarebytes.org/threat-analysis/2016/01/lechiffre-a-manually-run-ransomware/">https://blog.malwarebytes.org/threat-analysis/2016/01/lechiffre-a-manually-run-ransomware/</a>

## Lick

Ransomware Variant of Kirk

Table 415. 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 416. Table References*

Links

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

## LK Encryption

Ransomware Based on HiddenTear

*Table 417. Table References*

Links

<https://twitter.com/malwrhunterteam/status/845183290873044994>

## LLTP Locker

Ransomware Targeting Spanish speaking victims

*Table 418. Table References*

Links

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

## Locker

Ransomware has GUI

*Table 419. Table References*

Links

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

## LockLock

Ransomware

Table 420. Table References

Links
<a href="https://www.bleepingcomputer.com/forums/t/626750/locklock-ransomware-locklock-help-support/">https://www.bleepingcomputer.com/forums/t/626750/locklock-ransomware-locklock-help-support/</a>

## Locky

Ransomware Affiliations with Dridex and Necurs botnets

Table 421. Table References

Links
<a href="http://www.bleepingcomputer.com/news/security/new-locky-version-adds-the-zepto-extension-to-encrypted-files/">http://www.bleepingcomputer.com/news/security/new-locky-version-adds-the-zepto-extension-to-encrypted-files/</a>
<a href="http://blog.trendmicro.com/trendlabs-security-intelligence/new-locky-ransomware-spotted-in-the-brazilian-underground-market-uses-windows-script-files/">http://blog.trendmicro.com/trendlabs-security-intelligence/new-locky-ransomware-spotted-in-the-brazilian-underground-market-uses-windows-script-files/</a>
<a href="https://nakedsecurity.sophos.com/2016/10/06/odin-ransomware-takes-over-from-zepto-and-locky/">https://nakedsecurity.sophos.com/2016/10/06/odin-ransomware-takes-over-from-zepto-and-locky/</a>
<a href="https://www.bleepingcomputer.com/news/security/locky-ransomware-switches-to-egyptian-mythology-with-the-osiris-extension/">https://www.bleepingcomputer.com/news/security/locky-ransomware-switches-to-egyptian-mythology-with-the-osiris-extension/</a>

## Lortok

Ransomware

## LowLevel04

Ransomware Prepends filenames

## M4N1F3STO

Ransomware Does not encrypt Unlock code=suckmydicknigga

Table 422. Table References

Links
<a href="https://twitter.com/jiriavirlab/status/808015275367002113">https://twitter.com/jiriavirlab/status/808015275367002113</a>

## Mabouia

Ransomware OS X ransomware (PoC)

## MacAndChess

Ransomware Based on HiddenTear

# Magic

Ransomware Based on EDA2

# MaktubLocker

Ransomware

Table 423. Table References

Links
<a href="https://blog.malwarebytes.org/threat-analysis/2016/03/maktub-locker-beautiful-and-dangerous/">https://blog.malwarebytes.org/threat-analysis/2016/03/maktub-locker-beautiful-and-dangerous/</a>

# MarsJoke

Ransomware

Table 424. Table References

Links
<a href="https://securelist.ru/blog/issledovaniya/29376/polyglot-the-fake-ctb-locker/">https://securelist.ru/blog/issledovaniya/29376/polyglot-the-fake-ctb-locker/</a>
<a href="https://www.proofpoint.com/us/threat-insight/post/MarsJoke-Ransomware-Mimics-CTB-Locker">https://www.proofpoint.com/us/threat-insight/post/MarsJoke-Ransomware-Mimics-CTB-Locker</a>

# Meister

Ransomware Targeting French victims

Table 425. Table References

Links
<a href="https://twitter.com/siri_urz/status/840913419024945152">https://twitter.com/siri_urz/status/840913419024945152</a>

# Meteoritan

Ransomware

Table 426. Table References

Links
<a href="https://twitter.com/malwrhunterteam/status/844614889620561924">https://twitter.com/malwrhunterteam/status/844614889620561924</a>

# MIRCOP

Ransomware Prepends files Demands 48.48 BTC

MIRCOP is also known as:

- Crypt888

Table 427. Table References

Links
<a href="http://www.bleepingcomputer.com/forums/t/618457/mircop-ransomware-help-support-lock-mircop/">http://www.bleepingcomputer.com/forums/t/618457/mircop-ransomware-help-support-lock-mircop/</a>
<a href="https://www.avast.com/ransomware-decryption-tools#!">https://www.avast.com/ransomware-decryption-tools#!</a>
<a href="http://blog.trendmicro.com/trendlabs-security-intelligence/instruction-less-ransomware-mircop-channels-guy-fawkes/">http://blog.trendmicro.com/trendlabs-security-intelligence/instruction-less-ransomware-mircop-channels-guy-fawkes/</a>
<a href="http://www.nyxbone.com/malware/Mircop.html">http://www.nyxbone.com/malware/Mircop.html</a>

## MireWare

Ransomware Based on HiddenTear

## Mischa

Ransomware Packaged with Petya PDFBewerbungsmappe.exe

Mischa is also known as:

- "Petya's little brother"

Table 428. Table References

Links
<a href="http://www.bleepingcomputer.com/news/security/petya-is-back-and-with-a-friend-named-mischa-ransomware/">http://www.bleepingcomputer.com/news/security/petya-is-back-and-with-a-friend-named-mischa-ransomware/</a>

## MM Locker

Ransomware Based on EDA2

MM Locker is also known as:

- Booyah

Table 429. Table References

Links
<a href="https://www.proofpoint.com/us/threat-insight/post/ransomware-explosion-continues-cryptfile2-brlock-mm-locker-discovered">https://www.proofpoint.com/us/threat-insight/post/ransomware-explosion-continues-cryptfile2-brlock-mm-locker-discovered</a>

## Mobef

Ransomware

Mobef is also known as:

- Yakes
- CryptoBit

Table 430. Table References

Links
<a href="http://nyxbone.com/malware/Mobef.html">http://nyxbone.com/malware/Mobef.html</a>
<a href="http://researchcenter.paloaltonetworks.com/2016/07/unit42-cryptobit-another-ransomware-family-gets-an-update/">http://researchcenter.paloaltonetworks.com/2016/07/unit42-cryptobit-another-ransomware-family-gets-an-update/</a>
<a href="http://nyxbone.com/images/articulos/malware/mobef/0.png">http://nyxbone.com/images/articulos/malware/mobef/0.png</a>

## Monument

Ransomware Use the DarkLocker 5 porn screenlocker - Jigsaw variant

Table 431. Table References

Links
<a href="https://twitter.com/malwrhunterteam/status/844826339186135040">https://twitter.com/malwrhunterteam/status/844826339186135040</a>

## N-Splitter

Ransomware Russian Koolova Variant

Table 432. Table References

Links
<a href="https://twitter.com/JakubKroustek/status/815961663644008448">https://twitter.com/JakubKroustek/status/815961663644008448</a>
<a href="https://www.youtube.com/watch?v=dAVMgX8Zti4&amp;feature=youtu.be&amp;list=UU_TMZYaLIgjsdJMwurHAi4Q">https://www.youtube.com/watch?v=dAVMgX8Zti4&amp;feature=youtu.be&amp;list=UU_TMZYaLIgjsdJMwurHAi4Q</a>

## n1n1n1

Ransomware Filemaker: "333333333333"

Table 433. Table References

Links
<a href="https://twitter.com/demonslay335/status/790608484303712256">https://twitter.com/demonslay335/status/790608484303712256</a>
<a href="https://twitter.com/demonslay335/status/831891344897482754">https://twitter.com/demonslay335/status/831891344897482754</a>

## NanoLocker

Ransomware no extension change, has a GUI

Table 434. Table References

Links
-------



<http://github.com/Cyberclues/nanolocker-decryptor>

## Nemucod

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

Table 435. Table References

Links
<a href="https://decrypter.emsisoft.com/nemucod">https://decrypter.emsisoft.com/nemucod</a>
<a href="https://github.com/Antelox/NemucodFR">https://github.com/Antelox/NemucodFR</a>
<a href="http://www.bleepingcomputer.com/news/security/decryptor-released-for-the-nemucod-trojans-encrypted-ransomware/">http://www.bleepingcomputer.com/news/security/decryptor-released-for-the-nemucod-trojans-encrypted-ransomware/</a>
<a href="https://blog.cisecurity.org/malware-analysis-report-nemucod-ransomware/">https://blog.cisecurity.org/malware-analysis-report-nemucod-ransomware/</a>

## Netix

Ransomware

Netix is also known as:

- RANSOM\_NETIX.A

Table 436. Table References

Links
<a href="http://blog.trendmicro.com/trendlabs-security-intelligence/netflix-scam-delivers-ransomware/">http://blog.trendmicro.com/trendlabs-security-intelligence/netflix-scam-delivers-ransomware/</a>

## Nhtnwcuf

Ransomware Does not encrypt the files / Files are destroyed

Table 437. Table References

Links
<a href="https://twitter.com/demonslay335/status/839221457360195589">https://twitter.com/demonslay335/status/839221457360195589</a>

## NMoreira

Ransomware

NMoreira is also known as:

- XRatTeam
- XPan

Table 438. Table References

Links
<a href="https://decrypter.emsisoft.com/nmoreira">https://decrypter.emsisoft.com/nmoreira</a>
<a href="https://twitter.com/fwosar/status/803682662481174528">https://twitter.com/fwosar/status/803682662481174528</a>

## NoobCrypt

Ransomware

*Table 439. Table References*

Links
<a href="https://twitter.com/JakubKroustek/status/757267550346641408">https://twitter.com/JakubKroustek/status/757267550346641408</a>
<a href="https://www.bleepingcomputer.com/news/security/noobcrypt-ransomware-dev-shows-noobness-by-using-same-password-for-everyone/">https://www.bleepingcomputer.com/news/security/noobcrypt-ransomware-dev-shows-noobness-by-using-same-password-for-everyone/</a>

## Nuke

Ransomware

## Nullbyte

Ransomware

*Table 440. Table References*

Links
<a href="https://download.bleepingcomputer.com/demonslay335/NullByteDecrypter.zip">https://download.bleepingcomputer.com/demonslay335/NullByteDecrypter.zip</a>
<a href="https://www.bleepingcomputer.com/news/security/the-nullbyte-ransomware-pretends-to-be-the-necrobot-pokemon-go-application/">https://www.bleepingcomputer.com/news/security/the-nullbyte-ransomware-pretends-to-be-the-necrobot-pokemon-go-application/</a>

## ODCODC

Ransomware

*Table 441. Table References*

Links
<a href="http://download.bleepingcomputer.com/BloodDolly/ODCODCDecoder.zip">http://download.bleepingcomputer.com/BloodDolly/ODCODCDecoder.zip</a>
<a href="http://www.nyxbone.com/malware/odcodc.html">http://www.nyxbone.com/malware/odcodc.html</a>
<a href="https://twitter.com/PolarToffee/status/813762510302183424">https://twitter.com/PolarToffee/status/813762510302183424</a>
<a href="http://www.nyxbone.com/images/articulos/malware/odcodc/1c.png">http://www.nyxbone.com/images/articulos/malware/odcodc/1c.png</a>

## Offline ransomware

Ransomware email addresses overlap with .777 addresses

Offline ransomware is also known as:

- Vipasana
- Cryakl

*Table 442. Table References*

Links
<a href="https://support.kaspersky.com/viruses/disinfection/8547">https://support.kaspersky.com/viruses/disinfection/8547</a>
<a href="http://bartblaze.blogspot.com.co/2016/02/vipasana-ransomware-new-ransom-on-block.html">http://bartblaze.blogspot.com.co/2016/02/vipasana-ransomware-new-ransom-on-block.html</a>

## OMG! Ransomware

Ransomware

OMG! Ransomware is also known as:

- GPCode

## Operation Global III

Ransomware Is a file infector (virus)

*Table 443. Table References*

Links
<a href="http://news.thewindowsclub.com/operation-global-iii-ransomware-decryption-tool-released-70341/">http://news.thewindowsclub.com/operation-global-iii-ransomware-decryption-tool-released-70341/</a>

## Owl

Ransomware

Owl is also known as:

- CryptoWire

*Table 444. Table References*

Links
<a href="https://twitter.com/JakubKroustek/status/842342996775448576">https://twitter.com/JakubKroustek/status/842342996775448576</a>

## PadCrypt

Ransomware has a live support chat

*Table 445. 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 446. Table References

Links

<https://twitter.com/BleepinComputer/status/811635075158839296>

## Patcher

Ransomware Targeting macOS users

Table 447. 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 448. Table References

Links

<http://www.thewindowsclub.com/petya-ransomware-decrypt-tool-password-generator>

[https://www.youtube.com/watch?v=mSqxFjZq\\_z4](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 449. Table References

Links
<a href="https://decrypter.emsisoft.com/philadelphia">https://decrypter.emsisoft.com/philadelphia</a>
<a href="http://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/</a>

## PizzaCrypts

Ransomware

*Table 450. Table References*

Links
<a href="http://download.bleepingcomputer.com/BloodDolly/JuicyLemonDecoder.zip">http://download.bleepingcomputer.com/BloodDolly/JuicyLemonDecoder.zip</a>

## PokemonGO

Ransomware Based on Hidden Tear

*Table 451. Table References*

Links
<a href="http://www.nyxbone.com/malware/pokemonGO.html">http://www.nyxbone.com/malware/pokemonGO.html</a>
<a href="http://www.bleepingcomputer.com/news/security/pokemongo-ransomware-installs-backdoor-accounts-and-spreads-to-other-drives/">http://www.bleepingcomputer.com/news/security/pokemongo-ransomware-installs-backdoor-accounts-and-spreads-to-other-drives/</a>

## Polyglot

Ransomware Immitates CTB-Locker

*Table 452. Table References*

Links
<a href="https://support.kaspersky.com/8547">https://support.kaspersky.com/8547</a>
<a href="https://securelist.com/blog/research/76182/polyglot-the-fake-ctb-locker/">https://securelist.com/blog/research/76182/polyglot-the-fake-ctb-locker/</a>

## PowerWare

Ransomware Open-sourced PowerShell

PowerWare is also known as:

- PoshCoder

*Table 453. Table References*

Links
<a href="https://github.com/pan-unit42/public_tools/blob/master/powerware/powerware_decrypt.py">https://github.com/pan-unit42/public_tools/blob/master/powerware/powerware_decrypt.py</a>

<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 454. 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 455. Table References*

Links

<http://www.enigmasoftware.com/prismyourcomputerhasbeenlockedransomware-removal/>

## Ps2exe

Ransomware

*Table 456. Table References*

Links

<https://twitter.com/jiriatvirlab/status/803297700175286273>

## R

Ransomware

*Table 457. Table References*

Links

<https://twitter.com/malwrhunterteam/status/846705481741733892>

## R980

Ransomware

*Table 458. Table References*

Links

<https://otx.alienvault.com/pulse/57976b52b900fe01376feb01/>

## RAA encryptor

Ransomware Possible affiliation with Pony

RAA encryptor is also known as:

- RAA

*Table 459. Table References*

Links

<https://reakta.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 460. Table References*

Links

<https://twitter.com/CryptoInsane/status/846181140025282561>

## Radamant

Ransomware

*Table 461. 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 462. Table References*

Links
<a href="https://support.kaspersky.com/us/viruses/disinfection/10556">https://support.kaspersky.com/us/viruses/disinfection/10556</a>

# Ransomeer

Ransomware Based on the DUMB ransomware

# Rannoh

Ransomware

*Table 463. Table References*

Links
<a href="https://support.kaspersky.com/viruses/disinfection/8547">https://support.kaspersky.com/viruses/disinfection/8547</a>

# RanRan

Ransomware

*Table 464. Table References*

Links
<a href="https://github.com/pan-unit42/public_tools/tree/master/ranran_decryption">https://github.com/pan-unit42/public_tools/tree/master/ranran_decryption</a>
<a href="http://researchcenter.paloaltonetworks.com/2017/03/unit42-targeted-ransomware-attacks-middle-eastern-government-organizations-political-purposes/">http://researchcenter.paloaltonetworks.com/2017/03/unit42-targeted-ransomware-attacks-middle-eastern-government-organizations-political-purposes/</a>



<https://www.bleepingcomputer.com/news/security/new-ranran-ransomware-uses-encryption-tiers-political-messages/>

## Ransoc

Ransomware Doesn't encrypt user files

*Table 465. 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 466. Table References*

Links

[https://www.symantec.com/security\\_response/writeup.jsp?docid=2009-041513-1400-99&tabid=2](https://www.symantec.com/security_response/writeup.jsp?docid=2009-041513-1400-99&tabid=2)

## RarVault

Ransomware

## Razy

Ransomware

*Table 467. Table References*

Links

[http://www.nyxbone.com/malware/Razy\(German\).html](http://www.nyxbone.com/malware/Razy(German).html)

<http://nyxbone.com/malware/Razy.html>

## Rector

Ransomware

*Table 468. Table References*

Links
-------

<a href="https://support.kaspersky.com/viruses/disinfection/4264">https://support.kaspersky.com/viruses/disinfection/4264</a>
---

## RektLocker

Ransomware

*Table 469. Table References*

Links
-------

<a href="https://support.kaspersky.com/viruses/disinfection/4264">https://support.kaspersky.com/viruses/disinfection/4264</a>
---

## RemindMe

Ransomware

*Table 470. Table References*

Links
-------

<a href="http://www.nyxbone.com/malware/RemindMe.html">http://www.nyxbone.com/malware/RemindMe.html</a>
---

<a href="http://i.imgur.com/gV6i5SN.jpg">http://i.imgur.com/gV6i5SN.jpg</a>
---

## Rokku

Ransomware possibly related with Chimera

*Table 471. Table References*

Links
-------

<a href="https://blog.malwarebytes.org/threat-analysis/2016/04/rokku-ransomware/">https://blog.malwarebytes.org/threat-analysis/2016/04/rokku-ransomware/</a>
---

## RoshaLock

Ransomware Stores your files in a password protected RAR file

*Table 472. Table References*

Links
-------

<a href="https://twitter.com/siri_urz/status/842452104279134209">https://twitter.com/siri_urz/status/842452104279134209</a>
---

## Ransomewere

Ransomware Based on HT/EDA2 Utilizes the Jigsaw Ransomware background

*Table 473. Table References*

Links
-------

<https://twitter.com/struppigel/status/801812325657440256>

## RussianRoulette

Ransomware Variant of the Philadelphia ransomware

*Table 474. Table References*

Links

<https://twitter.com/struppigel/status/823925410392080385>

## SADStory

Ransomware Variant of CryPy

*Table 475. 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 476. 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 477. 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](http://www.intelsecurity.com/advanced-threat-research/content/Analysis_SamSa_Ransomware.pdf)

## Sanction

Ransomware Based on HiddenTear, but heavily modified keygen

## Sanctions

Ransomware

*Table 478. Table References*

Links

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

## Sardoninir

Ransomware

*Table 479. Table References*

Links

<https://twitter.com/BleepinComputer/status/835955409953357825>

## Satana

Ransomware

*Table 480. Table References*

Links

<https://blog.malwarebytes.com/threat-analysis/2016/06/satana-ransomware/>

<https://blog.kaspersky.com/satana-ransomware/12558/>

## Scraper

Ransomware

*Table 481. Table References*

Links

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

# Serpico

Ransomware DetoxCrypto Variant

Table 482. Table References

Links
<a href="http://www.nyxbone.com/malware/Serpico.html">http://www.nyxbone.com/malware/Serpico.html</a>

# Shark

Ransomware

Shark is also known as:

- Atom

Table 483. Table References

Links
<a href="http://www.bleepingcomputer.com/news/security/the-shark-ransomware-project-allows-to-create-your-own-customized-ransomware/">http://www.bleepingcomputer.com/news/security/the-shark-ransomware-project-allows-to-create-your-own-customized-ransomware/</a>
<a href="http://www.bleepingcomputer.com/news/security/shark-ransomware-rebrands-as-atom-for-a-fresh-start/">http://www.bleepingcomputer.com/news/security/shark-ransomware-rebrands-as-atom-for-a-fresh-start/</a>

# ShinoLocker

Ransomware

Table 484. Table References

Links
<a href="https://twitter.com/JakubKroustek/status/760560147131408384">https://twitter.com/JakubKroustek/status/760560147131408384</a>
<a href="http://www.bleepingcomputer.com/news/security/new-educational-shinolocker-ransomware-project-released/">http://www.bleepingcomputer.com/news/security/new-educational-shinolocker-ransomware-project-released/</a>

# Shujin

Ransomware

Shujin is also known as:

- KinCrypt

Table 485. Table References

Links
<a href="http://www.nyxbone.com/malware/chineseRansom.html">http://www.nyxbone.com/malware/chineseRansom.html</a>

<http://blog.trendmicro.com/trendlabs-security-intelligence/chinese-language-ransomware-makes-appearance/>

## Simple\_Encoder

Ransomware

*Table 486. 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 487. 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 488. Table References*

Links

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

## Smr32

Ransomware

## SNSLocker

Ransomware Based on EDA2

*Table 489. Table References*

Links
<a href="http://nyxbone.com/malware/SNSLocker.html">http://nyxbone.com/malware/SNSLocker.html</a>
<a href="http://nyxbone.com/images/articulos/malware/snslocker/16.png">http://nyxbone.com/images/articulos/malware/snslocker/16.png</a>

## Sport

Ransomware

## Stampado

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

*Table 490. Table References*

Links
<a href="https://success.trendmicro.com/portal_kb_articledetail?solutionid=1114221">https://success.trendmicro.com/portal_kb_articledetail?solutionid=1114221</a>
<a href="http://www.bleepingcomputer.com/news/security/stampado-ransomware-campaign-decrypted-before-it-started/">http://www.bleepingcomputer.com/news/security/stampado-ransomware-campaign-decrypted-before-it-started/</a>
<a href="https://decrypter.emsisoft.com/stampado">https://decrypter.emsisoft.com/stampado</a>
<a href="https://cdn.streamable.com/video/mp4/kfh3.mp4">https://cdn.streamable.com/video/mp4/kfh3.mp4</a>
<a href="http://blog.trendmicro.com/trendlabs-security-intelligence/the-economics-behind-ransomware-prices/">http://blog.trendmicro.com/trendlabs-security-intelligence/the-economics-behind-ransomware-prices/</a>

## Strictor

Ransomware Based on EDA2, shows Guy Fawkes mask

*Table 491. Table References*

Links
<a href="http://www.nyxbone.com/malware/Strictor.html">http://www.nyxbone.com/malware/Strictor.html</a>

## Surprise

Ransomware Based on EDA2

## Survey

Ransomware Still in development, shows FileIce survey

*Table 492. Table References*

Links
<a href="http://www.bleepingcomputer.com/news/security/in-dev-ransomware-forces-you-do-to-survey-before-unlocking-computer/">http://www.bleepingcomputer.com/news/security/in-dev-ransomware-forces-you-do-to-survey-before-unlocking-computer/</a>

# SynoLocker

Ransomware Exploited Synology NAS firmware directly over WAN

# SZFLocker

Ransomware

Table 493. Table References

Links
<a href="http://now.avg.com/dont-pay-the-ransom-avg-releases-six-free-decryption-tools-to-retrieve-your-files/">http://now.avg.com/dont-pay-the-ransom-avg-releases-six-free-decryption-tools-to-retrieve-your-files/</a>

# TeamXrat

Ransomware

Table 494. Table References

Links
<a href="https://securelist.com/blog/research/76153/teamxrat-brazilian-cybercrime-meets-ransomware/">https://securelist.com/blog/research/76153/teamxrat-brazilian-cybercrime-meets-ransomware/</a>

# TeslaCrypt 0.x - 2.2.0

Ransomware Factorization

TeslaCrypt 0.x - 2.2.0 is also known as:

- AlphaCrypt

Table 495. Table References

Links
<a href="http://www.bleepingcomputer.com/forums/t/576600/tesldecoder-released-to-decrypt-exx-ezz-ecc-files-encrypted-by-teslacrypt/">http://www.bleepingcomputer.com/forums/t/576600/tesldecoder-released-to-decrypt-exx-ezz-ecc-files-encrypted-by-teslacrypt/</a>
<a href="http://www.talosintel.com/teslacrypt_tool/">http://www.talosintel.com/teslacrypt_tool/</a>

# TeslaCrypt 3.0+

Ransomware 4.0+ has no extension

Table 496. Table References

Links
<a href="http://www.bleepingcomputer.com/forums/t/576600/tesldecoder-released-to-decrypt-exx-ezz-ecc-files-encrypted-by-teslacrypt/">http://www.bleepingcomputer.com/forums/t/576600/tesldecoder-released-to-decrypt-exx-ezz-ecc-files-encrypted-by-teslacrypt/</a>



<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 497. Table References

### Links

<http://www.bleepingcomputer.com/forums/t/576600/tesldecoder-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 498. Table References

### Links

<http://www.bleepingcomputer.com/forums/t/576600/tesldecoder-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 499. Table References

Links
<a href="http://www.bleepingcomputer.com/forums/t/547708/torrentlocker-ransomware-cracked-and-decrypter-has-been-made/">http://www.bleepingcomputer.com/forums/t/547708/torrentlocker-ransomware-cracked-and-decrypter-has-been-made/</a>
<a href="https://twitter.com/PolarToffee/status/804008236600934403">https://twitter.com/PolarToffee/status/804008236600934403</a>
<a href="http://blog.talosintelligence.com/2017/03/crypt0l0cker-torrentlocker-old-dog-new.html">http://blog.talosintelligence.com/2017/03/crypt0l0cker-torrentlocker-old-dog-new.html</a>

## TowerWeb

Ransomware

Table 500. Table References

Links
<a href="http://www.bleepingcomputer.com/forums/t/618055/towerweb-ransomware-help-support-topic-payment-instructionsjpg/">http://www.bleepingcomputer.com/forums/t/618055/towerweb-ransomware-help-support-topic-payment-instructionsjpg/</a>

## Toxcrypt

Ransomware

## Trojan

Ransomware

Trojan is also known as:

- BrainCrypt

Table 501. Table References

Links
<a href="https://download.bleepingcomputer.com/demonslay335/BrainCryptDecrypter.zip">https://download.bleepingcomputer.com/demonslay335/BrainCryptDecrypter.zip</a>
<a href="https://twitter.com/PolarToffee/status/811249250285842432">https://twitter.com/PolarToffee/status/811249250285842432</a>

## Troldesh orShade, XTBL

Ransomware May download additional malware after encryption

Table 502. Table References

Links
<a href="https://www.nomoreransom.org/uploads/ShadeDecryptor_how-to_guide.pdf">https://www.nomoreransom.org/uploads/ShadeDecryptor_how-to_guide.pdf</a>
<a href="http://www.nyxbone.com/malware/Troldesh.html">http://www.nyxbone.com/malware/Troldesh.html</a>

<https://www.bleepingcomputer.com/news/security/kelihos-botnet-delivering-shade-troldesh-ransomware-with-no-more-ransom-extension/>

## TrueCrypter

Ransomware

*Table 503. Table References*

Links

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

## Turkish

Ransomware

*Table 504. Table References*

Links

<https://twitter.com/struppigel/status/821991600637313024>

## Turkish Ransom

Ransomware

*Table 505. Table References*

Links

<http://www.nyxbone.com/malware/turkishRansom.html>

## UmbreCrypt

Ransomware CrypBoss Family

*Table 506. Table References*

Links

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

## UnblockUPC

Ransomware

*Table 507. 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 508. Table References*

Links

<https://twitter.com/malwrhunterteam/status/839038399944224768>

## VapeLauncher

Ransomware CryptoWire variant

*Table 509. Table References*

Links

<https://twitter.com/struppigel/status/839771195830648833>

## VaultCrypt

Ransomware

VaultCrypt is also known as:

- CrypVault
- Zlader

*Table 510. Table References*

Links

<http://www.nyxbone.com/malware/russianRansom.html>

## VBRANSOM 7

Ransomware

*Table 511. Table References*

Links

<https://twitter.com/BleepinComputer/status/817851339078336513>

# VenusLocker

Ransomware Based on EDA2

Table 512. Table References

Links
<a href="https://blog.malwarebytes.com/threat-analysis/2016/08/venus-locker-another-net-ransomware/?utm_source=twitter&amp;utm_medium=social">https://blog.malwarebytes.com/threat-analysis/2016/08/venus-locker-another-net-ransomware/?utm_source=twitter&amp;utm_medium=social</a>
<a href="http://www.nyxbone.com/malware/venusLocker.html">http://www.nyxbone.com/malware/venusLocker.html</a>

# Virlock

Ransomware Polymorphism / Self-replication

Table 513. Table References

Links
<a href="http://www.nyxbone.com/malware/Virlock.html">http://www.nyxbone.com/malware/Virlock.html</a>
<a href="http://www.welivesecurity.com/2014/12/22/win32virlock-first-self-reproducing-ransomware-also-shape-shifter/">http://www.welivesecurity.com/2014/12/22/win32virlock-first-self-reproducing-ransomware-also-shape-shifter/</a>

# Virus-Encoder

Ransomware

Virus-Encoder is also known as:

- CrySiS

Table 514. Table References

Links
<a href="http://www.welivesecurity.com/2016/11/24/new-decryption-tool-crysis-ransomware/">http://www.welivesecurity.com/2016/11/24/new-decryption-tool-crysis-ransomware/</a>
<a href="http://media.kaspersky.com/utilities/VirusUtilities/EN/rakhnidecryptor.zip">http://media.kaspersky.com/utilities/VirusUtilities/EN/rakhnidecryptor.zip</a>
<a href="http://www.nyxbone.com/malware/virus-encoder.html">http://www.nyxbone.com/malware/virus-encoder.html</a>
<a href="http://blog.trendmicro.com/trendlabs-security-intelligence/crysis-targeting-businesses-in-australia-new-zealand-via-brute-forced-rdps/">http://blog.trendmicro.com/trendlabs-security-intelligence/crysis-targeting-businesses-in-australia-new-zealand-via-brute-forced-rdps/</a>

# WildFire Locker

Ransomware Zyklon variant

WildFire Locker is also known as:

- Hades Locker

Table 515. Table References

Links
-------

<a href="https://labs.opendns.com/2016/07/13/wildfire-ransomware-gaining-momentum/">https://labs.opendns.com/2016/07/13/wildfire-ransomware-gaining-momentum/</a>
---

## Xorist

Ransomware encrypted files will still have the original non-encrypted header of 0x33 bytes length

*Table 516. Table References*

Links
-------

<a href="https://support.kaspersky.com/viruses/disinfection/2911">https://support.kaspersky.com/viruses/disinfection/2911</a>
---

<a href="https://decrypter.emsisoft.com/xorist">https://decrypter.emsisoft.com/xorist</a>
---

## XRTN

Ransomware VaultCrypt family

## You Have Been Hacked!!!

Ransomware Attempt to steal passwords

*Table 517. Table References*

Links
-------

<a href="https://twitter.com/malwrhunterteam/status/808280549802418181">https://twitter.com/malwrhunterteam/status/808280549802418181</a>
---

## Zcrypt

Ransomware

Zcrypt is also known as:

- Zcryptor

*Table 518. Table References*

Links
-------

<a href="https://blogs.technet.microsoft.com/mmpc/2016/05/26/link-lnk-to-ransom/">https://blogs.technet.microsoft.com/mmpc/2016/05/26/link-lnk-to-ransom/</a>
---

## Zeta

Ransomware

Zeta is also known as:

- CryptoMix

*Table 519. Table References*

Links

<https://twitter.com/JakubKroustek/status/804009831518572544>

## Zimbra

Ransomware [mpriksen@priest.com](mailto:mpriksen@priest.com)

*Table 520. 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 521. Table References*

Links

<http://www.nyxbone.com/malware/russianRansom.html>

## Zorro

Ransomware

*Table 522. 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 523. Table References

Links
<a href="http://blog.talosintelligence.com/2017/05/jaff-ransomware.html">http://blog.talosintelligence.com/2017/05/jaff-ransomware.html</a>
<a href="https://www.bleepingcomputer.com/news/security/jaff-ransomware-distributed-via-necurs-malspam-and-asking-for-a-3-700-ransom/">https://www.bleepingcomputer.com/news/security/jaff-ransomware-distributed-via-necurs-malspam-and-asking-for-a-3-700-ransom/</a>

## Uiwix Ransomware

Using EternalBlue SMB Exploit To Infect Victims

Table 524. Table References

Links
<a href="https://www.bleepingcomputer.com/news/security/uiwix-ransomware-using-eternalblue-smb-exploit-to-infect-victims/">https://www.bleepingcomputer.com/news/security/uiwix-ransomware-using-eternalblue-smb-exploit-to-infect-victims/</a>

## 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 525. Table References

Links
<a href="https://www.teamviewer.com">https://www.teamviewer.com</a>

## 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 526. Table References

Links
<a href="http://www.cultdeadcow.com/tools/bo.html">http://www.cultdeadcow.com/tools/bo.html</a>
<a href="http://www.symantec.com/avcenter/warn/backorifice.html">http://www.symantec.com/avcenter/warn/backorifice.html</a>

## 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 527. Table References

Links
<a href="http://www.symantec.com/avcenter/warn/backorifice.html">http://www.symantec.com/avcenter/warn/backorifice.html</a>
<a href="https://www.f-secure.com/v-descs/netbus.shtml">https://www.f-secure.com/v-descs/netbus.shtml</a>

## 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 528. Table References

Links
<a href="https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-poison-ivy.pdf">https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-poison-ivy.pdf</a>
<a href="https://www.f-secure.com/v-descs/backdoor_w32_poisonivy.shtml">https://www.f-secure.com/v-descs/backdoor_w32_poisonivy.shtml</a>

## 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 529. Table References*

Links
<a href="https://www.symantec.com/security_response/writeup.jsp?docid=2001-020114-5445-99">https://www.symantec.com/security_response/writeup.jsp?docid=2001-020114-5445-99</a>

## 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 530. Table References*

Links
<a href="https://en.wikipedia.org/wiki/Beast_(Trojan_horse)">https://en.wikipedia.org/wiki/Beast_(Trojan_horse)</a>

## 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 531. Table References*

Links
<a href="https://www.revolvvy.com/main/index.php?s=Bifrost%20(trojan%20horse)&amp;item_type=topic">https://www.revolvvy.com/main/index.php?s=Bifrost%20(trojan%20horse)&amp;item_type=topic</a>
<a href="http://malware-info.blogspot.lu/2008/10/bifrost-trojan.html">http://malware-info.blogspot.lu/2008/10/bifrost-trojan.html</a>

# 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 532. Table References

Links
<a href="https://krebsonsecurity.com/2014/05/blackshades-trojan-users-had-it-coming/">https://krebsonsecurity.com/2014/05/blackshades-trojan-users-had-it-coming/</a>

# 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 533. Table References

Links
<a href="https://blog.malwarebytes.com/threat-analysis/2012/06/you-dirty-rat-part-1-darkcomet/">https://blog.malwarebytes.com/threat-analysis/2012/06/you-dirty-rat-part-1-darkcomet/</a>
<a href="https://blogs.cisco.com/security/talos/darkkomet-rat-spam">https://blogs.cisco.com/security/talos/darkkomet-rat-spam</a>

# 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 534. Table References

Links
<a href="https://www.symantec.com/security_response/writeup.jsp?docid=2002-121116-0350-99">https://www.symantec.com/security_response/writeup.jsp?docid=2002-121116-0350-99</a>

# 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 535. Table References

Links
<a href="http://lexmarket.su/thread-27692.html">http://lexmarket.su/thread-27692.html</a>

## Optix Pro

Optix Pro is a configurable remote access tool or Trojan, similar to SubSeven or BO2K

Table 536. Table References

Links
<a href="https://en.wikipedia.org/wiki/Optix_Pro">https://en.wikipedia.org/wiki/Optix_Pro</a>
<a href="https://www.symantec.com/security_response/writeup.jsp?docid=2002-090416-0521-99">https://www.symantec.com/security_response/writeup.jsp?docid=2002-090416-0521-99</a>
<a href="https://www.symantec.com/security_response/attacksignatures/detail.jsp?asid=20208">https://www.symantec.com/security_response/attacksignatures/detail.jsp?asid=20208</a>

## 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 537. Table References

Links
<a href="https://en.wikipedia.org/wiki/Back_Orifice_2000">https://en.wikipedia.org/wiki/Back_Orifice_2000</a>
<a href="https://home.mcafee.com/VirusInfo/VirusProfile.aspx?key=10229">https://home.mcafee.com/VirusInfo/VirusProfile.aspx?key=10229</a>
<a href="https://www.symantec.com/security_response/writeup.jsp?docid=2000-121814-5417-99">https://www.symantec.com/security_response/writeup.jsp?docid=2000-121814-5417-99</a>
<a href="https://www.f-secure.com/v-descs/bo2k.shtml">https://www.f-secure.com/v-descs/bo2k.shtml</a>

## 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 538. Table References

Links
-------

<a href="https://www.realvnc.com/">https://www.realvnc.com/</a>
---

## 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

Table 539. Table References

Links
-------

<a href="https://securelist.com/securelist/files/2016/02/KL_AdwindPublicReport_2016.pdf">https://securelist.com/securelist/files/2016/02/KL_AdwindPublicReport_2016.pdf</a>
---

<a href="https://www.f-secure.com/v-descs/backdoor_java_adwind.shtml">https://www.f-secure.com/v-descs/backdoor_java_adwind.shtml</a>
---

## Albertino Advanced RAT

Table 540. Table References

Links
-------

<a href="https://www.virustotal.com/en/file/b31812e5b4c63c5b52c9b23e76a5ea9439465ab366a9291c6074bfae5c328e73/analysis/1359376345/">https://www.virustotal.com/en/file/b31812e5b4c63c5b52c9b23e76a5ea9439465ab366a9291c6074bfae5c328e73/analysis/1359376345/</a>
---

## Arcom

The malware is a Remote Access Trojan (RAT), known as Arcom RAT, and it is sold on underground forums for \$2000.00.

Table 541. Table References

Links
-------

<a href="https://www.symantec.com/security_response/writeup.jsp?docid=2012-112912-5237-99">https://www.symantec.com/security_response/writeup.jsp?docid=2012-112912-5237-99</a>
---

<a href="http://blog.trendmicro.com/trendlabs-security-intelligence/tsunami-warning-leads-to-arcom-rat/">http://blog.trendmicro.com/trendlabs-security-intelligence/tsunami-warning-leads-to-arcom-rat/</a>
---

## BlackNix

BlackNix rat is a rat coded in delphi.

Table 542. Table References

Links
-------

<a href="https://leakforums.net/thread-18123?tid=18123&amp;&amp;pq=1">https://leakforums.net/thread-18123?tid=18123&amp;&amp;pq=1</a>
---

# Blue Banana

Blue Banana is a RAT (Remote Administration Tool) created purely in Java

Table 543. Table References

Links
<a href="https://leakforums.net/thread-123872">https://leakforums.net/thread-123872</a>
<a href="https://techanarchy.net/2014/02/blue-banana-rat-config/">https://techanarchy.net/2014/02/blue-banana-rat-config/</a>

# 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 544. Table References

Links
<a href="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/2013/10/know-your-enemy-tracking-a-rapidly-evolving-apt-actor.html</a>

# ClientMesh

ClientMesh is a Remote Administration Application which allows a user to control a number of client PCs from around the world.

Table 545. Table References

Links
<a href="https://sinister.ly/Thread-ClientMesh-RAT-In-Built-FUD-Crypter-Stable-DDoSer-No-PortForwarding-40-Lifetime">https://sinister.ly/Thread-ClientMesh-RAT-In-Built-FUD-Crypter-Stable-DDoSer-No-PortForwarding-40-Lifetime</a>
<a href="https://blog.yakuza112.org/2012/clientmesh-rat-v5-cracked-clean/">https://blog.yakuza112.org/2012/clientmesh-rat-v5-cracked-clean/</a>

# 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 546. Table References

Links
<a href="http://www.hackersthirst.com/2011/03/cybergate-rat-hacking-facebook-twitter.html">http://www.hackersthirst.com/2011/03/cybergate-rat-hacking-facebook-twitter.html</a>
<a href="http://www.nbcnews.com/id/41584097/ns/technology_and_science-security/t/cybergate-leaked-emails-hint-corporate-hacking-conspiracy/">http://www.nbcnews.com/id/41584097/ns/technology_and_science-security/t/cybergate-leaked-emails-hint-corporate-hacking-conspiracy/</a>

## Dark DDoSeR

Table 547. Table References

Links
<a href="http://meinblogzumtesten.blogspot.lu/2013/05/dark-ddoser-v56c-cracked.html">http://meinblogzumtesten.blogspot.lu/2013/05/dark-ddoser-v56c-cracked.html</a>

## 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 548. Table References

Links
<a href="https://www.infosecurity-magazine.com/blogs/the-dark-rat/">https://www.infosecurity-magazine.com/blogs/the-dark-rat/</a>
<a href="http://darkratphp.blogspot.lu/">http://darkratphp.blogspot.lu/</a>

## Greame

Table 549. Table References

Links
<a href="https://sites.google.com/site/greymecompany/greame-rat-project">https://sites.google.com/site/greymecompany/greame-rat-project</a>

## 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 550. Table References

Links
<a href="http://securityaffairs.co/wordpress/54837/hacking/one-stop-shop-hacking.html">http://securityaffairs.co/wordpress/54837/hacking/one-stop-shop-hacking.html</a>

## 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.

Table 551. Table References

Links
<a href="https://www.rekings.com/shop/jrat/">https://www.rekings.com/shop/jrat/</a>

## jSpy

jSpy is a Java RAT.

Table 552. Table References

Links
<a href="https://leakforums.net/thread-479505">https://leakforums.net/thread-479505</a>

## Lost Door

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.

Table 553. Table References

Links
<a href="http://lost-door.blogspot.lu/">http://lost-door.blogspot.lu/</a>
<a href="http://blog.trendmicro.com/trendlabs-security-intelligence/lost-door-rat-accessible-customizable-attack-tool/">http://blog.trendmicro.com/trendlabs-security-intelligence/lost-door-rat-accessible-customizable-attack-tool/</a>
<a href="https://www.cyber.nj.gov/threat-profiles/trojan-variants/lost-door-rat">https://www.cyber.nj.gov/threat-profiles/trojan-variants/lost-door-rat</a>

## 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 554. Table References

Links
<a href="https://leakforums.net/thread-284656">https://leakforums.net/thread-284656</a>

## 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.



Table 555. Table References

Links
<a href="https://www.cyber.nj.gov/threat-profiles/trojan-variants/njrat">https://www.cyber.nj.gov/threat-profiles/trojan-variants/njrat</a>

## 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 556. Table References

Links
<a href="https://www.rekings.com/pandora-rat-2-2/">https://www.rekings.com/pandora-rat-2-2/</a>

## 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 557. Table References

Links
<a href="http://blog.trendmicro.com/trendlabs-security-intelligence/predator-pain-and-limitless-behind-the-fraud/">http://blog.trendmicro.com/trendlabs-security-intelligence/predator-pain-and-limitless-behind-the-fraud/</a>
<a href="https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-predator-pain-and-limitless.pdf">https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-predator-pain-and-limitless.pdf</a>

## Punisher RAT

Remote administration tool

Table 558. Table References

Links
<a href="http://punisher-rat.blogspot.lu/">http://punisher-rat.blogspot.lu/</a>

## SpyGate

This is tool that allow you to control your computer form anywhere in world with full support to

unicode language.

Table 559. Table References

Links
<a href="https://www.rekings.com/spygate-rat-3-2/">https://www.rekings.com/spygate-rat-3-2/</a>
<a href="https://www.symantec.com/security_response/attacksignatures/detail.jsp%3Fasid%3D27950">https://www.symantec.com/security_response/attacksignatures/detail.jsp%3Fasid%3D27950</a>
<a href="http://spygate-rat.blogspot.lu/">http://spygate-rat.blogspot.lu/</a>

## Small-Net

RAT

Small-Net is also known as:

- SmallNet

Table 560. Table References

Links
<a href="http://small-net-rat.blogspot.lu/">http://small-net-rat.blogspot.lu/</a>

## Vantom

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

Table 561. Table References

Links
<a href="https://www.rekings.com/vantom-rat/">https://www.rekings.com/vantom-rat/</a>

## 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 562. Table References

Links
<a href="https://leakforums.net/thread-497480">https://leakforums.net/thread-497480</a>

===

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 563. Table References

Links
-------

## Netwire

NetWire has a built-in keylogger that can capture inputs from peripheral devices such as USB card readers.

*Table 564. 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 565. 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 566. 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 567. Table References*

Links

<https://www.rekings.com/babylon-rat/>

# Imminent Monitor

RAT

Table 568. Table References

Links
<a href="http://www.imminentmethods.info/">http://www.imminentmethods.info/</a>

## 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 569. Table References

Links
<a href="http://droidjack.net/">http://droidjack.net/</a>

## 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 570. Table References

Links
<a href="https://github.com/quasar/QuasarRAT">https://github.com/quasar/QuasarRAT</a>

## 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 571. Table References

Links
<a href="https://github.com/qqshow/dendroid">https://github.com/qqshow/dendroid</a>

<https://github.com/nyx0/Dendroid>

## Ratty

A Java R.A.T. program

*Table 572. Table References*

Links

<https://github.com/shotskeber/Ratty>

## RaTRon

Java RAT

*Table 573. Table References*

Links

<http://level23hacktools.com/forum/showthread.php?t=27971>

<https://leakforums.net/thread-405562?tid=405562&&pq=1>

## Arabian-Attacker RAT

*Table 574. 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 575. 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 576. Table References*

Links

<http://adzok.com/>

# Schwarze-Sonne-RAT

Schwarze-Sonne-RAT is also known as:

- SS-RAT
- Schwarze Sonne

Table 577. Table References

Links
<a href="https://github.com/mwsrc/Schwarze-Sonne-RAT">https://github.com/mwsrc/Schwarze-Sonne-RAT</a>

# Cyber Eye RAT

Table 578. Table References

Links
<a href="https://www.indetectables.net/viewtopic.php?t=24245">https://www.indetectables.net/viewtopic.php?t=24245</a>

# Batch NET

# RWX RAT

Table 579. Table References

Links
<a href="https://leakforums.net/thread-530663">https://leakforums.net/thread-530663</a>

# 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 580. Table References

Links
<a href="http://spynet-rat-officiel.blogspot.lu/">http://spynet-rat-officiel.blogspot.lu/</a>

# CTOS

Table 581. Table References

Links
<a href="https://leakforums.net/thread-559871">https://leakforums.net/thread-559871</a>

# Virus RAT

Table 582. Table References

Links
<a href="https://github.com/mwsrc/Virus-RAT-v8.0-Beta">https://github.com/mwsrc/Virus-RAT-v8.0-Beta</a>

# Atelier Web Remote Commander

Table 583. Table References

Links
<a href="http://www.atelierweb.com/products/">http://www.atelierweb.com/products/</a>

# 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 584. Table References

Links
<a href="https://github.com/chrismattmann/drat">https://github.com/chrismattmann/drat</a>

# MoSucker

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

Table 585. Table References

Links
<a href="https://www.f-secure.com/v-descs/mosuck.shtml">https://www.f-secure.com/v-descs/mosuck.shtml</a>

# Theef

Table 586. Table References

Links
<a href="http://www.grayhatforum.org/thread-4373-post-5213.html#pid5213">http://www.grayhatforum.org/thread-4373-post-5213.html#pid5213</a>
<a href="http://www.spy-emergency.com/research/T/Theef_Download_Creator.html">http://www.spy-emergency.com/research/T/Theef_Download_Creator.html</a>
<a href="http://www.spy-emergency.com/research/T/Theef.html">http://www.spy-emergency.com/research/T/Theef.html</a>

# 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 587. Table References

Links
<a href="http://prorat.software.informer.com/">http://prorat.software.informer.com/</a>
<a href="http://malware.wikia.com/wiki/ProRat">http://malware.wikia.com/wiki/ProRat</a>

## Setro

Table 588. Table References

Links
<a href="https://sites.google.com/site/greymecompany/setro-rat-project">https://sites.google.com/site/greymecompany/setro-rat-project</a>

## Indetectables RAT

Table 589. Table References

Links
<a href="http://www.connect-trojan.net/2015/03/indetectables-rat-v.0.5-beta.html">http://www.connect-trojan.net/2015/03/indetectables-rat-v.0.5-beta.html</a>

## Luminosity Link

Table 590. Table References

Links
<a href="https://luminosity.link/">https://luminosity.link/</a>

## Orcus

Table 591. Table References

Links
<a href="https://orcustechnologies.com/">https://orcustechnologies.com/</a>

## Blizzard

Table 592. Table References

Links
<a href="http://www.connect-trojan.net/2014/10/blizzard-rat-lite-v1.3.1.html">http://www.connect-trojan.net/2014/10/blizzard-rat-lite-v1.3.1.html</a>

## Kazybot

Table 593. Table References

Links
-------



<a href="https://www.rekings.com/kazybot-lite-php-rat/">https://www.rekings.com/kazybot-lite-php-rat/</a>
---

<a href="http://telussecuritylabs.com/threats/show/TSL20150122-06">http://telussecuritylabs.com/threats/show/TSL20150122-06</a>
---

## **BX**

*Table 594. Table References*

Links
-------

<a href="http://www.connect-trojan.net/2015/01/bx-rat-v1.0.html">http://www.connect-trojan.net/2015/01/bx-rat-v1.0.html</a>
---

## **death**

### **Sky Wyder**

*Table 595. Table References*

Links
-------

<a href="https://rubear.me/threads/sky-wyder-2016-cracked.127/">https://rubear.me/threads/sky-wyder-2016-cracked.127/</a>
---

## **DarkTrack**

*Table 596. Table References*

Links
-------

<a href="https://www.rekings.com/darktrack-4-alien/">https://www.rekings.com/darktrack-4-alien/</a>
---

<a href="http://news.softpedia.com/news/free-darktrack-rat-has-the-potential-of-being-the-best-rat-on-the-market-508179.shtml">http://news.softpedia.com/news/free-darktrack-rat-has-the-potential-of-being-the-best-rat-on-the-market-508179.shtml</a>
---

## **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 597. Table References*

Links
-------

<a href="https://github.com/c4bbage/xRAT">https://github.com/c4bbage/xRAT</a>
---

## **Biodox**

*Table 598. Table References*

Links
-------

<a href="http://sakhackingarticles.blogspot.lu/2014/08/biodox-rat.html">http://sakhackingarticles.blogspot.lu/2014/08/biodox-rat.html</a>
---

# Offence

Offense RAT is a free remote administration tool made in Delphi 9.

Table 599. Table References

Links
<a href="https://leakforums.net/thread-31386?tid=31386&amp;&amp;pq=1">https://leakforums.net/thread-31386?tid=31386&amp;&amp;pq=1</a>

# Apocalypse

Table 600. Table References

Links
<a href="https://leakforums.net/thread-36962">https://leakforums.net/thread-36962</a>

# JCage

Table 601. Table References

Links
<a href="https://leakforums.net/thread-363920">https://leakforums.net/thread-363920</a>

# 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 602. Table References

Links
<a href="http://malware.wikia.com/wiki/Nuclear_RAT">http://malware.wikia.com/wiki/Nuclear_RAT</a>
<a href="http://www.nuclearwintercrew.com/Products-View/21/Nuclear_RAT_2.1.0/">http://www.nuclearwintercrew.com/Products-View/21/Nuclear_RAT_2.1.0/</a>

# Ozone

C++ REMOTE CONTROL PROGRAM

Table 603. Table References

Links
<a href="http://ozonercp.com/">http://ozonercp.com/</a>

# Xanity

Table 604. Table References

Links
-------

<https://github.com/alienwithin/xanity-php-rat>

## DarkMoon

DarkMoon is also known as:

- Dark Moon

## Xpert

*Table 605. Table References*

Links
<a href="http://broad-product.biz/forum/r-a-t-(remote-administration-tools)/xpert-rat-3-0-10-by-abronsius(vb6)/">http://broad-product.biz/forum/r-a-t-(remote-administration-tools)/xpert-rat-3-0-10-by-abronsius(vb6)/</a>
<a href="https://www.nulled.to/topic/18355-xpert-rat-309/">https://www.nulled.to/topic/18355-xpert-rat-309/</a>
<a href="https://trickytamilan.blogspot.lu/2016/03/xpert-rat.html">https://trickytamilan.blogspot.lu/2016/03/xpert-rat.html</a>

## 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.

*Table 606. Table References*

Links
<a href="https://www.alienvault.com/blogs/labs-research/kilerrrat-taking-over-where-njrat-remote-access-trojan-left-off">https://www.alienvault.com/blogs/labs-research/kilerrrat-taking-over-where-njrat-remote-access-trojan-left-off</a>

## 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 ([http://lost-door\[.\]blogspot\[.\]com/](http://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.

Table 607. Table References

Links
<a href="http://blog.trendmicro.com/trendlabs-security-intelligence/lost-door-rat-accessible-customizable-attack-tool/">http://blog.trendmicro.com/trendlabs-security-intelligence/lost-door-rat-accessible-customizable-attack-tool/</a>

## 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 608. Table References

Links
<a href="https://www.rekings.com/loki-rat-php-rat/">https://www.rekings.com/loki-rat-php-rat/</a>

## MLRat

Table 609. Table References

Links
<a href="https://github.com/BahNahNah/MLRat">https://github.com/BahNahNah/MLRat</a>

## SpyCronic

Table 610. Table References

Links
<a href="http://perfect-conexao.blogspot.lu/2014/09/spycronic-1021.html">http://perfect-conexao.blogspot.lu/2014/09/spycronic-1021.html</a>
<a href="http://www.connect-trojan.net/2013/09/spycronic-v1.02.1.html">http://www.connect-trojan.net/2013/09/spycronic-v1.02.1.html</a>
<a href="https://ranger-exploit.com/spycronic-v1-02-1/">https://ranger-exploit.com/spycronic-v1-02-1/</a>

## Pupy

Pupy is an opensource, cross-platform (Windows, Linux, OSX, Android) remote administration and post-exploitation tool mainly written in python

Table 611. Table References

Links
<a href="https://github.com/n1nj4sec/pupy">https://github.com/n1nj4sec/pupy</a>

# Nova

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

Table 612. Table References

Links
<a href="http://novarat.sourceforge.net/">http://novarat.sourceforge.net/</a>

# BD Y3K RAT

BD Y3K RAT is also known as:

- Back Door Y3K RAT

Table 613. Table References

Links
<a href="https://tools.cisco.com/security/center/viewIpsSignature.x?signatureId=9401&amp;signatureSubId=2">https://tools.cisco.com/security/center/viewIpsSignature.x?signatureId=9401&amp;signatureSubId=2</a>
<a href="https://tools.cisco.com/security/center/viewIpsSignature.x?signatureId=9401&amp;signatureSubId=0&amp;softwareVersion=6.0&amp;releaseVersion=S177">https://tools.cisco.com/security/center/viewIpsSignature.x?signatureId=9401&amp;signatureSubId=0&amp;softwareVersion=6.0&amp;releaseVersion=S177</a>
<a href="https://www.symantec.com/security_response/attacksignatures/detail.jsp?asid=20292">https://www.symantec.com/security_response/attacksignatures/detail.jsp?asid=20292</a>
<a href="https://www.symantec.com/security_response/attacksignatures/detail.jsp?asid=20264">https://www.symantec.com/security_response/attacksignatures/detail.jsp?asid=20264</a>

# Turkojan

Turkojan is a remote administration and spying tool for Microsoft Windows operating systems.

Table 614. Table References

Links
<a href="http://turkojan.blogspot.lu/">http://turkojan.blogspot.lu/</a>

# 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 615. Table References

Links
<a href="http://josh.com/tiny/">http://josh.com/tiny/</a>

# 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 616. Table References

Links
<a href="https://www.security-database.com/toolswatch/SharK-3-Remote-Administration-Tool.html">https://www.security-database.com/toolswatch/SharK-3-Remote-Administration-Tool.html</a>
<a href="http://lpc1.clpccd.cc.ca.us/lpc/mdaoud/CNT7501/NETLABS/Ethical_Hacking_Lab_05.pdf">http://lpc1.clpccd.cc.ca.us/lpc/mdaoud/CNT7501/NETLABS/Ethical_Hacking_Lab_05.pdf</a>

## 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 617. Table References

Links
<a href="https://www.symantec.com/security_response/writeup.jsp?docid=2003-022018-5040-99">https://www.symantec.com/security_response/writeup.jsp?docid=2003-022018-5040-99</a>

## Paradox

Table 618. Table References

Links
<a href="https://www.nulled.to/topic/155464-paradox-rat/">https://www.nulled.to/topic/155464-paradox-rat/</a>

## SpyNote

Android RAT

Table 619. Table References

Links
<a href="https://www.rekings.com/spynote-v4-android-rat/">https://www.rekings.com/spynote-v4-android-rat/</a>

# 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 620. Table References*

Links
<a href="https://networklookout.com/help/">https://networklookout.com/help/</a>

## 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 621. Table References*

Links
<a href="http://www.dameware.com/dameware-mini-remote-control">http://www.dameware.com/dameware-mini-remote-control</a>

## 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 622. Table References*

Links
<a href="https://www.remoteutilities.com/">https://www.remoteutilities.com/</a>

## 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.

*Table 623. Table References*

Links
<a href="http://ammyy-admin.soft32.com/">http://ammyy-admin.soft32.com/</a>

# 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 624. Table References

Links
<a href="http://www.uvnc.com/">http://www.uvnc.com/</a>

# 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 625. Table References

Links
<a href="http://www.aeroadmin.com/en/">http://www.aeroadmin.com/en/</a>

# 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 626. Table References

Links
<a href="https://www.remotepc.com/">https://www.remotepc.com/</a>

# 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 627. Table References

Links
<a href="http://seecreen.com/">http://seecreen.com/</a>



# 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 628. Table References

Links
<a href="https://chrome.google.com/webstore/detail/chrome-remote-desktop/gbchcmhahfdphkhkmpfmihenigmpp?hl=en">https://chrome.google.com/webstore/detail/chrome-remote-desktop/gbchcmhahfdphkhkmpfmihenigmpp?hl=en</a>

# AnyDesk

AnyDesk is a remote desktop program that you can run portably or install like a regular program.

Table 629. Table References

Links
<a href="https://anydesk.com/remote-desktop">https://anydesk.com/remote-desktop</a>

# 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 630. Table References

Links
<a href="http://www.litemanager.com/">http://www.litemanager.com/</a>

# 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 631. Table References

Links
<a href="https://www.comodo.com/home/download/download.php?prod=comodounite">https://www.comodo.com/home/download/download.php?prod=comodounite</a>

# 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 632. Table References

Links
<a href="https://showmypc.com/">https://showmypc.com/</a>

## 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 633. Table References

Links
<a href="https://www.join.me/">https://www.join.me/</a>

## 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 634. Table References

Links
<a href="http://www.nchsoftware.com/remotedesktop/index.html">http://www.nchsoftware.com/remotedesktop/index.html</a>

## 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 635. Table References

Links
<a href="http://www.beamyourscreen.com/">http://www.beamyourscreen.com/</a>

## 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 636. Table References

Links
-------

[http://www.nuclearwintercrew.com/Products-View/57/Bandook\\_RAT\\_v1.35](http://www.nuclearwintercrew.com/Products-View/57/Bandook_RAT_v1.35)  
NEW\_/[[http://www.nuclearwintercrew.com/Products-View/57/Bandook\\_RAT\\_v1.35](http://www.nuclearwintercrew.com/Products-View/57/Bandook_RAT_v1.35)NEW\_] ]

## Cerberus RAT

Table 637. 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 638. Table References

Links

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

### 5p00f3r.N\$ RAT

### P. Storrie RAT

### xHacker Pro RAT

### NetDevil

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

Table 639. Table References

Links

[https://www.symantec.com/security\\_response/writeup.jsp?docid=2002-021310-3452-99](https://www.symantec.com/security_response/writeup.jsp?docid=2002-021310-3452-99)

## 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 640. Table References*

Links

<https://keitarotds.com/>

# Sutra

Sutra TDS was dominant from 2012 till 2015

*Table 641. Table References*

Links

<http://kytoon.com/sutra-tds.html>

# SimpleTDS

SimpleTDS is a basic open source TDS

SimpleTDS is also known as:

- Stds

*Table 642. Table References*

Links

<https://sourceforge.net/projects/simpletds/>

# BossTDS

BossTDS

*Table 643. Table References*

Links

<http://bosstds.com/>

# BlackHat TDS

BlackHat TDS is sold underground.

*Table 644. Table References*

## 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](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

*Table 645. Table References*

Links
<a href="https://en.wikipedia.org/wiki/PLA_Unit_61398">https://en.wikipedia.org/wiki/PLA_Unit_61398</a>
<a href="http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf">http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf</a>

## 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 646. Table References*

Links
<a href="http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf">http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf</a>

### 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
- Sunshop Group

*Table 647. Table References*

Links
<a href="https://www.proofpoint.com/us/exploring-bergard-old-malware-new-tricks">https://www.proofpoint.com/us/exploring-bergard-old-malware-new-tricks</a>
<a href="https://www.nytimes.com/2016/06/12/technology/the-chinese-hackers-in-the-back-office.html">https://www.nytimes.com/2016/06/12/technology/the-chinese-hackers-in-the-back-office.html</a>

## Dust Storm

*Table 648. Table References*

Links
<a href="https://www.cylance.com/hubfs/2015_cylance_website/assets/operation-dust-storm/Op_Dust_Storm_Report.pdf">https://www.cylance.com/hubfs/2015_cylance_website/assets/operation-dust-storm/Op_Dust_Storm_Report.pdf</a>

## Karma Panda

Adversary targeting dissident groups in China and its surroundings.

*Table 649. Table References*

Links
<a href="http://www.rsaconference.com/writable/presentations/file_upload/anf-t07b-the-art-of-attribution-identifying-and-pursuing-your-cyber-adversaries_final.pdf">http://www.rsaconference.com/writable/presentations/file_upload/anf-t07b-the-art-of-attribution-identifying-and-pursuing-your-cyber-adversaries_final.pdf</a>

## Keyhole Panda

## Wet Panda

## Foxy Panda

Adversary group targeting telecommunication and technology organizations.

## Predator Panda

## Union Panda

## Spicy Panda

## Eloquent Panda

## 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 since 2012, 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 650. Table References*

Links
<a href="http://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf">http://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf</a>

## 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 651. Table References*

Links
<a href="https://www.fireeye.com/blog/threat-research/2015/06/operation-clandestine-wolf-adobe-flash-zero-day.html">https://www.fireeye.com/blog/threat-research/2015/06/operation-clandestine-wolf-adobe-flash-zero-day.html</a>
<a href="http://www.symantec.com/connect/blogs/buckeye-cyberespionage-group-shifts-gaze-us-hong-kong">http://www.symantec.com/connect/blogs/buckeye-cyberespionage-group-shifts-gaze-us-hong-kong</a>



# 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

Table 652. Table References

Links
<a href="https://securelist.com/blog/research/71713/darkhotels-attacks-in-2015/">https://securelist.com/blog/research/71713/darkhotels-attacks-in-2015/</a>
<a href="https://blogs.technet.microsoft.com/mmpc/2016/06/09/reverse-engineering-dubnium-2">https://blogs.technet.microsoft.com/mmpc/2016/06/09/reverse-engineering-dubnium-2</a>

# 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
- Crimson Iron
- APT12
- APT 12

Table 653. Table References

Links
<a href="http://www.crowdstrike.com/blog/whois-numbered-panda/">http://www.crowdstrike.com/blog/whois-numbered-panda/</a>

# APT 16

Table 654. Table References

Links
-------

## 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 655. Table References*

Links
<a href="http://www.fireeye.com/blog/technical/cyber-exploits/2013/09/operation-deputydog-zero-day-cve-2013-3893-attack-against-japanese-targets.html">http://www.fireeye.com/blog/technical/cyber-exploits/2013/09/operation-deputydog-zero-day-cve-2013-3893-attack-against-japanese-targets.html</a>
<a href="http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/hidden_lynx.pdf">http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/hidden_lynx.pdf</a>

## 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
- APT18

*Table 656. Table References*

Links
-------

## 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 have set 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 657. Table References*

Links
<a href="http://researchcenter.paloaltonetworks.com/2016/11/unit42-tropic-trooper-targets-taiwanese-government-and-fossil-fuel-provider-with-poison-ivy/">http://researchcenter.paloaltonetworks.com/2016/11/unit42-tropic-trooper-targets-taiwanese-government-and-fossil-fuel-provider-with-poison-ivy/</a>
<a href="http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-tropic-trooper.pdf">http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-tropic-trooper.pdf</a>

## 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

*Table 658. Table References*

Links
<a href="http://securelist.com/blog/research/57585/winnti-faq-more-than-just-a-game/">http://securelist.com/blog/research/57585/winnti-faq-more-than-just-a-game/</a>
<a href="http://williamshowalter.com/a-universal-windows-bootkit/">http://williamshowalter.com/a-universal-windows-bootkit/</a>
<a href="https://blogs.technet.microsoft.com/mmpc/2017/01/25/detecting-threat-actors-in-recent-german-industrial-attacks-with-windows-defender-atp">https://blogs.technet.microsoft.com/mmpc/2017/01/25/detecting-threat-actors-in-recent-german-industrial-attacks-with-windows-defender-atp</a>

## 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 659. Table References

Links
<a href="http://cybercampaigns.net/wp-content/uploads/2013/06/Deep-Panda.pdf">http://cybercampaigns.net/wp-content/uploads/2013/06/Deep-Panda.pdf</a>
<a href="http://www.rsaconference.com/writable/presentations/file_upload/anf-t07b-the-art-of-attribution-identifying-and-pursuing-your-cyber-adversaries_final.pdf">http://www.rsaconference.com/writable/presentations/file_upload/anf-t07b-the-art-of-attribution-identifying-and-pursuing-your-cyber-adversaries_final.pdf</a>

## 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
- Override Panda
- Camerashy
- APT.Naikon

Table 660. 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 661. Table References*

Links

<https://securelist.com/blog/research/70726/the-spring-dragon-apt/>

## Lotus Panda

Lotus Panda is also known as:

- Elise

## Hurricane Panda

*Table 662. 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
- HIPPOTeam
- APT27
- Operation Iron Tiger

Table 663. Table References

Links
<a href="http://www.secureworks.com/cyber-threat-intelligence/threats/threat-group-3390-targets-organizations-for-cyberespionage/">http://www.secureworks.com/cyber-threat-intelligence/threats/threat-group-3390-targets-organizations-for-cyberespionage/</a>
<a href="http://www.scmagazineuk.com/iran-and-russia-blamed-for-state-sponsored-espionage/article/330401/">http://www.scmagazineuk.com/iran-and-russia-blamed-for-state-sponsored-espionage/article/330401/</a>

## Stone Panda

Stone Panda is also known as:

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

Table 664. Table References

Links
<a href="http://researchcenter.paloaltonetworks.com/2017/02/unit42-menupass-returns-new-malware-new-attacks-japanese-academics-organizations/">http://researchcenter.paloaltonetworks.com/2017/02/unit42-menupass-returns-new-malware-new-attacks-japanese-academics-organizations/</a>

## Nightshade Panda

Nightshade Panda is also known as:

- APT 9
- Flowerlady/Flowershow
- Flowerlady
- Flowershow

Table 665. Table References

Links
<a href="https://otx.alienvault.com/pulse/55bbc68e67db8c2d547ae393/">https://otx.alienvault.com/pulse/55bbc68e67db8c2d547ae393/</a>

## Hellsing

Hellsing is also known as:

- Goblin Panda
- Cycldek

Table 666. Table References

Links

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

## Night Dragon

Table 667. 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
- Social Network Team

Table 668. Table References

Links

<https://www.fireeye.com/blog/threat-research/2014/09/forced-to-adapt-xslcmd-backdoor-now-on-os-x.html>

## Anchor Panda

PLA Navy

Anchor Panda is also known as:

- APT14
- APT 14
- QAZTeam
- ALUMINUM

Table 669. Table References

Links
<a href="http://www.crowdstrike.com/blog/whois-anchor-panda/">http://www.crowdstrike.com/blog/whois-anchor-panda/</a>

## NetTraveler

NetTraveler is also known as:

- APT 21

Table 670. Table References

Links
<a href="https://securelist.com/blog/research/35936/nettraveler-is-running-red-star-apt-attacks-compromise-high-profile-victims/">https://securelist.com/blog/research/35936/nettraveler-is-running-red-star-apt-attacks-compromise-high-profile-victims/</a>

## 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 671. Table References

Links
<a href="https://securelist.com/blog/research/57331/the-icefog-apt-a-tale-of-cloak-and-three-daggers/">https://securelist.com/blog/research/57331/the-icefog-apt-a-tale-of-cloak-and-three-daggers/</a>

## 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 672. Table References

Links
<a href="http://blog.airbuscybersecurity.com/post/2014/07/The-Eye-of-the-Tiger2">http://blog.airbuscybersecurity.com/post/2014/07/The-Eye-of-the-Tiger2</a>



# Roaming Tiger

Table 673. 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 674. 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
- Getkys
- SykipotGroup
- Wkysol

Table 675. Table References

Links

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

# Impersonating Panda

## Violin Panda

Violin Panda is also known as:

- APT20
- APT 20
- TH3Bug

Table 676. Table References

Links
<a href="http://researchcenter.paloaltonetworks.com/2014/09/recent-watering-hole-attacks-attributed-apt-group-th3bug-using-poison-ivy/">http://researchcenter.paloaltonetworks.com/2014/09/recent-watering-hole-attacks-attributed-apt-group-th3bug-using-poison-ivy/</a>

## Toxic Panda

A group targeting dissident groups in China and at the boundaries.

Table 677. Table References

Links
<a href="http://www.rsaconference.com/writable/presentations/file_upload/anf-t07b-the-art-of-attribution-identifying-and-pursuing-your-cyber-adversaries_final.pdf">http://www.rsaconference.com/writable/presentations/file_upload/anf-t07b-the-art-of-attribution-identifying-and-pursuing-your-cyber-adversaries_final.pdf</a>

## 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 678. Table References

Links
<a href="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/2013/10/know-your-enemy-tracking-a-rapidly-evolving-apt-actor.html</a>
<a href="https://www.fireeye.com/blog/threat-research/2015/11/china-based-threat.html">https://www.fireeye.com/blog/threat-research/2015/11/china-based-threat.html</a>

# Pirate Panda

Pirate Panda is also known as:

- APT23
- KeyBoy

Table 679. Table References

Links
<a href="https://community.rapid7.com/community/infosec/blog/2013/06/07/keyboy-targeted-attacks-against-vietnam-and-india">https://community.rapid7.com/community/infosec/blog/2013/06/07/keyboy-targeted-attacks-against-vietnam-and-india</a>

# 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 680. Table References

Links
<a href="https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-operation-saffron-rose.pdf">https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-operation-saffron-rose.pdf</a>

# 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 681. Table References

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

## 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
- Group 83
- Newsbeef

Table 682. Table References

Links
<a href="https://en.wikipedia.org/wiki/Operation_Newscaster">https://en.wikipedia.org/wiki/Operation_Newscaster</a>

## 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 683. Table References

Links
<a href="http://www.scmagazineuk.com/iran-and-russia-blamed-for-state-sponsored-espionage/article/330401/">http://www.scmagazineuk.com/iran-and-russia-blamed-for-state-sponsored-espionage/article/330401/</a>

## 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

Table 684. Table References

Links
<a href="https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-woolen-goldfish-when-kittens-go-phishing">https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-woolen-goldfish-when-kittens-go-phishing</a>
<a href="https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-spy-kittens-are-back.pdf">https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-spy-kittens-are-back.pdf</a>
<a href="http://www.clearskysec.com/thamar-reservoir/">http://www.clearskysec.com/thamar-reservoir/</a>
<a href="https://citizenlab.org/2015/08/iran_two_factor_phishing/">https://citizenlab.org/2015/08/iran_two_factor_phishing/</a>
<a href="https://blog.checkpoint.com/wp-content/uploads/2015/11/rocket-kitten-report.pdf">https://blog.checkpoint.com/wp-content/uploads/2015/11/rocket-kitten-report.pdf</a>

## 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

Table 685. Table References

Links
<a href="http://cdn2.hubspot.net/hubfs/270968/assets/Cleaver/Cylance_Operation_Cleaver_Report.pdf">http://cdn2.hubspot.net/hubfs/270968/assets/Cleaver/Cylance_Operation_Cleaver_Report.pdf</a>

## 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

*Table 686. Table References*

Links
<a href="https://en.wikipedia.org/wiki/Sofacy_Group">https://en.wikipedia.org/wiki/Sofacy_Group</a>

## 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

*Table 687. Table References*

Links
<a href="https://labsblog.f-secure.com/2015/09/17/the-dukes-7-years-of-russian-cyber-espionage/">https://labsblog.f-secure.com/2015/09/17/the-dukes-7-years-of-russian-cyber-espionage/</a>

## 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 Symantec's 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 688. Table References

Links
<a href="https://www.first.org/resources/papers/tbilisi2014/turla-operations_and_development.pdf">https://www.first.org/resources/papers/tbilisi2014/turla-operations_and_development.pdf</a>
<a href="https://www.circl.lu/pub/tr-25/">https://www.circl.lu/pub/tr-25/</a>
<a href="https://www.theguardian.com/technology/2014/aug/07/turla-hackers-spying-governments-researcher-kaspersky-symantec">https://www.theguardian.com/technology/2014/aug/07/turla-hackers-spying-governments-researcher-kaspersky-symantec</a>

## 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 689. Table References

Links
<a href="http://www.scmagazineuk.com/iran-and-russia-blamed-for-state-sponsored-espionage/article/330401/">http://www.scmagazineuk.com/iran-and-russia-blamed-for-state-sponsored-espionage/article/330401/</a>

## Sandworm

Sandworm is also known as:

- Sandworm Team
- Black Energy
- BlackEnergy
- Quedagh
- Voodoo Bear

Table 690. Table References

Links
<a href="http://www.isightpartners.com/2014/10/cve-2014-4114/">http://www.isightpartners.com/2014/10/cve-2014-4114/</a>

## 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.

Table 691. Table References

Links
<a href="http://www.welivesecurity.com/2016/12/13/rise-telebots-analyzing-disruptive-killdisk-attacks/">http://www.welivesecurity.com/2016/12/13/rise-telebots-analyzing-disruptive-killdisk-attacks/</a>

## Anunak

Groups targeting financial organizations or people with significant financial assets.

Anunak is also known as:

- Carbanak
- Carbon Spider

Table 692. Table References

Links

<https://en.wikipedia.org/wiki/Carbanak>

## TeamSpy Crew

TeamSpy Crew is also known as:

- TeamSpy
- Team Bear
- Berserk Bear

Table 693. Table References

Links

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

## BuhTrap

Table 694. 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 695. Table References

Links
<a href="http://www.rsaconference.com/writable/presentations/file_upload/anf-t07b-the-art-of-attribution-identifying-and-pursuing-your-cyber-adversaries_final.pdf">http://www.rsaconference.com/writable/presentations/file_upload/anf-t07b-the-art-of-attribution-identifying-and-pursuing-your-cyber-adversaries_final.pdf</a>

# Silent Chollima

Silent Chollima is also known as:

- OperationTroy
- Guardian of Peace
- GOP
- WHOis Team

Table 696. Table References

Links
<a href="http://www.rsaconference.com/writable/presentations/file_upload/anf-t07b-the-art-of-attribution-identifying-and-pursuing-your-cyber-adversaries_final.pdf">http://www.rsaconference.com/writable/presentations/file_upload/anf-t07b-the-art-of-attribution-identifying-and-pursuing-your-cyber-adversaries_final.pdf</a>

# 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
- Hidden Cobra

Table 697. Table References

Links
<a href="https://threatpost.com/operation-blockbuster-coalition-ties-destructive-attacks-to-lazarus-group/116422/">https://threatpost.com/operation-blockbuster-coalition-ties-destructive-attacks-to-lazarus-group/116422/</a>
<a href="https://www.us-cert.gov/ncas/alerts/TA17-164A">https://www.us-cert.gov/ncas/alerts/TA17-164A</a>

## Viceroy Tiger

Viceroy Tiger is also known as:

- Appin
- OperationHangover

*Table 698. Table References*

Links
<a href="http://enterprise-manage.norman.c.bitbit.net/resources/files/Unveiling_an_Indian_Cyberattack_Infrastructure.pdf">http://enterprise-manage.norman.c.bitbit.net/resources/files/Unveiling_an_Indian_Cyberattack_Infrastructure.pdf</a>

## Pizzo Spider

Pizzo Spider is also known as:

- DD4BC
- Ambiorx

## Corsair Jackal

Corsair Jackal is also known as:

- TunisianCyberArmy

## 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 699. Table References*

Links
<a href="https://securelist.com/blog/research/69114/animals-in-the-apt-farm/">https://securelist.com/blog/research/69114/animals-in-the-apt-farm/</a>

## 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 700. Table References

Links
<a href="https://en.wikipedia.org/wiki/Syrian_Electronic_Army">https://en.wikipedia.org/wiki/Syrian_Electronic_Army</a>

## 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 701. Table References

Links
<a href="http://documents.trendmicro.com/assets/pdf/Indian-military-personnel-targeted-by-information-theft-campaign-cmajor.pdf">http://documents.trendmicro.com/assets/pdf/Indian-military-personnel-targeted-by-information-theft-campaign-cmajor.pdf</a>

## Stealth Falcon

Group targeting Emirati journalists, activists, and dissidents.

Stealth Falcon is also known as:

- FruityArmor

Table 702. Table References

Links
<a href="https://citizenlab.org/2016/05/stealth-falcon/">https://citizenlab.org/2016/05/stealth-falcon/</a>

## 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 703. Table References*

Links
<a href="https://securelist.com/blog/research/75082/cve-2016-4171-adobe-flash-zero-day-used-in-targeted-attacks/">https://securelist.com/blog/research/75082/cve-2016-4171-adobe-flash-zero-day-used-in-targeted-attacks/</a>

## 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 704. Table References*

Links
<a href="http://download.bitdefender.com/resources/files/News/CaseStudies/study/115/Bitdefender-Whitepaper-PAC-A4-en-EN1.pdf">http://download.bitdefender.com/resources/files/News/CaseStudies/study/115/Bitdefender-Whitepaper-PAC-A4-en-EN1.pdf</a>

## 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 705. Table References*

Links
<a href="http://blog.checkpoint.com/wp-content/uploads/2016/07/HummingBad-Research-report_FINAL-62916.pdf">http://blog.checkpoint.com/wp-content/uploads/2016/07/HummingBad-Research-report_FINAL-62916.pdf</a>

## 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 706. Table References

Links
<a href="https://securelist.com/blog/research/75328/the-dropping-elephant-actor/">https://securelist.com/blog/research/75328/the-dropping-elephant-actor/</a>
<a href="http://www.symantec.com/connect/blogs/patchwork-cyberespionage-group-expands-targets-governments-wide-range-industries">http://www.symantec.com/connect/blogs/patchwork-cyberespionage-group-expands-targets-governments-wide-range-industries</a>

## 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 707. Table References

Links
<a href="https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf">https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf</a>

## 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 708. Table References

Links
<a href="https://attack.mitre.org/wiki/Groups">https://attack.mitre.org/wiki/Groups</a>
<a href="http://researchcenter.paloaltonetworks.com/2016/01/scarlet-mimic-years-long-espionage-targets-minority-activists/">http://researchcenter.paloaltonetworks.com/2016/01/scarlet-mimic-years-long-espionage-targets-minority-activists/</a>

## 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 709. Table References

Links
<a href="https://securelist.com/blog/research/73673/poseidon-group-a-targeted-attack-boutique-specializing-in-global-cyber-espionage/">https://securelist.com/blog/research/73673/poseidon-group-a-targeted-attack-boutique-specializing-in-global-cyber-espionage/</a>
<a href="https://attack.mitre.org/wiki/Groups">https://attack.mitre.org/wiki/Groups</a>

## 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 710. Table References

Links
<a href="https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-quantum-entanglement.pdf">https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-quantum-entanglement.pdf</a>
<a href="https://attack.mitre.org/wiki/Groups">https://attack.mitre.org/wiki/Groups</a>

## 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 711. Table References

Links
<a href="http://www.secureworks.com/cyber-threat-intelligence/threats/threat-group-3390-targets-organizations-for-cyberespionage/">http://www.secureworks.com/cyber-threat-intelligence/threats/threat-group-3390-targets-organizations-for-cyberespionage/</a>
<a href="https://attack.mitre.org">https://attack.mitre.org</a>

## 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 712. Table References*

Links
<a href="https://securelist.com/analysis/publications/75533/faq-the-projectsauron-apt/">https://securelist.com/analysis/publications/75533/faq-the-projectsauron-apt/</a>

## 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 713. Table References*

Links
<a href="https://www2.fireeye.com/rs/fireeye/images/rpt-apt30.pdf">https://www2.fireeye.com/rs/fireeye/images/rpt-apt30.pdf</a>
<a href="https://attack.mitre.org/wiki/Group/G0013">https://attack.mitre.org/wiki/Group/G0013</a>

## 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 714. 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 715. Table References*

Links

<http://www.symantec.com/connect/blogs/suckfly-revealing-secret-life-your-code-signing-certificates>

## FIN6

FIN is a group targeting financial assets including assets able to do financial transaction including PoS.

*Table 716. 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 717. Table References*

Links

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

## OilRig

Iranian threat agent OilRig has been targeting multiple organisations in Israel and other countries in the Middle East since the end of 2015.

*Table 718. Table References*

## Links

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

## 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 719. 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 720. Table References*

## Links

<https://blogs.technet.microsoft.com/mmperc/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
- Operation Molerats
- Extreme Jackal
- Moonlight

Table 721. Table References

Links
<a href="https://www.fireeye.com/blog/threat-research/2013/08/operation-molerats-middle-east-cyber-attacks-using-poison-ivy.html">https://www.fireeye.com/blog/threat-research/2013/08/operation-molerats-middle-east-cyber-attacks-using-poison-ivy.html</a>
<a href="http://blog.vectranetworks.com/blog/moonlight-middle-east-targeted-attacks">http://blog.vectranetworks.com/blog/moonlight-middle-east-targeted-attacks</a>

## 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 722. Table References

Links
<a href="https://blogs.technet.microsoft.com/mmpc/2016/12/14/twin-zero-day-attacks-promethium-and-neodymium-target-individuals-in-europe/">https://blogs.technet.microsoft.com/mmpc/2016/12/14/twin-zero-day-attacks-promethium-and-neodymium-target-individuals-in-europe/</a>
<a href="https://www.virusbulletin.com/conference/vb2016/abstracts/last-minute-paper-strongpity-waterhole-attacks-targeting-italian-and-belgian-encryption-users">https://www.virusbulletin.com/conference/vb2016/abstracts/last-minute-paper-strongpity-waterhole-attacks-targeting-italian-and-belgian-encryption-users</a>

## 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 723. Table References

Links
<a href="https://blogs.technet.microsoft.com/mmpc/2016/12/14/twin-zero-day-attacks-promethium-and-neodymium-target-individuals-in-europe/">https://blogs.technet.microsoft.com/mmpc/2016/12/14/twin-zero-day-attacks-promethium-and-neodymium-target-individuals-in-europe/</a>

## 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 724. Table References

Links
<a href="https://citizenlab.org/2015/12/packrat-report/">https://citizenlab.org/2015/12/packrat-report/</a>

## 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 725. Table References

Links
<a href="https://www.symantec.com/connect/blogs/iran-based-attackers-use-back-door-threats-spy-middle-eastern-targets">https://www.symantec.com/connect/blogs/iran-based-attackers-use-back-door-threats-spy-middle-eastern-targets</a>

## 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 726. Table References

Links
<a href="https://www.symantec.com/connect/blogs/iran-based-attackers-use-back-door-threats-spy-middle-eastern-targets">https://www.symantec.com/connect/blogs/iran-based-attackers-use-back-door-threats-spy-middle-eastern-targets</a>

## 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 727. Table References

Links
<a href="https://blog.cylance.com/digitally-signed-malware-targeting-gaming-companies">https://blog.cylance.com/digitally-signed-malware-targeting-gaming-companies</a>

## 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

*Table 728. Table References*

Links
<a href="https://en.wikipedia.org/wiki/Equation_Group">https://en.wikipedia.org/wiki/Equation_Group</a>

## 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 729. Table References*

Links
<a href="https://www.symantec.com/connect/blogs/greenbug-cyberespionage-group-targeting-middle-east-possible-links-shamoon">https://www.symantec.com/connect/blogs/greenbug-cyberespionage-group-targeting-middle-east-possible-links-shamoon</a>

## 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 730. 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

*Table 731. Table References*

Links

<http://www.darkreading.com/endpoint/chinese-cyberspies-pivot-to-russia-in-wake-of-obama-xi-pact/d/d-id/1324242>

## Barium

Barium is one of the groups using Winnti.

*Table 732. Table References*

Links

<https://blogs.technet.microsoft.com/mmpc/2017/01/25/detecting-threat-actors-in-recent-german-industrial-attacks-with-windows-defender-atp>

## Infy

Infy is a group of suspected Iranian origin.

Infy is also known as:

- Operation Mermaid

*Table 733. Table References*

Links

<https://www.blackhat.com/docs/us-16/materials/us-16-Guarnieri-Iran-And-The-Soft-War-For-Internet-Dominance-wp.pdf>

## Sima

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

*Table 734. Table References*

Links



<https://www.blackhat.com/docs/us-16/materials/us-16-Guarnieri-Iran-And-The-Soft-War-For-Internet-Dominance-wp.pdf>

## Blue Termite

Blue Termite is a group of suspected Chinese origin active in Japan.

Blue Termite is also known as:

- Cloudy Omega

*Table 735. Table References*

Links

<https://securelist.com/blog/research/71876/new-activity-of-the-blue-termite-apt/>

## Groundbait

Groundbait is a group targeting anti-government separatists in the self-declared Donetsk and Luhansk People's Republics.

*Table 736. 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 737. Table References*

Links

<https://www.symantec.com/connect/blogs/longhorn-tools-used-cyberespionage-group-linked-vault-7>

## 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 738. Table References

Links
<a href="https://www.f-secure.com/documents/996508/1030745/callisto-group">https://www.f-secure.com/documents/996508/1030745/callisto-group</a>

## 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
- APT-32
- APT 32

Table 739. Table References

Links
<a href="https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html">https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html</a>

## 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 740. Table References

Links
<a href="https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/silverterrier-next-evolution-in-nigerian-cybercrime.pdf">https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/silverterrier-next-evolution-in-nigerian-cybercrime.pdf</a>

## 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 741. Table References

Links
<a href="https://www.symantec.com/connect/blogs/butterfly-profiting-high-level-corporate-attacks">https://www.symantec.com/connect/blogs/butterfly-profiting-high-level-corporate-attacks</a>
<a href="https://securelist.com/71275/wild-neutron-economic-espionage-threat-actor-returns-with-new-tricks/">https://securelist.com/71275/wild-neutron-economic-espionage-threat-actor-returns-with-new-tricks/</a>
<a href="https://research.kudelskisecurity.com/2015/11/05/sphinx-moth-expanding-our-knowledge-of-the-wild-neutron-morpho-apt/">https://research.kudelskisecurity.com/2015/11/05/sphinx-moth-expanding-our-knowledge-of-the-wild-neutron-morpho-apt/</a>

## 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 742. Table References

Links
<a href="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">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</a>
<a href="https://blogs.technet.microsoft.com/mmpc/2016/04/26/digging-deep-for-platinum/">https://blogs.technet.microsoft.com/mmpc/2016/04/26/digging-deep-for-platinum/</a>

## 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.

Table 743. Table References

Links
-------

<https://dragos.com/blog/crashoverride/CrashOverride-01.pdf>

[https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32\\_Industroyer.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 744. Table References

Links
<a href="https://www.fireeye.com/blog/threat-research/2016/05/windows-zero-day-payment-cards.html">https://www.fireeye.com/blog/threat-research/2016/05/windows-zero-day-payment-cards.html</a>
<a href="https://www2.fireeye.com/WBNR-Know-Your-Enemy-UNC622-Spear-Phishing.html">https://www2.fireeye.com/WBNR-Know-Your-Enemy-UNC622-Spear-Phishing.html</a>
<a href="https://www.root9b.com/sites/default/files/whitepapers/PoS%20Malware%20ShellTea%20PoSlurp.pdf">https://www.root9b.com/sites/default/files/whitepapers/PoS%20Malware%20ShellTea%20PoSlurp.pdf</a>
<a href="http://files.shareholder.com/downloads/AMDA-254Q5F/0x0x938351/665BA6A3-9573-486C-B96F-80FA35759E8C/FEYE_rpt-mtrends-2017_FINAL2.pdf">http://files.shareholder.com/downloads/AMDA-254Q5F/0x0x938351/665BA6A3-9573-486C-B96F-80FA35759E8C/FEYE_rpt-mtrends-2017_FINAL2.pdf</a>

## 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 Vandeplass

## Tinba

Banking Malware

Tinba is also known as:

- Hunter
- Zusy
- TinyBanker

Table 745. Table References

Links
<a href="https://thehackernews.com/search/label/Zusy%20Malware">https://thehackernews.com/search/label/Zusy%20Malware</a>
<a href="https://blog.trendmicro.com/trendlabs-security-intelligence/the-tinbatinybanker-malware/">https://blog.trendmicro.com/trendlabs-security-intelligence/the-tinbatinybanker-malware/</a>

# PlugX

Malware

PlugX is also known as:

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

Table 746. Table References

Links
<a href="https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/112/pulling-the-plug-on-plugx">https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/112/pulling-the-plug-on-plugx</a>

# MSUpdater

Trojan (RAT) linked to current targeted attacks and others dating back to at least early 2009

Table 747. Table References

Links
<a href="https://www.zscaler.com/pdf/whitepapers/msupdater_trojan_whitepaper.pdf">https://www.zscaler.com/pdf/whitepapers/msupdater_trojan_whitepaper.pdf</a>

# Lazagne

A password stealing tool regularly used by attackers

Table 748. Table References

Links
<a href="https://github.com/AlessandroZ/LaZagne">https://github.com/AlessandroZ/LaZagne</a>

# 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 749. Table References

Links
<a href="https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-poison-ivy.pdf">https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-poison-ivy.pdf</a>
<a href="https://www.f-secure.com/v-descs/backdoor_w32_poisonivy.shtml">https://www.f-secure.com/v-descs/backdoor_w32_poisonivy.shtml</a>

## 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 750. Table References

Links
<a href="http://researchcenter.paloaltonetworks.com/2016/04/unit42-new-poison-ivy-rat-variant-targets-hong-kong-pro-democracy-activists/">http://researchcenter.paloaltonetworks.com/2016/04/unit42-new-poison-ivy-rat-variant-targets-hong-kong-pro-democracy-activists/</a>

## Torn RAT

Torn RAT is also known as:

- Anchor Panda

Table 751. Table References

Links
<a href="https://www.crowdstrike.com/blog/whois-anchor-panda/">https://www.crowdstrike.com/blog/whois-anchor-panda/</a>

## OzoneRAT

OzoneRAT is also known as:

- Ozone RAT
- ozonercp

Table 752. Table References

Links
<a href="https://blog.fortinet.com/2016/08/29/german-speakers-targeted-by-spam-leading-to-ozone-rat">https://blog.fortinet.com/2016/08/29/german-speakers-targeted-by-spam-leading-to-ozone-rat</a>

## 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 753. Table References

Links
<a href="https://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Backdoor%3aWin32%2fZegost.BW">https://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Backdoor%3aWin32%2fZegost.BW</a>

## 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 754. Table References

Links
<a href="http://thehackernews.com/2015/08/elise-malware-hacking.html">http://thehackernews.com/2015/08/elise-malware-hacking.html</a>

## 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 755. Table References

Links
<a href="http://www.symantec.com/connect/blogs/new-reconnaissance-threat-trojanlaziok-targets-energy-sector">http://www.symantec.com/connect/blogs/new-reconnaissance-threat-trojanlaziok-targets-energy-sector</a>

## Slempo

Android-based malware

Slempo is also known as:

- GM-Bot
- SlemBunk
- Bankosy
- Acecard

Table 756. Table References

Links
<a href="https://securityintelligence.com/android-malware-about-to-get-worse-gm-bot-source-code-leaked/">https://securityintelligence.com/android-malware-about-to-get-worse-gm-bot-source-code-leaked/</a>

## 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 757. Table References

Links
<a href="http://researchcenter.paloaltonetworks.com/2016/04/unit42-python-based-pwobot-targets-european-organizations/">http://researchcenter.paloaltonetworks.com/2016/04/unit42-python-based-pwobot-targets-european-organizations/</a>

## 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 758. Table References

Links
<a href="http://blog.trendmicro.com/trendlabs-security-intelligence/lost-door-rat-accessible-customizable-attack-tool/">http://blog.trendmicro.com/trendlabs-security-intelligence/lost-door-rat-accessible-customizable-attack-tool/</a>

## njRAT

njRAT is also known as:



- Bladabindi
- Jorik

Table 759. Table References

Links
<a href="http://www.fidelisecurity.com/files/files/FTA_1009-njRAT_Uncovered_rev2.pdf">http://www.fidelisecurity.com/files/files/FTA_1009-njRAT_Uncovered_rev2.pdf</a>
<a href="https://github.com/kevthehermit/RATDecoders/blob/master/yaraRules/njRat.yar">https://github.com/kevthehermit/RATDecoders/blob/master/yaraRules/njRat.yar</a>

## NanoCoreRAT

NanoCoreRAT is also known as:

- NanoCore
- Nancrat
- Zurten
- Atros2.CKPN

Table 760. Table References

Links
<a href="http://www.symantec.com/connect/blogs/nanocore-another-rat-tries-make-it-out-gutter">http://www.symantec.com/connect/blogs/nanocore-another-rat-tries-make-it-out-gutter</a>
<a href="https://nanocore.io/">https://nanocore.io/</a>

## Sakula

Sakula is also known as:

- Sakurel

Table 761. Table References

Links
<a href="https://www.secureworks.com/research/sakula-malware-family">https://www.secureworks.com/research/sakula-malware-family</a>

## Hi-ZOR

Table 762. Table References

Links
<a href="http://www.threatgeek.com/2016/01/introducing-hi-zor-rat.html">http://www.threatgeek.com/2016/01/introducing-hi-zor-rat.html</a>

## Derusbi

Derusbi is also known as:

- TROJ\_DLLSERV.BE

Table 763. Table References

Links
<a href="http://www.novetta.com/wp-content/uploads/2014/11/Derusbi.pdf">http://www.novetta.com/wp-content/uploads/2014/11/Derusbi.pdf</a>
<a href="https://www.rsaconference.com/writable/presentations/file_upload/hta-w02-dissecting-derusbi.pdf">https://www.rsaconference.com/writable/presentations/file_upload/hta-w02-dissecting-derusbi.pdf</a>

## EvilGrab

EvilGrab is also known as:

- BKDR\_HGDER
- BKDR\_EVILOGE
- BKDR\_NVICM
- Wmonder

Table 764. Table References

Links
<a href="http://blog.trendmicro.com/trendlabs-security-intelligence/evilgrab-malware-family-used-in-targeted-attacks-in-asia/">http://blog.trendmicro.com/trendlabs-security-intelligence/evilgrab-malware-family-used-in-targeted-attacks-in-asia/</a>
<a href="http://researchcenter.paloaltonetworks.com/2015/06/evilgrab-delivered-by-watering-hole-attack-on-president-of-myanmars-website/">http://researchcenter.paloaltonetworks.com/2015/06/evilgrab-delivered-by-watering-hole-attack-on-president-of-myanmars-website/</a>

## Trojan.Naid

Trojan.Naid is also known as:

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

Table 765. Table References

Links
<a href="https://www.symantec.com/connect/blogs/cve-2012-1875-exploited-wild-part-1-trojannaid">https://www.symantec.com/connect/blogs/cve-2012-1875-exploited-wild-part-1-trojannaid</a>
<a href="http://telussecuritylabs.com/threats/show/TSL20120614-05">http://telussecuritylabs.com/threats/show/TSL20120614-05</a>

## Moudoor

Backdoor.Moudoor, a customized version of Gh0st RAT

Moudoor is also known as:

- SCAR
- KillProc.14145

Table 766. Table References

Links
<a href="http://www.darkreading.com/attacks-breaches/elite-chinese-cyberspy-group-behind-bit9-hack/d/d-id/1140495">http://www.darkreading.com/attacks-breaches/elite-chinese-cyberspy-group-behind-bit9-hack/d/d-id/1140495</a>
<a href="https://securityledger.com/2013/09/apt-for-hire-symantec-outs-hidden-lynx-hacking-crew/">https://securityledger.com/2013/09/apt-for-hire-symantec-outs-hidden-lynx-hacking-crew/</a>

## 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 767. Table References

Links
<a href="https://securelist.com/blog/incidents/57455/nettraveler-is-back-the-red-star-apt-returns-with-new-tricks/">https://securelist.com/blog/incidents/57455/nettraveler-is-back-the-red-star-apt-returns-with-new-tricks/</a>

## 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 768. Table References

Links
<a href="https://securelist.com/blog/incidents/57455/nettraveler-is-back-the-red-star-apt-returns-with-new-tricks/">https://securelist.com/blog/incidents/57455/nettraveler-is-back-the-red-star-apt-returns-with-new-tricks/</a>

# Mimikatz

Ease Credential stealh and replay, A little tool to play with Windows security.

Mimikatz is also known as:

- Mikatz

*Table 769. Table References*

Links
<a href="https://github.com/gentilkiwi/mimikatz">https://github.com/gentilkiwi/mimikatz</a>

# WEBC2

Backdoor attributed to APT1

*Table 770. Table References*

Links
<a href="https://github.com/gnaegle/cse4990-practical3">https://github.com/gnaegle/cse4990-practical3</a>
<a href="https://www.securestate.com/blog/2013/02/20/apt-if-it-aint-broke">https://www.securestate.com/blog/2013/02/20/apt-if-it-aint-broke</a>

# 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 771. Table References*

Links
<a href="http://www.symantec.com/connect/blogs/buckeye-cyberespionage-group-shifts-gaze-us-hong-kong">http://www.symantec.com/connect/blogs/buckeye-cyberespionage-group-shifts-gaze-us-hong-kong</a>

# 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 772. Table References*

Links
-------

## 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 773. Table References

Links
<a href="https://www2.fireeye.com/WEB-2015RPTAPT30.html">https://www2.fireeye.com/WEB-2015RPTAPT30.html</a>
<a href="https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-southeast-asia-threat-landscape.pdf">https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-southeast-asia-threat-landscape.pdf</a>

## XSSControl

Backdoor user by the Naikon APT group

Table 774. Table References

Links
<a href="https://securelist.com/analysis/publications/69953/the-naikon-apt/">https://securelist.com/analysis/publications/69953/the-naikon-apt/</a>
<a href="https://kasperskycontenthub.com/securelist/files/2015/05/TheNaikonAPT-MsnMM.pdf">https://kasperskycontenthub.com/securelist/files/2015/05/TheNaikonAPT-MsnMM.pdf</a>

## 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 775. Table References

Links
<a href="https://attack.mitre.org/wiki/Software/S0034">https://attack.mitre.org/wiki/Software/S0034</a>
<a href="https://www2.fireeye.com/rs/fireeye/images/rpt-apt30.pdf">https://www2.fireeye.com/rs/fireeye/images/rpt-apt30.pdf</a>

## 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 776. Table References*

Links
<a href="https://blog.gdatasoftware.com/2015/01/23927-evolution-of-sophisticated-spyware-from-agent-btz-to-comrat">https://blog.gdatasoftware.com/2015/01/23927-evolution-of-sophisticated-spyware-from-agent-btz-to-comrat</a>

## 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 Tavidig and Epic Turla)

Wipbot is also known as:

- Tavidig
- Epic Turla
- WorldCupSec
- TadjMakhal

*Table 777. Table References*

Links
<a href="https://securelist.com/analysis/publications/65545/the-epic-turla-operation/">https://securelist.com/analysis/publications/65545/the-epic-turla-operation/</a>
<a href="https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/waterbug-attack-group.pdf">https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/waterbug-attack-group.pdf</a>

## Turla

Family of related sophisticated backdoor software - Name comes from Microsoft detection signature – anagram of Ultra (Ultra3 was a name of the fake driver).

Turla is also known as:

- Snake
- Uroburos
- Urouros

Table 778. Table References

Links
<a href="https://www.first.org/resources/papers/tbilisi2014/turla-operations_and_development.pdf">https://www.first.org/resources/papers/tbilisi2014/turla-operations_and_development.pdf</a>

## Winexe

## Dark Comet

RAT initially identified in 2011 and still actively used.

## Cadelspy

Cadelspy is also known as:

- WinSpy

## CMStar

Table 779. Table References

Links
<a href="http://researchcenter.paloaltonetworks.com/2016/03/digital-quartermaster-scenario-demonstrated-in-attacks-against-the-mongolian-government/">http://researchcenter.paloaltonetworks.com/2016/03/digital-quartermaster-scenario-demonstrated-in-attacks-against-the-mongolian-government/</a>

## DHS2015

DHS2015 is also known as:

- iRAT

Table 780. Table References

Links
<a href="https://securelist.com/files/2015/02/The-Desert-Falcons-targeted-attacks.pdf">https://securelist.com/files/2015/02/The-Desert-Falcons-targeted-attacks.pdf</a>

## 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 781. 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 782. 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 783. 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 784. 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 785. Table References

Links
<a href="https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf">https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf</a>

## EVILTOSS

backdoor used by apt28

EVILTOSS is also known as:

- Sedreco
- AZZY
- ADVSTORESHELL
- NETUI

Table 786. Table References

Links
<a href="https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf">https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf</a>

## GAMEFISH

backdoor

GAMEFISH is also known as:

- Sednit
- Seduploader
- JHUHUGIT
- Sofacy

Table 787. Table References

Links
<a href="https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf">https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf</a>

## SOURFACE

downloader - Older version of CORESHELL

SOURFACE is also known as:

- Sofacy

Table 788. Table References

Links
<a href="https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf">https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf</a>

## OLDBAIT

credential harvester

OLDBAIT is also known as:

- Sasfis
- BackDoor-FDU
- IEChecker

Table 789. Table References

Links
<a href="https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/troj_sasfis.tl">https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/troj_sasfis.tl</a>
<a href="https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf">https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf</a>

## CORESHELL

downloader - Newer version of SOURFACE

CORESHELL is also known as:

- Sofacy

Table 790. Table References

Links
<a href="https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf">https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf</a>

## Havex RAT

Havex RAT is also known as:

- Havex

## KjWorm

RAT initially written in VB.

Table 791. Table References

Links
-------

## 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 792. Table References

### Links

[https://en.wikipedia.org/wiki/Regin\\_\(malware\)](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 793. Table References

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

## T9000

Table 794. Table References

Links
<a href="http://researchcenter.paloaltonetworks.com/2016/02/t9000-advanced-modular-backdoor-uses-complex-anti-analysis-techniques/">http://researchcenter.paloaltonetworks.com/2016/02/t9000-advanced-modular-backdoor-uses-complex-anti-analysis-techniques/</a>

## T5000

T5000 is also known as:

- Plat1

Table 795. Table References

Links
<a href="http://www.cylance.com/techblog/Grand-Theft-Auto-Panda.shtml">http://www.cylance.com/techblog/Grand-Theft-Auto-Panda.shtml</a>

## Taidoor

Table 796. Table References

Links
<a href="http://www.symantec.com/connect/blogs/trojantaidoor-takes-aim-policy-think-tanks">http://www.symantec.com/connect/blogs/trojantaidoor-takes-aim-policy-think-tanks</a>

## Swisyn

Table 797. Table References

Links
<a href="http://labs.alienvault.com/labs/index.php/2013/latest-adobe-pdf-exploit-used-to-target-uyghur-and-tibetan-activists/">http://labs.alienvault.com/labs/index.php/2013/latest-adobe-pdf-exploit-used-to-target-uyghur-and-tibetan-activists/</a>

## Rekaf

Table 798. Table References

Links
<a href="https://www.proofpoint.com/us/exploring-bergard-old-malware-new-tricks">https://www.proofpoint.com/us/exploring-bergard-old-malware-new-tricks</a>

## Scieron

## SkeletonKey

Table 799. Table References

Links
<a href="http://www.secureworks.com/cyber-threat-intelligence/threats/skeleton-key-malware-analysis/">http://www.secureworks.com/cyber-threat-intelligence/threats/skeleton-key-malware-analysis/</a>

## Skipot

Table 800. Table References

Links
<a href="http://labs.alienvault.com/labs/index.php/2011/another-sykipot-sample-likely-targeting-us-federal-agencies/">http://labs.alienvault.com/labs/index.php/2011/another-sykipot-sample-likely-targeting-us-federal-agencies/</a>

## Spindest

Table 801. Table References

Links
<a href="http://www.threatconnect.com/news/threatconnect-enables-healthy-networking-biomed-life-sciences-industry/">http://www.threatconnect.com/news/threatconnect-enables-healthy-networking-biomed-life-sciences-industry/</a>

## Preshin

## Oficla

## PCClient RAT

Table 802. Table References

Links
<a href="http://researchcenter.paloaltonetworks.com/2014/10/new-indicators-compromise-apt-group-nitro-uncovered/">http://researchcenter.paloaltonetworks.com/2014/10/new-indicators-compromise-apt-group-nitro-uncovered/</a>

## Plexor

## Mongall

Table 803. Table References

Links
-------

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

## NeD Worm

*Table 804. Table References*

Links

<http://www.clearskysec.com/dustysky/>

## NewCT

*Table 805. Table References*

Links

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

## Nflog

*Table 806. Table References*

Links

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

## Janicab

*Table 807. 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 808. Table References*

Links

[http://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/butterfly-corporate-spies-out-for-financial-gain.pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/butterfly-corporate-spies-out-for-financial-gain.pdf)

# Jolob

Table 809. Table References

Links

[http://pwc.blogs.com/cyber\\_security\\_updates/2014/10/scanbox-framework-whos-affected-and-whos-using-it-1.html](http://pwc.blogs.com/cyber_security_updates/2014/10/scanbox-framework-whos-affected-and-whos-using-it-1.html)

# IsSpace

Table 810. 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 811. 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 812. Table References

Links

<http://www.secureworks.com/research/threats/htran/>

# HTTPBrowser

HTTPBrowser is also known as:

- TokenControl



Table 813. 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 814. Table References

Links

<https://www.circl.lu/pub/tr-13/>

## Aumlib

Aumlib is also known as:

- Yayih
- mswab
- Graftor

Table 815. Table References

Links

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

## CTRat

Table 816. 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 817. Table References

Links
<a href="http://www.symantec.com/connect/blogs/operation-cloudyomega-ichitaro-zero-day-and-ongoing-cyberespionage-campaign-targeting-japan">http://www.symantec.com/connect/blogs/operation-cloudyomega-ichitaro-zero-day-and-ongoing-cyberespionage-campaign-targeting-japan</a>

## Etumbot

Etumbot is also known as:

- Exploz
- Specfix
- RIPTIDE

Table 818. Table References

Links
<a href="http://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</a> [ <a href="http://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</a> ]

## Fexel

Fexel is also known as:

- Loneagent

## Fysbis

Table 819. Table References

Links
<a href="http://researchcenter.paloaltonetworks.com/2016/02/a-look-into-fysbis-sofacys-linux-backdoor/">http://researchcenter.paloaltonetworks.com/2016/02/a-look-into-fysbis-sofacys-linux-backdoor/</a>

## Hikit

Table 820. Table References

Links
<a href="https://blog.bit9.com/2013/02/25/bit9-security-incident-update/">https://blog.bit9.com/2013/02/25/bit9-security-incident-update/</a>

## Hancitor

Hancitor is also known as:

- Tordal
- Chanitor

- Pony

Table 821. Table References

Links

<https://www.proofpoint.com/us/threat-insight/post/hancitor-ruckguy-reappear>

## Ruckguy

Table 822. Table References

Links

<https://www.proofpoint.com/us/threat-insight/post/hancitor-ruckguy-reappear>

## HerHer Trojan

Table 823. Table References

Links

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

## Helminth backdoor

Table 824. Table References

Links

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

## HDRoot

Table 825. Table References

Links

<http://williamshowalter.com/a-universal-windows-bootkit/>

## IRONGATE

Table 826. Table References

Links

[https://www.fireeye.com/blog/threat-research/2016/06/irongate\\_ics\\_malware.html](https://www.fireeye.com/blog/threat-research/2016/06/irongate_ics_malware.html)

## ShimRAT

Table 827. Table References

Links
<a href="https://foxitsecurity.files.wordpress.com/2016/06/fox-it_mofang_threatreport_tlp-white.pdf">https://foxitsecurity.files.wordpress.com/2016/06/fox-it_mofang_threatreport_tlp-white.pdf</a>

## X-Agent

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.

X-Agent is also known as:

- XAgent

*Table 828. Table References*

Links
<a href="http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-update-ios-espionage-app-found/">http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-update-ios-espionage-app-found/</a>
<a href="https://app.box.com/s/l7n781ig6n8wlf1aff5hgwbh4qoi5jqqq">https://app.box.com/s/l7n781ig6n8wlf1aff5hgwbh4qoi5jqqq</a>

## X-Tunnel

X-Tunnel is also known as:

- XTunnel

## Foozer

*Table 829. Table References*

Links
<a href="https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/">https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/</a>

## WinIDS

*Table 830. Table References*

Links
<a href="https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/">https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/</a>

## DownRange

*Table 831. Table References*

Links
<a href="https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/">https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/</a>

## Mad Max

Table 832. Table References

Links
<a href="https://www.arbornetworks.com/blog/asert/mad-max-dga/">https://www.arbornetworks.com/blog/asert/mad-max-dga/</a>

## Crimson

Crimson is malware used as part of a campaign known as Operation Transparent Tribe that targeted Indian diplomatic and military victims

Table 833. Table References

Links
<a href="https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf">https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf</a>

## 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 834. Table References

Links
<a href="http://www.welivesecurity.com/wp-content/uploads/2016/05/Operation-Groundbait.pdf">http://www.welivesecurity.com/wp-content/uploads/2016/05/Operation-Groundbait.pdf</a>

## 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 835. Table References

Links
<a href="https://www.f-secure.com/documents/996508/1030745/nanhaishu_whitepaper.pdf">https://www.f-secure.com/documents/996508/1030745/nanhaishu_whitepaper.pdf</a>

## 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 836. 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 837. 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 838. 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 839. 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 840. Table References*

Links
<a href="https://securelist.com/blog/research/73660/adwind-faq/">https://securelist.com/blog/research/73660/adwind-faq/</a>

# 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 841. Table References*

Links
<a href="http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/dridex-financial-trojan.pdf">http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/dridex-financial-trojan.pdf</a>

## Fareit

## Gafgyt

## Gamarue

Gamarue is also known as:

- Andromeda

*Table 842. Table References*

Links
<a href="https://blog.gdatasoftware.com/2015/03/24274-the-andromeda-gamarue-botnet-is-on-the-rise-again">https://blog.gdatasoftware.com/2015/03/24274-the-andromeda-gamarue-botnet-is-on-the-rise-again</a>

## Necurs

The Necurs botnet is a distributor of many pieces of malware, most notably Locky.

*Table 843. Table References*

Links
<a href="https://en.wikipedia.org/wiki/Necurs_botnet">https://en.wikipedia.org/wiki/Necurs_botnet</a>

## Palevo

## Akbot

Akbot is also known as:

- Qbot
- Qakbot
- PinkSlipBot

*Table 844. Table References*

Links
<a href="https://en.wikipedia.org/wiki/Akbot">https://en.wikipedia.org/wiki/Akbot</a>

## 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 845. Table References

Links
<a href="https://www.sophos.com/medialibrary/PDFs/technical%20papers/sophos-vawtrak-international-crimeware-as-a-service-tpna.pdf">https://www.sophos.com/medialibrary/PDFs/technical%20papers/sophos-vawtrak-international-crimeware-as-a-service-tpna.pdf</a>

# 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 846. Table References

Links
<a href="https://github.com/adaptivethreat/Empire">https://github.com/adaptivethreat/Empire</a>

# 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 847. Table References

Links
<a href="https://www.checkpoint.com/downloads/volatile-cedar-technical-report.pdf">https://www.checkpoint.com/downloads/volatile-cedar-technical-report.pdf</a>

# 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 848. Table References

Links
<a href="https://citizenlab.org/2016/11/parliament-keyboy/">https://citizenlab.org/2016/11/parliament-keyboy/</a>
<a href="https://community.rapid7.com/community/infosec/blog/2013/06/07/keyboy-targeted-attacks-against-vietnam-and-india">https://community.rapid7.com/community/infosec/blog/2013/06/07/keyboy-targeted-attacks-against-vietnam-and-india</a>

# 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 849. Table References

Links
<a href="http://researchcenter.paloaltonetworks.com/2016/11/unit42-tropic-trooper-targets-taiwanese-government-and-fossil-fuel-provider-with-poison-ivy/">http://researchcenter.paloaltonetworks.com/2016/11/unit42-tropic-trooper-targets-taiwanese-government-and-fossil-fuel-provider-with-poison-ivy/</a>

# 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 850. Table References

Links
<a href="https://en.wikipedia.org/wiki/Mirai_(malware)">https://en.wikipedia.org/wiki/Mirai_(malware)</a>

# 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 851. Table References

Links
<a href="https://www.virusbulletin.com/conference/vb2014/abstracts/back-blackenergy-2014-targeted-attacks-ukraine-and-poland/">https://www.virusbulletin.com/conference/vb2014/abstracts/back-blackenergy-2014-targeted-attacks-ukraine-and-poland/</a>

## 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 852. Table References

Links
<a href="https://www.symantec.com/security_response/writeup.jsp?docid=2015-031915-4935-99">https://www.symantec.com/security_response/writeup.jsp?docid=2015-031915-4935-99</a>

## Backdoor.Tinybaron

## Incognito RAT

## DownRage

DownRage is also known as:

- Carberplike

Table 853. Table References

Links
<a href="https://labsblog.f-secure.com/2015/09/08/sofacy-recycles-carberp-and-metasploit-code/">https://labsblog.f-secure.com/2015/09/08/sofacy-recycles-carberp-and-metasploit-code/</a>
<a href="https://twitter.com/Timo_Steffens/status/814781584536719360">https://twitter.com/Timo_Steffens/status/814781584536719360</a>

## Chthonic

Table 854. 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 855. 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 856. Table References*

Links

[https://en.wikipedia.org/wiki/Zeus\\_\(malware\)](https://en.wikipedia.org/wiki/Zeus_(malware))

[https://www.symantec.com/security\\_response/writeup.jsp?docid=2010-011016-3514-99](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 857. 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 858. Table References*

Links

## 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 859. Table References*

Links
<a href="https://blogs.forcepoint.com/security-labs/mm-core-memory-backdoor-returns-bigboss-and-sillygoose">https://blogs.forcepoint.com/security-labs/mm-core-memory-backdoor-returns-bigboss-and-sillygoose</a>

## 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 860. Table References*

Links
<a href="https://en.wikipedia.org/wiki/Shamoon">https://en.wikipedia.org/wiki/Shamoon</a>

## 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 861. Table References*

Links
<a href="https://www.bleepingcomputer.com/news/security/new-ghostadmin-malware-used-for-data-theft-and-exfiltration/">https://www.bleepingcomputer.com/news/security/new-ghostadmin-malware-used-for-data-theft-and-exfiltration/</a>

## 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 862. Table References*

Links
<a href="http://blog.trendmicro.com/trendlabs-security-intelligence/uncovering-inner-workings-eyepyramid/">http://blog.trendmicro.com/trendlabs-security-intelligence/uncovering-inner-workings-eyepyramid/</a>

## LuminosityLink

LuminosityLink is a malware family costing \$40 that purports to be a system administration utility

*Table 863. Table References*

Links
<a href="http://researchcenter.paloaltonetworks.com/2016/07/unit42-investigating-the-luminositylink-remote-access-trojan-configuration/">http://researchcenter.paloaltonetworks.com/2016/07/unit42-investigating-the-luminositylink-remote-access-trojan-configuration/</a>

## 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

*Table 864. Table References*

Links
<a href="https://www.arbornetworks.com/blog/asert/flokibot-flock-bots/">https://www.arbornetworks.com/blog/asert/flokibot-flock-bots/</a>
<a href="https://blog.malwarebytes.com/threat-analysis/2016/11/floki-bot-and-the-stealthy-dropper/">https://blog.malwarebytes.com/threat-analysis/2016/11/floki-bot-and-the-stealthy-dropper/</a>

## 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 865. Table References*

Links
-------

<a href="https://www.proofpoint.com/us/threat-insight/post/APT-targets-russia-belarus-zero-plot">https://www.proofpoint.com/us/threat-insight/post/APT-targets-russia-belarus-zero-plot</a>
---

## 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 866. Table References*

Links
-------

<a href="https://blog.cylance.com/shell-crew-variants-continue-to-fly-under-big-avs-radar">https://blog.cylance.com/shell-crew-variants-continue-to-fly-under-big-avs-radar</a>
---

## adzok

Remote Access Trojan

*Table 867. Table References*

Links
-------

<a href="https://github.com/kevthehermit/RATDecoders">https://github.com/kevthehermit/RATDecoders</a>
---

## albertino

Remote Access Trojan

*Table 868. Table References*

Links
-------

<a href="https://github.com/kevthehermit/RATDecoders">https://github.com/kevthehermit/RATDecoders</a>
---

## arcom

Remote Access Trojan

*Table 869. Table References*

Links
-------

<a href="https://github.com/kevthehermit/RATDecoders">https://github.com/kevthehermit/RATDecoders</a>
---

## blacknix

Remote Access Trojan

*Table 870. Table References*

Links
-------

<a href="https://github.com/kevthehermit/RATDecoders">https://github.com/kevthehermit/RATDecoders</a>
---

## bluebanana

Remote Access Trojan

*Table 871. Table References*

Links
-------

<a href="https://github.com/kevthehermit/RATDecoders">https://github.com/kevthehermit/RATDecoders</a>
---

## bozok

Remote Access Trojan

*Table 872. Table References*

Links
-------

<a href="https://github.com/kevthehermit/RATDecoders">https://github.com/kevthehermit/RATDecoders</a>
---

## clientmesh

Remote Access Trojan

*Table 873. Table References*

Links
-------

<a href="https://github.com/kevthehermit/RATDecoders">https://github.com/kevthehermit/RATDecoders</a>
---

## cybergate

Remote Access Trojan

*Table 874. Table References*

Links
-------

<a href="https://github.com/kevthehermit/RATDecoders">https://github.com/kevthehermit/RATDecoders</a>
---

## darkcomet

Remote Access Trojan



Table 875. Table References

Links

<https://github.com/kevthehermit/RATDecoders>

## darkrat

Remote Access Trojan

Table 876. Table References

Links

<https://github.com/kevthehermit/RATDecoders>

## gh0st

Remote Access Trojan

Table 877. Table References

Links

<https://github.com/kevthehermit/RATDecoders>

## greame

Remote Access Trojan

Table 878. Table References

Links

<https://github.com/kevthehermit/RATDecoders>

## hawkeye

Remote Access Trojan

Table 879. Table References

Links

<https://github.com/kevthehermit/RATDecoders>

## javadropper

Remote Access Trojan

Table 880. Table References

Links

<https://github.com/kevthehermit/RATDecoders>

# lostdoor

Remote Access Trojan

*Table 881. Table References*

Links
<a href="https://github.com/kevthehermit/RATDecoders">https://github.com/kevthehermit/RATDecoders</a>

# luxnet

Remote Access Trojan

*Table 882. Table References*

Links
<a href="https://github.com/kevthehermit/RATDecoders">https://github.com/kevthehermit/RATDecoders</a>

# pandora

Remote Access Trojan

*Table 883. Table References*

Links
<a href="https://github.com/kevthehermit/RATDecoders">https://github.com/kevthehermit/RATDecoders</a>

# poisonivy

Remote Access Trojan

*Table 884. Table References*

Links
<a href="https://github.com/kevthehermit/RATDecoders">https://github.com/kevthehermit/RATDecoders</a>

# predatorpain

Remote Access Trojan

*Table 885. Table References*

Links
<a href="https://github.com/kevthehermit/RATDecoders">https://github.com/kevthehermit/RATDecoders</a>

# punisher

Remote Access Trojan

Table 886. Table References

Links

<https://github.com/kevthehermit/RATDecoders>

## grat

Remote Access Trojan

Table 887. Table References

Links

<https://github.com/kevthehermit/RATDecoders>

## shadowtech

Remote Access Trojan

Table 888. Table References

Links

<https://github.com/kevthehermit/RATDecoders>

## smallnet

Remote Access Trojan

Table 889. Table References

Links

<https://github.com/kevthehermit/RATDecoders>

## spygate

Remote Access Trojan

Table 890. Table References

Links

<https://github.com/kevthehermit/RATDecoders>

## template

Remote Access Trojan

Table 891. Table References

Links

<https://github.com/kevthehermit/RATDecoders>

## tapaoux

Remote Access Trojan

*Table 892. Table References*

Links
-------

<a href="https://github.com/kevthehermit/RATDecoders">https://github.com/kevthehermit/RATDecoders</a>
---

## vantom

Remote Access Trojan

*Table 893. Table References*

Links
-------

<a href="https://github.com/kevthehermit/RATDecoders">https://github.com/kevthehermit/RATDecoders</a>
---

## virusrat

Remote Access Trojan

*Table 894. Table References*

Links
-------

<a href="https://github.com/kevthehermit/RATDecoders">https://github.com/kevthehermit/RATDecoders</a>
---

## xena

Remote Access Trojan

*Table 895. Table References*

Links
-------

<a href="https://github.com/kevthehermit/RATDecoders">https://github.com/kevthehermit/RATDecoders</a>
---

## xtreme

Remote Access Trojan

*Table 896. Table References*

Links
-------

<a href="https://github.com/kevthehermit/RATDecoders">https://github.com/kevthehermit/RATDecoders</a>
---

## darkddoser

Remote Access Trojan

Table 897. Table References

Links

<https://github.com/kevthehermit/RATDecoders>

## jspy

Remote Access Trojan

Table 898. Table References

Links

<https://github.com/kevthehermit/RATDecoders>

## xrat

Remote Access Trojan

Table 899. 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 900. 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 901. Table References

Links

[https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/elf\\_imeij.a](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 902. Table References

Links
<a href="https://blogs.forcepoint.com/security-labs/trojanized-adobe-installer-used-install-dragonok%E2%80%99s-new-custom-backdoor">https://blogs.forcepoint.com/security-labs/trojanized-adobe-installer-used-install-dragonok%E2%80%99s-new-custom-backdoor</a>

## 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 903. Table References

Links
<a href="http://www.enigmasoftware.com/trochilusrat-removal/">http://www.enigmasoftware.com/trochilusrat-removal/</a>

## 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 904. Table References

Links
<a href="http://researchcenter.paloaltonetworks.com/2017/03/unit42-trochilus-rat-new-moonwind-rat-used-attack-thai-utility-organizations/">http://researchcenter.paloaltonetworks.com/2017/03/unit42-trochilus-rat-new-moonwind-rat-used-attack-thai-utility-organizations/</a>

## 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 905. Table References

Links
-------

## Sathurbot

The trojan serves as a backdoor. It can be controlled remotely.

*Table 906. Table References*

Links
<a href="http://virusradar.com/en/Win32_Sathurbot.A/description">http://virusradar.com/en/Win32_Sathurbot.A/description</a>
<a href="https://www.welivesecurity.com/2017/04/06/sathurbot-distributed-wordpress-password-attack/">https://www.welivesecurity.com/2017/04/06/sathurbot-distributed-wordpress-password-attack/</a>

## 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 907. Table References*

Links
<a href="http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html">http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html</a>

## 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 908. Table References*

Links
<a href="http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html">http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html</a>

# 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 909. Table References

Links
<a href="http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html">http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html</a>

# 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 910. Table References

Links
<a href="http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html">http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html</a>

# 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 911. Table References

Links
<a href="http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html">http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html</a>

# 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 912. Table References*

Links
<a href="http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html">http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html</a>

## COOKIEBAG

This 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.COOKIEBAG

*Table 913. Table References*

Links
<a href="http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html">http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html</a>

## 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 914. Table References*

Links
<a href="http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html">http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html</a>

## 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 915. Table References*

Links
<a href="http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html">http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html</a>

## 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 916. Table References

Links
<a href="http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html">http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html</a>

## 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 917. Table References

Links
<a href="http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html">http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html</a>

## 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 918. Table References

Links
<a href="http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html">http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html</a>

## 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 919. 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 920. 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 921. 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 922. Table References*

Links
<a href="http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html">http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html</a>

## 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 923. Table References*

Links
<a href="http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html">http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html</a>

## 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 924. Table References*

Links
<a href="http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html">http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html</a>

## 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 thequickbrownfxjimpsvalzydg 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 925. Table References*

Links
<a href="http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html">http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html</a>

## 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 926. Table References

Links
<a href="http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html">http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html</a>

## 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 927. Table References

Links
<a href="http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html">http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html</a>
<a href="http://contagiodump.blogspot.com/2010/06/these-days-i-see-spike-in-number-of.html">http://contagiodump.blogspot.com/2010/06/these-days-i-see-spike-in-number-of.html</a>

## 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 928. Table References

Links
<a href="http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html">http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html</a>

## 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 929. Table References

Links
<a href="http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html">http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html</a>

## 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 930. 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 931. 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 932. 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 933. Table References

Links
<a href="http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html">http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html</a>

## 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 934. Table References

Links
<a href="http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html">http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html</a>

## 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 935. Table References

Links
<a href="http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html">http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html</a>

## 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](http://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](http://www.bo2k.com). It also contains the hard disk identification code found at [www.winsim.com/diskid32/diskid32.cpp](http://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 936. Table References*

Links
<a href="http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html">http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html</a>

## 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 937. Table References*

Links
<a href="http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html">http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html</a>

## 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 938. Table References*

Links
<a href="http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html">http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html</a>

## 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 939. Table References

Links
<a href="http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html">http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html</a>

## 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 940. Table References

Links
<a href="http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html">http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html</a>

## 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 941. Table References

Links
<a href="http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html">http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html</a>

## 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 942. Table References

Links
-------

## WEBC2-GRENCAT

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 GRENCAT 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 943. 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 944. 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 945. 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 946. Table References*

Links
<a href="http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html">http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html</a>

## 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 947. Table References*

Links
<a href="http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html">http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html</a>

## 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 948. Table References*

Links
<a href="http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html">http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html</a>

## 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 949. Table References*

Links
-------

<a href="http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html">http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html</a>
---

## 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 950. Table References*

Links
-------

<a href="http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html">http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html</a>
---

## 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 951. Table References*

Links
-------

<a href="http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html">http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html</a>
---

## 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 952. Table References

Links
<a href="http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html">http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html</a>

## 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 953. Table References

Links
<a href="https://www.fireeye.com/blog/threat-research/2017/04/apt10_menuspass_grou.html">https://www.fireeye.com/blog/threat-research/2017/04/apt10_menuspass_grou.html</a>

## 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 954. Table References

Links
<a href="https://www.fireeye.com/blog/threat-research/2017/04/apt10_menuspass_grou.html">https://www.fireeye.com/blog/threat-research/2017/04/apt10_menuspass_grou.html</a>

## 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 955. Table References

Links
<a href="https://www.fireeye.com/blog/threat-research/2017/04/apt10_menuspass_grou.html">https://www.fireeye.com/blog/threat-research/2017/04/apt10_menuspass_grou.html</a>

## 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 956. Table References

Links
<a href="https://www.fireeye.com/blog/threat-research/2017/04/apt10_menus_pass_group.html">https://www.fireeye.com/blog/threat-research/2017/04/apt10_menus_pass_group.html</a>

## 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 957. Table References

Links
<a href="http://surveillance.rsf.org/en/hacking-team/">http://surveillance.rsf.org/en/hacking-team/</a>
<a href="https://wikileaks.org/hackingteam/emails/fileid/581640/267803">https://wikileaks.org/hackingteam/emails/fileid/581640/267803</a>
<a href="https://wikileaks.org/hackingteam/emails/emailid/31436">https://wikileaks.org/hackingteam/emails/emailid/31436</a>

## 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 958. Table References

Links
<a href="https://www.fireeye.com/blog/threat-research/2015/12/latentbot_trace_me.html">https://www.fireeye.com/blog/threat-research/2015/12/latentbot_trace_me.html</a>
<a href="https://www.fireeye.com/blog/threat-research/2017/04/cve-2017-0199_useda.html">https://www.fireeye.com/blog/threat-research/2017/04/cve-2017-0199_useda.html</a>

## **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 959. Table References*

Links
<a href="https://www.fireeye.com/blog/threat-research/2017/04/cve-2017-0199_useda.html">https://www.fireeye.com/blog/threat-research/2017/04/cve-2017-0199_useda.html</a>

## **RCS Galileo**

HackingTeam Remote Control System (RCS) Galileo hacking platform

*Table 960. Table References*

Links
<a href="https://www.f-secure.com/documents/996508/1030745/callisto-group">https://www.f-secure.com/documents/996508/1030745/callisto-group</a>

## **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

## **ENGLISHMANS DENTIST**

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 961. Table References*

Links
<a href="https://www.fireeye.com/blog/threat-research/2010/10/feodosoff-a-new-botnet-on-the-rise.html">https://www.fireeye.com/blog/threat-research/2010/10/feodosoff-a-new-botnet-on-the-rise.html</a>

## 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 962. Table References*

Links
<a href="http://researchcenter.paloaltonetworks.com/2017/04/unit42-cardinal-rat-active-two-years/">http://researchcenter.paloaltonetworks.com/2017/04/unit42-cardinal-rat-active-two-years/</a>

# 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 963. Table References

Links
<a href="https://www.us-cert.gov/ncas/alerts/TA17-117A">https://www.us-cert.gov/ncas/alerts/TA17-117A</a>

# 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 964. Table References

Links
<a href="http://researchcenter.paloaltonetworks.com/2017/05/unit42-kazuar-multiplatform-espionage-backdoor-api-access/">http://researchcenter.paloaltonetworks.com/2017/05/unit42-kazuar-multiplatform-espionage-backdoor-api-access/</a>

# 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 965. Table References

Links
<a href="https://blog.malwarebytes.com/threat-analysis/2016/10/trick-bot-dyrezas-successor/">https://blog.malwarebytes.com/threat-analysis/2016/10/trick-bot-dyrezas-successor/</a>
<a href="https://blog.fraudwatchinternational.com/malware/trickbot-malware-works">https://blog.fraudwatchinternational.com/malware/trickbot-malware-works</a>
<a href="https://securityintelligence.com/trickbot-is-hand-picking-private-banks-for-targets-with-redirectation-attacks-in-tow/">https://securityintelligence.com/trickbot-is-hand-picking-private-banks-for-targets-with-redirectation-attacks-in-tow/</a>

## Moneygram Adwind

Table 966. Table References

Links
<a href="https://myonlinesecurity.co.uk/new-guidelines-from-moneygram-malspam-delivers-a-brand-new-java-adwind-version/">https://myonlinesecurity.co.uk/new-guidelines-from-moneygram-malspam-delivers-a-brand-new-java-adwind-version/</a>