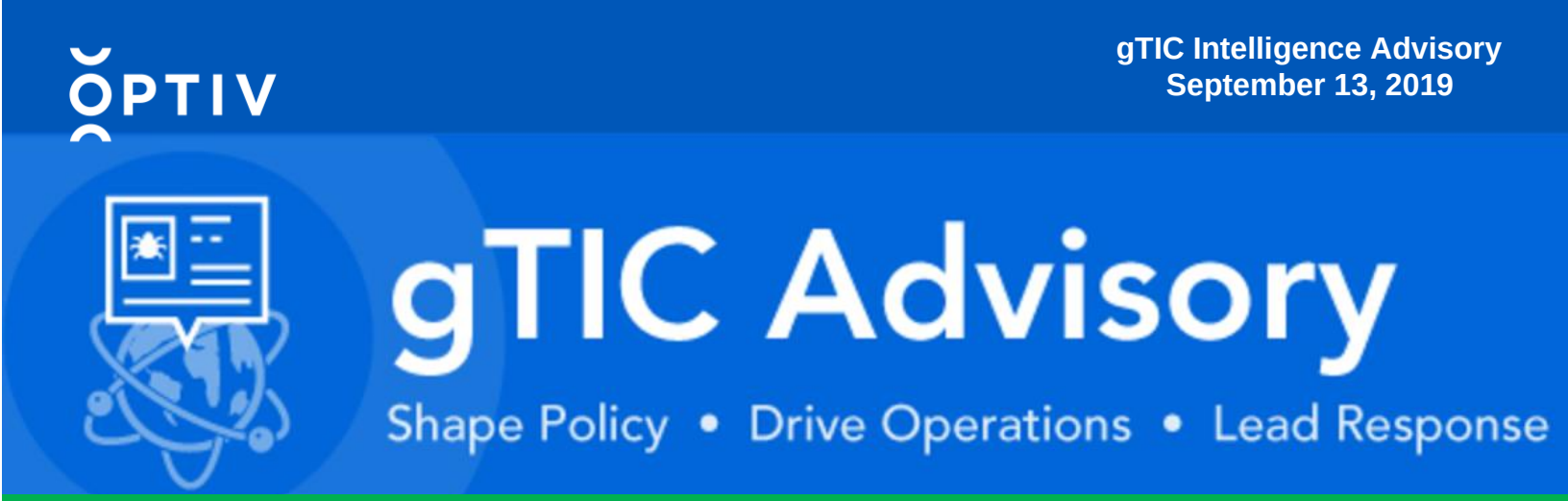

TLP GREEN

RIG Exploit Kit Delivering New Variation of Purple Fox Rootkit Malware

Executive Summary

Trend Micro has released a report on Purple Fox, a "fileless downloader malware" that is currently being dropped by the highly active RIG Exploit Kit. RIG has been involved in dropping a number of other high-profile malware that includes Pitou.B, SmokeLoader and just recently, the Nemty ransomware. This latest version of Purple Fox introduces new capabilities from previous iterations that includes abusing PowerShell for achieving fileless infections as well as a number of exploits. As Purple Fox is a fileless downloader malware, it is known for commonly retrieving and executing cryptocurrency-mining malware, however it has been used to download other types of malware families, which is what makes it a newly popular piece of malware.

Key Judgements

- Purple Fox, a fileless downloader malware, is being dropped by the RIG Exploit Kit
- This new iteration leverages the abuse of PowerShell that allows it to conduct fileless infections

Technical Information

The infection chain for this campaign relies on a user accessing a malicious site hosting the RIG Exploit Kit through one of three redirection methods.

- A Flash file that exploits an RCE vulnerability CVE-2018-15982 that could lead to malicious PowerShell script being executed.
- A pair of .htm files. The first exploiting a VBScript vulnerability within Internet Explorer, CVE-2014-6332. The second is a RCE vulnerability under the ID CVE-2018-8174.
- An .hta file that acts as a redirect to a malicious PowerShell script.

In addition, the PowerShell scripts are obfuscated and appear as a .jpg (jpeg) image file. If the compromised account has administrative access, the malicious PowerShell script utilizes the API calls of "msi.dll" which contains functions for installing Microsoft Installer packages that are easily exploitable. If the infected user does not have administrative privilege, the PowerShell script then attempts to exploits two Win32k privilege elevation vulnerabilities CVE-2015-1701 and CVE-2018-8120.

The payload delivery phase begins with the malware utilizing the “MsiInstallProductA” function from the “msi.dll” to download and execute the malicious payload file. An encrypted shellcode is contained in the payload file along with a 32-bit and 64-bit version of the payload. Upon execution, the malware will restart the computer and use the registry key "PendingFileRenameOperations" in order to rename its own components. The payload files are then hidden in the registry as part of its Rootkit functionality that will preserve itself upon a system reboot.

- A suspended svchost process is created that injects a DLL driver for the rootkit.
- Purple Fox abuses an open-source code for enabling its rootkit functions.
- It abuses a file utility software to obfuscate its DLL functions to hamper reverse engineering attempts.

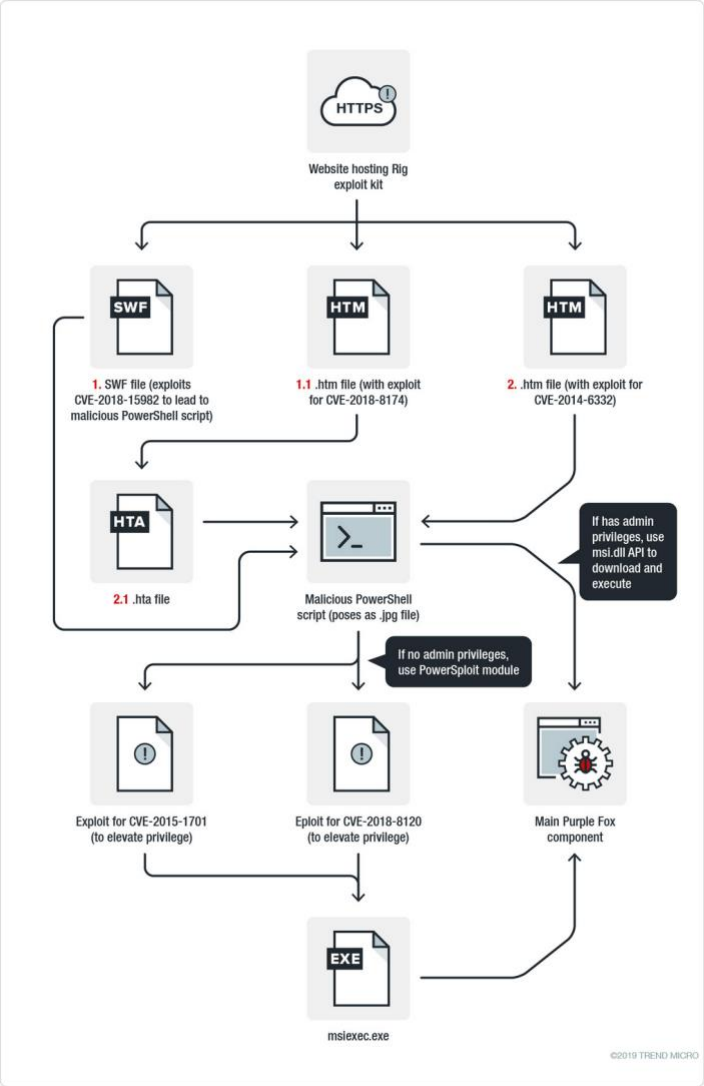

Figure 1. Screenshot of PowerShell abuse attack chain by Trend Micro

Conclusion

Intelligence Gaps

1.0 - What Optiv MSS or CTI clients are being targeted?
1.2 - What major event, vulnerability, or outbreak can pose an imminent threat to Optiv MSS or CTI clients?
3.1.0 - Who are the cyber-criminal groups?
3.1.1 - Who are the cyber-criminals targeting?
3.1.2 - When are the cyber-criminals planning to attack?

This product satisfies gTIC PIR(s):

2.0 - What are the high and critical vulnerabilities?
2.0.1 - Which high and critical vulnerabilities have exploit POCs available or published?
2.1 - What are the most commonly used exploit kits?
2.2 - What are the common persistence mechanisms?
3.1.0.1 - What IOCs are associated with cyber-criminal groups?
3.1.4 - What are the cyber-criminals' tools and TTPs?
3.2.0.2 – What is the intent of this threat actor?
4.0 - What threats pose a significant risk to the Financial Services & Insurance sector?
4.8 - What threats pose a significant risk to Other sectors?

Outlook

Purple Fox is one among many information stealers currently operating in the wild and appears likely it will maintain an active presence throughout the rest of 2019. This outlook is reinforced by changes seen in this latest variation along with the use of the RIG Exploit Kit that has also maintained a strong level of activity in 2019.

Analysis

The fileless nature and rootkit component of Purple Fox makes this malware type a high threat. This threat has been exacerbated by the use of the RIG Exploit Kit as a means of distribution. Malware authors continue to turn towards living-off-the-land techniques like PowerShell as opposed to lure documents containing malicious macro's as well. RIG EK has also been receiving a lot of attention over the last few months as it has been behind some high profile malware campaigns, including very recently with dropping the Nemty ransomware. While exploit kits have seen a decline in use since 2016, they still remain an effective delivery tool for malicious payloads.

Remediation Recommendations

In order to best protect against this threat, it is highly recommended to clients to take the following precautions.

- Apply patch updates regularly to your systems.
- Regulate and secure the use of system administrator tools.
- In addition, be mindful of pop-ups and ad domains related to your bank or financial institution and avoid interacting with such ads.
- Educate staff on the characteristics of malicious spam and spear-phishing emails as well as to avoid interacting with suspicious redirect links.
- Apply the indicators of compromise listed in Appendix I to your endpoint security tool.

Appendix I

Indicators of Compromise

SHA256 Hashes

07191e65af30541f71e876b6037079a070a34c435641897dc788c15e5f62f53c
b2cb65c9ac36f1e3fb31dfd5235c29b396be0968e6b225d625dc3c8fd72395f4
61113a0acd6469ce0d860db55c2afa3cdcbac2f5411fe8259cca43c10c042239
db09af7752eab8227c9ee1edad061a13aba08a6a53289a9c9bba9da2e6cc1f5f
517a523039a21e1961088cac8236bf5f6ee197d6a47d08abf114ee3418af0c08
87ea8d5bcd1056e76af822896db63f07732dbfab3fc632e7cf13802ae68afc40
33a584a0d4907b063af867fd33cc39362b74e96e72d2ad97db7748131364eab1
d9155d5e89692fac89a4defeb146ab6ad508d951bc4948067b44e5d0a6582b72
3e2c3d27d06c3b8a0106282b5d24dc6a44af7fdad74bc4993a3f3bcb7a82858d
a5a6be8b51439c793d903fb92c952c729db8e8050010c499607ee512f42bceff
09a6fe2764de81c7c5d588dc0542230a0d36aac69305139349fa43f4ab5a09d4
507fbe71ec4e059a6cffbf1f7c075073e51c20fa1bb0c9dbc830b5ad5179450a
14ae024e8e580904113eea52ce2a000b37b2998c2f257d3bc2cd176e8d9de1a2
ca7bd2830405ed53fd7f56738d7644ff8ecfd5bc63d079d322c99601c6106843
f0b0e0548b218fb81940a4daf85c3709b2159bb357cab2f55576af3d75d47094
498496827afc0aa5960d1cb1d60f7ae7699e0906e3a8c657b6864cff10772df0
164e96f9c19277d40cf58102c1d6fd75dab47bce4f79065ef996a2588b3f737a
ac05a938bbfc4ff0daeb1e45b6ccfdd7cae5bd6aa6e54c49ec6c8feef2ae06c4

Related IP Addresses

hxxp://141[.]98[.]216[.]130/1808164[.]jpg
hxxp://141[.]98[.]216[.]130/1603264[.]jpg
hxxp://141[.]98[.]216[.]130/1505164[.]jpg
hxxp://141[.]98[.]216[.]130/1808132[.]jpg
hxxp://141[.]98[.]216[.]130/1603232[.]jpg
hxxp://141[.]98[.]216[.]130/1505132[.]jpg
hxxp://141[.]98[.]216[.]130/pe[.]jpg

Related Domains and URLs

hxxp://jeitacave[.]org/ps004[.]jpg
hxxp://nw[.]brownsine[.]com/
hxxp://zopso[.]org/

Appendix II

References

Trend Micro (2018, December 6) Patch Now: Adobe Flash Zero Days Spread Via Spam. https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/patch-now-adobe-flash-zero-days-spread-via-spam?_ga=2.128269836.1058471897.1568309940-1546055497.1568309938

Trend Micro (2019, September 9) 'Purple Fox' Fileless Malware with Rootkit Component Delivered by Rig Exploit Kit Now Abuses PowerShell. https://blog.trendmicro.com/trendlabs-security-intelligence/purple-fox-fileless-malware-with-rookit-component-delivered-by-rig-exploit-kit-now-abuses-powershell/

Ilascu, Ionut (2019, September 3) Nemty Ransomware Gets Distribution from RIG Exploit Kit. https://www.bleepingcomputer.com/news/security/nemty-ransomware-gets-distribution-from-rig-exploit-kit/

Segura, Jerome (2019, May 14) Exploit kits: spring 2019 review. https://blog.malwarebytes.com/threat-analysis/2019/05/exploit-kits-spring-2019-review/

Classification Description: Information that may be available to the general public. It is defined as information with no existing legal restrictions on access or usage regardless of locality and bears no risk to the company when exposed outside the organizational boundary. Public data is available to all internal employees and all individuals outside of the company.