Clipminer Botnet Makes Operators at Least $1.7 Million

symantec-enterprise-blogs.security.com/blogs/threat-intelligence/clipminer-bitcoin-mining-hijacking

Threat Hunter TeamSymantec

Symantec's Threat Hunter Team, a part of Broadcom Software, has uncovered a cyber-criminal operation that has potentially made the actors behind it at least $1.7 million in illicit gains from cryptocurrency mining and theft via clipboard hijacking.

The malware being used, tracked by Symantec as Trojan.Clipminer, has a number of similarities to another crypto-mining Trojan called KryptoCibule, suggesting it may be a copycat or evolution of that threat.

Clipminer is likely spread via Trojanized downloads of cracked or pirated software. The malware arrives on compromised computers as a self-extracting WinRAR archive that drops and executes a downloader in the form of a packed portable executable DLL file with CPL file extension (although it does not follow the CPL format). The dropped file connects to the Tor network to download Clipminer's components.

Clipminer has the ability to use compromised computers' resources to mine for cryptocurrency. The malware also modifies the clipboard content in an attempt to redirect cryptocurrency transactions by users of the infected computer. On each clipboard update, it scans the clipboard content for wallet addresses, recognizing address formats used by at least a dozen different cryptocurrencies. The recognized addresses are then replaced with addresses of wallets controlled by the attacker. For the majority of the address formats, the attackers provide multiple replacement wallet addresses to choose from. The malware then picks the address that matches the prefix of the address to be replaced. This way, the victim is less likely to notice manipulation and is likely to proceed with the transaction. The malware includes a total of 4,375 unique addresses of wallets controlled by the attacker. Out of these, 3,677 addresses are used for just three different formats of Bitcoin addresses. Investigating just Bitcoin and Ethereum wallet addresses, we found that they, at the time of writing, contained approximately 34.3 Bitcoin and 129.9 Ethereum. However, some funds had also been transferred to what appear to be cryptocurrency tumblers, also known as cryptocurrency mixing services. These services mix potentially identifiable funds with others, so as to obscure the trail back to the fund's original source. If we include the funds transferred out to these services, the malware operators have potentially made at least $1.7 million from clipboard hijacking alone.

Technical analysis

The infection chain begins with a self-extracting WinRAR archive (bd48b5da093a37cfa5e3929c19ac06ce711bd581bc49040e68d2ba0e5610bf71) that drops and executes the masqueraded Control Panel (CPL) file:

> 1d31bea6a065fa20cf41861d21b7ea39979d40126c800ebc87d07adb41fe03f4 - m5ak8iW.cpl

The dropped file is actually a downloader in the form of a packed portable executable DLL, which has the following exports:

- GetExtensionVersion
- HttpExtensionProc
- TerminateExtension

Once the sample is executed, it arranges for itself to start again in case it gets interrupted.

To do so, it renames itself using the following format:

> C:\Windows\Temp\[VARIABLE]

It also creates the following registry value:

> HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\[VARIABLE]\"
> [VARIABLE]"="SHELL32.DLL|ShellExec_RunDLL|REGSVR32.EXE -s \"C:\\Windows\\Temp\\[VARIABLE].\""

(Note the extra DOT at the end of the filename)

Example file name:

> C:\Windows\Temp\and.loc

Example corresponding registry value:

- [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\zyqz
- "ipbfa"="SHELL32.DLL|ShellExec_RunDLL|REGSVR32.EXE -s \"C:\\Windows\\Temp\\and.loc.\""

Both of these will be deleted by the sample once it successfully downloads and installs its payload.

Next, the malware starts an embedded Tor client by downloading Tor consensus data:

> http://[HOST_IP_AND_PORT]/tor/status-vote/current/consensus.z

Where [HOST_IP_AND_PORT] is picked from a list embedded by the sample.

The malware then connects to the Tor network.

Next, it collects details from the affected computer, as shown in the following example:

[PUBLIC_IPv4_ADDRESS_AS_SEEN_ON_INTERNET];[REDACTED];"Intel(R) Core(TM) i5-10500 CPU @ 3.10GHz";L"\x005CDevice\x005CHarddiskVolume3\x005CWindows\x005CSystem32\x005Crundll32.exe",L"\x005CDevice\x005CHarddiskVolume3
[REDACTED]\x005CAppData\x005CLocal\x005CTemp\x005CM5aK8iW.cpL";"BC711 NVMe SK hynix 128GB[REDACTED];L"Windows Defender":61100;"PCI\[REDACTED]":"Intel(R) UHD Graphics; 630":1920:1200:59;113:[LIST_OF_RUNNING_PROCESSES];1920:1200:
[DESKTOP_SCREENSHOT_AS_BASE64_ENCODED_PNG];

It then sends the following HTTP GET request to an Onion Service over Tor:

> http://[ONION_SERVICE_AND_PORT]/[BINARY_AS_BASE64_ENCODED]

Where [BINARY_AS_BASE64_ENCODED] is a blob that appears to contain details of the infected machine, and [ONION_SERVICE_AND_PORT] is one of the following:

- miwia5zo4oxcj7n6:11472
- 6lmt3ott62q5pwae:52403
- nczflpbaow2ta7ua:19155
- re5sb73yb75nbkrm:33033
- qwhbbp6ye2l25wv6:13927
- 2q3n7ycm7vxe73g6:30656
- w4qjsuu5x5kwvkgu:61921
- gk7jrmr5v3nw3u7m:40090
- ip2djbz3xidmkmkw:53148
- pvy2atf27dq2d334:2720
- 3wquaem4x5qylhs5:17953

- niddw7jlqyc64xwc:36583
- ga3zm6uelxuniyq4:60117
- sv2fubnuttyzvfgl:39828
- kzzuxfvchn5kb73c:21646
- p2dw3umgw6qhrld3:25947
- wkhipwh6fb5j5hzx:25280
- ml7sphy7w3k2ge6d:12508
- dvivtswsxdxsqqxa:26960
- tq2srsgevhutzw42:43477
- xh6pciiw6yeqz3bs:19956
- xup6y7cxgjorezif:51516
- lbwgagk54ww5c3nj:32284
- rim3qyk3tdbt2iw3:60747
- krq2qyjhfwh4trww:51499
- obowq55leh2wguwg:35882
- xph6exfmdo7b4tkw:38607
- rs24qxgkhecjcgdn:51533
- i3uhj2pyh4cwwbmy:54343
- 7udhxrfpz6qwvspy:31399
- nwogcq7cmhth7e4x:15588
- gwtpcz4n3wtkwhj4:64393
- 5fajnveyn2bd4nm7:5990
- vcammjx7ddus5kfr:64148
- 42xgf6qae5wjbcva:45252

Note that the above are v2 Onion Services. In 2021, v2 Onion Services were depreciated and are no longer supported by current versions of Tor. However, many nodes on the Tor network have yet to be upgraded, meaning the services are still reachable.

The received response is roughly 10 MB in size and contains the Clipminer payload, which is used to perform coin mining and clipboard hijacking on the compromised computer.

The payload is stored in the following location:

> [EXISTING_TOP_DIRECTORY]\[VARIABLE]\[VARIABLE]\

Where [EXISTING_TOP_DIRECTORY] is one of the following:

- C:\Program Files (x86)\
- C:\Program Files (x86)\Common Files\
- C:\ProgramData\
- [USERPROFILE]\AppData\Local\

The following is an example of the location and directory naming convention used by the malware:

> C:\Program Files (x86)\Common Files\DevelTies\JueuiSirvices\

It also populates the two newly created directories with files copied from the local machine so that the malicious files are less likely to stand out.

It then drops the load point to the inner directory, where file hash, file directory, and file name vary:

> f49a5a0f2397609a3fb97728b5a997eb77cfa1b529188403fb5e8adaeac1860b rhnoiniye_ni.dll (Packed load point)

Then it creates scheduled tasks (similar to the following examples) to execute the load point for persistence (details vary between runs):

URI: \Microsoft\Windows\Active Directory Rights Management Services Client\Microc040e

Actions: Exec

Command: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe

Arguments: /u "C:\Program Files (x86)\Common Files\DevelTies\JueuiSirvices\imsgt_dvepr.dll"

WorkingDirectory: C:\Program Files (x86)\Common Files\DevelTies\JueuiSirvices

It creates the following empty registry key (likely as an infection marker):

> HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\[VARYING_UUID_FORMAT]

For example:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{19C316FE-770F-426C-9B63-F76C34154769}

The loaded payload starts a v3 Onion Service (the address changes per infection). We also observed traces of another v3 Onion Service (possibly used to ping the attackers whenever the compromised machine comes online).

The payload will monitor keyboard and mouse activity to determine if the machine is in use. It also appears to monitor running processes, checking for analysis/troubleshooting tools.

Whenever the malware determines that a machine is not in use (and at least some of the troubleshooting tools are not used), it starts the XMRig cryptocurrency miner. There are some indications that the attackers used a different miner in the past. Also, it is very likely that a different miner is used when a dedicated GPU is available (e.g. NVIDIA graphics card).

We also observed what looks like an XMRig command line (used during injection):

6Y6H --cpu-max-threads-hint=99 -k --pause-on-battery -o 94.75.205.148:443 -o 179.60.146.9:443

The sample includes a list of IPv4 addresses and picks two each time.

There is also an example JSONRPC request in memory (before encryption):

{"id":1,"jsonrpc":"2.0","method":"login","params":{"login":"x","pass":"x","agent":"app/1 (Windows NT 10.0; Win64; x64) libuv/1.41.0 msvc/2019
rnd/dywqmjcdytwkxewrvtqznxgmpmdzyqgulzacxcxx","algo":
["cn/1","cn/2","cn/r","cn/fast","cn/half","cn/xao","cn/rto","cn/rwz","cn/zls","cn/double","cn/ccx","rx/0","rx/wow","rx/arq","rx/sfx","rx/keva","argon2/chukv

Additionally, the malware monitors the clipboard for cryptocurrency addresses and replaces them with ones controlled by the attackers.

About the Author

Threat Hunter Team

Symantec

The Threat Hunter Team is a group of security experts within Symantec whose mission is to investigate targeted attacks, drive enhanced protection in Symantec products, and offer analysis that helps customers respond to attacks.