Underminer Exploit Kit: The More You Check The More Evasive You Become

blog.minerva-labs.com/underminer-exploit-kit-the-more-you-check-the-more-evasive-you-become

- Tweet

The Underminer exploit kit has surfaced numerous times since 2019, but here it is back again delivering the Amadey malware, as the Malwarebytes Threat Intelligence team found last week.

Exploit Kit

An exploit kit (EK), or an exploit pack, is a type of toolkit cybercriminals use to attack vulnerabilities in systems, for them to be able to distribute malware or perform other malicious activities. Exploit kits are packaged with exploits that can target commonly installed software, such as Adobe Flash®, Java®, Microsoft Silverlight®.

A typical exploit kit usually provides a management console, a bunch of vulnerabilities targeted to different applications, and several add-on functions that make it easier for a cybercriminal to launch an attack. Exploit kits typically integrate vulnerabilities of popular applications, which many users leave poorly patched.

It can also be used by someone who does not have any experience writing software code for creating, customizing, and distributing malware.

Underminer Exploit Kit

Underminer EK was first seen in the wild in 2017, targeting Asian countries by first deploying bootkits. This is a malware loaded during the boot process, which controlled the operating system start up, modifying the system before security components are loaded, for OS persistency and then a coinminer at a later stage. Back then, this EK spread by malvertising and exploiting browser vulnerabilities. One of the coinminers distributed by this EK was "Hidden Bee" - a covertly running Chinese miner.

When we dig into the Underminer EK, the authors seem to have a good grasp of anti-debugging techniques, as they applied plenty of them. We will discuss some interesting ones below.

The first check this EK performs is the use of assembly **rdtsc** instruction – this instruction is used to determine how many CPU ticks have taken place since the processor was reset. This can also be used as an anti-debugging technique. The most common way is to use this instruction to get the current timestamp, save it in a register, then get another timestamp and check if the delta between the two is below the exact number of ticks that were pre-decided by the author. In our sample, the second timestamp and the comparison were carried out long after the first timestamp was saved in the memory:

```
.text:00407E04 mov     eax, [eax+8]
.text:00407E07 mov     edx, [eax+20h]
.text:00407E0A mov     [ecx+esi*8+80h], edx
.text:00407E11 mov     eax, [eax+24h]
.text:00407E14 mov     [ecx+esi*8+84h], eax
.text:00407E1B rdtsc
.text:00407E1D push    64h ; 'd'
.text:00407E1F mov     [ecx+esi*8+200h], eax
.text:00407E26 mov     [ecx+esi*8+204h], edx
.text:00407E2D push    offset sub_407DE4
.text:00407E32 add     ecx, 8
.text:00407E35 push    ecx
.text:00407E36 jmp     short loc_407E4E
```

Figure 1 First Timestamp check

Next, in case the Avast library is loaded into the running process, the EK detaches the DLL_LOAD signal from aswhook.dll (Avast Hook Library) so that Avast AV will not capture the later DLL loading event.

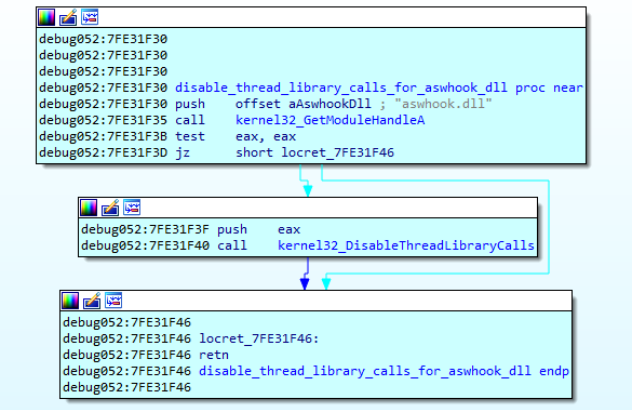


Figure 2 DLL_LOAD Detach

The Underminer remaps ntdll.dll and several others, a technique that might be used to bypass User-Mode Hooks.

The kit also checks if one of the following security products are installed under C:\Program Data by checking for the existence of the following products' directories:

- Avast Software
- Avira
- Kaspersky Lab
- Panda Security
- Doctor Web
- AVG
- 360TotalSecurity
- BitDefender
- Norton
- Sophos
- Comodo

In addition, Underminer EK uses several more popular techniques to check whether the process is being actively debugged. This EK didn't perform any anti-vm or anti-emulation techniques.

Request a demo to learn more about how Minerva Labs preemptively prevents malware attacks.

Later, the malware creates a "3e5d740863" folder under C:\Users\Username\AppData\local\Temp (user's temporary directory)and copies itself into it. The malware will add a registry key 'HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders' and pass the newly created folder path as a key value, which is a persistency technique in which the folder's content will be executed at user login, known as MITRE T1547.001.

After the file copy, the malware will execute the newly copied file and terminate the current process.

To become even more persistent in the system, Underminer creates a scheduled task that will execute malicious file every day at 01:00 AM. The scheduled task name is the executable's name, and it is run with the user's credentials.

Our sample connects two command and control servers, and passes the information of the infected station to them:

```
debug030:006EEAF0 aId152138566673 db 'id=152138566673&vs=2.71&sd=99459a&os=1&bi=1&ar=1&pc=[redacted]'
debug030:006EEAF0                                       ; DATA XREF: Stack[00001BE4]:2318FE7C↓o
debug030:006EEAF0 db 'F2&un=[redacted]&dm=&av=13&lv=0',0
```

The information being passed is:

- Victim ID
- A version of the malware
- PC name
- Username
- We assume, the number of binaries installed

The next stage is to download and execute additional malware. We checked the malware twice and got two different executables; one of them was an Oski Stealer and another new, well packed .Net stealer.

Oski Stealer is a malicious information stealer, which was first introduced in November 2019. The Oski stealer steals personal and sensitive credentials from its target, eventually being misused to clean out the user's liquid assets.

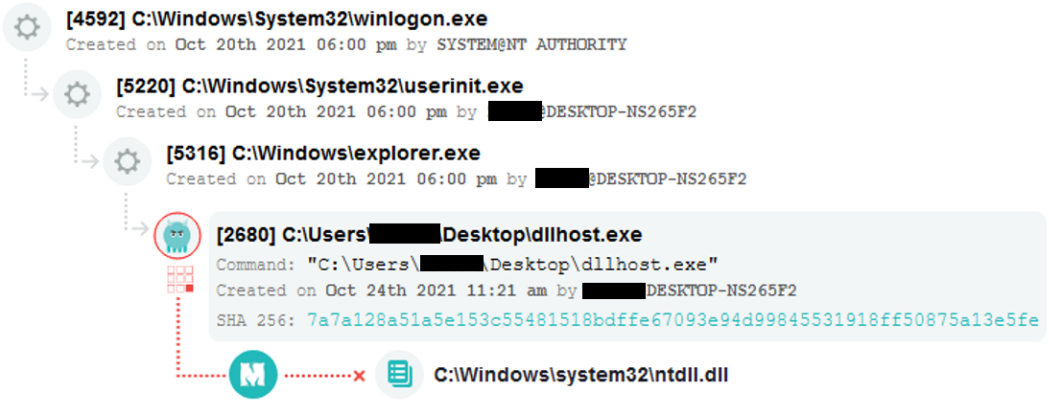
The second stealer, (with the original name of 'Licensing.exe') seems to have some code borrowed from RedLine Stealer. It steals browser credentials, crypto wallets, file share credentials etc. It connects to the command-and-control server via the 16713 TCP port.

As a side note, info stealers might be co-opted into the cycle of various kinds of attacks, and ransomware campaigns in particular. While serving a reliable method for criminals to obtain credentials tied to financial accounts, they have also started using 'information stealers' to obtain corporate remote network login credentials, like virtual private networks (VPNs) or remote desktop software. corporate remote network login credentials, like virtual private networks (VPNs) or remote desktop software.

Without being dependent on the drop file, Underminer exploit kit creates a new registry key to gain persistence over the dropped malware. The key will be added under HKCU\Software\Microsoft\Windows\CurrentVersion\Run.

At the time this blog was published, the command-and-control server was still operating and continues to distribute different types of malware.

Minerva Labs Hostile Environment Simulation and Critical Asset Protection modules prevent the remap of DLLs required for Underminer exploit kit to carry out its attack, thus preventing additional malware drops.



To learn more about about malware prevention:

Talk To Minerva Labs

IOC's:

Hashes:

- 7a7a128a51a5e153c55481518bdffe67093e94d99845531918ff50875a13e5fe – dllhost.exe – Underminer EK

- 0fa23ba39a85ad3a28d71e1d50edc2c39046d2ffe36fb257e8953acee7726924 – vt.zip – Oski Stealer
- eb0c56870fb482ff798dab0048ff1b8a7010f6ce6b769e9ffffc569070898624 – ic.exe (Licencing.exe)

Domains:

- web.jsonpost[.]xyz – C&C server
- web.xmlpost[.]xyz – C&C server

URL's:

- web.jsonpost[.]xyz/sj2vMs/index.php?scr=1 – C&C server
- web.xmlpost[.]xyz/sj2vMs/index.php?scr=1 – C&C server
- http://169.197.142[.]162/vt.zip - Oski Stealer

IP's:

169.197.142[.]162 - Underminer C&C

194.124.213[.]221 – Licensing C&C

References:

https://www.bleepingcomputer.com/news/security/new-underminer-exploit-kit-discovered-pushing-bootkits-and-coinminers/

https://socprime.com/news/underminer-exploit-kit-delivers-hidden-mellifera-malware/

https://www.aldeid.com/wiki/X86-assembly/Instructions/rdtsc

https://www.trendmicro.com/vinfo/us/security/definition/exploit-kit

https://intel471.com/blog/information-stealer-ransomware-account-takeover