New Underminer Exploit Kit Discovered Pushing Bootkits and CoinMiners

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

Catalin Cimpanu

By
Catalin Cimpanu

- July 28, 2018
- 10:33 AM
- 0

Security researchers have discovered a new exploit kit, currently active mainly in Asian countries, which, they say, has been busy spreading bootkits and cryptocurrency-mining (coinminer) malware.

This new exploit kit (EK) has been named Underminer in a report published yesterday by security firm Trend Micro. The company says it discovered the first clues of its existence last week, around July 17.

But fellow security firm Malwarebytes, which released an adjacent report that focused mainly on the coinminer malware spread by Underminer, says it tracked down earlier signs of this EK's activity dating back to late 2017 when it was first mentioned by Chinese security firm Qihoo 360.

The EK appears to have spent quite a few months operating at a smaller scale before expanding its activity to other countries.

According to Trend Micro, most of the web traffic flowing into Underminer is from Japan (70%), while the rest comes from Taiwan (10%), South Korea (6%), and other countries with smaller percentages.

EK uses a small number of exploits

At the technical level, the exploit kit is still small in terms of the number of exploits it deploys to infect users with malware. Researchers have spotted only three. They are:

CVE-2015-5119 —a use-after-free vulnerability in Adobe Flash Player patched in July 2015
CVE-2016-0189 —a memory corruption vulnerability in Internet Explorer (IE) patched in May 2016
CVE-2018-4878 —a use-after-free vulnerability in Adobe Flash Player patched in February 2018

None is specific to Underminer, and all have been used by other EKs in the past, suggesting the EK authors have built their operation by copying the ones before it.

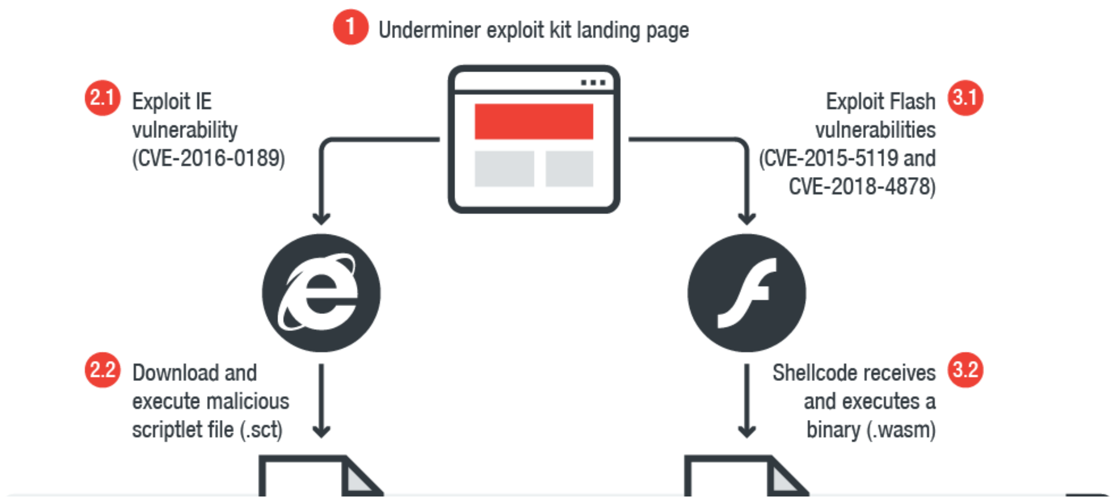
Underminer has been deploying Hidden Bee malware

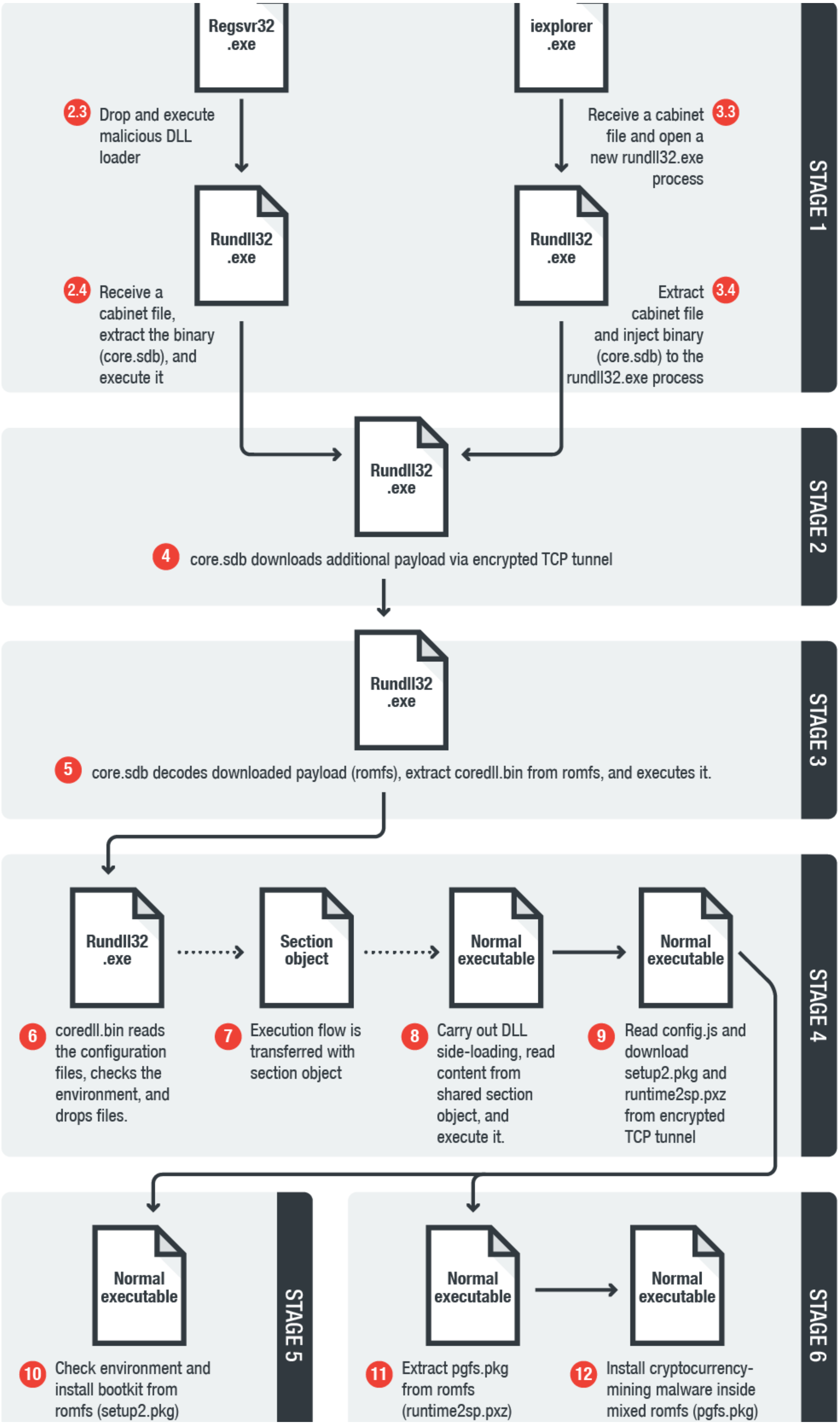
As for the malware delivery mechanism used in recent campaigns, the EK has been seen using encrypted TCP tunnels to deploy a bootkit first —for OS persistence— and then a coinminer.

Trend Micro calls this coinminer "Hidden Mellifera," while Malwarebytes refers to it as "Hidden Bee," the same name it received in the Chinese infosec community last year, when it was first spotted and analyzed [1, 2].

Exploit kits have been on a downward trend in the past two-three years, and usually keeping an up-to-date browser and OS is enough to safeguard users from getting infected.

A few new exploits pop up on the market once in a while, but all are short-lived, as they have a hard time keeping their operation at profitable levels, mainly because modern browsers are harder and harder to hack, while Flash usage has gone down in recent years [1, 2].


1 Underminer exploit kit landing page
2.1 Exploit IE vulnerability (CVE-2016-0189)
3.1 Exploit Flash vulnerabilities (CVE-2015-5119 and CVE-2018-4878)
2.2 Download and execute malicious scriptlet file (.sct)
3.2 Shellcode receives and executes a binary (.wasm)



2.3 Drop and execute malicious DLL loader

3.3 Receive a cabinet file and open a new rundll32.exe process

2.4 Receive a cabinet file, extract the binary (core.sdb), and execute it

3.4 Extract cabinet file and inject binary (core.sdb) to the rundll32.exe process

4 core.sdb downloads additional payload via encrypted TCP tunnel

5 core.sdb decodes downloaded payload (romfs), extract coredll.bin from romfs, and executes it.

6 coredll.bin reads the configuration files, checks the environment, and drops files.

7 Execution flow is transferred with section object

8 Carry out DLL side-loading, read content from shared section object, and execute it.

9 Read config.js and download setup2.pkg and runtime2sp.pxz from encrypted TCP tunnel

10 Check environment and install bootkit from romfs (setup2.pkg)

11 Extract pgfs.pkg from romfs (runtime2sp.pxz)

12 Install cryptocurrency-mining malware inside mixed romfs (pgfs.pkg)

Related Articles:

RIG Exploit Kit drops RedLine malware via Internet Explorer bug

Lenovo UEFI firmware driver bugs affect over 100 laptop models

Hackers exploit critical VMware CVE-2022-22954 bug, patch now

- Bootkit
- Coinminer
- Exploit Kit

Catalin Cimpanu

Catalin Cimpanu is the Security News Editor for Bleeping Computer, where he covers topics such as malware, breaches, vulnerabilities, exploits, hacking news, the Dark Web, and a few more. Catalin previously covered Web & Security news for Softpedia between May 2015 and October 2016. The easiest way to reach Catalin is via his XMPP/Jabber address at campuscodi@xmpp.is. For other contact methods, please visit Catalin's author page.

- Previous Article
- Next Article

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: