A Volatility Plugin Created for Detecting Malware Used in Targeted Attacks

Hello again – this is Shusei Tomonaga from Analysis Center.

This blog entry is to introduce "apt17scan.py" created by JPCERT/CC to detect certain malware used in targeted attacks, and to extract its configuration information. It is a plugin for the Volatility Framework (hereinafter "Volatility"), a memory forensics tool. My colleague Yuu Nakamura and I had the honour to introduce this at CODE BLUE 2015, an international conference for information security specialists, held in Tokyo on 28-29 October 2015.

The plugin is available for download on GitHub:

> JPCERTCC/aa-tools · GitHub
> https://github.com/JPCERTCC/aa-tools

Characteristics of the Adversary Group Targeting Japan

JPCERT/CC has confirmed that the following types of malware are being used by a certain attacker group targeting Japanese organisations:

- Agtid
- Hikit
- McRAT
- Preshin
- BlackCoffee
- Derusbi

The attacker group using these types of malware is referred to as "APT17" (by FireEye) [1] or "Aurora Panda" (by CrowdStrike) etc., and a number of security vendors have been investigating them.

One of the characteristics of this adversary group is that it sometimes uses malware which only exists in the memory (not saved as file). As such, you might not be able to detect the malware just by examining the hard disk when investigating the incident. Even if you could, its configuration information may be altered by the attacker's command.

Therefore, there is a need to examine the dumped memory image in an offline environment, in order to detect the malware which only exists in the memory, and to extract the configuration information of the malware which is running.

How To Use This Plugin

apt17scan.py has the following commands:

- apt17scan: Detect Agtid, Hikit, McRAT, Preshin, BlackCoffee and Derusbi in memory dump
- derusbiconfig: Detect Derusbi in memory dump and extract its configuration information

- hikitconfig: Detect Hikit in memory dump and extract its configuration information
- agtidconfig: Detect Agtid in memory dump and extract its configuration information

Upon its execution, save apt17scan.py in the "contrib/plugins/malware" folder in Volatility, and execute as follows:

```
$python vol.py [apt17scan|derusbiconfig|hikitconfig|agtidconfig] -f <memory.image>
 --profile=<profile>
```

Figure 1 below shows a sample result of executing apt17scan. It displays process names (Name), Process IDs (PID) and malware (Malware Name) that were detected.

```
mal@works:/opt/vol2.4$ python vol.py apt17scan -f mem.image --profile=Win7SP1x86
Volatility Foundation Volatility Framework 2.4
Name                 PID      Data VA    Malware Name
-------------------- -------- ---------- -------------
regsvr32.exe            3024 0x10000000 Derusbi
regsvr32.exe            3632 0x10000000 Derusbi
regsvr32.exe            2720 0x001f0000 Hikit
regsvr32.exe            2952 0x003e0000 Blackcoffee
regsvr32.exe            3108 0x10000000 Agtid
Appdata.exe             3196 0x00020000 Agtid
rundll32.exe            2360 0x004e0000 Preshin
```

Figure 1: A result of executing apt17scan

Figure 2 below shows a sample result of executing derusbiconfig. In many cases, Derusbi contains proxy information of internal networks. Also, the IDs contain strings that identify target organisations.

```
mal@works:/opt/vol2.4$ python vol.py derusbiconfig -f mem.image --profile=Win7SP1x86

Volatility Foundation Volatility Framework 2.4
------------------------------------------------------------------------------
Derusbi Config (Address: 0x10004778):

Process: regsvr32.exe (3632)

[Derusbi Config Info]
ID              : [redacted]20150126
Server list     : [redacted].140:443,[redacted].140:80
Sleep time      : 1
Service name    : wuauserv
Connect mode    : 4 (HTTP POST)
Proxy setting 1
   Server       : [redacted].31:8080
   User         :
   Password     :
Proxy setting 2
   Server       : [redacted].34:8080
   User         :
   Password     :
Proxy setting 3
   Server       :
   User         :
   Password     :
```

Figure 2: A result of executing derusbiconfig

Similarly, hikitconfig and agtidconfig can display malware configuration information as well.

Way Forward

JPCERT/CC has confirmed that the adversary group uses not only the aforementioned 6 types

of malware, but also other kinds of malware including PlugX. We will keep updating the plugin so that it can detect other malware as well.

We would highly appreciate your comments and feedback on the tool. Please contact aa-info@jpcert.or.jp.

Thank you.

- Shusei Tomonaga

Reference

[1] FireEye - APT17: Hiding in Plain Sight - FireEye and Microsoft Expose Obfuscation Tactic
https://www2.fireeye.com/WEB-2015RPTAPT17.html

Appendix

SHA-256 Hash Value of the samples

- Agtid: b33ffbec01b43301edd9db42a59dcd33dd45f638733e2f92f0cb5bfe86714734
- Hikit: 8da8dce703bc66d6ce57046151403f0972216b6b9d7b0127e8f1d5c788fea1ba
- McRAT: cc985872fe35fbb70b99c4adc5e51b52bc8358df08b4193e7b30251f967604f4
- Preshin: feafe1e3c9d93667e11712793f6c95fe953a1058519cfefb81f95ea2626af267
- BlackCoffee: 20cd49fd0f244944a8f5ba1d7656af3026e67d170133c1b3546c8b2de38d4f27
- Derusbi: 6d02c109b76267101c0d48c89b762d15b85c0eda4bbcd9f27bd76a905db202cd