

Volatility Plugin for Detecting RedLeaves Malware

Our [previous blog entry](#) introduced details of RedLeaves, a type of malware used for targeted attacks. Since then, we've seen reports including those from US-CERT that Management Service Providers (MSPs) have been targeted [1] [2]. In the US-CERT report, some instances have been identified where RedLeaves malware has only been found within memory with no on-disk evidence because of the behavior of self-elimination after the infection.

To verify the infection without on-disk evidence, investigation needs to be conducted through memory dump or logs (e.g. proxy logs) stored in network devices.

This article introduces a tool to detect RedLeaves in the memory.

It is available on GitHub:

JPCERTCC/aa-tools · GitHub

<https://github.com/JPCERTCC/aa-tools/blob/master/redleavesscan.py>

Tool Details

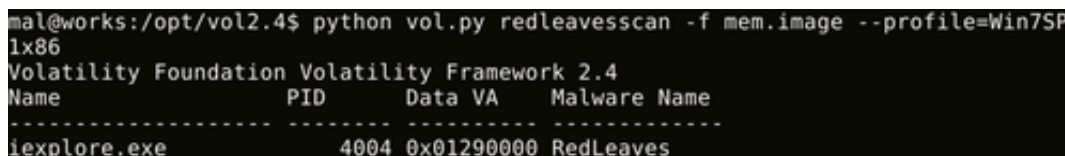
The tool works as a plugin for The Volatility Framework (hereafter "Volatility"), a memory forensic tool. redleavesscan.py has the following functions:

- redleavesscan: Detect RedLeaves in memory images
- redleavesconfig: Detect RedLeaves in memory images and extract malware configuration

To run the tool, save redleavesscan.py in "contrib/plugins/malware" folder within Volatility, and execute the following command:

```
$python vol.py [redleavesscan|redleavesconfig] -f <memory.image> - -profile=<profile>
```

Figure 1 shows an example output of redleavesscan. You can see the detected process name (Name), Process ID (PID) and the name of detected malware (Malware Name).



```
mal@works:/opt/vol2.4$ python vol.py redleavesscan -f mem.image --profile=Win7SP
1x86
Volatility Foundation Volatility Framework 2.4
Name          PID      Data VA    Malware Name
-----
iexplore.exe  4004    0x01290000 RedLeaves
```

Figure 1: Output of redleavesscan

Figure 2 shows an example output of redleavesconfig. For details about RedLeaves configuration, please see our [previous blog entry](#).

```
mal@works:/opt/vol2.4$ python vol.py redleavesconfig -f mem.image --profile=Win7
SP1x86
Volatility Foundation Volatility Framework 2.4
.....
RedLeaves Settings:

Process: iexplore.exe (4004)

[RedLeaves Config Info]
Server1      : 67.205.132.17
Server2      : 67.205.132.17
Server3      : 144.168.45.116
Port         : 443
Mode         : 4 (TCP and HTTP)
ID           : 2017-2-22-ALL
Mutex        : vv11287GD
Injection Process : %ProgramFiles\Internet Explorer\iexplore.exe
RC4 Key      : Lucky123
```

Figure 2: Output of redleavesconfig

In closing

It has been confirmed that the attacker group who uses RedLeaves also uses PlugX. To detect PlugX in memory, please use the Volatility plugin released by Airbus [3].

- Shusei Tomonaga

(Translated by Yukako Uchida)

Reference:

- [1] US-CERT: Intrusions Affecting Multiple Victims Across Multiple Sectors
https://www.us-cert.gov/sites/default/files/publications/IR-ALERT-MED-17-093-01C-Intrusions_Affecting_Multiple_Victims_Across_Multiple_Sectors.pdf
- [2] PwC: Operation Cloud Hopper
<https://www.pwc.co.uk/issues/cyber-security-data-privacy/insights/operation-cloud-hopper.html>
- [3] Volatility plugin for PlugX
https://bitbucket.org/cybertools/volatility_plugins/wiki/Home