Recent FK_Undead rootkit samples found in the wild

lab52.io/blog/recent-fk-undead-rootkit-samples-found-in-the-wild/

Malware that works at Ring0, generally known as rootkit, is one of the most concerning in many environments because it shares privileges and capabilities with antivirus and EDR solutions, which greatly complicates its detection as far as they can tamper and/or hide the data that allows its detection with relative ease.

One of these examples is a threat Known FK_Undead, which among its multiple stages of infection and modules, has at least 3 different Rootkit modules.

This malware family was detected for the first time in November 2018 and has remained active and in continuous evolution.

Regarding it's infecction chain, from what has been observed to date, the first element with which it infects a system is a dropper that renames itself as "ntprint.exe" and copies itself to the %TEMP% folder.

It check's the victim's location by contacting to "http://pv.sohu.]com/cityjson" after which downloads an executable protected with VMProtect that is stored in the %programdata% folder with a random name and executes it.

If this executable does not detect a virtualized environment, it downloads several malicious drivers of type Rootkit:

The first of this drivers, the most complete, is in charge of:

1. Monitoring all computer traffic, blocking access to anti-virus solution websites and modifying the content of some websites by injecting it's own code into the traffic results.
2. Adding a proxy to the browsers that routes all the victim's traffic through a server controlled by the actors behind this threat.
3. Protect the registry entry of it's own installation from being deleted from the system.
4. Avoid loading drivers with certain signatures to protect itself from other malware of the same kind. It downloads a list of signatures from it's command and control server every few seconds and prevents any driver with one of this signatures of being loaded. This is the updated list at the moment:

Zhou Donghang
Yuchengxian Feiwu service Co.,ltd
CHENGDU YIWO Tech Development Co., Ltd.

Chengdu Xiongdichuang Trading Co., Ltd.
Beijing Founder Apabi Technology Limited
Beijing Longweishengda Technology Co., Ltd.
Beijing Sages Education Consultant Co.,Ltd
Changsha Qiansheng Garden Landscape Co.,Ltd
Xi’ an JingTech electronic Technology Co.,LTD
Guangzhoushi Xunmeng Computer Technology Co.,Ltd
Henan Pushitong Intelligent Technology Co., Ltd.
Shanghai Huaqianshu Information Technology Co., Ltd.
Haining shengdun Network Information Technology Co., Ltd
金华米粒网络技术服务有限公司
梁富庆上海天游软件有限公司
姚秋玲
上海域联软件技术有限公司
北京新锐视锋科技有限公司

The second driver is part of the framework of the company “Callback Technologies” which offers an API for applications to control access to files on the disk by any program and even falsify the result. In particular, they only control when the process “svchost.exe” accesses the “HOSTS” file and serve to this process another file in its place, thus controlling the DNS resolutions of the victim without attracting attention, as far as when other software accesses the “HOSTS” file, it is the real one, which is clean, thus avoiding raising suspicion.

The third one is in charge of downloading and installing certificates in the victim machine, so that they can also control the victim’s SSL traffic completely, redirecting it to other sites or breaking the encryption on this legitimate traffic.

It should be noted that these are the modules currently known, but they probably have more modules from which no information has been obtained to date as this threat has been active for over a year and has a lot of new activity.

The majority of the downloads related to this malware are done over HTTP directly against IP addresses generally located in China and using relatively high ports.

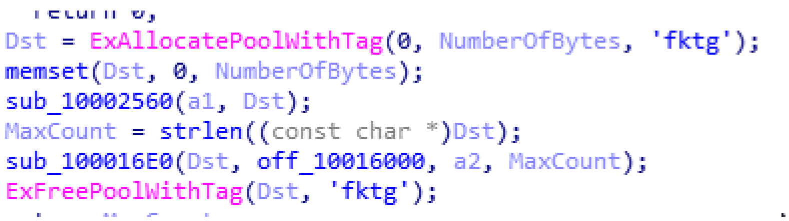
Some of the names of the threats at the time of download are as follows:

- “msdvdlx64.dat”
- “msdvdlx32.dat”
- “mshsdlx64.dat”
- “msadapdlx32.dat”

Regarding the different configurations of each driver, the download is identical, but with a different name structure, since in this case they contain the word “list” in it’s name and it’s contents are base64 encoded.

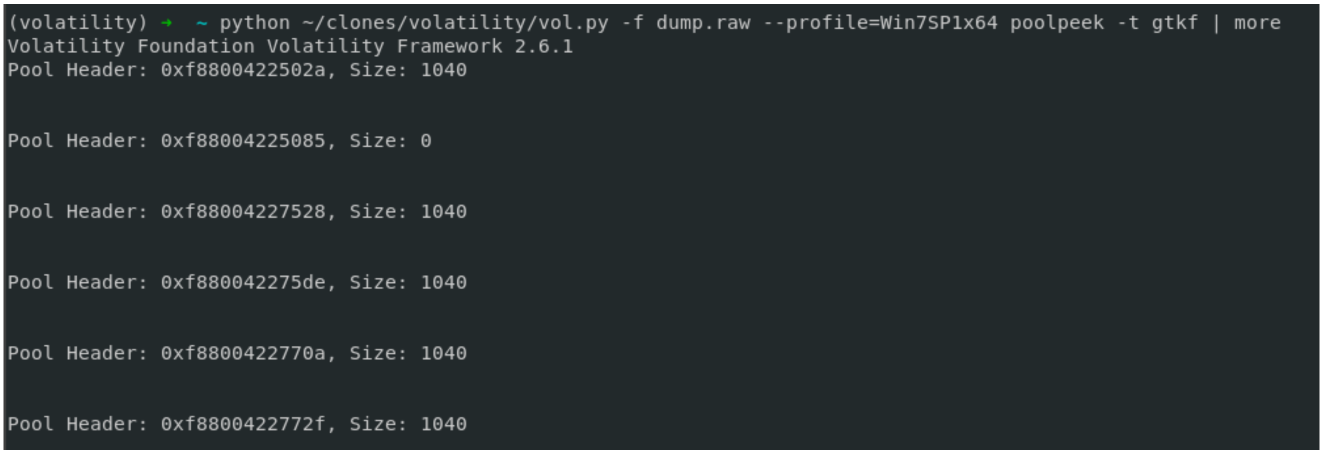
- “paclist.dat”
- “tdplist.dat”
- “dnlist.dat”

All the drivers developed by this group to date use the same “PoolTags” for allocating memory in the kernel space “fktg” and “fkhs”.



```
  return 0;
Dst = ExAllocatePoolWithTag(0, NumberOfBytes, 'fktg');
memset(Dst, 0, NumberOfBytes);
sub_10002560(a1, Dst);
MaxCount = strlen((const char *)Dst);
sub_100016E0(Dst, off_10016000, a2, MaxCount);
ExFreePoolWithTag(Dst, 'fktg');
```

During a forensic analysis, this data can be very interesting to take into account as IOC, because some tools like Volatility allow scanning the memory for these memory pools.



```
(volatility) ➜  ~ python ~/clones/volatility/vol.py -f dump.raw --profile=Win7SP1x64 poolpeek -t gtkf | more
Volatility Foundation Volatility Framework 2.6.1
Pool Header: 0xf8800422502a, Size: 1040


Pool Header: 0xf88004225085, Size: 0


Pool Header: 0xf88004227528, Size: 1040


Pool Header: 0xf880042275de, Size: 1040


Pool Header: 0xf8800422770a, Size: 1040


Pool Header: 0xf8800422772f, Size: 1040
```

Specifically, the volatility plugin in charge of doing this is “poolpeek” and requires as a parameter this PoolTag but reversed, since in memory, it is stored this way:

- “poolpeek -t gtkf”
- “poolpeek -t shkf”

IOCs

C2 IP List

106.]14.47.210
120.]77.36.184
183.]2.193.147
103.]216.154.25
139.]196.228.142
45.]113.201.205

Redirect Servers

115].231.218.133	182].61.182.114
115].231.218.86	182].61.182.123
182].61.164.201	182].61.182.97
182].61.177.32	182].61.183.212
182].61.177.37	182].61.183.215
182].61.180.119	182].61.188.252
182].61.180.134	192].126.127.199

PDBs found in drivers

fk_drv.pdb	fk_netfltdll32.pdb
fk_maindrv.pdb	fk_adswindll32.pdb
fk_svcsdll.pdb	fk_adsexdrv32.pdb