GAIS
Cyber Security

CRYPTOCURRENCY MINER MALWARE ANALYSIS REPORT

2018 | GAIS CERT

JUSTWORK OFİS KAMPÜSÜ ÜMRANİYE / İSTANBUL | www.gaissecurity.com
+90 216 999 4247 | info@gaissecurity.com

SUMMARY

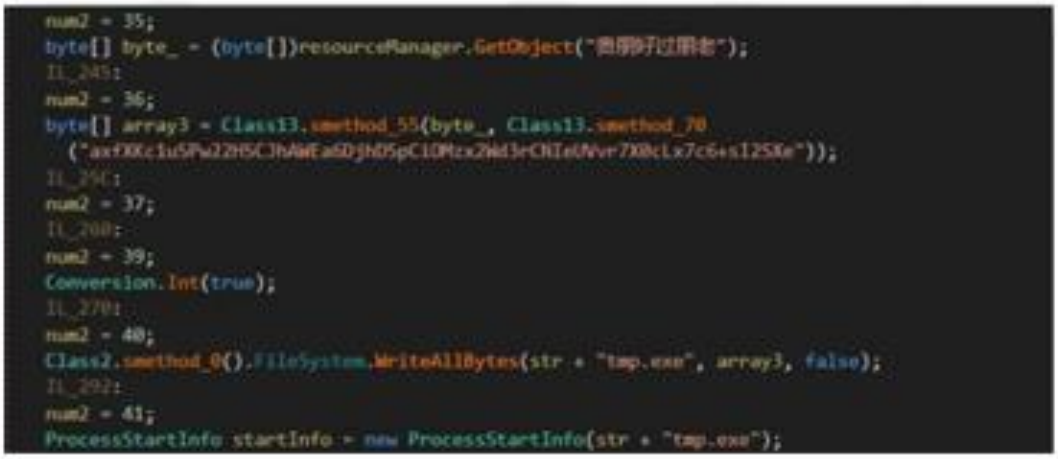
This is a miner type malicious based in Russia, which continues to spread with the file name "SteelSeries.exe" identified in the malware intelligence network.

The malware, that is in contact with the domains listed below during penetration and connection process with the control panel, uses the victims in the network to obtain crypto-currency called Monero(XMR).

- ✓ torroot.ru
- ✓ roottor.ru

Details of the Malware

It is the preloader of the malware that enters the system with the boot loader. It is an executable file that is compiled based on the .NET Framework 2.0 version. Its codes are mixed with the code mixer called SmartAssembly.



At the time of start-up, other software, which is contained in malicious software and is encrypted, is saved with “tmp.exe” file name under the folder where temporary files are stored on the user profile.

The folder paths and file names that are used at this time are assigned to the variables as encrypted.

During the operation, the decryption function (using the Rijndael algorithm) is called and the encrypted data is available.

The software that is started with the name “tmp.exe” is an executable file that is compiled based on the .NET Framework 2.0 version and is mixed with .NET Reactor. The main functions of malware are available here.

As you can see in this part of the dynamic analysis output of FenriScan, after starting malicious software, it creates 2 files with the file names "svhost.exe" and "tmp.exe" in the Temp folder and then runs them.

The two running applications are calling the application "curl.exe" with the "-o pool.minexmr.com:4444 -u 46uPTtPJRN3GZmqQLctZxY6R3XJHKi8zeggkjeU75xWa4VXp9vgyij52QgbUwQdeGe3FP7FK1RQRtA4mvB1uhadM2bjNLyV -p x --cpu-affinity 75" parameter.

This application is downloaded from "roottor.ru" address. "Curl.exe" is a software that is published by the file named "xmrig.com" and is used for mining of XMR.

After the Mining process is started, the malicious software performs the following requests to the command panel.

C&C

There are 5 folders on the domain where the malicious software spreads.

There is no access to the "cgi-bin" folder, nothing appears on the "q" at first glance, but when we examine the possible folders, there is an entry panel under "/ admin".

There are malicious software in "shares".

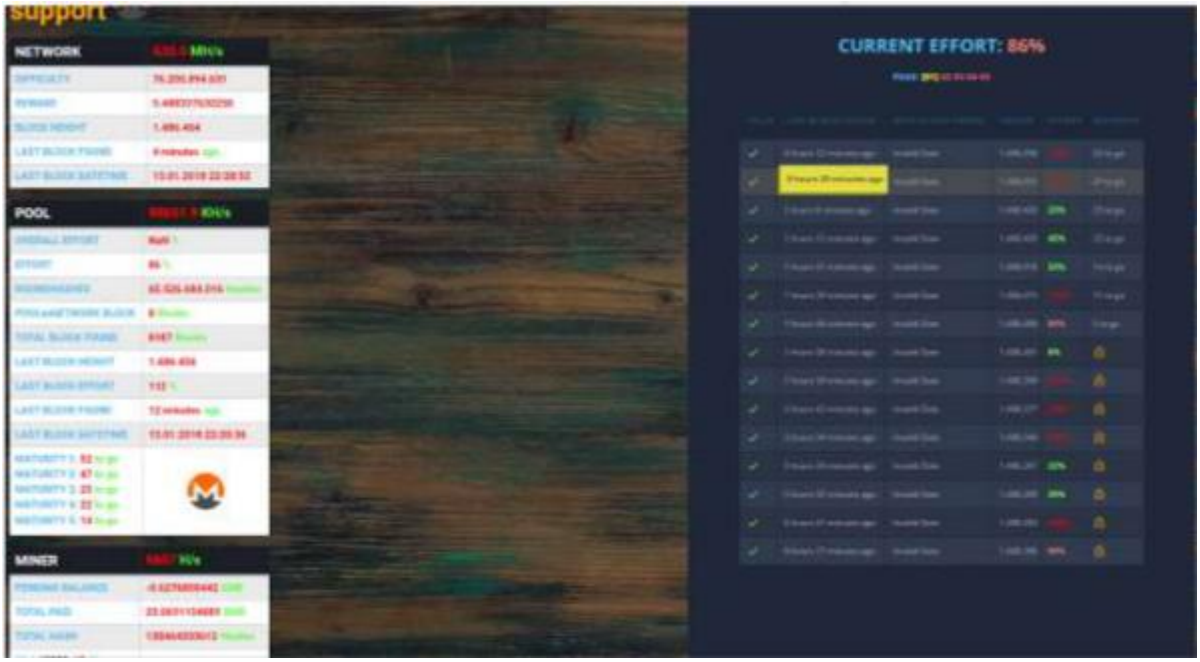
Name	Last modified	Size	Description
Parent Directory		-	
MSIReminder.exe	2018-01-10 16:19	674K	
Reminder.exe	2018-01-10 16:19	172K	
SteelSeries.exe	2018-01-10 16:59	193K	

“skyroot.ru” içerisinde klasör ismine sahip alan adının dosyaları bulunmaktadır.
In "skyroot.ru" there are files of domain name with folder name.

Index of /skyroot.ru

Name	Last modified	Size	Description
Parent Directory		-	
cgi-bin/	2018-01-12 06:49	-	
df/	2015-07-18 23:08	-	

"Xmr" contains a structure showing the statistics in the mining pool that has the hash value "46uPTtPJRN3GZmqQLctZxY6R3XJHKi8zeggkjeU75xWa4VXp9vgyij52QgbUwQdeGe3FP7FK1RQRtA4mvB1uhadM2bjNLyV" served by the malicious software.



When we examine the domain name of the malicious software that transfers data, we see the entry of the control panel.

We have contacted the following addresses at the time of harmful software operation.

DNS	roottor.ru
IP	178.250.241.22
HTTP	178.250.241.22
DNS	gulf.moneroocean.stream