Lab 2 Solutions - The Case of Remcos RAT

Lab 2- The case of Remcos RAT

This is the continuation of Lab 1, analyze the sample host.exe and answer the below questions

- What is the name of the file dropped by the malware?
- Where does it drop this file?
- Does the malware copies itself or does it drop a different component?
- How does malware execute this dropped file?
- What is the name of the C2 domain?
- What is the port on which malware is communicating?
- Do you see anything suspicious in the network traffic?
- How is Malware persisting on the system?

Answers

To answer the questions, first, we need to prepare the environment so that we can execute the malware (dynamic analysis) and determine its characteristics. Before executing the malware sample make sure the gateway of the windows machine is set to the IP address of Linux machine and then run the necessary monitoring tools (Process Hacker, Noriben) on Windows systems and on the Linux machine run Wireshark & INetSim. Before running INetsim make sure you run the script "***add_inetsim_redirect_entries.py***", this will add iptables rules to redirect any connection made by the malware to the IP address. With all the monitoring tools running, now, execute the malware sample for few seconds then terminate the malware process, stop the monitoring tools and looks at the results.

01. What is the name of the file dropped by the malware?

Looking at the results from Noriben shows that once executed host.exe creates a file "***remmy.exe***" as shown in the below screen shot

```
[CreateFile] host.exe:3364 > %AppData%\remmy\remmy.exe
```

02. Where does it drop this file?

As shown in the above screenshot the file "***remmy.exe***" is dropped in "***%AppData%\remmy***" folder

03. Does the malware copies itself or does it drop a different component?

Comparing the md5sum of the original file (***host.exe***) and the dropped file (***remmy.exe***) show that they both have the same cryptographic hash, this indicates that host.exe, when executed, copied itself to "***%AppData%\remmy***" directory

```
root@kratos:~/Desktop/malwares# md5sum remmy.exe
4a21e5957aeda4467dad810e29bf2cfa  remmy.exe
root@kratos:~/Desktop/malwares# md5sum remmy.exe
4a21e5957aeda4467dad810e29bf2cfa  remmy.exe
```

04. How does malware execute this dropped file?

Looking at the Noriben results based on the timeline shows that the ***host.exe*** first dropped the file ***remmy.exe*** in "***%AppData%\remmy***" directory and it also dropped a file "***install.bat***" which is a batch script executed via ***cmd.exe***, this in turn creates ***remmy.exe***

```
File,CreateFile,host.exe,3364,%AppData%\remmy\remmy.exe
File,CreateFile,host.exe,3364,%LocalAppData%\Temp\install.bat
Process,CreateProcess,host.exe,3364,%WinDir%\system32\cmd.exe /c %LocalAppData%\Temp
\install.bat
Process,CreateProcess,cmd.exe,3352,%AppData%\remmy\remmy.exe
```

05. What is the name of the C2 domain?

Inspecting Wireshark results show that when the malware is executed it tries to resolve the domain "***piergxrx.com***"

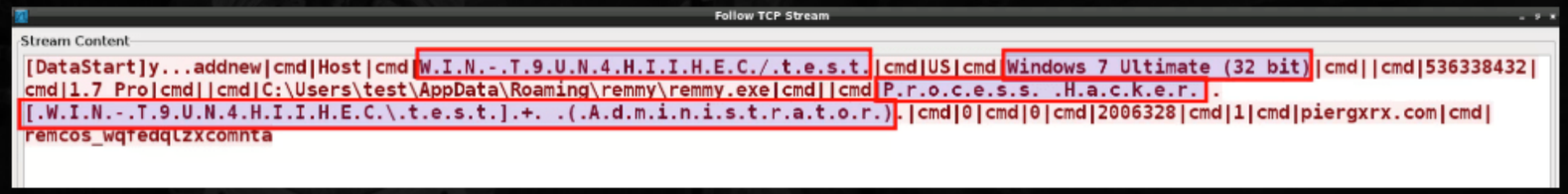
4	19.994666	192.168.1.60	192.168.1.100	DNS	Standard query A piergxrx.com
5	20.002911	192.168.1.100	192.168.1.60	DNS	Standard query response A 192.168.1.100
6	20.005144	192.168.1.60	192.168.1.100	TCP	49160 > 2404 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 S
7	20.005164	192.168.1.100	192.168.1.60	TCP	2404 > 49160 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1
8	20.005307	192.168.1.60	192.168.1.100	TCP	49160 > 2404 [ACK] Seq=1 Ack=1 Win=65536 Len=0
9	20.006734	192.168.1.60	192.168.1.100	104apci	<ERR 392 bytes>
10	20.006746	192.168.1.100	192.168.1.60	TCP	2404 > 49160 [ACK] Seq=1 Ack=393 Win=15680 Len=0

06. What is the port on which malware is communicating?

Once the malware resolves the domain "***piergxrx.com***" it communicates on the destination port ***2404*** as shown in the above screenshot

07. Do you see anything suspicious in the network traffic?

Looking at the TCP steam shows that the operating system information (like hostname, username, Windows version, active window) is sent to the attacker.



08. How is Malware persisting on the system?

Malware persists by adding an entry in the Run registry key. In the screenshots, malware added a value name "***flupdater***" and the value data is set to the path of the dropped file (***remmy.exe***), this ensures that when the system restarts, "***remmy.exe***" is executed

```
[RegCreateKey] remmy.exe:3340 > HKCU\Software\Microsoft\Windows\CurrentVersion\Run\
[RegSetValue] remmy.exe:3340 > HKCU\Software\Microsoft\Windows\CurrentVersion\Run
\flupdater  =  C:\Users\test\AppData\Roaming\remmy\remmy.exe
```