

RedLine Lab

Category: Endpoint Forensics

Tactics: Privilege Escalation Defense Evasion Command and Control

Tools: Volatility Strings

Easy Retired 45mins ★★★★★ 4.5

Scenario

As a member of the Security Blue team, your assignment is to analyze a memory dump using Redline and Volatility tools. Your goal is to trace the steps taken by the attacker on the compromised machine and determine how they managed to bypass the Network Intrusion Detection System (NIDS). Your investigation will identify the specific malware family employed in the attack and its characteristics. Additionally, your task is to identify and mitigate any traces or footprints left by the attacker.

Q1  Solved : 2979

What is the name of the suspicious process?

Para identificar el proceso sospechoso con la herramienta volatility3 hice uso de plugins malfind el cual ayuda a identificar posibles indicios de malware ejecutado en memoria con el comando

Python3 vol.py -f <direccion de memoria> windows.malfind

```

11:20:29 csi@csi /opt/volatility3
> python3 vol.py -f /home/csi/Downloads/temp_extract_dir/MemoryDump.mem windows.malfind
Volatility 3 Framework 2.0.2
Progress: 100.00 PDB scanning finished
PID Process Start VPN End VPN Tag Protection CommitCharge PrivateMemory File output Hexdump Disasm
5896 oneetx.exe 0x400000 0x437fff VadS PAGE_EXECUTE_READWRITE 56 1 Disabled
40 5a 50 00 03 00 00 00 MZ.....
04 00 00 00 ff ff 00 00 .....
b8 00 00 00 00 00 00 00 .....
40 00 00 00 00 00 00 00 @.....
00 00 00 00 00 00 00 00 .....
00 00 00 00 00 00 00 00 .....
00 00 00 00 00 00 00 00 .....
00 00 00 00 01 00 00 00 .....
0x400000: dec ebp
0x400001: pop edx
0x400002: nop
0x400003: add byte ptr [ebx], al
0x400005: add byte ptr [eax], al
0x400007: add byte ptr [eax + eax], al
0x40000a: add byte ptr [eax], al



```

visualizando encontré este proceso sospecho asi dando con la primera flag

Q1 ☒ Solved : 2979

What is the name of the suspicious process?

oneetx.exe



 Hints  Submit

La flag: oneetx.exe

Flag 2

Q2 ☐ Solved : 2938

What is the child process name of the suspicious process?

 Hints  Submit

Para encontrar esta flag utilizaremos el plugins pslist para ubicar el proceso hijo de este programa la metodologia para encontrarlo seria partiendo del proceso padre filtrar con el comando grep su pid

Python3 vol.py -f <direccion de memoria> windows.pslist | grep 5896

```

11:30:50 csi@csi /opt/volatility3
> python3 vol.py -f /home/csi/Downloads/temp_extract_dir/MemoryDump.mem windows.pslist | grep 5896
5896 8844 oneetx.exe 0xad8189b41080 5 - 1 True 2023-05-21 22:30:56.000000 N/A Disabled
7732 5896 rundll32.exe 0xad818d1912c0 1 - 1 True 2023-05-21 22:31:53.000000 N/A Disabled

```

Asi encontrado el subprocesso que sería el rundll32.exe

Q2 Solved : 2938

What is the child process name of the suspicious process?

Hints Submit

La flag: **rundll32.exe**

Flag 3

Q3 Solved : 2853

What is the memory protection applied to the suspicious process memory region?

**** *****

Hints Submit

Para encontrar esta tercera flag retrocedemos hasta nuestro anterior plugins de identificacion maliciosa pero ahora con el fin de buscar la apliccaion de proteccion de este.

Python3 vol.py -f <direccion de memoria> windows.malfind

PID	Process	Start VPN	End VPN	Tag	Protection	CommitCharge	PrivateMemory	File output	Hexdump	Disasm
5896	oneetx.exe	0x400000	0x437fff		VadS	PAGE_EXECUTE_READWRITE	56	1	Disabled	
4d 5a	00 00 03 00 00 00	MZ.....								
04 00	00 00 ff ff 00 00								
08 00	00 00 00 00 00 00								
40 00	00 00 00 00 00 00	@.....								
00 00	00 00 00 00 00 00								
00 00	00 00 00 00 00 00								
00 00	00 00 00 00 00 00								
00 00	00 00 00 00 01 00								
0x400000:	dec	ebp								
0x400001:	pop	edx								
0x400002:	nop									
0x400003:	add	byte ptr [ebx], al								
0x400005:	add	byte ptr [eax], al								
0x400007:	add	byte ptr [eax + eax], al								
0x40000a:	add	byte ptr [eax], al								

La flag: **PAGE_EXECUTE_READWRITE**

Q3 Solved : 2853

What is the memory protection applied to the suspicious process memory region?

**** *****

Hints Submit

Flag 4

Q4 ○ Solved : 2777

What is the name of the process responsible for the VPN connection?

💡 Hints

▶ Submit

para realizar esta flag realice una investigacion sobre las aplicaciones en ejecucion de los .exe que habian esta activo utilizando el comando

Python3 vol.py -f <direccion de memoria> windows.pslist | grep 3580

Para buscar el proceso de explorer.exe

```
11:54:47 csi@csi /opt/volatility3
> python3 vol.py -f /home/csi/Downloads/temp_extract_dir/MemoryDump.mem windows.pslist | grep 3580
3580 3556 explorer.exe 0xad818c047340 76 - 1 False 2023-05-21 22:30:28.000000 N/A Disabled
464 3580 SecurityHealth 0xad818979d080 3 - 1 False 2023-05-21 22:31:59.000000 N/A Disabled
3252 3580 vmtoolsd.exe 0xad8189796300 8 - 1 False 2023-05-21 22:31:59.000000 N/A Disabled
5328 3580 msedge.exe 0xad818d0980c0 54 - 1 False 2023-05-21 22:32:02.000000 N/A Disabled
6724 3580 Outline.exe 0xad818e578080 0 - 1 True 2023-05-21 22:36:09.000000 2023-05-21 23:01:24.000000 Disabled
2228 3580 FTK Imager.exe 0xad818d143080 10 - 1 False 2023-05-21 22:43:56.000000 N/A Disabled
5636 3580 notepad.exe 0xad818db45080 1 - 1 False 2023-05-21 22:46:50.000000 N/A Disabled
8920 3580 FTK Imager.exe 0xad818ef81080 20 - 1 False 2023-05-21 23:02:28.000000 N/A Disabled
```

visualizando los procesos encontrado descartamos algunos como el FTK imager y lo que se ejecutan en segundo plano en el sistema operativo nuestra aplicacion de vpn siendo **outline.exe**

```
11:54:47 csi@csi /opt/volatility3
> python3 vol.py -f /home/csi/Downloads/temp_extract_dir/MemoryDump.mem windows.pslist | grep 3580
3580 3556 explorer.exe 0xad818c047340 76 - 1 False 2023-05-21 22:30:28.000000 N/A Disabled
464 3580 SecurityHealth 0xad818979d080 3 - 1 False 2023-05-21 22:31:59.000000 N/A Disabled
3252 3580 vmtoolsd.exe 0xad8189796300 8 - 1 False 2023-05-21 22:31:59.000000 N/A Disabled
5328 3580 msedge.exe 0xad818d0980c0 54 - 1 False 2023-05-21 22:32:02.000000 N/A Disabled
6724 3580 Outline.exe 0xad818e578080 0 - 1 True 2023-05-21 22:36:09.000000 2023-05-21 23:01:24.000000 Disabled
2228 3580 FTK Imager.exe 0xad818d143080 10 - 1 False 2023-05-21 22:43:56.000000 N/A Disabled
5636 3580 notepad.exe 0xad818db45080 1 - 1 False 2023-05-21 22:46:50.000000 N/A Disabled
8920 3580 FTK Imager.exe 0xad818ef81080 20 - 1 False 2023-05-21 23:02:28.000000 N/A Disabled
```

Q4 ✔ Solved : 2777

What is the name of the process responsible for the VPN connection?

outline.exe

💡 Hints

▶ Submit

La flag: outline.exe

Flag 5

Q5 ○ Solved : 2731

What is the attacker's IP address?

💡 Hints

▶ Submit


Para buscar la direccion ip atacante utilizaremos el plugin de **netscan** y partiendo de que ya sabemos cual es el pid malicioso siendo el **5896** utilizamos el comando

Python3 vol.py -f <direccion de memoria> windows.netscan | grep 5896

```
12:17:01 csi@csi /opt/volatility3
> python3 vol.py -f /home/csi/Downloads/temp_extract_dir/MemoryDump.mem windows.netscan | grep 5896
0xad818de4aa20.0TCPv4 10.0.85.2DB scan55462f177.91.124.20 80 CLOSED 5896 oneetx.exe 2023-05-21 23:01:22.000000
```



asi aplicando este filtro encontramos la ip atacante que es la **77.91.124.20**

La flag: 77.91.124.20


Q5  Solved : 2731

What is the attacker's IP address?

77.91.124.20

 Hints  Submit

Flag 6

Q6  Solved : 2585

What is the full URL of the PHP file that the attacker visited?

URL(e.g.,http://<IP>/...)

Para encontrar la URL del cual fue descargado el malware primero me propuse a buscar el usuario desde donde se descargó con el comando

Python3 vol.py -f <direccion de memoria> windows.sessions

para ver todos los usuarios del sistema

```

- 5340 msedge.exe - 2023-05-21 22:32:39.000000
- 5704 RuntimeBroker. DESKTOP-2HF6AEV/Tammam 2023-05-21 22:32:44.000000
- 1764 dllhost.exe - 2023-05-21 22:32:48.000000
- 1916 SearchApp.exe - 2023-05-21 22:33:05.000000
- 7312 ApplicationFra DESKTOP-2HF6AEV/Tammam 2023-05-21 22:35:44.000000
- 6724 Outline.exe - 2023-05-21 22:36:09.000000
- 4224 Outline.exe - 2023-05-21 22:36:23.000000
- 7160 SearchApp.exe - 2023-05-21 22:39:13.000000
- 4628 tun2socks.exe - 2023-05-21 22:40:10.000000
- 6048 taskhostw.exe - 2023-05-21 22:40:20.000000
- 8264 RuntimeBroker. - 2023-05-21 22:40:33.000000
- 6644 SkypeApp.exe - 2023-05-21 22:41:52.000000
- 5656 RuntimeBroker. - 2023-05-21 21:58:19.000000
- 8952 TextInputHost. DESKTOP-2HF6AEV/Tammam 2023-05-21 21:59:11.000000
- 5808 HxTsr.exe - 2023-05-21 21:59:58.000000
- 2388 msedge.exe - 2023-05-21 22:05:35.000000
- 6292 msedge.exe - 2023-05-21 22:06:15.000000
- 3876 taskhostw.exe - 2023-05-21 22:08:02.000000
- 372 SkypeBackgroun - 2023-05-21 22:10:00.000000
- 6076 ShellExperienc - 2023-05-21 22:11:36.000000
- 7336 RuntimeBroker. - 2023-05-21 22:11:39.000000
- 7964 msedge.exe - 2023-05-21 22:22:09.000000
- 6544 msedge.exe - 2023-05-21 22:22:35.000000
- 8896 msedge.exe - 2023-05-21 22:28:21.000000
- 5156 msedge.exe - 2023-05-21 22:28:22.000000
- 5896 oneetx.exe - 2023-05-21 22:30:56.000000
- 7732 rundll32.exe - 2023-05-21 22:31:53.000000
- 2228 FTK Imager.exe - 2023-05-21 22:43:56.000000
- 5636 notepad.exe - 2023-05-21 22:46:50.000000
- 7540 smartscreen.ex DESKTOP-2HF6AEV/Tammam 2023-05-21 23:02:26.000000
- 8920 FTK Imager.exe DESKTOP-2HF6AEV/Tammam 2023-05-21 23:02:28.000000
- 5480 oneetx.exe - 2023-05-21 23:03:00.000000
/A - 1280 MemCompression - 2023-05-21 22:27:49.000000

```

El usuario llamado **Tammam**

Luego decide buscarlo a través de los filtros con **strings y grep**

Filtre teniendo estos parámetros en mente

La IP atacante 77.91.124.20


Siendo el comando **strings memoryDump.mem | grep 77.91.124.20**

```

> strings MemoryDump.mem | grep 77.91.124.20
http://77.91.124.20/ E
77.91.124.20/stor
http://77.91.124.20/store/gamel
http://77.91.124.20/store/games/i
77.91.124.20
http://77.91.124.20/ E
http://77.91.124.20/DSC01491/
77.91.124.20
http://77.91.124.20/DSC01491/
http://77.91.124.20/store/games/index.php
77.91.124.20
77.91.124.20
77.91.124.20
77.91.124.20
77.91.124.20
http://77.91.124.20/store/games/index.php
http://77.91.124.20/store/games/index.php



```

La flag: **http://77.91.124.20/store/games/index.php**


Q6  Solved : 2586

What is the full URL of the PHP file that the attacker visited?

URL(e.g.,http://<IP>/...)



 Hints  Submit

Flag 7

Q7  Solved : 2569

What is the full path of the malicious executable?

FilePath(e.g., C:\U...*.exe)


 Hints  Submit

para encontrar esta flag observando que nos pide el full path del ejecutable malicioso utilizaremos el plugin de volatilité llamado **File.scan** y filtrado por el nombre de nuestro programa malicioso siendo **oneetx.exe**

Python3 vol.py -f <direccion de memoria> windows.filescan | grep oneetx.exe



```
12:53:56 csi@csi /opt/volatility3
> python3 vol.py -f /home/csi/Downloads/temp_extract_dir/MemoryDump.mem windows.filescan | grep oneetx.exe
0xad818d436c70 0 Users\Tammam\AppData\Local\Temp\c3912af058\oneetx.exe 216
0xad818da36c30 0 Users\Tammam\AppData\Local\Temp\c3912af058\oneetx.exe 216
0xad818ef1a0b0 0 Users\Tammam\AppData\Local\Temp\c3912af058\oneetx.exe 216
```

la flag: C:\Users\Tammam\AppData\Local\Temp\c3912af058\oneetx.exe

Q7  Solved : 2570

What is the full path of the malicious executable?

FilePath(e.g., C:\U...*.exe)

 Hints  Submit

