RedLine Challenge

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 involve identifying the specific malware family employed in the attack, along with its characteristics. Additionally, your task is to identify and mitigate any traces or footprints left by the attacker.

Task 1:
What is the name of the suspicious process?

I checked the windows.pstree.PsTree plugin and found a weird process with suspicious path

```
5896    8844    oneetx.exe      0xad8189041080  5       -       1       True    2023-05-21 22:30:56.000000      N/A     \Device\HarddiskVolume3\Users\Tamman\AppData\Local\Temp\c3912af058\oneetx.exe
* 7732  5896    rundll32.exe    0xad818d1912c0  1       -       1       True    2023-05-21 22:31:53.000000      N/A     \Device\HarddiskVolume3\Windows\SysWOW64\rundll32.exe   -       -
```

Answer: oneetx.exe

Task 2:
What is the child process name of the suspicious process?

Same like task 1

```
5896    8844    oneetx.exe      0xad8189041080  5       -       1       True    2023-05-21 22:30:56.000000      N/A     \Device\HarddiskVolume3\Users\Tamman\AppData\Local\Temp\c3912af058\oneetx.exe
* 7732  5896    rundll32.exe    0xad818d1912c0  1       -       1       True    2023-05-21 22:31:53.000000      N/A     \Device\HarddiskVolume3\Windows\SysWOW64\rundll32.exe   -       -
```

Answer: rundll32.exe

Task 3:
What is the memory protection applied to the suspicious process memory region?

I used the windows.malfind.MalFind plugin on the oneetx.exe PID

```
remnux@remnux:~/volatility3$ python3 vol.py -f '/home/remnux/Challenge/MemoryDump.mem' windows.malfind.Malfind --pid 5896
Volatility 3 Framework 2.7.0
Progress:  100.00               PDB scanning finished
PID     Process Start VPN       End VPN Tag     Protection      CommitCharge    PrivateMemory   File output     Notes   Hexdump Disasm

5896    oneetx.exe      0x400000        0x437fff        VadS    PAGE_EXECUTE_READWRITE  56      1       Disabled        MZ header
4d 5a 90 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 ........
80 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
```

Answer: PAGE_EXECUTE_READWRITE

Task 4:
What is the name of the process responsible for the VPN connection?

I checked the windows.netscan.NetScan plugin and saw the malicious process oneetx.exe and also another process that initiataed a connection to 2 IP addresses

```
0xad818de4aa20  TCPv4   10.0.85.2       55462   77.91.124.20    80      CLOSED  5896    oneetx.exe      2023-05-21 23:01:22.000000
0xad818dfld920  TCPv4   192.168.190.141 55433   38.121.43.65    443     CLOSED  4628    tun2socks.exe   2023-05-21 23:08:02.000000
```

I thought the answer will be tun2socks.exe but it was wrong so I checked inside the pstree which PID is associated too

```
*** 6724        3580    Outline.exe     0xad818e578080  0       -       1       True    2023-05-21 22:36:09.000000      2023-05-21 23:01:24.000000      \Device\HarddiskVolume3\Program Files (x86)\Outline\Outline.exe -       -
**** 4224       6724    Outline.exe     0xad818e88b080  0       -       1       True    2023-05-21 22:36:23.000000      2023-05-21 23:01:24.000000      \Device\HarddiskVolume3\Program Files (x86)\Outline\Outline.exe -       -
**** 4628       6724    tun2socks.exe   0xad818de82340  0       -       1       True    2023-05-21 22:40:10.000000      2023-05-21 23:01:24.000000      \Device\HarddiskVolume3\Program Files (x86)\Outline\resources\app.asar.unpacked\third_party\outline-go-tun2socks\win32\tun2socks.e
xe      -       -
```

Answer: Outline.exe

Task 5:
What is the attacker's IP address?

I checked the windows.netscan.NetScan plugin and noticed the oneetx.exe connection

```
0xad818de4aa20  TCPv4   10.0.85.2       55462   77.91.124.20    80      CLOSED  5896    oneetx.exe      2023-05-21 23:01:22.000000
0xad818dfld920  TCPv4   192.168.190.141 55433   38.121.43.65    443     CLOSED  4628    tun2socks.exe   2023-05-21 23:08:02.000000
```

Answer: 77.91.124.20

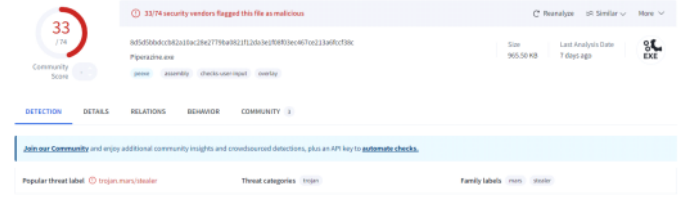
Task 6:
Based on the previous artifacts. What is the name of the malware family?

I used the windows.filescan.FileScan and grepped for the malicious file oneetx.exe and then dumped it and checked for the MD5 inside Virus Total

```
remnux@remnux:~/volatility3$ python3 vol.py -f '/home/remnux/Challenge/MemoryDump.mem' windows.filescan.FileScan | grep -i oneetx
0xad818d436c70.0\Users\Tamman\AppData\Local\Temp\c3912af058\oneetx.exe  216
0xad818da36c30  \Users\Tamman\AppData\Local\Temp\c3912af058\oneetx.exe  216
0xad818efla0b0  \Users\Tamman\AppData\Local\Temp\c3912af058\oneetx.exe  216
```

```
remnux@remnux:~/volatility3$ python3 vol.py -f '/home/remnux/Challenge/MemoryDump.mem' windows.dumpfiles.DumpFiles --virtaddr=0xad818d436c70
Volatility 3 Framework 2.7.0
Progress:  100.00               PDB scanning finished
Cache   FileObject      FileName        Result

ImageSectionObject      0xad818d436c70  oneetx.exe      file.0xad818d436c70.0xad818ca48660.ImageSectionObject.oneetx.exe.img
```



I didn't find specific name but I assumed because the challenge called Redline and a lot of the reports on Virus Total classified this malware as a stealer I thought the answer will be redline stealer

Answer: redline stealer

Task 7:
What is the full URL of the PHP file that the attacker visited?

I saw that the answer format is contain an IP address so I assumed the IP address is the same from the attacker IP so I used strings on the memory dump and grepped for the attacker IP 77.91.124.20

```
remnux@remnux:~/Challenge$ 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
ttp://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
```

Answer: http://77.91.124.20/store/games/index.php

Task 8:
What is the full path of the malicious executable?

I used the windows.filescan.FileScan and grepped for the malicious file oneetx.exe

```
remnux@remnux:~/volatility3$ python3 vol.py -f '/home/remnux/Challenge/MemoryDump.mem' windows.filescan.FileScan | grep -i oneetx
0xad818d436c70.0\Users\Tamnam\AppData\Local\Temp\c3912af058\oneetx.exe  216
0xad818da36c30  \Users\Tamnam\AppData\Local\Temp\c3912af058\oneetx.exe  216
0xad81efla8b0  \Users\Tamnam\AppData\Local\Temp\c3912af058\oneetx.exe  216
```

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