RedLine Lab (Cyber Defenders) - Walkthrough

Thursday, September 19, 2024 8:03 AM

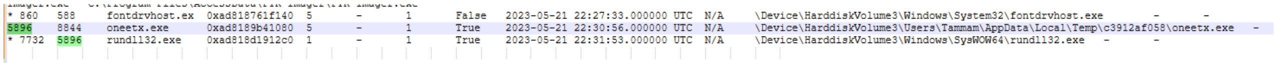
Story: As a member of the Security Blue team, your assignment is to analyze a memory dump using Redline and Volatility tools. Your goal is to trace the steps taken by the attacker on the compromised machine and determine how they managed to bypass the Network Intrusion Detection System "NIDS". Your investigation 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.

Q1: What is the name of the suspicious process?

- To investigate this issue, I utilized the 'Windows.Pstree' plugin to display the process tree. The final process, '**oneetx.exe**,' appears suspicious due to its execution path: C:\Users\Tammam \AppData\Local\Temp\c3912af058\oneetx.exe.
  This location in the Temp folder raises concerns about its legitimacy.

Q2: What is the child process name of the suspicious process?

- The PID of the malicious process is '**5896**', and it was followed by the execution of 'rundll32.exe,' which was initiated by its parent process, '5896'. This indicates a potential chain of malicious activity, with 'oneetx.exe' likely being used to launch 'rundll32.exe' for further execution.



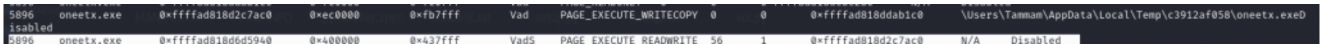
```
* 860   588    fontdrvhost.ex  0xad818761f140  5    -    1      False   2023-05-21 22:27:33.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\fontdrvhost.exe       -       -
5896    8844   oneetx.exe      0xad8189b41080  5    -    1      True    2023-05-21 22:30:56.000000 UTC  N/A     \Device\HarddiskVolume3\Users\Tammam\AppData\Local\Temp\c3912af058\oneetx.exe   -
* 7732  5896   rundll32.exe    0xad818d1912c0  1    -    1      True    2023-05-21 22:31:53.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\SysWOW64\rundll32.exe   -       -
```

Q3:What is the memory protection applied to the suspicious process memory region?

- A memory region is a block of a program's memory used for specific tasks. Each program, when running, needs memory to store things like code, data, and temporary variables. These different parts of memory are divided into "regions."

  In malware analysis, looking at the memory regions can help you see if something suspicious is happening, like code being run from a region that should only store data.

  If you see a memory region with permissions like READ, WRITE, and EXECUTE all together **(PAGE_EXECUTE_READWRITE)**, that can be suspicious because malware might inject code into that region and execute it. Regular programs don't usually need to modify executable code during runtime.



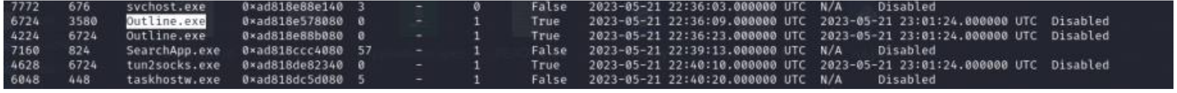
```
5896    oneetx.exe     0xffffad818d2c7ac0      0xec0000      0xfb7fff      Vad     PAGE_EXECUTE_WRITECOPY  0      0       0xffffad818ddab1c0      \Users\Tammam\AppData\Local\Temp\c3912af058\oneetx.exeD
isabled
5896    oneetx.exe     0xffffad818d6d5940      0x400000      0x437fff      VadS    PAGE_EXECUTE_READWRITE  56     1       0xffffad818d2c7ac0      N/A     Disabled
```

  5896: The process ID (PID) of oneetx.exe.
  0xffffad818d6d5940: The kernel memory address of the process.
  0x400000 - 0x437fff: The virtual memory range being analyzed.
  VadS: This indicates the region is part of the Virtual Address Descriptor (VAD).
  PAGE_EXECUTE_READWRITE: This is the memory protection setting, allowing reading, writing, and executing code in this region.

  The memory region allocated to oneetx.exe has the protection flag PAGE_EXECUTE_READWRITE. This means the process can **read**, **write**, and **execute** code in this region. Such permissions are unusual and suspicious because it allows the process to modify code and then execute it

Q4: What is the name of the process responsible for the VPN connection?

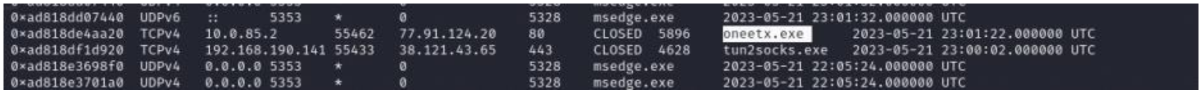
- I used the 'Pslist' plugin to identify the processes running on the machine. Among them, I found the process Outline.exe, which is associated with a VPN service.



```
7772    676     svchost.exe     0xad818e88e140  3     -     0     False   2023-05-21 22:36:03.000000 UTC  N/A     Disabled
6724    3580    Outline.exe     0xad818e578080  0     -     1     True    2023-05-21 22:36:09.000000 UTC  2023-05-21 23:01:24.000000 UTC  Disabled
4224    6724    Outline.exe     0xad818e88b080  0     -     1     True    2023-05-21 22:36:23.000000 UTC  2023-05-21 23:01:24.000000 UTC  Disabled
7160    824     SearchApp.exe   0xad818ccc4080  57    -     1     False   2023-05-21 22:39:13.000000 UTC  N/A     Disabled
4628    6724    tun2socks.exe   0xad818de82340  0     -     1     True    2023-05-21 22:40:10.000000 UTC  2023-05-21 23:01:24.000000 UTC  Disabled
6048    448     taskhostw.exe   0xad818dc5d080  5     -     1     False   2023-05-21 22:40:20.000000 UTC  N/A     Disabled
```

Q5:What is the attacker's IP address?

- I used the 'Netscan' plugin to identify suspicious network connections and noticed that the malicious process oneetx.exe was connected to the IP address **77.91.124.20**, which is likely the attacker's command and control server.



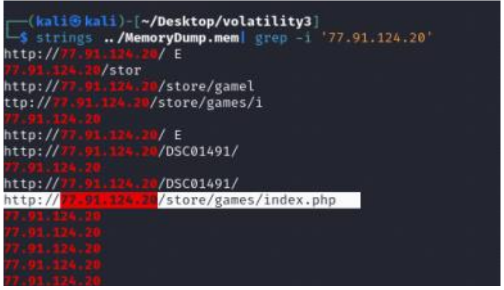
```
0xad818dd07440  UDPv6   ::      5353    *       0               5328    msedge.exe      2023-05-21 23:01:32.000000 UTC
0xad818de4aa20  TCPv4   10.0.85.2       55462   77.91.124.20    80      CLOSED  5896    oneetx.exe      2023-05-21 23:01:22.000000 UTC
0xad818df1d920  TCPv4   192.168.190.141 55433   38.121.43.65    443     CLOSED  4628    tun2socks.exe   2023-05-21 23:00:02.000000 UTC
0xad818e3698f0  UDPv4   0.0.0.0 5353    *       0               5328    msedge.exe      2023-05-21 22:05:24.000000 UTC
0xad818e3701a0  UDPv4   0.0.0.0 5353    *       0               5328    msedge.exe      2023-05-21 22:05:24.000000 UTC
```

Q6: Based on the previous artifacts. What is the name of the malware family?

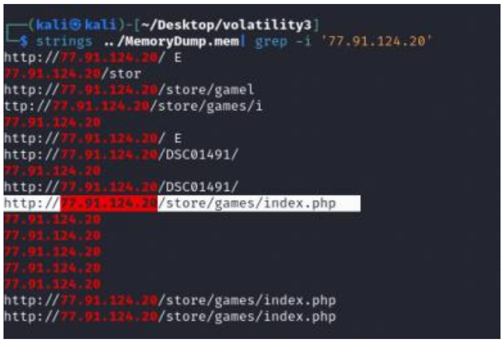
- Based on the challenge name "ReadLine," it can be inferred that the malware family is likely "RedLine Stealer." To analyze it further, you should dump the process and then check the dumped file using VirusTotal

Q7: What is the full URL of the PHP file that the attacker visited?

- To address this question, I used 'strings' utility and filtered the attacker IP



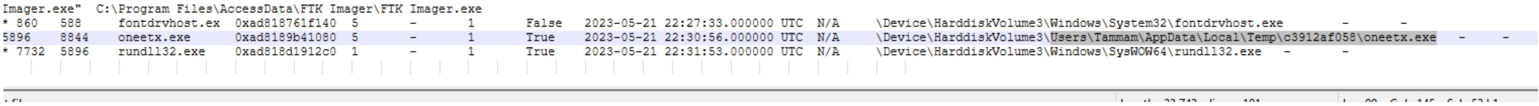
```
┌──(kali㉿kali)-[~/Desktop/volatility3]
└─$ strings ../MemoryDump.mem| grep -i '77.91.124.20'
http://77.91.124.20/ E
77.91.124.20/stor
http://77.91.124.20/store/gamel
ttp://77.91.124.20/store/games/i
77.91.124.20
http://77.91.124.20/ E
http://77.91.124.20/DSC01491/
77.91.124.20
http://77.91.124.20/DSC01491/
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
```



```
┌──(kali㉿kali)-[~/Desktop/volatility3]
└─$ strings ../MemoryDump.mem| grep -i '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
```

Q8: What is the full path of the malicious executable?

- We already found the path in the process tree at the beginning of challenge.



```
Imager.exe"  C:\Program Files\AccessData\FTK Imager\FTK Imager.exe
* 860    588     fontdrvhost.ex  0xad818761f140  5       -       1       False   2023-05-21 22:27:33.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\fontdrvhost.exe        -       -
5896     8844    oneetx.exe      0xad8189b41080  5       -       1       True    2023-05-21 22:30:56.000000 UTC  N/A     \Device\HarddiskVolume3\Users\Tammam\AppData\Local\Temp\c3912af058\oneetx.exe   -       -
* 7732   5896    rundll32.exe    0xad818d1912c0  1       -       1       True    2023-05-21 22:31:53.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\SysWOW64\rundll32.exe   -       -
```