RedLine Lab
Analyst: Ruslan
Date: 2026-01-26

Overview

A detailed analysis was conducted on a memory dump extracted from a compromised system. This report outlines the key findings and provides insights into the attacker’s activities, malicious processes, and network interactions. The analysis was carried out using Volatility framework to investigate the system’s memory for any suspicious processes, child processes, network activity, and potential malicious files.

1. Suspicious Process Identification:

The primary suspicious process discovered during the memory analysis is oneetx.exe. This executable was flagged as potentially malicious due to its uncommon presence and behavior. The process was found during the execution of commands such as windows.pstree and windows.malfind. The windows.pstree command revealed the process tree, showing oneetx.exe running in the system memory. The process’s integrity was further questioned by conducting a hash check on the associated files, which confirmed its suspicious nature.

2. Child Process of the Suspicious Process:

In examining the process tree for oneetx.exe, it was revealed that the suspicious process spawned a child process, rundll32.exe. This Windows utility, when used by legitimate processes, is often exploited by attackers to run malicious code. The child process was traced by using the windows.pstree command, which showed that it was launched by the parent oneetx.exe process.

3. Memory Protection of the Malicious Process:

The memory region in which oneetx.exe was executing was protected with PAGE_EXECUTE_READWRITE memory protection. This setting allows the process to execute, read, and write within the same memory region, which is commonly used by malicious software. This type of protection is often associated with memory injection techniques, allowing an attacker to modify and execute their code undetected.

4. VPN Process Identification:

An analysis of the memory dump also revealed a process responsible for a VPN connection. The process identified was Outline.exe, which is often used to mask network traffic and potentially facilitate the attacker's communication with the compromised system. While VPNs are used for legitimate purposes, in this case, its presence suggests that the attacker may have used it to conceal their activities.

5. Attacker's IP Address:

The network scan conducted through the windows.netscan plugin revealed the IP address associated with the attacker. This address was active during the attack, likely being used for Command and Control (C2) communication with the infected system. By tracing the IP address, the investigator identified that it was linked to malicious activities involving the attacker’s infrastructure.

6. Malicious URL Accessed by the Attacker:

Further inspection of the memory dump using the strings command revealed a PHP file URL that the attacker accessed. The URL was associated with the IP address 77.91.124.20, and it appears that the attacker visited this remote server to potentially exploit the system or upload additional malicious payloads.

7. Full Path of the Malicious Executable:

The full path of the malicious executable oneetx.exe was found within the system's temporary directory. The windows.filescan command was used to scan the file system and identify the location of the file. This path is consistent with typical malware deployment methods, where files are placed in temporary directories to avoid detection by the system.

Conclusion:

The analysis of the memory dump provided critical insights into the nature of the attack. The presence of oneetx.exe, its associated child process rundll32.exe, and the abnormal memory protection settings strongly suggest that this was a targeted attack, likely involving malware. The attacker used a VPN (Outline.exe) to mask their activities and accessed a remote server to further exploit the system. Additionally, the attacker's IP address 77.91.124.20 was actively involved in the attack, and the attacker accessed a PHP file to further compromise the system. The malicious executable was located in a temporary directory, which is typical of files used in malicious operations.

1. What is the name of the suspicious process?

To identify suspicious processes, we need to search through the memory dump using tools like windows.pstree to list running processes. A command like md5sum can help verify the integrity of suspicious files. Here, the suspicious process is identified as oneetx.exe based on the memory and file analysis. This file could be indicative of malware, as it does not correspond to any known legitimate process in the system.

```
ruslan@pop-os:~/Downloads/106-RedLine/temp_extract_dir$ vol -f MemoryDump.mem windows.info
Volatility 3 Framework 2.28.0
Progress:  100.00               PDB scanning finished
Variable        Value

Kernel Base     0xf8076221a000
DTB     0x1ad000
Symbols file:///home/ruslan/.local/pipx/venvs/volatility3/lib/python3.10/site-packages/volatility3/symbols/windows/ntkrnlmp.pdb/68A17FAF3012B7846079AEECDBE0A583-1.json.xz
Is64Bit True
IsPAE   False
layer_name      0 WindowsIntel32e
memory_layer    1 FileLayer
KdVersionBlock  0xf80762e29398
Major/Minor     15.19041
MachineType     34404
KeNumberProcessors      4
SystemTime      2023-05-21 23:02:39+00:00
NtSystemRoot    C:\Windows
NtProductType   NtProductWinNt
NtMajorVersion  10
NtMinorVersion  0
PE MajorOperatingSystemVersion  10
PE MinorOperatingSystemVersion  0
PE Machine      34404
PE TimeDateStamp        Wed Jun 28 04:14:26 1995
```

vol -f MemoryDump.mem windows.pstree

```
** 3004 676     svchost.exe     0xad818c4212c0  7       -       0       False   2023-05-21 22:30:55.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\svchost.exe    C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation -p
** 448  676     svchost.exe     0xad8187212401  54      -       0       False   2023-05-21 22:27:41.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\svchost.exe    C:\Windows\system32\svchost.exe -k netsvcs -p
*** 1600        448     taskhostw.exe   0xad8189d07300  10      -       1       False   2023-05-21 22:30:09.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\taskhostw.exe  -       -
*** 6048        448     taskhostw.exe   0xad818dc5d080  5       -       1       False   2023-05-21 22:40:20.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\taskhostw.exe  -       -
*** 3876        448     taskhostw.exe   0xad8189b30080  8       -       1       False   2023-05-21 22:08:02.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\taskhostw.exe  -       -
*** 5480        448     oneetx.exe      0xad818d3d6080  6       -       1       True    2023-05-21 23:03:00.000000 UTC  N/A     \Device\HarddiskVolume3\Users\Tammam\AppData\Local\Temp\c3912af058\oneetx.exe -       -
```

vol -f MemoryDump.mem windows.malfind

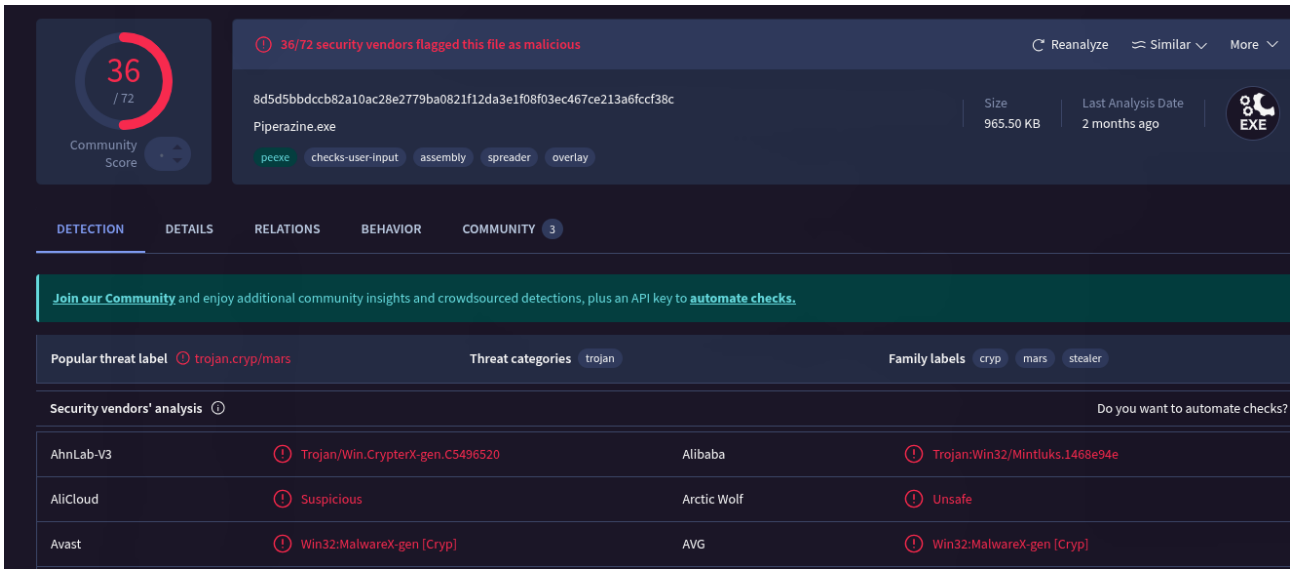
```
PID     Process Start VPN       End VPN Tag     Protection      CommitCharge    PrivateMemory   File output     Notes   Hexdump Disasm
/home/ruslan/.local/pipx/venvs/volatility3/lib/python3.10/site-packages/volatility3/framework/deprecation.py:105: FutureWarning: This p
 been renamed and will be removed in the first release after 2026-06-07. Please ensure all method calls to this plugin are replaced wit
Malfind
  warnings.warn(

5704    RuntimeBroker.  0x21ddbca0000   0x21ddbcaffff   VadS    PAGE_EXECUTE_READ       16      1       Disabled        N/A
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 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 00 00 00 00 00 00 00 00 00 00
0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
5896    oneetx.exe      0x400000        0x437fff        VadS    PAGE_EXECUTE_READWRITE  56      1       Disabled        MZ header
4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ..............
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 00 01 00 00 ................        4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00
0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00
7540    smartscreen.ex  0x2505c140000   0x2505c15ffff   VadS    PAGE_EXECUTE_READWRITE  1       1       Disabled        N/A
48 89 54 24 10 48 89 4c 24 08 4c 89 44 24 18 4c H.T$.H.L$.L.D$.L
89 4c 24 20 48 8b 41 28 48 8b 48 08 48 8b 51 50 .L$ H.A(H.H.H.QP
48 83 e2 f8 48 8b ca 48 b8 60 00 14 5c 50 02 00 H...H..H.`..\P..
00 48 2b c8 48 81 f9 70 0f 00 00 76 09 48 c7 c1 .H+.H..p...v.H..        48 89 54 24 10 48 89 4c 24 08 4c 89 44 24 18 4c 89 4c 24 20 48
8 b8 60 00 14 5c 50 02 00 00 48 2b c8 48 81 f9 70 0f 00 00 76 09 48 c7 c1
```

vol -f MemoryDump.mem windows.dumpfile --pid 5896

```
ImageSectionObject      0xad818e37b8e0  AcLayers.dll    file.0xad818e37b8e0.0xad818ea09d00.ImageSectionObject.AcLayers.dll.img
ImageSectionObject      0xad818da36c30  oneetx.exe      file.0xad818da36c30.0xad818ca48660.ImageSectionObject.oneetx.exe.img
ImageSectionObject      0xad818e48a450  sfc.dll Error dumping file
```

md5sum file.0xad818da36c30.0xad818ca48660.ImageSectionObject.oneetx.exe.img

```
ruslan@pop-os:~/Downloads/106-RedLine/temp_extract_dir$ md5sum file.0xad818da36c30.0xad818ca48660.ImageSectionObject.oneetx.exe.img
f40168cc10f8cb6fe05322fc391e6947  file.0xad818da36c30.0xad818ca48660.ImageSectionObject.oneetx.exe.img
ruslan@pop-os:~/Downloads/106-RedLine/temp_extract_dir$
```



Answer: oneetx.exe

After identifying the suspicious parent process (oneetx.exe), we can use the windows.pstree command to view the process tree and trace its child processes. The grep command helps filter the process ID (PID) of the parent process, revealing the child process. Here, the child process associated with oneetx.exe is rundll32.exe, which could indicate further malicious activity or an attempt to execute malicious code in a legitimate process.

2. What is the child process name of the suspicious process?

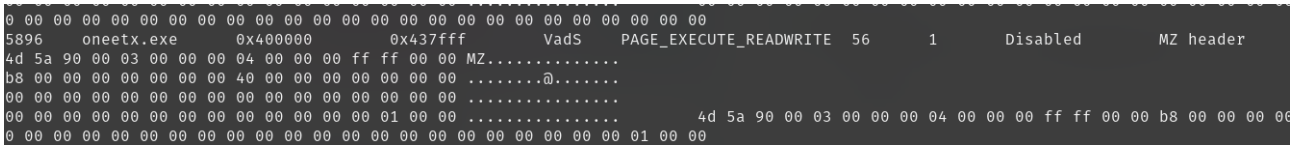
vol -f MemoryDump.mem windows.pstree | grep "5896"

Answer: rundll32.exe

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

The windows.malfind command helps locate suspicious memory regions where malicious code may be executing. One of the key indicators of malicious activity is the memory protection applied to the process. In this case, PAGE_EXECUTE_READWRITE protection means that the memory region can be read, written to, and executed. This is a common characteristic of malicious processes as it allows the attacker to modify and execute code in memory.

vol -f MemoryDump.mem windows.malfind

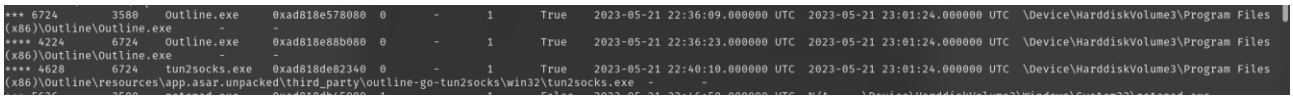


Answer: PAGE_EXECUTE_READWRITE

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

This command examines the memory dump to find processes related to network connections. By analyzing the process tree, we can identify processes that may be associated with a VPN. In this case, Outline.exe is identified as the process responsible for maintaining the VPN connection. This could be a legitimate or malicious VPN tool, depending on the context.

vol -f MemoryDump.mem windows.pstree



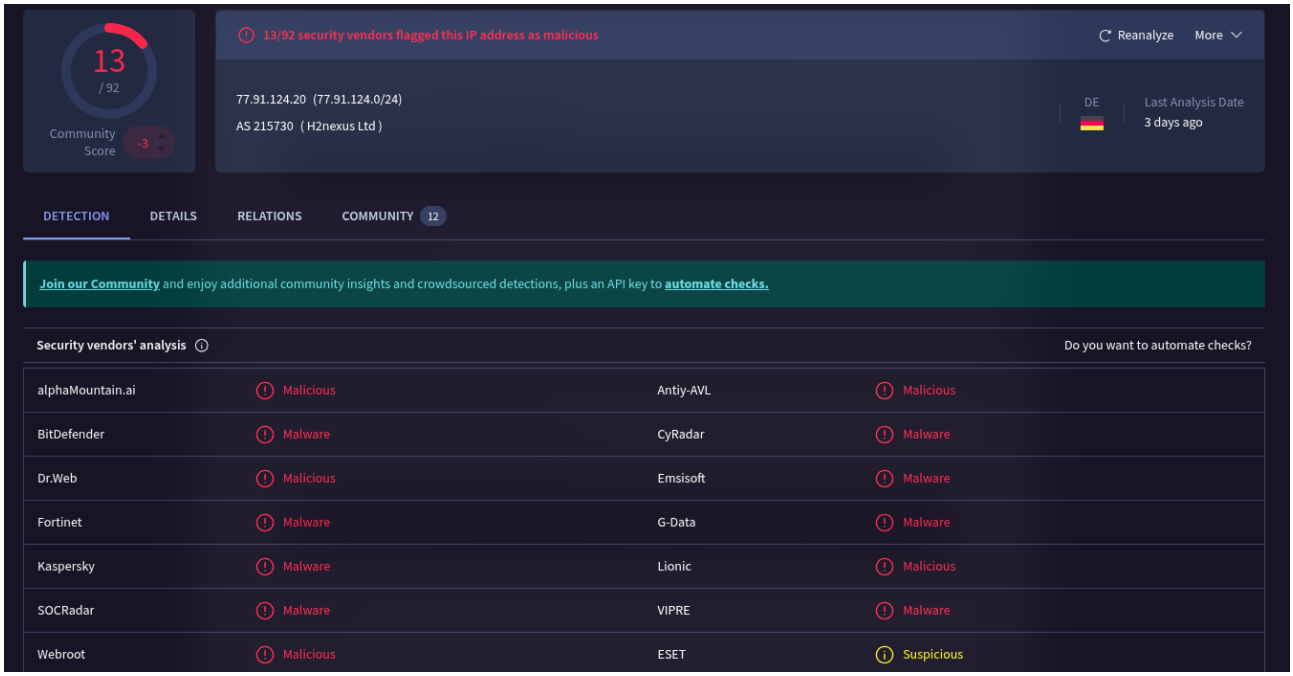
Answer: Outline.exe

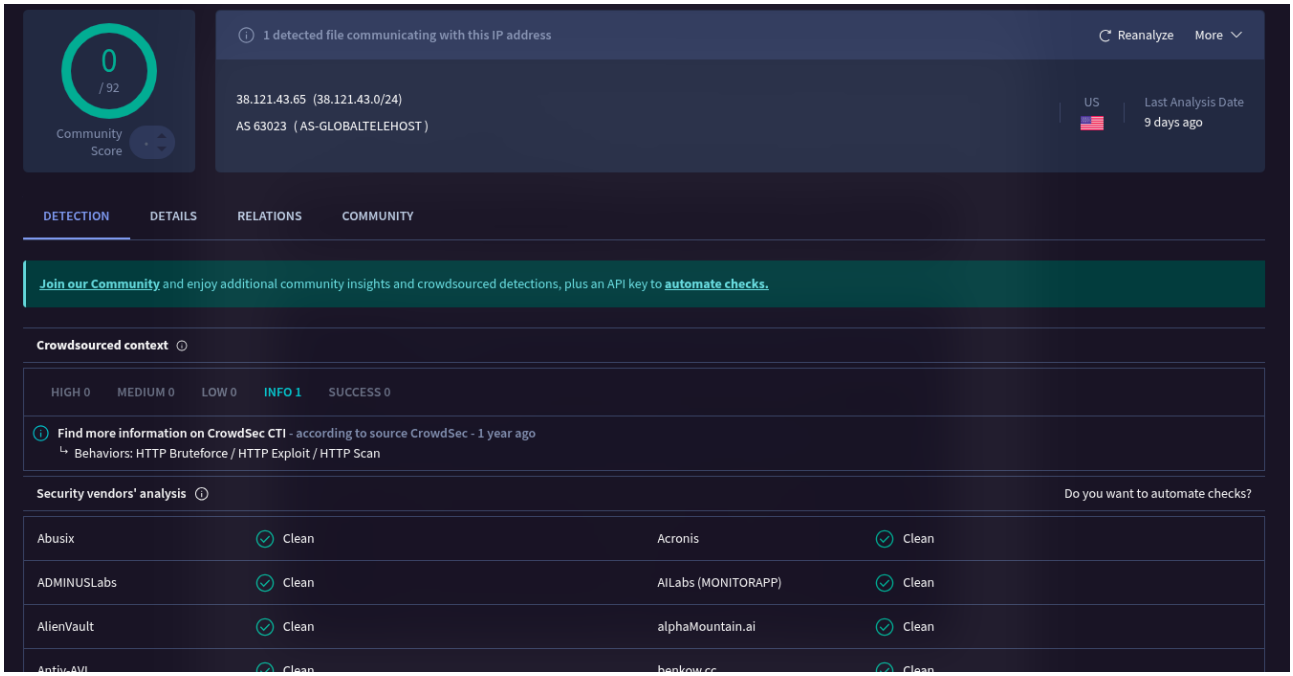
5. What is the attacker's IP address?

The windows.netscan command is used to scan the memory for network activity, such as active connections or open ports. The attacker's IP address can be identified by analyzing the network traffic and correlating it with suspicious activity. In this case, the attacker's IP address is 77.91.124.20, which can be used for further investigation.

vol -f MemoryDump.mem windows.netscan

```
0xad818dd07440  UDPv4   0.0.0.0 5353    *       0               5328    msedge.exe      2023-05-21 23:01:32.000000 UTC
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
```





Answer: 77.91.124.20

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

The strings command is used to extract readable strings from a memory dump, and grep filters the strings related to the attacker's IP address. By analyzing these strings, we can identify the URL that the attacker visited, which is crucial for understanding the attack vector. Here, the attacker accessed a PHP file at the URL http://77.91.124.20/store/games/index.php.

strings MemoryDump.mem | grep "77.91.124.20"

```
ruslan@pop-os:~/Downloads/106-RedLine/temp_extract_dir$ 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

7. What is the full path of the malicious executable?

The windows.filescan command is used to identify files in the system, and filtering it with the filename oneetx.exe helps us locate the exact location of the malicious executable. Alternatively, the windows.pstree command can provide insights into the file path by tracing the processes. The full path of the malicious executable in this case is C:\Users\Tammam\AppData\Local\Temp\c3912af058\oneetx.exe.

vol -f MemoryDump.mem windows.filescan | grep "oneetx.exe"

```
ruslan@pop-os:~/Downloads/106-RedLine/temp_extract_dir$ vol -f MemoryDump.mem windows.filescan | grep "oneetx.exe"
0xad818d436c70.0\Users\Tammam\AppData\Local\Temp\c3912af058\oneetx.exe
0xad818da36c30  \Users\Tammam\AppData\Local\Temp\c3912af058\oneetx.exe
0xad818ef1a0b0  \Users\Tammam\AppData\Local\Temp\c3912af058\oneetx.exe
```

or we see it from windows.pstree

```
** 3004 676     svchost.exe     0xad818c4212c0  7       -       0       False   2023-05-21 22:30:55.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\svchost.exe    C:\Windows\sys
tem32\svchost.exe -k LocalServiceAndNoImpersonation -p  C:\Windows\system32\svchost.exe
** 448  676     svchost.exe     0xad8187721240  54      -       0       False   2023-05-21 22:27:41.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\svchost.exe    C:\Windows\sys
tem32\svchost.exe -k netsvcs -p C:\Windows\system32\svchost.exe
*** 1600        448     taskhostw.exe   0xad8189d07300  10      -       1       False   2023-05-21 22:30:09.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\taskhostw.exe  -       -
*** 6048        448     taskhostw.exe   0xad818dc5d080  5       -       1       False   2023-05-21 22:40:20.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\taskhostw.exe  -       -
*** 3876        448     taskhostw.exe   0xad8189b30080  8       -       1       False   2023-05-21 22:08:02.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\taskhostw.exe  -       -
*** 5480        448     oneetx.exe      0xad818d3d6080  6       -       1       True    2023-05-21 23:03:00.000000 UTC  N/A     \Device\HarddiskVolume3\Users\Tammam\AppData\Local\Temp\c3912a
f058\oneetx.exe -       -
*** 1392        448     sihost.exe      0xad8189e94280  11      -       1       False   2023-05-21 22:30:08.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\sihost.exe     sihost
```

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