CyberDefenders Lab: REDLINE

Glen Taberima

```
┌──(kali㉿kali)-[~/Documents/REDLINE]
└─$ python3 ~/Documents/volatility3-2.5.0/vol.py -f MemoryDump.mem windows.info
Volatility 3 Framework 2.5.0
Progress:  100.00               PDB scanning finished
Variable        Value

Kernel Base     0×f8076221a000
DTB     0×1ad000
Symbols file:///home/kali/Documents/volatility3-2.5.0/volatility3/symbols/windows/ntkrnlmp.pdb/68A17FAF3012B7846079A
-1.json.xz
Is64Bit True
IsPAE   False
layer_name      0 WindowsIntel32e
memory_layer    1 FileLayer
KdVersionBlock  0×f80762e29398
Major/Minor     15.19041
MachineType     34404
KeNumberProcessors      4
SystemTime      2023-05-21 23:02:39
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
```

Q1.What is the name of the suspicious process?

```
┌──(kali㉿kali)-[~/Documents/REDLINE]
└─$ python3 ~/Documents/volatility3-2.5.0/vol.py -f MemoryDump.mem windows.pslist
```

```
5480    448     oneetx.exe      0×ad818d3d6080  6       -       1       True    2023-05-21 23:03:00.000000      N/AD
isabled
```

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

```
5896    8844    oneetx.exe      0×ad8189b41080  5       -       1       True    2023-05-21 22:30:56.000000      N/A
* 7732  5896    rundll32.exe    0×ad818d1912c0  1       -       1       True    2023-05-21 22:31:53.000000      N/A
```

ANS: rundll32.exe

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

python3 ~/Documents/volatility3-2.5.0/vol.py -f MemoryDump.mem windows.malfind

CyberDefenders Lab: REDLINE

Glen Taberima

```
PID    Process Start VPN       End VPN Tag     Protection      CommitCharge    PrivateMemory   File output     Hexdump Disasm

5896    oneetx.exe      0×400000        0×437fff        VadS    PAGE_EXECUTE_READWRITE  56      1       Disabled
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 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 01 00 00 ........
0×400000:       dec     ebp
0×400001:       pop     edx
0×400002:       nop
0×400003:       add     byte ptr [ebx], al
0×400005:       add     byte ptr [eax], al
0×400007:       add     byte ptr [eax + eax], al
0×40000a:       add     byte ptr [eax], al
7540    smartscreen.ex  0×2505c140000   0×2505c15ffff   VadS    PAGE_EXECUTE_READWRITE  1       1       Disabled
48 89 54 24 10 48 89 4c H.T$.H.L
24 08 4c 89 44 24 18 4c $.L.D$.L
89 4c 24 20 48 8b 41 28 .L$.H.A(
48 8b 48 08 48 8b 51 50 H.H.H.QP
48 83 e2 f8 48 8b ca 48 H...H..H
b8 60 00 14 5c 50 02 00 .`..\P..
00 48 2b c8 48 81 f9 70 .H+.H..p
0f 00 00 76 09 48 c7 c1 ...v.H..
0×2505c140000:  mov     qword ptr [rsp + 0×10], rdx
0×2505c140005:  mov     qword ptr [rsp + 8], rcx
0×2505c14000a:  mov     qword ptr [rsp + 0×18], r8
0×2505c14000f:  mov     qword ptr [rsp + 0×20], r9
0×2505c140014:  mov     rax, qword ptr [rcx + 0×28]
0×2505c140018:  mov     rcx, qword ptr [rax + 8]
0×2505c14001c:  mov     rdx, qword ptr [rcx + 0×50]
0×2505c140020:  and     rdx, 0×fffffffffffffff8
0×2505c140024:  mov     rcx, rdx
0×2505c140027:  movabs  rax, 0×2505c140060
0×2505c140031:  sub     rcx, rax
0×2505c140034:  cmp     rcx, 0×f70
0×2505c14003b:  jbe     0×2505c140046
```

ANS: protection -> PAGE_EXECUTE_READWRITE

VALIDASI:

```
└─$ python3 ~/Documents/volatility3-2.5.0/vol.py -f MemoryDump.mem windows.vadinfo --pid 5896
Volatility 3 Framework 2.5.0
Progress:  100.00               PDB scanning finished
PID     Process Offset  Start VPN       End VPN Tag     Protection      CommitCharge    PrivateMemory   Parent  File    File output

5896    oneetx.exe      0×ffffad818ddb2c40      0×73da0000      0×74024fff      Vad     PAGE_EXECUTE_WRITECOPY  554     0       0×0     \Windows\SysWOW64\AcLayers.dll  Disabled
5896    oneetx.exe      0×ffffad818ddc5200      0×1a60000       0×2e60fff       Vad     PAGE_READONLY   0       0       0×ffffad818ddb2c40      N/A     Disabled
5896    oneetx.exe      0×ffffad818d6d5b70      0×1390000       0×139ffff       VadS    PAGE_READWRITE  10      1       0×ffffad818ddc5200      N/A     Disabled
5896    oneetx.exe      0×ffffad818d6bc2b0      0×1000000       0×11fffff       VadS    PAGE_READWRITE  11      1       0×ffffad818d6d5b70      N/A     Disabled
5896    oneetx.exe      0×ffffad818ddab1c0      0×fc0000        0×fc0fff        Vad     PAGE_READONLY   0       0       0×ffffad818d6bc2b0      N/A     Disabled
5896    oneetx.exe      0×ffffad818d2c7ac0      0×ec0000        0×fb7fff        Vad     PAGE_EXECUTE_WRITECOPY  0       0       0×ffffad818ddab1c0      \Users\Tammam\AppData\Local\Temp\c3912af058\oneetx.exe  Disabled
5896    oneetx.exe      0×ffffad818d6d5940      0×400000        0×437fff        VadS    PAGE_EXECUTE_READWRITE  56      1       0×ffffad818d2c7ac0      N/A     Disabled
5896    oneetx.exe      0×ffffad818ddade20      0×fe0000        0×fe0fff        Vad     PAGE_READONLY   0       0       0×ffffad818ddab1c0      N/A     Disabled
```

HASIL VALIDASI: *The PAGE_EXECUTE_READWRITE memory protection attribute is not considered a good security practice. Allowing a memory region to be both writable and executable can introduce security risks*

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

python3 ~/Documents/volatility3-2.5.0/vol.py -f MemoryDump.mem windows.pstree

```
**  6724    3580    Outline.exe     0×ad818e578080  0       -       1       True    2023-05-21 22:36:09.000000      2023-05-21 23:01:24.000000
****  4224      6724    Outline.exe     0×ad818e88b080  0       -       1       True    2023-05-21 22:36:23.000000      2023-05-21 23:01:24.000000
****  4628      6724    tun2socks.exe   0×ad818de82340  0       -       1       True    2023-05-21 22:40:10.000000      2023-05-21 23:01:24.000000
```

ANS: outline.exe

What is the attacker's IP address?

```
└─$ python3 ~/Documents/volatility3-2.5.0/vol.py -f MemoryDump.mem windows.netscan | grep -i "oneetx.exe"
0×ad818de4aa20.0TCPv4   10.0.85.2DB scan55462fin77.91.124.20     80      CLOSED  5896    oneetx.exe      2023-05-21 23:01:22.000000
0×ad818e4a6900  UDPv4   0.0.0.0 0       *       0               5480    oneetx.exe      2023-05-21 22:39:47.000000
0×ad818e4a6900  UDPv6   ::      0       *       0               5480    oneetx.exe      2023-05-21 22:39:47.000000
0×ad818e4a9650  UDPv4   0.0.0.0 0       *       0               5480    oneetx.exe      2023-05-21 22:39:47.000000
```

CyberDefenders Lab: REDLINE

Glen Taberima

ANS: 77.91.124.20

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

python3 ~/Documents/volatility3-2.5.0/vol.py -f MemoryDump.mem windows.dumpfile --pid 5896

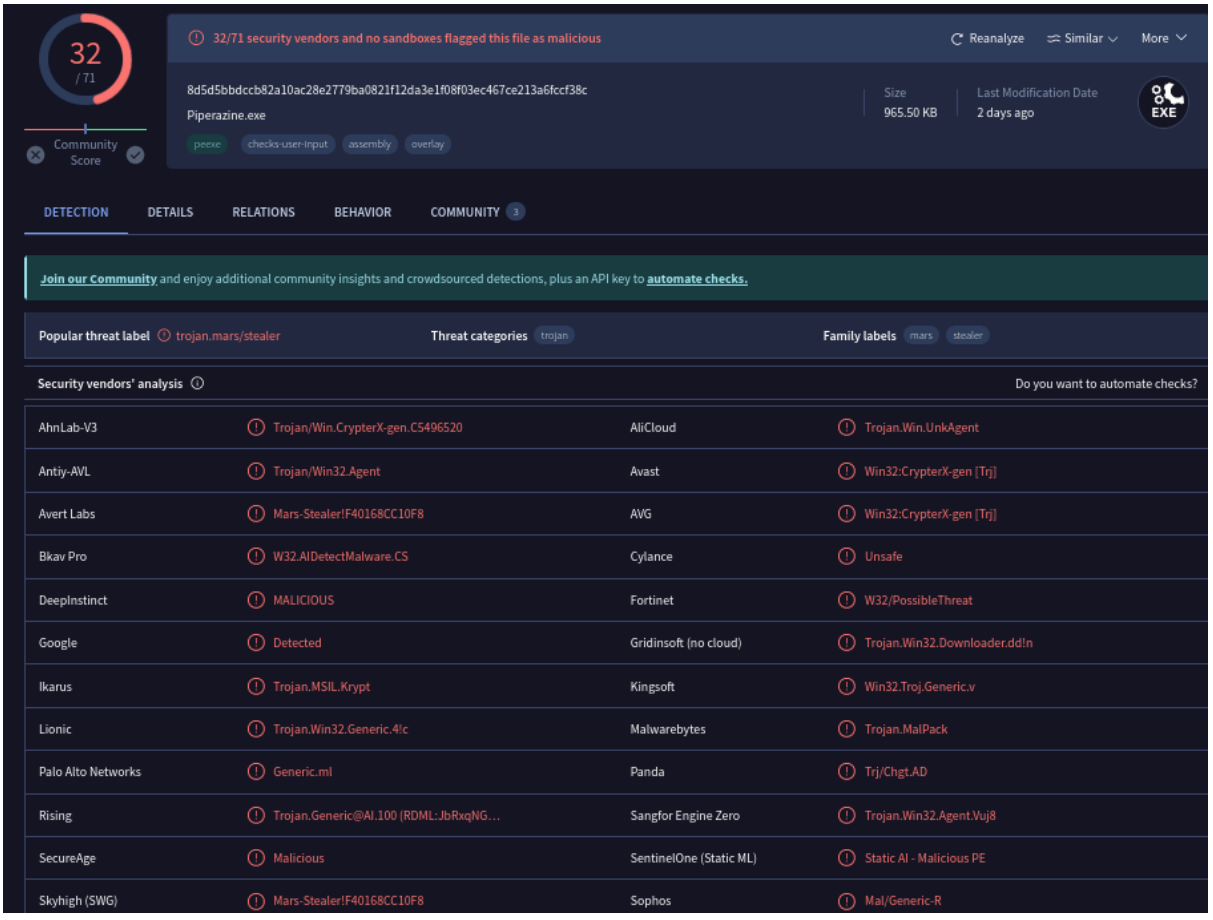
setelah melakukan download, terdapat banyak file .img. cari yang terkait “oneext” menggunakan grep.

```
└─$ ls memdump | grep "oneetx"
file.0×ad818da36c30.0×ad818ca48660.ImageSectionObject.oneetx.exe.img
```

Kemudian gunakan MD5sum

```
└─$ md5sum file.0×ad818da36c30.0×ad818ca48660.ImageSectionObject.oneetx.exe.img
f40168cc10f8cb6fe05322fc391e6947  file.0×ad818da36c30.0×ad818ca48660.ImageSectionObject.oneetx.exe.img
```

Menuju ke virustotal untuk pengecekan.



Kategori adalah trojan dan popular label stealer.

ANS: REDLINE(judul) Stealer(Label)

Verifikasi:

CyberDefenders Lab: REDLINE

Glen Taberima

```
└─$ strings MemoryDump.mem | grep -i "redline" | grep -i "stealer"
!RedLineStealer
!RedLineStealer.
RedLineStealer
!RedLineStealer.MEn
RedLineStealer.EBn
!RedLineStealer.
RedLineStealer
RedlineStealer.RPJ6
RedLineStealer.KT.
RedLineStealer
RedLineStealer.E
Redlinestealer!mclgU$PDF/Phish.
RedLineStealer
RedLineStealer.KT.
RedLineStealer
RedLineStealer
RedlinestealerB
RedLineStealer.MCO
RedLineStealer.MW!MTB
RedLineStealer
RedLineStealer.MW!MTB
RedLineStealer.KD
RedLineStealer.D
!RedLineStealer.NEF!MT
!RedLineStealer.NEF!MT
Redlinestealer!mclgU$PDF/Phish.
RedLineStealer
```

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

```
└─$ 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
```

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

Menggunakan HybridAnalysis:

CyberDefenders Lab: REDLINE

Glen Taberima

Input	Threat level	Analysis Summary	Countries	Environment
http://77.91.124.20/	malicious	Threat Score: 100/100 AV Detection: **Marked as clean** Matched **5** Indicators		Windows 7 32 bit (HWP Support)
http://77.91.124.20/	malicious	Threat Score: 100/100 AV Detection: **Marked as clean** Matched **10** Indicators		Windows 11 64 bit
a.exe PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows 2f754e3af873f1a43e9dbe382497313ecad3f559f1bb27156b81a79c668d7c00 (Sample (576KiB))	malicious	Threat Score: 100/100 AV Detection: **68%** Zusy.Generic Matched **95** Indicators #windows-server-utility		Windows 10 64 bit
http://77.91.124.20/store/games/Plugins/clip.dll	malicious	Threat Score: 100/100 AV Detection: **Marked as clean** Matched **13** Indicators		Windows 7 32 bit (HWP Support)
http://77.91.124.20/DSC01491/fotocr05.exe	malicious	Threat Score: 100/100 AV Detection: **29%** Malicious site Matched **15** Indicators		Windows 7 32 bit (HWP Support)
https://77.91.124.20/	malicious	Threat Score: 100/100 AV Detection: **12%** Malicious site Matched **11** Indicators		Windows 7 32 bit
http://77.91.124.20/store/games/index.php	malicious	Threat Score: 100/100 AV Detection: **26%** Malicious site Matched **13** Indicators		Windows 7 32 bit
http://77.91.124.20/	malicious	Threat Score: 100/100 AV Detection: **Marked as clean** Matched **14** Indicators		Windows 7 32 bit
http://77.91.124.20/	malicious	Threat Score: 100/100 AV Detection: **Marked as clean** Matched **16** Indicators		Windows 10 64 bit
a.bin PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows 188e97ba18d7394cb3949e66c8aeb062e3ea8675371d0ee2b5126b52366530ae (Sample (5KiB))	malicious	Threat Score: 100/100 AV Detection: **22%** MSILHeracles.Generic Matched **371** Indicators #windows-server-utility #evasive		Windows 10 64 bit
http://77.91.124.20/store/games/index.php	malicious	Threat Score: 100/100 AV Detection: **1%** Malicious site Matched **9** Indicators		Windows 10 64 bit

What is the full path of the malicious executable?

python3 ~/Documents/volatility3-2.5.0/vol.py -f MemoryDump.mem windows.filescan | grep -i "oneetx"

```
└─$ python3 ~/Documents/volatility3-2.5.0/vol.py -f MemoryDump.mem windows.filescan | grep -i "oneetx"
0×ad818d436c70.0\Users\Tammam\AppData\Local\Temp\c3912af058\oneetx.exe  216
0×ad818da36c30  \Users\Tammam\AppData\Local\Temp\c3912af058\oneetx.exe  216
0×ad818ef1a0b0  \Users\Tammam\AppData\Local\Temp\c3912af058\oneetx.exe  216
```

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