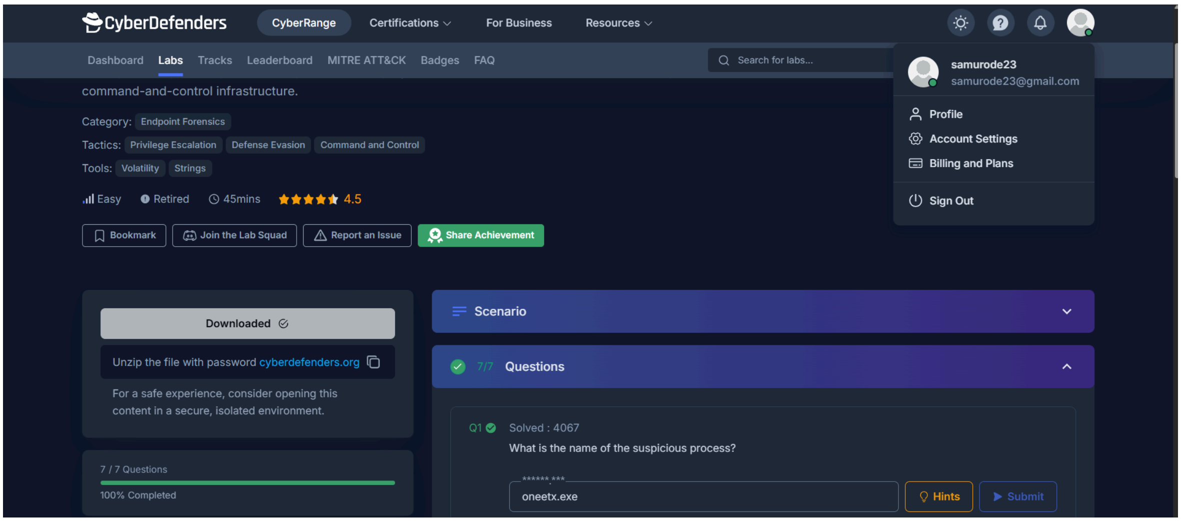
Tarea 2.5: Laboratorio RedLine

Trabajo realizado por:
Samuel Romero de los Reyes

Curso de espacialización en:
CETI

Índice

CyberDefenders



command-and-control infrastructure.

Category: Endpoint Forensics

Tactics: Privilege Escalation · Defense Evasion · Command and Control

Tools: Volatility · Strings

Easy · Retired · 45mins · ★★★★★ 4.5

Unzip the file with password cyberdefenders.org

For a safe experience, consider opening this content in a secure, isolated environment.

7 / 7 Questions

100% Completed

7/7 Questions

Q1 Solved : 4067

What is the name of the suspicious process?

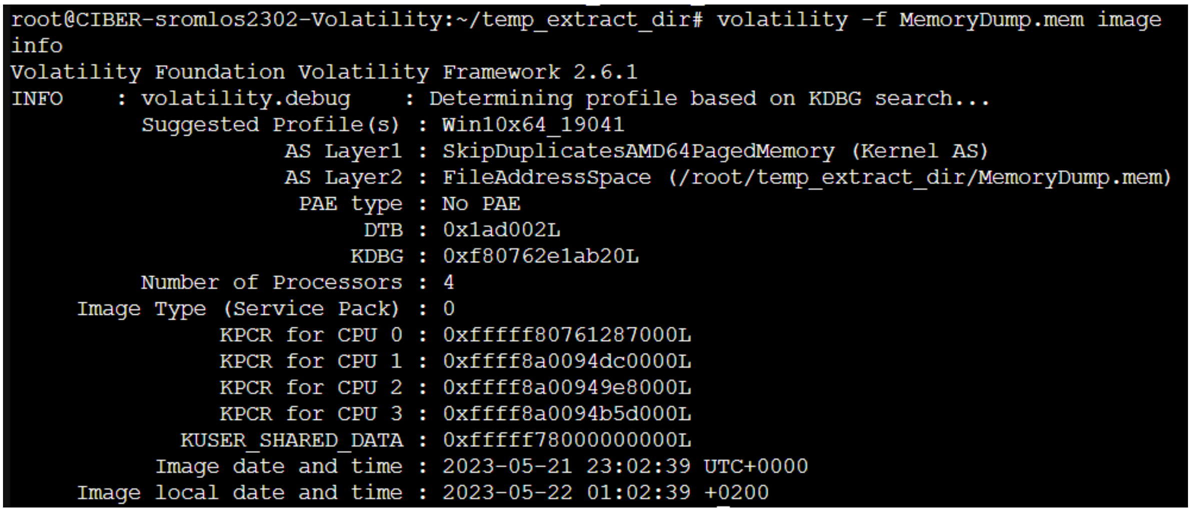
******.***

oneetx.exe

Ejercicio 1 y 2

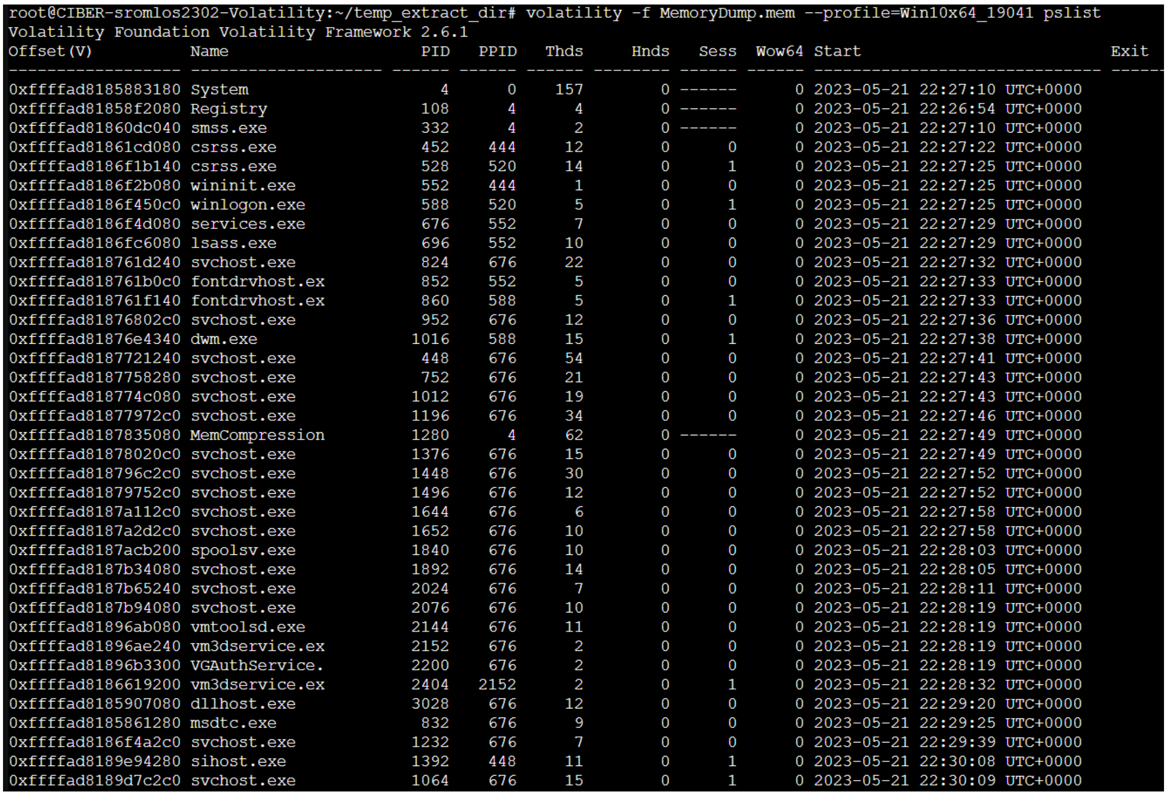
Primero, vemos de qué sistema operativo se trata (Win10x64_19041) con el siguiente comando:

volatility -f MemoryDump.mem imageinfo

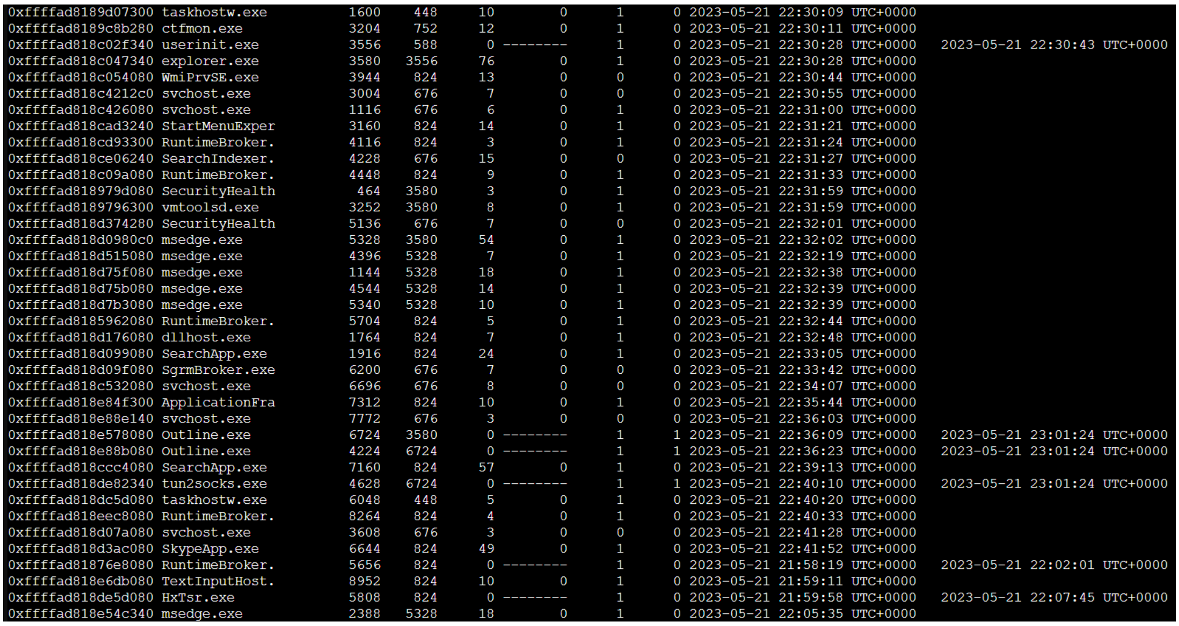


```
root@CIBER-sromlos2302-Volatility:~/temp_extract_dir# volatility -f MemoryDump.mem image
info
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win10x64_19041
                     AS Layer1 : SkipDuplicatesAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/root/temp_extract_dir/MemoryDump.mem)
                      PAE type : No PAE
                           DTB : 0x1ad002L
                          KDBG : 0xf80762e1ab20L
          Number of Processors : 4
     Image Type (Service Pack) : 0
                KPCR for CPU 0 : 0xfffff80761287000L
                KPCR for CPU 1 : 0xffff8a0094dc0000L
                KPCR for CPU 2 : 0xffff8a00949e8000L
                KPCR for CPU 3 : 0xffff8a0094b5d000L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2023-05-21 23:02:39 UTC+0000
     Image local date and time : 2023-05-22 01:02:39 +0200
```

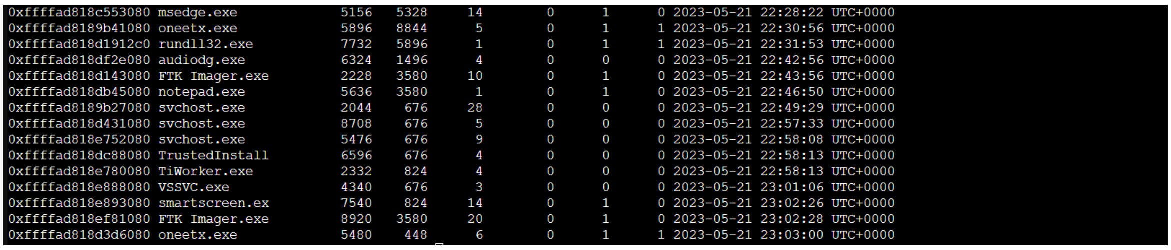
Ahora, vemos los procesos activos usando el comando:
volatility -f MemoryDump.mem --profile=Win10x64_19041 pslist



```
root@CIBER-sromlos2302-Volatility:~/temp_extract_dir# volatility -f MemoryDump.mem --profile=Win10x64_19041 pslist
Volatility Foundation Volatility Framework 2.6.1
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ -----
0xffffad8185883180 System                    4      0    157        0 ------      0 2023-05-21 22:27:10 UTC+0000
0xffffad81858f2080 Registry                108      4      4        0 ------      0 2023-05-21 22:26:54 UTC+0000
0xffffad81860dc040 smss.exe                332      4      2        0 ------      0 2023-05-21 22:27:10 UTC+0000
0xffffad81861cd080 csrss.exe               452    444     12        0      0      0 2023-05-21 22:27:22 UTC+0000
0xffffad8186f1b140 csrss.exe               528    520     14        0      1      0 2023-05-21 22:27:25 UTC+0000
0xffffad8186f2b080 wininit.exe             552    444      1        0      0      0 2023-05-21 22:27:25 UTC+0000
0xffffad8186f450c0 winlogon.exe            588    520      5        0      1      0 2023-05-21 22:27:25 UTC+0000
0xffffad8186f4d080 services.exe            676    552      7        0      0      0 2023-05-21 22:27:29 UTC+0000
0xffffad8186fc6080 lsass.exe               696    552     10        0      0      0 2023-05-21 22:27:29 UTC+0000
0xffffad818761d240 svchost.exe             824    676     22        0      0      0 2023-05-21 22:27:32 UTC+0000
0xffffad818761b0c0 fontdrvhost.ex          852    552      5        0      0      0 2023-05-21 22:27:33 UTC+0000
0xffffad818761f140 fontdrvhost.ex          860    588      5        0      1      0 2023-05-21 22:27:33 UTC+0000
0xffffad81876802c0 svchost.exe             952    676     12        0      0      0 2023-05-21 22:27:36 UTC+0000
0xffffad81876e4340 dwm.exe                1016    588     15        0      1      0 2023-05-21 22:27:38 UTC+0000
0xffffad8187721240 svchost.exe             448    676     54        0      0      0 2023-05-21 22:27:41 UTC+0000
0xffffad8187758280 svchost.exe             752    676     21        0      0      0 2023-05-21 22:27:43 UTC+0000
0xffffad818774c080 svchost.exe            1012    676     19        0      0      0 2023-05-21 22:27:43 UTC+0000
0xffffad81877972c0 svchost.exe            1196    676     34        0      0      0 2023-05-21 22:27:46 UTC+0000
0xffffad8187835080 MemCompression         1280      4     62        0 ------      0 2023-05-21 22:27:49 UTC+0000
0xffffad81878020c0 svchost.exe            1376    676     15        0      0      0 2023-05-21 22:27:49 UTC+0000
0xffffad818796c2c0 svchost.exe            1448    676     30        0      0      0 2023-05-21 22:27:52 UTC+0000
0xffffad81879752c0 svchost.exe            1496    676     12        0      0      0 2023-05-21 22:27:52 UTC+0000
0xffffad8187a112c0 svchost.exe            1644    676      6        0      0      0 2023-05-21 22:27:58 UTC+0000
0xffffad8187a2d2c0 svchost.exe            1652    676     10        0      0      0 2023-05-21 22:27:58 UTC+0000
0xffffad8187acb200 spoolsv.exe            1840    676     10        0      0      0 2023-05-21 22:28:03 UTC+0000
0xffffad8187b34080 svchost.exe            1892    676     14        0      0      0 2023-05-21 22:28:05 UTC+0000
0xffffad8187b65240 svchost.exe            2024    676      7        0      0      0 2023-05-21 22:28:11 UTC+0000
0xffffad8187b94080 svchost.exe            2076    676     10        0      0      0 2023-05-21 22:28:19 UTC+0000
0xffffad81896ab080 vmtoolsd.exe           2144    676     11        0      0      0 2023-05-21 22:28:19 UTC+0000
0xffffad81896ae240 vm3dservice.ex         2152    676      2        0      0      0 2023-05-21 22:28:19 UTC+0000
0xffffad81896b3300 VGAuthService.         2200    676      2        0      0      0 2023-05-21 22:28:19 UTC+0000
0xffffad8186619200 vm3dservice.ex         2404   2152      2        0      1      0 2023-05-21 22:28:32 UTC+0000
0xffffad8185907080 dllhost.exe            3028    676     12        0      0      0 2023-05-21 22:29:20 UTC+0000
0xffffad8185861280 msdtc.exe               832    676      9        0      0      0 2023-05-21 22:29:25 UTC+0000
0xffffad8186f4a2c0 svchost.exe            1232    676      7        0      0      0 2023-05-21 22:29:39 UTC+0000
0xffffad8189e94280 sihost.exe             1392    448     11        0      1      0 2023-05-21 22:30:08 UTC+0000
0xffffad8189d7c2c0 svchost.exe            1064    676     15        0      1      0 2023-05-21 22:30:09 UTC+0000
```

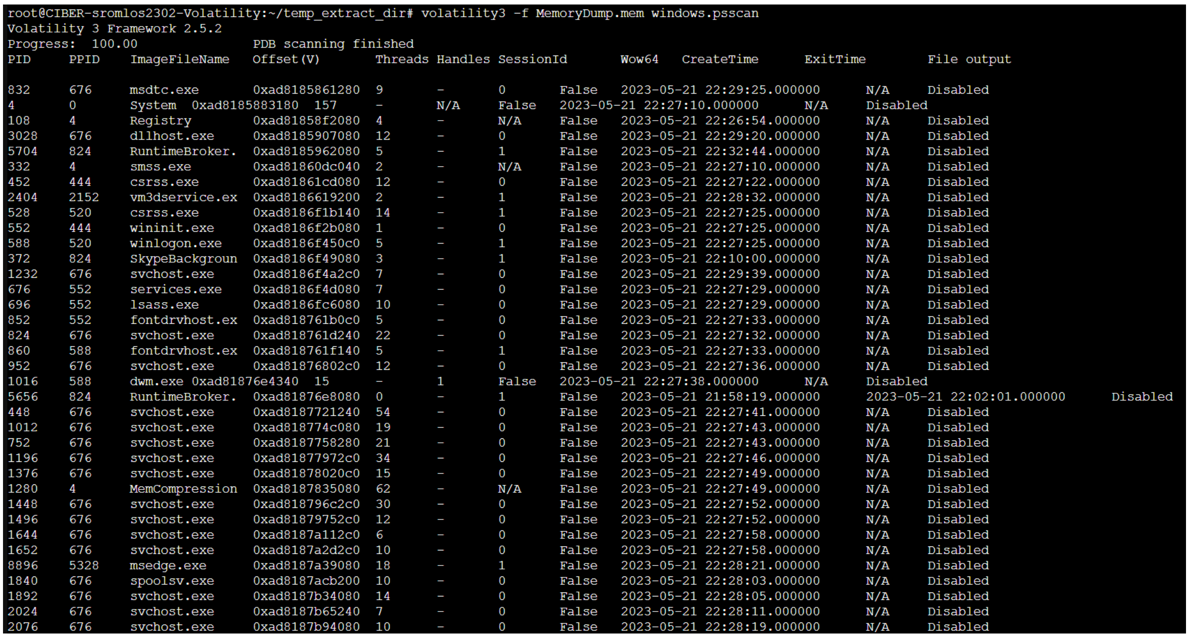


```
0xffffad8189d07300 taskhostw.exe          1600    448     10        0      1      0 2023-05-21 22:30:09 UTC+0000
0xffffad8189c8b280 ctfmon.exe             3204    752     12        0      1      0 2023-05-21 22:30:11 UTC+0000
0xffffad818c02f340 userinit.exe           3556    588      0 --------      1      0 2023-05-21 22:30:28 UTC+0000   2023-05-21 22:30:43 UTC+0000
0xffffad818c047340 explorer.exe           3580   3556     76        0      1      0 2023-05-21 22:30:28 UTC+0000
0xffffad818c054080 WmiPrvSE.exe           3944    824     13        0      0      0 2023-05-21 22:30:44 UTC+0000
0xffffad818c4212c0 svchost.exe            3004    676      7        0      0      0 2023-05-21 22:30:55 UTC+0000
0xffffad818c426080 svchost.exe            1116    676      6        0      1      0 2023-05-21 22:31:00 UTC+0000
0xffffad818cad3240 StartMenuExper         3160    824     14        0      1      0 2023-05-21 22:31:21 UTC+0000
0xffffad818cd93300 RuntimeBroker.         4116    824      3        0      1      0 2023-05-21 22:31:24 UTC+0000
0xffffad818ce06240 SearchIndexer.         4228    676     15        0      0      0 2023-05-21 22:31:27 UTC+0000
0xffffad818c09a080 RuntimeBroker.         4448    824      9        0      1      0 2023-05-21 22:31:33 UTC+0000
0xffffad818979d080 SecurityHealth          464   3580      3        0      1      0 2023-05-21 22:31:59 UTC+0000
0xffffad8189796300 vmtoolsd.exe           3252   3580      8        0      1      0 2023-05-21 22:31:59 UTC+0000
0xffffad818d374280 SecurityHealth         5136    676      7        0      0      0 2023-05-21 22:32:01 UTC+0000
0xffffad818d0980c0 msedge.exe             5328   3580     54        0      1      0 2023-05-21 22:32:02 UTC+0000
0xffffad818d515080 msedge.exe             4396   5328      7        0      1      0 2023-05-21 22:32:19 UTC+0000
0xffffad818d75f080 msedge.exe             1144   5328     18        0      1      0 2023-05-21 22:32:38 UTC+0000
0xffffad818d75b080 msedge.exe             4544   5328     14        0      1      0 2023-05-21 22:32:39 UTC+0000
0xffffad818d7b3080 msedge.exe             5340   5328     10        0      1      0 2023-05-21 22:32:39 UTC+0000
0xffffad8185962080 RuntimeBroker.         5704    824      5        0      1      0 2023-05-21 22:32:44 UTC+0000
0xffffad818d176080 dllhost.exe            1764    824      7        0      1      0 2023-05-21 22:32:48 UTC+0000
0xffffad818d099080 SearchApp.exe          1916    824     24        0      1      0 2023-05-21 22:33:05 UTC+0000
0xffffad818d09f080 SgrmBroker.exe         6200    676      7        0      0      0 2023-05-21 22:33:42 UTC+0000
0xffffad818c532080 svchost.exe            6696    676      8        0      0      0 2023-05-21 22:34:07 UTC+0000
0xffffad818e84f300 ApplicationFra         7312    824     10        0      1      0 2023-05-21 22:35:44 UTC+0000
0xffffad818e88e140 svchost.exe            7772    676      3        0      0      0 2023-05-21 22:36:03 UTC+0000
0xffffad818e578080 Outline.exe            6724   3580      0 --------      1      1 2023-05-21 22:36:09 UTC+0000   2023-05-21 23:01:24 UTC+0000
0xffffad818e88b080 Outline.exe            4224   6724      0 --------      1      1 2023-05-21 22:36:23 UTC+0000   2023-05-21 23:01:24 UTC+0000
0xffffad818ccc4080 SearchApp.exe          7160    824     57        0      1      0 2023-05-21 22:39:13 UTC+0000
0xffffad818de82340 tun2socks.exe          4628   6724      0 --------      1      1 2023-05-21 22:40:10 UTC+0000   2023-05-21 23:01:24 UTC+0000
0xffffad818dc5d080 taskhostw.exe          6048    448      5        0      1      0 2023-05-21 22:40:20 UTC+0000
0xffffad818eec8080 RuntimeBroker.         8264    824      4        0      1      0 2023-05-21 22:40:33 UTC+0000
0xffffad818d07a080 svchost.exe            3608    676      3        0      0      0 2023-05-21 22:41:28 UTC+0000
0xffffad818d3ac080 SkypeApp.exe           6644    824     49        0      1      0 2023-05-21 22:41:52 UTC+0000
0xffffad81876e8080 RuntimeBroker.         5656    824      0 --------      1      0 2023-05-21 21:58:19 UTC+0000   2023-05-21 22:02:01 UTC+0000
0xffffad818e6db080 TextInputHost.         8952    824     10        0      1      0 2023-05-21 21:59:11 UTC+0000
0xffffad818de5d080 HxTsr.exe              5808    824      0 --------      1      0 2023-05-21 21:59:58 UTC+0000   2023-05-21 22:07:45 UTC+0000
0xffffad818e54c340 msedge.exe             2388   5328     18        0      1      0 2023-05-21 22:05:35 UTC+0000
```

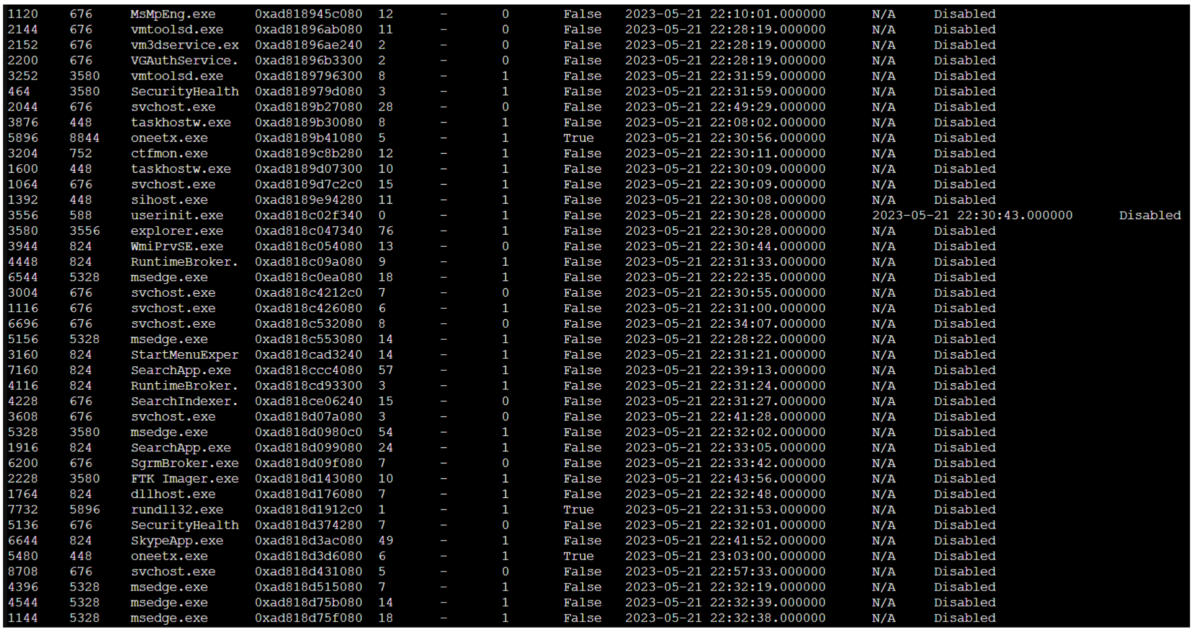


```
0xffffad818c553080 msedge.exe             5156   5328     14        0      1      0 2023-05-21 22:28:22 UTC+0000
0xffffad8189b41080 oneetx.exe             5896   8844      5        0      1      1 2023-05-21 22:30:56 UTC+0000
0xffffad818d1912c0 rundll32.exe           7732   5896      1        0      1      1 2023-05-21 22:31:53 UTC+0000
0xffffad818df2e080 audiodg.exe            6324   1496      4        0      0      0 2023-05-21 22:42:56 UTC+0000
0xffffad818d143080 FTK Imager.exe         2228   3580     10        0      1      0 2023-05-21 22:43:56 UTC+0000
0xffffad818db45080 notepad.exe            5636   3580      1        0      1      0 2023-05-21 22:46:50 UTC+0000
0xffffad8189b27080 svchost.exe            2044    676     28        0      0      0 2023-05-21 22:49:29 UTC+0000
0xffffad818d431080 svchost.exe            8708    676      5        0      0      0 2023-05-21 22:57:33 UTC+0000
0xffffad818e752080 svchost.exe            5476    676      9        0      0      0 2023-05-21 22:58:08 UTC+0000
0xffffad818dc88080 TrustedInstall         6596    676      4        0      0      0 2023-05-21 22:58:13 UTC+0000
0xffffad818e780080 TiWorker.exe           2332    824      4        0      0      0 2023-05-21 22:58:13 UTC+0000
0xffffad818e888080 VSSVC.exe              4340    676      3        0      0      0 2023-05-21 23:01:06 UTC+0000
0xffffad818e893080 smartscreen.ex         7540    824     14        0      1      0 2023-05-21 23:02:26 UTC+0000
0xffffad818ef81080 FTK Imager.exe         8920   3580     20        0      1      0 2023-05-21 23:02:28 UTC+0000
0xffffad818d3d6080 oneetx.exe             5480    448      6        0      1      1 2023-05-21 23:03:00 UTC+0000
```

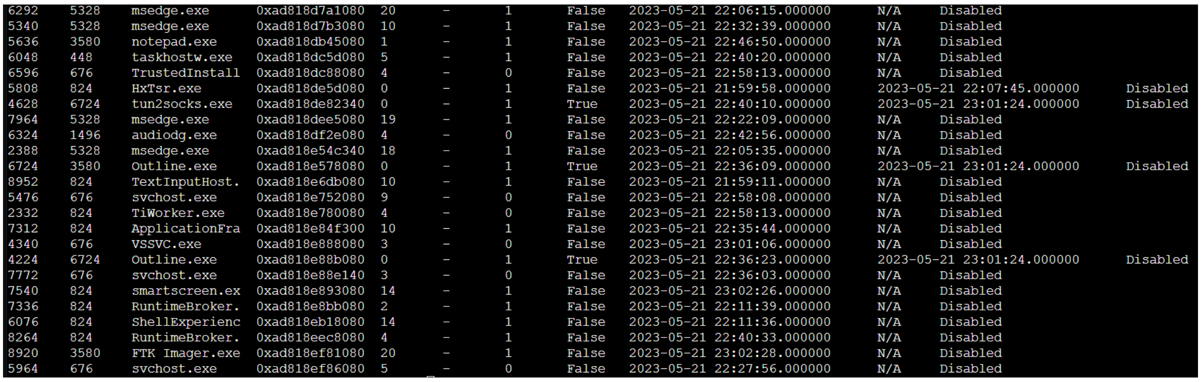
Y ahora vemos los procesos terminados y ocultos con:
volatility3 -f MemoryDump.mem windows.psscan



```
root@CIBER-sromlos2302-Volatility:~/temp_extract_dir# volatility3 -f MemoryDump.mem windows.psscan
Volatility 3 Framework 2.5.2
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

832     676     msdtc.exe       0xad8185861280  9       -       0       False   2023-05-21 22:29:25.000000      N/A     Disabled
4       0       System  0xad8185883180  157     -       N/A     False   2023-05-21 22:27:10.000000      N/A     Disabled
108     4       Registry        0xad81858f2080  4       -       N/A     False   2023-05-21 22:26:54.000000      N/A     Disabled
3028    676     dllhost.exe     0xad8185907080  12      -       0       False   2023-05-21 22:29:20.000000      N/A     Disabled
5704    824     RuntimeBroker.  0xad8185962080  5       -       1       False   2023-05-21 22:32:44.000000      N/A     Disabled
332     4       smss.exe        0xad81860dc040  2       -       N/A     False   2023-05-21 22:27:10.000000      N/A     Disabled
452     444     csrss.exe       0xad81861cd080  12      -       0       False   2023-05-21 22:27:22.000000      N/A     Disabled
2404    2152    vm3dservice.ex  0xad8186619200  2       -       1       False   2023-05-21 22:28:32.000000      N/A     Disabled
528     520     csrss.exe       0xad8186f1b140  14      -       1       False   2023-05-21 22:27:25.000000      N/A     Disabled
552     444     wininit.exe     0xad8186f2b080  1       -       0       False   2023-05-21 22:27:25.000000      N/A     Disabled
588     520     winlogon.exe    0xad8186f450c0  5       -       1       False   2023-05-21 22:27:25.000000      N/A     Disabled
372     824     SkypeBackgroun  0xad8186f49080  3       -       1       False   2023-05-21 22:10:00.000000      N/A     Disabled
1232    676     svchost.exe     0xad8186f4a2c0  7       -       0       False   2023-05-21 22:29:39.000000      N/A     Disabled
676     552     services.exe    0xad8186f4d080  7       -       0       False   2023-05-21 22:27:29.000000      N/A     Disabled
696     552     lsass.exe       0xad8186fc6080  10      -       0       False   2023-05-21 22:27:29.000000      N/A     Disabled
852     552     fontdrvhost.ex  0xad818761b0c0  5       -       0       False   2023-05-21 22:27:33.000000      N/A     Disabled
824     676     svchost.exe     0xad818761d240  22      -       0       False   2023-05-21 22:27:32.000000      N/A     Disabled
860     588     fontdrvhost.ex  0xad818761f140  5       -       1       False   2023-05-21 22:27:33.000000      N/A     Disabled
952     676     svchost.exe     0xad81876802c0  12      -       0       False   2023-05-21 22:27:36.000000      N/A     Disabled
1016    588     dwm.exe 0xad81876e4340  15      -       1       False   2023-05-21 22:27:38.000000      N/A     Disabled
5656    824     RuntimeBroker.  0xad81876e8080  0       -       1       False   2023-05-21 21:58:19.000000      2023-05-21 22:02:01.000000      Disabled
448     676     svchost.exe     0xad8187721240  54      -       0       False   2023-05-21 22:27:41.000000      N/A     Disabled
1012    676     svchost.exe     0xad818774c080  19      -       0       False   2023-05-21 22:27:43.000000      N/A     Disabled
752     676     svchost.exe     0xad8187758280  21      -       0       False   2023-05-21 22:27:43.000000      N/A     Disabled
1196    676     svchost.exe     0xad81877972c0  34      -       0       False   2023-05-21 22:27:46.000000      N/A     Disabled
1376    676     svchost.exe     0xad81878020c0  15      -       0       False   2023-05-21 22:27:49.000000      N/A     Disabled
1280    4       MemCompression  0xad8187835080  62      -       N/A     False   2023-05-21 22:27:49.000000      N/A     Disabled
1448    676     svchost.exe     0xad818796c2c0  30      -       0       False   2023-05-21 22:27:52.000000      N/A     Disabled
1496    676     svchost.exe     0xad81879752c0  12      -       0       False   2023-05-21 22:27:52.000000      N/A     Disabled
1644    676     svchost.exe     0xad8187a112c0  6       -       0       False   2023-05-21 22:27:58.000000      N/A     Disabled
1652    676     svchost.exe     0xad8187a2d2c0  10      -       0       False   2023-05-21 22:27:58.000000      N/A     Disabled
8896    5328    msedge.exe      0xad8187a39080  18      -       1       False   2023-05-21 22:28:21.000000      N/A     Disabled
1840    676     spoolsv.exe     0xad8187acb200  10      -       0       False   2023-05-21 22:28:03.000000      N/A     Disabled
1892    676     svchost.exe     0xad8187b34080  14      -       0       False   2023-05-21 22:28:05.000000      N/A     Disabled
2024    676     svchost.exe     0xad8187b65240  7       -       0       False   2023-05-21 22:28:11.000000      N/A     Disabled
2076    676     svchost.exe     0xad8187b94080  10      -       0       False   2023-05-21 22:28:19.000000      N/A     Disabled
```



```
1120    676     MsMpEng.exe     0xad818945c080  12      -       0       False   2023-05-21 22:10:01.000000      N/A     Disabled
2144    676     vmtoolsd.exe    0xad81896ab080  11      -       0       False   2023-05-21 22:28:19.000000      N/A     Disabled
2152    676     vm3dservice.ex  0xad81896ae240  2       -       0       False   2023-05-21 22:28:19.000000      N/A     Disabled
2200    676     VGAuthService.  0xad81896b3300  2       -       0       False   2023-05-21 22:28:19.000000      N/A     Disabled
3252    3580    vmtoolsd.exe    0xad8189796300  8       -       1       False   2023-05-21 22:31:59.000000      N/A     Disabled
464     3580    SecurityHealth  0xad818979d080  3       -       1       False   2023-05-21 22:31:59.000000      N/A     Disabled
2044    676     svchost.exe     0xad8189b27080  28      -       0       False   2023-05-21 22:49:29.000000      N/A     Disabled
3876    448     taskhostw.exe   0xad8189b30080  8       -       1       False   2023-05-21 22:08:02.000000      N/A     Disabled
5896    8844    oneetx.exe      0xad8189b41080  5       -       1       True    2023-05-21 22:30:56.000000      N/A     Disabled
3204    752     ctfmon.exe      0xad8189c8b280  12      -       1       False   2023-05-21 22:30:11.000000      N/A     Disabled
1600    448     taskhostw.exe   0xad8189d07300  10      -       1       False   2023-05-21 22:30:09.000000      N/A     Disabled
1064    676     svchost.exe     0xad8189d7c2c0  15      -       1       False   2023-05-21 22:30:09.000000      N/A     Disabled
1392    448     sihost.exe      0xad8189e94280  11      -       1       False   2023-05-21 22:30:08.000000      N/A     Disabled
3556    588     userinit.exe    0xad818c02f340  0       -       1       False   2023-05-21 22:30:28.000000      2023-05-21 22:30:43.000000      Disabled
3580    3556    explorer.exe    0xad818c047340  76      -       1       False   2023-05-21 22:30:28.000000      N/A     Disabled
3944    824     WmiPrvSE.exe    0xad818c054080  13      -       0       False   2023-05-21 22:30:44.000000      N/A     Disabled
4448    824     RuntimeBroker.  0xad818c09a080  9       -       1       False   2023-05-21 22:31:33.000000      N/A     Disabled
6544    5328    msedge.exe      0xad818c0ea080  18      -       1       False   2023-05-21 22:22:35.000000      N/A     Disabled
3004    676     svchost.exe     0xad818c4212c0  7       -       0       False   2023-05-21 22:30:55.000000      N/A     Disabled
1116    676     svchost.exe     0xad818c426080  6       -       1       False   2023-05-21 22:31:00.000000      N/A     Disabled
6696    676     svchost.exe     0xad818c532080  8       -       0       False   2023-05-21 22:34:07.000000      N/A     Disabled
5156    5328    msedge.exe      0xad818c553080  14      -       1       False   2023-05-21 22:28:22.000000      N/A     Disabled
3160    824     StartMenuExper  0xad818cad3240  14      -       1       False   2023-05-21 22:31:21.000000      N/A     Disabled
7160    824     SearchApp.exe   0xad818ccc4080  57      -       1       False   2023-05-21 22:39:13.000000      N/A     Disabled
4116    824     RuntimeBroker.  0xad818cd93300  3       -       1       False   2023-05-21 22:31:24.000000      N/A     Disabled
4228    676     SearchIndexer.  0xad818ce06240  15      -       0       False   2023-05-21 22:31:27.000000      N/A     Disabled
3608    676     svchost.exe     0xad818d07a080  3       -       0       False   2023-05-21 22:41:28.000000      N/A     Disabled
5328    3580    msedge.exe      0xad818d0980c0  54      -       1       False   2023-05-21 22:32:02.000000      N/A     Disabled
1916    824     SearchApp.exe   0xad818d099080  24      -       1       False   2023-05-21 22:33:05.000000      N/A     Disabled
6200    676     SgrmBroker.exe  0xad818d09f080  7       -       0       False   2023-05-21 22:33:42.000000      N/A     Disabled
2228    3580    FTK Imager.exe  0xad818d143080  10      -       1       False   2023-05-21 22:43:56.000000      N/A     Disabled
1764    824     dllhost.exe     0xad818d176080  7       -       1       False   2023-05-21 22:32:48.000000      N/A     Disabled
7732    5896    rundll32.exe    0xad818d1912c0  1       -       1       True    2023-05-21 22:31:53.000000      N/A     Disabled
5136    676     SecurityHealth  0xad818d374280  7       -       0       False   2023-05-21 22:32:01.000000      N/A     Disabled
6644    824     SkypeApp.exe    0xad818d3ac080  49      -       1       False   2023-05-21 22:41:52.000000      N/A     Disabled
5480    448     oneetx.exe      0xad818d3d6080  6       -       1       True    2023-05-21 23:03:00.000000      N/A     Disabled
8708    676     svchost.exe     0xad818d431080  5       -       0       False   2023-05-21 22:57:33.000000      N/A     Disabled
4396    5328    msedge.exe      0xad818d515080  7       -       1       False   2023-05-21 22:32:19.000000      N/A     Disabled
4544    5328    msedge.exe      0xad818d75b080  14      -       1       False   2023-05-21 22:32:39.000000      N/A     Disabled
1144    5328    msedge.exe      0xad818d75f080  18      -       1       False   2023-05-21 22:32:38.000000      N/A     Disabled
```

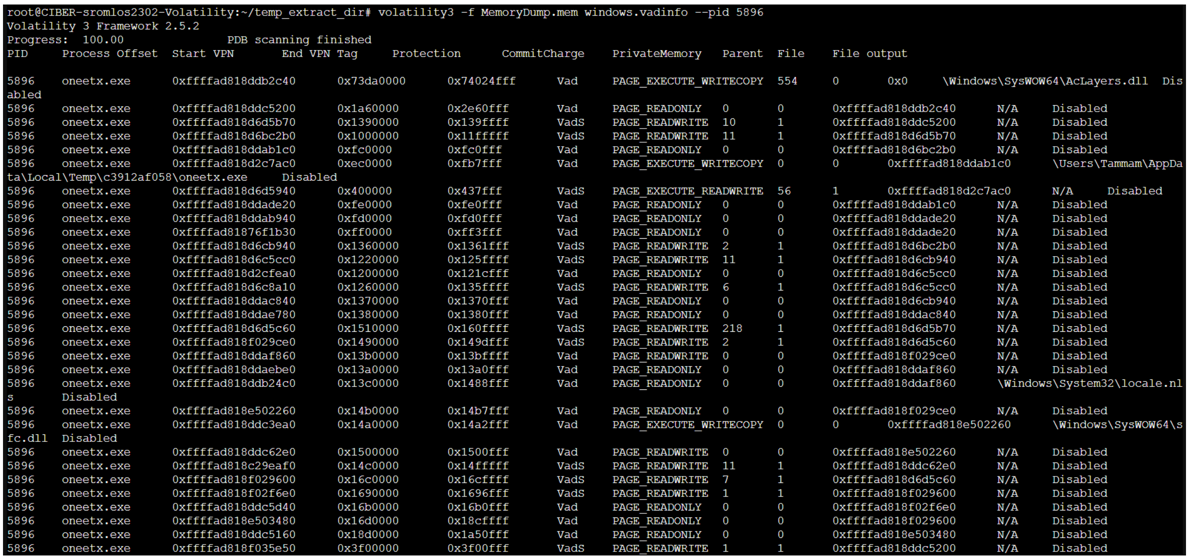


```
6292    5328    msedge.exe      0xad818d7a1080  20      -       1       False   2023-05-21 22:06:15.000000      N/A     Disabled
5340    5328    msedge.exe      0xad818d7b3080  10      -       1       False   2023-05-21 22:32:39.000000      N/A     Disabled
5636    3580    notepad.exe     0xad818db45080  1       -       1       False   2023-05-21 22:46:50.000000      N/A     Disabled
6048    448     taskhostw.exe   0xad818dc5d080  5       -       1       False   2023-05-21 22:40:20.000000      N/A     Disabled
6596    676     TrustedInstall  0xad818dc88080  4       -       0       False   2023-05-21 22:58:13.000000      N/A     Disabled
5808    824     HxTsr.exe       0xad818de5d080  0       -       1       False   2023-05-21 21:59:58.000000      2023-05-21 22:07:45.000000      Disabled
4628    6724    tun2socks.exe   0xad818de82340  0       -       1       True    2023-05-21 22:40:10.000000      2023-05-21 23:01:24.000000      Disabled
7964    5328    msedge.exe      0xad818dee5080  19      -       1       False   2023-05-21 22:22:09.000000      N/A     Disabled
6324    1496    audiodg.exe     0xad818df2e080  4       -       0       False   2023-05-21 22:42:56.000000      N/A     Disabled
2388    5328    msedge.exe      0xad818e54c340  18      -       1       False   2023-05-21 22:05:35.000000      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
8952    824     TextInputHost.  0xad818e6db080  10      -       1       False   2023-05-21 21:59:11.000000      N/A     Disabled
5476    676     svchost.exe     0xad818e752080  9       -       0       False   2023-05-21 22:58:08.000000      N/A     Disabled
2332    824     TiWorker.exe    0xad818e780080  4       -       0       False   2023-05-21 22:58:13.000000      N/A     Disabled
7312    824     ApplicationFra  0xad818e84f300  10      -       1       False   2023-05-21 22:35:44.000000      N/A     Disabled
4340    676     VSSVC.exe       0xad818e888080  3       -       0       False   2023-05-21 23:01:06.000000      N/A     Disabled
4224    6724    Outline.exe     0xad818e88b080  0       -       1       True    2023-05-21 22:36:23.000000      2023-05-21 23:01:24.000000      Disabled
7772    676     svchost.exe     0xad818e88e140  3       -       0       False   2023-05-21 22:36:03.000000      N/A     Disabled
7540    824     smartscreen.ex  0xad818e893080  14      -       1       False   2023-05-21 23:02:26.000000      N/A     Disabled
7336    824     RuntimeBroker.  0xad818e8bb080  2       -       1       False   2023-05-21 22:11:39.000000      N/A     Disabled
6076    824     ShellExperienc  0xad818eb18080  14      -       1       False   2023-05-21 22:11:36.000000      N/A     Disabled
8264    824     RuntimeBroker.  0xad818eec8080  4       -       1       False   2023-05-21 22:40:33.000000      N/A     Disabled
8920    3580    FTK Imager.exe  0xad818ef81080  20      -       1       False   2023-05-21 23:02:28.000000      N/A     Disabled
5964    676     svchost.exe     0xad818ef86080  5       -       0       False   2023-05-21 22:27:56.000000      N/A     Disabled
```

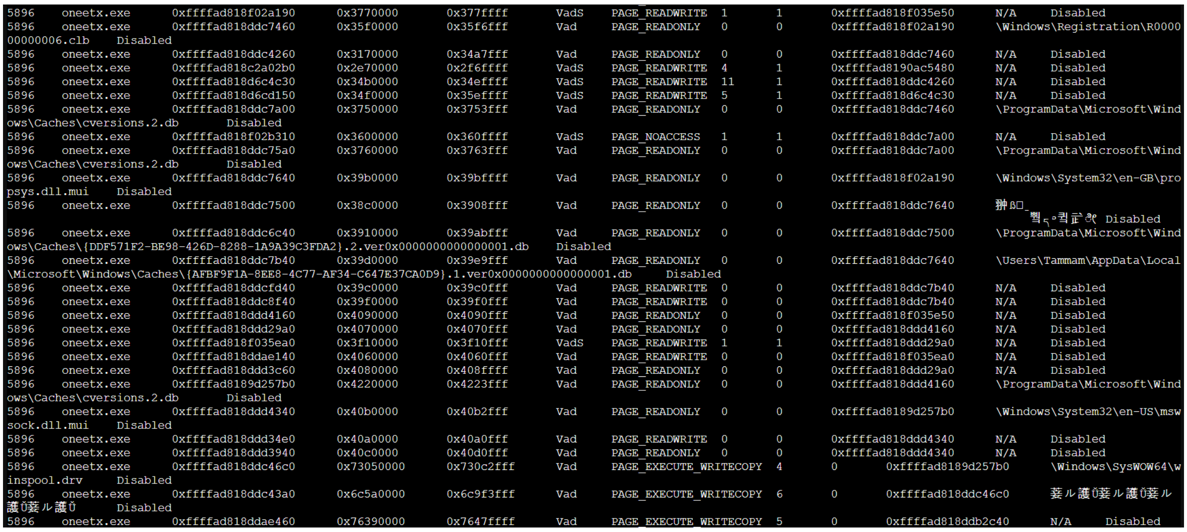
El proceso sospechoso es **oneetx.exe** porque no corresponde a ningún ejecutable legítimo de Windows, aparece dos veces en memoria con nombres y rutas incoherentes, uno de sus PPID no existe en la lista de procesos válidos, y además genera un proceso hijo **rundll32.exe**, un comportamiento típico en cargas de malware que usan rundll32 para ejecutar código malicioso.

Ejercicio 3

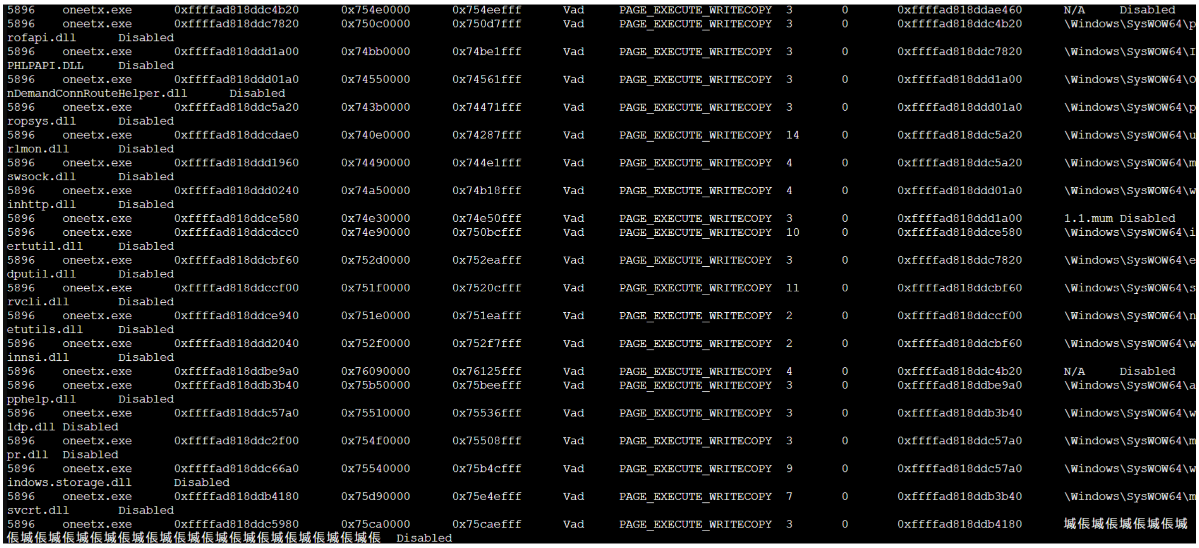
Necesitamos ver las VADs, para ello, ejecutamos los siguientes comandos:
volatility3 -f MemoryDump.mem windows.vadinfo --pid 5896



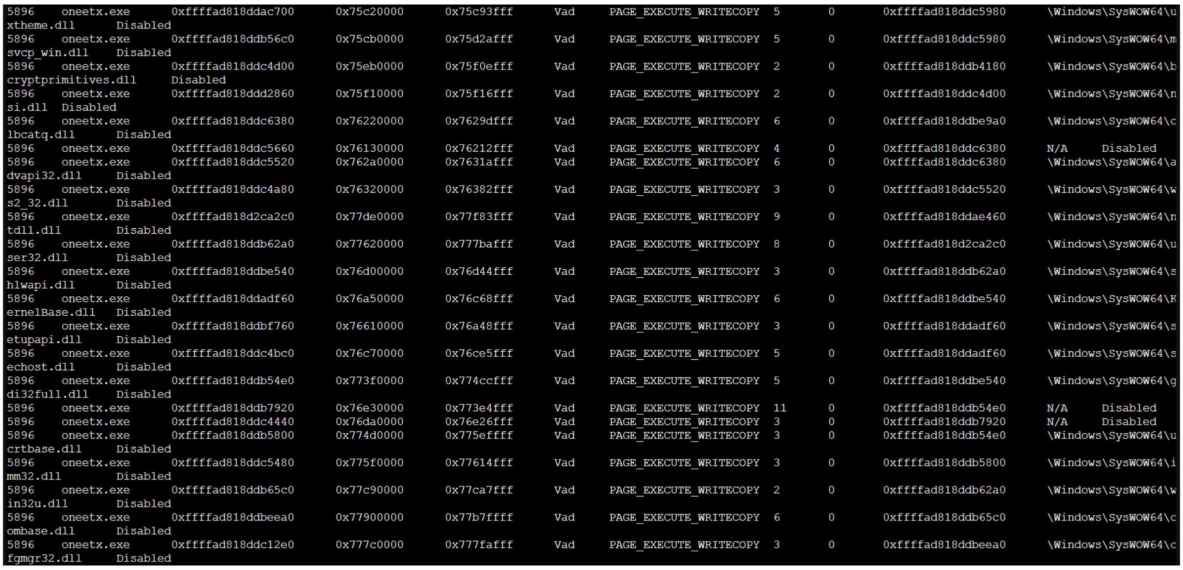
```
root@CIBER-sromlos2302-Volatility:~/temp_extract_dir# volatility3 -f MemoryDump.mem windows.vadinfo --pid 5896
Volatility 3 Framework 2.5.2
Progress:  100.00               PDB scanning finished
PID     Process Offset  Start VPN       End VPN Tag     Protection      CommitCharge    PrivateMemory   Parent  File    File output

5896    oneetx.exe      0xffffad818ddb2c40      0x73da0000      0x74024fff      Vad     PAGE_EXECUTE_WRITECOPY  554     0       0x0     \Windows\SysWOW64\AcLayers.dll  Dis
abled
5896    oneetx.exe      0xffffad818ddc5200      0x1a60000       0x2e60fff       Vad     PAGE_READONLY   0       0       0xffffad818ddb2c40      N/A     Disabled
5896    oneetx.exe      0xffffad818d6d5b70      0x1390000       0x139ffff       VadS    PAGE_READWRITE  10      1       0xffffad818ddc5200      N/A     Disabled
5896    oneetx.exe      0xffffad818d6bc2b0      0x1000000       0x11fffff       VadS    PAGE_READWRITE  11      1       0xffffad818d6d5b70      N/A     Disabled
5896    oneetx.exe      0xffffad818ddab1c0      0xfc0000        0xfc0fff        Vad     PAGE_READONLY   0       0       0xffffad818d6bc2b0      N/A     Disabled
5896    oneetx.exe      0xffffad818d2c7ac0      0xec0000        0xfb7fff        Vad     PAGE_EXECUTE_WRITECOPY  0       0       0xffffad818ddab1c0      \Users\Tammam\AppDa
ta\Local\Temp\c3912af058\oneetx.exe     Disabled
5896    oneetx.exe      0xffffad818d6d5940      0x400000        0x437fff        VadS    PAGE_EXECUTE_READWRITE  56      1       0xffffad818d2c7ac0      N/A     Disabled
5896    oneetx.exe      0xffffad818ddade20      0xfe0000        0xfe0fff        Vad     PAGE_READONLY   0       0       0xffffad818ddab1c0      N/A     Disabled
5896    oneetx.exe      0xffffad818ddab940      0xfd0000        0xfd0fff        Vad     PAGE_READONLY   0       0       0xffffad818ddade20      N/A     Disabled
5896    oneetx.exe      0xffffad81876f1b30      0xff0000        0xff3fff        Vad     PAGE_READONLY   0       0       0xffffad818ddade20      N/A     Disabled
5896    oneetx.exe      0xffffad818d6cb940      0x1360000       0x1361fff       VadS    PAGE_READWRITE  2       1       0xffffad818d6bc2b0      N/A     Disabled
5896    oneetx.exe      0xffffad818d6c5cc0      0x1220000       0x125ffff       VadS    PAGE_READWRITE  11      1       0xffffad818d6cb940      N/A     Disabled
5896    oneetx.exe      0xffffad818d2cfea0      0x1200000       0x121cfff       Vad     PAGE_READONLY   0       0       0xffffad818d6c5cc0      N/A     Disabled
5896    oneetx.exe      0xffffad818d6c8a10      0x1260000       0x135ffff       VadS    PAGE_READWRITE  6       1       0xffffad818d6c5cc0      N/A     Disabled
5896    oneetx.exe      0xffffad818ddac840      0x1370000       0x1370fff       Vad     PAGE_READONLY   0       0       0xffffad818d6cb940      N/A     Disabled
5896    oneetx.exe      0xffffad818ddae780      0x1380000       0x1380fff       Vad     PAGE_READONLY   0       0       0xffffad818ddac840      N/A     Disabled
5896    oneetx.exe      0xffffad818d6d5c60      0x1510000       0x160ffff       VadS    PAGE_READWRITE  218     1       0xffffad818d6d5b70      N/A     Disabled
5896    oneetx.exe      0xffffad818f029ce0      0x1490000       0x149dfff       VadS    PAGE_READWRITE  2       1       0xffffad818d6d5c60      N/A     Disabled
5896    oneetx.exe      0xffffad818ddaf860      0x13b0000       0x13bffff       Vad     PAGE_READWRITE  0       0       0xffffad818f029ce0      N/A     Disabled
5896    oneetx.exe      0xffffad818ddaebe0      0x13a0000       0x13a0fff       Vad     PAGE_READONLY   0       0       0xffffad818ddaf860      N/A     Disabled
5896    oneetx.exe      0xffffad818ddb24c0      0x13c0000       0x1488fff       Vad     PAGE_READONLY   0       0       0xffffad818ddaf860      \Windows\System32\locale.nl
s       Disabled
5896    oneetx.exe      0xffffad818e502260      0x14b0000       0x14b7fff       Vad     PAGE_READONLY   0       0       0xffffad818f029ce0      N/A     Disabled
5896    oneetx.exe      0xffffad818ddc3ea0      0x14a0000       0x14a2fff       Vad     PAGE_EXECUTE_WRITECOPY  0       0       0xffffad818e502260      \Windows\SysWOW64\s
fc.dll  Disabled
5896    oneetx.exe      0xffffad818ddc62e0      0x1500000       0x1500fff       Vad     PAGE_READWRITE  0       0       0xffffad818e502260      N/A     Disabled
5896    oneetx.exe      0xffffad818c29eaf0      0x14c0000       0x14fffff       VadS    PAGE_READWRITE  11      1       0xffffad818ddc62e0      N/A     Disabled
5896    oneetx.exe      0xffffad818f029600      0x16c0000       0x16cffff       VadS    PAGE_READWRITE  7       1       0xffffad818d6d5c60      N/A     Disabled
5896    oneetx.exe      0xffffad818f02f6e0      0x1690000       0x1696fff       VadS    PAGE_READWRITE  1       1       0xffffad818f029600      N/A     Disabled
5896    oneetx.exe      0xffffad818ddc5d40      0x16b0000       0x16b0fff       Vad     PAGE_READONLY   0       0       0xffffad818f02f6e0      N/A     Disabled
5896    oneetx.exe      0xffffad818e503480      0x16d0000       0x18cffff       Vad     PAGE_READONLY   0       0       0xffffad818f029600      N/A     Disabled
5896    oneetx.exe      0xffffad818ddc5160      0x18d0000       0x1a50fff       Vad     PAGE_READONLY   0       0       0xffffad818e503480      N/A     Disabled
5896    oneetx.exe      0xffffad818f035e50      0x3f00000       0x3f00fff       VadS    PAGE_READWRITE  1       1       0xffffad818ddc5200      N/A     Disabled
```



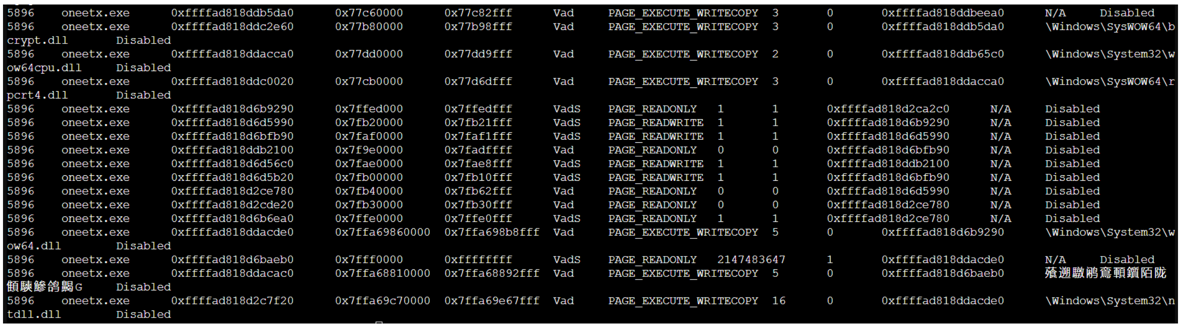
```
5896    oneetx.exe      0xffffad818f02a190      0x3770000       0x377ffff       VadS    PAGE_READWRITE  1       1       0xffffad818f035e50      N/A     Disabled
5896    oneetx.exe      0xffffad818ddc7460      0x35f0000       0x35f6fff       Vad     PAGE_READONLY   0       0       0xffffad818f02a190      \Windows\Registration\R0000
00000006.clb    Disabled
5896    oneetx.exe      0xffffad818ddc4260      0x3170000       0x34a7fff       Vad     PAGE_READONLY   0       0       0xffffad818ddc7460      N/A     Disabled
5896    oneetx.exe      0xffffad818c2a02b0      0x2e70000       0x2f6ffff       VadS    PAGE_READWRITE  4       1       0xffffad8190ac5480      N/A     Disabled
5896    oneetx.exe      0xffffad818d6c4c30      0x34b0000       0x34effff       VadS    PAGE_READWRITE  11      1       0xffffad818ddc4260      N/A     Disabled
5896    oneetx.exe      0xffffad818d6cd150      0x34f0000       0x35effff       VadS    PAGE_READWRITE  5       1       0xffffad818d6c4c30      N/A     Disabled
5896    oneetx.exe      0xffffad818ddc7a00      0x3750000       0x3753fff       Vad     PAGE_READONLY   0       0       0xffffad818ddc7460      \ProgramData\Microsoft\Wind
ows\Caches\cversions.2.db       Disabled
5896    oneetx.exe      0xffffad818f02b310      0x3600000       0x360ffff       VadS    PAGE_NOACCESS   1       1       0xffffad818ddc7a00      N/A     Disabled
5896    oneetx.exe      0xffffad818ddc75a0      0x3760000       0x3763fff       Vad     PAGE_READONLY   0       0       0xffffad818ddc7a00      \ProgramData\Microsoft\Wind
ows\Caches\cversions.2.db       Disabled
5896    oneetx.exe      0xffffad818ddc7640      0x39b0000       0x39bffff       Vad     PAGE_READONLY   0       0       0xffffad818f02a190      \Windows\System32\en-GB\pro
psys.dll.mui    Disabled
5896    oneetx.exe      0xffffad818ddc7500      0x38c0000       0x3908fff       Vad     PAGE_READONLY   0       0       0xffffad818ddc7640      翀ß□_
                                                                                                                                                   뾀ς°킠亡ળ Disabled
5896    oneetx.exe      0xffffad818ddc6c40      0x3910000       0x39abfff       Vad     PAGE_READONLY   0       0       0xffffad818ddc7500      \ProgramData\Microsoft\Wind
ows\Caches\{DDF571F2-BE98-426D-8288-1A9A39C3FDA2}.2.ver0x0000000000000001.db    Disabled
5896    oneetx.exe      0xffffad818ddc7b40      0x39d0000       0x39e9fff       Vad     PAGE_READONLY   0       0       0xffffad818ddc7640      \Users\Tammam\AppData\Local
\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000001.db     Disabled
5896    oneetx.exe      0xffffad818ddcfd40      0x39c0000       0x39c0fff       Vad     PAGE_READWRITE  0       0       0xffffad818ddc7b40      N/A     Disabled
5896    oneetx.exe      0xffffad818ddc8f40      0x39f0000       0x39f0fff       Vad     PAGE_READWRITE  0       0       0xffffad818ddc7b40      N/A     Disabled
5896    oneetx.exe      0xffffad818ddd4160      0x4090000       0x4090fff       Vad     PAGE_READONLY   0       0       0xffffad818f035e50      N/A     Disabled
5896    oneetx.exe      0xffffad818ddd29a0      0x4070000       0x4070fff       Vad     PAGE_READONLY   0       0       0xffffad818ddd4160      N/A     Disabled
5896    oneetx.exe      0xffffad818f035ea0      0x3f10000       0x3f10fff       VadS    PAGE_READWRITE  1       1       0xffffad818ddd29a0      N/A     Disabled
5896    oneetx.exe      0xffffad818ddae140      0x4060000       0x4060fff       Vad     PAGE_READWRITE  0       0       0xffffad818f035ea0      N/A     Disabled
5896    oneetx.exe      0xffffad818ddd3c60      0x4080000       0x408ffff       Vad     PAGE_READONLY   0       0       0xffffad818ddd29a0      N/A     Disabled
5896    oneetx.exe      0xffffad8189d257b0      0x4220000       0x4223fff       Vad     PAGE_READONLY   0       0       0xffffad818ddd4160      \ProgramData\Microsoft\Wind
ows\Caches\cversions.2.db       Disabled
5896    oneetx.exe      0xffffad818ddd4340      0x40b0000       0x40b2fff       Vad     PAGE_READONLY   0       0       0xffffad8189d257b0      \Windows\System32\en-US\msw
sock.dll.mui    Disabled
5896    oneetx.exe      0xffffad818ddd34e0      0x40a0000       0x40a0fff       Vad     PAGE_READWRITE  0       0       0xffffad818ddd4340      N/A     Disabled
5896    oneetx.exe      0xffffad818ddd3940      0x40c0000       0x40d0fff       Vad     PAGE_READONLY   0       0       0xffffad818ddd4340      N/A     Disabled
5896    oneetx.exe      0xffffad818ddc46c0      0x73050000      0x730c2fff      Vad     PAGE_EXECUTE_WRITECOPY  4       0       0xffffad8189d257b0      \Windows\SysWOW64\w
inspool.drv     Disabled
5896    oneetx.exe      0xffffad818ddc43a0      0x6c5a0000      0x6c9f3fff      Vad     PAGE_EXECUTE_WRITECOPY  6       0       0xffffad818ddc46c0      蒌ル護Ǔ蒌ル護Ǔ蒌ル
護Ǔ蒌ル護Ǔ      Disabled
5896    oneetx.exe      0xffffad818ddae460      0x76390000      0x7647ffff      Vad     PAGE_EXECUTE_WRITECOPY  5       0       0xffffad818ddb2c40      N/A     Disabled
```



```
5896    oneetx.exe      0xffffad818ddc4b20      0x754e0000      0x754eefff      Vad     PAGE_EXECUTE_WRITECOPY  3       0       0xffffad818ddae460      N/A     Disabled
5896    oneetx.exe      0xffffad818ddc7820      0x750c0000      0x750d7fff      Vad     PAGE_EXECUTE_WRITECOPY  3       0       0xffffad818ddc4b20      \Windows\SysWOW64\p
rofapi.dll      Disabled
5896    oneetx.exe      0xffffad818ddd1a00      0x74bb0000      0x74be1fff      Vad     PAGE_EXECUTE_WRITECOPY  3       0       0xffffad818ddc7820      \Windows\SysWOW64\I
PHLPAPI.DLL     Disabled
5896    oneetx.exe      0xffffad818ddd01a0      0x74550000      0x74561fff      Vad     PAGE_EXECUTE_WRITECOPY  3       0       0xffffad818ddd1a00      \Windows\SysWOW64\O
nDemandConnRouteHelper.dll      Disabled
5896    oneetx.exe      0xffffad818ddc5a20      0x743b0000      0x74471fff      Vad     PAGE_EXECUTE_WRITECOPY  3       0       0xffffad818ddd01a0      \Windows\SysWOW64\p
ropsys.dll      Disabled
5896    oneetx.exe      0xffffad818ddcdae0      0x740e0000      0x74287fff      Vad     PAGE_EXECUTE_WRITECOPY  14      0       0xffffad818ddc5a20      \Windows\SysWOW64\u
rlmon.dll       Disabled
5896    oneetx.exe      0xffffad818ddd1960      0x74490000      0x744e1fff      Vad     PAGE_EXECUTE_WRITECOPY  4       0       0xffffad818ddc5a20      \Windows\SysWOW64\m
swsock.dll      Disabled
5896    oneetx.exe      0xffffad818ddd0240      0x74a50000      0x74b18fff      Vad     PAGE_EXECUTE_WRITECOPY  4       0       0xffffad818ddd01a0      \Windows\SysWOW64\w
inhttp.dll      Disabled
5896    oneetx.exe      0xffffad818ddce580      0x74e30000      0x74e50fff      Vad     PAGE_EXECUTE_WRITECOPY  3       0       0xffffad818ddd1a00      1.1.mum Disabled
5896    oneetx.exe      0xffffad818ddcdcc0      0x74e90000      0x750bcfff      Vad     PAGE_EXECUTE_WRITECOPY  10      0       0xffffad818ddce580      \Windows\SysWOW64\i
ertutil.dll     Disabled
5896    oneetx.exe      0xffffad818ddcbf60      0x752d0000      0x752eafff      Vad     PAGE_EXECUTE_WRITECOPY  3       0       0xffffad818ddc7820      \Windows\SysWOW64\e
dputil.dll      Disabled
5896    oneetx.exe      0xffffad818ddccf00      0x751f0000      0x7520cfff      Vad     PAGE_EXECUTE_WRITECOPY  11      0       0xffffad818ddcbf60      \Windows\SysWOW64\s
rvcli.dll       Disabled
5896    oneetx.exe      0xffffad818ddce940      0x751e0000      0x751eafff      Vad     PAGE_EXECUTE_WRITECOPY  2       0       0xffffad818ddccf00      \Windows\SysWOW64\n
etutils.dll     Disabled
5896    oneetx.exe      0xffffad818ddd2040      0x752f0000      0x752f7fff      Vad     PAGE_EXECUTE_WRITECOPY  2       0       0xffffad818ddcbf60      \Windows\SysWOW64\w
innsi.dll       Disabled
5896    oneetx.exe      0xffffad818ddbe9a0      0x76090000      0x76125fff      Vad     PAGE_EXECUTE_WRITECOPY  4       0       0xffffad818ddc4b20      N/A     Disabled
5896    oneetx.exe      0xffffad818ddb3b40      0x75b50000      0x75beefff      Vad     PAGE_EXECUTE_WRITECOPY  3       0       0xffffad818ddbe9a0      \Windows\SysWOW64\a
pphelp.dll      Disabled
5896    oneetx.exe      0xffffad818ddc57a0      0x75510000      0x75536fff      Vad     PAGE_EXECUTE_WRITECOPY  3       0       0xffffad818ddb3b40      \Windows\SysWOW64\w
ldp.dll Disabled
5896    oneetx.exe      0xffffad818ddc2f00      0x754f0000      0x75508fff      Vad     PAGE_EXECUTE_WRITECOPY  3       0       0xffffad818ddc57a0      \Windows\SysWOW64\m
pr.dll  Disabled
5896    oneetx.exe      0xffffad818ddc66a0      0x75540000      0x75b4cfff      Vad     PAGE_EXECUTE_WRITECOPY  9       0       0xffffad818ddc57a0      \Windows\SysWOW64\w
indows.storage.dll      Disabled
5896    oneetx.exe      0xffffad818ddb4180      0x75d90000      0x75e4efff      Vad     PAGE_EXECUTE_WRITECOPY  7       0       0xffffad818ddb3b40      \Windows\SysWOW64\m
svcrt.dll       Disabled
5896    oneetx.exe      0xffffad818ddc5980      0x75ca0000      0x75caefff      Vad     PAGE_EXECUTE_WRITECOPY  3       0       0xffffad818ddb4180      城倀城倀城倀城倀城
倀城倀城倀城倀城倀城倀城倀城倀城倀城倀城倀城倀城倀城倀城倀城倀  Disabled
```

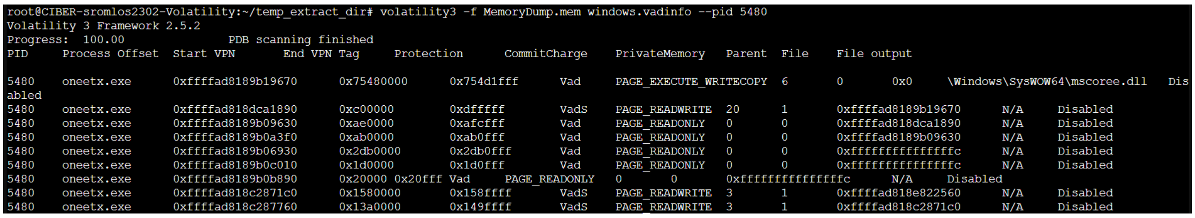


```
5896    oneetx.exe      0xffffad818ddac700      0x75c20000      0x75c93fff      Vad     PAGE_EXECUTE_WRITECOPY  5       0       0xffffad818ddc5980      \Windows\SysWOW64\u
xtheme.dll      Disabled
5896    oneetx.exe      0xffffad818ddb56c0      0x75cb0000      0x75d2afff      Vad     PAGE_EXECUTE_WRITECOPY  5       0       0xffffad818ddc5980      \Windows\SysWOW64\m
svcp_win.dll    Disabled
5896    oneetx.exe      0xffffad818ddc4d00      0x75eb0000      0x75f0efff      Vad     PAGE_EXECUTE_WRITECOPY  2       0       0xffffad818ddb4180      \Windows\SysWOW64\b
cryptprimitives.dll     Disabled
5896    oneetx.exe      0xffffad818ddd2860      0x75f10000      0x75f16fff      Vad     PAGE_EXECUTE_WRITECOPY  2       0       0xffffad818ddc4d00      \Windows\SysWOW64\n
si.dll  Disabled
5896    oneetx.exe      0xffffad818ddc6380      0x76220000      0x7629dfff      Vad     PAGE_EXECUTE_WRITECOPY  6       0       0xffffad818ddbe9a0      \Windows\SysWOW64\c
lbcatq.dll      Disabled
5896    oneetx.exe      0xffffad818ddc5660      0x76130000      0x76212fff      Vad     PAGE_EXECUTE_WRITECOPY  4       0       0xffffad818ddc6380      N/A     Disabled
5896    oneetx.exe      0xffffad818ddc5520      0x762a0000      0x7631afff      Vad     PAGE_EXECUTE_WRITECOPY  6       0       0xffffad818ddc6380      \Windows\SysWOW64\a
dvapi32.dll     Disabled
5896    oneetx.exe      0xffffad818ddc4a80      0x76320000      0x76382fff      Vad     PAGE_EXECUTE_WRITECOPY  3       0       0xffffad818ddc5520      \Windows\SysWOW64\w
s2_32.dll       Disabled
5896    oneetx.exe      0xffffad818d2ca2c0      0x77de0000      0x77f83fff      Vad     PAGE_EXECUTE_WRITECOPY  9       0       0xffffad818ddae460      \Windows\SysWOW64\n
tdll.dll        Disabled
5896    oneetx.exe      0xffffad818ddb62a0      0x77620000      0x777bafff      Vad     PAGE_EXECUTE_WRITECOPY  8       0       0xffffad818d2ca2c0      \Windows\SysWOW64\u
ser32.dll       Disabled
5896    oneetx.exe      0xffffad818ddbe540      0x76d00000      0x76d44fff      Vad     PAGE_EXECUTE_WRITECOPY  3       0       0xffffad818ddb62a0      \Windows\SysWOW64\s
hlwapi.dll      Disabled
5896    oneetx.exe      0xffffad818ddadf60      0x76a50000      0x76c68fff      Vad     PAGE_EXECUTE_WRITECOPY  6       0       0xffffad818ddbe540      \Windows\SysWOW64\K
ernelBase.dll   Disabled
5896    oneetx.exe      0xffffad818ddbf760      0x76610000      0x76a48fff      Vad     PAGE_EXECUTE_WRITECOPY  3       0       0xffffad818ddadf60      \Windows\SysWOW64\s
etupapi.dll     Disabled
5896    oneetx.exe      0xffffad818ddc4bc0      0x76c70000      0x76ce5fff      Vad     PAGE_EXECUTE_WRITECOPY  5       0       0xffffad818ddadf60      \Windows\SysWOW64\s
echost.dll      Disabled
5896    oneetx.exe      0xffffad818ddb54e0      0x773f0000      0x774ccfff      Vad     PAGE_EXECUTE_WRITECOPY  5       0       0xffffad818ddbe540      \Windows\SysWOW64\g
di32full.dll    Disabled
5896    oneetx.exe      0xffffad818ddb7920      0x76e30000      0x773e4fff      Vad     PAGE_EXECUTE_WRITECOPY  11      0       0xffffad818ddb54e0      N/A     Disabled
5896    oneetx.exe      0xffffad818ddc4440      0x76da0000      0x76e26fff      Vad     PAGE_EXECUTE_WRITECOPY  3       0       0xffffad818ddb7920      N/A     Disabled
5896    oneetx.exe      0xffffad818ddb5800      0x774d0000      0x775effff      Vad     PAGE_EXECUTE_WRITECOPY  3       0       0xffffad818ddb54e0      \Windows\SysWOW64\u
crtbase.dll     Disabled
5896    oneetx.exe      0xffffad818ddc5480      0x775f0000      0x77614fff      Vad     PAGE_EXECUTE_WRITECOPY  3       0       0xffffad818ddb5800      \Windows\SysWOW64\i
mm32.dll        Disabled
5896    oneetx.exe      0xffffad818ddb65c0      0x77c90000      0x77ca7fff      Vad     PAGE_EXECUTE_WRITECOPY  2       0       0xffffad818ddb62a0      \Windows\SysWOW64\w
in32u.dll       Disabled
5896    oneetx.exe      0xffffad818ddbeea0      0x77900000      0x77b7ffff      Vad     PAGE_EXECUTE_WRITECOPY  6       0       0xffffad818ddb65c0      \Windows\SysWOW64\c
ombase.dll      Disabled
5896    oneetx.exe      0xffffad818ddc12e0      0x777c0000      0x777fafff      Vad     PAGE_EXECUTE_WRITECOPY  3       0       0xffffad818ddbeea0      \Windows\SysWOW64\c
fgmgr32.dll     Disabled
```



```
5896    oneetx.exe      0xffffad818ddb5da0      0x77c60000      0x77c82fff      Vad     PAGE_EXECUTE_WRITECOPY  3       0       0xffffad818ddbeea0      N/A     Disabled
5896    oneetx.exe      0xffffad818ddc2e60      0x77b80000      0x77b98fff      Vad     PAGE_EXECUTE_WRITECOPY  3       0       0xffffad818ddb5da0      \Windows\SysWOW64\b
crypt.dll       Disabled
5896    oneetx.exe      0xffffad818ddacca0      0x77dd0000      0x77dd9fff      Vad     PAGE_EXECUTE_WRITECOPY  2       0       0xffffad818ddb65c0      \Windows\System32\w
ow64cpu.dll     Disabled
5896    oneetx.exe      0xffffad818ddc0020      0x77cb0000      0x77d6dfff      Vad     PAGE_EXECUTE_WRITECOPY  3       0       0xffffad818ddacca0      \Windows\SysWOW64\r
pcrt4.dll       Disabled
5896    oneetx.exe      0xffffad818d6b9290      0x7ffed000      0x7ffedfff      VadS    PAGE_READONLY   1       1       0xffffad818d2ca2c0      N/A     Disabled
5896    oneetx.exe      0xffffad818d6d5990      0x7fb20000      0x7fb21fff      VadS    PAGE_READWRITE  1       1       0xffffad818d6b9290      N/A     Disabled
5896    oneetx.exe      0xffffad818d6bfb90      0x7faf0000      0x7faf1fff      VadS    PAGE_READWRITE  1       1       0xffffad818d6d5990      N/A     Disabled
5896    oneetx.exe      0xffffad818ddb2100      0x7f9e0000      0x7fadffff      Vad     PAGE_READONLY   0       0       0xffffad818d6bfb90      N/A     Disabled
5896    oneetx.exe      0xffffad818d6d56c0      0x7fae0000      0x7fae8fff      VadS    PAGE_READWRITE  1       1       0xffffad818ddb2100      N/A     Disabled
5896    oneetx.exe      0xffffad818d6d5b20      0x7fb00000      0x7fb10fff      VadS    PAGE_READWRITE  1       1       0xffffad818d6bfb90      N/A     Disabled
5896    oneetx.exe      0xffffad818d2ce780      0x7fb40000      0x7fb62fff      Vad     PAGE_READONLY   0       0       0xffffad818d6d5990      N/A     Disabled
5896    oneetx.exe      0xffffad818d2cde20      0x7fb30000      0x7fb30fff      Vad     PAGE_READONLY   0       0       0xffffad818d2ce780      N/A     Disabled
5896    oneetx.exe      0xffffad818d6b6ea0      0x7ffe0000      0x7ffe0fff      VadS    PAGE_READONLY   1       1       0xffffad818d2ce780      N/A     Disabled
5896    oneetx.exe      0xffffad818ddacde0      0x7ffa69860000  0x7ffa698b8fff  Vad     PAGE_EXECUTE_WRITECOPY  5       0       0xffffad818d6b9290      \Windows\System32\w
ow64.dll        Disabled
5896    oneetx.exe      0xffffad818d6baeb0      0x7fff0000      0xffffffff      VadS    PAGE_READONLY   2147483647      1       0xffffad818ddacde0      N/A     Disabled
5896    oneetx.exe      0xffffad818ddacac0      0x7ffa68810000  0x7ffa68892fff  Vad     PAGE_EXECUTE_WRITECOPY  5       0       0xffffad818d6baeb0      殖遡斅鹇鴬頼鑦陌陇
餇贌鰺鴿鷃G     Disabled
5896    oneetx.exe      0xffffad818d2c7f20      0x7ffa69c70000  0x7ffa69e67fff  Vad     PAGE_EXECUTE_WRITECOPY  16      0       0xffffad818ddacde0      \Windows\System32\n
tdll.dll        Disabled
```

volatility3 -f MemoryDump.mem windows.vadinfo --pid 5480



```
root@CIBER-sromlos2302-Volatility:~/temp_extract_dir# volatility3 -f MemoryDump.mem windows.vadinfo --pid 5480
Volatility 3 Framework 2.5.2
Progress:  100.00               PDB scanning finished
PID     Process Offset  Start VPN       End VPN Tag     Protection      CommitCharge    PrivateMemory   Parent  File    File output

5480    oneetx.exe      0xffffad8189b19670      0x75480000      0x754d1fff      Vad     PAGE_EXECUTE_WRITECOPY  6       0       0x0     \Windows\SysWOW64\mscoree.dll   Dis
abled
5480    oneetx.exe      0xffffad818dca1890      0xc00000        0xdfffff        VadS    PAGE_READWRITE  20      1       0xffffad8189b19670      N/A     Disabled
5480    oneetx.exe      0xffffad8189b09630      0xae0000        0xafcfff        Vad     PAGE_READONLY   0       0       0xffffad818dca1890      N/A     Disabled
5480    oneetx.exe      0xffffad8189b0a3f0      0xab0000        0xab0fff        Vad     PAGE_READONLY   0       0       0xffffad8189b09630      N/A     Disabled
5480    oneetx.exe      0xffffad8189b06930      0x2db0000       0x2db0fff       Vad     PAGE_READONLY   0       0       0xfffffffffffffffc      N/A     Disabled
5480    oneetx.exe      0xffffad8189b0c010      0x1d0000        0x1d0fff        Vad     PAGE_READONLY   0       0       0xfffffffffffffffc      N/A     Disabled
5480    oneetx.exe      0xffffad8189b0b890      0x20000 0x20fff Vad     PAGE_READONLY   0       0       0xfffffffffffffffc      N/A     Disabled
5480    oneetx.exe      0xffffad818c2871c0      0x1580000       0x158ffff       VadS    PAGE_READWRITE  3       1       0xffffad818e822560      N/A     Disabled
5480    oneetx.exe      0xffffad818c287760      0x13a0000       0x149ffff       VadS    PAGE_READWRITE  3       1       0xffffad818c2871c0      N/A     Disabled
```

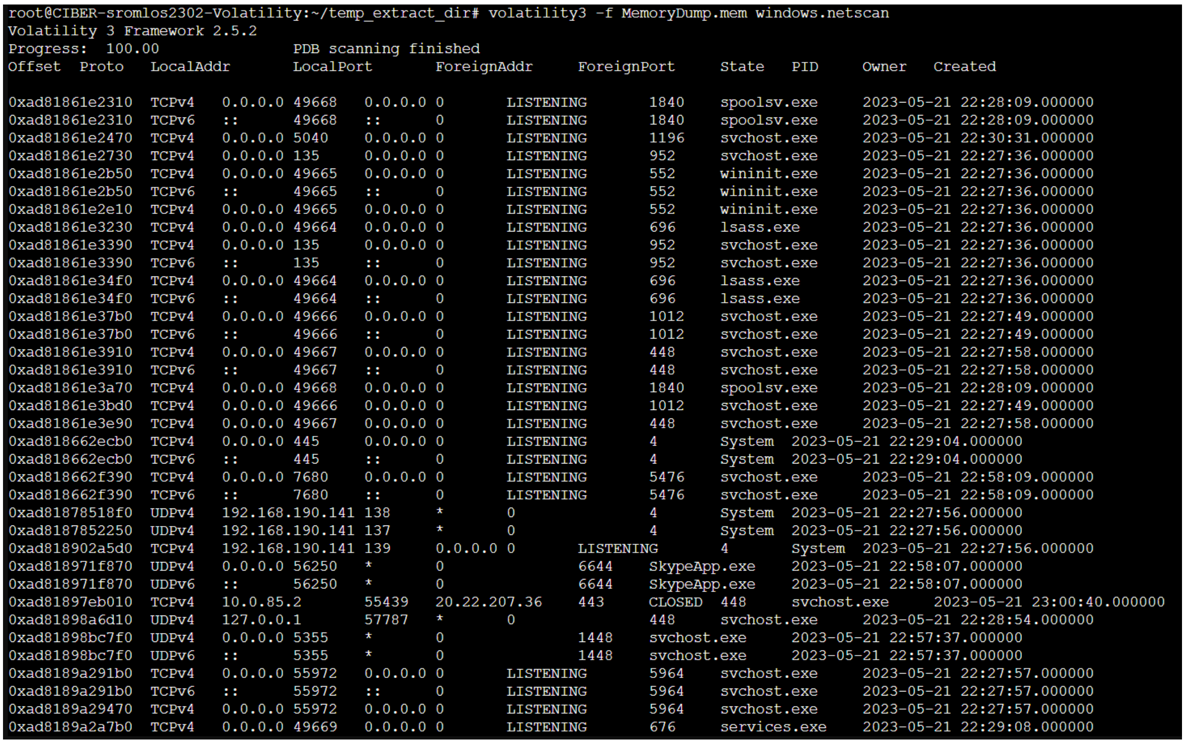
Para el proceso sospechoso oneetx.exe (PID 5896): en la columna Protection aparecen muchas regiones con distintos permisos, pero una de ellas muestra claramente **PAGE_EXECUTE_READWRITE** (en el rango que empieza en 0x400000), lo que indica una zona de memoria que se puede leer, escribir y además ejecutar, algo muy típico en código malicioso o inyección en memoria, por eso esa es la protección de memoria relevante y sospechosa que se pide en la pregunta.

Ejercicio 4

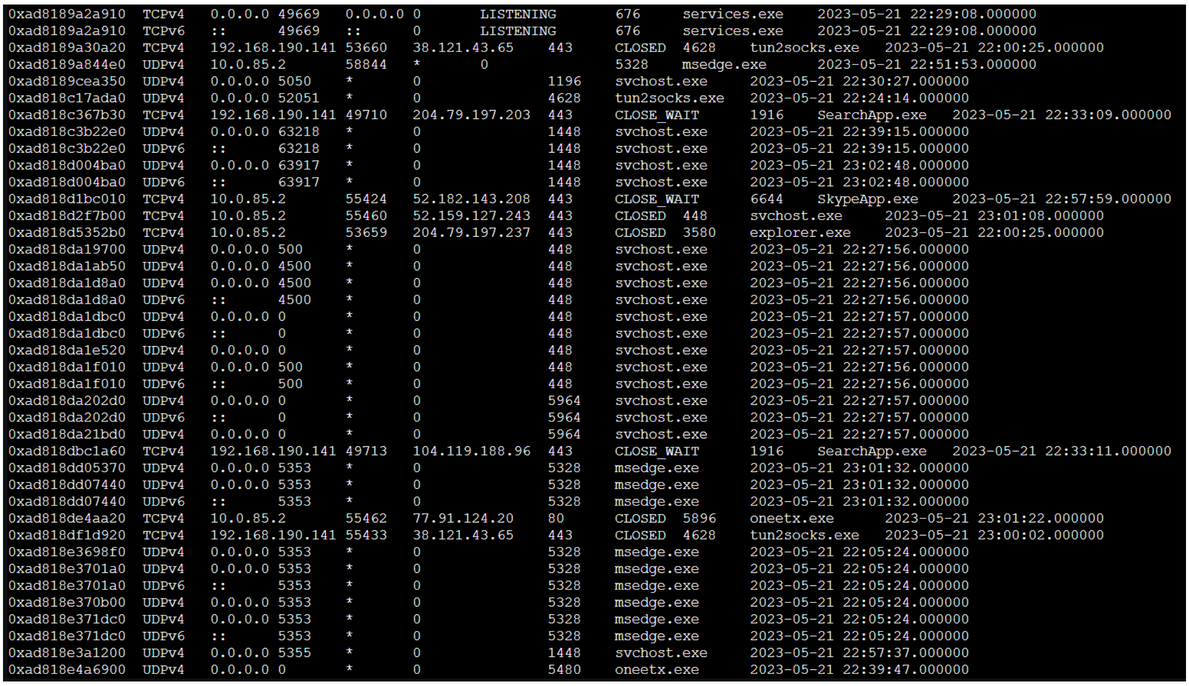
El proceso principal de la aplicación VPN instalada en el sistema es quien inicia, gestiona y mantiene la conexión cifrada. Aunque tun2socks.exe aparece como un proceso relacionado, este solo actúa como componente auxiliar encargado de redirigir el tráfico, mientras que el origen y controlador de toda la conexión VPN es **Outline.exe**, que además aparece como proceso padre en el árbol de procesos, confirmando que es la aplicación responsable de la conexión VPN.

Ejercicio 5

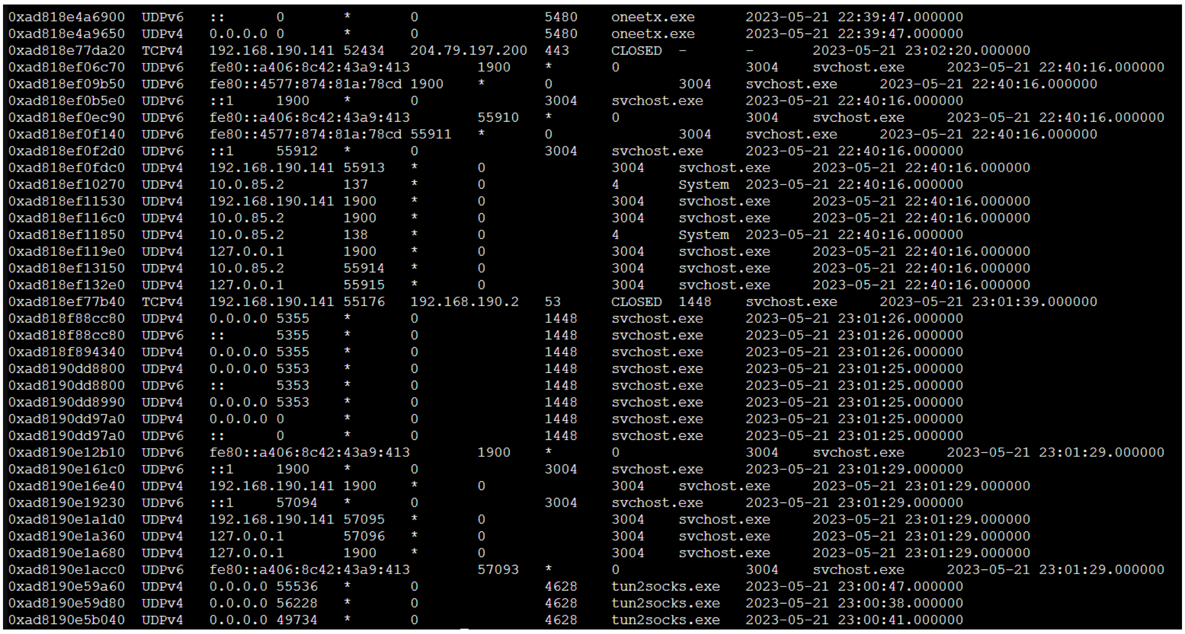
Para extraer todas las conexiones de red que existían en el sistema Windows cuando se creó el volcado de memoria, usamos el siguiente comando:
volatility3 -f MemoryDump.mem windows.netscan



```
root@CIBER-sromlos2302-Volatility:~/temp_extract_dir# volatility3 -f MemoryDump.mem windows.netscan
Volatility 3 Framework 2.5.2
Progress:  100.00               PDB scanning finished
Offset  Proto   LocalAddr       LocalPort       ForeignAddr     ForeignPort     State   PID     Owner   Created

0xad81861e2310  TCPv4   0.0.0.0 49668   0.0.0.0 0       LISTENING       1840    spoolsv.exe     2023-05-21 22:28:09.000000
0xad81861e2310  TCPv6   ::      49668   ::      0       LISTENING       1840    spoolsv.exe     2023-05-21 22:28:09.000000
0xad81861e2470  TCPv4   0.0.0.0 5040    0.0.0.0 0       LISTENING       1196    svchost.exe     2023-05-21 22:30:31.000000
0xad81861e2730  TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       952     svchost.exe     2023-05-21 22:27:36.000000
0xad81861e2b50  TCPv4   0.0.0.0 49665   0.0.0.0 0       LISTENING       552     wininit.exe     2023-05-21 22:27:36.000000
0xad81861e2b50  TCPv6   ::      49665   ::      0       LISTENING       552     wininit.exe     2023-05-21 22:27:36.000000
0xad81861e2e10  TCPv4   0.0.0.0 49665   0.0.0.0 0       LISTENING       552     wininit.exe     2023-05-21 22:27:36.000000
0xad81861e3230  TCPv4   0.0.0.0 49664   0.0.0.0 0       LISTENING       696     lsass.exe       2023-05-21 22:27:36.000000
0xad81861e3390  TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       952     svchost.exe     2023-05-21 22:27:36.000000
0xad81861e3390  TCPv6   ::      135     ::      0       LISTENING       952     svchost.exe     2023-05-21 22:27:36.000000
0xad81861e34f0  TCPv4   0.0.0.0 49664   0.0.0.0 0       LISTENING       696     lsass.exe       2023-05-21 22:27:36.000000
0xad81861e34f0  TCPv6   ::      49664   ::      0       LISTENING       696     lsass.exe       2023-05-21 22:27:36.000000
0xad81861e37b0  TCPv4   0.0.0.0 49666   0.0.0.0 0       LISTENING       1012    svchost.exe     2023-05-21 22:27:49.000000
0xad81861e37b0  TCPv6   ::      49666   ::      0       LISTENING       1012    svchost.exe     2023-05-21 22:27:49.000000
0xad81861e3910  TCPv4   0.0.0.0 49667   0.0.0.0 0       LISTENING       448     svchost.exe     2023-05-21 22:27:58.000000
0xad81861e3910  TCPv6   ::      49667   ::      0       LISTENING       448     svchost.exe     2023-05-21 22:27:58.000000
0xad81861e3a70  TCPv4   0.0.0.0 49668   0.0.0.0 0       LISTENING       1840    spoolsv.exe     2023-05-21 22:28:09.000000
0xad81861e3bd0  TCPv4   0.0.0.0 49666   0.0.0.0 0       LISTENING       1012    svchost.exe     2023-05-21 22:27:49.000000
0xad81861e3e90  TCPv4   0.0.0.0 49667   0.0.0.0 0       LISTENING       448     svchost.exe     2023-05-21 22:27:58.000000
0xad818662ecb0  TCPv4   0.0.0.0 445     0.0.0.0 0       LISTENING       4       System  2023-05-21 22:29:04.000000
0xad818662ecb0  TCPv6   ::      445     ::      0       LISTENING       4       System  2023-05-21 22:29:04.000000
0xad818662f390  TCPv4   0.0.0.0 7680    0.0.0.0 0       LISTENING       5476    svchost.exe     2023-05-21 22:58:09.000000
0xad818662f390  TCPv6   ::      7680    ::      0       LISTENING       5476    svchost.exe     2023-05-21 22:58:09.000000
0xad81878518f0  UDPv4   192.168.190.141 138     *       0               4       System  2023-05-21 22:27:56.000000
0xad8187852250  UDPv4   192.168.190.141 137     *       0               4       System  2023-05-21 22:27:56.000000
0xad818902a5d0  TCPv4   192.168.190.141 139     0.0.0.0 0       LISTENING       4       System  2023-05-21 22:27:56.000000
0xad818971f870  UDPv4   0.0.0.0 56250   *       0               6644    SkypeApp.exe    2023-05-21 22:58:07.000000
0xad818971f870  UDPv6   ::      56250   *       0               6644    SkypeApp.exe    2023-05-21 22:58:07.000000
0xad81897eb010  TCPv4   10.0.85.2       55439   20.22.207.36    443     CLOSED  448     svchost.exe     2023-05-21 23:00:40.000000
0xad81898a6d10  UDPv4   127.0.0.1       57787   *       0               448     svchost.exe     2023-05-21 22:28:54.000000
0xad81898bc7f0  UDPv4   0.0.0.0 5355    *       0               1448    svchost.exe     2023-05-21 22:57:37.000000
0xad81898bc7f0  UDPv6   ::      5355    *       0               1448    svchost.exe     2023-05-21 22:57:37.000000
0xad8189a291b0  TCPv4   0.0.0.0 55972   0.0.0.0 0       LISTENING       5964    svchost.exe     2023-05-21 22:27:57.000000
0xad8189a291b0  TCPv6   ::      55972   ::      0       LISTENING       5964    svchost.exe     2023-05-21 22:27:57.000000
0xad8189a29470  TCPv4   0.0.0.0 55972   0.0.0.0 0       LISTENING       5964    svchost.exe     2023-05-21 22:27:57.000000
0xad8189a2a7b0  TCPv4   0.0.0.0 49669   0.0.0.0 0       LISTENING       676     services.exe    2023-05-21 22:29:08.000000
```



```
0xad8189a2a910  TCPv4   0.0.0.0 49669   0.0.0.0 0       LISTENING       676     services.exe    2023-05-21 22:29:08.000000
0xad8189a2a910  TCPv6   ::      49669   ::      0       LISTENING       676     services.exe    2023-05-21 22:29:08.000000
0xad8189a30a20  TCPv4   192.168.190.141 53660   38.121.43.65    443     CLOSED  4628    tun2socks.exe   2023-05-21 22:00:25.000000
0xad8189a844e0  UDPv4   10.0.85.2       58844   *       0               5328    msedge.exe      2023-05-21 22:51:53.000000
0xad8189cea350  UDPv4   0.0.0.0 5050    *       0               1196    svchost.exe     2023-05-21 22:30:27.000000
0xad818c17ada0  UDPv4   0.0.0.0 52051   *       0               4628    tun2socks.exe   2023-05-21 22:24:14.000000
0xad818c367b30  TCPv4   192.168.190.141 49710   204.79.197.203  443     CLOSE_WAIT      1916    SearchApp.exe   2023-05-21 22:33:09.000000
0xad818c3b22e0  UDPv4   0.0.0.0 63218   *       0               1448    svchost.exe     2023-05-21 22:39:15.000000
0xad818c3b22e0  UDPv6   ::      63218   *       0               1448    svchost.exe     2023-05-21 22:39:15.000000
0xad818d004ba0  UDPv4   0.0.0.0 63917   *       0               1448    svchost.exe     2023-05-21 23:02:48.000000
0xad818d004ba0  UDPv6   ::      63917   *       0               1448    svchost.exe     2023-05-21 23:02:48.000000
0xad818d1bc010  TCPv4   10.0.85.2       55424   52.182.143.208  443     CLOSE_WAIT      6644    SkypeApp.exe    2023-05-21 22:57:59.000000
0xad818d2f7b00  TCPv4   10.0.85.2       55460   52.159.127.243  443     CLOSED  448     svchost.exe     2023-05-21 23:01:08.000000
0xad818d5352b0  TCPv4   10.0.85.2       53659   204.79.197.237  443     CLOSED  3580    explorer.exe    2023-05-21 22:00:25.000000
0xad818da19700  UDPv4   0.0.0.0 500     *       0               448     svchost.exe     2023-05-21 22:27:56.000000
0xad818da1ab50  UDPv4   0.0.0.0 4500    *       0               448     svchost.exe     2023-05-21 22:27:56.000000
0xad818da1d8a0  UDPv4   0.0.0.0 4500    *       0               448     svchost.exe     2023-05-21 22:27:56.000000
0xad818da1d8a0  UDPv6   ::      4500    *       0               448     svchost.exe     2023-05-21 22:27:56.000000
0xad818da1dbc0  UDPv4   0.0.0.0 0       *       0               448     svchost.exe     2023-05-21 22:27:57.000000
0xad818da1dbc0  UDPv6   ::      0       *       0               448     svchost.exe     2023-05-21 22:27:57.000000
0xad818da1e520  UDPv4   0.0.0.0 0       *       0               448     svchost.exe     2023-05-21 22:27:57.000000
0xad818da1f010  UDPv4   0.0.0.0 500     *       0               448     svchost.exe     2023-05-21 22:27:56.000000
0xad818da1f010  UDPv6   ::      500     *       0               448     svchost.exe     2023-05-21 22:27:56.000000
0xad818da202d0  UDPv4   0.0.0.0 0       *       0               5964    svchost.exe     2023-05-21 22:27:57.000000
0xad818da202d0  UDPv6   ::      0       *       0               5964    svchost.exe     2023-05-21 22:27:57.000000
0xad818da21bd0  UDPv4   0.0.0.0 0       *       0               5964    svchost.exe     2023-05-21 22:27:57.000000
0xad818dbc1a60  TCPv4   192.168.190.141 49713   104.119.188.96  443     CLOSE_WAIT      1916    SearchApp.exe   2023-05-21 22:33:11.000000
0xad818dd05370  UDPv4   0.0.0.0 5353    *       0               5328    msedge.exe      2023-05-21 23:01:32.000000
0xad818dd07440  UDPv4   0.0.0.0 5353    *       0               5328    msedge.exe      2023-05-21 23:01:32.000000
0xad818dd07440  UDPv6   ::      5353    *       0               5328    msedge.exe      2023-05-21 23:01:32.000000
0xad818de4aa20  TCPv4   10.0.85.2       55462   77.91.124.20    80      CLOSED  5896    oneetx.exe      2023-05-21 23:01:22.000000
0xad818df1d920  TCPv4   192.168.190.141 55433   38.121.43.65    443     CLOSED  4628    tun2socks.exe   2023-05-21 23:00:02.000000
0xad818e3698f0  UDPv4   0.0.0.0 5353    *       0               5328    msedge.exe      2023-05-21 22:05:24.000000
0xad818e3701a0  UDPv4   0.0.0.0 5353    *       0               5328    msedge.exe      2023-05-21 22:05:24.000000
0xad818e3701a0  UDPv6   ::      5353    *       0               5328    msedge.exe      2023-05-21 22:05:24.000000
0xad818e370b00  UDPv4   0.0.0.0 5353    *       0               5328    msedge.exe      2023-05-21 22:05:24.000000
0xad818e371dc0  UDPv4   0.0.0.0 5353    *       0               5328    msedge.exe      2023-05-21 22:05:24.000000
0xad818e371dc0  UDPv6   ::      5353    *       0               5328    msedge.exe      2023-05-21 22:05:24.000000
0xad818e3a1200  UDPv4   0.0.0.0 5355    *       0               1448    svchost.exe     2023-05-21 22:57:37.000000
0xad818e4a6900  UDPv4   0.0.0.0 0       *       0               5480    oneetx.exe      2023-05-21 22:39:47.000000
```



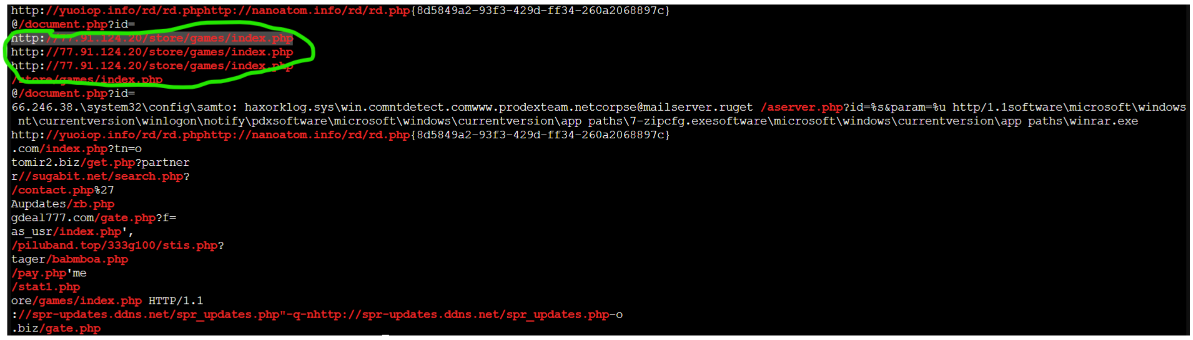
```
0xad818e4a6900  UDPv6   ::      0       *       0               5480    oneetx.exe      2023-05-21 22:39:47.000000
0xad818e4a9650  UDPv4   0.0.0.0 0       *       0               5480    oneetx.exe      2023-05-21 22:39:47.000000
0xad818e77da20  TCPv4   192.168.190.141 52434   204.79.197.200  443     CLOSED  -       -       2023-05-21 23:02:20.000000
0xad818ef06c70  UDPv6   fe80::a406:8c42:43a9:413        1900    *       0               3004    svchost.exe     2023-05-21 22:40:16.000000
0xad818ef09b50  UDPv6   fe80::4577:874:81a:78cd 1900    *       0               3004    svchost.exe     2023-05-21 22:40:16.000000
0xad818ef0b5e0  UDPv6   ::1     1900    *       0               3004    svchost.exe     2023-05-21 22:40:16.000000
0xad818ef0ec90  UDPv6   fe80::a406:8c42:43a9:413        55910   *       0               3004    svchost.exe     2023-05-21 22:40:16.000000
0xad818ef0f140  UDPv6   fe80::4577:874:81a:78cd 55911   *       0               3004    svchost.exe     2023-05-21 22:40:16.000000
0xad818ef0f2d0  UDPv6   ::1     55912   *       0               3004    svchost.exe     2023-05-21 22:40:16.000000
0xad818ef0fdc0  UDPv4   192.168.190.141 55913   *       0               3004    svchost.exe     2023-05-21 22:40:16.000000
0xad818ef10270  UDPv4   10.0.85.2       137     *       0               4       System  2023-05-21 22:40:16.000000
0xad818ef11530  UDPv4   192.168.190.141 1900    *       0               3004    svchost.exe     2023-05-21 22:40:16.000000
0xad818ef116c0  UDPv4   10.0.85.2       1900    *       0               3004    svchost.exe     2023-05-21 22:40:16.000000
0xad818ef11850  UDPv4   10.0.85.2       138     *       0               4       System  2023-05-21 22:40:16.000000
0xad818ef119e0  UDPv4   127.0.0.1       1900    *       0               3004    svchost.exe     2023-05-21 22:40:16.000000
0xad818ef13150  UDPv4   10.0.85.2       55914   *       0               3004    svchost.exe     2023-05-21 22:40:16.000000
0xad818ef132e0  UDPv4   127.0.0.1       55915   *       0               3004    svchost.exe     2023-05-21 22:40:16.000000
0xad818ef77b40  TCPv4   192.168.190.141 55176   192.168.190.2   53      CLOSED  1448    svchost.exe     2023-05-21 23:01:39.000000
0xad818f88cc80  UDPv4   0.0.0.0 5355    *       0               1448    svchost.exe     2023-05-21 23:01:26.000000
0xad818f88cc80  UDPv6   ::      5355    *       0               1448    svchost.exe     2023-05-21 23:01:26.000000
0xad818f894340  UDPv4   0.0.0.0 5355    *       0               1448    svchost.exe     2023-05-21 23:01:26.000000
0xad8190dd8800  UDPv4   0.0.0.0 5353    *       0               1448    svchost.exe     2023-05-21 23:01:25.000000
0xad8190dd8800  UDPv6   ::      5353    *       0               1448    svchost.exe     2023-05-21 23:01:25.000000
0xad8190dd8990  UDPv4   0.0.0.0 5353    *       0               1448    svchost.exe     2023-05-21 23:01:25.000000
0xad8190dd97a0  UDPv4   0.0.0.0 0       *       0               1448    svchost.exe     2023-05-21 23:01:25.000000
0xad8190dd97a0  UDPv6   ::      0       *       0               1448    svchost.exe     2023-05-21 23:01:25.000000
0xad8190e12b10  UDPv6   fe80::a406:8c42:43a9:413        1900    *       0               3004    svchost.exe     2023-05-21 23:01:29.000000
0xad8190e161c0  UDPv6   ::1     1900    *       0               3004    svchost.exe     2023-05-21 23:01:29.000000
0xad8190e16e40  UDPv4   192.168.190.141 1900    *       0               3004    svchost.exe     2023-05-21 23:01:29.000000
0xad8190e19230  UDPv6   ::1     57094   *       0               3004    svchost.exe     2023-05-21 23:01:29.000000
0xad8190e1a1d0  UDPv4   192.168.190.141 57095   *       0               3004    svchost.exe     2023-05-21 23:01:29.000000
0xad8190e1a360  UDPv4   127.0.0.1       57096   *       0               3004    svchost.exe     2023-05-21 23:01:29.000000
0xad8190e1a680  UDPv4   127.0.0.1       1900    *       0               3004    svchost.exe     2023-05-21 23:01:29.000000
0xad8190e1acc0  UDPv6   fe80::a406:8c42:43a9:413        57093   *       0               3004    svchost.exe     2023-05-21 23:01:29.000000
0xad8190e59a60  UDPv4   0.0.0.0 55536   *       0               4628    tun2socks.exe   2023-05-21 23:00:47.000000
0xad8190e59d80  UDPv4   0.0.0.0 56228   *       0               4628    tun2socks.exe   2023-05-21 23:00:38.000000
0xad8190e5b040  UDPv4   0.0.0.0 49734   *       0               4628    tun2socks.exe   2023-05-21 23:00:41.000000
```

Se ve en la salida de windows.netscan que el proceso malicioso oneetx.exe (PID 5896) establece una conexión TCP desde la IP local 10.0.85.2 al puerto 80 de la IP remota **77.91.124.20**, que es la máquina a la que se conecta el malware, es decir, la del atacante.

Ejercicio 6

Vamos a volcar el proceso para analizarlo, para ello, usamos el siguiente comando: volatility3 -f MemoryDump.mem windows.memmap --pid 5896 --dump

Luego, vemos algunas URLs con el siguiente comando y vemos que hay algunas sospechosas (**http://77.91.124.20/store/games/index.php**):
strings * | grep -Ei "/[^]+\.php"



```
http://yuoiop.info/rd/rd.phphttp://nanoatom.info/rd/rd.php{8d5849a2-93f3-429d-ff34-260a2068897c}
@/document.php?id=
http://77.91.124.20/store/games/index.php
http://77.91.124.20/store/games/index.php
http://77.91.124.20/store/games/index.php
/store/games/index.php
@/document.php?id=
66.246.38.\system32\config\samto: haxorklog.sys\win.comntdetect.comwww.prodexteam.netcorpse@mailserver.ruget /aserver.php?id=%s&param=%u http/1.1software\microsoft\windows
 nt\currentversion\winlogon\notify\pdxsoftware\microsoft\windows\currentversion\app paths\7-zipcfg.exesoftware\microsoft\windows\currentversion\app paths\winrar.exe
http://yuoiop.info/rd/rd.phphttp://nanoatom.info/rd/rd.php{8d5849a2-93f3-429d-ff34-260a2068897c}
.com/index.php?tn=o
tomir2.biz/get.php?partner
r//sugabit.net/search.php?
/contact.php%27
Aupdates/rb.php
gdeal777.com/gate.php?f=
as_usr/index.php',
/piluband.top/333g100/stis.php?
tager/babmboa.php
/pay.php'me
/stat1.php
ore/games/index.php HTTP/1.1
://spr-updates.ddns.net/spr_updates.php"-q-nhttp://spr-updates.ddns.net/spr_updates.php-o
.biz/gate.php
```

Ejercicio 7

La ruta completa del ejecutable malicioso es **C:\Users\Tammam\AppData\Local\Temp\c3912af058\oneetx.exe** porque, al analizar el proceso sospechoso con windows.vadinfo, aparece una entrada VAD asociada a este archivo, indicando que fue cargado directamente desde esa ubicación. Además, la ruta está en una carpeta temporal del usuario, un lugar típico donde el malware se descarga y se ejecuta sin permisos elevados, lo que confirma que este ejecutable es el que el atacante utilizó para comprometer el sistema.