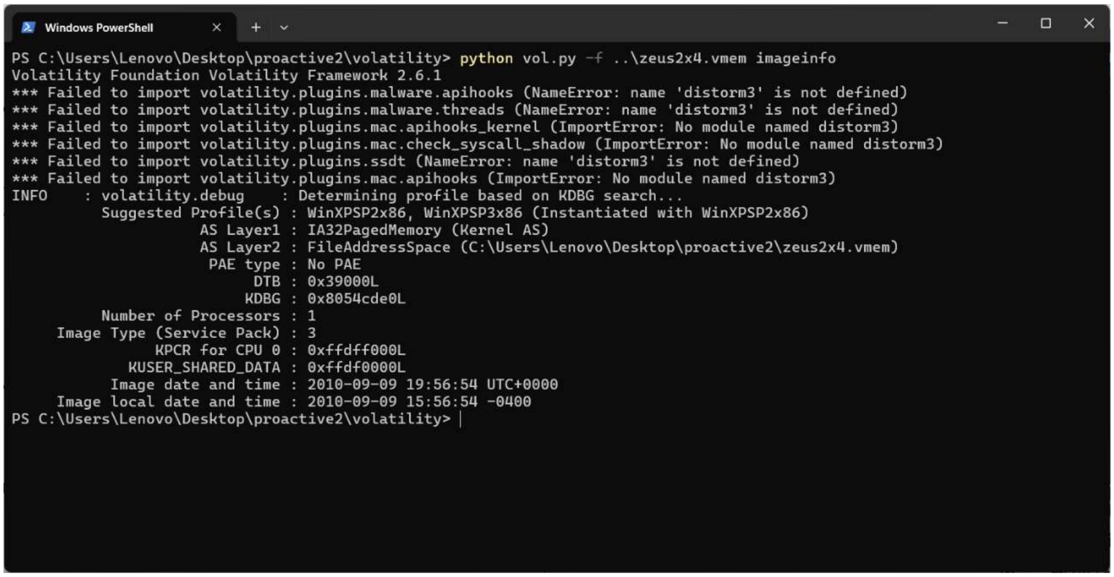
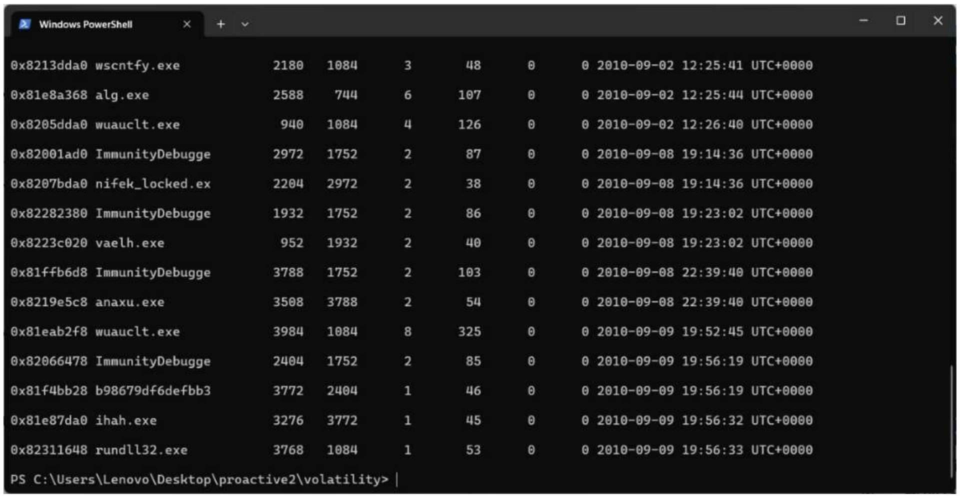
Memory Analysis of Zeus with Volatility

- **we started by identifying the profile of the image using imageinfo plugin**



```
PS C:\Users\Lenovo\Desktop\proactive2\volatility> python vol.py -f ..\zeus2x4.vmem imageinfo
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (C:\Users\Lenovo\Desktop\proactive2\zeus2x4.vmem)
                      PAE type : No PAE
                           DTB : 0x39000L
                          KDBG : 0x8054cde0L
          Number of Processors : 1
     Image Type (Service Pack) : 3
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2010-09-09 19:56:54 UTC+0000
     Image local date and time : 2010-09-09 15:56:54 -0400
PS C:\Users\Lenovo\Desktop\proactive2\volatility> |
```

- **Listing all the process using pslist plugin**



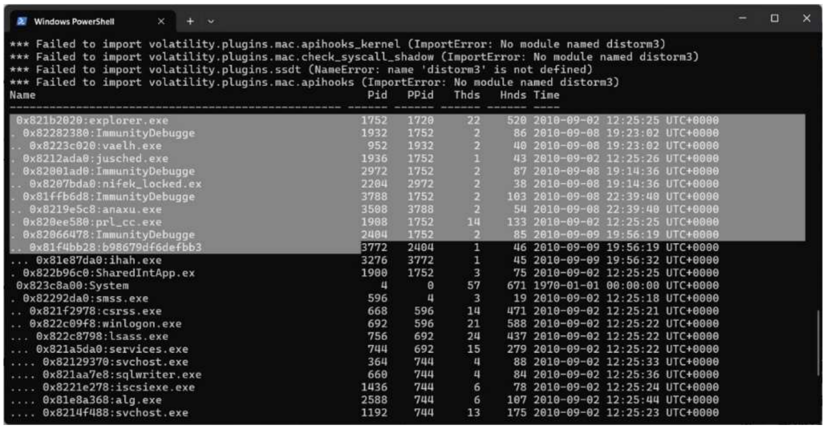
```
0x8213dda0 wscntfy.exe          2180   1084      3      48      0      0 2010-09-02 12:25:41 UTC+0000
0x81e8a368 alg.exe              2588    744      6     107      0      0 2010-09-02 12:25:44 UTC+0000
0x8205dda0 wuauclt.exe           940   1084      4     126      0      0 2010-09-02 12:26:40 UTC+0000
0x82001ad0 ImmunityDebugge      2972   1752      2      87      0      0 2010-09-08 19:14:36 UTC+0000
0x8207bda0 nifek_locked.ex      2204   2972      2      38      0      0 2010-09-08 19:14:36 UTC+0000
0x82282380 ImmunityDebugge      1932   1752      2      86      0      0 2010-09-08 19:23:02 UTC+0000
0x8223c020 vaelh.exe             952   1932      2      40      0      0 2010-09-08 19:23:02 UTC+0000
0x81ffb6d8 ImmunityDebugge      3788   1752      2     103      0      0 2010-09-08 22:39:40 UTC+0000
0x8219e5c8 anaxu.exe            3508   3788      2      54      0      0 2010-09-08 22:39:40 UTC+0000
0x81eab2f8 wuauclt.exe          3984   1084      8     325      0      0 2010-09-09 19:52:45 UTC+0000
0x82066478 ImmunityDebugge      2404   1752      2      85      0      0 2010-09-09 19:56:19 UTC+0000
0x81f4bb28 b98679df6defbb3      3772   2404      1      46      0      0 2010-09-09 19:56:19 UTC+0000
0x81e87da0 ihah.exe             3276   3772      1      45      0      0 2010-09-09 19:56:32 UTC+0000
0x82311648 rundll32.exe         3768   1084      1      53      0      0 2010-09-09 19:56:33 UTC+0000
PS C:\Users\Lenovo\Desktop\proactive2\volatility> |
```

Key observations:

- **We find unusual process name like “b98679df6defbb3” that has ID 3772 and its parent process is “ImmunityDebugge” which has ID of 2404 .**

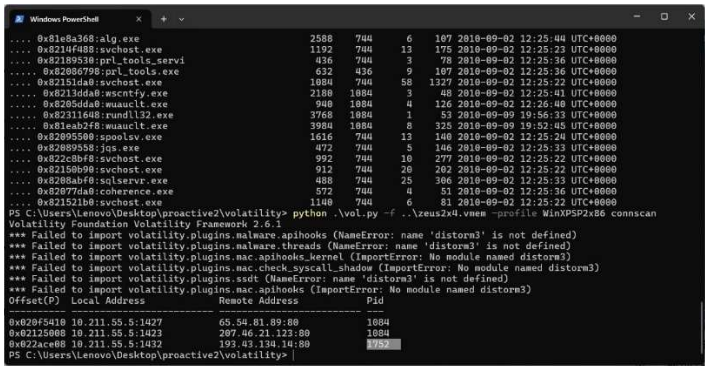
- **“ImmunityDebugge” which has ID of 2404 has parent process which has ID of 1752 (explorer.exe)**

To clarify the view we will use pstree plugin

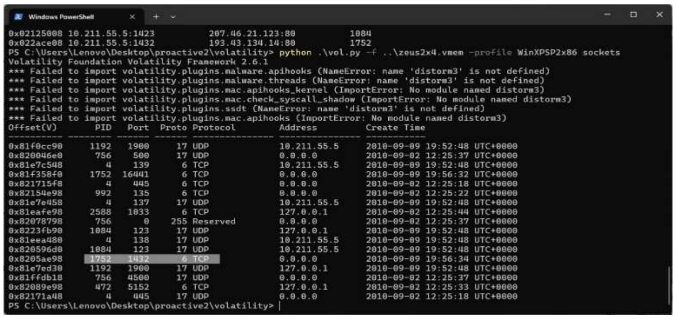


```
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x821b2020:explorer.exe                             1752   1720     22    520 2010-09-02 12:25:25 UTC+0000
. 0x82282380:ImmunityDebugge                         1932   1752      2     86 2010-09-08 19:23:02 UTC+0000
.. 0x8223c020:vaelh.exe                               952   1932      2     40 2010-09-08 19:23:02 UTC+0000
. 0x8212ada0:jusched.exe                             1936   1752      1     43 2010-09-02 12:25:26 UTC+0000
. 0x82001ad0:ImmunityDebugge                         2972   1752      2     87 2010-09-08 19:14:36 UTC+0000
.. 0x8207bda0:nifek_locked.ex                        2204   2972      2     38 2010-09-08 19:14:36 UTC+0000
. 0x81ffb6d8:ImmunityDebugge                         3788   1752      2    103 2010-09-08 22:39:40 UTC+0000
.. 0x8219e5c8:anaxu.exe                              3508   3788      2     54 2010-09-08 22:39:40 UTC+0000
. 0x820ee580:prl_cc.exe                              1908   1752     14    133 2010-09-02 12:25:25 UTC+0000
. 0x82066478:ImmunityDebugge                         2404   1752      2     85 2010-09-09 19:56:19 UTC+0000
.. 0x81f4bb28:b98679df6defbb3                        3772   2404      1     46 2010-09-09 19:56:19 UTC+0000
... 0x81e87da0:ihah.exe                              3276   3772      1     45 2010-09-09 19:56:32 UTC+0000
. 0x822b96c0:SharedIntApp.ex                         1900   1752      3     75 2010-09-02 12:25:25 UTC+0000
 0x823c8a00:System                                      4      0     57    671 1970-01-01 00:00:00 UTC+0000
. 0x82292da0:smss.exe                                 596      4      3     19 2010-09-02 12:25:18 UTC+0000
.. 0x821f2978:csrss.exe                               668    596     14    471 2010-09-02 12:25:21 UTC+0000
.. 0x822c09f8:winlogon.exe                            692    596     21    588 2010-09-02 12:25:22 UTC+0000
... 0x822c8798:lsass.exe                              756    692     24    437 2010-09-02 12:25:22 UTC+0000
... 0x821a5da0:services.exe                           744    692     15    279 2010-09-02 12:25:22 UTC+0000
.... 0x82129370:svchost.exe                           364    744      4     88 2010-09-02 12:25:33 UTC+0000
.... 0x821aa7e8:sqlwriter.exe                         660    744      4     84 2010-09-02 12:25:36 UTC+0000
.... 0x8221e278:iscsiexe.exe                         1436    744      6     78 2010-09-02 12:25:24 UTC+0000
.... 0x81e8a368:alg.exe                              2588    744      6    107 2010-09-02 12:25:44 UTC+0000
.... 0x8214f488:svchost.exe                          1192    744     13    175 2010-09-02 12:25:23 UTC+0000
```

- **Then we used connscan plugin to see the connections while taking the image . after that we used sockets plugin to see the opening port in the connections**



```
.... 0x81e8a368:alg.exe                              2588    744      6    107 2010-09-02 12:25:44 UTC+0000
.... 0x8214f488:svchost.exe                          1192    744     13    175 2010-09-02 12:25:23 UTC+0000
.... 0x82189530:prl_tools_servi                       436    744      3     78 2010-09-02 12:25:36 UTC+0000
..... 0x82086798:prl_tools.exe                        632    436      9    107 2010-09-02 12:25:36 UTC+0000
.... 0x82151da0:svchost.exe                          1084    744     58   1327 2010-09-02 12:25:22 UTC+0000
..... 0x8213dda0:wscntfy.exe                         2180   1084      3     48 2010-09-02 12:25:41 UTC+0000
..... 0x8205dda0:wuauclt.exe                          940   1084      4    126 2010-09-02 12:26:40 UTC+0000
..... 0x82311648:rundll32.exe                        3768   1084      1     53 2010-09-09 19:56:33 UTC+0000
..... 0x81eab2f8:wuauclt.exe                         3984   1084      8    325 2010-09-09 19:52:45 UTC+0000
.... 0x82095500:spoolsv.exe                          1616    744     13    140 2010-09-02 12:25:24 UTC+0000
.... 0x82089558:jqs.exe                               472    744      5    146 2010-09-02 12:25:33 UTC+0000
.... 0x822c8bf8:svchost.exe                           992    744     10    277 2010-09-02 12:25:22 UTC+0000
.... 0x82150b90:svchost.exe                           912    744     20    202 2010-09-02 12:25:22 UTC+0000
.... 0x8208abf0:sqlservr.exe                          488    744     25    306 2010-09-02 12:25:33 UTC+0000
.... 0x82077da0:coherence.exe                         572    744      4     51 2010-09-02 12:25:36 UTC+0000
.... 0x821521b0:svchost.exe                          1140    744      6     81 2010-09-02 12:25:22 UTC+0000
PS C:\Users\Lenovo\Desktop\proactive2\volatility> python .\vol.py -f ..\zeus2x4.vmem -profile WinXPSP2x86 connscan
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ---
0x020f5410 10.211.55.5:1427          65.54.81.89:80            1084
0x02125008 10.211.55.5:1423          207.46.21.123:80          1084
0x022ace08 10.211.55.5:1432          193.43.134.14:80          1752
PS C:\Users\Lenovo\Desktop\proactive2\volatility> |
```

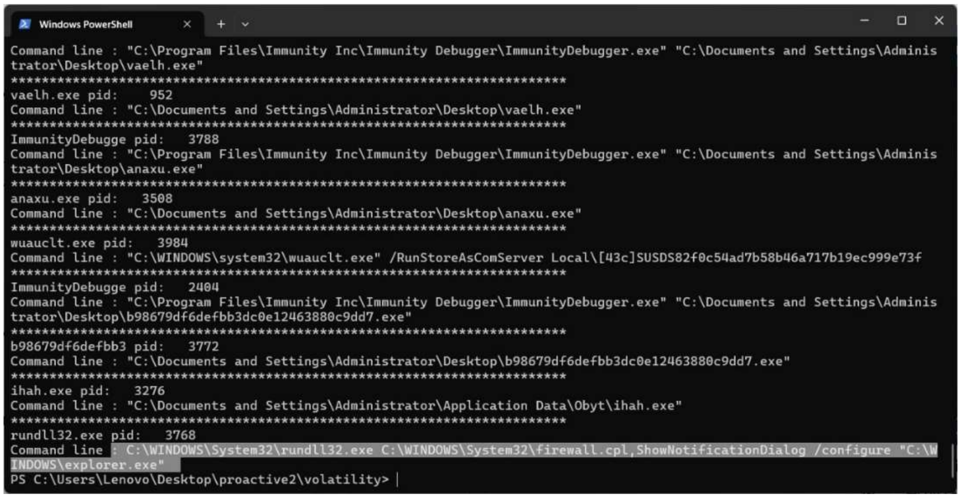


```
0x02125008 10.211.55.5:1423          207.46.21.123:80          1084
0x022ace08 10.211.55.5:1432          193.43.134.14:80          1752
PS C:\Users\Lenovo\Desktop\proactive2\volatility> python .\vol.py -f ..\zeus2x4.vmem -profile WinXPSP2x86 sockets
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
Offset(V)       PID   Port  Proto Protocol        Address         Create Time
---------- -------- ------ ------ --------------- --------------- -----------
0x81f0cc90     1192   1900     17 UDP             10.211.55.5     2010-09-09 19:52:48 UTC+0000
0x820046e0      756    500     17 UDP             0.0.0.0         2010-09-02 12:25:37 UTC+0000
0x81e7c548        4    139      6 TCP             10.211.55.5     2010-09-09 19:52:48 UTC+0000
0x81f358f0     1752  16441      6 TCP             0.0.0.0         2010-09-09 19:56:32 UTC+0000
0x821715f8        4    445      6 TCP             0.0.0.0         2010-09-02 12:25:18 UTC+0000
0x82154e98      992    135      6 TCP             0.0.0.0         2010-09-02 12:25:22 UTC+0000
0x81e7e458        4    137     17 UDP             10.211.55.5     2010-09-09 19:52:48 UTC+0000
0x81eafe98     2588   1033      6 TCP             127.0.0.1       2010-09-02 12:25:44 UTC+0000
0x82078798      756      0    255 Reserved        0.0.0.0         2010-09-02 12:25:37 UTC+0000
0x8223fb90     1084    123     17 UDP             127.0.0.1       2010-09-09 19:52:48 UTC+0000
0x81eea480        4    138     17 UDP             10.211.55.5     2010-09-09 19:52:48 UTC+0000
0x820596d0     1084    123     17 UDP             10.211.55.5     2010-09-09 19:52:48 UTC+0000
0x8205ae98     1752   1432      6 TCP             0.0.0.0         2010-09-09 19:56:34 UTC+0000
0x81e7ed30     1192   1900     17 UDP             127.0.0.1       2010-09-09 19:52:48 UTC+0000
0x81ffdb18      756   4500     17 UDP             0.0.0.0         2010-09-02 12:25:37 UTC+0000
0x82089e98      472   5152      6 TCP             127.0.0.1       2010-09-02 12:25:33 UTC+0000
0x82171a48        4    445     17 UDP             0.0.0.0         2010-09-02 12:25:18 UTC+0000
PS C:\Users\Lenovo\Desktop\proactive2\volatility> |
```

Key observations:

- **10.211.55.5:1432 193.43.134.14:80 1752 this IP which are used within the parent suspicious process (explorer.exe)**

- **We used cmdline plugin to see all the process command line arguments**



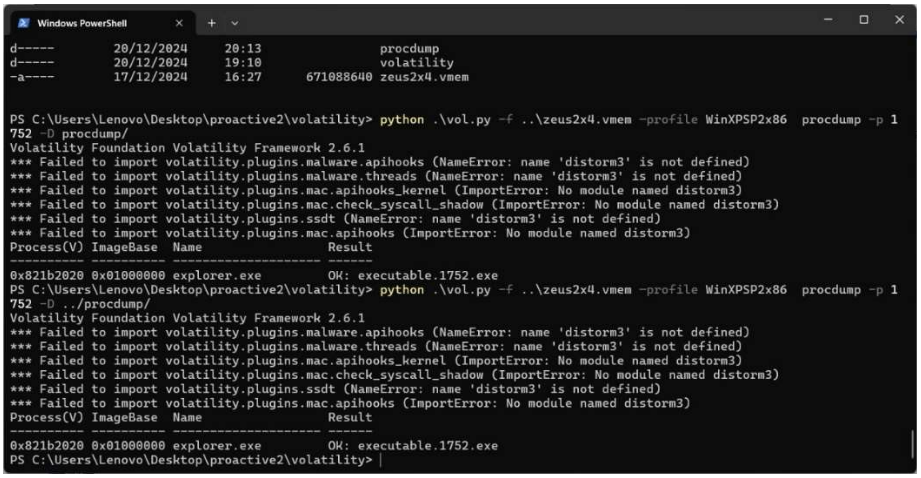
```
Command line : "C:\Program Files\Immunity Inc\Immunity Debugger\ImmunityDebugger.exe" "C:\Documents and Settings\Adminis
trator\Desktop\vaelh.exe"
************************************************************************
vaelh.exe pid:    952
Command line : "C:\Documents and Settings\Administrator\Desktop\vaelh.exe"
************************************************************************
ImmunityDebugge pid:   3788
Command line : "C:\Program Files\Immunity Inc\Immunity Debugger\ImmunityDebugger.exe" "C:\Documents and Settings\Adminis
trator\Desktop\anaxu.exe"
************************************************************************
anaxu.exe pid:   3508
Command line : "C:\Documents and Settings\Administrator\Desktop\anaxu.exe"
************************************************************************
wuauclt.exe pid:   3984
Command line : "C:\WINDOWS\system32\wuauclt.exe" /RunStoreAsComServer Local\[43c]SUSDS82f0c54ad7b58b46a717b19ec999e73f
************************************************************************
ImmunityDebugge pid:   2404
Command line : "C:\Program Files\Immunity Inc\Immunity Debugger\ImmunityDebugger.exe" "C:\Documents and Settings\Adminis
trator\Desktop\b98679df6defbb3dc0e12463880c9dd7.exe"
************************************************************************
b98679df6defbb3 pid:   3772
Command line : "C:\Documents and Settings\Administrator\Desktop\b98679df6defbb3dc0e12463880c9dd7.exe"
************************************************************************
ihah.exe pid:   3276
Command line : "C:\Documents and Settings\Administrator\Application Data\Obyt\ihah.exe"
************************************************************************
rundll32.exe pid:   3768
Command line : C:\WINDOWS\System32\rundll32.exe C:\WINDOWS\System32\firewall.cpl,ShowNotificationDialog /configure "C:\W
INDOWS\explorer.exe"
PS C:\Users\Lenovo\Desktop\proactive2\volatility> |
```

Key observations:

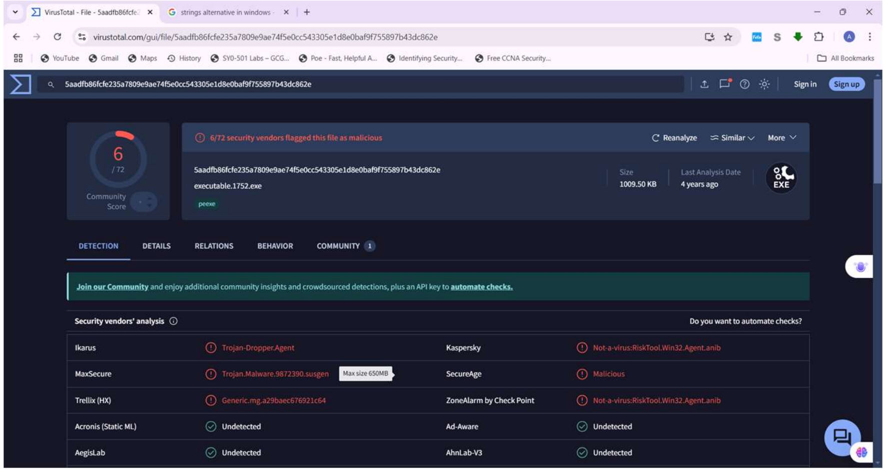
- **Suspicious command with processes that has ID of 3772 and 3768**

- **Now we used procdump plugin to extract the executable memory of a process from a memory dump (for suspicious processes) then we use (virus total) site to make malware identification (VirusTotal scans your uploaded file against a large database of antivirus engines and Provides the detection ratio)**

We first make this in process that has ID 1752 . but it had a small ratio detection



```
d-----        20/12/2024     20:13                procdump
d-----        20/12/2024     19:10                volatility
-a----        17/12/2024     16:27      671088640 zeus2x4.vmem


PS C:\Users\Lenovo\Desktop\proactive2\volatility> python .\vol.py -f ..\zeus2x4.vmem -profile WinXPSP2x86  procdump -p 1
752 -D procdump/
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
Process(V) ImageBase  Name                 Result
---------- ---------- -------------------- ------
0x821b2020 0x01000000 explorer.exe         OK: executable.1752.exe
PS C:\Users\Lenovo\Desktop\proactive2\volatility> python .\vol.py -f ..\zeus2x4.vmem -profile WinXPSP2x86  procdump -p 1
752 -D ../procdump/
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
Process(V) ImageBase  Name                 Result
---------- ---------- -------------------- ------
0x821b2020 0x01000000 explorer.exe         OK: executable.1752.exe
PS C:\Users\Lenovo\Desktop\proactive2\volatility> |
```



virustotal.com/gui/file/5aadfb86fcfe235a7809e9ae74f5e0cc543305e1d8e0baf9f755897b43dc862e

5aadfb86fcfe235a7809e9ae74f5e0cc543305e1d8e0baf9f755897b43dc862e

6 / 72 Community Score

6/72 security vendors flagged this file as malicious

5aadfb86fcfe235a7809e9ae74f5e0cc543305e1d8e0baf9f755897b43dc862e
executable.1752.exe
peexe

Size 1009.50 KB

Last Analysis Date 4 years ago

EXE

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

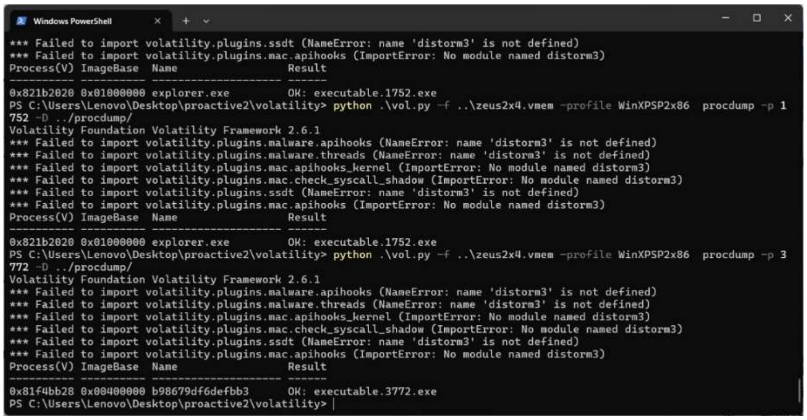
Security vendors' analysis

Do you want to automate checks?

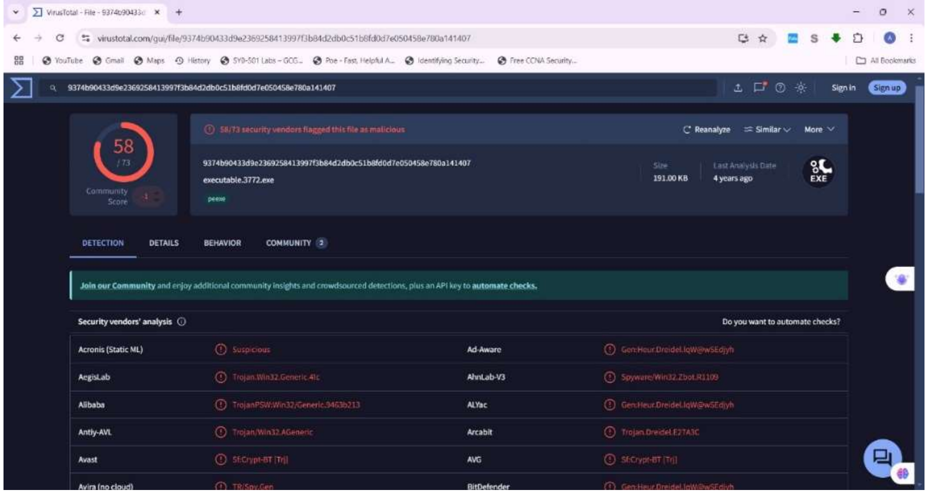
Ikarus	Trojan-Dropper.Agent	Kaspersky	Not-a-virus:RiskTool.Win32.Agent.anib
MaxSecure	Trojan.Malware.9872390.susgen	SecureAge	Malicious
Trellix (HX)	Generic.mg.a29baec676921c64	ZoneAlarm by Check Point	Not-a-virus:RiskTool.Win32.Agent.anib
Acronis (Static ML)	Undetected	Ad-Aware	Undetected
AegisLab	Undetected	AhnLab-V3	Undetected

Max size 650MB

Then we make this process again in process that has ID 3772 and It had big ratio detection



```
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
Process(V) ImageBase  Name                 Result
---------- ---------- -------------------- ------
0x821b2020 0x01000000 explorer.exe         OK: executable.1752.exe
PS C:\Users\Lenovo\Desktop\proactive2\volatility> python .\vol.py -f ..\zeus2x4.vmem -profile WinXPSP2x86  procdump -p 1
752 -D ../procdump/
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
Process(V) ImageBase  Name                 Result
---------- ---------- -------------------- ------
0x821b2020 0x01000000 explorer.exe         OK: executable.1752.exe
PS C:\Users\Lenovo\Desktop\proactive2\volatility> python .\vol.py -f ..\zeus2x4.vmem -profile WinXPSP2x86  procdump -p 3
772 -D ../procdump/
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
Process(V) ImageBase  Name                 Result
---------- ---------- -------------------- ------
0x81f4bb28 0x00400000 b98679df6defbb3      OK: executable.3772.exe
PS C:\Users\Lenovo\Desktop\proactive2\volatility> |
```



58/73 security vendors flagged this file as malicious

9374b90433d9e2369258413997f3b84d2db0c51b8fd0d7e050458e780a141407
executable.3772.exe
peexe

Size 191.00 KB
Last Analysis Date 4 years ago

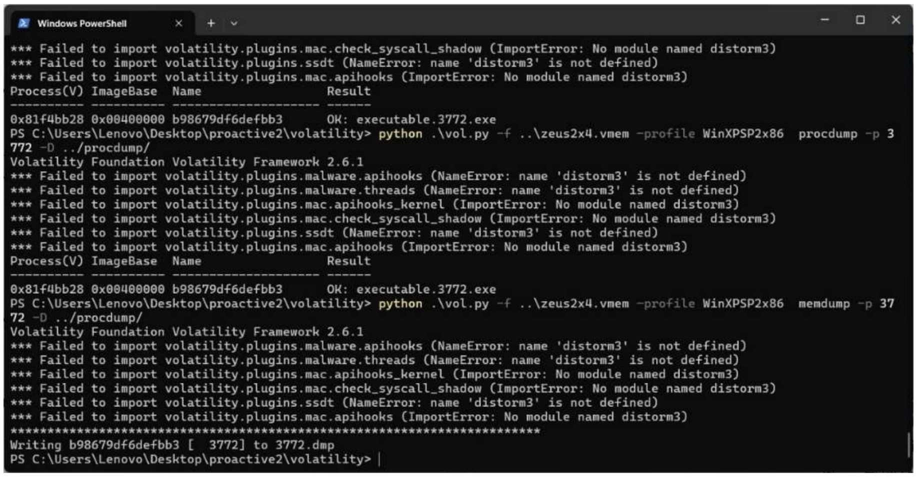
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Acronis (Static ML)	Suspicious	Ad-Aware	Gen:Heur.Dreidel.lqW@wSEdjyh
AegisLab	Trojan.Win32.Generic.4!c	AhnLab-V3	Spyware/Win32.Zbot.R1109
Alibaba	TrojanPSW:Win32/Generic.9463b213	ALYac	Gen:Heur.Dreidel.lqW@wSEdjyh
Antiy-AVL	Trojan/Win32.AGeneric	Arcabit	Trojan.Dreidel.E27A3C
Avast	Sf:Crypt-BT [Trj]	AVG	Sf:Crypt-BT [Trj]
Avira (no cloud)	TR/Spy.Gen	BitDefender	Gen:Heur.Dreidel.lqW@wSEdjyh

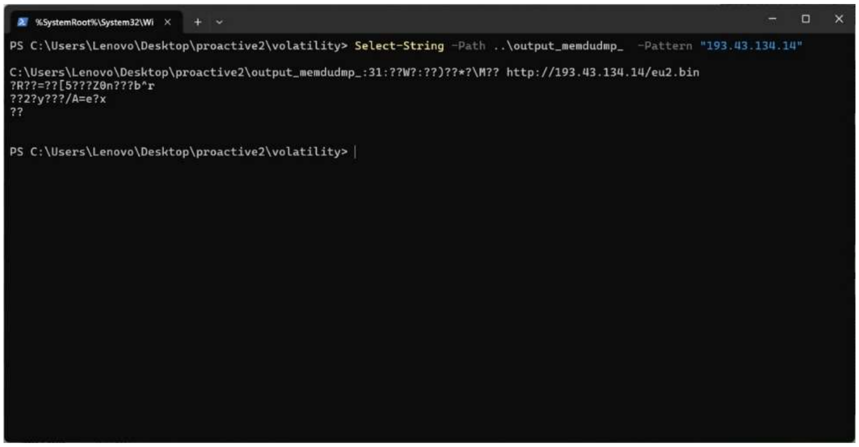
then we used memdump plugin to make memory dump of this process.



```
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
Process(V) ImageBase  Name                 Result
---------- ---------- -------------------- ------
0x81f4bb28 0x00400000 b98679df6defbb3      OK: executable.3772.exe
PS C:\Users\Lenovo\Desktop\proactive2\volatility> python .\vol.py -f ..\zeus2x4.vmem -profile WinXPSP2x86  procdump -p 3
772 -D ../procdump/
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
Process(V) ImageBase  Name                 Result
---------- ---------- -------------------- ------
0x81f4bb28 0x00400000 b98679df6defbb3      OK: executable.3772.exe
PS C:\Users\Lenovo\Desktop\proactive2\volatility> python .\vol.py -f ..\zeus2x4.vmem -profile WinXPSP2x86  memdump -p 37
72 -D ../procdump/
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
************************************************************************
Writing b98679df6defbb3 [  3772] to 3772.dmp
PS C:\Users\Lenovo\Desktop\proactive2\volatility> |
```

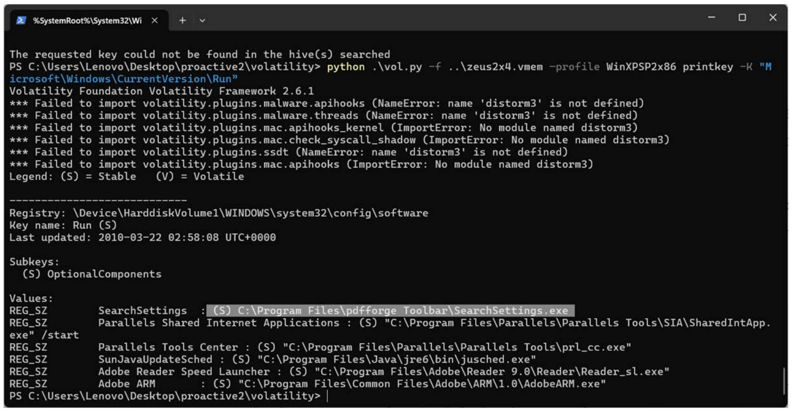
Then we grep the content of this memdump and save it in file called “output_memorydum” , then we use select-string (as strings in linux) and we searched about the IP that we have seen before that suspicious process (Explorer.exe interact with)

And we find it in this file



```
PS C:\Users\Lenovo\Desktop\proactive2\volatility> Select-String -Path ..\output_memdudmp_  -Pattern "193.43.134.14"

C:\Users\Lenovo\Desktop\proactive2\output_memdudmp_:31:??W?:??)??*?\M?? http://193.43.134.14/eu2.bin
?R??=??[5???Z0n???b^r
???2?y???/A=e?x
??


PS C:\Users\Lenovo\Desktop\proactive2\volatility> |
```

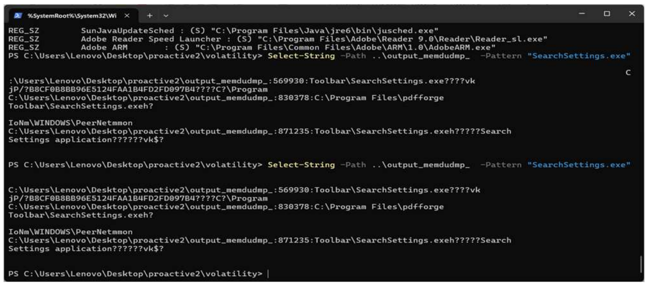
After that we searced for persistence mechanisms that a malware commonly uses . Some of the common registry keys that malwares use for persistence are Run and Winlogon keys



```
The requested key could not be found in the hive(s) searched
PS C:\Users\Lenovo\Desktop\proactive2\volatility> python .\vol.py -f ..\zeus2x4.vmem -profile WinXPSP2x86 printkey -K "M
icrosoft\Windows\CurrentVersion\Run"
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\software
Key name: Run (S)
Last updated: 2010-03-22 02:58:08 UTC+0000

Subkeys:
  (S) OptionalComponents

Values:
REG_SZ        SearchSettings  : (S) C:\Program Files\pdfforge Toolbar\SearchSettings.exe
REG_SZ        Parallels Shared Internet Applications : (S) "C:\Program Files\Parallels\Parallels Tools\SIA\SharedIntApp.
exe" /start
REG_SZ        Parallels Tools Center : (S) "C:\Program Files\Parallels\Parallels Tools\prl_cc.exe"
REG_SZ        SunJavaUpdateSched : (S) "C:\Program Files\Java\jre6\bin\jusched.exe"
REG_SZ        Adobe Reader Speed Launcher : (S) "C:\Program Files\Adobe\Reader 9.0\Reader\Reader_sl.exe"
REG_SZ        Adobe ARM       : (S) "C:\Program Files\Common Files\Adobe\ARM\1.0\AdobeARM.exe"
PS C:\Users\Lenovo\Desktop\proactive2\volatility> |
```

The presence of SearchSettings.exe from pdfforge Toolbar is a bit suspicious.

And when we searched about it in the file memdump we find it



```
REG_SZ        SunJavaUpdateSched : (S) "C:\Program Files\Java\jre6\bin\jusched.exe"
REG_SZ        Adobe Reader Speed Launcher : (S) "C:\Program Files\Adobe\Reader 9.0\Reader\Reader_sl.exe"
REG_SZ        Adobe ARM       : (S) "C:\Program Files\Common Files\Adobe\ARM\1.0\AdobeARM.exe"
PS C:\Users\Lenovo\Desktop\proactive2\volatility> Select-String -Path ..\output_memdudmp_  -Pattern "SearchSettings.exe"

                                                                                                                    C
:\Users\Lenovo\Desktop\proactive2\output_memdudmp_:569930:Toolbar\SearchSettings.exe????vk
jP/?B8CF0B8BB96E5124FAA1B4FD2FD097B4????C?\Program
C:\Users\Lenovo\Desktop\proactive2\output_memdudmp_:830378:C:\Program Files\pdfforge
Toolbar\SearchSettings.exeh?

IoNm\WINDOWS\PeerNetmmon
C:\Users\Lenovo\Desktop\proactive2\output_memdudmp_:871235:Toolbar\SearchSettings.exeh?????Search
Settings application??????vk$?


PS C:\Users\Lenovo\Desktop\proactive2\volatility> Select-String -Path ..\output_memdudmp_  -Pattern "SearchSettings.exe"


C:\Users\Lenovo\Desktop\proactive2\output_memdudmp_:569930:Toolbar\SearchSettings.exe????vk
jP/?B8CF0B8BB96E5124FAA1B4FD2FD097B4????C?\Program
C:\Users\Lenovo\Desktop\proactive2\output_memdudmp_:830378:C:\Program Files\pdfforge
Toolbar\SearchSettings.exeh?

IoNm\WINDOWS\PeerNetmmon
C:\Users\Lenovo\Desktop\proactive2\output_memdudmp_:871235:Toolbar\SearchSettings.exeh?????Search
Settings application??????vk$?


PS C:\Users\Lenovo\Desktop\proactive2\volatility> |
```

Findings from the analysis :

- An process **b98679df6defbb3** (PID 3772) with Explorer as a parent (PID 1752)
- An opened connection towards 193.43.134.14:80 used by PID 3772
- Bank domains and 193.43.134.14 are found in the dump of the process 3772
- Perform changes in registries