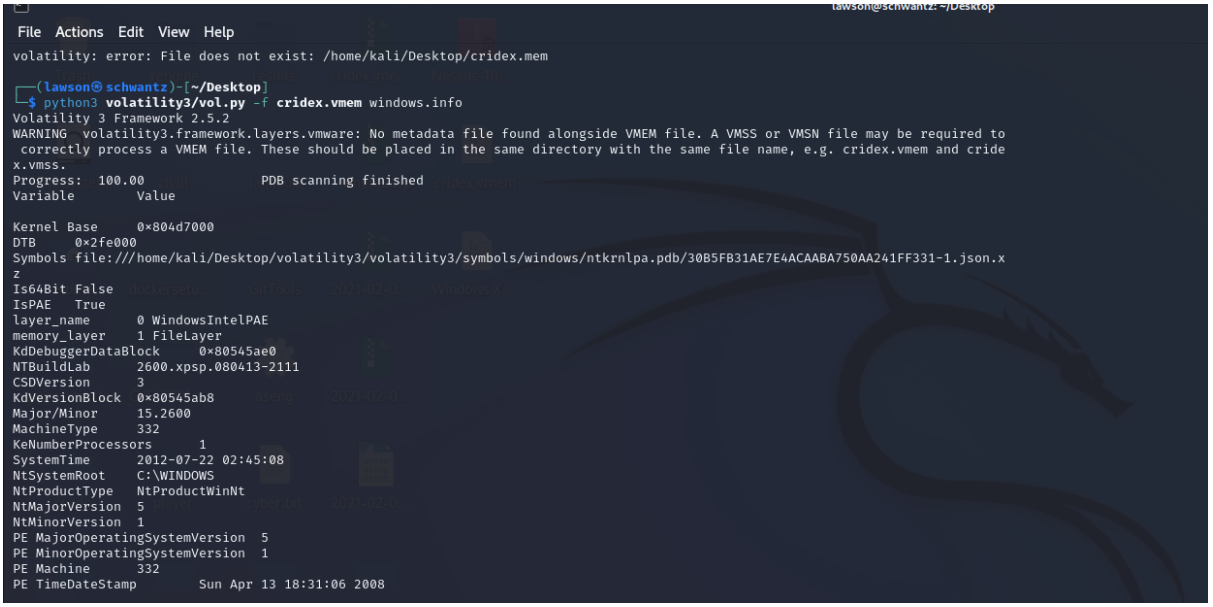
Computer Forensic Volatility

Nama Kelompok:

- 2540123403 - Bertrand Redondo Mulyono
- 2502064303 - Betrand Gabrialdi Leonard
- 2540125024 - Felysia Meytri
- 2540123100 - Victor Benaya

Cridex

Image Info:



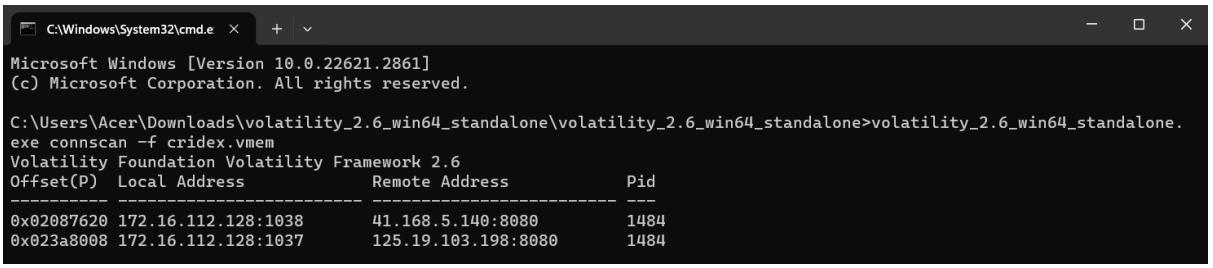
Date of time of image: 22 July 2012 02:45:08

Operating System: Windows XP (From NTBuildLab)

Service Pack: 3 (CSDVersion)

Hardware Architecture: 32 Bit

Network Activity:



Connscan shows that the victim was connected to IP address 41.168.5.140 and 125.19.103.198 at port 8080 from pid 1484.

Profile List:

```
┌──(lawson㉿schwantz)-[~/Desktop]
└─$ python volatility3/vol.py -f cridex.vmem  windows.pslist
Volatility 3 Framework 2.5.2
WARNING  volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may
be required to correctly process a VMEM file. These should be placed in the same directory with the same file name
, e.g. cridex.vmem and cridex.vmss.
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0×823c89c8      53      240     N/A     False   N/A     N/A     Disabled
368     4       smss.exe        0×822f1020      3       19      N/A     False   2012-07-22 02:42:31.000000      N/A     Disabled
584     368     csrss.exe       0×822a0598      9       326     0       False   2012-07-22 02:42:32.000000      N/A     Disabled
608     368     winlogon.exe    0×82298700      23      519     0       False   2012-07-22 02:42:32.000000      N/A     Disabled
652     608     services.exe    0×81e2ab28      16      243     0       False   2012-07-22 02:42:32.000000      N/A     Disabled
664     608     lsass.exe       0×81e2a3b8      24      330     0       False   2012-07-22 02:42:32.000000      N/A     Disabled
824     652     svchost.exe     0×82311360      20      194     0       False   2012-07-22 02:42:33.000000      N/A     Disabled
908     652     svchost.exe     0×81e29ab8      9       226     0       False   2012-07-22 02:42:33.000000      N/A     Disabled
1004    652     svchost.exe     0×823001d0      64      1118    0       False   2012-07-22 02:42:33.000000      N/A     Disabled
1056    652     svchost.exe     0×821dfda0      5       60      0       False   2012-07-22 02:42:33.000000      N/A     Disabled
1220    652     svchost.exe     0×82295650      15      197     0       False   2012-07-22 02:42:35.000000      N/A     Disabled
1484    1464    explorer.exe    0×821dea70      17      415     0       False   2012-07-22 02:42:36.000000      N/A     Disabled
1512    652     spoolsv.exe     0×81eb17b8      14      113     0       False   2012-07-22 02:42:36.000000      N/A     Disabled
1640    1484    reader_sl.exe   0×81e7bda0      5       39      0       False   2012-07-22 02:42:36.000000      N/A     Disabled
788     652     alg.exe 0×820e8da0      7       104     0       False   2012-07-22 02:43:01.000000      N/A     Disabled
1136    1004    wuauclt.exe     0×821fcda0      8       173     0       False   2012-07-22 02:43:46.000000      N/A     Disabled
1588    1004    wuauclt.exe     0×8205bda0      5       132     0       False   2012-07-22 02:44:01.000000      N/A     Disabled
```

Pslist shows that PID 1484 belongs to explorer.exe and gives the memory location.

Process Activity:

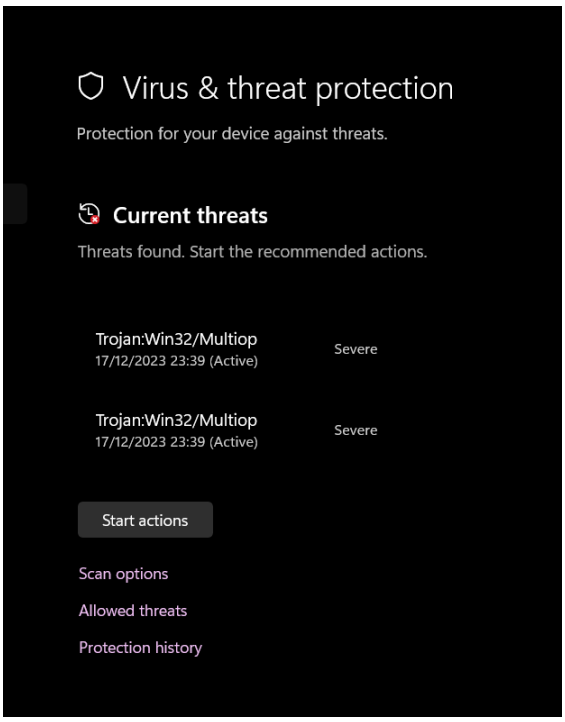
```
C:\Windows\System32\cmd.e
Microsoft Windows [Version 10.0.22621.2861]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Acer\Downloads\volatility_2.6_win64_standalone\volatility_2.6_win64_standalone>volatility_2.6_win64_standalone.
exe handles -f cridex.vmem -p 1484 -t Process
Volatility Foundation Volatility Framework 2.6
Offset(V)     Pid     Handle     Access Type             Details
---------- ------ ---------- ---------- ---------------- -------
0x821dea70   1484       0x388   0x1f0fff Process          explorer.exe(1484)
```

Key:

```
C:\Users\Acer\Downloads\volatility_2.6_win64_standalone\volatility_2.6_win64_standalone>volatility_2.6_win64_standalone.exe -f cridex.vmem handles -p 1484 -
t key
Volatility Foundation Volatility Framework 2.6
Offset(V)     Pid     Handle     Access Type             Details
---------- ------ ---------- ---------- ---------------- -------
0xe1bac260   1484       0x28  0x20f003f Key             MACHINE
0xe18a2d00   1484       0x44  0x20f003f Key             USER\S-1-5-21-789336058-261478967-1417001333-1003
0xe1acb730   1484       0x54    0x2001f Key             USER\S-1-5-21-789336058-261478967-1417001333-1003\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNE
T SETTINGS
0xe1b63100   1484       0x78  0x20f003f Key             USER\S-1-5-21-789336058-261478967-1417001333-1003_CLASSES
0xe185e580   1484       0x8c    0x20019 Key             MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\DRIVERS32
0xe1c97d48   1484       0x98    0x20019 Key             MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\NETWORK\WORLD FULL ACCESS SHARED PARAMETERS
0xe185cd58   1484       0xac    0xf003f Key             USER\S-1-5-21-789336058-261478967-1417001333-1003\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORE
R
0xe1911d68   1484       0xb8    0xf003f Key             MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER
0xe1911e40   1484       0xbc    0xf003f Key             USER\S-1-5-21-789336058-261478967-1417001333-1003\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORE
R
0xe18c1f30   1484       0xc0    0xf003f Key             MACHINE\SOFTWARE\CLASSES
0xe1806b18   1484       0xcc    0xf003f Key             USER\S-1-5-21-789336058-261478967-1417001333-1003_CLASSES
0xe1ac9e30   1484       0xd4    0xf003f Key             MACHINE\SOFTWARE\MICROSOFT\COM3
0xe181ae40   1484       0xdc       0x10 Key             USER
0xe1a3fe40   1484       0xe4    0xf003f Key             MACHINE\SOFTWARE\CLASSES
0xe17bdc30   1484       0xec       0x10 Key             USER
0xe1bcb688   1484       0xf4    0xf003f Key             MACHINE\SOFTWARE\MICROSOFT\COM3
0xe1bc75c0   1484       0xfc    0xf003f Key             MACHINE\SOFTWARE\MICROSOFT\COM3
0xe1866a28   1484      0x104    0xf003f Key             MACHINE\SOFTWARE\CLASSES\CLSID
0xe1ba5518   1484      0x10c    0xf003f Key             MACHINE\SOFTWARE\CLASSES
0xe1bc9590   1484      0x114    0xf003f Key             MACHINE\SOFTWARE\MICROSOFT\COM3
0xe191ac60   1484      0x11c       0x10 Key             USER
0xe1bac780   1484      0x124    0xf003f Key             MACHINE\SOFTWARE\MICROSOFT\COM3
```

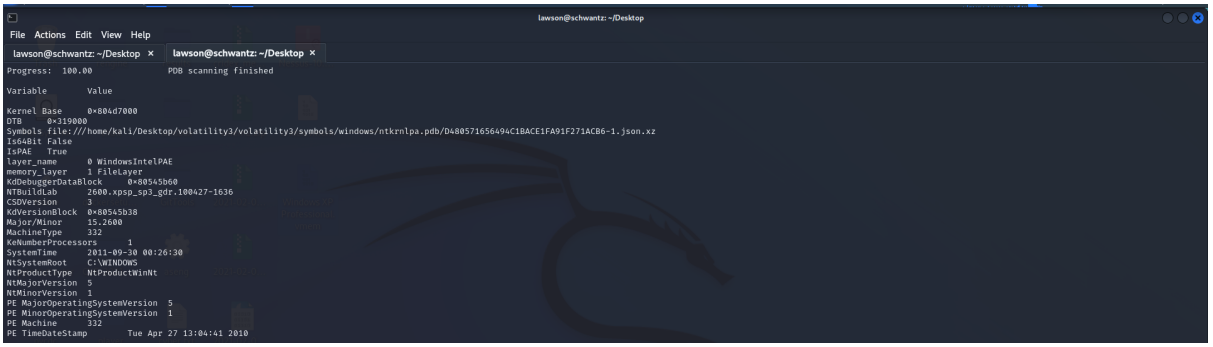
Checking one by one and not find any interesting finding in the keys, let's try to dump the explorer.exe (Command: volatility_2.6_win64_standalone.exe -f cridex.vmem --profile=WinXPSP2x86 procdump -p 1484 --dump-dir .).



Windows defender detecting that the code inside explorer.exe contains Trojan. That means the memory has malware inside.

Shylock

Image Info:



Date of time of image: 30 September 2011 00:26:30

Operating System: Windows XP (From NTBuildLab)

Service Pack: 3 (CSDVersion)

Hardware Architecture: 32 Bit

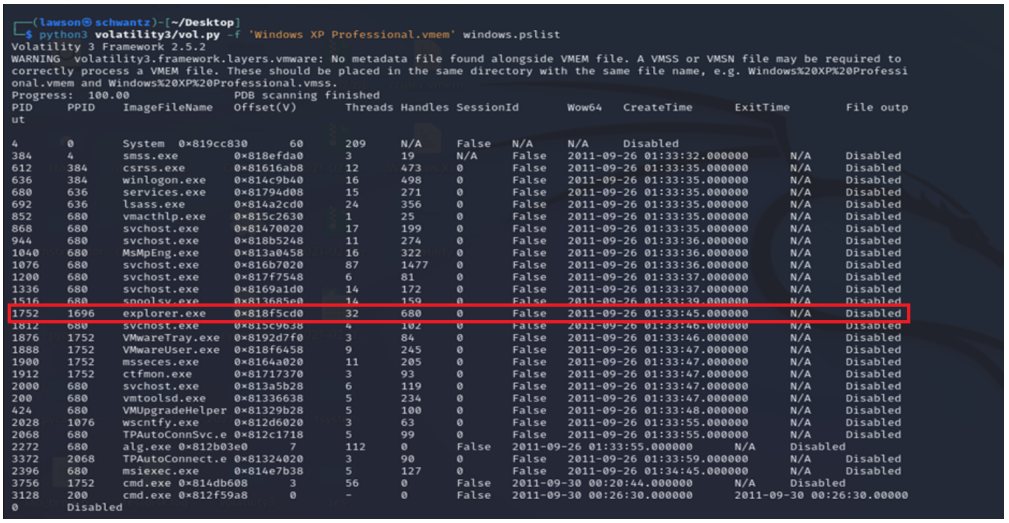
Network Activity:

```
C:\Users\Acer\Downloads\volatility_2.6_win64_standalone\volatility_2.6_win64_standalone>volatility_2.6_win64_standalone.
exe -f shylock.vmem connscan
Volatility Foundation Volatility Framework 2.6
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------ ------------------------- ---
0x014f6ab0 10.0.0.109:1072          209.190.4.84:443          1752
0x01507380 10.0.0.109:1073          209.190.4.84:443          1752
0x016c2b00 10.0.0.109:1065          184.173.252.227:443       1752
0x017028a0 10.0.0.109:1067          184.173.252.227:443       1752
0x01858cb0 10.0.0.109:1068          209.190.4.84:443          1752

C:\Users\Acer\Downloads\volatility_2.6_win64_standalone\volatility_2.6_win64_standalone>
```

Connscan shows that the victim was connected to IP address 209.190.4.84, and 184.173.252.227 at port 443 from pid 1752.

Profile List:



Pslist shows that PID 1752 belongs to explorer.exe and gives the memory location.

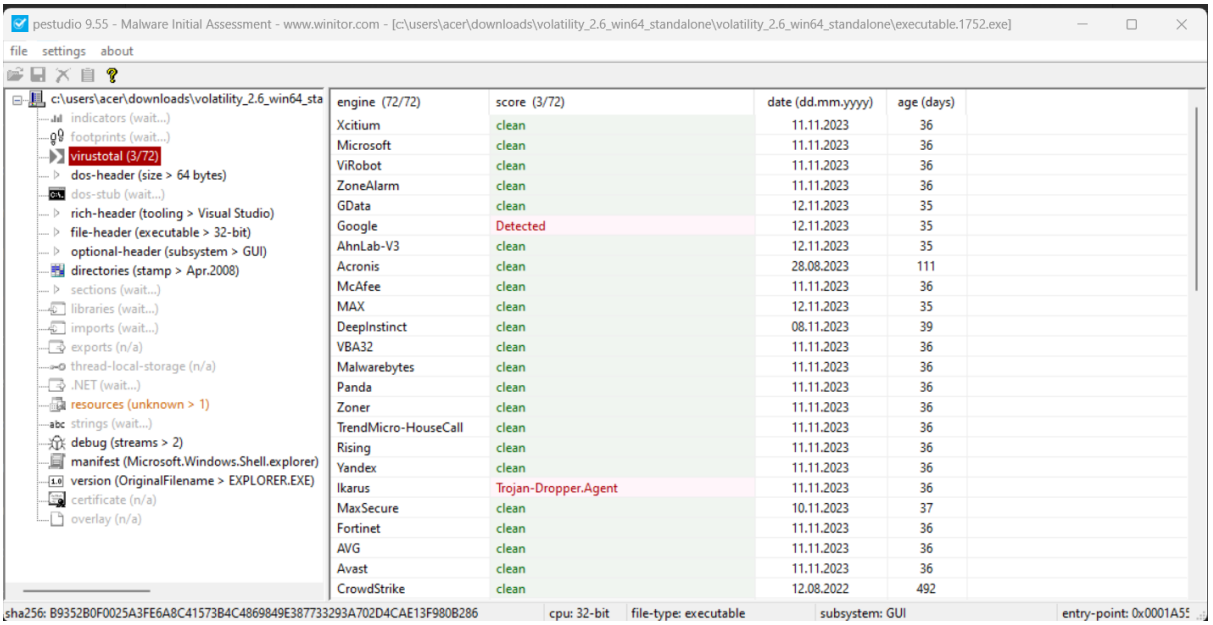
Process Activity:

```
C:\Users\Acer\Downloads\volatility_2.6_win64_standalone\volatility_2.6_win64_standalone>volatility_2.6_win64_standalone.
exe handles -f shylock.vmem -p 1752 -t process
Volatility Foundation Volatility Framework 2.6
Offset(V)     Pid     Handle     Access Type             Details
---------- ------ ---------- ---------- ---------------- -------
0x818f5cd0   1752        0x64   0x1f0fff Process          explorer.exe(1752)
0x818f5cd0   1752       0x84c   0x100000 Process          explorer.exe(1752)
0x8192d7f0   1752       0x8c4   0x100000 Process          VMwareTray.exe(1876)
0x818f6458   1752       0x8d8   0x100000 Process          VMwareUser.exe(1888)
0x8164a020   1752       0x8e0   0x100000 Process          msseces.exe(1900)
0x81717370   1752       0x8e8   0x100000 Process          ctfmon.exe(1912)
0x81324020   1752       0x8f4   0x100000 Process          TPAutoConnect.e(3372)
0x812d6020   1752       0x8f8   0x100000 Process          wscntfy.exe(2028)
0x814db608   1752       0x8fc   0x100000 Process          cmd.exe(3756)
```

Key:

```
C:\Users\Acer\Downloads\volatility_2.6_win64_standalone\volatility_2.6_win64_standalone>volatility_2.6_win64_standalone.exe -f shylock.vmem handles -p 1752
-t key
Volatility Foundation Volatility Framework 2.6
Offset(V)     Pid     Handle     Access Type             Details
---------- ------ ---------- ---------- ---------------- -------
0xe1756c40   1752        0xc    0x20019 Key              USER\S-1-5-21-1957994488-1326574676-839522115-500_CLASSES
0xe181c480   1752       0x28  0x20f003f Key              MACHINE
0xe181d5a8   1752       0x44  0x20f003f Key              USER\S-1-5-21-1957994488-1326574676-839522115-500
0xe15d6708   1752       0x7c    0x2001f Key              USER\S-1-5-21-1957994488-1326574676-839522115-500\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNE
T SETTINGS
0xe17f2428   1752       0xa0  0x20f003f Key              USER\S-1-5-21-1957994488-1326574676-839522115-500_CLASSES
0xe18d4bb0   1752       0xb4    0x20019 Key              MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\DRIVERS32
0xe191b9b8   1752       0xc8    0xf003f Key              USER\S-1-5-21-1957994488-1326574676-839522115-500\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORE
R
0xe17b5378   1752       0xe0    0xf003f Key              MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER
0xe18d2bb8   1752       0xe4    0xf003f Key              USER\S-1-5-21-1957994488-1326574676-839522115-500\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORE
R
0xe177d3d0   1752       0xe8    0xf003f Key              MACHINE\SOFTWARE\CLASSES
0xe17b6570   1752       0xec    0xf003f Key              USER\S-1-5-21-1957994488-1326574676-839522115-500_CLASSES
0xe17a0378   1752       0xf4    0xf003f Key              MACHINE\SOFTWARE\MICROSOFT\COM3
0xe18e7fb8   1752       0xfc      0x10 Key               USER
0xe18ab978   1752      0x104    0xf003f Key              MACHINE\SOFTWARE\CLASSES
0xe15e6fb8   1752      0x10c      0x10 Key               USER
0xe15e3a98   1752      0x114    0xf003f Key              MACHINE\SOFTWARE\MICROSOFT\COM3
0xe18df358   1752      0x11c    0xf003f Key              MACHINE\SOFTWARE\MICROSOFT\COM3
0xe18df598   1752      0x124    0xf003f Key              MACHINE\SOFTWARE\CLASSES\CLSID
0xe14d1eb0   1752      0x12c    0xf003f Key              MACHINE\SOFTWARE\CLASSES
0xe1844580   1752      0x134    0xf003f Key              MACHINE\SOFTWARE\MICROSOFT\COM3
```

Again, try to dump the explorer.exe file (Command: volatility_2.6_win64_standalone.exe -f shylock.vmem --profile=WinXPSP2x86 procdump -p 1752 --dump-dir .) and it results that virustotal detecting that the code inside explorer.exe contains Trojan. That means the memory has malware inside.



r2d2

Image Info:

```
Microsoft Windows [Version 10.0.22621.2715]
(c) Microsoft Corporation. All rights reserved.

C:\Users\User\Downloads\volatility_2.6_win64_standalone\volatility_2.6_win64_standalone>volatility_2.6_win64_standalone.
exe imageinfo -f 0zapftis.vmem
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (C:\Users\User\Downloads\volatility_2.6_win64_standalone\volatility_2.
6_win64_standalone\0zapftis.vmem)
                      PAE type : PAE
                           DTB : 0x319000L
                          KDBG : 0x80544ce0L
          Number of Processors : 1
     Image Type (Service Pack) : 2
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2011-10-10 17:06:54 UTC+0000
     Image local date and time : 2011-10-10 13:06:54 -0400
```

Date of time of image: 10 October 2011 17:06:54

Operating System: Windows XP (From NTBuildLab)

Service Pack: 2 (CSDVersion)

Hardware Architecture: 32 Bit

Network Activity

```
C:\Windows\System32\cmd.exe

A:\Malware\0zapftis>volatility_2.6_win64_standalone.exe -f 0zapftis.vmem connscan
Volatility Foundation Volatility Framework 2.6
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------ ------------------------ ---
0x01a25a50 0.0.0.0:1026             172.16.98.1:6666          1956

A:\Malware\0zapftis>
```

Process Running:

```
C:\Users\User\Downloads\volatility_2.6_win64_standalone\volatility_2.6_win64_standalone>volatility_2.6_win64_standalone.
exe -f 0zapftis.vmem --profile=WinXPSP2x86 pstree
Volatility Foundation Volatility Framework 2.6
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x819cc830:System                                      4      0     55    162 1970-01-01 00:00:00 UTC+0000
. 0x81945020:smss.exe                                 536      4      3     21 2011-10-10 17:03:56 UTC+0000
.. 0x816c6020:csrss.exe                               608    536     11    355 2011-10-10 17:03:58 UTC+0000
.. 0x813a9020:winlogon.exe                            632    536     24    533 2011-10-10 17:03:58 UTC+0000
... 0x816da020:services.exe                           676    632     16    261 2011-10-10 17:03:58 UTC+0000
.... 0x817757f0:svchost.exe                           916    676      9    217 2011-10-10 17:03:59 UTC+0000
.... 0x81772ca8:vmacthlp.exe                          832    676      1     24 2011-10-10 17:03:59 UTC+0000
.... 0x816c6da0:svchost.exe                           964    676     63   1058 2011-10-10 17:03:59 UTC+0000
..... 0x815c4da0:wscntfy.exe                         1920    964      1     27 2011-10-10 17:04:39 UTC+0000
..... 0x815e7be0:wuauclt.exe                          400    964      8    173 2011-10-10 17:04:46 UTC+0000
.... 0x8167e9d0:svchost.exe                           848    676     20    194 2011-10-10 17:03:59 UTC+0000
.... 0x81754990:VMwareService.e                      1444    676      3    145 2011-10-10 17:04:00 UTC+0000
.... 0x8136c5a0:alg.exe                              1616    676      7     99 2011-10-10 17:04:01 UTC+0000
.... 0x813aeda0:svchost.exe                          1148    676     12    187 2011-10-10 17:04:00 UTC+0000
.... 0x817937e0:spoolsv.exe                          1260    676     13    140 2011-10-10 17:04:00 UTC+0000
.... 0x815daca8:svchost.exe                          1020    676      5     58 2011-10-10 17:03:59 UTC+0000
... 0x813c4020:lsass.exe                              688    632     23    336 2011-10-10 17:03:58 UTC+0000
 0x813bcda0:explorer.exe                             1956   1884     18    322 2011-10-10 17:04:39 UTC+0000
. 0x8180b478:VMwareUser.exe                           192   1956      6     83 2011-10-10 17:04:41 UTC+0000
. 0x817a34b0:cmd.exe                                  544   1956      1     30 2011-10-10 17:06:42 UTC+0000
. 0x816d63d0:VMwareTray.exe                           184   1956      1     28 2011-10-10 17:04:41 UTC+0000
. 0x818233c8:reader_sl.exe                            228   1956      2     26 2011-10-10 17:04:41 UTC+0000
```

Network Activity:

```
C:\Users\User\Downloads\volatility_2.6_win64_standalone\volatility_2.6_win64_standalone>volatility_2.6_win64_standalone.
exe -f 0zapftis.vmem --profile=WinXPSP2x86 sockets
Volatility Foundation Volatility Framework 2.6
Offset(V)       PID   Port  Proto Protocol        Address         Create Time
---------- -------- ------ ------ --------------- --------------- -----------
0x8177e3c0     1956   1026      6 TCP             0.0.0.0         2011-10-10 17:04:39 UTC+0000
0x81596a78      688    500     17 UDP             0.0.0.0         2011-10-10 17:04:00 UTC+0000
0x8166a008      964   1029     17 UDP             127.0.0.1       2011-10-10 17:04:42 UTC+0000
0x818ddc08        4    445      6 TCP             0.0.0.0         2011-10-10 17:03:55 UTC+0000
0x818328d8      916    135      6 TCP             0.0.0.0         2011-10-10 17:03:59 UTC+0000
0x81687e98     1616   1025      6 TCP             127.0.0.1       2011-10-10 17:04:01 UTC+0000
0x817517e8      964    123     17 UDP             127.0.0.1       2011-10-10 17:04:00 UTC+0000
0x81753b20      688      0    255 Reserved        0.0.0.0         2011-10-10 17:04:00 UTC+0000
0x8174fe98     1148   1900     17 UDP             127.0.0.1       2011-10-10 17:04:41 UTC+0000
0x81753008      688   4500     17 UDP             0.0.0.0         2011-10-10 17:04:00 UTC+0000
0x816118d8        4    445     17 UDP             0.0.0.0         2011-10-10 17:03:55 UTC+0000
```

From the information above, we can see that a process with PID 1956 is communicating with a remote address, 172.16.98.1:6666 on port 1026.

Referring to the process list that we had enumerated before, we know that the process with PID 1956 is explorer.exe and reader_sl.exe is a child of explorer.exe. At this point, reader_sl.exe is definitely a suspect.

Key:

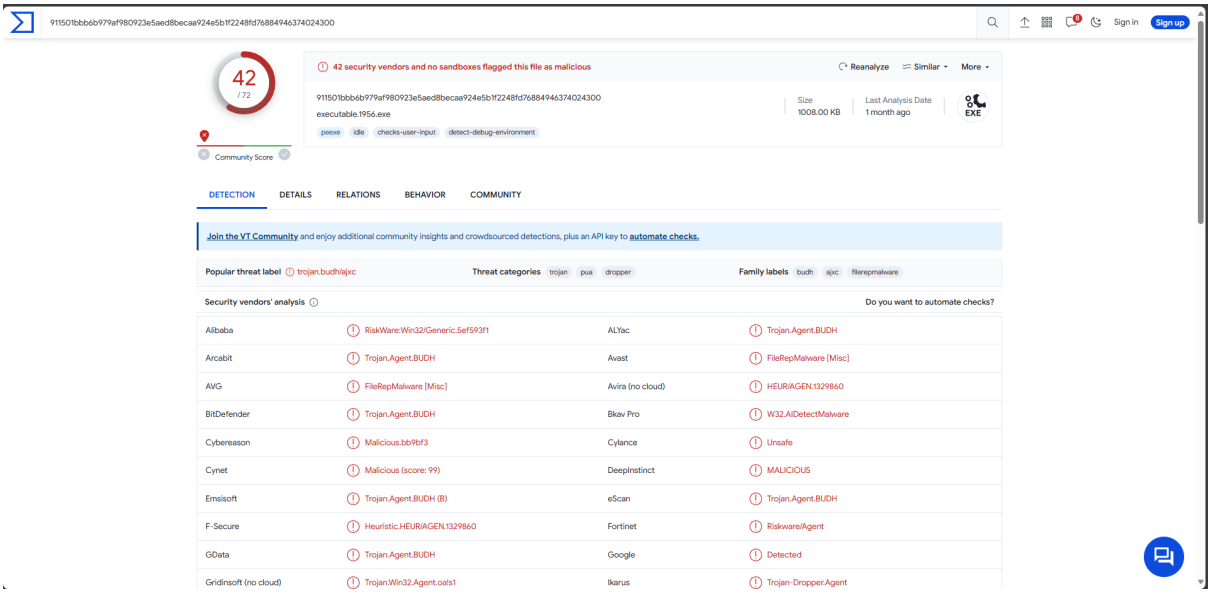
```
C:\Users\User\Downloads\volatility_2.6_win64_standalone\volatility_2.6_win64_standalone>volatility_2.6_win64_standalone.
exe handles -f 0zapftis.vmem -p 1956 -t key
Volatility Foundation Volatility Framework 2.6
Offset(V)     Pid     Handle     Access Type            Details
---------- ------ ---------- ---------- --------------- -------
0xe17f0718   1956        0x1c  0x20f003f Key             MACHINE
0xe1ccbbc0   1956        0x64  0x20f003f Key             USER\S-1-5-21-839522115-73586283-2147125571-500
0xe1c82e20   1956        0x6c    0x2001f Key             USER\S-1-5-21-839522115-73586283-2147125571-500\SOFTWARE\MICROS
OFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS
0xe1ca3a10   1956        0x7c  0x20f003f Key             USER\S-1-5-21-839522115-73586283-2147125571-500_CLASSES
0xe1cd1ad0   1956        0x8c    0x20019 Key             MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\DRIVERS32
0xe1ccbb58   1956        0x98    0x20019 Key             MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\WINLOGON
0xe1d188e8   1956      0x148    0xf003f Key             MACHINE\SYSTEM\CONTROLSET001\SERVICES\WINSOCK2\PARAMETERS\PROTO
COL_CATALOG9
0xe1d18950   1956      0x150    0xf003f Key             MACHINE\SYSTEM\CONTROLSET001\SERVICES\WINSOCK2\PARAMETERS\NAMES
PACE_CATALOG5
0xe1d18a70   1956      0x170    0xf003f Key             USER\S-1-5-21-839522115-73586283-2147125571-500\SOFTWARE\MICROS
OFT\WINDOWS\CURRENTVERSION\EXPLORER
0xe1d19710   1956      0x178    0xf003f Key             MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER
0xe1d47280   1956      0x180    0xf003f Key             USER\S-1-5-21-839522115-73586283-2147125571-500\SOFTWARE\MICROS
OFT\WINDOWS\CURRENTVERSION\EXPLORER
0xe1d195a0   1956      0x184    0xf003f Key             MACHINE\SOFTWARE\CLASSES
0xe1d19050   1956      0x190    0xf003f Key             USER\S-1-5-21-839522115-73586283-2147125571-500_CLASSES
0xe1d19538   1956      0x198    0xf003f Key             MACHINE\SOFTWARE\MICROSOFT\COM3
0xe1d47848   1956      0x1a0       0x10 Key             USER
0xe1d2c7b8   1956      0x1a8    0xf003f Key             MACHINE\SOFTWARE\CLASSES
0xe1d477e0   1956      0x1b0       0x10 Key             USER
0xe1d2c718   1956      0x1b8    0xf003f Key             MACHINE\SOFTWARE\MICROSOFT\COM3
```

Again, try to dump the executable file and check the dumped file into virustotal.com

```
A:\Malware\0zapftis>volatility_2.6_win64_standalone.exe -f 0zapftis.vmem --profile=WinXPSP2x86 procdump -p 1956 --dump-dir A:\Malware\0zapftis
Volatility Foundation Volatility Framework 2.6
Process(V) ImageBase  Name                 Result
---------- ---------- -------------------- ------
0x813bcda0 0x01000000 explorer.exe         OK: executable.1956.exe

A:\Malware\0zapftis>
```

Virustotal detects that “explorer.exe” is malware, in the category of trojan.



Also, windows can detect that the file contains malware.