



Universidad Carlos III de Madrid

Report for Memory Analysis - Evidences

Juan Diego Llano Miraval

Fecha: 18/05/2024

questions

1. What profile is the most appropriate for this machine? (ex: Win10x86_14393)

The most appropriate profile is Win7SP1x64

```
root@z:/home/zud/Desktop/adam# volatility -f adam.mem imageinfo
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.addrspaces.ieee1394 (AttributeError: /usr/local/lib/libforensic1394.so.2: undefined symbol: forensic1394_get_device_nodeid)
INFO : volatility.debug : Determining profile based on KDBG search...
      Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_24000, Win2008R2SP1x64_23418, Win2008R2SP1x64_24000, Win7SP1x64_23418
      AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
      AS Layer2 : FileAddressSpace (/home/zud/Desktop/adam/adam.mem)
      PAE type : No PAE
```

2. What was the process ID of notepad.exe?

The process ID of notepad is: 3032 we executed a pstree on volatility and grep notepad.

```
root@z:/home/zud/Desktop/adam# volatility -f adam.mem --profile=Win7SP1x64 pstree | grep notepad
Volatility Foundation Volatility Framework 2.6.1
. 0xfffffa80054f9060:notepad.exe          3032  1432    1    60 2019-03-22 05:32:22 UTC+0000
```

3. Name the child processes of wscript.exe.

The child processes of wscript.exe are: UWkpiFjDzM.exe and a child of UWkpiFjDzM.exe is: cmd.exe we executed a pstree on volatility and grep wscript.

```
root@z:/home/zud/Desktop/adam# volatility -f adam.mem --profile=Win/SPIx64
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.addrspaces.ieee1394 (AttributeError:
ce_nodeid)
Name                               Pid    PPid    Thds
-----
0xffffffffa8003de39c0:explorer.exe  1432    1308    28
. 0xffffffffa80042aa430:cmd.exe      1408    1432     1
. 0xffffffffa8005d067d0:StikyNot.exe  1628    1432     8
. 0xffffffffa80042dbb30:chrome.exe   3248    1432    32
.. 0xffffffffa8005442b30:chrome.exe  4232    3248    14
.. 0xffffffffa80047beb30:chrome.exe  3244    3248     7
.. 0xffffffffa80053306f0:chrome.exe  1816    3248    14
.. 0xffffffffa8005300b30:chrome.exe  4156    3248    14
.. 0xffffffffa8005419b30:chrome.exe  4240    3248    14
.. 0xffffffffa800540db30:chrome.exe  4520    3248    10
.. 0xffffffffa80052f0060:chrome.exe  2100    3248     2
.. 0xffffffffa80053cbb30:chrome.exe  4688    3248    13
. 0xffffffffa800474c060:OUTLOOK.EXE  3688    1432    30
. 0xffffffffa8004798320:calc.exe     3548    1432     3
. 0xffffffffa80053d3060:POWERPNT.EXE 4048    1432    23
. 0xffffffffa8004905620:hfs.exe      3952    1432     6
.. 0xffffffffa8005a80060:wscript.exe  5116    3952     8
... 0xffffffffa8005a1d9e0:UWkpjFjDzM.exe 3496    5116     5
.... 0xffffffffa8005bb0060:cmd.exe    4660    3496     1
```

4. What was the IP address of the machine at the time the RAM dump was created?

With netscan we can visualize the network and the local IP of the machine, besides the ipv6 and local address we get that the IPv4 of the machine is: [10].[0].[0].[101]

```

root@z:/home/zud/Desktop/adam# volatility -f adam.mem --profile=Win7SP1x64 netscan
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.addrspaces.ieee1394 (AttributeError: /usr/local/lib/python3.10/site-packages/addrspaces/ieee1394.py:10: ModuleNotFoundError: No module named 'volatility.plugins.addrspaces.ieee1394')
Offset(P)          Proto    Local Address          Foreign Address        State
0x13e057300         UDPv4    10.0.0.101:55736       *:.*
0x13e05b4f0         UDPv6    :::55735               *:.*
0x13e05b790         UDPv6    fe80::7475:ef30:be18:7807:55734 *:.*
0x13e05d4b0         UDPv6    fe80::7475:ef30:be18:7807:1900 *:.*
0x13e05dec0         UDPv4    127.0.0.1:55737       *:.*
0x13e05e3f0         UDPv4    10.0.0.101:1900       *:.*
0x13e05eab0         UDPv6    :::1900                *:.*
0x13e064d70         UDPv4    127.0.0.1:1900       *:.*
0x13e02bcf0         TCPv4    -:49220                72.51.60.132:443      CLOSED
0x13e035790         TCPv4    -:49223                72.51.60.132:443      CLOSED
0x13e036470         TCPv4    -:49224                72.51.60.132:443      CLOSED
0x13e258010         UDPv4    127.0.0.1:55560       *:.*
0x13e305a50         UDPv4    0.0.0.0:5355          *:.*
0x13e360be0         UDPv4    0.0.0.0:63790        *:.*
0x13e490ec0         UDPv4    0.0.0.0:5355          *:.*
0x13e490ec0         UDPv6    :::5355               *:.*
0x13e5683e0         UDPv4    10.0.0.101:137        *:.*
0x13e594250         UDPv4    10.0.0.101:138        *:.*
0x13e597ec0         UDPv4    0.0.0.0:0             *:.*
0x13e597ec0         UDPv6    :::0                   *:.*
0x13e61fb30         UDPv6    fe80::7475:ef30:be18:7807:546 *:.*
0x13e918010         UDPv4    0.0.0.0:56372         *:.*
0x13e9cd730         UDPv4    127.0.0.1:57374       *:.*
0x13ea8e6a0         UDPv4    127.0.0.1:61704       *:.*
0x13ead0bf0         UDPv4    127.0.0.1:55614       *:.*

```

5. Based on the answer regarding to the infected PID, can you determine what the IP of the attacker was?

with a grep on the netscan we checked for notepad, wscript and UWkpjFjDzM (the child of the wscript) and we got 2 connections, and 1 of them containing the IP of the attacker, which is: [10].[0].[0].[106]

```

root@z:/home/zud/Desktop/adam# volatility -f adam.mem --profile=Win7SP1x64 netscan | grep 'notepad\|wscript\|UWkpjFjDzM'
Volatility Foundation Volatility Framework 2.6.1
0x13e258010         UDPv4    127.0.0.1:55560       *:.*          5116      wscript.exe    2019-03-22 05:35:32 UTC+0000
0x13e397190         TCPv4    10.0.0.101:49217      10.0.0.106:4444    ESTABLISHED 3496      UWkpjFjDzM.exe

```

6. What process name is VCRUNTIME140.dll associated with?

I ran dlllist and check for all the processes with that dll with the search function of the console: C:\Program Files (x86)\Internet Explorer\iexplore.exe C:\Program Files (x86)\Microsoft Office\root\Office16\OUTLOOK.EXE C:\Program Files (x86)\Microsoft Office\root\Office16\EXCEL.EXE C:\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeClickToRun.exe C:\Program Files (x86)\Microsoft Office\root\Office16\POWERPNT.EXE

Command line : "C:\Program Files (x86)\Microsoft Office\root\Office16\POWERPNT.EXE"

Base	Size	LoadCount	LoadTime	Path
0x000000000050000	0x1ce000	0xffff	1970-01-01 00:00:00 UTC+0000	C:\Program Files (x86)\Microsoft Office\root\Office16\POWERPNT.EXE
0x0000000077260000	0x1a9000	0xffff	1970-01-01 00:00:00 UTC+0000	C:\Windows\SYSTEM32\nt
0x0000000073bd0000	0x3f000	0x3	2019-03-22 05:35:09 UTC+0000	C:\Windows\SYSTEM32\wo
0x0000000073b70000	0x5c000	0x1	2019-03-22 05:35:09 UTC+0000	C:\Windows\SYSTEM32\wo
0x0000000073b60000	0x8000	0x1	2019-03-22 05:35:09 UTC+0000	C:\Windows\SYSTEM32\wo
0x000000000050000	0x1ce000	0xffff	1970-01-01 00:00:00 UTC+0000	C:\Program Files (x86)\Microsoft Office\root\Office16\POWERPNT.EXE
0x0000000077440000	0x180000	0xffff	1970-01-01 00:00:00 UTC+0000	C:\Windows\SysWOW64\nt
0x0000000075560000	0x110000	0xffff	2019-03-22 05:35:09 UTC+0000	C:\Windows\syswow64\ke
0x0000000075890000	0x46000	0xffff	2019-03-22 05:35:09 UTC+0000	C:\Windows\syswow64\ke
0x0000000073dc0000	0x1ea000	0xffff	2019-03-22 05:35:09 UTC+0000	C:\Program Files (x86)\Microsoft Office\root\Office16\POWERPNT.EXE
0x0000000072a40000	0x1c0000	0xffff	2019-03-22 05:35:09 UTC+0000	C:\Program Files (x86)\Microsoft Office\root\Office16\c2r32.dll
0x0000000076b90000	0x8f000	0xffff	2019-03-22 05:35:09 UTC+0000	C:\Windows\syswow64\OLEAUT32.dll
0x0000000076bd0000	0x15c000	0xffff	2019-03-22 05:35:09 UTC+0000	C:\Windows\syswow64\ole32.dll
0x00000000758e0000	0xac000	0xffff	2019-03-22 05:35:09 UTC+0000	C:\Windows\syswow64\msvcrt.dll
0x0000000075990000	0x90000	0xffff	2019-03-22 05:35:09 UTC+0000	C:\Windows\syswow64\GDI32.dll
0x0000000075740000	0x100000	0xffff	2019-03-22 05:35:09 UTC+0000	C:\Windows\syswow64\USER32.dll
0x0000000075180000	0xa0000	0xffff	2019-03-22 05:35:09 UTC+0000	C:\Windows\syswow64\ADVAPI32.dll
0x0000000076990000	0x19000	0xffff	2019-03-22 05:35:09 UTC+0000	C:\Windows\SysWOW64\sechost.dll
0x0000000075420000	0xf0000	0xffff	2019-03-22 05:35:09 UTC+0000	C:\Windows\syswow64\RPCRT4.dll
0x0000000074f90000	0x60000	0xffff	2019-03-22 05:35:09 UTC+0000	C:\Windows\syswow64\SspiCli.dll
0x0000000074f80000	0xc000	0xffff	2019-03-22 05:35:09 UTC+0000	C:\Windows\syswow64\CRYPTBASE.dll
0x0000000077410000	0xa000	0xffff	2019-03-22 05:35:09 UTC+0000	C:\Windows\syswow64\LPK.dll
0x0000000076d20000	0x9d000	0xffff	2019-03-22 05:35:09 UTC+0000	C:\Windows\syswow64\USP10.dll
0x0000000075a80000	0xc4a000	0xffff	2019-03-22 05:35:09 UTC+0000	C:\Windows\syswow64\SHELL32.dll
0x0000000075a20000	0x57000	0xffff	2019-03-22 05:35:09 UTC+0000	C:\Windows\syswow64\SHLWAPI.dll
0x0000000074620000	0x17000	0xffff	2019-03-22 05:35:09 UTC+0000	C:\Windows\system32\USERENV.dll
0x0000000074610000	0xb000	0xffff	2019-03-22 05:35:09 UTC+0000	C:\Windows\system32\profapi.dll
0x00000000745f0000	0x15000	0xffff	2019-03-22 05:35:09 UTC+0000	C:\Program Files (x86)\Microsoft Office\root\Office16\VCRUNTIME140.dll

7. What is the md5 hash value the potential malware on the system?

The PID of UWkpjFjDzM is 3496, and we are sure this PID is malicious, so we extract the process from the memory:

```
root@z:/home/zud/Desktop/adam# volatility -f adam.mem --profile=Win7SP1x64 procdump -D ./3496/ -p 3496
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.addrspaces.ieee1394 (AttributeError: /usr/local/lib/libforensic1394.so.2: undefined symbol: forensic1394_get_device_nodeid)
Process(V)      ImageBase      Name      Result
-----
0xfffffa8005a1d9e0 0x0000000000400000 UWkpjFjDzM.exe OK: executable.3496.exe
```

and then we get the md5 hash from it: 690ea20bc3bdfb328e23005d9a80c290 ./3496/executable.3496.exe

```
root@z:/home/zud/Desktop/adam# md5sum ./3496/executable.3496.exe
690ea20bc3bdfb328e23005d9a80c290 ./3496/executable.3496.exe
```

8. An application was run at 2019-03-07 23:06:58 UTC, what is the name of the program? (Include extension)

I ran shimcache that let me know when was the last time an executable was accessed or modified, the program was: Skype.exe

```
root@z:/home/zud/Desktop/adam# volatility -f adam.mem --profile=Win7SP1x64 shimcache | grep '2019-03-07 23:06:58'
Volatility Foundation Volatility Framework 2.6.1
2019-03-07 23:06:58 UTC+0000 \??\C:\Program Files (x86)\Microsoft\Skype for Desktop\Skype.exe
```

9. What is the shortname of the file at file record 59045?

I use mftparser to check the Master File Table. In here I use the grep tool again to find the 59045 record. There are 2 file names, the short name is: EMPLOY~1.XLS

```
*****
*****
MFT entry found at offset 0x2193d400
Attribute: In Use & File
Record Number: 59045
Link count: 2

$STANDARD_INFORMATION
Creation          Modified          MFT Altered          Access Date          Type
-----
2019-03-17 06:50:07 UTC+0000 2019-03-17 07:04:43 UTC+0000 2019-03-17 07:04:43 UTC+0000 2019-03-17 07:04:42 UTC+0000 Archive

$FILE_NAME
Creation          Modified          MFT Altered          Access Date          Name/Path
-----
2019-03-17 06:50:07 UTC+0000 2019-03-17 07:04:43 UTC+0000 2019-03-17 07:04:43 UTC+0000 2019-03-17 07:04:42 UTC+0000 Users\Bob\DOCUME~1\EMPLOY~1\EMPLOY~1.XLS

$FILE_NAME
Creation          Modified          MFT Altered          Access Date          Name/Path
-----
2019-03-17 06:50:07 UTC+0000 2019-03-17 07:04:43 UTC+0000 2019-03-17 07:04:43 UTC+0000 2019-03-17 07:04:42 UTC+0000 Users\Bob\DOCUME~1\EMPLOY~1\EmployeeInformation.xlsx
```

10. This box was exploited and is running meterpreter. What PID was infected?

The PID running meterpreter which is PID 3496 a child of wscript with PID 5116.

We are sure of meterpreter running on 3496 as it was the PID who established the connection with the attacker.