Universidad Carlos III de Madrid

Report for Memory Analysis - Evidences

Juan Diego Llano Miraval

Fecha: 18/05/2024

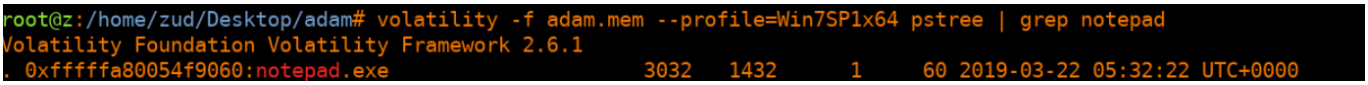
questions

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

The most appropriate profile is Win7SP1x64

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.



3. Name the child processes of wscript.exe.

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

```
root@z:/home/zud/Desktop/adam# volatility -f adam.mem --profile=Win7SP1x64
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.addrspaces.ieee1394 (AttributeErro
ce_nodeid)
Name                                                 Pid   PPid   Thds
---------------------------------------------------- ------ ------ ------ --
 0xfffffa8003de39c0:explorer.exe                     1432   1308     28
. 0xfffffa80042aa430:cmd.exe                         1408   1432      1
. 0xfffffa8005d067d0:StikyNot.exe                    1628   1432      8
. 0xfffffa80042dbb30:chrome.exe                      3248   1432     32
.. 0xfffffa8005442b30:chrome.exe                     4232   3248     14
.. 0xfffffa80047beb30:chrome.exe                     3244   3248      7
.. 0xfffffa80053306f0:chrome.exe                     1816   3248     14
.. 0xfffffa8005300b30:chrome.exe                     4156   3248     14
.. 0xfffffa8005419b30:chrome.exe                     4240   3248     14
.. 0xfffffa800540db30:chrome.exe                     4520   3248     10
.. 0xfffffa80052f0060:chrome.exe                     2100   3248      2
.. 0xfffffa80053cbb30:chrome.exe                     4688   3248     13
. 0xfffffa800474c060:OUTLOOK.EXE                     3688   1432     30
. 0xfffffa8004798320:calc.exe                        3548   1432      3
. 0xfffffa80053d3060:POWERPNT.EXE                    4048   1432     23
. 0xfffffa8004905620:hfs.exe                         3952   1432      6
.. 0xfffffa8005a80060:wscript.exe                    5116   3952      8
... 0xfffffa8005a1d9e0:UWkpjFjDzM.exe                3496   5116      5
.... 0xfffffa8005bb0060: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/loc
ce_nodeid)
Offset(P)          Proto    Local Address                  Foreign Address      State
0x13e057300        UDPv4    10.0.0.101:55736               *:*
0x13e05b4f0        UDPv6    ::1:55735                      *:*
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    ::1:1900                       *:*
0x13e064d70        UDPv4    127.0.0.1:1900                 *:*
0x13e02bcf0        TCPv4    -:49220                        72.51.60.132:443     CLOSE
0x13e035790        TCPv4    -:49223                        72.51.60.132:443     CLOSE
0x13e036470        TCPv4    -:49224                        72.51.60.132:443     CLOSE
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                *:*
```

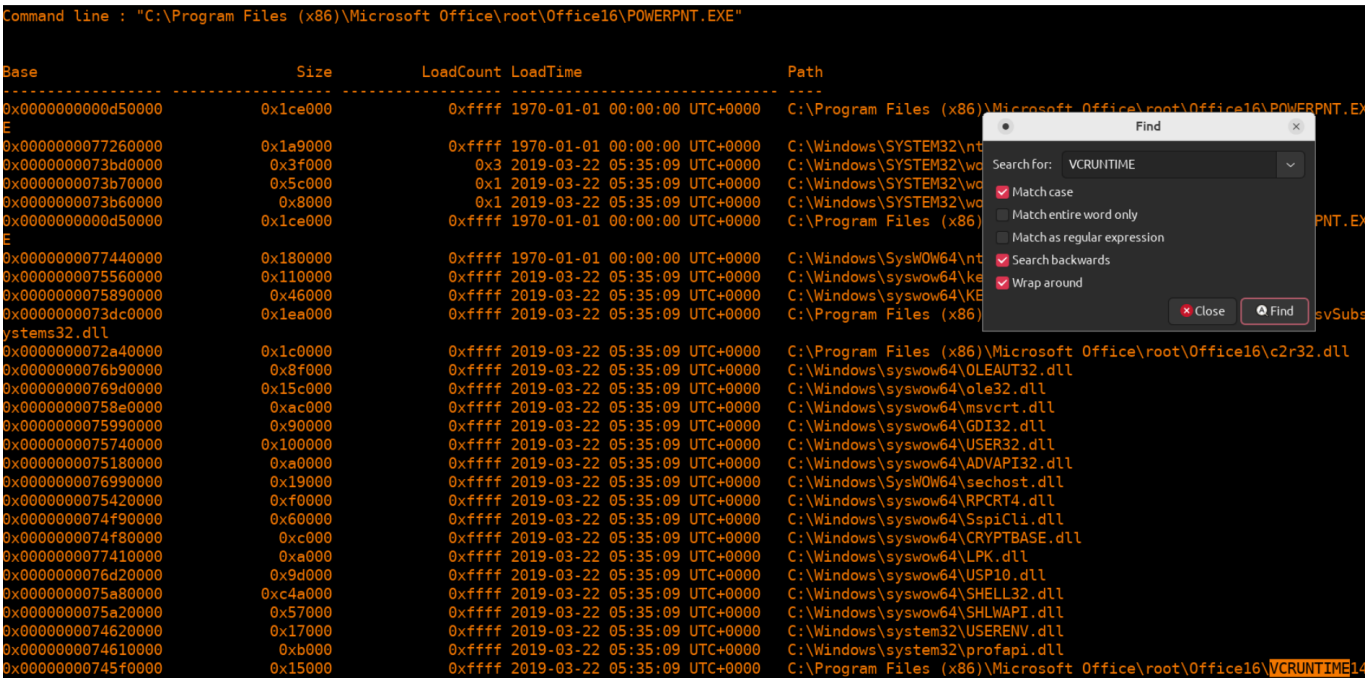
5. Based on the answer regarding to the infected PID, can you determine what the IP of the attacker was?

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
```

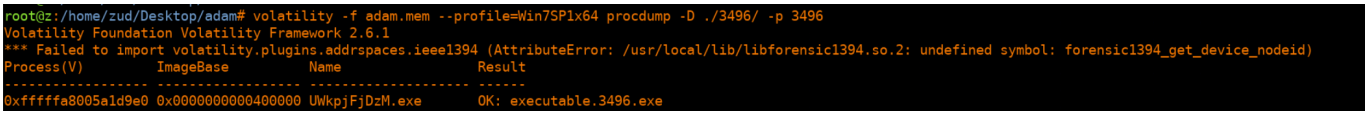
6. What process name is VCRUNTIME140.dll associated with?

I ran dllist 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



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

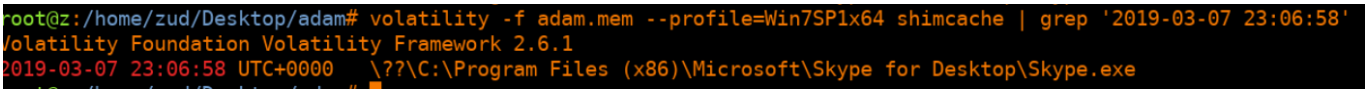
The PID of UWkpjFjDzM is 3496, and we are sure this PID is malicious, so we extract the process from the memory:



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

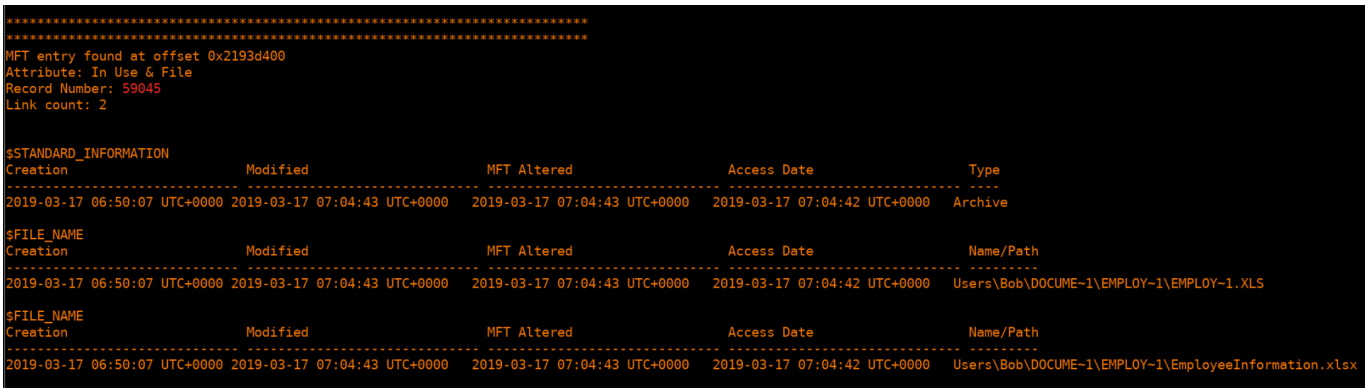
8. An application was run at 2019-03-07 23:06:58 UTC, what is the name of the program? (Include extension)

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



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 meterptreter 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.