Universidad Carlos III de Madrid

Report for Memory Analysis (I) - IP Address

Juan Diego Llano Miraval

Fecha: 18/05/2024

Procedure

The first step on this is to get the profile of the memory:

```
root@z:/home/zud/Desktop/memory# volatility -f memdump imageinfo
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.addrspaces.ieee1394 (AttributeError: /usr/local/lib
ce_nodeid)
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 (/home/zud/Desktop/memory/memdump)
                      PAE type : PAE
                           DTB : 0xb2a000L
                          KDBG : 0x80544ce0L
          Number of Processors : 1
     Image Type (Service Pack) : 2
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2018-06-14 10:56:44 UTC+0000
     Image local date and time : 2018-06-14 05:56:44 -0500
```

with this we analice the processes inside the memory:

```
root@z:/home/zud/Desktop/memory# volatility -f memdump --profile=WinXPSP2x86 pslist
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.addrspaces.ieee1394 (AttributeError: /usr/local/lib/libforensic1394.so.2: undefined symbol: for
ce_nodeid)
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0x817cc830 System                    4      0     54      822 ------      0
0x812e69e0 smss.exe                548      4      3       21 ------      0 2018-06-14 10:38:40 UTC+0000
0x81356550 csrss.exe               596    548     11      463      0      0 2018-06-14 10:38:40 UTC+0000
0x813618d8 winlogon.exe            620    548     18      440      0      0 2018-06-14 10:38:40 UTC+0000
0x8118b020 services.exe            664    620     16      353      0      0 2018-06-14 10:38:40 UTC+0000
0x8118f020 lsass.exe               676    620     21      349      0      0 2018-06-14 10:38:40 UTC+0000
0x8144c610 vmacthlp.exe            832    664      1       24      0      0 2018-06-14 10:38:40 UTC+0000
0x8166c8f0 svchost.exe             848    664     19      207      0      0 2018-06-14 10:38:40 UTC+0000
0x8166c460 svchost.exe             932    664     10      280      0      0 2018-06-14 10:38:41 UTC+0000
0x815a6da0 svchost.exe            1024    664     70     1388      0      0 2018-06-14 10:38:41 UTC+0000
0x813289a0 svchost.exe            1072    664      6       93      0      0 2018-06-14 10:38:41 UTC+0000
0x816df800 svchost.exe            1224    664     13      201      0      0 2018-06-14 10:38:42 UTC+0000
0x81331ae8 spoolsv.exe            1352    664     10      120      0      0 2018-06-14 10:38:42 UTC+0000
0x81570810 explorer.exe           1620   1580     13      372      0      0 2018-06-14 10:38:47 UTC+0000
0x812adb30 VMwareTray.exe         1696   1620      1       55      0      0 2018-06-14 10:38:47 UTC+0000
0x8144d500 VMwareUser.exe         1708   1620      8      218      0      0 2018-06-14 10:38:47 UTC+0000
0x812aa7f8 ctfmon.exe             1720   1620      1       67      0      0 2018-06-14 10:38:47 UTC+0000
0x813c6980 tlntsvr.exe            1960    664      3      103      0      0 2018-06-14 10:39:01 UTC+0000
0x8162b980 vmtoolsd.exe            204    664      4      229      0      0 2018-06-14 10:39:08 UTC+0000
0x811903c8 VMUpgradeHelper         288    664      3       96      0      0 2018-06-14 10:39:08 UTC+0000
0x81547870 alg.exe                1184    664      6      104      0      0 2018-06-14 10:39:09 UTC+0000
0x8154c020 cmd.exe                1392   1620      1       31      0      0 2018-06-14 10:39:41 UTC+0000
0x81478da0 hot_pictures.ex         324   1620      0 --------      0      0 2018-06-14 10:39:57 UTC+0000   2018-06-14 10:50:26 UTC+0000
0x81714980 wuauclt.exe            1788   1024      3      141      0      0 2018-06-14 10:40:08 UTC+0000
0x8143c6f8 wscntfy.exe            1332   1024      1       36      0      0 2018-06-14 10:40:09 UTC+0000
0x8147c650 cmd.exe                 640    324      1       35      0      0 2018-06-14 10:40:14 UTC+0000
0x813ec418 ping.exe               1688    640      1       51      0      0 2018-06-14 10:45:05 UTC+0000
0x816f0da0 firefox.exe            1116   1620     30      406      0      0 2018-06-14 10:45:47 UTC+0000
0x81397da0 TFTPServer.exe         1572   1620     12      254      0      0 2018-06-14 10:45:56 UTC+0000
0x8147ada0 SolarWinds TFTP        1776    664      9      211      0      0 2018-06-14 10:46:13 UTC+0000
                                                                                                  enp0s3: 10.0.2.15
```

with pstree on volatility we get some interested processes associated to a potential attack vector:

```
. 0x81478da0:hot_pictures.ex                    324   1620      0 ------ 2018-06-14 10:39:57 UTC+0000
.. 0x8147c650:cmd.exe                           640    324      1     35 2018-06-14 10:40:14 UTC+0000
... 0x813ec418:ping.exe                        1688    640      1     51 2018-06-14 10:45:05 UTC+0000
. 0x816f0da0:firefox.exe                       1116   1620     30    406 2018-06-14 10:45:47 UTC+0000
. 0x81397da0:TFTPServer.exe                    1572   1620     12    254 2018-06-14 10:45:56 UTC+0000
. 0x8154c020:cmd.exe                           1392   1620      1     31 2018-06-14 10:39:41 UTC+0000
.. 0x81739020:mdd.exe                          1264   1392      1     23 2018-06-14 10:56:44 UTC+0000
. 0x812ddda0:samba_service.e                   1176   1620      2    101 2018-06-14 10:53:40 UTC+0000
.. 0x812bb8d0:cmd.exe                          1940   1176      1     35 2018-06-14 10:54:19 UTC+0000
... 0x813cb658:ping.exe                        1944   1940      1     51 2018-06-14 10:54:31 UTC+0000
. 0x8159ada0:IEXPLORE.EXE                      1956   1620     14    356 2018-06-14 10:46:31 UTC+0000
```

We proceed to check the connections, most of them are from the firefox process, but there are this ones from the samba service:

```
root@z:/home/zud/Desktop/memory# volatility -f memdump --profile=WinXPSP2x86 connscan
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.addrspaces.ieee1394 (AttributeError: /usr/local/lib/
ce_nodeid)
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------ ------------------------ ---
0x0159ed40 192.168.21.140:1159      216.58.210.131:80        1116
0x01697610 192.168.21.140:1148      216.58.210.130:443       1116
0x016a1008 192.168.21.140:1139      192.168.21.161:445       1176
0x016ae088 127.0.0.1:8099           127.0.0.1:1073           1776
0x016b3a68 192.168.21.140:1164      216.58.211.35:443        1116
0x016b5a88 192.168.21.140:1176      216.58.211.35:443        1116
0x016c24f8 127.0.0.1:1051           127.0.0.1:1050           1116
0x016dace0 127.0.0.1:1054           127.0.0.1:1055           1116
0x016db440 192.168.21.140:1165      216.58.211.35:80         1116
0x016df220 192.168.21.140:1171      216.58.211.46:443        1116
0x017082a8 177.50.1.0:0             0.0.0.0:0                2167440064
0x01796928 192.168.21.140:1156      104.19.199.151:443       1116
0x01799008 192.168.21.140:1177      216.58.211.35:443        1116
0x01799c58 192.168.21.140:1161      104.83.54.35:443         1116
0x0179a4a0 192.168.21.140:1174      216.58.211.33:443        1116
0x017a5840 192.168.21.140:1154      104.19.199.151:443       1116
0x017a9b48 192.168.21.140:1160      216.58.211.46:80         1116
0x017ca888 192.168.21.140:1147      172.217.16.228:443       1116
0x017cf228 192.168.21.140:1167      216.58.210.130:443       1116
0x017d1630 192.168.21.140:1178      216.58.211.35:443        1116
0x017d1bf8 127.0.0.1:1073           127.0.0.1:8099           1572
```

we did find suspicious processes that could have infected the system, and an odd connection through the samba process, the IP is [192].[168].[21].[161] at port 445.