ANÁLISIS FORENSE MEMORIA WINDOWS 7 CASO 03

https://github.com/aguayro @9v@yr0

Nos llega un correo electrónico con un pdf adjunto un tanto sospechoso, preparamos un entorno con Windows 7 y abrimos el correo electrónico y procedemos a realizar un volcado de memoria ram para su estudio.

1.- Realizo el cálculo del hash de la imagen.
Obtengo con el comando sha1sum el hash del fichero que se ha entregado para su comprobación con el documento de custodia.

$ sha256sum memdump.mem

```
└─# sha256sum win7-malware.raw
350335781ad44c022574c355d90164a530651de54de977fb20e8d1f61d85f3d2  win7-malware.raw
```

2.- Averiguo el sistema operativo de la memoria:
Ejecuto el comando siguiente:

$ volatility -f memdump.mem imageinfo

```
└─# volatility -f win7-malware.raw imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_23418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/kali/Documents/forense/memory_case03/win7-malware.raw)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf8000283b0a0L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff8000283cd00L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2023-08-16 21:35:48 UTC+0000
     Image local date and time : 2023-08-16 22:35:48 +0100
```

Volatility nos indica que el sistema de la imagen es un Windows 7 sp1 x64

3.- Veamos que procesos se están ejecutando, la estructura de los procesos así como si hay procesos sospechosos.

$ volatility -f win7-malware.raw --profile=Win7SP1x64 psscan

```
└─# volatility -f win7-malware.raw --profile=Win7SP1x64 psscan
Volatility Foundation Volatility Framework 2.6
Offset(P)          Name                PID   PPID PDB              Time created                   Time exited
------------------ ---------------- ------ ------ ---------------- ------------------------------ ------------------------------
0x00000000070cc040 System                4      0 0x0000000000187000 2023-08-16 21:29:15 UTC+0000
0x00000000071a17c0 BraveCrashHand     1456   1700 0x000000008f184000 2023-08-16 21:31:45 UTC+0000
0x00000000071ccb30 ProcessHacker.     1932   1548 0x0000000090634000 2023-08-16 21:31:40 UTC+0000
0x000000011e2cd7c0 taskhost.exe       1600    468 0x0000000097942000 2023-08-16 21:30:00 UTC+0000
0x000000011e30eb30 sppsvc.exe         1808    468 0x000000009645c000 2023-08-16 21:30:15 UTC+0000
0x000000011e357b30 explorer.exe       1548   1656 0x00000000866fc000 2023-08-16 21:31:17 UTC+0000
0x000000011e4b29e0 svchost.exe        1048    468 0x000000009bb0a000 2023-08-16 21:29:37 UTC+0000
0x000000011e4d3b30 armsvc.exe         1160    468 0x000000009b3fa000 2023-08-16 21:29:41 UTC+0000
0x000000011e6788d0 svchost.exe         596    468 0x00000000a1e5a000 2023-08-16 21:29:25 UTC+0000
0x000000011e67cb30 svchost.exe         672    468 0x00000000a1d5b000 2023-08-16 21:29:29 UTC+0000
0x000000011e758060 dwm.exe            1452    840 0x0000000091d1a000 2023-08-16 21:31:04 UTC+0000
0x000000011e75b2d0 svchost.exe         800    468 0x000000009fea8000 2023-08-16 21:29:31 UTC+0000
0x000000011e75fb30 svchost.exe         840    468 0x000000009f270000 2023-08-16 21:29:32 UTC+0000
0x000000011e78f740 svchost.exe         880    468 0x000000009f479000 2023-08-16 21:29:32 UTC+0000
0x000000011e79db30 svchost.exe         912    468 0x000000009f37f000 2023-08-16 21:29:32 UTC+0000
0x000000011e7bdb30 spoolsv.exe         532    468 0x000000009bedd000 2023-08-16 21:29:37 UTC+0000
0x000000011e7fbb30 svchost.exe         876    468 0x000000009c857000 2023-08-16 21:29:36 UTC+0000
0x000000011e95cb30 wininit.exe         372    316 0x00000000a3dbb000 2023-08-16 21:29:23 UTC+0000
0x000000011e9688e0 csrss.exe           324    316 0x00000000a4675000 2023-08-16 21:29:22 UTC+0000
0x000000011e973060 csrss.exe           384    364 0x00000000a394a000 2023-08-16 21:29:23 UTC+0000
0x000000011e986910 winlogon.exe        424    364 0x00000000a3450000 2023-08-16 21:29:23 UTC+0000
0x000000011e9d9810 services.exe        468    372 0x00000000a3136000 2023-08-16 21:29:23 UTC+0000
0x000000011e9e4910 lsass.exe           484    372 0x00000000a2c1c000 2023-08-16 21:29:23 UTC+0000
0x000000011e9eab30 lsm.exe             492    372 0x00000000a2d63000 2023-08-16 21:29:23 UTC+0000
0x000000011ec9b250 BraveCrashHand      768   1700 0x0000000091cbc000 2023-08-16 21:31:33 UTC+0000
0x000000011f06ab30 taskeng.exe        1636    912 0x000000009710a000 2023-08-16 21:30:00 UTC+0000   2023-08-16 21:37:10 UTC+0000
0x000000011f14d630 svchost.exe        1208    468 0x000000009ac2b000 2023-08-16 21:29:46 UTC+0000
0x000000011f194770 smss.exe            248      4 0x00000000a9040000 2023-08-16 21:29:15 UTC+0000
0x000000011fa25060 taskeng.exe        1460    912 0x000000005f930000 2023-08-16 21:39:40 UTC+0000
0x000000011faddb30 RdrCEF.exe         4032   3044 0x000000001de17000 2023-08-16 21:33:41 UTC+0000   2023-08-16 21:33:45 UTC+0000
0x000000011faff630 WmiPrvSE.exe       3416    596 0x000000001a7be000 2023-08-16 21:33:52 UTC+0000
```

ANÁLISIS FORENSE MEMORIA WINDOWS 7 CASO 03

https://github.com/aguayro @9v@yr0

$ volatility -f win7-malware.raw --profile=Win7SP1x64 pslist

```
└─# volatility -f win7-malware.raw --profile=Win7SP1x64 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0xfffffa80036cc040 System                    4      0     80      534 ------      0 2023-08-16 21:29:15 UTC+0000
0xfffffa8004794770 smss.exe                248      4      2       29 ------      0 2023-08-16 21:29:15 UTC+0000
0xfffffa8004f688e0 csrss.exe               324    316      9      382      0      0 2023-08-16 21:29:22 UTC+0000
0xfffffa8004f5cb30 wininit.exe             372    316      3       74      0      0 2023-08-16 21:29:23 UTC+0000
0xfffffa8004f73060 csrss.exe               384    364      9      255      1      0 2023-08-16 21:29:23 UTC+0000
0xfffffa8004f86910 winlogon.exe            424    364      3      111      1      0 2023-08-16 21:29:23 UTC+0000
0xfffffa8004fd9810 services.exe            468    372      9      198      0      0 2023-08-16 21:29:23 UTC+0000
0xfffffa8004fe4910 lsass.exe               484    372      8      699      0      0 2023-08-16 21:29:23 UTC+0000
0xfffffa8004feab30 lsm.exe                 492    372     10      144      0      0 2023-08-16 21:29:23 UTC+0000
0xfffffa80050788d0 svchost.exe             596    468      9      348      0      0 2023-08-16 21:29:25 UTC+0000
0xfffffa800507cb30 svchost.exe             672    468      6      257      0      0 2023-08-16 21:29:29 UTC+0000
0xfffffa800515b2d0 svchost.exe             800    468     21      532      0      0 2023-08-16 21:29:31 UTC+0000
0xfffffa800515fb30 svchost.exe             840    468     25      520      0      0 2023-08-16 21:29:32 UTC+0000
0xfffffa800518f740 svchost.exe             880    468     20      525      0      0 2023-08-16 21:29:32 UTC+0000
0xfffffa800519db30 svchost.exe             912    468     35     1145      0      0 2023-08-16 21:29:32 UTC+0000
0xfffffa80051fbb30 svchost.exe             876    468     15      386      0      0 2023-08-16 21:29:36 UTC+0000
0xfffffa80051bdb30 spoolsv.exe             532    468     12      278      0      0 2023-08-16 21:29:37 UTC+0000
0xfffffa80052b29e0 svchost.exe            1048    468     17      306      0      0 2023-08-16 21:29:37 UTC+0000
0xfffffa80052d3b30 armsvc.exe             1160    468      4       63      0      1 2023-08-16 21:29:41 UTC+0000
0xfffffa800474d630 svchost.exe            1208    468     20      296      0      0 2023-08-16 21:29:46 UTC+0000
0xfffffa80054cd7c0 taskhost.exe           1600    468      7      157      1      0 2023-08-16 21:30:00 UTC+0000
0xfffffa800550eb30 sppsvc.exe             1808    468      4      149      0      0 2023-08-16 21:30:15 UTC+0000
0xfffffa8005158060 dwm.exe                1452    840      6       81      1      0 2023-08-16 21:31:04 UTC+0000
0xfffffa8005557b30 explorer.exe           1548   1656     23      920      1      0 2023-08-16 21:31:17 UTC+0000
0xfffffa8004a9b250 BraveCrashHand          768   1700      5       99      0      1 2023-08-16 21:31:33 UTC+0000
0xfffffa80037a17c0 BraveCrashHand         1456   1700      5       93      0      0 2023-08-16 21:31:45 UTC+0000
0xfffffa8003890740 svchost.exe            1880    468     15      318      0      0 2023-08-16 21:31:47 UTC+0000
0xfffffa800388c060 SearchIndexer.         1892    468     11      648      0      0 2023-08-16 21:31:48 UTC+0000
0xfffffa800390ab30 wmpnetwk.exe           1340    468      9      203      0      0 2023-08-16 21:31:59 UTC+0000
0xfffffa800398a2b0 svchost.exe            2220    468     10      349      0      0 2023-08-16 21:32:07 UTC+0000
0xfffffa8003a53b30 notepad.exe            2984   1548      2       77      1      0 2023-08-16 21:32:42 UTC+0000
0xfffffa8003a5eb30 AcroRd32.exe           3044   1548     16      529      1      1 2023-08-16 21:32:49 UTC+0000
0xfffffa8003a62b30 AcroRd32.exe           1956   3044     13      340      1      1 2023-08-16 21:32:49 UTC+0000
```

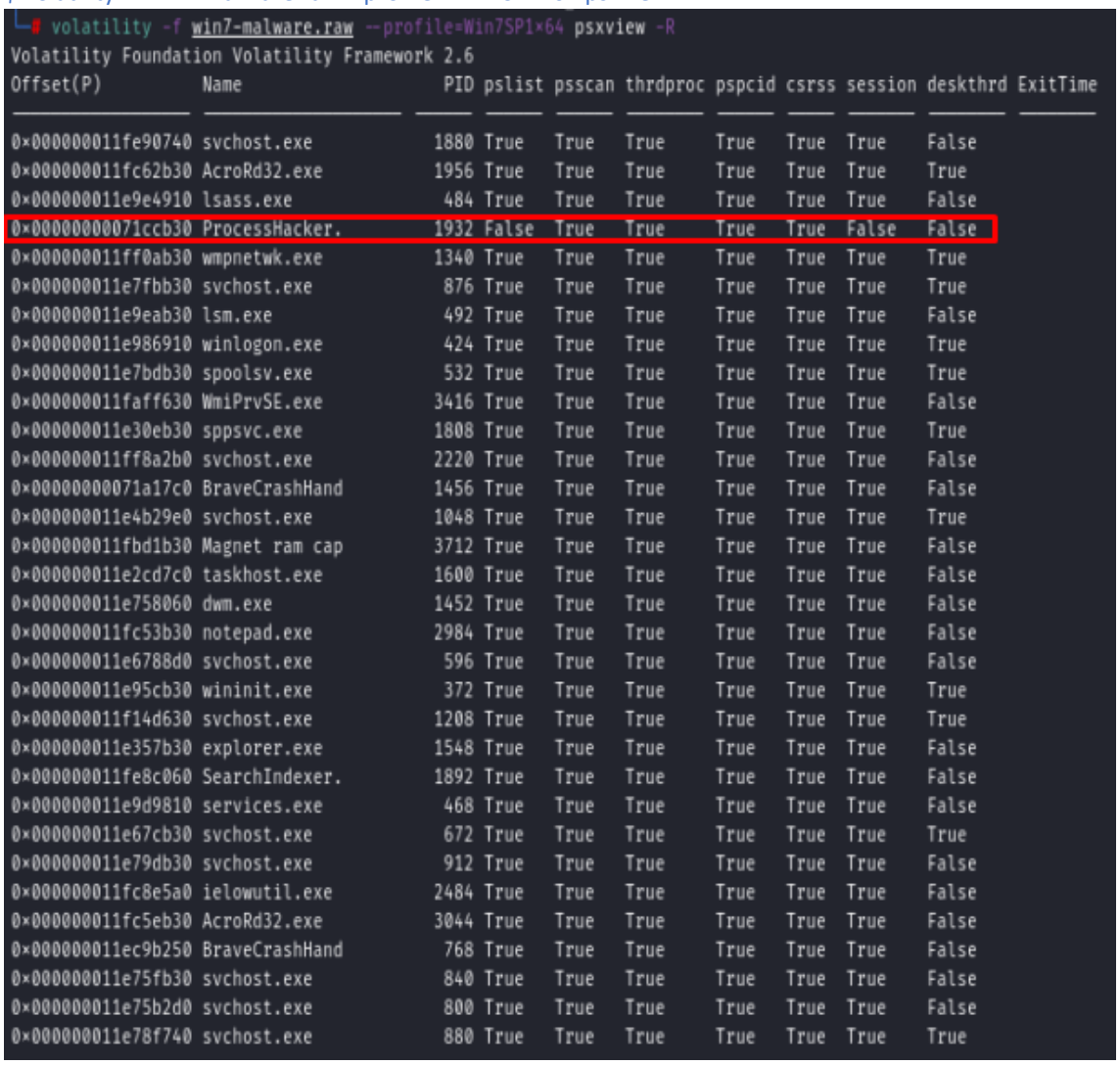
$ volatility -f win7-malware.raw --profile=Win7SP1x64 pstree

```
└─# volatility -f win7-malware.raw --profile=Win7SP1x64 pstree
Volatility Foundation Volatility Framework 2.6
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0xfffffa8004f73060:csrss.exe                         384    364      9    255 2023-08-16 21:29:23 UTC+0000
 0xfffffa8004f86910:winlogon.exe                      424    364      3    111 2023-08-16 21:29:23 UTC+0000
 0xfffffa8004a9b250:BraveCrashHand                    768   1700      5     99 2023-08-16 21:31:33 UTC+0000
 0xfffffa80037a17c0:BraveCrashHand                   1456   1700      5     93 2023-08-16 21:31:45 UTC+0000
 0xfffffa80036cc040:System                              4      0     80    534 2023-08-16 21:29:15 UTC+0000
. 0xfffffa8004794770:smss.exe                         248      4      2     29 2023-08-16 21:29:15 UTC+0000
 0xfffffa8004f688e0:csrss.exe                         324    316      9    382 2023-08-16 21:29:22 UTC+0000
 0xfffffa8004f5cb30:wininit.exe                       372    316      3     74 2023-08-16 21:29:23 UTC+0000
. 0xfffffa8004fd9810:services.exe                     468    372      9    198 2023-08-16 21:29:23 UTC+0000
.. 0xfffffa80052d3b30:armsvc.exe                     1160    468      4     63 2023-08-16 21:29:41 UTC+0000
.. 0xfffffa80051fbb30:svchost.exe                     876    468     15    386 2023-08-16 21:29:36 UTC+0000
.. 0xfffffa800519db30:svchost.exe                     912    468     35   1145 2023-08-16 21:29:32 UTC+0000
... 0xfffffa8003c25060:taskeng.exe                   1460    912      4 15 ... 4 2023-08-16 21:39:40 UTC+0000
.. 0xfffffa80051bdb30:spoolsv.exe                     532    468     12    278 2023-08-16 21:29:37 UTC+0000
.. 0xfffffa80052b29e0:svchost.exe                    1048    468     17    306 2023-08-16 21:29:37 UTC+0000
.. 0xfffffa80038bd060:svchost.exe                    2676    468      5 21 ... 8 2023-08-16 21:41:39 UTC+0000
.. 0xfffffa800507cb30:svchost.exe                     672    468      6    257 2023-08-16 21:29:29 UTC+0000
.. 0xfffffa800474d630:svchost.exe                    1208    468     20    296 2023-08-16 21:29:46 UTC+0000
.. 0xfffffa800390ab30:wmpnetwk.exe                   1340    468      9    203 2023-08-16 21:31:59 UTC+0000
.. 0xfffffa80054cd7c0:taskhost.exe                   1600    468      7    157 2023-08-16 21:30:00 UTC+0000
.. 0xfffffa800515b2d0:svchost.exe                     800    468     21    532 2023-08-16 21:29:31 UTC+0000
.. 0xfffffa800515fb30:svchost.exe                     840    468     25    520 2023-08-16 21:29:32 UTC+0000
... 0xfffffa8005158060:dwm.exe                       1452    840      6     81 2023-08-16 21:31:04 UTC+0000
.. 0xfffffa8003890740:svchost.exe                    1880    468     15    318 2023-08-16 21:31:47 UTC+0000
.. 0xfffffa800388c060:SearchIndexer.                 1892    468     11    648 2023-08-16 21:31:48 UTC+0000
.. 0xfffffa800550eb30:sppsvc.exe                     1808    468      4    149 2023-08-16 21:30:15 UTC+0000
.. 0xfffffa800518f740:svchost.exe                     880    468     20    525 2023-08-16 21:29:32 UTC+0000
.. 0xfffffa800398a2b0:svchost.exe                    2220    468     10    349 2023-08-16 21:32:07 UTC+0000
.. 0xfffffa80050788d0:svchost.exe                     596    468      9    348 2023-08-16 21:29:25 UTC+0000
... 0xfffffa8003cff630:WmiPrvSE.exe                  3416    596      6    112 2023-08-16 21:33:52 UTC+0000
```

ANÁLISIS FORENSE MEMORIA WINDOWS 7 CASO 03

https://github.com/aguayro @9v@yr0

$ volatility -f win7-malware.raw --profile=Win7SP1x64 psxview -R



```
└─# volatility -f win7-malware.raw --profile=Win7SP1x64 psxview -R
Volatility Foundation Volatility Framework 2.6
Offset(P)          Name                    PID pslist psscan thrdproc pspcid csrss session deskthrd ExitTime
------------------ -------------------- ------ ------ ------ -------- ------ ----- ------- -------- --------
0x000000011fe90740 svchost.exe            1880 True   True   True     True   True  True    False
0x000000011fc62b30 AcroRd32.exe           1956 True   True   True     True   True  True    True
0x000000011e9e4910 lsass.exe               484 True   True   True     True   True  True    False
0x00000000071ccb30 ProcessHacker.         1932 False  True   True     True   True  False   False
0x000000011ff0ab30 wmpnetwk.exe           1340 True   True   True     True   True  True    True
0x000000011e7fbb30 svchost.exe             876 True   True   True     True   True  True    True
0x000000011e9eab30 lsm.exe                 492 True   True   True     True   True  True    False
0x000000011e986910 winlogon.exe            424 True   True   True     True   True  True    True
0x000000011e7bdb30 spoolsv.exe             532 True   True   True     True   True  True    True
0x000000011faff630 WmiPrvSE.exe           3416 True   True   True     True   True  True    False
0x000000011e30eb30 sppsvc.exe             1808 True   True   True     True   True  True    True
0x000000011ff8a2b0 svchost.exe            2220 True   True   True     True   True  True    False
0x00000000071a17c0 BraveCrashHand         1456 True   True   True     True   True  True    False
0x000000011e4b29e0 svchost.exe            1048 True   True   True     True   True  True    True
0x000000011fbd1b30 Magnet ram cap         3712 True   True   True     True   True  True    False
0x000000011e2cd7c0 taskhost.exe           1600 True   True   True     True   True  True    False
0x000000011e758060 dwm.exe                1452 True   True   True     True   True  True    False
0x000000011fc53b30 notepad.exe            2984 True   True   True     True   True  True    False
0x000000011e6788d0 svchost.exe             596 True   True   True     True   True  True    False
0x000000011e95cb30 wininit.exe             372 True   True   True     True   True  True    True
0x000000011f14d630 svchost.exe            1208 True   True   True     True   True  True    True
0x000000011e357b30 explorer.exe           1548 True   True   True     True   True  True    False
0x000000011fe8c060 SearchIndexer.         1892 True   True   True     True   True  True    False
0x000000011e9d9810 services.exe            468 True   True   True     True   True  True    False
0x000000011e67cb30 svchost.exe             672 True   True   True     True   True  True    True
0x000000011e79db30 svchost.exe             912 True   True   True     True   True  True    False
0x000000011fc8e5a0 ielowutil.exe          2484 True   True   True     True   True  True    False
0x000000011fc5eb30 AcroRd32.exe           3044 True   True   True     True   True  True    False
0x000000011ec9b250 BraveCrashHand          768 True   True   True     True   True  True    False
0x000000011e75fb30 svchost.exe             840 True   True   True     True   True  True    False
0x000000011e75b2d0 svchost.exe             800 True   True   True     True   True  True    False
0x000000011e78f740 svchost.exe             880 True   True   True     True   True  True    True
```

Nos muestra el proceso processhacker como False, no hay nada que sospechar pues es una aplicación que monitoriza todos los procesos que se han arrancado en el equipo, así como las conexiones abiertas.

https://github.com/aguayro @9v@yr0

4.- Consultemos que ejecutada cada proceso en la línea de comandos a ver si vemos alguna cosa atípica.

$ volatility -f win7-malware.raw --profile=Win7SP1x64 cmdline

```
Volatility Foundation Volatility Framework 2.6
**************************************************
System pid:      4
**************************************************
smss.exe pid:    248
Command line : \SystemRoot\System32\smss.exe
**************************************************
csrss.exe pid:    324
Command line : %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16
**************************************************
wininit.exe pid:    372
Command line : wininit.exe
**************************************************
csrss.exe pid:    384
Command line : %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16
**************************************************
winlogon.exe pid:    424
Command line : winlogon.exe
**************************************************
services.exe pid:    468
Command line : C:\Windows\system32\services.exe
**************************************************
lsass.exe pid:    484
Command line : C:\Windows\system32\lsass.exe
**************************************************
lsm.exe pid:    492
Command line : C:\Windows\system32\lsm.exe
**************************************************
svchost.exe pid:    596
Command line : C:\Windows\system32\svchost.exe -k DcomLaunch
**************************************************
svchost.exe pid:    672
Command line : C:\Windows\system32\svchost.exe -k RPCSS
```

Aquí tenemos dos procesos que debemos investigar, no sólo porque ya está puesto como MALWARE 😉

```
**************************************************
AcroRd32.exe pid:   3044
Command line : "C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" "C:\temp\hotelpaymentproof-MALWARE.pdf"
**************************************************
AcroRd32.exe pid:   1956
Command line : "C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" --type=renderer  "C:\temp\hotelpaymentproof-MALWARE.pdf"
**************************************************
```

Hay dos procesos con se han ejecutado doblemente, pid 3044 y pir 1956.

```
└─# cat psscan.txt| grep 3044
0x000000011faddb30 RdrCEF.exe        4032   3044 0x000000001de17000 2023-08-16 21:33:41 UTC+0000   2023-08-16 21:33:45 UTC+0000
0x000000011fc5eb30 AcroRd32.exe      3044   1548 0x0000000077738000 2023-08-16 21:32:49 UTC+0000
0x000000011fc62b30 AcroRd32.exe      1956   3044 0x000000007624a000 2023-08-16 21:32:49 UTC+0000
```

$ volatility -f win7-malware.raw --profile=Win7SP1x64 psxview -R

```
└─# volatility -f win7-malware.raw --profile=Win7SP1x64 shellbags
Volatility Foundation Volatility Framework 2.6
Scanning for registries....
Gathering shellbag items and building path tree ...
**************************************************************************
Registry: \??\C:\Users\numis\ntuser.dat
Key: Software\Microsoft\Windows\Shell\Bags\1\Desktop
Last updated: 2023-08-16 12:55:18 UTC+0000
Value                File Name      Modified Date                Create Date                  Access Date                  File Attr            Unicode Name
-------------------- -------------- ---------------------------- ---------------------------- ---------------------------- -------------------- --------------------
ItemPos800×600×96(1) ACROBA~1.LNK   2023-08-16 12:51:14 UTC+0000 2023-08-16 12:51:14 UTC+0000 2023-08-16 12:51:14 UTC+0000 ARC                  Acrobat Reader.lnk
ItemPos800×600×96(1) ANALIS~1       2023-06-16 07:44:46 UTC+0000 2023-06-16 07:44:08 UTC+0000 2023-06-16 07:44:46 UTC+0000 DIR                  Analisis Dinamico
ItemPos800×600×96(1) ANALIS~2       2023-06-16 07:47:10 UTC+0000 2023-06-16 07:44:54 UTC+0000 2023-06-16 07:47:10 UTC+0000 DIR                  Analisis Estatico
ItemPos800×600×96(1) HOTELP~1.PDF   2023-08-16 12:44:06 UTC+0000 2023-08-16 12:44:04 UTC+0000 2023-08-16 12:43:46 UTC+0000 ARC                  hotelpaymentproof-MALWARE.pdf
ItemPos800×600×96(1) MAGNET~1.EXE   2023-08-09 13:14:36 UTC+0000 2023-08-09 13:14:06 UTC+0000 2023-08-09 13:14:02 UTC+0000 ARC                  Magnet ram capture.exe
ItemPos800×600×96(1) NEWTEX~1.TXT   2023-08-16 12:21:04 UTC+0000 2023-08-16 12:20:58 UTC+0000 2023-08-16 12:20:58 UTC+0000 ARC                  New Text Document.txt
**************************************************************************

**************************************************************************
Registry: \??\C:\Users\numis\AppData\Local\Microsoft\Windows\UsrClass.dat
Key: Local Settings\Software\Microsoft\Windows\Shell\BagMRU
Last updated: 2023-08-16 21:36:10 UTC+0000
Value  Mru  Entry Type     GUID                                 GUID Description     Folder IDs
-----  ---  -------------- ------------------------------------ -------------------- ----------
1      4    Folder Entry   26ee0668-a00a-44d7-9371-beb064c98683 {Unknown CSIDL}      EXPLORER, MY_COMPUTER, RECYCLE_BIN, UKNOWN
0      1    Folder Entry   20d04fe0-3aea-1069-a2d8-08002b30309d My Computer          EXPLORER, MY_COMPUTER
3      3    Folder Entry   59031a47-3f72-44a7-89c5-5595fe6b30ee Users                EXPLORER, USERS
2      2    Folder Entry   031e4825-7b94-4dc3-b131-e946b44c8dd5 Libraries            EXPLORER, LIBRARIES
5      7    Folder Entry   323ca680-c24d-4099-b94d-446dd2d7249e Unknown GUID         EXPLORER, MY_GAMES
4      8    Folder Entry   f02c1a0d-be21-4350-88b0-7367fc96ef3c Network             EXPLORER, MY_DOCUMENTS, MY_COMPUTER, NETWORK
```

https://github.com/aguayro @9v@yr0

El último fichero que se ha accedido es un documento en pdf, que está abierto con el adobe reader y está relacionado con un proceso sospechoso con pid 3044 y pid 1956.

Veámos que nos devuelve el plugin malfind

$ volatility -f win7-malware.raw --profile=Win7SP1x64 malfind

```
└─# volatility -f win7-malware.raw --profile=Win7SP1x64 malfind
Volatility Foundation Volatility Framework 2.6
Process: svchost.exe Pid: 800 Address: 0x0d30000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 16, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x00d30000  41 ba 80 00 00 00 48 b8 38 a1 f5 fd fe 07 00 00   A.....H.8.......
0x00d30010  48 ff 20 90 41 ba 81 00 00 00 48 b8 38 a1 f5 fd   H ... A.....H.8 ...
0x00d30020  fe 07 00 00 48 ff 20 90 41 ba 82 00 00 00 48 b8   ....H ... A.....H.
0x00d30030  38 a1 f5 fd fe 07 00 00 48 ff 20 90 41 ba 83 00   8.......H ... A ...
```

Nos detecta varios procesos como sospechosos de tener código malicioso, veamos cuáles son y haremos un volcado de los mismos.

```
└─# cat malfind.txt | grep Process:
Process: svchost.exe Pid: 800 Address: 0x0d30000
Process: svchost.exe Pid: 880 Address: 0xce0000
Process: explorer.exe Pid: 1548 Address: 0x3e90000
Process: explorer.exe Pid: 1548 Address: 0x4590000
Process: svchost.exe Pid: 1880 Address: 0x24d0000
Process: svchost.exe Pid: 1880 Address: 0x4d70000
Process: Magnet ram cap Pid: 3712 Address: 0x4a10000
Process: Magnet ram cap Pid: 3712 Address: 0x4a00000
```

Muestra varios procesos de servicios de red svchost.exe con pid 800, pid 880, pid 1880, además de proceso pid 1548 explorer.exe. Del proceso pid 3712 es una aplicación que use para hacer el volcado de memoria por lo que lo descargamos.

Volcamos los ejecutables al disco para su análisis con pid 800, pid 880 pid 1880 y pir 1548

$ volatility -f win7-malware.raw -p 800,880,1548,1880 --profile=Win7SP1x64 procdump --dump-dir ./

```
└─# volatility -f win7-malware.raw -p 800,880,1548,1880 --profile=Win7SP1x64 procdump --dump-dir ./
Volatility Foundation Volatility Framework 2.6
Process(V)         ImageBase          Name                 Result
------------------ ------------------ -------------------- ------
0xfffffa800515b2d0 0x00000000ff320000 svchost.exe          OK: executable.800.exe
0xfffffa800518f740 0x00000000ff320000 svchost.exe          OK: executable.880.exe
0xfffffa8005557b30 0x00000000ffe20000 explorer.exe         OK: executable.1548.exe
0xfffffa8003890740 0x00000000ff320000 svchost.exe          OK: executable.1880.exe
```

Volcamos los procesos al disco para su análisis con pid 800, pid 880 pid 1880 y pir 1548

$ volatility -f win7-malware.raw -p 800,880,1548,1880 --profile=Win7SP1x64 memdump --dump-dir ./

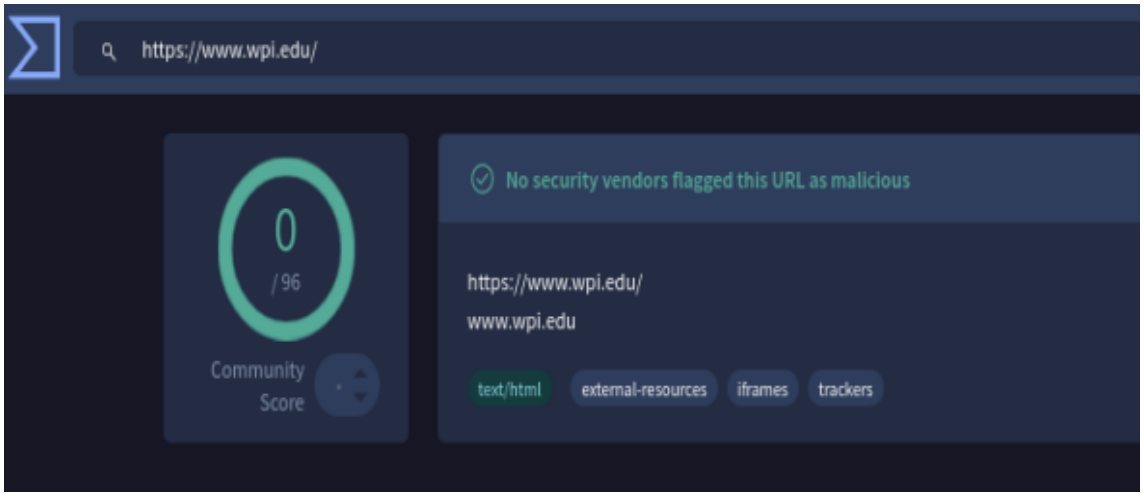
https://github.com/aguayro @9v@yr0

Una vez volcado el contenido de los procesos a disco, veamos que accesos a url o ips contienen los distintos procesos. Veamos primero los pid 800, pid 880.

$ strings 800.dmp | grep '\<www\....\>'

```
└─# strings 800.dmp | grep '\<www\....\>'
www.msn.com
[{"r":[{"f":"^http://(?:www\\.)?wpi\\.edu/","t":"https://www.wpi.edu/"},{"f":"^http://my\\.wpi\\.edu/","t":"https://my.wpi.edu/"}]}]
[{"r":[{"f":"^http://(?:www\\.)?wpi\\.edu/","t":"https://www.wpi.edu/"},{"f":"^http://my\\.wpi\\.edu/","t":"https://my.wpi.edu/"}]}]

┌──(root㉿kali)-[/home/…/Documents/forense/Memoria/case_03]
└─# strings 880.dmp | grep '\<www\....\>'
[{"r":[{"f":"^http://(?:www\\.)?wpi\\.edu/","t":"https://www.wpi.edu/"},{"f":"^http://my\\.wpi\\.edu/","t":"https://my.wpi.edu/"}]}]
[{"r":[{"f":"^http://(?:www\\.)?wpi\\.edu/","t":"https://www.wpi.edu/"},{"f":"^http://my\\.wpi\\.edu/","t":"https://my.wpi.edu/"}]}]
```

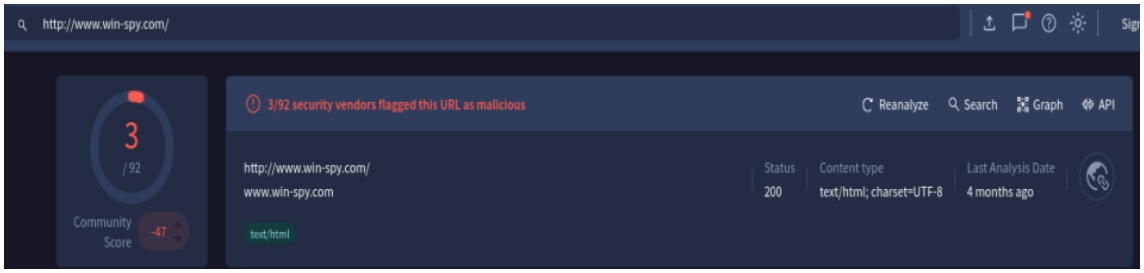


Dicho proceso no tiene nada malisioso, veamos el pid 1880.

$ strings 1880.dmp | grep '\<www\....\>'

```
└─# strings 1880.dmp | grep '\<www\....\>'
https://www.ver
://www.ver
/www.ver
www.a-d-w-a-r-e.com
http://www.now.cn/?SCPMCID=
www.win-spy.com
www.avp.ch
www.avp.ru
```

Parecemos que tenemos algo, nos devuelve muchas url de dominios .ru .br verificamos la url www.win-spy.com en virustotal.com



https://github.com/aguayro @9v@yr0

Vamos a volver a revisar el volcado de memoria correspondiente con el pid 1880.
En el listado de url, hay una que me llama la atención pues para que ejecuta algún código en php

```
└─# strings 1880.dmp | grep 'www\.131377\.com' -B 10
pD|T
]JS!V&
baiduba.DLL
C:\WINDOWS\system32\ieset.ini
refurl=
exid=
regURL=
seo=
smsid=
=aiyu
www.131377.com?accect
asiafind.com/go/g
shop.7cv.com/index.php?asstfrom=
cnt.zhaopin.com/Market/whole_counter.jsp?sid=
f=http://www.netxboy.com/
http://go.58.com/?f=
http://www.now.cn/?SCPMCID=
www.joyo.com/default.asp?source=ad4all
union.99jk.com/xf200/click.asp?u=1&uname=
www.131377.com?accect=
```

Todas las url que contiene dicha strings los cataloga como malware.

Vamos a ver los ficheros que hay en en equipo a ver si encontramos algo anómalo, la llamada a un dominio .cn me hace sospechar sobre algún malware de dicho origen.

$ volatility -f win7-malware.raw --profile=Win7SP1x64 filescan

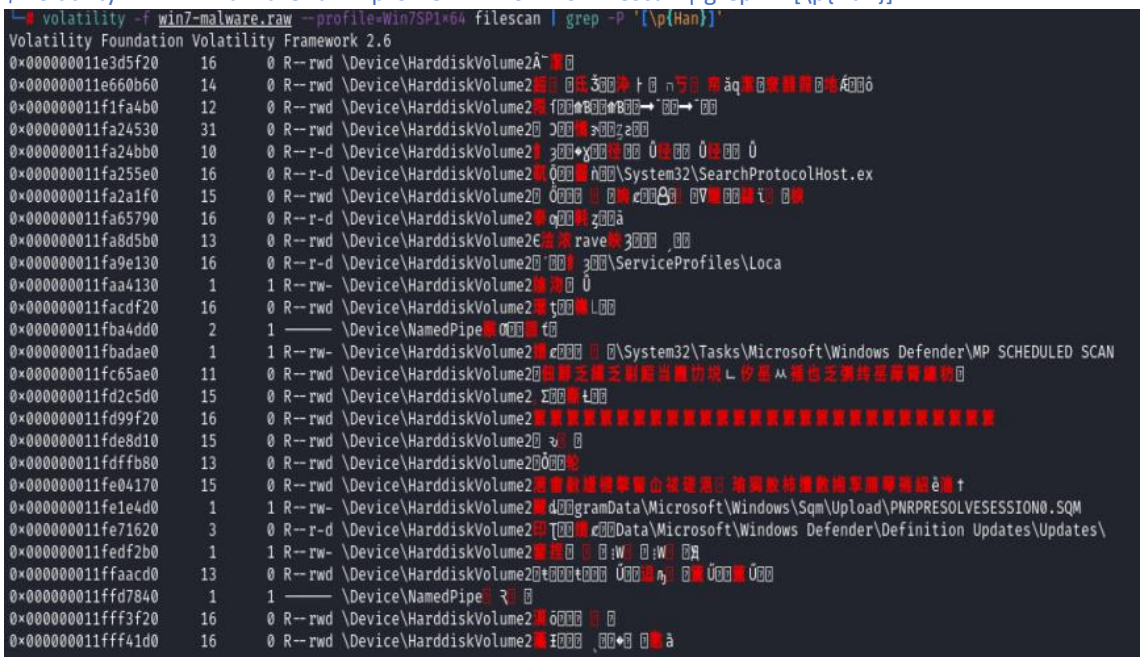
```
└─# volatility -f win7-malware.raw --profile=Win7SP1x64 filescan
Volatility Foundation Volatility Framework 2.6
Offset(P)          #Ptr   #Hnd Access Name
------------------ ------ ------ ------ ----

0x000000000706f330     16      0 RW---- \Device\HarddiskVolume2\Windows\AppCompat\Programs\RecentFileCache.bcf
0x000000000706f500     16      0 R--r-d \Device\HarddiskVolume2\Windows\SysWOW64\tzres.dll
0x000000000706f650     11      0 R--r-d \Device\HarddiskVolume2\Windows\System32\notepad.exe
0x000000000706f7a0     18      0 RW-rwd \Device\HarddiskVolume2\$Directory
0x000000000706f8f0     12      0 R--r-d \Device\HarddiskVolume2\Windows\SysWOW64\api-ms-win-crt-runtime-l1-1-0.dll
0x000000000708c070      8      0 R--r-d \Device\HarddiskVolume2\Windows\System32\negoexts.dll
0x0000000070d15e0     15      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Sens.dll
```

ANÁLISIS FORENSE MEMORIA WINDOWS 7 CASO 03

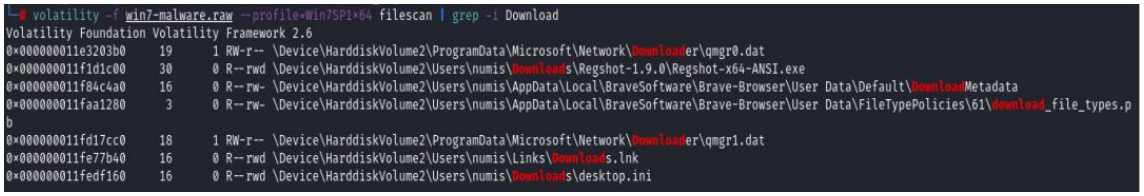
https://github.com/aguayro @9v@yr0

$ volatility -f win7-malware.raw --profile=Win7SP1x64 filescan | grep -P '[\p{Han}]'



Veamos que ficheros se hayan descargado

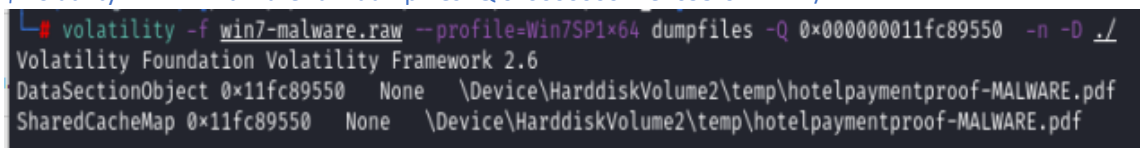
$ volatility -f win7-malware.raw --profile=Win7SP1x64 filescan | grep -i Download



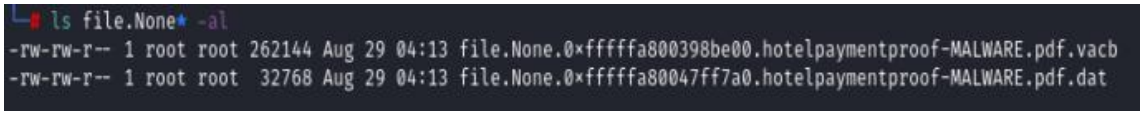
Vuelco los ficheros a disco para analizarlos, pero no veo nada anormal en ellos.

Descargamos el fichero pdf hotelpaymentproof-MALWARE.pdf

$ volatility -f win7-malware.raw dumpfiles -Q 0x000000011e2695f0 -n -D ./



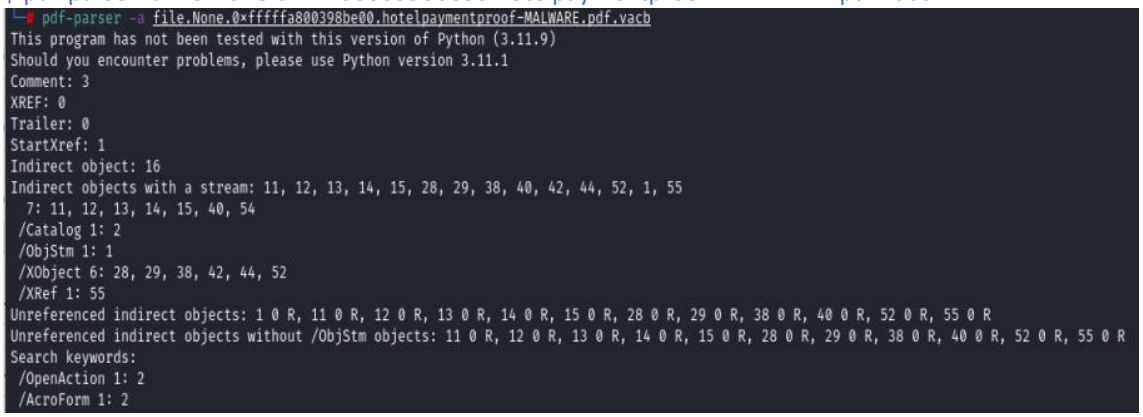
El volcado nos ha generado dos ficheros:



https://github.com/aguayro @9v@yr0

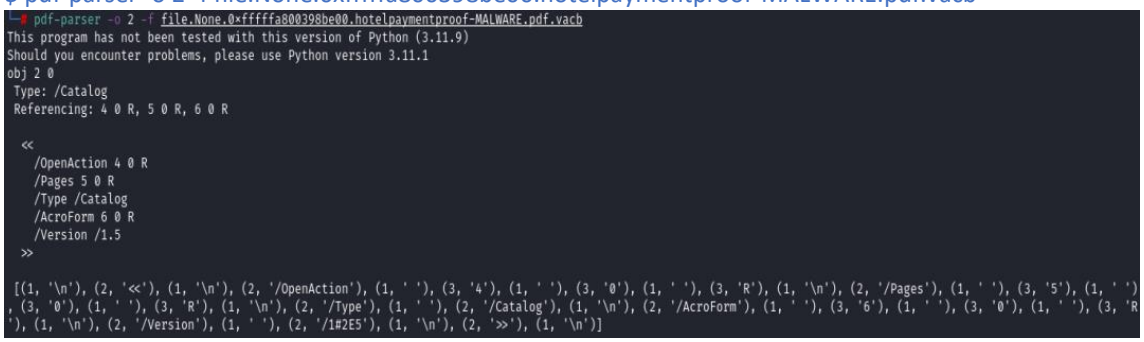
Analizamos el pdf

$ pdf-parser -a file.None.0xfffffa800398be00.hotelpaymentproof-MALWARE.pdf.vacb



La estructura nos indica que ha una acción OpenAction en el objeto 2, veámos que contiene.

$ pdf-parser -o 2 -f file.None.0xfffffa800398be00.hotelpaymentproof-MALWARE.pdf.vacb



El estudio del pdf se encuentra en otro documento en el que me encuentro trabajando.

Software:

Volatility 2

Pdf-parser