

STUXNET - ANÁLISIS DE MALWARE

Vamos a analizar un volcado de memoria RAM de un equipo infectado por **Stuxnet**, y para ello se hará uso de la herramienta **Volatility**.

STUXNET

Disponemos del volcado de la memoria RAM situado en el archivo stuxnet.vmem.

Sacamos la información del perfil del sistema:

```
kali@kali:~/Desktop/volatility-master/volatility-master$ python vol.py -f stuxnet.vmem imageinfo
Volatility Foundation Volatility Framework 2.6.1
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/kali/Desktop/volatility-master/volatility-master/stuxnet.vmem)
      PAE type : PAE
      DTB : 0x319000L
      KDBG : 0x80545ae0L
      Number of Processors : 1
      Image Type (Service Pack) : 3
      KPCR for CPU 0 : 0xffdff000L
      KUSER_SHARED_DATA : 0xffdf0000L
      Image date and time : 2011-06-03 04:31:36 UTC+0000
      Image local date and time : 2011-06-03 00:31:36 -0400
```

Podemos comprobar que el perfil que estamos analizando pertenece a WinXPSP3x86 y el huso horario es de -0400.

Ahora observamos los procesos activos:

```
kali@kali:~/Desktop/volatility-master/volatility-master$ python vol.py -f stuxnet.vmem --profile=WinXPSP3x86 pslist
Volatility Foundation Volatility Framework 2.6.1
Offset(V)  Name                PID  PPID  Thds  Hnds  Sess  Wow64  Start                Exit
-----
0x823c8830 System                4    0    59   403  -----  0
0x820df020 smss.exe       376   4    3    19  -----  0  2010-10-29 17:08:53 UTC+0000
0x821a2da0 csrss.exe       600  376   11   395  0        0  2010-10-29 17:08:54 UTC+0000
0x81da5650 winlogon.exe    624  376   19   570  0        0  2010-10-29 17:08:54 UTC+0000
0x82073020 services.exe   668  624   21   431  0        0  2010-10-29 17:08:54 UTC+0000
0x81e70020 lsass.exe       680  624   19   342  0        0  2010-10-29 17:08:54 UTC+0000
0x823315d8 vmacthlp.exe    844  668    1    25  0        0  2010-10-29 17:08:55 UTC+0000
0x81db8da0 svchost.exe   856  668   17   193  0        0  2010-10-29 17:08:55 UTC+0000
0x81e61da0 svchost.exe   940  668   13   312  0        0  2010-10-29 17:08:55 UTC+0000
0x822843e8 svchost.exe  1032 668   61  1169  0        0  2010-10-29 17:08:55 UTC+0000
0x81e18b28 svchost.exe  1080 668    5    80  0        0  2010-10-29 17:08:55 UTC+0000
0x81ff7020 svchost.exe  1200 668   14   197  0        0  2010-10-29 17:08:55 UTC+0000
0x81fee8b0 spoolsv.exe   1412 668   10   118  0        0  2010-10-29 17:08:56 UTC+0000
0x81e0eda0 jqs.exe       1580 668    5   148  0        0  2010-10-29 17:09:05 UTC+0000
0x81fe52d0 vmtoolsd.exe   1664 668    5   284  0        0  2010-10-29 17:09:05 UTC+0000
0x821a0568 VMUpgradeHelper 1816 668    3    96  0        0  2010-10-29 17:09:08 UTC+0000
0x8205ada0 alg.exe       188  668    6   107  0        0  2010-10-29 17:09:09 UTC+0000
0x820ec7e8 explorer.exe  1196 1728   16   582  0        0  2010-10-29 17:11:49 UTC+0000
0x820ecc10 wscntfy.exe    2040 1032    1    28  0        0  2010-10-29 17:11:49 UTC+0000
0x81e86978 TSVNCache.exe   324  1196    7    54  0        0  2010-10-29 17:11:49 UTC+0000
0x81fc5da0 VMwareTray.exe 1912 1196    1    50  0        0  2010-10-29 17:11:50 UTC+0000
0x81e6b660 VMwareUser.exe 1356 1196    9   251  0        0  2010-10-29 17:11:50 UTC+0000
0x8210d478 jusched.exe    1712 1196    1    26  0        0  2010-10-29 17:11:50 UTC+0000
0x82279998 imapi.exe      756  668    4   116  0        0  2010-10-29 17:11:54 UTC+0000
0x822b9a10 wuauclt.exe    976  1032    3   133  0        0  2010-10-29 17:12:03 UTC+0000
0x81c543a0 Procmon.exe   660  1196   13   189  0        0  2011-06-03 04:25:56 UTC+0000
0x81fa5390 wmiprivse.exe  1872 856    5   134  0        0  2011-06-03 04:25:58 UTC+0000
0x81c498c8 lsass.exe       868  668    2    23  0        0  2011-06-03 04:26:55 UTC+0000
0x81c47c00 lsass.exe     1928 668    4    65  0        0  2011-06-03 04:26:55 UTC+0000
0x81c0cda0 cmd.exe        968  1664    0  -----  0  2011-06-03 04:31:35 UTC+0000 2011-06-03 04:31:36 UTC+0000
0x81f14938 ipconfig.exe   304  968    0  -----  0  2011-06-03 04:31:35 UTC+0000 2011-06-03 04:31:36 UTC+0000
```

A simple vista no hay nada que llame notablemente la atención. Así que pasamos a analizar las conexiones de red:

```
kali@kali:~/Desktop/volatility-master/volatility-master$ python vol.py -f stuxnet.vmem --profile=WinXPSP3x86 connections
Volatility Foundation Volatility Framework 2.6.1
Offset(V)  Local Address          Remote Address          Pid
-----
kali@kali:~/Desktop/volatility-master/volatility-master$ python vol.py -f stuxnet.vmem --profile=WinXPSP3x86 connscan
Volatility Foundation Volatility Framework 2.6.1
Offset(P)  Local Address          Remote Address          Pid
-----
```

Parece que tampoco hay nada por esta parte. Así que vamos a utilizar la funcionalidad malfind de Volatility la cual busca código malicioso dentro de los procesos:

```
kali@kali:~/Desktop/volatility-master/volatility-master$ python vol.py -f stuxnet.vmem --profile=WinXPSP3x86 malfind -D malfind/stuxnet/
Volatility Foundation Volatility Framework 2.6.1
Process: csrss.exe Pid: 600 Address: 0x7f6f0000
Vad Tag: Vad Protection: PAGE_EXECUTE_READWRITE
Flags: Protection: 6

0x7f6f0000 c8 00 00 00 1f 01 00 00 ff ee ff ee 08 70 00 00 .....p..
0x7f6f0010 08 00 00 00 00 fe 00 00 00 10 00 00 20 00 00 .....
0x7f6f0020 00 02 00 00 00 20 00 00 8d 01 00 00 ff ef fd 7f .....
0x7f6f0030 03 00 08 06 00 00 00 00 00 00 00 00 00 00 00 .....

0x7f6f0000 c8000000      ENTER 0x0, 0x0
0x7f6f0004 1f          POP DS
0x7f6f0005 0100      ADD [EAX], EAX
0x7f6f0007 00ff      ADD BH, BH
```

De aquí obtenemos un listado de procesos con contenido detectado como malicioso, que son csrss.exe, services.exe, svchost.exe, explorer.exe y dos procesos de lsass.exe, tanto el 868 como el 1928, aunque este último aparece en más ocasiones. También nos devuelve los correspondientes volcados de memoria, que podemos analizar con el comando file:

```
kali@kali:~/Desktop/volatility-master/volatility-master/malfind/stuxnet$ file *
process.0x81c47c00.0x1000000.dmp: PE32 executable (GUI) Intel 80386, for MS Windows
process.0x81c47c00.0x680000.dmp: data
process.0x81c47c00.0x6f0000.dmp: data
process.0x81c47c00.0x800000.dmp: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows, UPX compressed
process.0x81c47c00.0x870000.dmp: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows, UPX compressed
process.0x81c498c8.0x1000000.dmp: PE32 executable (GUI) Intel 80386, for MS Windows
process.0x81c498c8.0x800000.dmp: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows, UPX compressed
process.0x81e61da0.0xb70000.dmp: data
process.0x81e61da0.0xbf0000.dmp: data
process.0x81e61da0.0xd00000.dmp: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows, UPX compressed
process.0x82073020.0x13f0000.dmp: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows, UPX compressed
process.0x82073020.0x940000.dmp: data
process.0x820ec7e8.0x2550000.dmp: data
process.0x821a2da0.0x7f6f0000.dmp: data
```

Podemos ver que algunos ficheros mencionan UPX compressed, una técnica habitual de empaquetado de malware. Ahora habría que analizar a través de VirusTotal la información obtenida. Por ejemplo, vamos a sacar el MD5 de uno de los volcados que “file” nos indica que ha sido comprimido con UPX:

```
kali@kali:~/Desktop/volatility-master/volatility-master/malfind/stuxnet$ md5sum process.0x81c47c00.0x800000.dmp
7cbdefe442a13e7fa7931e165e82e6f1 process.0x81c47c00.0x800000.dmp
```

59

/ 71

Community Score

59 engines detected this file

2b2945f7cc7cf5b30ccdf37e2adbb236594208e409133bcd56f5777c009ffe6d
process.0x81c47c00.0x800000.dmp

488.00 KB
Size

2020-03-23 09:46:42 UTC
2 months ago

DLL

DETECTION	DETAILS	COMMUNITY
Ad-Aware	Win32.Worm.Stuxnet.D	AegisLab
AhnLab-V3	Worm/Win32.Stuxnet.R124086	Alibaba
ALYac	Win32.Worm.Stuxnet.D	Antiy-AVL
SecureAge APEX	Malicious	Arcabit
Avast	FileRep/Malware	AVG
Avira (no cloud)	WORM/Stuxnet.A.7	BitDefender
BitDefenderTheta	Gen:NN.ZedlaF.34100.EmPfauCpyygi	Bkav
CAT-QuickHeal	Worm.Stuxnet.B4	ClamAV
CMC	Worm.Win32.Stuxnet.O	Comodo
CrowdStrike Falcon	Win/malicious_confidence_70% (D)	Cylance
Cyren	W32/Risk.CKEZ-6474	DrWeb

Podemos observar que al meter el MD5 en VirusTotal este nos lo detecta como malware en 59 de las 71 herramientas, y muchas de ellas nos informa de que se trata del Stuxnet.

Ahora ya conocemos los procesos implicados. Podemos volver a ver la lista de procesos para analizar por otro camino alguno de estos procesos. Usamos pstree:

```
kali@kali:~/Desktop/volatility-master/volatility-master$ python vol.py -f stuxnet.vmem --profile=WinXPSP3x86 pstree
Volatility Foundation Volatility Framework 2.6.1
Name                               Pid  PPid  Thds  Hnds Time
-----
0x823c8830:System                   4     0    59   403 1970-01-01 00:00:00 UTC+0000
. 0x820df020:smss.exe               376    4     3    19 2010-10-29 17:08:53 UTC+0000
.. 0x821a2da0:csrss.exe             600   376    11   395 2010-10-29 17:08:54 UTC+0000
... 0x81da5650:winlogon.exe          624   376    19   570 2010-10-29 17:08:54 UTC+0000
.... 0x82073020:services.exe         668   624    21   431 2010-10-29 17:08:54 UTC+0000
..... 0x81fe52d0:vmtoolsd.exe         1664   668     5    284 2010-10-29 17:09:05 UTC+0000
..... 0x81c0cda0:cmd.exe               968   1664    0 ----- 2011-06-03 04:31:35 UTC+0000
..... 0x81f14938:ipconfig.exe          304   968    0 ----- 2011-06-03 04:31:35 UTC+0000
..... 0x822843e8:svchost.exe           1032   668    61  1169 2010-10-29 17:08:55 UTC+0000
..... 0x822b9a10:wuaucflt.exe          976   1032     3    133 2010-10-29 17:12:03 UTC+0000
..... 0x820ecc10:wscntfy.exe           2040  1032     1     28 2010-10-29 17:11:49 UTC+0000
..... 0x81e61da0:svchost.exe           940   668    13    312 2010-10-29 17:08:55 UTC+0000
..... 0x81db8da0:svchost.exe            856   668    17    193 2010-10-29 17:08:55 UTC+0000
..... 0x81fa5390:wmiprvse.exe          1872   856     5    134 2011-06-03 04:25:58 UTC+0000
..... 0x821a0568:VMUpgradeHelper       1816   668     3     96 2010-10-29 17:09:08 UTC+0000
..... 0x81fee8b0:spoolsv.exe           1412   668    10    118 2010-10-29 17:08:56 UTC+0000
..... 0x81ff7020:svchost.exe           1200   668    14    197 2010-10-29 17:08:55 UTC+0000
..... 0x81c47c00:lsass.exe             1928   668     4     65 2011-06-03 04:26:55 UTC+0000
..... 0x81e18b28:svchost.exe           1080   668     5     80 2010-10-29 17:08:55 UTC+0000
..... 0x8205ada0:alg.exe                188   668     6    107 2010-10-29 17:09:09 UTC+0000
..... 0x823315d8:vmacthlp.exe          844   668     1     25 2010-10-29 17:08:55 UTC+0000
..... 0x81e0eda0:jqc.exe               1580   668     5    148 2010-10-29 17:09:05 UTC+0000
..... 0x81c498c8:lsass.exe             868   668     2     23 2011-06-03 04:26:55 UTC+0000
..... 0x82279998:imapi.exe             756   668     4    116 2010-10-29 17:11:54 UTC+0000
..... 0x81e70020:lsass.exe             680   624    19    342 2010-10-29 17:08:54 UTC+0000
..... 0x820ec7e8:explorer.exe          1196  1728    16    582 2010-10-29 17:11:49 UTC+0000
..... 0x81c543a0:Procmon.exe            660  1196    13    189 2011-06-03 04:25:56 UTC+0000
..... 0x81e86978:TSVNCache.exe          324  1196     7     54 2010-10-29 17:11:49 UTC+0000
..... 0x81e6b660:VMwareUser.exe        1356  1196     9    251 2010-10-29 17:11:50 UTC+0000
..... 0x8210d478:jusched.exe           1712  1196     1     26 2010-10-29 17:11:50 UTC+0000
..... 0x81fc5da0:VMwareTray.exe         1912  1196     1     50 2010-10-29 17:11:50 UTC+0000
```

Vamos a analizar, por ejemplo, el proceso lsass.exe que ya nos informó el malfind sobre él. El pid del lsass que vamos a analizar es 1928 y su proceso padre es el 668 services.exe, que también fue notificado por malfind.

Lo primero que vamos a hacer es un dlllist sobre ambos procesos:

```
kali@kali:~/Desktop/volatility-master/volatility-master$ python vol.py -f stuxnet.vmem --profile=WinXPSP3x86 dlllist -p1928,668
Volatility Foundation Volatility Framework 2.6.1
*****
services.exe pid: 668
Command line : C:\WINDOWS\system32\services.exe
Service Pack 3
```

Base	Size	LoadCount	LoadTime	Path
0x01000000	0x1c000	0xffff		C:\WINDOWS\system32\services.exe
0x7c900000	0xaf000	0xffff		C:\WINDOWS\system32\ntdll.dll
0x7c800000	0xf6000	0xffff		C:\WINDOWS\system32\kernel32.dll
0x77dd0000	0x9b000	0xffff		C:\WINDOWS\system32\ADVAPI32.dll
0x77e70000	0x92000	0xffff		C:\WINDOWS\system32\RPCRT4.dll
0x77fe0000	0x11000	0xffff		C:\WINDOWS\system32\Secur32.dll
0x77c10000	0x58000	0xffff		C:\WINDOWS\system32\msvcrt.dll
0x5f770000	0xc000	0xffff		C:\WINDOWS\system32\NCOBJAPI.DLL
0x76080000	0x65000	0xffff		C:\WINDOWS\system32\MSVCP60.dll
0x7dbd0000	0x51000	0xffff		C:\WINDOWS\system32\SCESRV.dll
0x776c0000	0x12000	0xffff		C:\WINDOWS\system32\AUTHZ.dll
0x7e410000	0x91000	0xffff		C:\WINDOWS\system32\USER32.dll
0x77f10000	0x49000	0xffff		C:\WINDOWS\system32\GDI32.dll
0x769c0000	0xb4000	0xffff		C:\WINDOWS\system32\USERENV.dll
0x7dba0000	0x21000	0xffff		C:\WINDOWS\system32\umpnpmgr.dll
0x76360000	0x10000	0xffff		C:\WINDOWS\system32\WINSTA.dll
0x5b860000	0x55000	0xffff		C:\WINDOWS\system32\NETAPI32.dll
0x5cb70000	0x26000	0x1		C:\WINDOWS\system32\ShimEng.dll
0x47260000	0xf000	0x1		C:\WINDOWS\AppPatch\AcAdProc.dll
0x77b40000	0x22000	0x2		C:\WINDOWS\system32\Apphelp.dll
0x77c00000	0x8000	0x4		C:\WINDOWS\system32\VERSION.dll
0x77b70000	0x11000	0x1		C:\WINDOWS\system32\eventlog.dll
0x76bf0000	0xb000	0x3		C:\WINDOWS\system32\PSAPI.DLL
0x71ab0000	0x17000	0xb		C:\WINDOWS\system32\WS2_32.dll
0x71aa0000	0x8000	0x9		C:\WINDOWS\system32\WS2HELP.dll
0x76f50000	0x8000	0x1		C:\WINDOWS\system32\wtsapi32.dll
0x76c30000	0x2e000	0x1		C:\WINDOWS\system32\WINTRUST.dll
0x77a80000	0x95000	0x4		C:\WINDOWS\system32\CRYPT32.dll
0x77b20000	0x12000	0x5		C:\WINDOWS\system32\MSASN1.dll
0x76c90000	0x28000	0x2		C:\WINDOWS\system32\IMAGEHLP.dll
0x01020000	0x2c5000	0x1		C:\WINDOWS\system32\xpssp2res.dll
0x68000000	0x36000	0x1		C:\WINDOWS\system32\rsaenh.dll
0x5ad70000	0x38000	0x2		C:\WINDOWS\system32\uxtheme.dll
0x75150000	0x13000	0x1		C:\WINDOWS\system32\Cabinet.dll
0x774e0000	0x13d000	0x6		C:\WINDOWS\system32\ole32.dll
0x013f0000	0x138000	0x1		C:\WINDOWS\system32\KERNEL32.DLL.ASLR.0360c5e2

```
0x76f20000 0x27000 0x2 C:\WINDOWS\system32\DNSAPI.dll
0x76d60000 0x19000 0x2 C:\WINDOWS\system32\IPHLPAPI.DLL
0x77120000 0x8b000 0x4 C:\WINDOWS\system32\OLEAUT32.dll
0x7c9c0000 0x817000 0x2 C:\WINDOWS\system32\SHELL32.dll
0x77f60000 0x76000 0x8 C:\WINDOWS\system32\SHLWAPI.dll
0x771b0000 0xaa800 0x2 C:\WINDOWS\system32\WININET.dll
0x71ad0000 0x9000 0x2 C:\WINDOWS\system32\WSOCK32.dll
0x773d0000 0x103000 0x2 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
0x5d090000 0x9a000 0x1 C:\WINDOWS\system32\comctl32.dll
*****
lsass.exe pid: 1928
Command line : "C:\WINDOWS\system32\lsass.exe"
Service Pack 3
```

Base	Size	LoadCount	LoadTime	Path
0x01000000	0x6000	0xffff		C:\WINDOWS\system32\lsass.exe
0x7c900000	0xaf000	0xffff		C:\WINDOWS\system32\ntdll.dll
0x7c800000	0xf6000	0xffff		C:\WINDOWS\system32\kernel32.dll
0x77dd0000	0x9b000	0xffff		C:\WINDOWS\system32\ADVAPI32.dll
0x77e70000	0x92000	0xffff		C:\WINDOWS\system32\RPCRT4.dll
0x77fe0000	0x11000	0xffff		C:\WINDOWS\system32\Secur32.dll
0x77c10000	0x58000	0xffff		C:\WINDOWS\system32\USER32.dll
0x77f10000	0x49000	0xffff		C:\WINDOWS\system32\GDI32.dll
0x00870000	0x138000	0x1		C:\WINDOWS\system32\KERNEL32.DLL.ASLR.0360b7ab
0x76f20000	0x27000	0x2		C:\WINDOWS\system32\DNSAPI.dll
0x77120000	0x8b000	0x27		C:\WINDOWS\system32\msvcrt.dll
0x71ab0000	0x17000	0xa		C:\WINDOWS\system32\WS2_32.dll
0x71aa0000	0x8000	0x8		C:\WINDOWS\system32\WS2HELP.dll
0x76d60000	0x19000	0x2		C:\WINDOWS\system32\IPHLPAPI.DLL
0x5b860000	0x55000	0x2		C:\WINDOWS\system32\NETAPI32.dll
0x774e0000	0x13d000	0x5		C:\WINDOWS\system32\ole32.dll
0x77120000	0x8b000	0x4		C:\WINDOWS\system32\OLEAUT32.dll
0x76bf0000	0xb000	0x2		C:\WINDOWS\system32\PSAPI.DLL
0x7c9c0000	0x817000	0x2		C:\WINDOWS\system32\SHELL32.dll
0x77f60000	0x76000	0x8		C:\WINDOWS\system32\SHLWAPI.dll
0x769c0000	0xb4000	0x2		C:\WINDOWS\system32\USERENV.dll
0x77c00000	0x8000	0x2		C:\WINDOWS\system32\VERSION.dll
0x771b0000	0xaa800	0x2		C:\WINDOWS\system32\WININET.dll
0x77a80000	0x95000	0x2		C:\WINDOWS\system32\CRYPT32.dll
0x77b20000	0x12000	0x2		C:\WINDOWS\system32\MSASN1.dll
0x71ad0000	0x9000	0x2		C:\WINDOWS\system32\WSOCK32.dll
0x773d0000	0x103000	0x2		C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
0x5d090000	0x9a000	0x1		C:\WINDOWS\system32\comctl32.dll

Lo que más llama la atención es el “command line” del proceso lsass.exe, el cual está entre comillas y la ruta utiliza doble barra vertical en lugar una barra simple como suele ser lo habitual.

Ahora entramos en los handles de este proceso:

```
kali@kali:~/Desktop/volatility-master/volatility-master$ python vol.py -f stuxnet.vmem --profile=WinXPSP3x86 handles -p 1928 -t Key,Mutant,File,Event
Volatility Foundation Volatility Framework 2.6.1
-----
Offset(V)      Pid      Handle      Access Type      Details
-----
0x8225b710    1928     0xc         0x100020 File           \Device\HarddiskVolume1\WINDOWS\system32
0x81be6390    1928     0x700       0x1f0003 Event          WkssvcShutdownEvent2
0x81f5f398    1928     0x70c       0x1f0003 Event
0x81f60278    1928     0x714       0x1f0003 Event
0x81fc3c08    1928     0x71c       0x1f0001 Mutant          {5EC1718B-F130-4a19-B782-B6E655E091B2}
0x81c72958    1928     0x720       0x1f0003 Event
0x81f40288    1928     0x724       0x1f0003 Event          {CAA68D26-6C78-4af0-95E2-53DE46FDDF26}
0x81f64390    1928     0x728       0x1f0001 Mutant
0x81f63b78    1928     0x72c       0x1f0001 Mutant
0x81f8ce08    1928     0x734       0x1f0001 Mutant
0x81f8ce08    1928     0x738       0x1f0001 Mutant
0x81f9d2b0    1928     0x73c       0x1f0001 Mutant
0x81f90490    1928     0x740       0x1f0001 Mutant
0x81f9cc00    1928     0x744       0x1f0001 Mutant
0x81c685d8    1928     0x748       0x1f0001 Mutant
0x821318d0    1928     0x74c       0x1f0001 Mutant
0x81fa2b08    1928     0x750       0x1f0001 Mutant
0x81ea9340    1928     0x754       0x1f0001 Mutant
0xe247ece8    1928     0x758       0x2001f Key           USER\DEFAULT\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS
0x82062740    1928     0x75c       0x100020 File           \Device\HarddiskVolume1\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
0xe2b40830    1928     0x760       0x20f003f Key           USER\DEFAULT
0x82259f68    1928     0x764       0x1f0003 Event          crypt32LogoffEvent
0x82103138    1928     0x768       0x100020 File           \Device\HarddiskVolume1\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
0x8209a5a0    1928     0x76c       0x1f0003 Event          userenv: User Profile setup event
0x81c79fa0    1928     0x774       0x21f0003 Event
0x81eb8d98    1928     0x77c       0x100001 File           \Device\KsecDD
0xe1a61bf8    1928     0x780       0x20019 Key           MACHINE\SYSTEM\CONTROLSET001\SERVICES\NETBT\PARAMETERS
0xe273ec00    1928     0x784       0x20019 Key           MACHINE\SYSTEM\CONTROLSET001\SERVICES\NETBT\PARAMETERS\INTERFACES
0xe2b3e830    1928     0x788       0x20019 Key           MACHINE\SYSTEM\CONTROLSET001\SERVICES\TCP\PARAMETERS
0xe1edf4f8    1928     0x78c       0x20019 Key           MACHINE\SYSTEM\CONTROLSET001\SERVICES\TCP\LINKAGE
0x82136208    1928     0x798       0x1200a0 File           \Device\Ip
0x81f0d730    1928     0x79c       0x100003 File           \Device\Ip
0x81f8e870    1928     0x7a0       0x1200a0 File           \Device\Ip
0x82215128    1928     0x7a4       0x120116 File           \Device\Tcp
0x81f40308    1928     0x7a8       0x1200a0 File           \Device\Tcp
0x81dba3e0    1928     0x7bc       0x1f0003 Event
0x820ee060    1928     0x7c0       0x1f0003 Event
0x81ee4d08    1928     0x7c4       0x1f0003 Event
0x81dbbe58    1928     0x7c8       0x1f0003 Event
0x81c0f8c8    1928     0x7e0       0x21f0003 Event
0xe131c020    1928     0x7e4       0x20f003f Key           MACHINE
```

Vemos que cuenta con secciones críticas y zonas de exclusión mutua. También nos fijamos en algunos eventos, como WkssvcShutdownEvent2, y en los múltiples ficheros relacionados que tiene.

Lo siguiente que podemos hacer, por ejemplo, es un filescan buscando ficheros lsass:

```
kali@kali:~/Desktop/volatility-master/volatility-master$ python vol.py -f stuxnet.vmem --profile=WinXPSP3x86 filescan | grep lsass
Volatility Foundation Volatility Framework 2.6.1
0x00000000001e26d20 2 1 ----- \Device\NamedPipe\lsass
0x00000000002142770 2 1 ----- \Device\NamedPipe\lsass
0x0000000000214b1c8 1 1 ----- \Device\NamedPipe\lsass
0x0000000000218a5e8 2 1 ----- \Device\NamedPipe\lsass
0x00000000002430120 1 0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\lsass.exe
0x000000000024813b0 1 0 R--r-- \Device\HarddiskVolume1\WINDOWS\system32\lsass.exe
```

De aquí tenemos dos .exe que podemos seleccionar, por lo que le hacemos a uno de ellos un dumpfiles lo cual nos genera un par de archivos, uno img y otro dat:

```
kali@kali:~/Desktop/volatility-master/volatility-master$ python vol.py -f stuxnet.vmem --profile=WinXPSP3x86 dumpfiles -Q 0x00000000002430120 -D dumpfiles/stuxnet/
Volatility Foundation Volatility Framework 2.6.1
ImageSectionObject 0x02430120 None \Device\HarddiskVolume1\WINDOWS\system32\lsass.exe
DataSectionObject 0x02430120 None \Device\HarddiskVolume1\WINDOWS\system32\lsass.exe
```

Le calculamos el MD5:

```
kali@kali:~/Desktop/volatility-master/volatility-master/dumpfiles/stuxnet$ md5sum *
0a7386a5a3d94a9e9e9aece3e50516dc file.None.0x820de4f8.dat
33b0c8ae90fea91eabbbbc72ec8721bd2 file.None.0x823e4008.img
```

Y comprobamos qué ocurre en VirusTotal al subir el archivo .img:

4 / 68

Community Score

4 engines detected this file

2fa0b6faa8ae56044143bd81255355bbe6ada7b92e312bc95019321e6f728cbc
lsass.exe

14.00 KB
Size

2018-11-07 09:17:09 UTC
1 year ago

EXE

overlay

peexe

DETECTION	DETAILS	BEHAVIOR	COMMUNITY
CrowdStrike Falcon	Malicious_confidence_60% (W)	Cybereason	Malicious.847055
Cylance	Unsafe	SentinelOne (Static ML)	Static Engine - Malicious
Ad-Aware	Undetected	AegisLab	Undetected
AhnLab-V3	Undetected	Alibaba	Undetected

Podemos ver que este archivo es detectado como malware por 4 de 68 herramientas.

Otra tarea que podemos realizar es hacer un memdump de este proceso y de su proceso padre:

```
kali@kali:~/Desktop/volatility-master/volatility-master$ python vol.py -f stuxnet.vmem --profile=WinXPSP3x86 memdump -p1928,668 -D memdumps/stuxnet/
Volatility Foundation Volatility Framework 2.6.1
*****
Writing services.exe [ 668] to 668.dmp
*****
Writing lsass.exe [ 1928] to 1928.dmp
```

Ambos procesos podríamos analizarlo con strings, por ejemplo si analizamos el lsass.exe podemos encontrar una línea que parece una consulta en las que incluye un uid (WinCCConnect) y un pwd (2WSXcder):

[illegible]

Pero vamos a sacar los MD5 de cada volcado:

```
kali@kali:~/Desktop/volatility-master/volatility-master/memdumps/stuxnet$ md5sum *
d055737a7efa7d4fe0002aa4c5451db0  1928.dmp
0b74df5001b98b16646f6812bfa3b903  668.dmp
```

Y comprobar los resultados que nos devuelve VirusTotal:

2

/ 57

Community Score

① 2 engines detected this file

4e52a84df989d76186506b4727304ccdd2c0a98e75494cabd8ef164a328bff20

1928.dmp

130.60 MB

Size

2019-04-11 06:36:44 UTC

1 year ago

🔄

🔍

📄

DETECTION	DETAILS	COMMUNITY
Avast	① Win32:Small-HTML [Trj]	AVG ① Win32:Small-HTML [Trj]
Ad-Aware	✓ Undetected	AegisLab ✓ Undetected
AhnLab-V3	✓ Undetected	ALYac ✓ Undetected
Antiy-AVL	✓ Undetected	Arcabit ✓ Undetected
Avast-Mobile	✓ Undetected	Avira (no cloud) ✓ Undetected
Babable	✓ Undetected	Baidu ✓ Undetected
BitDefender	✓ Undetected	Bkav ✓ Undetected
CAT-QuickHeal	✓ Undetected	ClamAV ✓ Undetected
CMC	✓ Undetected	Comodo ✓ Undetected
Cyren	✓ Undetected	DrWeb ✓ Undetected

El proceso lsass.exe es detectado como malware por 2 herramientas (Avast y AVG).

2

/ 57

2 engines detected this file

dfd4b02e2423c6961a790d371c115910558112f104325545932e7ba07615596

668.dmp

132.99 MB

Size

2019-03-21 18:43:31 UTC

1 year ago

Community Score

DETECTION	DETAILS	COMMUNITY
Avast	Win32-Smail-HTMLB [Trj]	AVG
Ad-Aware	Undetected	AegisLab
AhnLab-V3	Undetected	ALYac
Antiy-AVL	Undetected	Arcabit

Y exactamente lo mismo ocurre con el proceso padre, el services.exe.

Y para finalizar vamos a sacar la línea temporal de procesos. Para ello sacamos con el Volatility el timeliner, el mftparser y el shellbags. Y posteriormente unimos todo en un único fichero:

```

kali@kali:~/Desktop/volatility-master/volatility-master$ python vol.py -f stuxnet.vmem --profile=WinXPSP3x86 timeliner --output-file=timeliner/stuxnet/timeline.txt --output-body
Volatility Foundation Volatility Framework 2.6.1
Outputting to: timeliner/stuxnet/timeline.txt
kali@kali:~/Desktop/volatility-master/volatility-master$ python vol.py -f stuxnet.vmem --profile=WinXPSP3x86 mftparser --output-file=timeliner/stuxnet/mftparser.txt --output-body
Volatility Foundation Volatility Framework 2.6.1
Outputting to: timeliner/stuxnet/mftparser.txt
Scanning for MFT entries and building directory, this can take a while
kali@kali:~/Desktop/volatility-master/volatility-master$ python vol.py -f stuxnet.vmem --profile=WinXPSP3x86 shellbags --output-file=timeliner/stuxnet/shellbags.txt --output-body
Volatility Foundation Volatility Framework 2.6.1
Scanning for registries....
Gathering shellbag items and building path tree...
Outputting to: timeliner/stuxnet/shellbags.txt
kali@kali:~/Desktop/volatility-master/volatility-master$ cd timeliner/stuxnet/
kali@kali:~/Desktop/volatility-master/volatility-master/timeliner/stuxnet$ cat timeline.txt > targettimeliner.txt
kali@kali:~/Desktop/volatility-master/volatility-master/timeliner/stuxnet$ cat mftparser.txt > targettimeliner.txt
kali@kali:~/Desktop/volatility-master/volatility-master/timeliner/stuxnet$ cat shellbags.txt > targettimeliner.txt

```

Y por último, conociendo el huso horario, podemos hacer uso de mactime y more para ir viendo la información de la línea temporal:

```

kali@kali:~/Desktop/volatility-master/volatility-master/timeliner/stuxnet$ mactime -b targettimeliner.txt -d -z UTC-0400 | more
Date,Size,Type,Mode,UID,GID,Meta,File Name
Xxx Xxx 00 0000 00:00:00,0,m,...,-----,0,0,0,"[PROCESS] Procmon.exe PID: 660/PPID: 1196/POffset: 0x01e543a0"
Xxx Xxx 00 0000 00:00:00,0,m,...,-----,0,0,0,"[PROCESS] TSVNCache.exe PID: 324/PPID: 1196/POffset: 0x02086978"
Xxx Xxx 00 0000 00:00:00,0,m,...,-----,0,0,0,"[PROCESS] VMUpgradeHelper PID: 1816/PPID: 668/POffset: 0x023a0568"
Xxx Xxx 00 0000 00:00:00,0,m,...,-----,0,0,0,"[PROCESS] VMwareTray.exe PID: 1912/PPID: 1196/POffset: 0x021c5da0"
Xxx Xxx 00 0000 00:00:00,0,m,...,-----,0,0,0,"[PROCESS] VMwareUser.exe PID: 1356/PPID: 1196/POffset: 0x0206b660"
Xxx Xxx 00 0000 00:00:00,0,m,...,-----,0,0,0,"[PROCESS] alg.exe PID: 188/PPID: 668/POffset: 0x0225ada0"
Xxx Xxx 00 0000 00:00:00,0,m,...,-----,0,0,0,"[PROCESS] csrss.exe PID: 600/PPID: 376/POffset: 0x023a2da0"
Xxx Xxx 00 0000 00:00:00,0,m,...,-----,0,0,0,"[PROCESS] explorer.exe PID: 1196/PPID: 1728/POffset: 0x022ec7e8"
Xxx Xxx 00 0000 00:00:00,0,m,...,-----,0,0,0,"[PROCESS] imapi.exe PID: 756/PPID: 668/POffset: 0x02479998"
Xxx Xxx 00 0000 00:00:00,0,m,...,-----,0,0,0,"[PROCESS] jqs.exe PID: 1580/PPID: 668/POffset: 0x0200eda0"
Xxx Xxx 00 0000 00:00:00,0,m,...,-----,0,0,0,"[PROCESS] jusched.exe PID: 1712/PPID: 1196/POffset: 0x0230d478"
Xxx Xxx 00 0000 00:00:00,0,m,...,-----,0,0,0,"[PROCESS] lsass.exe PID: 1928/PPID: 668/POffset: 0x01e47c00"
Xxx Xxx 00 0000 00:00:00,0,m,...,-----,0,0,0,"[PROCESS] lsass.exe PID: 680/PPID: 624/POffset: 0x02070020"
Xxx Xxx 00 0000 00:00:00,0,m,...,-----,0,0,0,"[PROCESS] lsass.exe PID: 868/PPID: 668/POffset: 0x01e498c8"

```

```

Sat Jun 04 2011 04:31:37,0,macb,-----,0,0,0,"[TIMER] netbt.sys Signaled: -/Routine: 0xb2d4c48a/Period(ms): 0/Offset: 0x823262c8"
Sat Jun 04 2011 04:31:37,0,macb,-----,0,0,0,"[TIMER] ntoskrnl.exe Signaled: -/Routine: 0x805279e2/Period(ms): 0/Offset: 0x8055a060"
Sat Jun 04 2011 04:31:37,0,macb,-----,0,0,0,"[TIMER] ntoskrnl.exe Signaled: Yes/Routine: 0x804f3716/Period(ms): 1000/Offset: 0x80551800"
Sat Jun 04 2011 04:31:40,0,macb,-----,0,0,0,"[TIMER] Ntfs.sys Signaled: -/Routine: 0xf84111b4/Period(ms): 0/Offset: 0xf842f270"
Sat Jun 04 2011 04:31:41,0,macb,-----,0,0,0,"[TIMER] ntoskrnl.exe Signaled: -/Routine: 0x8053b8fc/Period(ms): 0/Offset: 0x80550ce0"
Sat Jun 04 2011 04:31:42,0,macb,-----,0,0,0,"[TIMER] NDIS.sys Signaled: -/Routine: 0xf83faf6f/Period(ms): 0/Offset: 0x8232e1a0"
Sat Jun 04 2011 04:31:43,0,macb,-----,0,0,0,"[TIMER] FltMgr.sys Signaled: -/Routine: 0xf84c9226/Period(ms): 0/Offset: 0xf84cfa68"
Sat Jun 04 2011 04:31:44,0,macb,-----,0,0,0,"[TIMER] ntoskrnl.exe Signaled: -/Routine: 0x80534e48/Period(ms): 0/Offset: 0x82255720"
Sat Jun 04 2011 04:31:44,0,macb,-----,0,0,0,"[TIMER] watchdog.sys Signaled: Yes/Routine: 0xf8a0a6c4/Period(ms): 10000/Offset: 0x81da3240"
Sat Jun 04 2011 04:31:44,0,macb,-----,0,0,0,"[TIMER] watchdog.sys Signaled: Yes/Routine: 0xf8a0a6c4/Period(ms): 10000/Offset: 0x81e70848"
Sat Jun 04 2011 04:31:45,0,macb,-----,0,0,0,"[TIMER] srv.sys Signaled: -/Routine: 0xb27e4385/Period(ms): 0/Offset: 0xb27f3990"
Sat Jun 04 2011 04:31:48,0,macb,-----,0,0,0,"[TIMER] HTTP.sys Signaled: -/Routine: 0xb250c9fc/Period(ms): 0/Offset: 0xb25191c0"
Sat Jun 04 2011 04:31:48,0,macb,-----,0,0,0,"[TIMER] HTTP.sys Signaled: Yes/Routine: 0xb24ff1f8/Period(ms): 60000/Offset: 0xb2516990"
Sat Jun 04 2011 04:31:48,0,macb,-----,0,0,0,"[TIMER] HTTP.sys Signaled: Yes/Routine: 0xb2506418/Period(ms): 30000/Offset: 0xb2516be0"
Sat Jun 04 2011 04:31:50,0,macb,-----,0,0,0,"[TIMER] ntoskrnl.exe Signaled: -/Routine: 0x80534e48/Period(ms): 0/Offset: 0x82069678"
Sat Jun 04 2011 04:31:58,0,macb,-----,0,0,0,"[TIMER] FltMgr.sys Signaled: Yes/Routine: 0xf84c923c/Period(ms): 60000/Offset: 0x81bf51a0"
Sat Jun 04 2011 04:32:04,0,macb,-----,0,0,0,"[TIMER] afd.sys Signaled: Yes/Routine: 0xb2d2a385/Period(ms): 30000/Offset: 0x820a1e08"
Sat Jun 04 2011 04:32:15,0,macb,-----,0,0,0,"[TIMER] ntoskrnl.exe Signaled: -/Routine: 0x80534e48/Period(ms): 0/Offset: 0x81eb8e28"
Sat Jun 04 2011 04:32:27,0,macb,-----,0,0,0,"[TIMER] ntoskrnl.exe Signaled: Yes/Routine: 0x804f3eae/Period(ms): 60000/Offset: 0x805516d0"
Sat Jun 04 2011 04:32:30,0,macb,-----,0,0,0,"[TIMER] Ntfs.sys Signaled: -/Routine: 0xf84113d8/Period(ms): 0/Offset: 0xf842f2d0"
Sat Jun 04 2011 04:32:31,0,macb,-----,0,0,0,"[TIMER] NDIS.sys Signaled: Yes/Routine: 0xf83fb6bc/Period(ms): 60000/Offset: 0x81dc52a0"
Sat Jun 04 2011 04:32:32,0,macb,-----,0,0,0,"[TIMER] ipnat.sys Signaled: Yes/Routine: 0xb2c32266/Period(ms): 60000/Offset: 0xb2c3ad60"
Sat Jun 04 2011 04:32:32,0,macb,-----,0,0,0,"[TIMER] ipsec.sys Signaled: -/Routine: 0xb2dcd3e7/Period(ms): 0/Offset: 0xb2ddcd08"
Sat Jun 04 2011 04:32:32,0,macb,-----,0,0,0,"[TIMER] ipsec.sys Signaled: Yes/Routine: 0xb2dcd471/Period(ms): 60000/Offset: 0xb2dddc1c"
Sat Jun 04 2011 04:32:41,0,macb,-----,0,0,0,"[TIMER] ntoskrnl.exe Signaled: -/Routine: 0x8050aa28/Period(ms): 0/Offset: 0x80553ec0"
Sat Jun 04 2011 04:32:48,0,macb,-----,0,0,0,"[TIMER] HTTP.sys Signaled: -/Routine: 0xb250a832/Period(ms): 0/Offset: 0xb2519260"
Sat Jun 04 2011 04:42:27,0,macb,-----,0,0,0,"[TIMER] ntoskrnl.exe Signaled: -/Routine: 0x80534a2a/Period(ms): 0/Offset: 0x8055b200"
Sat Jun 04 2011 04:42:32,0,macb,-----,0,0,0,"[TIMER] ipsec.sys Signaled: -/Routine: 0xb2dcd3e7/Period(ms): 0/Offset: 0xb2ddcd70"
Sat Jun 04 2011 04:42:32,0,macb,-----,0,0,0,"[TIMER] netbt.sys Signaled: -/Routine: 0xb2d4c48a/Period(ms): 0/Offset: 0x82083240"
Sat Jun 04 2011 06:54:46,0,macb,-----,0,0,0,"[TIMER] NDIS.sys Signaled: -/Routine: 0xf83faf6f/Period(ms): 0/Offset: 0x822f2438"
Sat Jun 04 2011 06:54:46,0,macb,-----,0,0,0,"[TIMER] NDIS.sys Signaled: -/Routine: 0xf83faf6f/Period(ms): 0/Offset: 0x822be9a8"
Sun Jun 05 2011 01:07:01,0,macb,-----,0,0,0,"[TIMER] NDIS.sys Signaled: -/Routine: 0xf83faf6f/Period(ms): 0/Offset: 0x81dbeb78"
Sun Jun 05 2011 01:07:01,0,macb,-----,0,0,0,"[TIMER] NDIS.sys Signaled: -/Routine: 0xf83faf6f/Period(ms): 0/Offset: 0x81e8b4f0"
Sun Jun 05 2011 01:07:01,0,macb,-----,0,0,0,"[TIMER] NDIS.sys Signaled: -/Routine: 0xf83faf6f/Period(ms): 0/Offset: 0x822771a0"

```

De la cual podríamos filtrar con `grep` o `egrep` para buscar información más concreta en la que queramos profundizar.