ANÁLISIS FORENSE: TRY TO HACK ME - MEMORY WINDOWS

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

Try to hack me forensics

Sistema comprometido, realiza un análisis forense del volcado de memoria de kung-fu

¿Cúal es le Sistema operative? (OS name)

volatility -f victim.raw imageinfo

```
volatility -f victim.raw imageinfo
         Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_23418
                    AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                    AS Layer2 : FileAddressSpace (/home/kali/Documents/forense/hackthebox/case_02/victim.raw)
                     PAE type : No PAE
                          DTB : 0x187000L
                         KDBG : 0xf80002842a0L
         Number of Processors : 1
    Image Type (Service Pack) : 1
               KPCR for CPU 0 : 0xfffff80002843d00L
            KUSER_SHARED_DATA : 0xfffff78000000000L
          Image date and time : 2019-05-02 18:11:45 UTC+0000
    Image local date and time : 2019-05-02 11:11:45 -0700
```

¿Cúale sel pid del proceso SearchIndexer?

volatility -f victim.raw --profile=Win7SP1x64 pslist

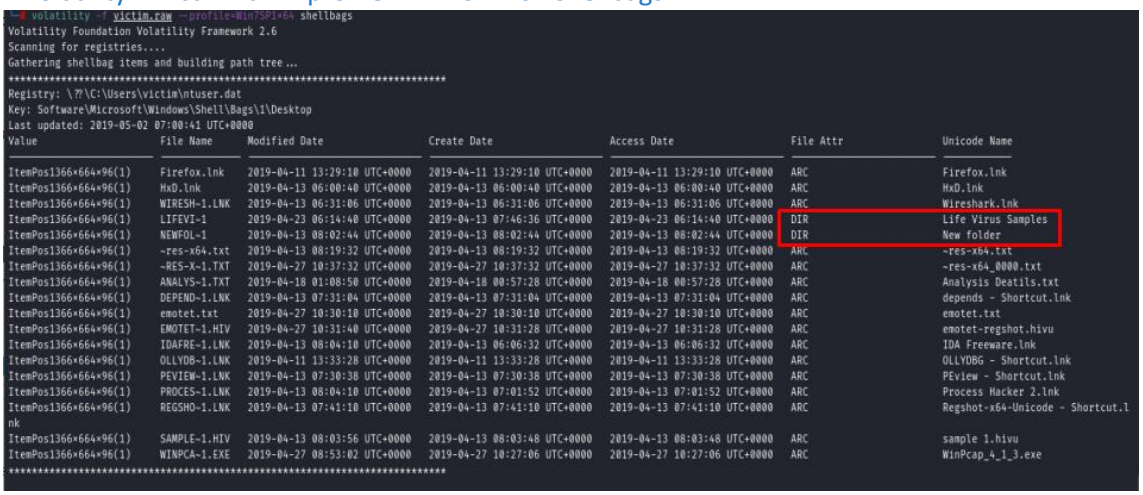
```
└─# volatility -f victim.raw --profile=Win7SP1x64 pslist

Volatility Foundation Volatility Framework 2.6
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0xfffffa8001252040 System                    4      0     88      624 ------      0 2019-05-03 06:32:24 UTC+0000
0xfffffa800234d8a0 smss.exe                268      4      2       29 ------      0 2019-05-03 06:32:24 UTC+0000
0xfffffa8002264550 csrss.exe               360    352      9      363      0      0 2019-05-03 06:32:34 UTC+0000
0xfffffa80027d67d0 csrss.exe               408    400      7      162      1      0 2019-05-03 06:32:35 UTC+0000
0xfffffa8002b601c0 wininit.exe             416    352      3       76      0      0 2019-05-03 06:32:35 UTC+0000
0xfffffa8002b71680 winlogon.exe            444    400      3      111      1      0 2019-05-03 06:32:35 UTC+0000
0xfffffa8002c69b30 services.exe            504    416      6      184      0      0 2019-05-03 06:32:36 UTC+0000
0xfffffa80027d9b30 lsass.exe               512    416      6      534      0      0 2019-05-03 06:32:37 UTC+0000
0xfffffa80027d81f0 lsm.exe                 520    416     10      143      0      0 2019-05-03 06:32:37 UTC+0000
0xfffffa80029cd3e0 svchost.exe             628    504      9      345      0      0 2019-05-03 06:32:48 UTC+0000
0xfffffa8002d38b30 VBoxService.ex          688    504     12      135      0      0 2019-05-03 06:32:48 UTC+0000
0xfffffa8002a1bb30 svchost.exe             752    504      7      235      0      0 2019-05-02 18:02:51 UTC+0000
0xfffffa8002d70650 svchost.exe             852    504     22      473      0      0 2019-05-02 18:02:51 UTC+0000
0xfffffa8002d9c780 svchost.exe             892    504     17      427      0      0 2019-05-02 18:02:51 UTC+0000
0xfffffa8002dbe9e0 svchost.exe             920    504     29      878      0      0 2019-05-02 18:02:51 UTC+0000
0xfffffa8002e3db30 svchost.exe             400    504     10      281      0      0 2019-05-02 18:02:56 UTC+0000
0xfffffa8002e57890 svchost.exe            1004    504     20      379      0      0 2019-05-02 18:02:56 UTC+0000
0xfffffa8002dfdab0 spoolsv.exe            1140    504     12      279      0      0 2019-05-02 18:02:57 UTC+0000
0xfffffa8002f2cb30 svchost.exe            1268    504     17      297      0      0 2019-05-02 18:02:59 UTC+0000
0xfffffa8002f81460 svchost.exe            1368    504     20      295      0      0 2019-05-02 18:02:59 UTC+0000
0xfffffa8003148b30 taskhost.exe           1788    504      8      159      1      0 2019-05-02 18:03:09 UTC+0000
0xfffffa8003172b30 explorer.exe           1860   1756     19      645      1      0 2019-05-02 18:03:09 UTC+0000
0xfffffa800315eb30 dwm.exe                1896    892      3       69      1      0 2019-05-02 18:03:09 UTC+0000
0xfffffa800300d700 VBoxTray.exe           1600   1860     13      141      1      0 2019-05-02 18:03:25 UTC+0000
0xfffffa8003367060 SearchIndexer.         2180    504     11      629      0      0 2019-05-02 18:03:32 UTC+0000
0xfffffa80033f6060 wmiPrvSE.exe           2876    628      5      113      0      0 2019-05-02 18:03:55 UTC+0000
0xfffffa8003162060 svchost.exe            1820    504     11      317      0      0 2019-05-02 18:05:09 UTC+0000
0xfffffa8003371540 wmpnetwk.exe           2464    504     14      440      0      0 2019-05-02 18:05:10 UTC+0000
0xfffffa80014eeb30 taskhost.exe           1148    504      8      176      0      0 2019-05-02 18:09:58 UTC+0000
```

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

¿Cuál es el último directorio visitado por el usuario?

volatility -f victim.raw --profile=Win7SP1x64 shellbags



```
Volatility Foundation Volatility Framework 2.6
Scanning for registries....
Gathering shellbag items and building path tree ...
**************************************************
Registry: \??\C:\Users\victim\ntuser.dat
Key: Software\Microsoft\Windows\Shell\Bags\1\Desktop
Last updated: 2019-05-02 07:00:41 UTC+0000
```

Value	File Name	Modified Date	Create Date	Access Date	File Attr	Unicode Name
ItemPos1366×664×96(1)	Firefox.lnk	2019-04-11 13:29:10 UTC+0000	2019-04-11 13:29:10 UTC+0000	2019-04-11 13:29:10 UTC+0000	ARC	Firefox.lnk
ItemPos1366×664×96(1)	HxD.lnk	2019-04-13 06:00:40 UTC+0000	2019-04-13 06:00:40 UTC+0000	2019-04-13 06:00:40 UTC+0000	ARC	HxD.lnk
ItemPos1366×664×96(1)	WIRESH~1.LNK	2019-04-13 06:31:06 UTC+0000	2019-04-13 06:31:06 UTC+0000	2019-04-13 06:31:06 UTC+0000	ARC	Wireshark.lnk
ItemPos1366×664×96(1)	LIFEVI~1	2019-04-23 06:14:40 UTC+0000	2019-04-13 07:46:36 UTC+0000	2019-04-23 06:14:40 UTC+0000	DIR	Life Virus Samples
ItemPos1366×664×96(1)	NEWFOL~1	2019-04-13 08:02:44 UTC+0000	2019-04-13 08:02:44 UTC+0000	2019-04-13 08:02:44 UTC+0000	DIR	New folder
ItemPos1366×664×96(1)	~res-x64.txt	2019-04-13 08:19:32 UTC+0000	2019-04-13 08:19:32 UTC+0000	2019-04-13 08:19:32 UTC+0000	ARC	~res-x64.txt
ItemPos1366×664×96(1)	~RES-X~1.TXT	2019-04-27 10:37:32 UTC+0000	2019-04-27 10:37:32 UTC+0000	2019-04-27 10:37:32 UTC+0000	ARC	~res-x64_0000.txt
ItemPos1366×664×96(1)	ANALYS~1.TXT	2019-04-18 01:08:50 UTC+0000	2019-04-18 00:57:28 UTC+0000	2019-04-18 00:57:28 UTC+0000	ARC	Analysis Deatils.txt
ItemPos1366×664×96(1)	DEPEND~1.LNK	2019-04-13 07:31:04 UTC+0000	2019-04-13 07:31:04 UTC+0000	2019-04-13 07:31:04 UTC+0000	ARC	depends - Shortcut.lnk
ItemPos1366×664×96(1)	emotet.txt	2019-04-27 10:30:10 UTC+0000	2019-04-27 10:30:10 UTC+0000	2019-04-27 10:30:10 UTC+0000	ARC	emotet.txt
ItemPos1366×664×96(1)	EMOTET~1.HIV	2019-04-27 10:31:40 UTC+0000	2019-04-27 10:31:28 UTC+0000	2019-04-27 10:31:28 UTC+0000	ARC	emotet-regshot.hivu
ItemPos1366×664×96(1)	IDAFRE~1.LNK	2019-04-13 08:04:10 UTC+0000	2019-04-13 06:06:32 UTC+0000	2019-04-13 06:06:32 UTC+0000	ARC	IDA Freeware.lnk
ItemPos1366×664×96(1)	OLLYDB~1.LNK	2019-04-11 13:33:28 UTC+0000	2019-04-11 13:33:28 UTC+0000	2019-04-11 13:33:28 UTC+0000	ARC	OLLYDBG - Shortcut.lnk
ItemPos1366×664×96(1)	PEVIEW~1.LNK	2019-04-13 07:30:38 UTC+0000	2019-04-13 07:30:38 UTC+0000	2019-04-13 07:30:38 UTC+0000	ARC	PEview - Shortcut.lnk
ItemPos1366×664×96(1)	PROCES~1.LNK	2019-04-13 08:04:10 UTC+0000	2019-04-13 07:01:52 UTC+0000	2019-04-13 07:01:52 UTC+0000	ARC	Process Hacker 2.lnk
ItemPos1366×664×96(1)	REGSHO~1.LNK	2019-04-13 07:41:10 UTC+0000	2019-04-13 07:41:10 UTC+0000	2019-04-13 07:41:10 UTC+0000	ARC	Regshot-x64-Unicode - Shortcut.lnk
ItemPos1366×664×96(1)	SAMPLE~1.HIV	2019-04-13 08:03:56 UTC+0000	2019-04-13 08:03:48 UTC+0000	2019-04-13 08:03:48 UTC+0000	ARC	sample 1.hivu
ItemPos1366×664×96(1)	WINPCA~1.EXE	2019-04-27 08:53:02 UTC+0000	2019-04-27 10:27:06 UTC+0000	2019-04-27 10:27:06 UTC+0000	ARC	WinPcap_4_1_3.exe

Revisando la columna Access Date vemos que el último directorio que se ha accedido en la siguiente, vamos a ayudarnos con el comando grep para ir al grano.

cat shellbags.txt | grep "Access Date" -B 10

```
Key: Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\1\0
Last updated: 2019-04-27 10:33:47 UTC+0000
```

Value	Mru	File Name	Modified Date	Create Date	Access Date	File Attr	Path
0	0	victim	2019-04-10 15:59:34 UTC+0000	2019-04-10 15:58:54 UTC+0000	2019-04-10 15:59:34 UTC+0000	DIR	C:\Users\victim

```
**************************************************

**************************************************
Registry: \??\C:\Users\victim\AppData\Local\Microsoft\Windows\UsrClass.dat
Key: Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\1\1
Last updated: 2019-04-27 10:34:47 UTC+0000
```

Value	Mru	File Name	Modified Date	Create Date	Access Date	File Attr	Path
0	0	Microsoft	1970-01-01 00:00:00 UTC+0000	1970-01-01 00:00:00 UTC+0000	1970-01-01 00:00:00 UTC+0000	DIR	C:\ProgramData\Microsoft

```
**************************************************

**************************************************
Registry: \??\C:\Users\victim\AppData\Local\Microsoft\Windows\UsrClass.dat
Key: Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\1\2
Last updated: 2019-04-27 10:38:03 UTC+0000
```

Value	Mru	File Name	Modified Date	Create Date	Access Date	File Attr	Path
0	0	Capture	2019-04-27 10:36:06 UTC+0000	2019-04-18 00:49:00 UTC+0000	2019-04-27 10:36:06 UTC+0000	DIR	C:\Program Files (x86)\Capture

```
**************************************************

**************************************************
Registry: \??\C:\Users\victim\AppData\Local\Microsoft\Windows\UsrClass.dat
Key: Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\2\0
Last updated: 2019-04-27 10:48:33 UTC+0000
```

Value	Mru	File Name	Modified Date	Create Date	Access Date	File Attr	Path
0	0	deleted_files	2019-04-27 10:30:26 UTC+0000	2019-04-27 10:38:24 UTC+0000	2019-04-27 10:38:24 UTC+0000	NI, DIR	Z:\logs\deleted_files

```
**************************************************
```

La última carpeta que se ha accedido en z:\logs\deletes_files

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

Hay conexiones un tanto sospechosos, indica direccion y puerto:

Ejecutamos volatility con el plugin sockscan o connscan si bien en ambos casos no soporte con el profile de Win7sp1

volatility -f victim.raw --profile=Win7SP1x64 sockscan
volatility -f victim.raw --profile=Win7SP1x64 connscan

```
└─# volatility -f victim.raw --profile=Win7SP1x64 sockscan
Volatility Foundation Volatility Framework 2.6
ERROR   : volatility.debug    : This command does not support the profile Win7SP1x64

┌──(root㉿kali)-[/home/…/Documents/forense/trytohackme/case_01]
└─# volatility -f victim.raw --profile=Win7SP1x64 connscan
Volatility Foundation Volatility Framework 2.6
ERROR   : volatility.debug    : This command does not support the profile Win7SP1x64
```

volatility -f victim.raw --profile=Win7SP1x64 netscan

```
┌──(root㉿kali)-[/home/…/Documents/forense/trytohackme/case_01]
└─# volatility -f victim.raw --profile=Win7SP1x64 netscan
Volatility Foundation Volatility Framework 2.6
Offset(P)          Proto    Local Address                  Foreign Address      State          Pid      Owner          Created
0x5c201ca0         UDPv4    0.0.0.0:5005                   *:*                                 2464     wmpnetwk.exe   2019-05-02 18:05:14 UTC+0000
0x5c201ca0         UDPv6    :::5005                        *:*                                 2464     wmpnetwk.exe   2019-05-02 18:05:14 UTC+0000
0x5c49cbb0         UDPv4    0.0.0.0:59471                  *:*                                 1368     svchost.exe    2019-05-02 18:03:06 UTC+0000
0x5c4a31c0         UDPv4    0.0.0.0:59472                  *:*                                 1368     svchost.exe    2019-05-02 18:03:06 UTC+0000
0x5c4a31c0         UDPv6    :::59472                       *:*                                 1368     svchost.exe    2019-05-02 18:03:06 UTC+0000
0x5c4ac630         UDPv4    0.0.0.0:3702                   *:*                                 1368     svchost.exe    2019-05-02 18:03:14 UTC+0000
0x5c4ac630         UDPv6    :::3702                        *:*                                 1368     svchost.exe    2019-05-02 18:03:14 UTC+0000
0x5c519b30         UDPv4    0.0.0.0:3702                   *:*                                 1368     svchost.exe    2019-05-02 18:03:14 UTC+0000
0x5c537ec0         UDPv4    0.0.0.0:3702                   *:*                                 1368     svchost.exe    2019-05-02 18:03:14 UTC+0000
0x5c690360         UDPv4    0.0.0.0:0                      *:*                                 1004     svchost.exe    2019-05-02 18:02:56 UTC+0000
0x5c690360         UDPv6    :::0                           *:*                                 1004     svchost.exe    2019-05-02 18:02:56 UTC+0000
0x5c6918e0         UDPv4    0.0.0.0:5355                   *:*                                 1004     svchost.exe    2019-05-02 18:02:56 UTC+0000
0x5c6918e0         UDPv6    :::5355                        *:*                                 1004     svchost.exe    2019-05-02 18:02:56 UTC+0000
0x5c692940         UDPv4    0.0.0.0:5005                   *:*                                 2464     wmpnetwk.exe   2019-05-02 18:05:14 UTC+0000
0x5c692ae0         UDPv4    0.0.0.0:5355                   *:*                                 1004     svchost.exe    2019-05-02 18:02:56 UTC+0000
0x5c7bac70         UDPv4    0.0.0.0:5004                   *:*                                 2464     wmpnetwk.exe   2019-05-02 18:05:14 UTC+0000
0x5c7bac70         UDPv6    :::5004                        *:*                                 2464     wmpnetwk.exe   2019-05-02 18:05:14 UTC+0000
0x5c7f9600         UDPv4    0.0.0.0:3702                   *:*                                 1368     svchost.exe    2019-05-02 18:03:14 UTC+0000
0x5c7f9600         UDPv6    :::3702                        *:*                                 1368     svchost.exe    2019-05-02 18:03:14 UTC+0000
0x5c44e1b0         TCPv4    0.0.0.0:5357                   0.0.0.0:0            LISTENING      4        System
0x5c44e1b0         TCPv6    :::5357                        :::0                 LISTENING      4        System
0x5c528010         TCPv4    0.0.0.0:445                    0.0.0.0:0            LISTENING      4        System
0x5c528010         TCPv6    :::445                         :::0                 LISTENING      4        System
0x5c534c60         TCPv4    0.0.0.0:49156                  0.0.0.0:0            LISTENING      504      services.exe
0x5c534c60         TCPv6    :::49156                       :::0                 LISTENING      504      services.exe
0x5c535010         TCPv4    0.0.0.0:49156                  0.0.0.0:0            LISTENING      504      services.exe
0x5c6de720         TCPv4    0.0.0.0:49154                  0.0.0.0:0            LISTENING      920      svchost.exe
0x5c6de720         TCPv6    :::49154                       :::0                 LISTENING      920      svchost.exe
0x5c6e0df0         TCPv4    0.0.0.0:49154                  0.0.0.0:0            LISTENING      920      svchost.exe
0x5c717460         TCPv4    0.0.0.0:49155                  0.0.0.0:0            LISTENING      512      lsass.exe
```

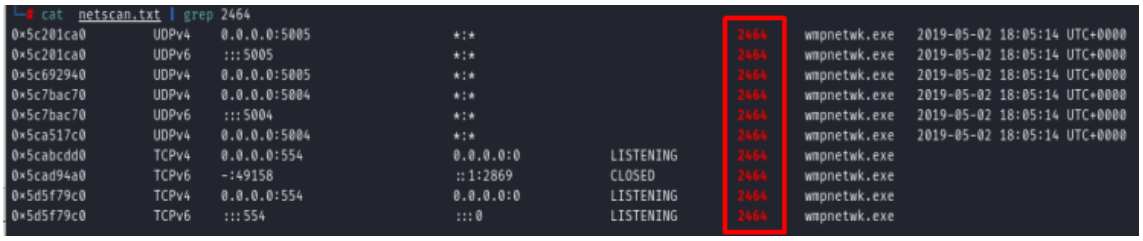
Los puertos abiertos son los siguientes:

4	TCP:5357, TCP:445, UDP:138, UDP:137,TCP:2869 Puertos del sistema	
416	TCP:49152	
504	TCP:49156	
512	TCP:49155	
752	TCP:135	samba
688		vbox
852	TCP:49153	
920	TCP:49154	
1004	UDP:5355	
1368	**UDP:59471, UDP:59471, UDP:3702, UDP:1900, UDP:61556, UDP:61555**	**Puertos sospechosos**

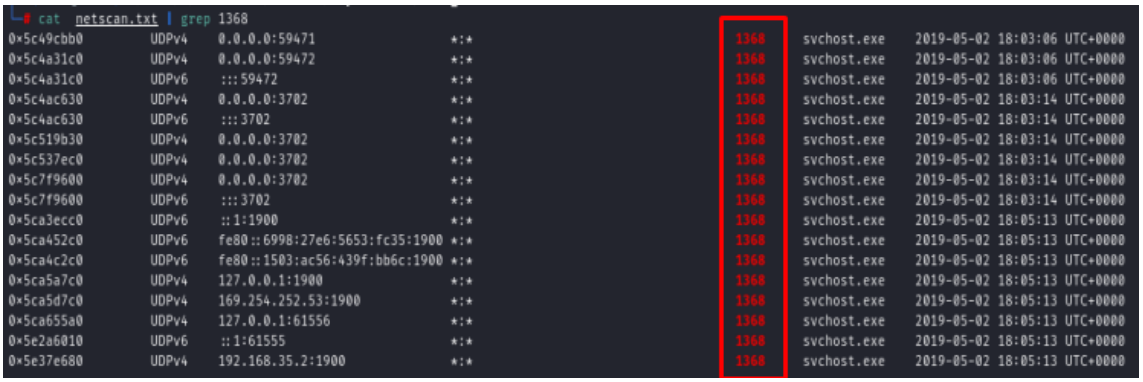
https://github.com/aguayro @9v@yr0

2464 UDP:5005, UDP:5004, TCP:554 Puertos sospechosos

Revisamos ambos procesos para identificar los procesos sospechosos con el proceso pid 1368 y 2454

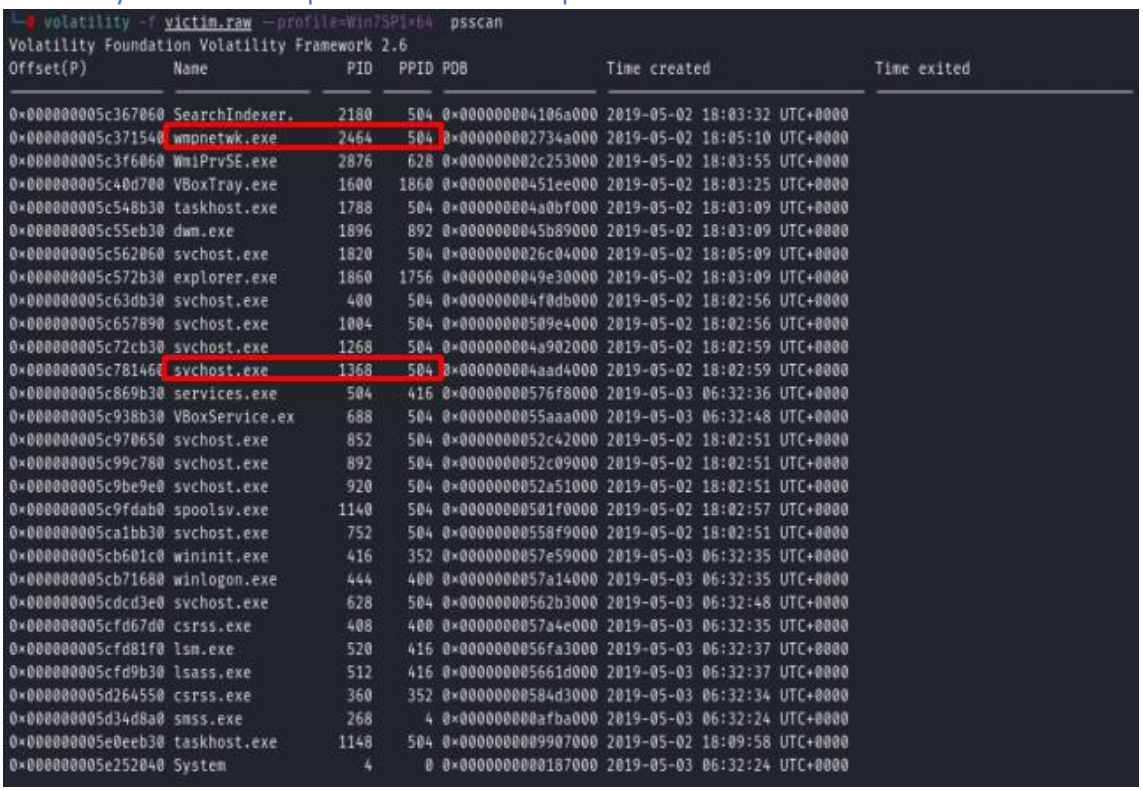


```
# cat netscan.txt | grep 2464
0x5c201ca0  UDPv4  0.0.0.0:5005          *:*                    2464  wmpnetwk.exe  2019-05-02 18:05:14 UTC+0000
0x5c201ca0  UDPv6  :::5005              *:*                    2464  wmpnetwk.exe  2019-05-02 18:05:14 UTC+0000
0x5c692940  UDPv4  0.0.0.0:5005          *:*                    2464  wmpnetwk.exe  2019-05-02 18:05:14 UTC+0000
0x5c7bac70  UDPv4  0.0.0.0:5004          *:*                    2464  wmpnetwk.exe  2019-05-02 18:05:14 UTC+0000
0x5c7bac70  UDPv6  :::5004              *:*                    2464  wmpnetwk.exe  2019-05-02 18:05:14 UTC+0000
0x5ca517c0  UDPv4  0.0.0.0:5004          *:*                    2464  wmpnetwk.exe  2019-05-02 18:05:14 UTC+0000
0x5cabcdd0  TCPv4  0.0.0.0:554           0.0.0.0:0      LISTENING 2464  wmpnetwk.exe
0x5cad94a0  TCPv6  -:49158              ::1:2869       CLOSED    2464  wmpnetwk.exe
0x5d5f79c0  TCPv4  0.0.0.0:554           0.0.0.0:0      LISTENING 2464  wmpnetwk.exe
0x5d5f79c0  TCPv6  :::554               :::0           LISTENING 2464  wmpnetwk.exe
```



```
# cat netscan.txt | grep 1368
0x5c49cbb0  UDPv4  0.0.0.0:59471         *:*                    1368  svchost.exe   2019-05-02 18:03:06 UTC+0000
0x5c4a31c0  UDPv4  0.0.0.0:59472         *:*                    1368  svchost.exe   2019-05-02 18:03:06 UTC+0000
0x5c4a31c0  UDPv6  :::59472             *:*                    1368  svchost.exe   2019-05-02 18:03:06 UTC+0000
0x5c4ac630  UDPv4  0.0.0.0:3702          *:*                    1368  svchost.exe   2019-05-02 18:03:14 UTC+0000
0x5c4ac630  UDPv6  :::3702              *:*                    1368  svchost.exe   2019-05-02 18:03:14 UTC+0000
0x5c519b30  UDPv4  0.0.0.0:3702          *:*                    1368  svchost.exe   2019-05-02 18:03:14 UTC+0000
0x5c537ec0  UDPv4  0.0.0.0:3702          *:*                    1368  svchost.exe   2019-05-02 18:03:14 UTC+0000
0x5c7f9600  UDPv4  0.0.0.0:3702          *:*                    1368  svchost.exe   2019-05-02 18:03:14 UTC+0000
0x5c7f9600  UDPv6  :::3702              *:*                    1368  svchost.exe   2019-05-02 18:03:14 UTC+0000
0x5ca3ecc0  UDPv6  ::1:1900             *:*                    1368  svchost.exe   2019-05-02 18:05:13 UTC+0000
0x5ca452c0  UDPv6  fe80::6998:27e6:5653:fc35:1900 *:*           1368  svchost.exe   2019-05-02 18:05:13 UTC+0000
0x5ca4c2c0  UDPv6  fe80::1503:ac56:439f:bb6c:1900 *:*           1368  svchost.exe   2019-05-02 18:05:13 UTC+0000
0x5ca5a7c0  UDPv4  127.0.0.1:1900        *:*                    1368  svchost.exe   2019-05-02 18:05:13 UTC+0000
0x5ca5d7c0  UDPv4  169.254.252.53:1900    *:*                    1368  svchost.exe   2019-05-02 18:05:13 UTC+0000
0x5ca655a0  UDPv4  127.0.0.1:61556       *:*                    1368  svchost.exe   2019-05-02 18:05:13 UTC+0000
0x5e2a6010  UDPv6  ::1:61555            *:*                    1368  svchost.exe   2019-05-02 18:05:13 UTC+0000
0x5e37e680  UDPv4  192.168.35.2:1900     *:*                    1368  svchost.exe   2019-05-02 18:05:13 UTC+0000
```

volatility -f victim.raw --profile=Win7SP1x64 psscan



```
# volatility -f victim.raw --profile=Win7SP1x64 psscan
Volatility Foundation Volatility Framework 2.6
Offset(P)          Name                PID   PPID PDB              Time created                   Time exited
------------------ ---------------- ------ ------ ---------------- ------------------------------ ------------------------------
0x000000005c367060 SearchIndexer.     2180    504 0x000000004106a000 2019-05-02 18:03:32 UTC+0000
0x000000005c371540 wmpnetwk.exe       2464    504 0x000000002734a000 2019-05-02 18:05:10 UTC+0000
0x000000005c3f6060 WmiPrvSE.exe       2876    628 0x000000002c253000 2019-05-02 18:03:55 UTC+0000
0x000000005c40d700 VBoxTray.exe       1600   1860 0x000000000451ee000 2019-05-02 18:03:25 UTC+0000
0x000000005c548b30 taskhost.exe       1788    504 0x000000004a0bf000 2019-05-02 18:03:09 UTC+0000
0x000000005c55eb30 dwm.exe            1896    892 0x0000000045b89000 2019-05-02 18:03:09 UTC+0000
0x000000005c562060 svchost.exe        1820    504 0x000000026c04000 2019-05-02 18:05:09 UTC+0000
0x000000005c572b30 explorer.exe       1860   1756 0x0000000049e30000 2019-05-02 18:03:09 UTC+0000
0x000000005c63db30 svchost.exe         400    504 0x000000004f0db000 2019-05-02 18:02:56 UTC+0000
0x000000005c657890 svchost.exe        1004    504 0x000000000509e4000 2019-05-02 18:02:56 UTC+0000
0x000000005c72cb30 svchost.exe        1268    504 0x000000004a902000 2019-05-02 18:02:59 UTC+0000
0x000000005c781460 svchost.exe        1368    504 0x000000004aad4000 2019-05-02 18:02:59 UTC+0000
0x000000005c869b30 services.exe        504    416 0x000000000576f8000 2019-05-03 06:32:36 UTC+0000
0x000000005c938b30 VBoxService.ex      688    504 0x0000000055aaa000 2019-05-03 06:32:48 UTC+0000
0x000000005c970650 svchost.exe         852    504 0x000000052c42000 2019-05-02 18:02:51 UTC+0000
0x000000005c99c780 svchost.exe         892    504 0x000000052c09000 2019-05-02 18:02:51 UTC+0000
0x000000005c9be9e0 svchost.exe         920    504 0x000000052a51000 2019-05-02 18:02:51 UTC+0000
0x000000005c9fdab0 spoolsv.exe        1140    504 0x000000000501f0000 2019-05-02 18:02:57 UTC+0000
0x000000005ca1bb30 svchost.exe         752    504 0x000000000558f9000 2019-05-02 18:02:51 UTC+0000
0x000000005cb601c0 wininit.exe         416    352 0x000000057e59000 2019-05-03 06:32:35 UTC+0000
0x000000005cb71680 winlogon.exe        444    400 0x000000057a14000 2019-05-03 06:32:35 UTC+0000
0x000000005cdcd3e0 svchost.exe         628    504 0x000000000562b3000 2019-05-03 06:32:48 UTC+0000
0x000000005cfd67d0 csrss.exe           408    400 0x000000057a4e000 2019-05-03 06:32:35 UTC+0000
0x000000005cfd81f0 lsm.exe             520    416 0x000000056fa3000 2019-05-03 06:32:37 UTC+0000
0x000000005cfd9b30 lsass.exe           512    416 0x0000000056610000 2019-05-03 06:32:37 UTC+0000
0x000000005d264550 csrss.exe           360    352 0x000000000584d3000 2019-05-03 06:32:34 UTC+0000
0x000000005d34d8a0 smss.exe            268      4 0x000000000afba000 2019-05-03 06:32:24 UTC+0000
0x000000005e0eeb30 taskhost.exe       1148    504 0x0000000089907000 2019-05-02 18:09:58 UTC+0000
0x000000005e252040 System                4      0 0x0000000000187000 2019-05-03 06:32:24 UTC+0000
```

El proceso pid 1368 está relacionado con el servicio svchost.exe y el proceso 2464 se refiere a una aplicación wmpnetwk.exe. Es un proceso de Windows asociado al servicio de compartición en red del reproductor Windows media. Ambos procesos tienen el mismo proceso padre PID 504 un tanto sospechoso.

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

Seguimos revisando los procesos, veamos el árbol de procesos para identificar procesos que no tienen procesos padres.

volatility -f victim.raw --profile=Win7SP1x64 pstree

```
└─# volatility -f victim.raw --profile=Win7SP1x64 pstree
Volatility Foundation Volatility Framework 2.6
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0xfffffa8002b601c0:wininit.exe                       416    352      3     76 2019-05-03 06:32:35 UTC+0000
. 0xfffffa80027d9b30:lsass.exe                        512    416      6    534 2019-05-03 06:32:37 UTC+0000
. 0xfffffa80027d81f0:lsm.exe                          520    416     10    143 2019-05-03 06:32:37 UTC+0000
. 0xfffffa8002c69b30:services.exe                     504    416      6    184 2019-05-03 06:32:36 UTC+0000
.. 0xfffffa8002e3db30:svchost.exe                     400    504     10    281 2019-05-02 18:02:56 UTC+0000
... 0xfffffa80027d67d0:csrss.exe                      408    400      7    162 2019-05-03 06:32:35 UTC+0000
... 0xfffffa8002b71680:winlogon.exe                   444    400      3    111 2019-05-03 06:32:35 UTC+0000
.. 0xfffffa8002dbe9e0:svchost.exe                     920    504     29    878 2019-05-02 18:02:51 UTC+0000
.. 0xfffffa8003367060:SearchIndexer.                 2180    504     11    629 2019-05-02 18:03:32 UTC+0000
.. 0xfffffa8003162060:svchost.exe                    1820    504     11    317 2019-05-02 18:05:09 UTC+0000
.. 0xfffffa8002d38b30:VBoxService.ex                  688    504     12    135 2019-05-03 06:32:48 UTC+0000
.. 0xfffffa80029cd3e0:svchost.exe                     628    504      9    345 2019-05-03 06:32:48 UTC+0000
... 0xfffffa80033f6060:WmiPrvSE.exe                  2876    628      5    113 2019-05-02 18:03:55 UTC+0000
.. 0xfffffa8002dfdab0:spoolsv.exe                    1140    504     12    279 2019-05-02 18:02:57 UTC+0000
.. 0xfffffa8003371540:wmpnetwk.exe                   2464    504     14    440 2019-05-02 18:05:10 UTC+0000
.. 0xfffffa8002d70650:svchost.exe                     852    504     22    473 2019-05-02 18:02:51 UTC+0000
.. 0xfffffa8002f81460:svchost.exe                    1368    504     20    295 2019-05-02 18:02:59 UTC+0000
.. 0xfffffa8003148b30:taskhost.exe                   1788    504      8    159 2019-05-02 18:03:09 UTC+0000
.. 0xfffffa8002e57890:svchost.exe                    1004    504     20    379 2019-05-02 18:02:56 UTC+0000
.. 0xfffffa8002a1bb30:svchost.exe                     752    504      7    235 2019-05-02 18:02:51 UTC+0000
.. 0xfffffa8002f2cb30:svchost.exe                    1268    504     17    297 2019-05-02 18:02:59 UTC+0000
.. 0xfffffa80014eeb30:taskhost.exe                   1148    504      8    176 2019-05-02 18:09:58 UTC+0000
.. 0xfffffa8002d9c780:svchost.exe                     892    504     17    427 2019-05-02 18:02:51 UTC+0000
... 0xfffffa800315eb30:dwm.exe                       1896    892      3     69 2019-05-02 18:03:09 UTC+0000
 0xfffffa8002264550:csrss.exe                         360    352      9    363 2019-05-03 06:32:34 UTC+0000
 0xfffffa8001252040:System                              4      0     88    624 2019-05-03 06:32:24 UTC+0000
 0xfffffa800234d8a0:smss.exe                          268      4      2     29 2019-05-03 06:32:24 UTC+0000
0xfffffa8003172b30:explorer.exe                      1860   1756     19    645 2019-05-02 18:03:09 UTC+0000
. 0xfffffa800300d700:VBoxTray.exe                    1600   1860     13    141 2019-05-02 18:03:25 UTC+0000
```

El proceso id 1860 explorer.exe tiene con ppid 1756 que no aparece dicho proceso padre.

```
└─# cat psscan.txt | grep 1756
0x000000005c572b30 explorer.exe       1860   1756 0x0000000049e30000 2019-05-02 18:03:09 UTC+0000
0x000000005c572b30 explorer.exe       1860   1756 0x0000000049e30000 2019-05-02 18:03:09 UTC+0000
```

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

Veamos procesos que se hayan ocultado a propósito.

volatility -f victim.raw --profile=Win7SP1x64 psxview -R

```
# volatility -f victim.raw --profile=Win7SP1x64 psxview -R
Volatility Foundation Volatility Framework 2.6
Offset(P)          Name                    PID pslist psscan thrdproc pspcid csrss session deskthrd ExitTime
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------- -------- --------
0x000000005c99c780 svchost.exe             892 True   True   False    True   True   True    True
0x000000005c40d700 VBoxTray.exe           1600 True   True   False    True   True   True    True
0x000000005c367060 SearchIndexer.         2180 True   True   False    True   True   True    True
0x000000005c657890 svchost.exe            1004 True   True   False    True   True   True    True
0x000000005c548b30 taskhost.exe           1788 True   True   False    True   True   True    True
0x000000005c72cb30 svchost.exe            1268 True   True   False    True   True   True    True
0x000000005ca1bb30 svchost.exe             752 True   True   False    True   True   True    True
0x000000005e0eeb30 taskhost.exe           1148 True   True   False    True   True   True    True
0x000000005cb71680 winlogon.exe            444 True   True   False    True   True   True    True
0x000000005cb601c0 wininit.exe             416 True   True   False    True   True   True    True
0x000000005c9be9e0 svchost.exe             920 True   True   False    True   True   True    True
0x000000005c572b30 explorer.exe           1860 True   True   False    True   True   True    True
0x000000005c562060 svchost.exe            1820 True   True   False    True   True   True    True
0x000000005c970650 svchost.exe             852 True   True   False    True   True   True    True
0x000000005c938b30 VBoxService.ex          688 True   True   False    True   True   True    True
0x000000005c3f6060 WmiPrvSE.exe           2876 True   True   False    True   True   True    True
0x000000005cfd9b30 lsass.exe               512 True   True   False    True   True   True    False
0x000000005cdcd3e0 svchost.exe             628 True   True   False    True   True   True    True
0x000000005c781460 svchost.exe            1368 True   True   False    True   True   True    True
0x000000005cfd81f0 lsm.exe                 520 True   True   False    True   True   True    False
0x000000005c63db30 svchost.exe             400 True   True   False    True   True   True    True
0x000000005c55eb30 dwm.exe                1896 True   True   False    True   True   True    True
0x000000005c9fdab0 spoolsv.exe            1140 True   True   False    True   True   True    True
0x000000005c371540 wmpnetwk.exe           2464 True   True   False    True   True   True    True
0x000000005c869b30 services.exe            504 True   True   False    True   True   True    False
0x000000005d34d8a0 smss.exe                268 True   True   False    True   Okay   Okay    Okay
0x000000005e252040 System                    4 True   True   False    True   Okay   Okay    Okay
0x000000005cfd67d0 csrss.exe               408 True   True   False    True   Okay   True    True
0x000000005d264550 csrss.exe               360 True   True   False    True   Okay   True    True
```

Pues no hay procesos ocultos según nos dice la columna pslist y psscan, ambos están en True.

Volcamos el proceso explorer.exe pid 1860

volatility -f victim.raw --profile=Win7SP1x64 cmdline | grep explorer -C 2

```
# volatility -f victim.raw --profile=Win7SP1x64 cmdline | grep explorer -C 2
Volatility Foundation Volatility Framework 2.6
Command line : "taskhost.exe"
************************************************************************
explorer.exe pid:   1860
Command line : C:\Windows\Explorer.EXE
************************************************************************
```

El Explorer se Lanza desde la carpeta correcta si bien puede estar infectado, vamos a volcar el proceso y analizarlo en virustotal.com

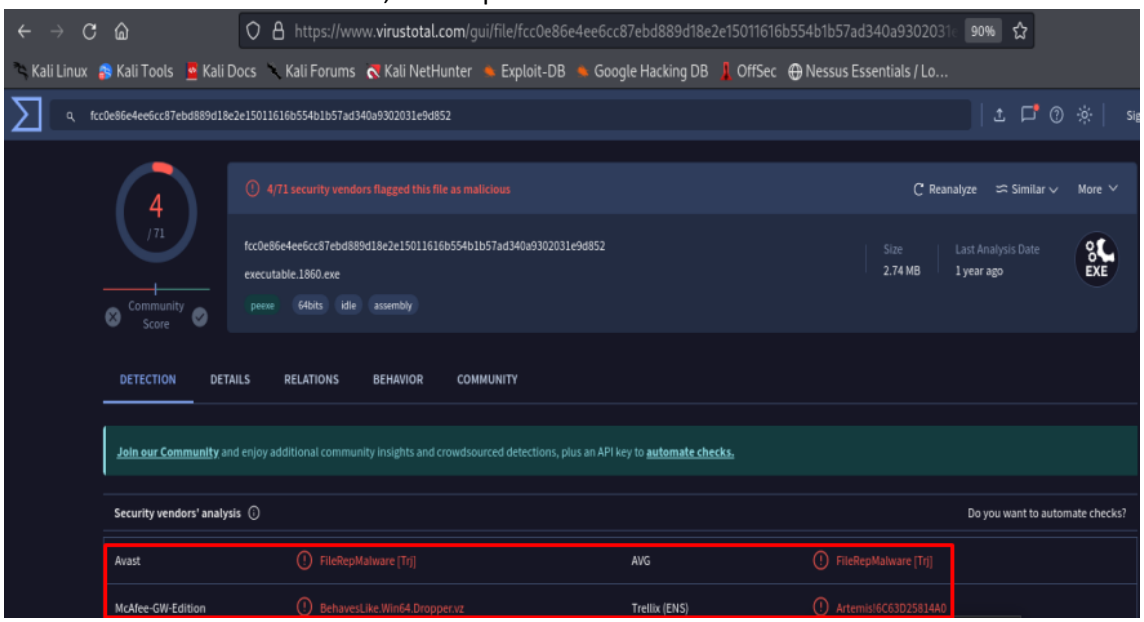
volatility -f victim.raw -p 1860 --profile=Win7SP1x64 procdump --dump-dir ./

```
# volatility -f victim.raw -p 1860 --profile=Win7SP1x64 procdump --dump-dir ./
Volatility Foundation Volatility Framework 2.6
Process(V)         ImageBase          Name                 Result
------------------ ------------------ -------------------- ------
0xfffffa8003172b30 0x00000000ffa20000 explorer.exe         OK: executable.1860.exe
```

ANÁLISIS FORENSE: TRY TO HACK ME - MEMORY WINDOWS

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

Análisis del fichero en virustotal, nos da positivo en cuatro antivirus



Vamos a volcar el contenido de la memoria de dicho proceso

```
# volatility -f victim.raw -p 1860 --profile=Win7SP1x64 memdump --dump-dir ./
```

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

Veamos que nos dice el plugin malfind

volatility -f victim.raw --profile=Win7SP1x64 malfind

```
Volatility Foundation Volatility Framework 2.6
Process: explorer.exe Pid: 1860 Address: 0x3ee0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x03ee0000  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x03ee0010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x03ee0020  00 00 ee 03 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x03ee0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................

0x03ee0000 0000              ADD [EAX], AL
0x03ee0002 0000              ADD [EAX], AL
0x03ee0004 0000              ADD [EAX], AL
0x03ee0006 0000              ADD [EAX], AL
0x03ee0008 0000              ADD [EAX], AL
0x03ee000a 0000              ADD [EAX], AL
0x03ee000c 0000              ADD [EAX], AL
0x03ee000e 0000              ADD [EAX], AL
0x03ee0010 0000              ADD [EAX], AL
0x03ee0012 0000              ADD [EAX], AL
0x03ee0014 0000              ADD [EAX], AL
0x03ee0016 0000              ADD [EAX], AL
0x03ee0018 0000              ADD [EAX], AL
0x03ee001a 0000              ADD [EAX], AL
0x03ee001c 0000              ADD [EAX], AL
0x03ee001e 0000              ADD [EAX], AL
0x03ee0020 0000              ADD [EAX], AL
0x03ee0022 ee                OUT DX, AL
0x03ee0023 0300              ADD EAX, [EAX]
0x03ee0025 0000              ADD [EAX], AL
0x03ee0027 0000              ADD [EAX], AL
0x03ee0029 0000              ADD [EAX], AL
```

Nos identifica el proceso pid 1860 explorer.exe como malware, como ya habíamos comprobado

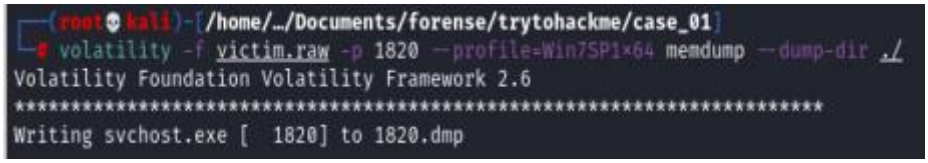
```
Process: svchost.exe Pid: 1820 Address: 0x24f0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 128, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x024f0000  20 00 00 00 e0 ff 07 00 0c 00 00 00 01 00 05 00   ................
0x024f0010  00 42 00 50 00 30 00 70 00 60 00 00 00 00 00 00   .B.P.0.p.`......
0x024f0020  48 8b 45 28 c7 00 00 00 00 00 c7 40 04 00 00 00   H.E(.......@....
0x024f0030  00 48 8b 45 28 48 8d 40 08 48 89 c2 48 8b 45 20   .H.E(H.@.H..H.E.

0x024f0000 2000              AND [EAX], AL
0x024f0002 0000              ADD [EAX], AL
0x024f0004 e0ff              LOOPNZ 0x24f0005
0x024f0006 07                POP ES
0x024f0007 000c00            ADD [EAX+EAX], CL
0x024f000a 0000              ADD [EAX], AL
0x024f000c 0100              ADD [EAX], EAX
0x024f000e 0500004200        ADD EAX, 0x420000
0x024f0013 50                PUSH EAX
0x024f0014 0030              ADD [EAX], DH
0x024f0016 007000            ADD [EAX+0x0], DH
0x024f0019 60                PUSHA
0x024f001a 0000              ADD [EAX], AL
0x024f001c 0000              ADD [EAX], AL
0x024f001e 0000              ADD [EAX], AL
0x024f0020 48                DEC EAX
0x024f0021 8b4528            MOV EAX, [EBP+0x28]
0x024f0024 c70000000000      MOV DWORD [EAX], 0x0
0x024f002a c7400400000000    MOV DWORD [EAX+0x4], 0x0
0x024f0031 48                DEC EAX
0x024f0032 8b4528            MOV EAX, [EBP+0x28]
0x024f0035 48                DEC EAX
0x024f0036 8d4008            LEA EAX, [EAX+0x8]
0x024f0039 48                DEC EAX
0x024f003a 89c2              MOV EDX, EAX
```

Pero nos muestra otro proceso que no teníamos identificado previamente como malware, pid 1820 svchost.com . Servicio que se encarga de los servicios de red, vamos a hacer un volcado del proceso y ver lo que esconde.

$ volatility -f victim.raw -p 1820 --profile=Win7SP1x64 memdump --dump-dir ./



Veamos si encontramos algún acceso a alguna url en el volcado de memoria del proceso pid 1820.

Con el siguiente comando obtenemos cualquier dirección ipv4 registrada en el servicio svchost.exe (no es muy útil el grep, pero algo permite buscar 😉)

$ strings 1820.dmp | grep -xE '((25[0-5]|2[0-4][0-9]|1[0-9][0-9]|[1-9]?[0-9])\.){3}(25[0-5]|2[0-4][0-9]|1[0-9][0-9]|[1-9]?[0-9])'

Aquí encontramos varias url y direcciones ip donde hay conexiones con los servicios svchost.exe

ANÁLISIS FORENSE: TRY TO HACK ME - MEMORY WINDOWS

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

Recursos:

https://tryhackme.com/r/room/forensics