

**XIII
JORNADAS
STIC
CCN-CERT**



**Reto de
Jörmundgander**

**COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD**

#XIIIJORNADASCCNCERT



Germán Sánchez Garcés

Entelgy Innotec Security

german.sanchez@innotec.security

Índice

1. Descripción del reto
2. Identificación del sistema operativo bajo estudio
3. Búsqueda de anomalías en conexiones, procesos, MFT...
4. Revisión de los controladores del Kernel
5. Extracción del binario sospechoso
6. Análisis del binario
7. Descifrado y solución al reto!

Descripción del reto

Jörmundgander (300pts)

- Se ha tenido constancia del compromiso de un servidor de la empresa **Biffco Enterprises**. El triaje inicial no ha encontrado indicios de la intrusión. ¿Puedes encontrar algún rastro de la actividad del atacante?
- Los usuarios reciben un volcado de memoria llamado memory.1f785001.img
- MD5: d356f0ddf32a50d40b5ec696f4807324
- Es un equipo Windows y deberán de encontrar el flag.
- *Pista! Mira en el **ring 0**.*



Análisis de la memoria RAM

¿Qué queremos encontrar?

- Malware
 - Exploits
 - Packers
 - Downloaders
 - Droppers
 - Rootkits
 - ...
- ¿Qué sucede en el sistema con uno de estos?
 - Creación, modificación, borrado de archivos (MFT)
 - Conexiones
 - Persistencia
 - Servicios, registros..
 - Procesos
 - ...



Análisis de la memoria RAM

¿Alternativas?

- **Volatility**
 - Memory dumps.
 - Archivo de hibernación de Windows.
- **Rekall**
 - Memory dumps.



Identificación del sistema operativo

- *volatility -f memory.1f785001.img imageinfo*

```
german@german:~/CCN$ volatility -f memory.1f785001.img imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO : volatility.debug : Determining profile based on KDBG search...
      Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_24000
      AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
      AS Layer2 : FileAddressSpace (/home/german/CCN/memory.1f785001.img)
      PAE type : No PAE
      DTB : 0x187000L
      KDBG : 0xf800027fd0f0L
      Number of Processors : 1
      Image Type (Service Pack) : 1
      KPCR for CPU 0 : 0xfffff800027fed00L
      KUSER_SHARED_DATA : 0xfffff78000000000L
      Image date and time : 2019-06-03 19:36:32 UTC+0000
      Image local date and time : 2019-06-03 21:36:32 +0200
```

- *volatility -f memory.1f785001.img kdbgscan*

```
german@german:~/CCN$ volatility -f memory.1f785001.img kdbgscan
Volatility Foundation Volatility Framework 2.6.1
*****
Instantiating KDBG using: /home/german/CCN/memory.1f785001.img WinXPSP2x86 (5.1.0 32bit)
Offset (P) : 0x27fd0f0
KDBG owner tag check : True
Profile suggestion (KDBGHeader): Win7SP1x64
PsActiveProcessHead : 0x2834420
PsLoadedModuleList : 0x2852730
KernelBase : 0xfffff8000260b000
*****
```

Revisión de las conexiones de red

- `volatility -f memory.1f785001.img --profile=Win7SP1x64 netscan`

```

german@operaciones:~/CCNS$ volatility -f memory.1f785001.img --profile=Win7SP1x64 netscan
Volatility Foundation Volatility Framework 2.6
Offset(P)      Proto  Local Address      Foreign Address    State      Pid    Owner              Created
0x59f3cf0      TCPv4  -:49439            151.139.128.14:80  CLOSED    3848   TeamViewer.exe
0x7d6695a0     UDPv4  0.0.0.0:0          *:.*               1052     svchost.exe        2019-06-03 19:33:11 UTC+0000
0x7d6695a0     UDPv6  :::0              *:.*               1052     svchost.exe        2019-06-03 19:33:11 UTC+0000
0x7d6a2a80     UDPv4  0.0.0.0:63589      *:.*               3696     TeamViewer_Ser     2019-06-03 19:34:46 UTC+0000
0x7d8b3010     TCPv4  127.0.0.1:49454    127.0.0.1:49455   ESTABLISHED 3848   TeamViewer.exe
0x7db98aa0     UDPv6  ::1:1900           *:.*               1328     svchost.exe        2019-06-03 19:33:17 UTC+0000
0x7dbaa7d0     UDPv4  10.0.2.15:1900     *:.*               1328     svchost.exe        2019-06-03 19:33:17 UTC+0000
0x7dbec3a0     UDPv4  127.0.0.1:1900     *:.*               1328     svchost.exe        2019-06-03 19:33:17 UTC+0000
0x7de084d0     UDPv4  10.0.2.15:138      *:.*               4        System             2019-06-03 19:33:10 UTC+0000
0x7e0b2990     UDPv4  0.0.0.0:5355       *:.*               1052     svchost.exe        2019-06-03 19:33:13 UTC+0000
0x7e0b2990     UDPv6  :::5355            *:.*               1052     svchost.exe        2019-06-03 19:33:13 UTC+0000
0x7e256010     UDPv4  10.0.2.15:137      *:.*               4        System             2019-06-03 19:33:10 UTC+0000
0x7dba1a60     TCPv4  0.0.0.0:49156      0.0.0.0:0         LISTENING   508     lsass.exe
0x7dba1a60     TCPv6  :::49156           :::0               LISTENING   508     lsass.exe
0x7dba1cd0     TCPv4  0.0.0.0:49156      0.0.0.0:0         LISTENING   508     lsass.exe
0x7dc0e250     TCPv4  0.0.0.0:49155      0.0.0.0:0         LISTENING   492     services.exe
0x7dc10340     TCPv4  0.0.0.0:445        0.0.0.0:0         LISTENING   4        System
0x7dc10340     TCPv6  :::445             :::0               LISTENING   4        System
0x7dd146e0     TCPv4  0.0.0.0:49155      0.0.0.0:0         LISTENING   492     services.exe
0x7dd146e0     TCPv6  :::49155           :::0               LISTENING   492     services.exe
0x7e0398d0     TCPv4  0.0.0.0:135        0.0.0.0:0         LISTENING   732     svchost.exe
0x7e03dc90     TCPv4  0.0.0.0:135        0.0.0.0:0         LISTENING   732     svchost.exe
0x7e03dc90     TCPv6  :::135             :::0               LISTENING   732     svchost.exe

```

Inyección en secciones ejecutables

- `volatility -f memory.1f785001.img --profile=Win7SP1x64 malfind`

```

german@operaciones:~/CCN$ volatility -f memory.1f785001.img --profile=Win7SP1x64 malfind
Volatility Foundation Volatility Framework 2.6
Process: mscorsvw.exe Pid: 2636 Address: 0x7d0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, PrivateMemory: 1, Protection: 6

0x007d0000  48 66 10 e6 1d 9a 00 01 ee ff ee ff 00 00 00 00  Hf.....
0x007d0010  a8 00 7d 00 a8 00 7d 00 00 00 7d 00 00 00 7d 00  ..}...}...}...}.
0x007d0020  40 00 00 00 88 05 7d 00 00 00 81 00 3f 00 00 00  @.....}.....?...
0x007d0030  01 00 00 00 00 00 00 00 f0 0f 7d 00 f0 0f 7d 00  .....}...}.

0x007d0000 48          DEC EAX
0x007d0001 6610e6      ADC DH, AH
0x007d0004 1d9a0001ee  SBB EAX, 0xee01009a
0x007d0009 ff          DB 0xff
0x007d000a ee          OUT DX, AL
0x007d000b ff00      INC DWORD [EAX]
0x007d000d 0000      ADD [EAX], AL
0x007d000f 00a8007d00a8  ADD [EAX-0x57ff8300], CH
0x007d0015 007d00      ADD [EBP+0x0], BH
0x007d0018 0000      ADD [EAX], AL

```

- `volatility -f memory.1f785001.img --profile=Win7SP1x64 malfind | grep -C 5 'MZ'`

Búsqueda de *mutex* conocidos

- `volatility -f memory.1f785001.img --profile=Win7SP1x64 mutantscan`

```

0x000000007f8be9b0      2      1      1 0x0000000000000000      AMResourceMutex3
0x000000007f900c90      3      2      1 0x0000000000000000      DBWinMutex
0x000000007f901fc0      2      1      0 0xfffffa8001f10ac0 325...452 ADAP_WMI_ENTRY
0x000000007f9041e0      2      1      1 0x0000000000000000      RstrMgr-3887CAB8-533F-4C85-B0DC-3E5639F8D511-Session0000
0x000000007f9044b0      2      1      1 0x0000000000000000      process_hacker2_setup_mutex
0x000000007f905f00      2      1      1 0x0000000000000000      RstrMgr3887CAB8-533F-4C85-B0DC-3E5639F8D511
0x000000007f922fc0      1      1      1 0x0000000000000000
0x000000007f924270      1      1      1 0x0000000000000000
0x000000007f9588a0      4      3      1 0x0000000000000000      TeamViewerHooks Mutex5

```

Procesos y sus padres e hijos...

- `volatility -f memory.1f785001.img --profile=Win7SP1x64 pslist... (pstree)`

```

german@operaciones:~/CCN$ volatility -f memory.1f785001.img --profile=Win7SP1x64 pstree
Volatility Foundation Volatility Framework 2.6
Name                               Pid    PPid    Thds    Hnds Time
-----
0xfffffa80038aa260:explorer.exe     2692   2688    36     840 2019-06-03 19:33:50 UTC+0000
. 0xfffffa8001ed0760:cmd.exe         3456   2692     1      20 2019-06-03 19:35:49 UTC+0000
.. 0xfffffa8001b97600:powershell.exe 4024   3456     9     258 2019-06-03 19:36:00 UTC+0000
. 0xfffffa8001e7bb10:cmd.exe         3416   2692     1      23 2019-06-03 19:36:18 UTC+0000
.. 0xfffffa8001e19060:Memoryze.exe   3828   3416     2      97 2019-06-03 19:36:32 UTC+0000
. 0xfffffa8003a25060:VBoxTray.exe    1340   2692    12     150 2019-06-03 19:33:51 UTC+0000
. 0xfffffa8001fa3b10:taskmgr.exe     3172   2692     7     124 2019-06-03 19:35:17 UTC+0000
. 0xfffffa8003a90750:BraveBrowserSe 1712   2692     4     123 2019-06-03 19:33:58 UTC+0000
.. 0xfffffa8001c90b10:BraveUpdate.ex 1632   1712     4     156 2019-06-03 19:34:17 UTC+0000
... 0xfffffa8001b57060:BraveUpdateSet 472    1632     1      59 2019-06-03 19:34:24 UTC+0000
.... 0xfffffa8001cdbb10:BraveUpdate.ex 1720   472      4     156 2019-06-03 19:34:25 UTC+0000
..... 0xfffffa8001b81060:BraveUpdate.ex 804    1720     6     131 2019-06-03 19:34:26 UTC+0000
. 0xfffffa8001b72b10:iexplore.exe    444    2692    12     485 2019-06-03 19:34:01 UTC+0000
.. 0xfffffa8001c3fb10:iexplore.exe   2680   444     30     666 2019-06-03 19:34:03 UTC+0000
. 0xfffffa8001d48b10:processhacker- 3516   2692     1      47 2019-06-03 19:35:05 UTC+0000
.. 0xfffffa8001c97b10:processhacker- 3548   3516     2     137 2019-06-03 19:35:05 UTC+0000
... 0xfffffa8001f16060:processhacker- 3444   3548     1      47 2019-06-03 19:35:07 UTC+0000
.... 0xfffffa8001e71060:processhacker- 3588   3444     1      99 2019-06-03 19:35:07 UTC+0000

```

Revisión de la MFT

Carpeta de descarga...

- `volatility -f memory.1f785001.img --profile=Win7SP1x64 mftparser > mftparser.txt`

\$FILE_NAME Creation	Modified	MFT Altered	Name/Path
2019-06-03 19:32:39 UTC+0000	2019-06-03 19:32:39 UTC+0000	2019-06-03 19:32:39 UTC+0000	Users\Sam\Downloads\Battle.net-Setup.exe
2019-06-03 19:32:39 UTC+0000	2019-06-03 19:32:39 UTC+0000	2019-06-03 19:32:39 UTC+0000	Users\Sam\Downloads\Install Lightroom 5.exe
2019-06-03 19:32:39 UTC+0000	2019-06-03 19:32:39 UTC+0000	2019-06-03 19:32:39 UTC+0000	Users\Sam\Downloads\jdk-11.0.3_windows-x64_bin.exe
2019-06-03 19:32:39 UTC+0000	2019-06-03 19:32:39 UTC+0000	2019-06-03 19:32:39 UTC+0000	Users\Sam\Downloads\BraveBrowserSetup.exe
2019-06-03 19:32:39 UTC+0000	2019-06-03 19:32:39 UTC+0000	2019-06-03 19:32:39 UTC+0000	Users\Sam\Downloads\Battle.net-Setup.exe
2019-06-03 19:32:40 UTC+0000	2019-06-03 19:32:40 UTC+0000	2019-06-03 19:32:40 UTC+0000	Users\Sam\Downloads\md5sum.exe
2019-06-03 19:32:40 UTC+0000	2019-06-03 19:32:40 UTC+0000	2019-06-03 19:32:40 UTC+0000	Users\Sam\Downloads\processhacker-2.39-setup.exe
2019-06-03 19:32:40 UTC+0000	2019-06-03 19:32:40 UTC+0000	2019-06-03 19:32:40 UTC+0000	Users\Sam\Downloads\TeamViewer_Setup.exe

- `volatility -f memory.1f785001.img --profile=Win7SP1x64 pslist`

0xfffffa8003a25060	VBoxTray.exe	1340	2692	12	150	2	0	2019-06-03 19:33:51 UTC+0000
0xfffffa8003a90750	BraveBrowserSe	1712	2692	4	123	2	1	2019-06-03 19:33:58 UTC+0000
0xfffffa8001b72b10	iexplore.exe	444	2692	12	485	2	0	2019-06-03 19:34:01 UTC+0000
0xfffffa8001a257e0	taskhost.exe	820	492	5	173	2	0	2019-06-03 19:34:03 UTC+0000
0xfffffa8001c3fb10	iexplore.exe	2680	444	30	666	2	1	2019-06-03 19:34:03 UTC+0000
0xfffffa8001c6fb10	WmiPrvSE.exe	2376	616	8	182	0	0	2019-06-03 19:34:06 UTC+0000
0xfffffa8001c90b10	BraveUpdate.ex	1632	1712	4	156	2	1	2019-06-03 19:34:17 UTC+0000
0xfffffa8001d1eb10	Battle.net-Set	3000	1040	13	320	2	1	2019-06-03 19:34:22 UTC+0000
0xfffffa8001d525f0	SearchProtocol	2380	1764	7	265	2	0	2019-06-03 19:34:24 UTC+0000
0xfffffa8001b57060	BraveUpdateSet	472	1632	1	59	2	1	2019-06-03 19:34:24 UTC+0000
0xfffffa8001cdbb10	BraveUpdate.ex	1720	472	4	156	2	1	2019-06-03 19:34:25 UTC+0000
0xfffffa8001b81060	BraveUpdate.ex	804	1720	6	131	2	1	2019-06-03 19:34:26 UTC+0000
0xfffffa8001e8db10	BraveUpdate.ex	1296	492	10	353	0	1	2019-06-03 19:34:26 UTC+0000

Revisión de la MFT

Papelera de reciclaje

- Realización de búsquedas concisas
 - Downloads
 - \$Recycle.Bin
 - ...

```

$FILE_NAME
Creation                               Modified                               MFT Altered
-----
2019-06-03 19:34:40 UTC+0000 2019-06-03 19:34:40 UTC+0000 2019-06-03 19:34:40 UTC+0000

Access Date                           Name/Path
-----
2019-06-03 19:34:40 UTC+0000 $Recycle.Bin\S-1-5--1\IT0A244.sys

$DATA
0000000000: 01 00 00 00 00 00 00 00 00 16 00 00 00 00 00 00 .....
0000000010: b0 f4 40 63 43 1a d5 01 43 00 3a 00 5c 00 55 00 ..@cC...C.:.\.U.
0000000020: 73 00 65 00 72 00 73 00 5c 00 53 00 61 00 6d 00 s.e.r.s.\.S.a.m.
0000000030: 5c 00 44 00 6f 00 77 00 6e 00 6c 00 6f 00 61 00 \.D.o.w.n.l.o.a.
0000000040: 64 00 73 00 5c 00 6e 00 70 00 66 00 2e 00 73 00 d.s.\.n.p.f...s.
0000000050: 79 00 73 00 00 00 00 00 00 00 00 00 00 00 00 00 y.s.....

```

Módulos (Controladores de Kernel)

Obtención del nombre de los módulos en ejecución

- *volatility -f memory.1f785001.img --profile=Win7SP1x64 modules*
- (Aparentemente sin información de interés)

```

german@german:~/CCN$ volatility -f memory.1f785001.img --profile=Win7SP1x64 modules
Volatility Foundation Volatility Framework 2.6.1
Offset(V)      Name                Base                Size File
-----
0xffffffffa800183f890 ntoskrnl.exe        0xffffffff8000260b000 0x5ec000 \SystemRoot\system32\ntoskrnl.exe
0xffffffffa80018390d0 hal.dll              0xffffffff80002bf7000 0x49000 \SystemRoot\system32\hal.dll
0xffffffffa800183f7b0 kdcom.dll            0xffffffff80000ba9000 0xa000 \SystemRoot\system32\kdcom.dll
0xffffffffa800183f6c0 mcupdate.dll         0xffffffff88000ca7000 0x4f000 \SystemRoot\system32\mcupdate GenuineIntel.dll
0xffffffffa8001840010 PSHEd.dll            0xffffffff88000cf6000 0x14000 \SystemRoot\system32\PSHEd.dll
0xffffffffa8001840f20 CLFS.SYS             0xffffffff88000d0a000 0x5e000 \SystemRoot\system32\CLFS.SYS
0xffffffffa8001840e40 CI.dll                      0xffffffff88000d68000 0x75000 \SystemRoot\system32\CI.dll
0xffffffffa8001840d40 Wdf01000.sys         0xffffffff88000e9c000 0xc2000 \SystemRoot\system32\drivers\Wdf01000.sys
0xffffffffa8001840c60 WDFLDR.SYS          0xffffffff88000f5e000 0x10000 \SystemRoot\system32\drivers\WDFLDR.SYS
0xffffffffa8001840b70 ACPI.sys                 0xffffffff88000f6e000 0x57000 \SystemRoot\system32\drivers\ACPI.sys
0xffffffffa8001840a90 WMILIB.SYS           0xffffffff88000fc5000 0x9000 \SystemRoot\system32\drivers\WMILIB.SYS
0xffffffffa80018409a0 msisadrv.sys          0xffffffff88000fce000 0xa000 \SystemRoot\system32\drivers\msisadrv.sys
0xffffffffa80018408c0 pci.sys                      0xffffffff88000e00000 0x33000 \SystemRoot\system32\drivers\pci.sys
0xffffffffa80018407d0 vdrvroot.sys        0xffffffff88000e33000 0xd000 \SystemRoot\system32\drivers\vdrvroot.sys
0xffffffffa80018406e0 partmgr.sys          0xffffffff88000e40000 0x15000 \SystemRoot\System32\drivers\partmgr.sys
0xffffffffa80018405f0 compbatt.sys        0xffffffff88000e55000 0x9000 \SystemRoot\system32\DRIVERS\compbatt.sys
0xffffffffa8001840510 BATTC.SYS           0xffffffff88000e5e000 0xc000 \SystemRoot\system32\DRIVERS\BATTC.SYS
0xffffffffa8001840430 volmgr.sys          0xffffffff88000e6a000 0x15000 \SystemRoot\system32\drivers\volmgr.sys
0xffffffffa8001840340 volmgrx.sys         0xffffffff88000e00000 0x5c000 \SystemRoot\System32\drivers\volmgrx.sys
0xffffffffa8001840250 mountmgr.sys       0xffffffff88000e7f000 0x1a000 \SystemRoot\System32\drivers\mountmgr.sys

```

Módulos (Controladores de Kernel)

Obtención del nombre de los módulos en ejecución

- *volatility -f memory.1f785001.img --profile=Win7SP1x64 modscan*
- (Aparentemente sin información de interés)

```

german@german:~/CCN$ volatility -f memory.1f785001.img --profile=Win7SP1x64 modscan
Volatility Foundation Volatility Framework 2.6.1
Offset(P)      Name      Base      Size File
-----
0x000000007cd8ae60 HDAudBus.sys 0xfffff88003c5d000 0x24000 \SystemRoot\system32\DRIVERS\HDAudBus.sys
0x000000007d826e60 HIDCLASS.SYS 0xfffff880025b4000 0x19000 \SystemRoot\system32\DRIVERS\HIDCLASS.SYS
0x000000007d97c550 mouhid.sys 0xfffff880025cd000 0xd000 \SystemRoot\system32\DRIVERS\mouhid.sys
0x000000007dc81170 usbhub.sys 0xfffff88002cd1000 0x5a000 \SystemRoot\system32\DRIVERS\usbhub.sys
0x000000007dcdcl80 portcls.sys 0xfffff88002d9c000 0x3d000 \SystemRoot\system32\drivers\portcls.sys
0x000000007dcde180 drmk.sys 0xfffff88002dd9000 0x22000 \SystemRoot\system32\drivers\drmk.sys
0x000000007dce4010 dxg.sys 0xfffff960005b0000 0x1e000 \SystemRoot\System32\drivers\dxg.sys
0x000000007dce5180 ksthunk.sys 0xfffff88002c00000 0x6000 \SystemRoot\system32\drivers\ksthunk.sys
0x000000007dce72b0 VBoxDisp.dll 0xfffff96000910000 0x19000 \SystemRoot\System32\VBoxDisp.dll
0x000000007dd10180 hidusb.sys 0xfffff880025a6000 0xe000 \SystemRoot\system32\DRIVERS\hidusb.sys
0x000000007dd12170 HIDPARSE.SYS 0xfffff88002c82000 0x9000 \SystemRoot\system32\DRIVERS\HIDPARSE.SYS
0x000000007dd40170 crashdmp.sys 0xfffff88002c23000 0xe000 \SystemRoot\System32\Drivers\crashdmp.sys
0x000000007dd42170 dump_msahci.sys 0xfffff88002c3d000 0xb000 \SystemRoot\System32\Drivers\dump_msahci.sys
0x000000007dd48170 dump_dumpfve.sys 0xfffff88002c48000 0x13000 \SystemRoot\System32\Drivers\dump_dumpfve.sys
0x000000007ddb5290 NDProxy.SYS 0xfffff88002d2b000 0x15000 \SystemRoot\System32\Drivers\NDProxy.SYS
0x000000007ddcc4a0 HdAudio.sys 0xfffff88002d40000 0x5c000 \SystemRoot\system32\drivers\HdAudio.sys

```

Módulos (Controladores de Kernel)

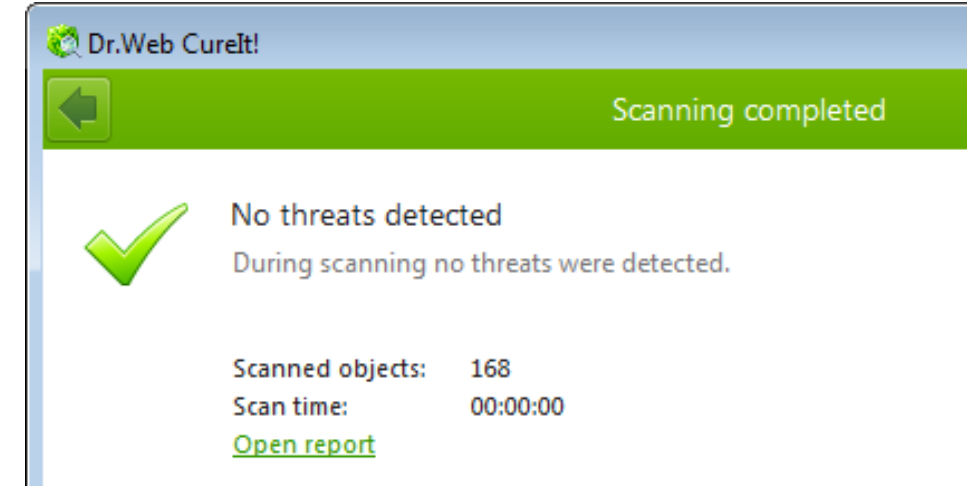
Revisión de los *drivers*

- `volatility --profile Win7SP1x64 -f memory.1f785001.img moddump -D drivers/`
- Solución rápida y ágil... (Antivirus)

```

german@german:~/CCN$ volatility --profile Win7SP0x64 -f memory.1f785001.img moddump -D drivers/
Volatility Foundation Volatility Framework 2.6.1
Module Base      Module Name      Result
-----
0xffffffff8000260b000 ntoskrnl.exe     OK: driver.fffff8000260b000.sys
0xffffffff80002bf7000 hal.dll           OK: driver.fffff80002bf7000.sys
0xffffffff88002dd9000 drmk.sys          OK: driver.fffff88002dd9000.sys
0xffffffff88003d90000 kbdclass.sys      OK: driver.fffff88003d90000.sys
0xffffffff88003aba000 afd.sys           OK: driver.fffff88003aba000.sys
0xffffffff880024d1000 bowser.sys         OK: driver.fffff880024d1000.sys
0xffffffff88003c5d000 HDAudBus.sys      OK: driver.fffff88003c5d000.sys
0xffffffff8800295b000 srv.sys           OK: driver.fffff8800295b000.sys
0xffffffff88003d9f000 VBoxMouse.sys     OK: driver.fffff88003d9f000.sys
0xffffffff88003c00000 VBoxVideo.sys      OK: driver.fffff88003c00000.sys
0xffffffff88000fe1000 msahci.sys         OK: driver.fffff88000fe1000.sys
0xffffffff880019c2000 vga.sys           OK: driver.fffff880019c2000.sys
0xffffffff88002ca6000 monitor.sys        OK: driver.fffff88002ca6000.sys
0xffffffff88002c23000 crashdump.sys      OK: driver.fffff88002c23000.sys
0xffffffff88004104000 rasl2tp.sys        OK: driver.fffff88004104000.sys
0xffffffff88003d4c000 tunnel.sys          OK: driver.fffff88003d4c000.sys
0xffffffff880041c6000 luafv.sys          OK: driver.fffff880041c6000.sys
0xffffffff88000ca7000 mcupdate.dll      OK: driver.fffff88000ca7000.sys
0xffffffff88003b88000 wfplwf.sys          OK: driver.fffff88003b88000.sys

```



Módulos Descargados

Módulos descargados recientemente.

- *volatility -f memory.1f785001.img --profile=Win7SP1x64 unloadedmodules*
- El *driver* vulnerable de **VirtualBox** pudo ser utilizado para cargar el código dañino como se hizo en la campaña de Turla con **Uroburos**...

```
german@german:~/CCN$ volatility -f memory.1f785001.img --profile=Win7SP0x64 unloadedmodules
Volatility Foundation Volatility Framework 2.6.1
Name                               StartAddress                     EndAddress                       Time
-----
dump_dumpfve.sys                   0xffffffff88001975000             0xffffffff88001988000             2019-06-03 18:59:41
dump_msahci.sys                    0xffffffff8800196a000             0xffffffff88001975000             2019-06-03 18:59:41
dump_pciidex.sys                   0xffffffff8800195e000             0xffffffff8800196a000             2019-06-03 18:59:41
crashdmp.sys                       0xffffffff88001950000             0xffffffff8800195e000             2019-06-03 18:59:41
mouhid.sys                         0xffffffff88002c8d000             0xffffffff88002c9a000             2019-06-03 19:00:48
hidusb.sys                         0xffffffff88002c5b000             0xffffffff88002c69000             2019-06-03 19:00:48
HIDCLASS.SYS                      0xffffffff88002c69000             0xffffffff88002c82000             2019-06-03 19:00:48
USBBD.SYS                         0xffffffff88002c8b000             0xffffffff88002c8d000             2019-06-03 19:00:48
VBoxDrv.sys                       0xffffffff880068aa000             0xffffffff880068b9000             2019-06-03 19:33:40
```

Revisión de los drivers

Ausencia de VBoxDrv entre los módulos cargados

- `volatility --profile Win7SP1x64 -f memory.1f785001.img modules | grep VBox`
- `volatility --profile Win7SP1x64 -f memory.1f785001.img modscan | grep VBox`

```

german@german:~/CCN$ volatility --profile Win7SP1x64 -f memory.1f785001.img modules | grep VBox
Volatility Foundation Volatility Framework 2.6.1
0xffffffffa80018416b0 VBoxGuest.sys 0xffffffff88001072000 0x34000 \SystemRoot\system32\DRIVERS\VBoxGuest.sys
0xffffffffa8002b0d220 VBoxSF.sys 0xffffffff88003a00000 0x56000 \SystemRoot\System32\drivers\VBoxSF.sys
0xffffffffa8002e34460 VBoxMouse.sys 0xffffffff88003d9f000 0x33000 \SystemRoot\system32\DRIVERS\VBoxMouse.sys
0xffffffffa8002b83bb0 VBoxVideo.sys 0xffffffff88003c00000 0x39000 \SystemRoot\system32\DRIVERS\VBoxVideo.sys
0xffffffffa8003ae72b0 VBoxDisp.dll 0xffffffff96000910000 0x19000 \SystemRoot\System32\VBoxDisp.dll
german@german:~/CCN$ volatility --profile Win7SP1x64 -f memory.1f785001.img modscan | grep VBox
Volatility Foundation Volatility Framework 2.6.1
0x000000007dce72b0 VBoxDisp.dll 0xffffffff96000910000 0x19000 \SystemRoot\System32\VBoxDisp.dll
0x000000007e834460 VBoxMouse.sys 0xffffffff88003d9f000 0x33000 \SystemRoot\system32\DRIVERS\VBoxMouse.sys
0x000000007ed0d220 VBoxSF.sys 0xffffffff88003a00000 0x56000 \SystemRoot\System32\drivers\VBoxSF.sys
0x000000007ed83bb0 VBoxVideo.sys 0xffffffff88003c00000 0x39000 \SystemRoot\system32\DRIVERS\VBoxVideo.sys
0x000000007ffbe6b0 VBoxGuest.sys 0xffffffff88001072000 0x34000 \SystemRoot\system32\DRIVERS\VBoxGuest.sys

```

Kernel Patch Protection

Protección contra revisiones del núcleo

- **PatchGuard**

- Implantado por **Microsoft** en 2005, para sistemas de 64 bits.
- Comprueba la integridad del núcleo de Windows para asegurarse de que no hay partes críticas modificadas. Si se detecta una modificación nociva en el *kernel*, la función **KeBugCheckEx()** se ejecuta, llamándose con un argumento con el valor **0x109** (CRITICAL_STRUCTURE_CORRUPTION) como código de error. El resultado es un cierre del sistema con una pantalla azul.

- **Malware Uroburos**

- Aprovechaba la existencia de una vulnerabilidad en un controlador legítimamente firmado, conocido como (VBoxDrv.sys) y perteneciente a **Oracle VirtualBox** en su versión 1.6.2.
- Puede ser utilizado para realizar un *hook* en la llamada a la función KeBugCheckEx() y evitar finalmente a **PatchGuard** mediante su *bypass*.

Driver Scan

Búsqueda de drivers mediante el escaneo de etiquetas de grupo

- `volatility -f memory.1f785001.img --profile=Win7SP1x64 driverscan`
- Se identifica el nombre de *driver* **\Driver\npf** con dirección inválida en el espacio del Kernel.

```

german@german:~/CCN$ volatility -f memory.1f785001.img --profile=Win7SP0x64 driverscan
Volatility Foundation Volatility Framework 2.6.1
Offset(P)      #Ptr      #Hnd Start      Size Service Key      Name      Driver Name
-----
0x000000007dba77b0      3      0 0x0000000000000000      0x0 \Driver\npf      npf      \Driver\npf
0x000000007dc83990      4      0 0xffffffff88002c06000      0x1d000 cdfs      cdfs      \FileSystem\cdfs
0x000000007dd0a470      3      0 0xffffffff880025cd000      0xd000 mouhid      mouhid      \Driver\mouhid
0x000000007ddb0550      5      0 0xffffffff88002cd1000      0x5a000 usbhub      usbhub      \Driver\usbhub
0x000000007ddbc060      3      0 0xffffffff88002d40000      0x5c000 HdAudAddService      HdAud...vice \Driver\HdAudAddService
0x000000007ddc6060      3      0 0xffffffff88002c00000      0x5200 ksthunk      ksthunk      \Driver\ksthunk
0x000000007ddc7550      3      0 0xffffffff88002d2b000      0x15000 NDPProxy      NDPProxy      \Driver\NDProxy
0x000000007de67b10      4      0 0xffffffff880025a6000      0xe000 HidUsb      HidUsb      \Driver\HidUsb
0x000000007deb5af0      3      0 0xffffffff880024d1000      0x1e000 bowser      bowser      \FileSystem\bowser
0x000000007deb8060      3      0 0xffffffff880024ef000      0x18000 mpsdrv      mpsdrv      \Driver\mpsdrv
0x000000007debfa00      2      0 0xffffffff88002534000      0x4e000 mrxsmb10      mrxsmb10      \FileSystem\mrxsmb10
0x000000007debfa60      2      0 0xffffffff88002582000      0x24000 mrxsmb20      mrxsmb20      \FileSystem\mrxsmb20
0x000000007df2c060      3      0 0xffffffff88002805000      0xaa000 PEAUTH      PEAUTH      \Driver\PEAUTH
0x000000007df2d780      2      0 0xffffffff880028e0000      0x12000 tcpipreg      tcpipreg      \Driver\tcpipreg
0x000000007df30590      4      0 0xffffffff880028af000      0x31000 srvnet      srvnet      \FileSystem\srvnet

```

Driver Module

- *volatility -f memory.1f785001.img --profile=Win7SP1x64 drivermodule*
- El objeto **npf** no tiene un driver asociado. ¿Código dañino inyectado en el kernel?

```

german@german:~/CCN$ volatility -f memory.1f785001.img --profile=Win7SP1x64 drivermodule
Volatility Foundation Volatility Framework 2.6.1
Module                               Driver                               Alt. Name                           Service Key
-----
UNKNOWN                             npf                                  \Driver\npf                         \Driver\npf
cdfs.sys                            cdfs                                 cdfs                                 \FileSystem\cdfs
mouhid.sys                          mouhid                              mouhid                              \Driver\mouhid
usbhub.sys                          usbhub                              usbhub                              \Driver\usbhub
HdAudio.sys                         HdAudAddService                    HdAudAddService                    \Driver\HdAudAddService
ksthunk.sys                         ksthunk                            ksthunk                            \Driver\ksthunk
NDProxy.SYS                         NDProxy                             NDProxy                             \Driver\NDProxy
hidusb.sys                          HidUsb                              HidUsb                              \Driver\HidUsb
bowser.sys                          bowser                              bowser                              \FileSystem\bowser
mpsdrv.sys                          mpsdrv                              mpsdrv                              \Driver\mpsdrv
mrxsmb10.sys                        mrxsmb10                           mrxsmb10                           \FileSystem\mrxsmb10
mrxsmb20.sys                        mrxsmb20                           mrxsmb20                           \FileSystem\mrxsmb20
peauth.sys                          PEAUTH                             PEAUTH                             \Driver\PEAUTH
tcpipreg.sys                        tcpipreg                            tcpipreg                            \Driver\tcpipreg
srvnet.sys                          srvnet                              srvnet                              \FileSystem\srvnet
srv2.sys                            srv2                                srv2                                \FileSystem\srv2
srv.sys                             srv                                  srv                                  \FileSystem\srv
luafl.sys                           luafl                               luafl                               \FileSystem\luafl

```

Driver IRP

- *volatility -f memory.1f785001.img --profile=Win7SP1x64 driverirp*
- Los punteros de la estructura IRP apuntan a secciones desconocidas...

```
german@german:~/CCN$ volatility --profile Win7SP1x64 -f memory.1f785001.img driverirp | grep npf -a32
Volatility Foundation Volatility Framework 2.6.1
-----
DriverName: npf
DriverStart: 0x0
DriverSize: 0x0
DriverStartIo: 0x0
 0 IRP_MJ_CREATE                0xffffffff8001b0f1e0 Unknown
 1 IRP_MJ_CREATE_NAMED_PIPE     0xffffffff8001b0f1b0 Unknown
 2 IRP_MJ_CLOSE                 0xffffffff8001b0f1e0 Unknown
 3 IRP_MJ_READ                  0xffffffff8001b0f1b0 Unknown
 4 IRP_MJ_WRITE                 0xffffffff8001b0f1b0 Unknown
 5 IRP_MJ_QUERY_INFORMATION     0xffffffff8001b0f1b0 Unknown
 6 IRP_MJ_SET_INFORMATION      0xffffffff8001b0f1b0 Unknown
 7 IRP_MJ_QUERY_EA              0xffffffff8001b0f1b0 Unknown
 8 IRP_MJ_SET_EA                0xffffffff8001b0f1b0 Unknown
 9 IRP_MJ_FLUSH_BUFFERS        0xffffffff8001b0f1b0 Unknown
10 IRP_MJ_QUERY_VOLUME_INFORMATION 0xffffffff8001b0f1b0 Unknown
11 IRP_MJ_SET_VOLUME_INFORMATION 0xffffffff8001b0f1b0 Unknown
12 IRP_MJ_DIRECTORY_CONTROL     0xffffffff8001b0f1b0 Unknown
13 IRP_MJ_FILE_SYSTEM_CONTROL   0xffffffff8001b0f1b0 Unknown
14 IRP_MJ_DEVICE_CONTROL        0xffffffff8001b0f000 Unknown
15 IRP_MJ_INTERNAL_DEVICE_CONTROL 0xffffffff8001b0f1b0 Unknown
16 IRP_MJ_SHUTDOWN              0xffffffff8001b0f1b0 Unknown
17 IRP_MJ_LOCK_CONTROL          0xffffffff8001b0f1b0 Unknown
18 IRP_MJ_CLEANUP               0xffffffff8001b0f1b0 Unknown
19 IRP_MJ_CREATE_MAILSLIST      0xffffffff8001b0f1b0 Unknown
20 IRP_MJ_QUERY_SECURITY        0xffffffff8001b0f1b0 Unknown
21 IRP_MJ_SET_SECURITY          0xffffffff8001b0f1b0 Unknown
22 IRP_MJ_POWER                 0xffffffff8001b0f1b0 Unknown
23 IRP_MJ_SYSTEM_CONTROL        0xffffffff8001b0f1b0 Unknown
24 IRP_MJ_DEVICE_CHANGE         0xffffffff8001b0f1b0 Unknown
25 IRP_MJ_QUERY_QUOTA           0xffffffff8001b0f1b0 Unknown
26 IRP_MJ_SET_QUOTA             0xffffffff8001b0f1b0 Unknown
27 IRP_MJ_PNP                   0xffffffff8001b0f1b0 Unknown
-----
```

Device Tree

- `volatility --profile Win7SP1x64 -f memory.1f785001.img devicetree | grep npf`
- La información obtenida sobre la ubicación del objeto es desconocida...

```
german@german:~/CCN$ volatility --profile Win7SP1x64 -f memory.1f785001.img devicetree | grep npf
Volatility Foundation Volatility Framework 2.6.1
DRV 0x7dba77b0 \Driver\npf
---| DEV 0xfffffa8001b40a90 npf FILE DEVICE UNKNOWN
```

Hágame Carving!

- *volatility --profile Win7SP1x64 -f memory.1f785001.img volshell*

```
start=0xfffffa8001b40a90-0x100000
```

```
end=0xfffffa8001b40a90
```

```
while start < end:
```

```
    if addrspace().zread(start, 4) == "MZ\x90\x00":
```

```
        print(hex(start))
```

```
        break
```

```
    start += 1
```

Hágamos Carving!

- La ejecución del código devuelve el *offset* con el inicio de la cabecera del ejecutable.

```
german@operaciones:~/CCN$ volatility --profile Win7SP1x64 -f memory.1f785001.img volshell
Volatility Foundation Volatility Framework 2.6
Current context: System @ 0xfffffa80018cc040, pid=4, ppid=0 DTB=0x187000
Welcome to volshell! Current memory image is:
file:///home/german/CCN/memory.1f785001.img
To get help, type 'hh()'
>>> start=0xfffffa8001b40a90-0x100000
>>> end=0xfffffa8001b40a90
>>> while start < end:
...     if addrspace().zread(start, 4) == "MZ\x90\x00":
...         print(hex(start))
...         break
...     start += 1
...
0xfffffa8001b0e000L
```

Lectura de la cabecera

- Comprobación de lectura de los primeros bytes de la cabecera PE.

```
>>> db(0xfffffa8001b0e000)
0xfffffa8001b0e000  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00  MZ.....
0xfffffa8001b0e010  b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  .....@.....
0xfffffa8001b0e020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0xfffffa8001b0e030  00 00 00 00 00 00 00 00 00 00 00 00 e0 00 00 00  .....
0xfffffa8001b0e040  0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68  .....!...L.!Th
0xfffffa8001b0e050  69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f  is.program.canno
0xfffffa8001b0e060  74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20  t.be.run.in.DOS.
0xfffffa8001b0e070  6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00  mode....$.
>>> █
```

- volatility --profile Win7SP1x64 -f memory.1f785001.img moddump -D drivers/ -b 0xfffffa8001b0e000*

```
german@operaciones:~/CCN$ volatility --profile Win7SP1x64 -f memory.1f785001.img moddump -D drivers/ -b 0xfffffa8001b0e000
Volatility Foundation Volatility Framework 2.6
Module Base      Module Name      Result
-----
0xfffffa8001b0e000 UNKNOWN_         OK: driver.fffffa8001b0e000.sys
```

Lectura de la cabecera

Extracción de información del *driver*

```
4N4LDetector v1.6 - (@enelpc)
C:\Users\matu\Desktop\driver.ffffa8001b0e000.sys

Information:
Size: 5.50 KB
md5 Hash: BAC9BCDEE2A3262E3227B81E9659066F
MajorOSVersion: 10
Checksum: 22996
EntryPoint (rva): 5000
SizeOfHeaders: 400
SizeOfImage: 7000
Characteristics: 22
TimeStamp: 5CF539FD
Date: 6/3/2019 3:17:17 PM
Architecture: x64
File Type: EXE
Number Of Sections: 6
Section Names (Optional Header): .text, .rdata, .data, .pdata, INIT, .reloc
Number Of Executable Sections: 2
Subsystem: Native

Entry Point:
The section number (5) have the Entry Point
Information -> EntryPoint (raw) - 3A00

Checksum Integrity Problem:
Header: 22996 - Calculated: 39750

IT Functions:
KERNEL32.DLL -> WriteFile

File Access:
ntoskrnl.exe
c:\WINDOWS\certutil.txt

Payloads:
Unusual BP Cave > 15 Bytes - (0xCCCCCCCCCCCCCCCCCCCCCCCCCCCC...)

Extra 4n4lysis:
Rich Signature Analyzer -> Unusual or modified structure: (56 Bytes)
Ascii Code: (1387) - Total/Ascii: (24.6271%)
Null Byte Code: (3893) - Total/Null Bytes: (69.1229%)
```

Reversing con IDA x64

Identificación de la función que realiza la escritura del TXT

```

loc_13FB91050:          ; "\\DosDevices\\C:\\WINDOWS\\certutil.txt"
lea     rdx, aDosdevicesCWin
lea     rcx, [rbp+57h+DestinationString] ; DestinationString
call    cs:RtlInitUnicodeString
mov     [rsp+000h+EaLength], esi ; EaLength
lea     rax, [rbp+57h+DestinationString]
mov     [rsp+000h+EaBuffer], rsi ; EaBuffer
lea     r9, [rbp+57h+IoStatusBlock] ; IoStatusBlock
mov     [rsp+000h+CreateOptions], 20h ; CreateOptions
lea     r8, [rbp+57h+ObjectAttributes] ; ObjectAttributes
mov     [rsp+000h+CreateDisposition], 5 ; CreateDisposition
lea     rcx, [rbp+57h+FileHandle] ; FileHandle
mov     [rsp+000h+ShareAccess], esi ; ShareAccess
xorps   xmm0, xmm0
mov     [rsp+000h+FileAttributes], 80h ; FileAttributes
mov     edx, 40000000h ; DesiredAccess
mov     [rsp+000h+AllocationSize], rsi ; AllocationSize
mov     [rbp+57h+ObjectAttributes.Length], 30h
mov     [rbp+57h+ObjectAttributes.RootDirectory], rsi
mov     [rbp+57h+ObjectAttributes.Attributes], 240h
mov     [rbp+57h+ObjectAttributes.ObjectName], rax
movdqu  xmmword ptr [rbp+57h+ObjectAttributes.SecurityDescriptor], xmm0
call    cs:ZwCreateFile
mov     [rbp+57h+Buffer], 0DDDC6493h
lea     r8, [rbp+57h+Buffer]
mov     r9d, eax
mov     [rbp+57h+var_4C], 5B0E7685h
mov     [rbp+57h+var_48], 53D68F78h
mov     edx, esi
mov     [rbp+57h+var_44], 6A7DCF70h
mov     [rbp+57h+var_40], 0E2018868h
mov     [rbp+57h+var_3C], 0C682h
db      66h, 66h
nop     word ptr [rax+rax+00000000h]

```

Rutina de descifrado

```

loc_13FB91100:
movzx   ecx, byte ptr [r8]
lea     r8, [r8+1]
sub     cl, dl
movzx   eax, dl
sub     cl, 1Eh
add     al, al
ror     cl, 1
dec     al
inc     cl
add     cl, dl
inc     edx
rol     cl, 3
sub     cl, 4Fh
ror     cl, 1
add     cl, al
mov     [r8-1], cl
cmp     edx, 16h
jb      short loc_13FB91100

```

Código fuente del driver

Revisión del Pesudocódigo generado con IDA

```
RtlInitUnicodeString(&DestinationString, L"\\DosDevices\\C:\\WINDOWS\\certutil.txt");
ObjectAttributes.Length = 48;
ObjectAttributes.RootDirectory = 0i64;
ObjectAttributes.Attributes = 576;
ObjectAttributes.ObjectName = &DestinationString;
__mm_storeu_si128((__m128i *)&ObjectAttributes.SecurityDescriptor, 0i64);
v5 = ZwCreateFile(&FileHandle, 0x40000000u, &ObjectAttributes, &IoStatusBlock, 0i64, 0x80u, 0, 5u, 0x20u, 0i64, 0);
Buffer = 0xDDDC6493;
v6 = (int *)&Buffer;
v7 = v5;
v18 = 0x5B0E7685;
v19 = 0x53D68F78;
v8 = 0;
v20 = 0x6A7DCF70;
v21 = 0xE2018868;
v22 = 0xC682u;
do
{
    v9 = *(_BYTE *)v6;
    v6 = (int *)((char *)v6 + 1);
    v10 = __ROR1__(v9 - v8 - 30, 1);
    v11 = 2 * v8 - 1;
    v12 = v8++ + v10 + 1;
    v12 = __ROL1__(v12, 3);
    v13 = __ROR1__(v12 - 79, 1);
    *(_BYTE *)v6 - 1 = v11 + v13;
}
while ( v8 < 0x16 );
if ( v7 >= 0 )
{
    ZwWriteFile(FileHandle, 0i64, 0i64, 0i64, &IoStatusBlock, &Buffer, 0x16u, 0i64, 0i64);
    ZwClose(FileHandle);
}
```

Conversión del código fuente a Python

Preparación del descifrado del Flag

```

rol = lambda val, r_bits, max_bits = 8: \
    (val << r_bits%max_bits) & (2**max_bits-1) | \
    ((val & (2**max_bits-1)) >> (max_bits-(r_bits%max_bits)))

ror = lambda val, r_bits, max_bits = 8: \
    ((val & (2**max_bits-1)) >> r_bits%max_bits) | \
    (val << (max_bits-(r_bits%max_bits)) & (2**max_bits-1))

max_bits = 8

```

```

buffer = [
    "\x93","\x64","\xDC","\xDD",
    "\x85","\x76","\x0E","\x5B",
    "\x78","\x8F","\xD6","\x53",
    "\x70","\xCF","\x7D","\x6A",
    "\x68","\x88","\x01","\xe2",
    "\x82","\xc6"
]

v6 = 0
v8 = 0
v9 = 0
v10 = 0
v11 = 0
res = []

while (v8 < 21):
    v9 = ord(buffer[v8])
    v10 = 2 * v8 - 1
    v11 = v8 + ror(v9 - v8 - 30, 1) + 1
    v8 += 1
    temp = v10 + ror(rol(v11,3)-79, 1)
    res.append(chr(temp))

print("".join(res))

```

Ejecución descifrado en Python

Descifrado del Flag!

```
german@operaciones:~/CCN$ python decrypt.py  
Flag: Ur0bur0sR00tk1t
```



¿Preguntas?

No seáis cabroncetes que os conozco...



COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD

#XIIIJORNADASCCNCERT

OC.CCN.CNI.ES

WWW.CCN.CNI.ES

WWW.CCN-CERT.CNI.ES

**XIII
JORNADAS
STIC
CCN-CERT**

ccn-cert
centro criptológico nacional