

WRITE-UP SILICON VALLEY – CTF UAM

ARSENICS

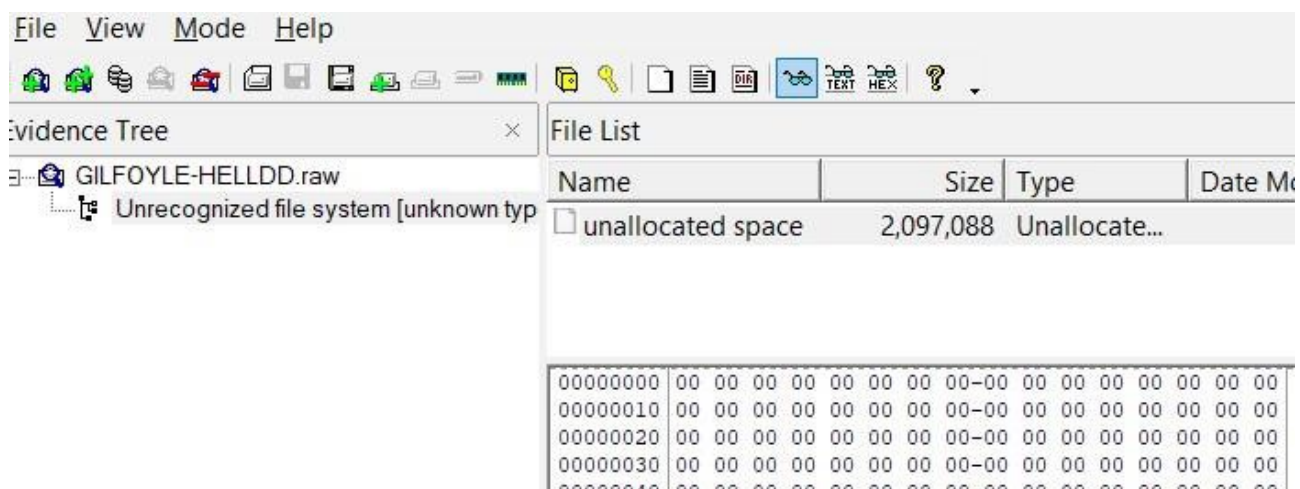
EPISODIO-1

Información del caso:

Alguien ha denunciado a "El Flautista" por hacer actividades empresariales en una vivienda personal. Necesitamos encontrar a la persona en cuestión para convencerlo de que retire la denuncia o se nos caerá el pelo. El problema es que ha habido un apagón en la incubadora de Erlich y todos los discos duros han muerto menos el de Gilfoyle. En ellos estaban las credenciales de acceso (encriptadas) a la plataforma de la empresa y la única pista del denunciante. Debes conseguir las credenciales de alguno de los archivos de Gilfoyle para entrar y poder encontrar la dirección de la persona que ha montado todo este lío.

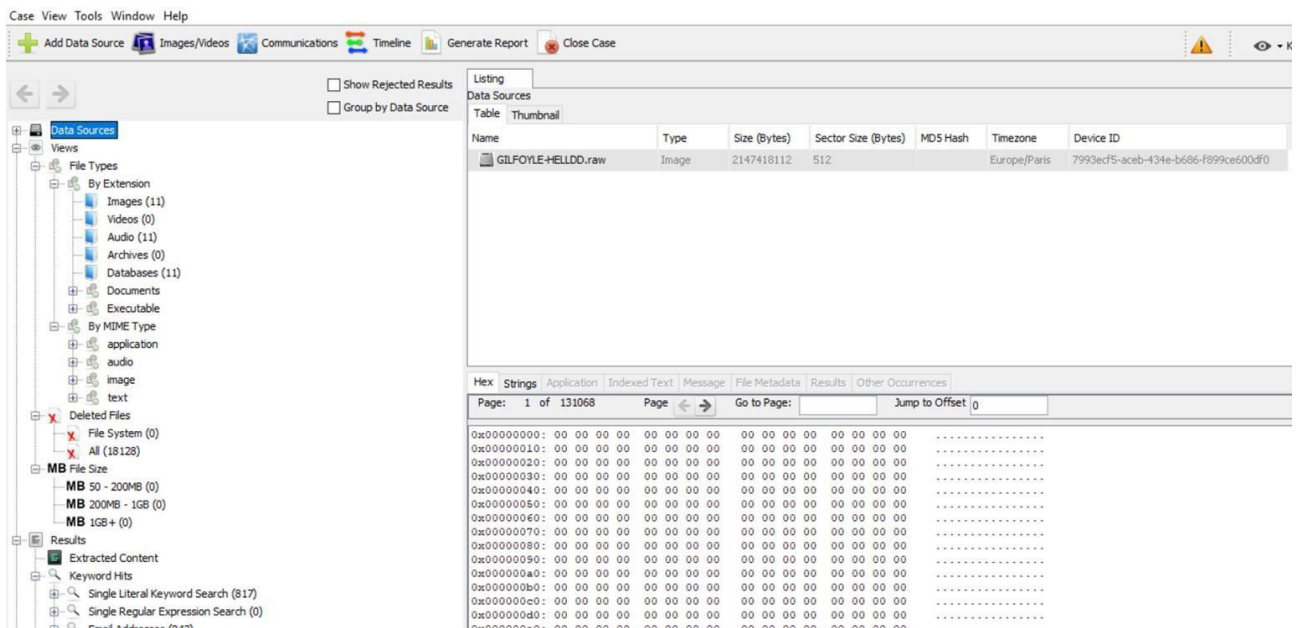
Se nos proporciona el disco duro de Gilfoyle y la siguiente plataforma:
<http://34.247.69.86/siliconvalley/episodio1/login.php>

Descargamos el disco duro de Gilfoyle y nos ya solo por el título nos damos cuenta que es un caso de forensics pues se titula Gilfoyle-hellDD.raw. Sabemos que las copias de disco suelen ser dd que es uno de los programas de dicha materia forense. De modo que el investigador (yo) inicialmente abre el access data FTK imager y al ser un .raw el disco está dañado y toda la información aparece en el unallocated space.



Dado que trabajar sí complica las cosas se toma la decisión de probar con autopsy.

En este caso observamos que es un solo sector de 512 bytes y nos detecta 11 imágenes, 11 audios, 11 databases y 18128 deleted files, mezclados donde hay dll, sqlite, txt, de todo.... Un mundo para perderse buscando el archivo con las credenciales que hay como objetivo (Primer shock xD). Entre los deleted files el investigador se percató de que se haya malware dentro del disco. Por precaución decide continuar con Volatility para tratar el caso.



En volatility en primer lugar se analiza el tipo de imagen en el que vemos que es un profile de windows y que la imagen data del 15/09/2018.

```
root@Kali:~/Downloads# volatility imageinfo -f GILFOYLE-HELLDD.raw
Volatility Foundation Volatility Framework 2.6
INFO      : volatility.debug      : Determining profile based on KDBG search...
Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64, Win7SP1x64_23418
AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
AS Layer2 : FileAddressSpace (/root/Downloads/GILFOYLE-HELLDD.raw)
PAE type  : No PAE
DTB       : 0x187000L
KDBG      : 0xf800029f00a0L
Number of Processors : 1
Image Type (Service Pack) : 1
KPCR for CPU 0 : 0xffffffff800029f1d00L
KUSER_SHARED_DATA : 0xffffffff7800000000L
Image date and time : 2018-09-15 09:56:27 UTC+0000
Image local date and time : 2018-09-15 11:56:27 +0200
```

Con la información del profile extraemos los datos de la hivelist y se procede al volcado la información del SAM y el SYSTEM ha ver si nos es útil para la web que nos proporcionan sin éxito, por lo que hay que continuar buscando. volatility -f GILFOYLE-HELLDD.raw --profile=Win7SP1x64 hivelist

```
Volatility Foundation Volatility Framework 2.6
Virtual      Physical      Name
-----
0xffffffff8a00000d010 0x000000002d73f010 [no name]
0xffffffff8a000024010 0x000000002d6a4010 \REGISTRY\MACHINE\SYSTEM
0xffffffff8a00004f010 0x000000002d5cf010 \REGISTRY\MACHINE\HARDWARE
0xffffffff8a0000962410 0x000000002c541410 \Device\HarddiskVolume1\Boot\BCD
0xffffffff8a000097b010 0x000000002bfa0010 \SystemRoot\System32\Config\SOFTWARE
0xffffffff8a0000cdd010 0x0000000023ade010 \SystemRoot\System32\Config\SECURITY
0xffffffff8a0000d62010 0x000000002329b010 \SystemRoot\System32\Config\SAM
0xffffffff8a0000d80410 0x0000000022dc6410 \\?\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0xffffffff8a0000df3010 0x0000000022152010 \\?\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0xffffffff8a001316410 0x0000000017d19410 \\?\C:\System Volume Information\Syscache.hve
0xffffffff8a001380010 0x0000000016502010 \\?\C:\Users\unaalme\ntuser.dat
0xffffffff8a001459010 0x00000000164c6010 \\?\C:\Users\unaalme\AppData\Local\Microsoft\Windows\UsrClass.dat
0xffffffff8a006d08010 0x000000002ac03010 \SystemRoot\System32\Config\DEFAULT
```

```

root@Kali:~/Downloads# volatility --profile=Win7SP1x64 -f GILFOYLE-HELLDD.raw hashdump -y 0xffffffff8a000024010 -s
0xffffffff8a0000d62010 > hashes.txt
Volatility Foundation Volatility Framework 2.6
root@Kali:~/Downloads# cat hashes.txt
Administrador:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
unaalmes:1001:aad3b435b51404eeaad3b435b51404ee:777e926012b1c652e8866847b1bd64fa:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:211d6fd0a9f90f4967f52f09d9770038:::

```

Se prosigue mirando los servicios que estuvieron corriendo hasta el momento del incidente y llama la atención un Soffice.

volatility -f GILFOYLE-HELLDD.raw --profile=Win7SP1x64 pslist

```

0xffffffff8a002d24b30 soffice.exe          1756    1900         1         66         1         1 2018-09-15
Offset(V)      Name                      PID    PPID    Thds      Hnds      Sess      Wow64  Start
Exit
-----
0xffffffff8a0018ac040 System                4         0        80       557      -----      0 2018-09-15 09:47:47
0xffffffff8a002101040 smss.exe             248         4         2         29      -----      0 2018-09-15 09:47:47
0xffffffff8a0028c6b30 csrss.exe            324        316         9        411         0         0 2018-09-15 09:47:51

0xffffffff8a002d24b30 soffice.exe          1756    1900         1         66         1         1 2018-09-15

```

De modo que nos centramos en la actividad de usuario con el comando userassist:

```

root@Kali:~/Downloads# volatility --profile=Win7SP1x64 -f GILFOYLE-HELLDD.raw userassist
Volatility Foundation Volatility Framework 2.6
-----
Registry: \??\C:\Users\unaalmes\ntuser.dat
Path: Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-917
Last updated: 2018-09-15 09:56:24 UTC+0000

Subkeys:
Values:
REG_BINARY      Microsoft.Windows.GettingStarted :
Count:          14
Focus Count:    21
Time Focused:   0:07:00.500000
Last updated:   2017-10-30 19:16:24 UTC+0000
Raw Data:
0x00000000  00 00 00 00 0e 00 00 00 15 00 00 00 a0 68 06 00 .....h..
0x00000010  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf .....
0x00000020  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf .....
0x00000030  00 00 80 bf 00 00 80 bf ff ff ff ff ca 10 90 93 .....
0x00000040  b3 51 d3 01 00 00 00 00 .....Q.....

```

```


REG_BINARY      %ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs\OpenOffice 4.1.4\OpenOffice Math.lnk :
Count:          1
Focus Count:    0
Time Focused:   0:00:00.501000
Last updated:   2017-11-14 00:10:28 UTC+0000
Raw Data:
0x00000000  00 00 00 00 01 00 00 00 00 00 00 00 01 00 00 00 .....
0x00000010  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf .....
0x00000020  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf .....
0x00000030  00 00 80 bf 00 00 80 bf ff ff ff ff 80 d7 8a fa .....
0x00000040  dc 5c d3 01 00 00 00 00 .....\.

```

Viendo que el usuario utiliza openoffice es posible que haya algún archivo de este tipo con las credenciales que necesitamos.


```
root@Kali:~/Downloads# volatility --profile=Win7SP1x64 -f GILFOYLE-HELLDD.raw filescan
Volatility Foundation Volatility Framework 2.6
Offset(P)          #Ptr    #Hnd Access Name
-----
0x0000000007e6015e0      12       0 R--r-d \Device\HarddiskVolume2\Program Files (x86)\OpenOf
0x0000000007e603340        2       1 ----- \Device\Afd\Endpoint
0x0000000007e603f20        1       1 R--rw- \Device\HarddiskVolume2\Windows\winsxs\x86_microsc
el8e3b_9.0.30729.6161_none_50934f2ebcb7eb57
0x0000000007e604740        1       1 R--rw- \Device\HarddiskVolume2\Windows\winsxs\amd64_micr
ntrols_6595b64144ccfldf_6.0.7601.17514_none_fa396087175ac9ac
0x0000000007e604890        2       0 R--r- \Device\HarddiskVolume2\Windows\System32\Microsof
```

Dado que la extensión más habitual de openoffice es “.odt” seleccionamos Search /Find “.odt” y nos encuentra el documento info.odt en el escritorio del disco de los users unaalmes.



The screenshot shows a Windows command prompt window with a directory listing. The files and folders listed are:

- fca93a0
- fca9c50
- fcaa070
- fcaa680
- fcaadd0
- fcaaf20
- fcaab50
- fcaab00
- fcaab50
- fcaab00

A 'Find' dialog box is open, showing the search term 'odt' and the 'Wrap around' option checked.

Que fichero más succulento!! procedemos a su volcado para ver el contenido.

```
volatility -f GILFOYLE-HELLDD.raw --profile=Win7SP1x64 dumpfiles -Q 0x000000007fcabd50 -D ./ -u -n
```

Se crea un archivo en la carpeta que estamos trabajando en la cmd llamado file.None.0xfffffa8001acdf10.info.odt.dat eliminando la extensión.dat y abriéndolo en openoffice se abren 4 páginas codificadas en base64. Se procede a su descodificación (2º Shock 4 páginas de texto hablando sobre el malware que detectamos en autopsy al principio. Se trata de Stuxnet.vmem).

The output shows eleven services printed in three unique timeframes. The most recent timeframe (1307075207) translates to 2011-06-03 04:26:47 UTC. At this time, the MRxCls and MRxNet services were either created or modified. It should be immediately suspicious that neither of these services is visible in the output of svcsn. This is a strong indicator that the two services are hidden (or they were started inappropriately); otherwise, the SCM would know about them:

```
$ python vol.py -f stuxnet.vmem --profile=WinXPSP3x86 svcscan
```

```
| egrep -i '(mrXnet|mrXcls)'
```

Volatility Foundation Volatility Framework 2.4

\$

One way to verify whether the services are actually running, despite the fact that there are no `SERVICE_RECORD` structures, involves first determining the associated kernel module.

The path is stored in the ImagePath value of the corresponding registry key. As you can see

in the following output, the module is `mrxdnet.sys`: `$ python vol.py -f stuxnet.vmem --`

```
profile=WinXPSP3x86 printkey
```

-K 'ControlSet001\Services\MRxNet'

Volatility Foundation Volatility Framework 2.4

Legend: (S) = Stable (V) = Volatile

No aparece el número de la dirección del enunciante como se explica en el enunciado del CTF a simple vista, sin embargo, debe estar en la imagen según la información proporcionada. En consecuencia, se sospecha de técnica de esteganografía.

Practicamos una autopsia a la imagen confirmando que existe texto oculto en ella.

Hex	Strings	Application	Indexed Text	Message	File Metadata	Results	Other Occurrences
Page: 1 of 12	Page	Go to Page:	Jump to Offset 0				
0x000000e0:	2D 72 64 66	2D 73 79 6E	74 61 78 2D	6E 73 23 27	-rdf-syntax-ns#'		
0x000000f0:	3E 0A 0A 20	3C 72 64 66	3A 44 65 73	63 72 69 70	>... <rdf:Descrip		
0x00000100:	74 69 6F 6E	20 72 64 66	3A 61 62 6F	75 74 3D 27	tion rdf:about='		
0x00000110:	27 0A 20 20	78 6D 6C 6E	73 3A 49 70	74 63 34 78	' . xmlns:Iptc4x		
0x00000120:	6D 70 43 6F	72 65 3D 27	68 74 74 70	3A 2F 2F 69	mpCore='http://i		
0x00000130:	70 74 63 2E	6F 72 67 2F	73 74 64 2F	49 70 74 63	ptc.org/std/Iptc		
0x00000140:	34 78 6D 70	43 6F 72 65	2F 31 2E 30	2F 78 6D 6C	4:xmpCore/1.0/xml		
0x00000150:	6E 73 2F 27	3E 0A 20 20	3C 49 70 74	63 34 78 6D	ns/'>. <Iptc4xm		
0x00000160:	70 43 6F 72	65 3A 4C 6F	63 61 74 69	6F 6E 3E 33	pCore:Location>3		
0x00000170:	37 2E 34 33	36 37 31 32	2C 20 2D 31	32 32 2E 31	7.436712, -122.1		
0x00000180:	33 37 38 33	37 3C 2F 49	70 74 63 34	78 6D 70 43	37837</Iptc4xmpC		
0x00000190:	6F 72 65 3A	4C 6F 63 61	74 69 6F 6E	3E 0A 20 3C	ore:Location>. <		
0x000001a0:	2F 72 64 66	3A 44 65 73	63 72 69 70	74 69 6F 6E	/rdf:Description		
0x000001b0:	3E 0A 3C 2F	72 64 66 3A	52 44 46 3E	0A 3C 2F 78	>.</rdf:RDF>.</x		
0x000001c0:	3A 78 6D 70	6D 65 74 61	3E 0A 20 20	20 20 20 20	:xmpmeta>.		
0x000001d0:	20 20 20 20	20 20 20 20	20 20 20 20	20 20 20 20			
0x000001e0:	20 20 20 20	20 20 20 20	20 20 20 20	20 20 20 20			
0x000001f0:	20 20 20 20	20 20 20 20	20 20 20 20	20 20 20 20			
0x00000200:	20 20 20 20	20 20 20 20	20 20 20 20	20 20 20 20			
0x00000210:	20 20 20 20	20 20 20 20	20 20 20 20	20 20 20 20			
0x00000220:	20 20 20 20	20 20 20 20	20 20 20 20	20 20 0A 20			

Location 37.436712, -122.137837 > Pinta a coordenadas geográficas de latitud y longitud. De modo que vamos a google maps a situarlas.



El número de la casa es 2126, que transformado al formato UAM{md5} queda:
UAM{3b92d18aa7a6176dd37d372bc2f1eb71}