Silicon Valley - Episodio 1

UAM CTF 2018-09-15

El reto



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.

· Disco duro de Gilfoyle (escoged el enlace que mejor os venga):

http://www.mediafire.com/file/31pj2a5umpfm345/GILFOYLE-HELLDD.zip

https://mega.nz/#!3lkWlSiK!MkrFlvvt7JBWm-_vrhlv-JFLoNFVh8_dDvFCE-qjKuc

Login: http://34.247.69.86/siliconvalley/episodio1/login.php

Info: La flag es el número de la casa en formato UAM{md5}

Flag	Submit
------	--------

Dump de memoria

Hemos bajado el fichero de mega y vemos un archivo GILFOYLE-HELLDD.raw

Tras probar con algunas herramientas, veo que el raw tiene el aspecto de un dump de memoria. Voy a usar Volatility, a ver qué encuentro.

Voy a sacar el filescan a un fichero de texto para ver todos los archivos que tenga en memoria:

volatility -f GILFOYLE-HELLDD.raw --profile=Win7SP1x64 filescan > filescan.volatility

Buscando entre los archivos encuentro un documento de openoffice: un odt

volatility -f GILFOYLE-HELLDD.raw --profile=Win7SP1x64 filescan | grep odt

```
      4 > 13:31:01 /media/root/Data/ctf-hispasec/2018-09 /media/root/Data/ctf-hispa
```

Lo extraemos con:

volatility -f GILFOYLE-HELLDD.raw --profile=Win7SP1x64 dumpfiles -Q 0x00000007fcabd50 --dump-dir=.

```
→ 13:13:63. /media/root/Data/ctf-hispasec/2018-09 volatility -f GILFOYLE-HELLDD.raw --profile=Win7SP1x64 dumpfiles -Q 0x000000007fcabd50 --dump-dir=. Volatility Framework 2.6

DataSectionObject 0x7fcabd50 None \Device\HarddiskVolume2\Users\unaalmes\Desktop\info.odt

| DataSectionObject 0x7fcabd50 None \Device\HarddiskVolume2\Users\unaalmes\Desktop\info.odt
| DataSectionObject 0x7fcabd50 None \Device\HarddiskVolume2\Users\unaalmes\Desktop\info.odt
| DataSectionObject 0x7fcabd50 None \Device\HarddiskVolume2\Users\unaalmes\Desktop\info.odt
| DataSectionObject 0x7fcabd50 None \Device\HarddiskVolume2\Users\unaalmes\Desktop\info.odt
| DataSectionObject 0x7fcabd50 None \Device\HarddiskVolume2\Users\unaalmes\Desktop\info.odt
| DataSectionObject 0x7fcabd50 None \Device\HarddiskVolume2\Users\unaalmes\Desktop\info.odt
| DataSectionObject 0x7fcabd50 None \Device\Users\unaalmes\Desktop\info.odt
| DataSectionObject 0x7fcabd50 None \Device\Users\unaalmes\Desktop\Users\unaalmes\Users\unaalmes\Users\unaalmes\Users\unaalmes\Users\unaalmes\Users\unaalmes\Users\unaalmes\Users\unaalmes\Users\unaalmes\Users\unaalmes\Users\unaalmes\Users\unaalmes\Users\unaalmes\Users\unaalmes\Users\unaalmes\Users\unaalmes\Users\unaalmes\unaalmes\Users\unaalmes\Users\unaalmes\Users\unaalmes\Users\unaalmes\Users\unaalmes\Users\unaalmes\Users\unaalmes\Users\unaalmes\Users\unaalmes\Users\unaalmes\Users\unaalmes\Users\unaalmes\Users\unaalmes\Users\unaalmes\Users\unaalmes\Users\unaalmes\Users\unaalmes\Users\unaalmes\Users\unaalmes\Users\unaalmes\Users\unaalmes\Users\unaalmes\Users\unaalmes\Users\unaalmes\Users\unaalmes\Users\unaalmes\Users\unaalmes\Users\unaalmes\Users\unaalmes\Users\unaalmes\Users\unaalmes\Users\unaalmes\Users\unaalmes\unaalmes\Users\unaalmes\Users\unaalmes\unaalmes\Users\unaalmes\unaalmes\Users\unaalmes\unaalmes\unaalmes\Users\unaalmes\Users\unaalmes\unaalmes\unaalmes\Users\unaalmes\unaalmes\unaalmes\unaalmes\unaalmes\unaalmes\unaalmes\unaalmes\unaalmes\unaalmes\unaalmes\unaalmes\unaalmes\unaalmes\unaalmes\unaalmes\unaalmes\unaalmes
```

El odt

El archivo extraido contiene texto codificado en base64 y parece que se rompe al tratar de decodificarlo, pero si nos fijamos mejor...

[b3f894165d6166da47d52ffbf77b5d87]ZXQgKFMpCkxhc3QgdXBkYXRlZDogMjAxMS0wNi0w MyAwNDoyNjo0NyBVVEMrMDAwMApTdWJrZXlzOgooVikgRW51bQpWYWx1ZXM6ClJFR1 9TWiBEZXNjcmlwdGlvbiA6IChTKSBNUlhORVQKUkVHX1NaIERpc3BsYXlOYW1llDogKFM pIE1SWE5FVApSRUdfRFdPUkQgRXJyb3JDb250cm9sIDogKFMpIDAKUkVHX1NaIEdyb3VwI DogKFMpIE5ldHdvcmsKUkVHX1NaIEltyWdlUGF0aCA6IChTKSBcPz9cOzpcV0lORE9XU1xz

¿Lo habéis visto? ¿No? Pues lo que buscamos está ahí xD

Encontramos este texto entre medias:

[448333920e12dc9fd9c5e8c30e6b1ea2]:[b3f894165d6166da47d52ffbf77b5d87] y buscando estos hashes en crackstation encontramos un usuario y pass.

Hash	Туре	F	Result
448333920e12dc9fd9c5e8c30e6b1ea2	md5	Gilfoyle	
Hash		Туре	Result
b3f894165d6166da47d52ffbf77b5d87	m	d5	Satan

La denuncia

Con esas credenciales hacemos Login en la plataforma que nos dieron al principio de la prueba:



Abrimos el enlace y nos muestra una imagen

JUZGADO DE INSTRUCCION N° 2 PLAZA CASTILLA,1 Teléfono: Fax: Número de Identificación Único: DILIGENCIAS PREVIAS PROC. ABREVIADO Procurador/a: SIN PROFESIONAL ASIGNADO PROVIDENCIA DEL MAGISTRADO-JUEZ SR. , a · Vista la anterior diligencia se tiene por personado y parte en las mismas al en nombre y la dirección letrada de D. y al propio representación de tiempo, dese traslado de las actuaciones al Procurador por medio de copia de las mismas, para que, conforme a lo dispuesto en el artículo 784, 1° de la Ley de Enjuiciamiento Criminal, presente escrito de defensa en el plazo de diez días frente a las acusaciones formuladas, con la prevención de que en caso de no verificarlo se entenderá que se opone a las actuaciones y seguirá su curso el procedimiento sin perjuicio de la responsabilidad en que pueda incurrir. MODO DE IMPUGNACION: mediante interposición de recurso de

reforma en el plazo de tres días ante este órgano judicial.

Si miramos los metadatos de la imagen vemos datos de geolocalización.

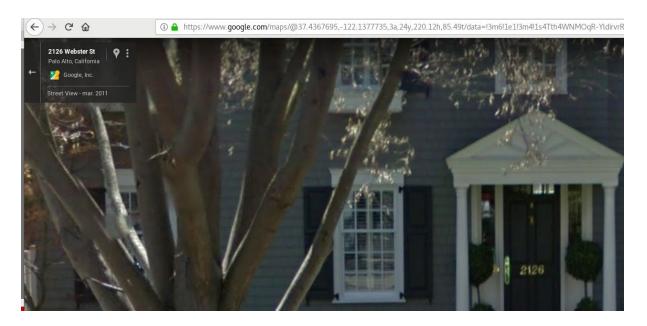
Lo mandó y firma S.Sª. Doy fe.-

exiftool denuncia.jpeg

```
13:25:06 /media/root/Data/ctf-hispasec/2018-09 exiftool denuncia.jpeg
ExifTool Version Number
                                  : 11.10
ile Name
                                  : denuncia.jpeg
Directory
File Size
                                 : 177 kB
File Modification Date/Time
File Access Date/Time
File Inode Change Date/Time
                                : 2018:09:16 13:03:53+02:00
                                : 2018:09:16 13:06:27+02:00
                                : 2018:09:16 13:03:53+02:00
File Permissions
                                  : JPEG
File Type
File Type Extension
                                  : jpg
MIME Type
                                  : image/jpeg
JFIF Version
Resolution Unit
                                  : inches
( Resolution
Resolution
XMP Toolkit
                                  : Image::ExifTool 11.10
                                  : 37.436712, -122.137837
Location
Profile CMM Type
                                  : Little CMS
Profile Version
                                  : 2.1.0
Profile Class
                                  : Display Device Profile
Color Space Data
                                  : RGB
Profile Connection Space
```

Coordenadas

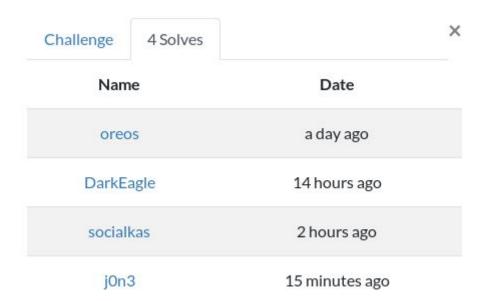
Tenemos unas coordenadas que buscaremos en google maps y al bajar a streetview podremos ver una casa:



Flag

Como la flag que nos piden es el número de la casa en md5, debe tener el formato $UAM\{md5(2126)\} = UAM\{3b92d18aa7a6176dd37d372bc2f1eb71\}$

Lo metemos en la plataforma y bingo!



4º puesto.. no está mal!;)

Enhorabuena a todos pero en especial a Oreos, que parece que tenía el writeup por lo rápido que lo consiguió xD

Conclusión

Hemos aprendido a analizar dumps de memoria con volatility y extraer sus archivos y a sacar información de una imagen para conseguir sus datos de geolocalización.

El reto ha sido sencillo aunque al principio perdí mucho tiempo tratando de encontrar las credenciales de acceso a la plataforma en las bases de datos (sqlite) de firefox, ya que se veía un proceso abierto de firefox en el dump y busqué en las cookies y demás. Con un filescan de volatility y algo de paciencia, encontré el archivo odt que contenía las credenciales de acceso a la plataforma de Pied Piper encriptadas en md5 y buscando en crackstation las encontramos fácilmente.

Siempre es divertido hacer estos retos. Seguid así, @devploit y @mrb0b0t.

José Ángel Sánchez <u>o jon3</u>