CTF Una-al-mes

SILICON VALLEY. Episodio 1.

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/#!3IkWlSiK!MkrFIvvt7JBWm-_vrhIv-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}

Resolución

Descargamos el fichero y descomprimimos, nos encontramos con un archivo raw.

Buscamos algunas cadenas (Gilfoyle, Pied Pipper ..) en el archivo, pero sin éxito.

El fichero parece un volcado de memoria, por lo que vamos a utilizar **volatility**

Primero identificar el sistema, aunque visualizando el raw, ya se intuye que es Windows.

volatility -f GILFOYLE-HELLDD.raw imageinfo

Suggested Profile(s) : Win7SP1x64

Una vez identificado, visualizamos los procesos activos.

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

Si nos fijamos en la lista de procesos encontramos dos que nos llaman la atención, fuera de los servicios de windows:

0xfffffa8002fc7b30 soffice.bin 2340 1756 11 464 1 1 2018-09-15 09:48:18 UTC+0000

0xfffffa8001d61b30 firefox.exe 956 3052 0 -------- 1 0 2018-09-15 09:55:59 UTC+0000 2018-09-15 09:56:08 UTC+0000

El primero de OpenOffice y el segundo el del navegador Firefox.

Buscamos los ficheros abiertos por el proceso de OpenOffice

volatility --profile=Win7SP1x64 -f GILFOYLE-HELLDD.raw -p 2340 handles

Entre todos los fichero, encontramos un fichero, **info.odt** que parece interesante…

0xfffffa8001aabd50 2340 0x2e8 0x12019f File \Device\HarddiskVolume2\Users\unaalmes\Desktop\info.odt

Volcamos el fichero info.odt.

volatility --profile=Win7SP1x64 -f GILFOYLE-HELLDD.raw dumpfiles -r odt$ -D T/

Nos encontramos con un texto cifrado de cuatro páginas, comenzando así:

VGhlIG91dHB1dCBzaG93cyBlbGV2ZW4gc2VydmljZXMgcHJpbnRlZCBpbiB0aHJlZSB1bmlxdWUgdGltZWZyYW1lcy4gVGhlIG1vc3QgcmVjZW50CnRpbWVmcmFtZSAoMTMwNzA3NTIwNykgdHJhbn…...

Si nos fijamos bien, en el texto, en la segunda hoja, aparecen unas cadenas con formato diferente:
W0zMlxjb25maWdcc3lzd[**448333920e12dc9fd9c5e8c30e6b1ea2**]:[**b3f894165d6166da47d52ffbf77b5d87**]ZXQgKFMpCkxhc3QgdXBkYXRlZDogMjAxMS0wNi0w

Tiene toda la pinta de ser cadenas MD5. Buscamos las cadenas en www.md5online.es

Hash = 448333920e12dc9fd9c5e8c30e6b1ea2
Encontrado : **Gilfoyle**
Hash = b3f894165d6166da47d52ffbf77b5d87
Encontrado : **Satan**

Lo que nos hubiésemos ahorrado con un simple grep del Md5 de Gilfoyle en el raw….

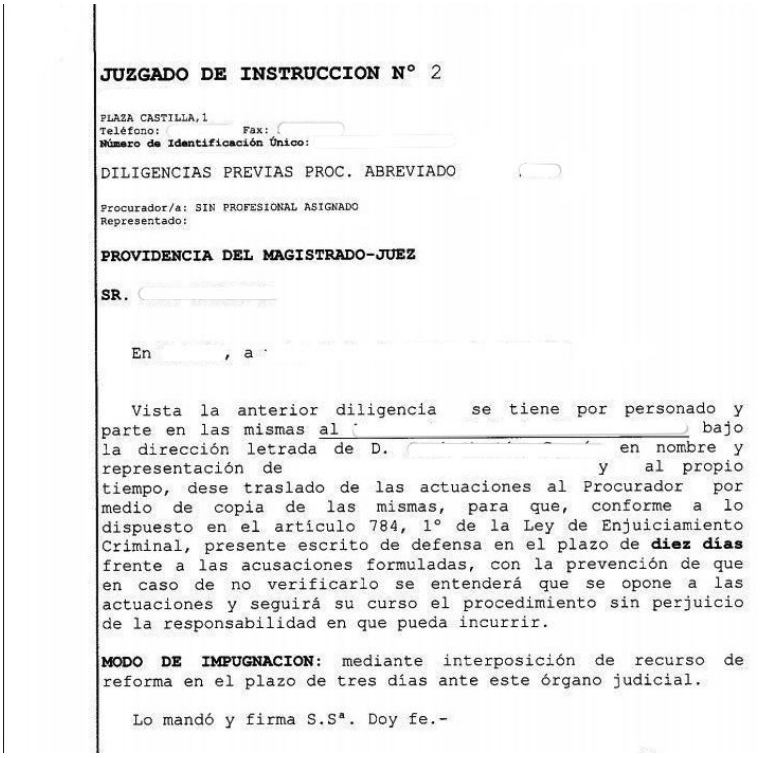
Ya tenemos usuario y contraseña, vamos a la página:

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

Introducimos los datos, y nos aparece:

Denuncia recibida:
https://drive.google.com/open?id=10iguWjRmx3mB0Y4g9iRrJOlXZ1HIJ_zC

Descargamos la imagen



JUZGADO DE INSTRUCCION Nº 2

PLAZA CASTILLA,1
Teléfono: Fax:
Número de Identificación Único:

DILIGENCIAS PREVIAS PROC. ABREVIADO

Procurador/a: SIN PROFESIONAL ASIGNADO
Representado:

PROVIDENCIA DEL MAGISTRADO-JUEZ

SR.

En , a

Vista la anterior diligencia se tiene por personado y parte en las mismas al bajo la dirección letrada de D. en nombre y representación de y al propio 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, 1º 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.

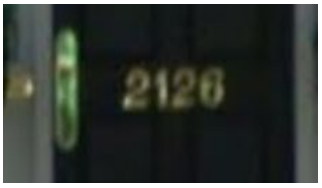
MODO DE IMPUGNACION: mediante interposición de recurso de reforma en el plazo de tres días ante este órgano judicial.

Lo mandó y firma S.Sª. Doy fe.-

En la imagen no hay referencias a una dirección, salvo la del juzgado, por lo que debe tener "algo" oculto. Abrimos con un editor hexadecimal y vemos en la cabecera ya metadatos interesantes:

<Iptc4xmpCore:Location>37.436712, -122.137837</Iptc4xmpCore:Location>

Ya tenemos las coordenadas, y con GoogleMap localizamos la casa y visualizamos su número: **2126**



Solución:

UAM{3b92d18aa7a6176dd37d372bc2f1eb71}

@bicacaro