WRITE-UP SILICON VALLEY – CTF UAM ARSENICS

EPISODIO-2

Información del caso

Dinesh ha perdido la clave VERDADERA que usaba para abrir su zip secreto pero gracias a DIOS tiene un archivo .raw donde puede recuperarla y necesita que le echemos una mano.

A Dinesh le encantan los mensajes con doble sentido, debéis tenerlo en cuenta...

- Archivo .raw (escoged el que mejor os venga):

https://www.mediafire.com/file/piv4t8514bp5dpg/pied_piper_bak.zip/file

https://mega.nz/#!iAUDnKwA!Y2g23qnZ9rwZvzZA3Bg8cbENe_ZtASOi1NFgrgfL8sg

Info: Las pistas os servirán a partir de que tengáis la contraseña del zip adjunto (Secretos_Dinesh.zip). Recordad que flag.txt tiene dos cifrados (leed bien README).

Info: La flag tiene el formato UAM{md5}

Walktrough

El investigador recoge el archivo .raw de Dinesh y comienza a recopilar información de la evidencia con volatility.

Con un imageinfo se desvela que es un windows 7 SP1 de 64 bits

```
root@kali:~# volatility imageinfo -f /root/Downloads/pied_piper_bak.raw
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win200
8R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_23418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/root/Downloads/pied_piper_ba
k.raw)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf80002a520a0L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff80002a53d00L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2018-10-15 10:48:27 UTC+0000
     Image local date and time : 2018-10-15 12:48:27 +0200
```

Realiza una búsqueda para ver que documentación ha quedado guardada en el clipboard comprobando que no se ha dejado rastro en esta parte de la memoria.

Acto seguido, se revisa que actividad ha tenido el usuario para determinar en que lugar puede encontrarse el archivo con la clave objetivo.

```
root@kali:~# volatility -f /root/Downloads/pied_piper_bak.raw --profile=Win7SP1x
64 userassist
Volatility Foundation Volatility Framework 2.6
----------------------------
Registry: \??\C:\Users\Richard\ntuser.dat
Path: Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-AC
E2-4F4F-9178-9926F41749EA}\Count
Last updated: 2018-10-15 10:48:26 UTC+0000
```

He aquí varia información interesante a destacar. El usuario del raw no es Dinesh, sino Richard. Este utiliza: notepad, stickynotes, HxD, paint, y SQLite Browser

```
REG_BINARY    C:\Users\Richard\Downloads\DB.Browser.for.SQLite-3.10.1-win64.exe
:
Count:          0
Focus Count:    1
Time Focused:   0:00:35.968000
Last updated:   1970-01-01 00:00:00 UTC+0000
Raw Data:
0x00000000  00 00 00 00 00 00 00 00 01 00 00 00 8c 8a 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 00 00 00 00   ................
0x00000040  00 00 00 00 00 00 00 00                           ........
```

De modo que se realiza una búsqueda de archivos, filtrando por los “.txt” en búsqueda de algún notepad interesante. El investigador se percata de un piper.txt que sin embargo no resulta ser de utilidad, por lo que se prosigue con la búsqueda.

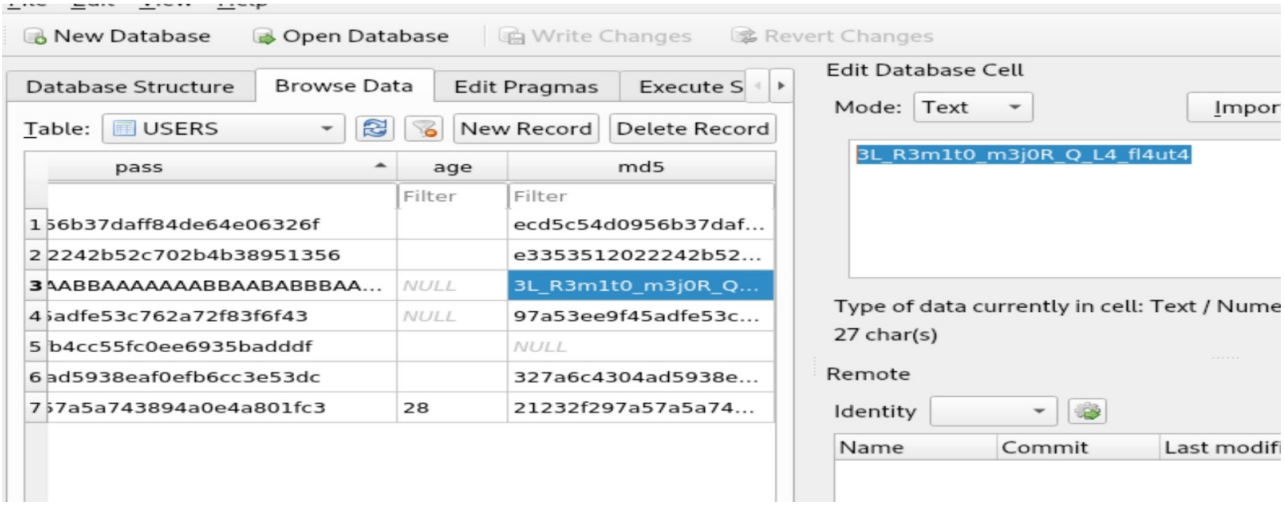
```
0x000000004146c660     16      0 R--rwd \Device\HarddiskVolume2\Users\Richard\De
sktop\piper.txt
```

Profundizando en los archivos del disco y teniendo en mente el SQLitebrowser que hemos visto anteriormente nos centramos en buscar bases de datos y tras una larga sesión se obtiene un piper.db

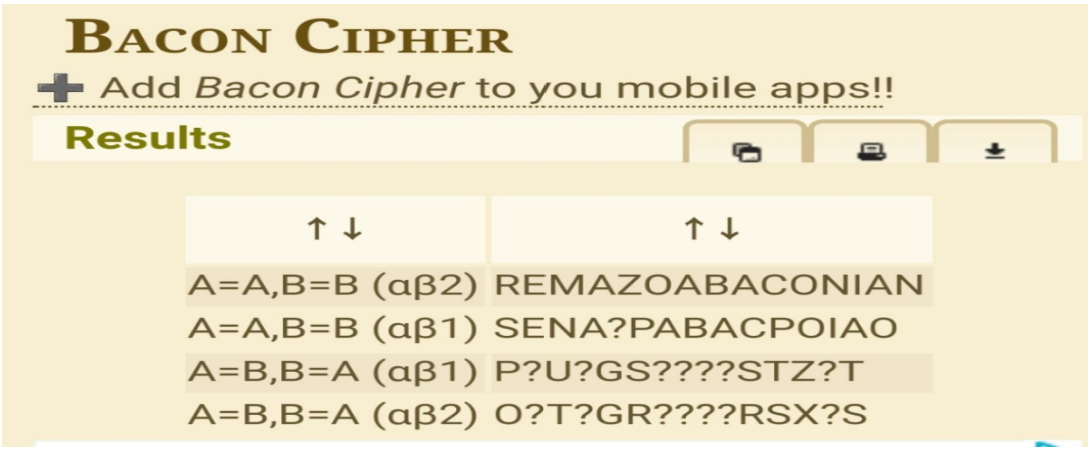
```
0x0000000040501860     16      0 R--rw- \Device\HarddiskVolume2\Users\Richard\De
sktop\piperdb.db
```

Volcamos el contenido de la base de datos y se obtienen 2 archivos, de los cuáles solo nos interesa el .dat

Abrimos file.None.Oxfffffa800.273v2d0.piperdb.db con SQLitebrowser y buscando en la base de datos obtenemos información en la tabla users.



La pass de la izquierda y el md5 de la derecha en todos los casos son iguales excepto en uno. Se encuentra diferencia en el número 3. A la derecha tenemos “El remito mejor que la flauta” mientras q a la izquierda vemos un código un tanto peculiar formado únicamente por A y B. Se realiza una búsqueda entre los cifrados clásicos y encontramos el baconio.

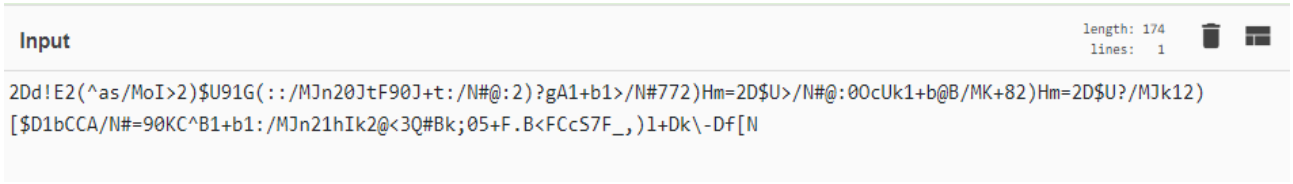


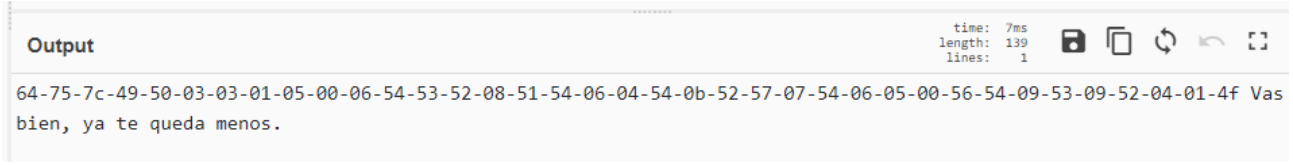
De las cuatro posibilidades vemos clara la primera REMAZOABACONIAN. Se prosigue con la apertura del zip de Dinesh y se abre el zip mostrando un README y un flag.txt. Al abrir el README se introduce la clave encontrada en el raw “REMAZOABACONIAN” y nos aparece la siguiente información:

1. “We are the DATE” https://www.youtube.com/watcn?v=tYITRRLj-n4

2. La clave final de todo está en el corazón de Telegram, en sus comienzos...

En el flag.txt se haya un cifrado que a priori parece muy extraño no sabemos relacionar. Miramos el vídeo que nos parece en la parte 1 del README. Un entrañable vídeo de 1985. En el que 45 cantantes, la mayoría estadounidenses cantan “We are the world” escrita por Michael Jackson con motivo de ayudar a la población africana. Dado que DATE está en mayúsculas y no pertenece al título de la canción determinamos que la fecha es importante. Pero importante... para qué? En un primer momento el pensamiento es que hay que descubrir el cifrado y que 1985 puede ser la clave del cifrado probando varios sin éxito. Tras ello damos con el cifrado base85 y descodificamos.





Con este primer descifrado eliminando los guiones tenemos un hex para encontrar la manera de descifrarlo recordamos la segunda pista del README. La respuesta final está en el corazón de telegram, en los comienzos. Comenzamos con una exhaustiva búsqueda sobre telegram en sus comienzos en 2013, sobre como funciona, su API , su cifrado end to end, etc. Nada parece aportar algo nos sirva. Se prueban varios cifrados sin éxito con clave 2013 y similares. Vemos incluso un artículo que se llama exactamente “el corazón de telegram” esta es la mía...pues no.

El corazón de Telegram, solo para usuarios

Comparto la info que me pareció más importante, que se encuentra en preguntas frecuentes, son datos muy precisos y escritos por ellos mismos, por lo que es la fuente de origen.

En lo personal comparto que Telegram se destaca por su Nube ilimitada (SI ILIMITADA) y sus particulares bots. Dejo enlace a mi otro post.

Mi objetivo con este post, es mostrar las diferencias que no están a simple vista, y que pueden ser más importantes de lo que parecen, y si sos usuario te Telegram y otros sistemas de mensajería, vas a ver más clara la diferencia básica.

Tras una larga lista de cifrados esotéricos y pruebas varias se cambia de pensamiento. El corazón de telegram debe andar ligado al aniversario de la UAM que se cumple justo el mes siguiente 15 de noviembre. Probamos diversos cifrados con 15112017 sin éxito. Se continua con la búsqueda el corazón de telegram y vamos al histórico del canal del grupo encontrando su comienzo el 14 de diciembre de 2017. Debe de ser esta. Se prueba en diferentes cifrados sin éxito. Se prueba la clave en hex, en binario, en fecha americana, nada.

Al final, tras decidir abandonar, se vuelve a intentar hayando la ansiada respuesta aplicando un XOR con clave de cifrado 14122017:

UAM{b326447fab9fe25f9bf0e242dd8d8f53}

Gracias a los creadores del reto. Hasta la próxima!