

Silicon Valley - Episodio 2

UAM CTF 2018-10-15

El reto

<https://unaalmes.hispasec.com/challenges#EPISODIO%202>

EPISODIO 2

300

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}

TOP 3:

1. oreos
- 2.
- 3.

Unlock Hint for 30 points

Unlock Hint for 40 points

 Secretos_Din...

Tras un vistazo inicial a todos los ficheros veo que hay un usuario Richard con cosas interesantes en desktop:

grep "Richard\\\\Desktop" filescan

```
0x000000003fa18b30      1      1 R--rw- \\Device\\HarddiskVolume2\\Users\\Richard\\Desktop
0x0000000040501860     16      0 R--rw- \\Device\\HarddiskVolume2\\Users\\Richard\\Desktop\\piperdb.db
0x00000000406ac310      1      1 R--rw- \\Device\\HarddiskVolume2\\Users\\Richard\\Desktop
0x000000004123a8d0      1      1 RW-rw- \\Device\\HarddiskVolume2\\Users\\Richard\\Desktop\\piperdb.db
0x000000004146c660     16      0 R--rwd \\Device\\HarddiskVolume2\\Users\\Richard\\Desktop\\piper.txt
0x000000004149b7c0      2      1 R--rwd \\Device\\HarddiskVolume2\\Users\\Richard\\Desktop
0x000000004149df20      2      1 R--rwd \\Device\\HarddiskVolume2\\Users\\Richard\\Desktop
```

Extraigo todos los ficheros interesantes, aunque el txt no puedo extraerlo...

```
vol -f pied_piper_bak.raw --profile=Win7SP1x64 dumpfiles --dump-dir=. -Q
0x0000000040501860
```

Esto nos deja un fichero que parece sqlite:

file file.None.0xfffffa80013806d0.vacb

```
file.None.0xfffffa80013806d0.vacb: SQLite 3.x database, last written using SQLite version 3015002
```

Sqlite

Aunque con un simple cat se puede ver perfectamente el contenido, que sqlite no pase hambre... xD

sqlite3 file.None.0xfffffa800273c2d0.dat

Vemos las tablas con el comando .schema

```
sqlite> .schema
CREATE TABLE 'USERS' (
  'id'      INTEGER UNIQUE,
  'user'    TEXT,
  'pass'    TEXT,
  'age'     INTEGER,
  'md5'     INTEGER
);
CREATE TABLE 'FLAG' (
  'id_flag'      INTEGER,
  'char_flag'    TEXT,
  'falso'        TEXT
);
CREATE TABLE 'COMMUNICATIONS' (
  'idmsg' INTEGER,
  'msg'   TEXT,
  'rcv'   INTEGER,
  'user'  TEXT,
  'sum'   TEXT
);
sqlite> █
```

REMAZOABACONIAN tiene toda la pinta de ser lo que buscamos...

Con esta clave podemos descomprimir el fichero secreto de Dinesh:

unzip Secretos_Dinesh.zip

Nos deja dos ficheros, README y flag.txt

cat README

1. "We are the DATE" <https://www.youtube.com/watch?v=tYIYRRLj-n4>

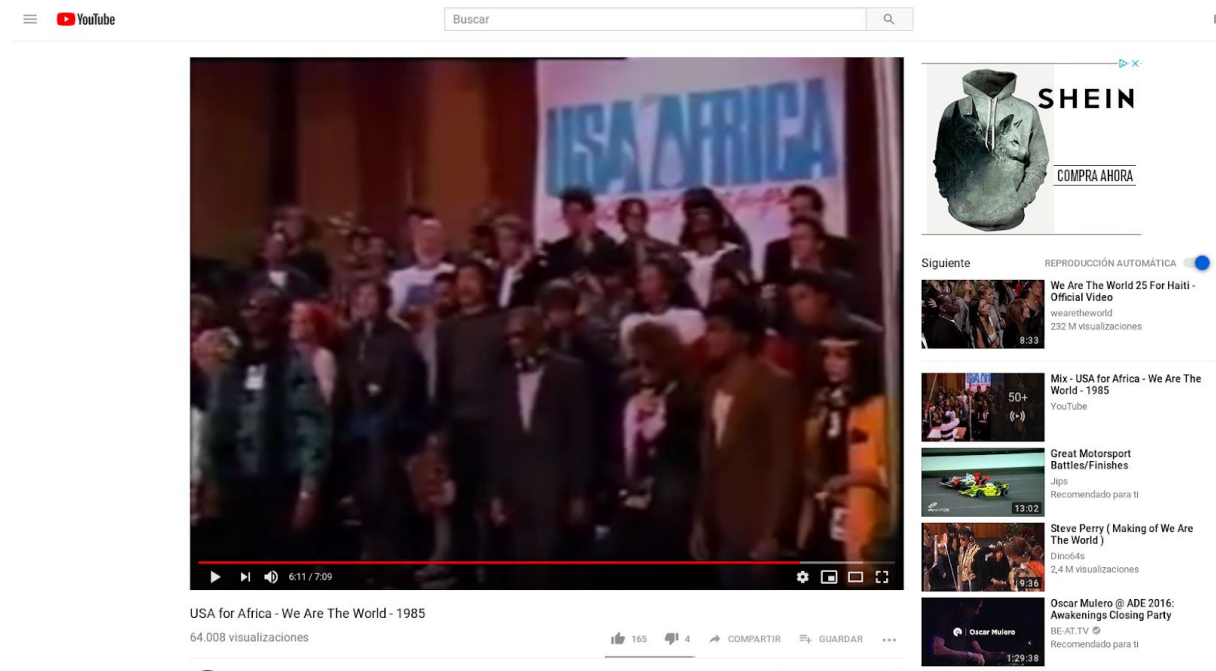
2. La clave final de todo está en el corazón de Telegram, en sus comienzos..

Flag.txt

cat flag.txt

2Dd!E2(^as/Mol>2)\$U91G(:/MJn20JtF90J+t:/N#@:2)?gA1+b1>/N#772)Hm=2D\$U>/N#@:
0OcUk1+b@B/MK+82)Hm=2D\$U?/MJk12)[\$D1bCCA/N#=90KC^B1+b1:/MJn21hk2@<3Q#
Bk;05+F.B<FCcS7F_,)l+Dk\ -Df[N

Vamos a ver qué es ese enlace en youtube...



We are the DATE?

USA for Africa - We Are The World - 1985

64.008 visualizaciones



Carlos Sanz

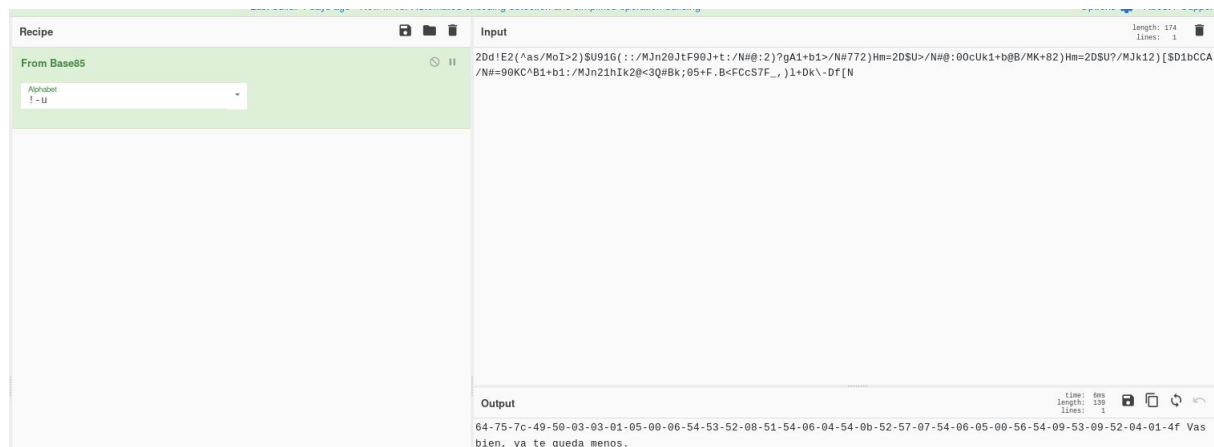
Publicado el 28 mar. 2009

El vídeo está publicado el 28 mar. 2009 y el título es 1985...

Después de probar todo tipo de combinaciones de rotaciones xors y demás en [CyberChef](#) con el contenido de flag.txt y todas las combinaciones y formatos de fecha que se me ocurren, doy con un pasito hacia adelante usando base85:

Base85

[https://gchq.github.io/CyberChef/#recipe=From_Base85\('!-u'\)&input=MkRkIUUyKF5hcy9Nb0k%2BMikkVTkxRyg6Oi9NSm4yMEp0RjkwSit0Oi9OI0A6Mik/Z0ExK2IxPi9OIzc3MillbT0yRCRVPi9OI0A6ME9jVWsxK2JAJi9NSys4MillbT0yRCRVPy9NSmsxMilbJEQxYkNDQS9OIz05MEtDXklxK2IxOi9NSm4yMWhJazJAPDNRI0JrOzA1K0YuQjxGQ2NTN0ZFLLCsK0RrXC1EZltO](https://gchq.github.io/CyberChef/#recipe=From_Base85('!-u')&input=MkRkIUUyKF5hcy9Nb0k%2BMikkVTkxRyg6Oi9NSm4yMEp0RjkwSit0Oi9OI0A6Mik/Z0ExK2IxPi9OIzc3MillbT0yRCRVPi9OI0A6ME9jVWsxK2JAJi9NSys4MillbT0yRCRVPy9NSmsxMilbJEQxYkNDQS9OIz05MEtDXklxK2IxOi9NSm4yMWhJazJAPDNRI0JrOzA1K0YuQjxGQ2NTN0ZFLLCsK0RrXC1EZltO)



64-75-7c-49-50-03-03-01-05-00-06-54-53-52-08-51-54-06-04-54-0b-52-57-07-54-06-05-00-56-54-09-53-09-52-04-01-4f Vas bien, ya te queda menos.

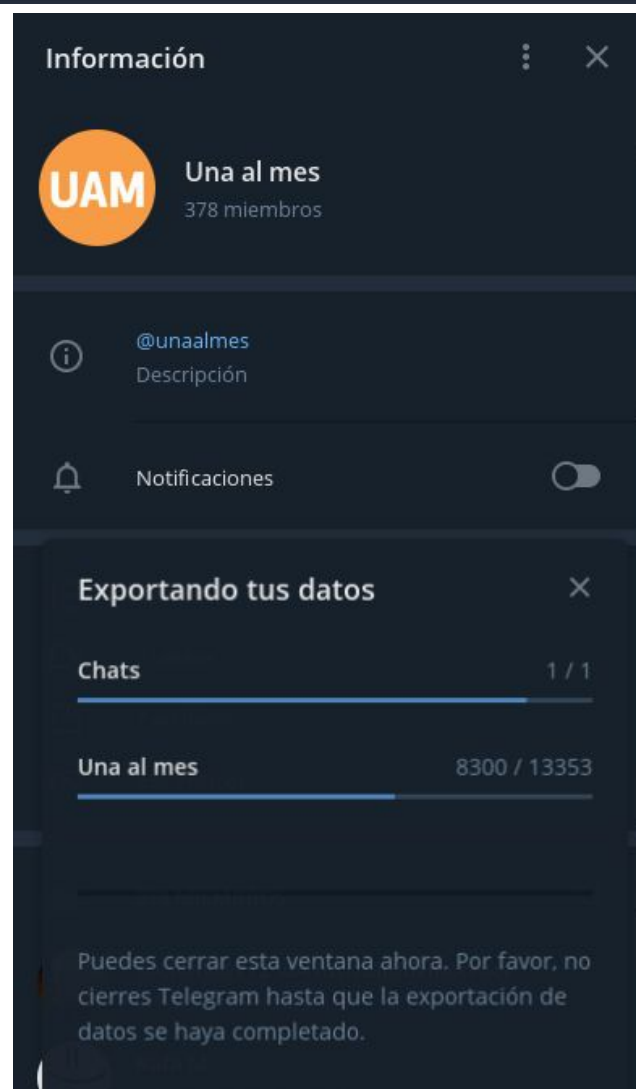
Podemos probar durante horas y no sacar absolutamente nada con esto... así que vamos a revisar el README.

Telegram

La segunda parte del readme dice que *"2. La clave final de todo está en el corazón de Telegram, en sus comienzos.."*

Me bajo el historial de Télegram del grupo de Una al Mes:

Telegram > Grupo UAM > Opciones de grupo > Información > Exportar historial del chat




La exportación nos deja un montón de htmls con todos los mensajes del grupo. Abrimos el primero de ellos:

firefox messages.html

Una al mes

14 December 2017

Mario converted a basic group to this supergroup «Una al mes»



Mario

18:04

●●● ÚNICA NORMA: NO REVELAR INFORMACIÓN SOBRE LOS RETOS (Y MENOS LA FLAG) ●●●


14.12.2017 18:04:07

Mario pinned [this message](#)

José joined group by link from Mario

15 December 2017


danielcues joined group by link from Mario



danielcues

11:55

Muy buenas, que tal



Mario

11:55

bienvenido

We are the DATES y el comienzo de Telegram... voy a quedarme con la fecha.

14.12.2017

XOR

Después de mucho probar infinitas combinaciones di con ello usando un xor y la fecha del primer mensaje de Telegram en el grupo. ¿He dicho después de mucho probar?. Pues eso, probar y probar y probar cosas hasta llegar al xor con la fecha pero algo faltaba..:

Recipe		Input
XOR <div> <div>Key</div> <div>64-75-7c-49-50-03-03-01-05-00-06-54-53-52-08-51-54-06-04-5 ...</div> <div>HEX ▾</div> </div> <div> <div>Scheme</div> <div>Standard</div> <div><input type="checkbox"/> Null preserving</div> </div>		14122017
		Output
		UAM{b326

Y tras probar unas cuantas cosas más, repitiendo la fecha varias veces sacamos la flag :D

[https://qchq.github.io/CyberChef/#recipe=XOR\(%7B'option':'Hex','string':'64-75-7c-49-50-03-03-01-05-00-06-54-53-52-08-51-54-06-04-54-0b-52-57-07-54-06-05-00-56-54-09-53-09-52-04-01-4f%20Vas%20bien,%20ya%20te%20queda%20menos.'%7D,'Standard',true\)&input=MTQxMjIwMTcxNDYyMjE0MTIyMDE3MTQxMjIwMTcxNDYyMg](https://qchq.github.io/CyberChef/#recipe=XOR(%7B'option':'Hex','string':'64-75-7c-49-50-03-03-01-05-00-06-54-53-52-08-51-54-06-04-54-0b-52-57-07-54-06-05-00-56-54-09-53-09-52-04-01-4f%20Vas%20bien,%20ya%20te%20queda%20menos.'%7D,'Standard',true)&input=MTQxMjIwMTcxNDYyMjE0MTIyMDE3MTQxMjIwMTcxNDYyMg)

Recipe

XOR

Key
64-75-7c-49-50-03-03-01-05-00-06-54-53-52-08-51-54-06-04-5 ...
HEX ▾

Scheme
Standard

☐ Null preserving

Input

141220171412201714122017141220171412201714122

Output

UAM{b326447fab9fe25f9bf0e242dd8d8f53}

Flag

UAM{b326447fab9fe25f9bf0e242dd8d8f53}

Challenge

3 Solves

Name	Date
oreos	a day ago
DarkEagle	a day ago
j0n3	an hour ago

3º puesto esta vez. ¡Yujuu!

¡Enhorabuena de nuevo a Oreos y a DarkEagle, que han estado rapidísimos!

Conclusión

Volvemos al análisis de imágenes de memoria y extracción de datos. Hemos jugado con encriptaciones, bases de datos sqlite y algunos puzzles algo enrevesados, pero siempre hay luz al final del túnel. Aunque a ratos me daba por vencido, perseverar y seguir buscando cosas ha sido clave. ¡Nunca os deis por vencidos!

Como siempre, gracias a @mrb0b0t y @devploit por otro buen rato con sus ctfs :D

José Ángel Sánchez

[@_j0n3](#)