EPISODIO 2
946

Misión:

Después de la explotación del programa de reclutamiento infiltramos a un informático como agente de Hydra. Tras unos días sin noticias, nos ha notificado que tiene en su poder el PC que utilizaban para las comunicaciones de los ataques, pero que este se ha visto afectado por un ransomware desconocido.

Tu misión es conseguir desencriptar el archivo principal, entender las comunicaciones que realizan y conseguir la fecha del próximo ataque.

Mucha suerte soldado.

Nick Furia.

Enlace de descarga de la VM: https://drive.google.com/open?id=1AvXC-ywgpmPFTaQKIk2WkIx5eD_xBNUj

Info: La flag tiene el formato UAM{md5 de la frase en mayúsculas y sin espacios}

TOP 3: 1. 2. 3.

Flag

Submit

Nos descargamos la imagen que contiene una VM. La ejecutamos y nos encontramos con dos ficheros en el Desktop.

Primero lo que hago es hacer una copia del directorio Desktop para no alterar el contenido de este por si más adelante tengo que recuperar algo.

cp -R Desktop/ /Desktop2

Damos permiso de ejecución al ransomware UAMsom de nuestra copia de Desktop

chmod u+x UAMsom

Al ejecutar el ransomware nos dice:

./UAMsom
Welcome to UAMsomware

E: Could not open input file../flag.txt
Time: 1547818118

Aquí ya nos está dando algunas pistas .. primero .. necesita un archivo llamado flag.txt que seguramente el encripta y lo convierte en flag.txt.uam.

Segundo, nos da un Timestamp, que si pasamos los números a date tenemos:

date -d @1547818118
Fri Jan 18 04:28:38 AKST 2019

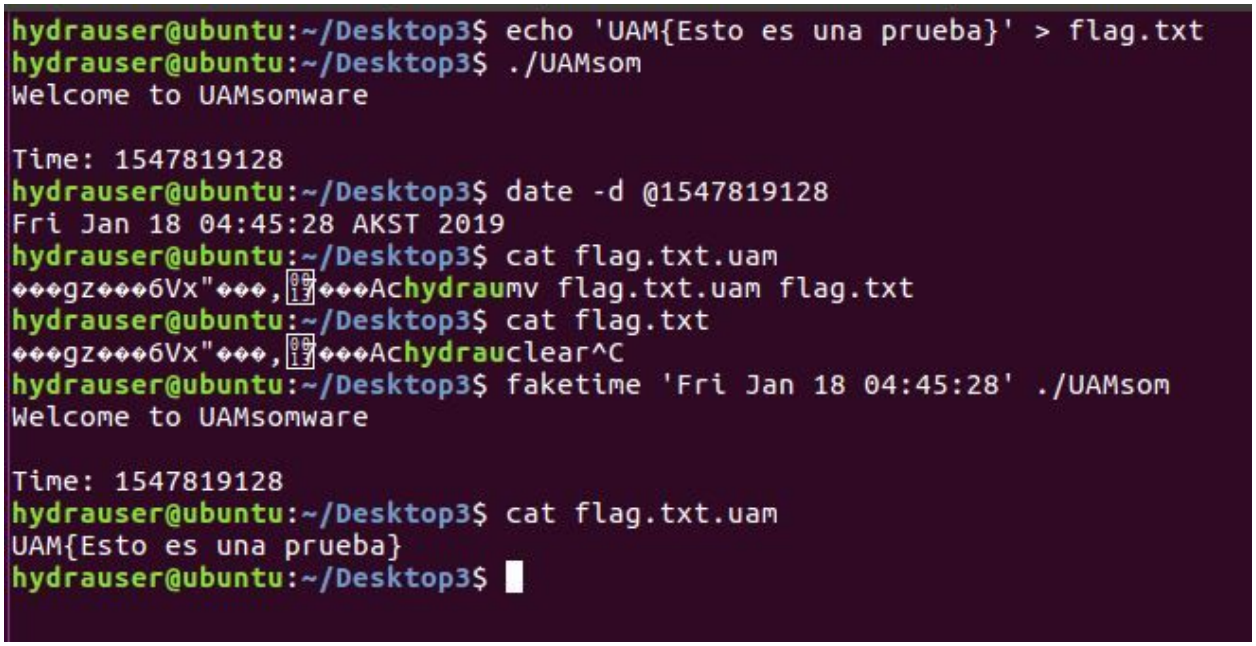
Que era ni más ni menos que la fecha del sistema en ese momento.
Creamos un flag.txt de prueba.
Si pasados unos segundo volvemos a repetir la operación vemos que el Time nos cambia al nuevo time de nuestro sistema y vemos que el fichero que encripta el ransomware flag.txt.uam va cambiando.

Con esto tenemos claro ya el funcionamiento de este ransomware.

Cuando se ejecuta el programa, codifica nuestro flag.txt teniendo en cuenta la fecha de nuestro sistema.

Con esto lo primero que nos viene a la cabeza es .. ¿Que pasaria si ejecutamos el programa con exactamente el mismo Tiemstamp y le pasamos nuestra flag codificada?.

Vamos a verlo:



Bien, pues funciona .. así que vamos a hacer esto con la flag.txt.uam real

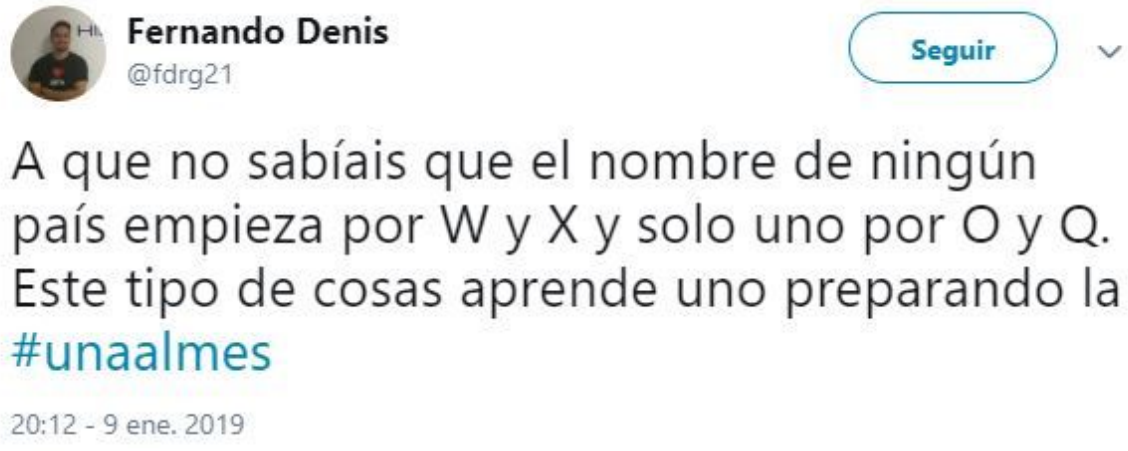
```
hydrauser@ubuntu:~/Desktop3$ cp ../Desktop/flag.txt.uam ./flag.txt
hydrauser@ubuntu:~/Desktop3$ stat ../Desktop/flag.txt.uam
  File: '../Desktop/flag.txt.uam'
  Size: 108             Blocks: 8          IO Block: 4096   regular file
Device: 801h/2049d      Inode: 1047348     Links: 1
Access: (0664/-rw-rw-r--)  Uid: ( 1000/hydrauser)   Gid: ( 1000/hydrauser)
Access: 2019-01-18 04:28:07.623003000 -0900
Modify: 2019-01-15 03:15:36.000000000 -0900
Change: 2019-01-15 03:17:01.747666426 -0900
 Birth: -
hydrauser@ubuntu:~/Desktop3$ faketime '2019-01-15 03:15:36' ./UAMsom
Welcome to UAMsomware

Time: 1547554536
hydrauser@ubuntu:~/Desktop3$ cat flag.txt.uam
+20+234+33+20+55+7+20+7+968+355+886+355+56+355+7+20+356+968+34+218+355+55+355+34+20+45+20+504+355+39+886+39
hydrauser@ubuntu:~/Desktop3$
```

Pues .. ya lo tenemos. A tener en cuenta que: Se ha utilizado faketime para engañar el programa y pasarle la fecha de sistema.
Por otra parte, con stat podemos ver cuando fue modificado el fichero de flag.txt.uam por ende … sabemos cuando se encripto el flag.

Ahora tenemos que el flag es:

cat flag.txt.uam
+20+234+33+20+55+7+20+7+968+355+886+355+56+355+7+20+356+968+34+218+355+55+355+34+20+45+20+504+355+39+886+39

Gracias a la pista que se dió por twitter:



Tenemos que relacionar los códigos esos con países … el mismo google nos da la solución:

Después de buscar todos los códigos que nos aparecen en la flag, en por ejemplo este recurso online: https://www.auslandsvorwahlen.net/en/ tenemos:

```
+20     Egypt
+234    Nigeria

+33     France
+20     Egypt
+55     Brazil
+7      Rusia
+20     Egypt
+7      Rusia
+968    Oman

+355    Albania
+886    Taiwan
+355    Albania
+56     Chile
+355    Albania
+7      Rusia
+20     Egypt
+356    Malta
+968    Oman
+34     Spain

+218    Libia
+355    Albania

+55     Brazil
+355    Albania
+34     Spain
+20     Egypt

+45     Denmark
+20     Egypt

+504    Honduras
+355    Albania
+39     Italy
+886    Taiwan
+39     Italy

ENFEBREROATACAREMOSLABASEDEHAITI

MD5 hash for ENFEBREROATACAREMOSLABASEDEHAITI is : 0f34e05951b864bd0621680af1f94acc
```

Es decir: MD5 hash for ENFEBREROATACAREMOSLABASEDEHAITI is : 0f34e05951b864bd0621680af1f94acc

UAM{0f34e05951b864bd0621680af1f94acc}

Un reto .. técnicamente muy fácil (si no usamos reversing) pero … un poco difícil saber qué hacer de buenas a primeras.

DarkEagle