UNIVERSO MARVEL. Episodio 2.

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-ywgpmPFTaQKlk2Wklx5eD_xBNUj

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

Resolución

Descargamos la máquina virtual: *Hydrabuntu.zip, la descomprimimos y la importamos en VirtualBox. En el zip, aparecen las credenciales de acceso:* ***hydrauser:hailhydra***

Tras acceder, nos aparecen en el escritorio dos ficheros, UAMsom y flag.txt.uam.

El primero se corresponde con el “ransomware” y el segundo el fichero cifrado por el mismo. Realizamos una copia del fichero cifrado.

Si intentamos ejecutar el programa nos indica que no puede abrir el fichero flag.txt.

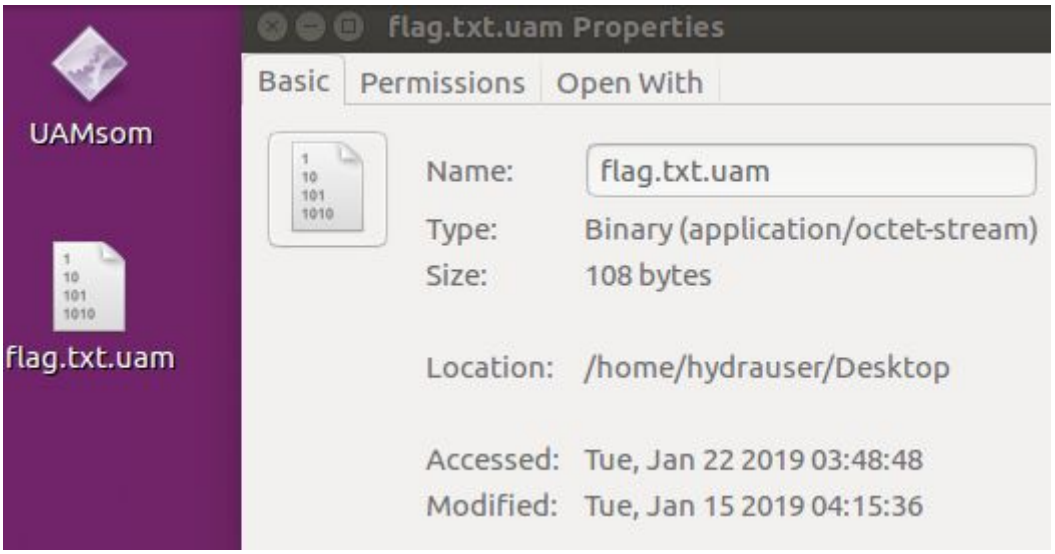
Creamos el fichero de texto **echo "test" > flag.txt.**
Realizamos una copia del fichero cifrado flag.txt.uam

Ejecutamos nuevamente:
./UAMsom
Welcome to UAMsomware

Time: 1548157208

Parece que la fecha del sistema, tiene algo que ver con el cifrado de texto. Si ejecutamos varias veces, siempre se genera un fichero flag.txt.uam diferente, lo que confirma que está asociado a la fecha y hora del sistema.

Comprobamos las propiedades del fichero cifrado.



Renombramos el fichero flag.txt.uam a flag.txt para descifrarlo.

Procedemos a cambiar la fecha del sistema desde el mismo panel de control, de tal manera que ejecutemos el ransomware a la misma hora que fue modificado el fichero. **15 Jan 2019 04:15:36**.

Ahora el fichero flag.txt.uam nos muestra un “texto” legible.

+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

Para esta parte, tenemos un Hint:

https://twitter.com/fdrg21/status/1083079138095886339

Twitter

Fernando Denis

A que no sabíais que el nombre de ningún país empieza por W y X y solo uno por O y Q. Este tipo de cosas aprende uno preparando la #unaalmes

Lo primero que se nos pasa por la cabeza son prefijos telefónicos internacionales (+34).

Buscamos una página con la relación completa, por ejemplo:

https://en.wikipedia.org/wiki/List_of_country_calling_codes

Empezamos la sustitución

+20: +20 – **E**gypt
+234 +234 – **N**igeria
+33 +33 – **F**rance
+20 +20 – **E**gypt
+55 +55 – **B**razil
+7 +7 – **R**ussia
+20 +20 – **E**gypt
+7 +7 – **R**ussia
+968 +968 – **O**man

….

Tras realizar todas las sustituciones, y tomando la primera letra de cada país, aparece la solución:

ENFEBREROATACAREMOSLABASEDEHAITI

MD5 es 0f34e05951b864bd0621680af1f94acc

UAM{0f34e05951b864bd0621680af1f94acc}

P.D. La solución aquí expuesta es simple y nada técnica, pero no me resultó nada evidente a primeras. Antes, pasé por r2, analizando el ejecutable, llegando a deducir que parece el algoritmo de cifrado Salsa20, por las variables de inicialización, también que no se utilizaban ni los parámetros de entrada, ni variables de entorno para el cifrado, únicamente la función rand y srand. Analizé también el sistema de ficheros, en busca de ficheros borrados, por ver flag.txt en la papelera (Autopsy, FTKimager), los logs, el historial de .bash_history, ….. y un largo, largo etc....