Cifrado xor y cuarentena

Objetivo

Que el alumno conozca el algoritmo de cifrado xor, utilizado tanto por herramientas de seguridad como por programas maliciosos.

Que el alumno identifique una forma en que los antivirus procesan los archivos sospechosos que son puestos en cuarentena.

Que el alumno se familiarice con los ataques de fuerza bruta a contraseñas; y el uso de un editor hexadecimal comúnmente utilizado en el análisis forense, de malware y de tráfico de red.

Requisitos

- Se sugiere usar un sistema operativo GNU/Linux Debian.
- Editor hexadecimal Bless o algún otro.
- Descargar este malware.

Introducción

Cuarentena

La Cuarentena es un almacenamiento especial para los archivos sospechosos posiblemente infectados con un malware.

A veces no es posible asegurar si un archivo ha sido infectado o no, por alguna de las siguientes razones

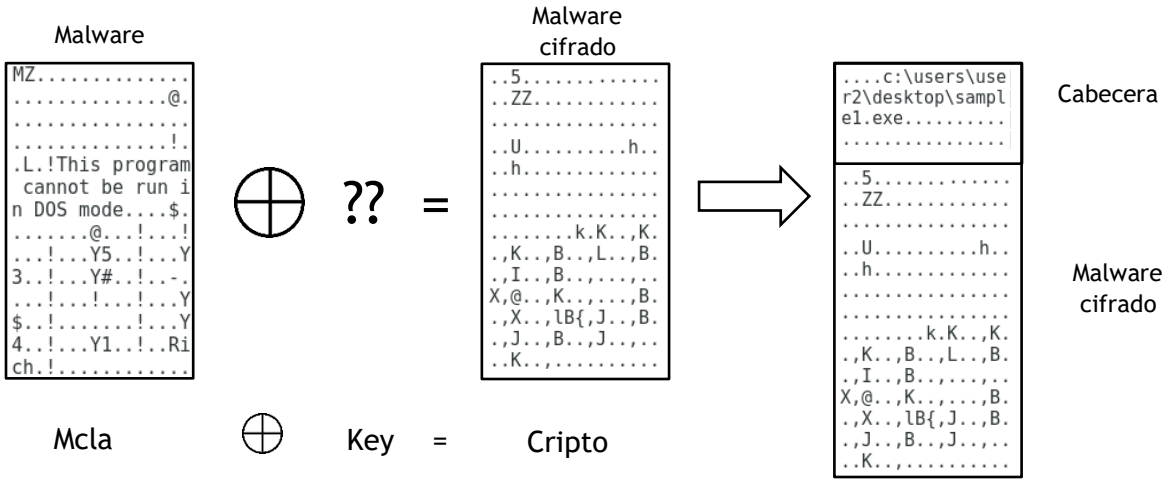
- El código del archivo es parecido a un malware ya identificado, pero ha sido modificado parcialmente, y la casa antivirus aún no tiene en su base de datos la firma asociada a este nuevo malware, por lo que solamente indicará que es sospechoso y a que amenaza conocida se asemeja.
- Es un nuevo tipo de amenaza que aún no ha sido identificada.

Para Karspersky Lab, el componente que define los archivos posiblemente infectados es el analizador heurístico del código.

De forma común las casas antivirus realizan un procedimiento para mover el archivo posiblemente infectado de su ubicación de origen con el fin de evitar su operación, por ejemplo comprimen el archivo sospechoso en formato zip añadiendo una contraseña para su apertura; o colocan datos adicionales al inicio del archivo, cifrándolo después usando una operación XOR a todo el archivo usando una contraseña de uno o más bytes. Algunos de los formatos utilizados son:

- ESET (NQF)
- Kaspersky (KLQ)
- MalwareBytes Data files (DATA)
- MalwareBytes Quarantine files (QUAR)
- McAfee Quarantine files (BUP)
- Symantec Quarantine Data files (QBD)
- Symantec Quarantine files (VBN)
- Symantec Quarantine Index files (QBI)

Para esta práctica se usará el archivo `57FD6325.VBN` el cual corresponde a un malware puesto en cuarentena. El antivirus cifró el malware aplicando una función Xor con una llave de un byte, y después agregó una cabecera al malware cifrado.



Desarrollo

1. Programe una función que obtenga a través de fuerza bruta la llave, de tamaño un byte, con la que se cifró el archivo. Recuerde que el malware es un archivo binario que se puede ejecutar en Windows, es decir contiene cadenas comunes a los archivos ejecutables.
   También recuerde las propiedades de la operación Xor vistas en clase y la tarea del reto.

2. Programe una función que reciba la llave obtenida en el paso anterior y descifre el archivo guardándolo en un archivo diferente.

3. El programa recibirá al menos dos argumentos desde la línea de comandos, el primero corresponderá al archivo a descifrar y como segundo el nombre del archivo en donde se guardará ya descifrado.

   por ejemplo,

   ```
   ./xor.pl 57FD6325.VBN malware.bin
   ```

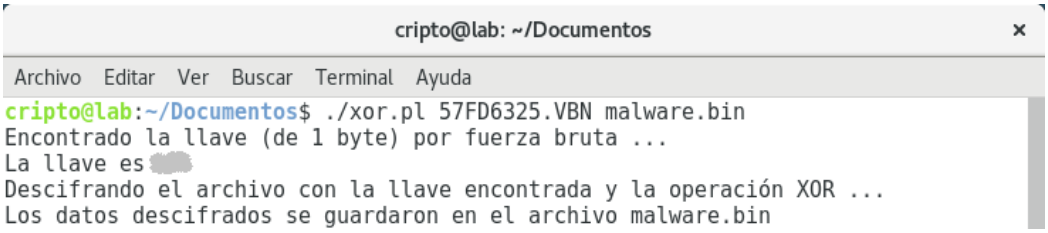


Fig. 1 Ejemplo de la ejecución del programa

4. Abrir el archivo descifrado con un editor hexadecimal, el recomendado es Bless. Eliminar la cabecera colocada por el antivirus, el tamaño de la cabecera será delimitado por el inicio del malware que es un binario, es decir, justo cuando se encuentre el número mágico de los archivos ejecutables, investigar cuál es el número mágico para los archivos ejecutables.

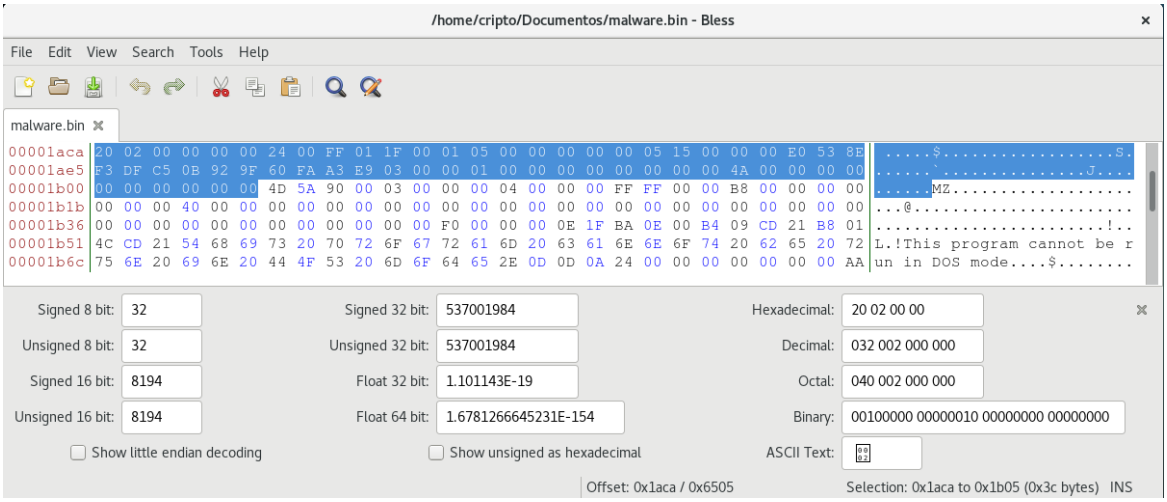


Fig. 2 Editor hexadecimal, borrar cabecera

¡¡¡Advertencia!!!

Este archivo no debe ser ejecutado en sistemas operativos Windows,
ya que puede infectarse. Se recomienda hacer todo el procedimiento con Linux.

5. Una vez guardado el archivo del malware, subirlo al sitio de análisis Virus Total https://www.virustotal.com

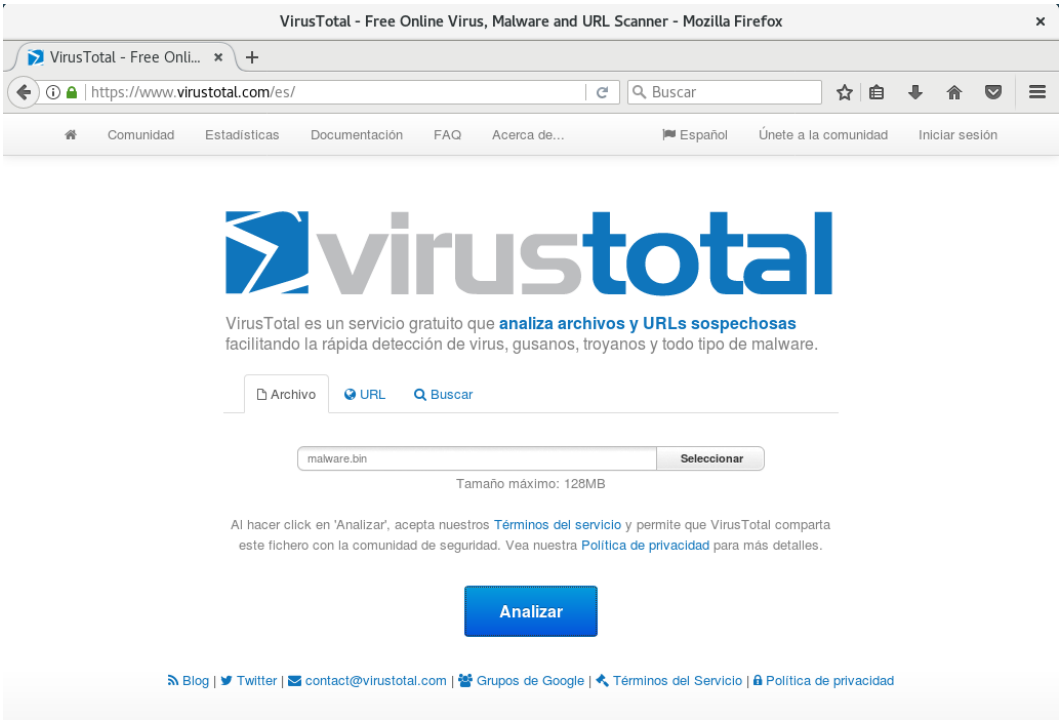


Fig. 3 Subir malware a VirusTotal

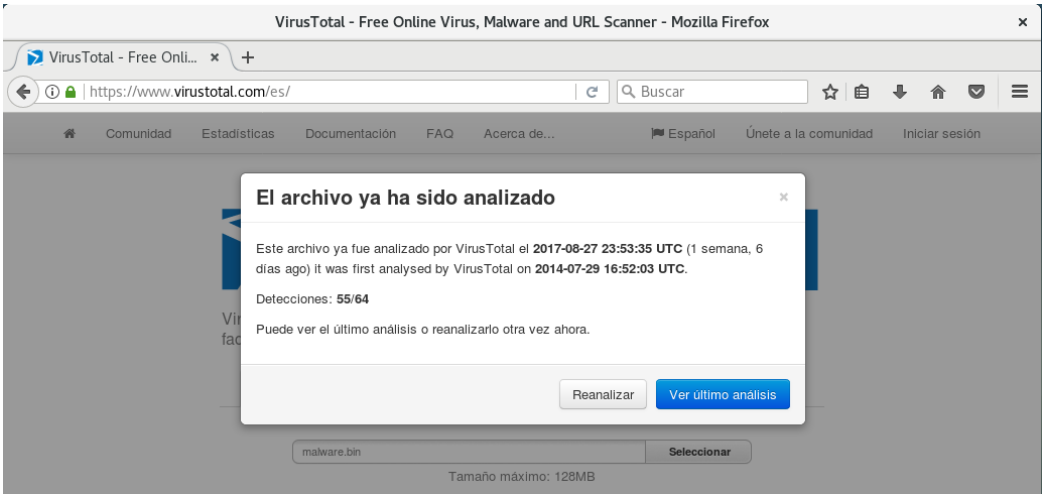


Fig. 4 Análisis con VirusTotal

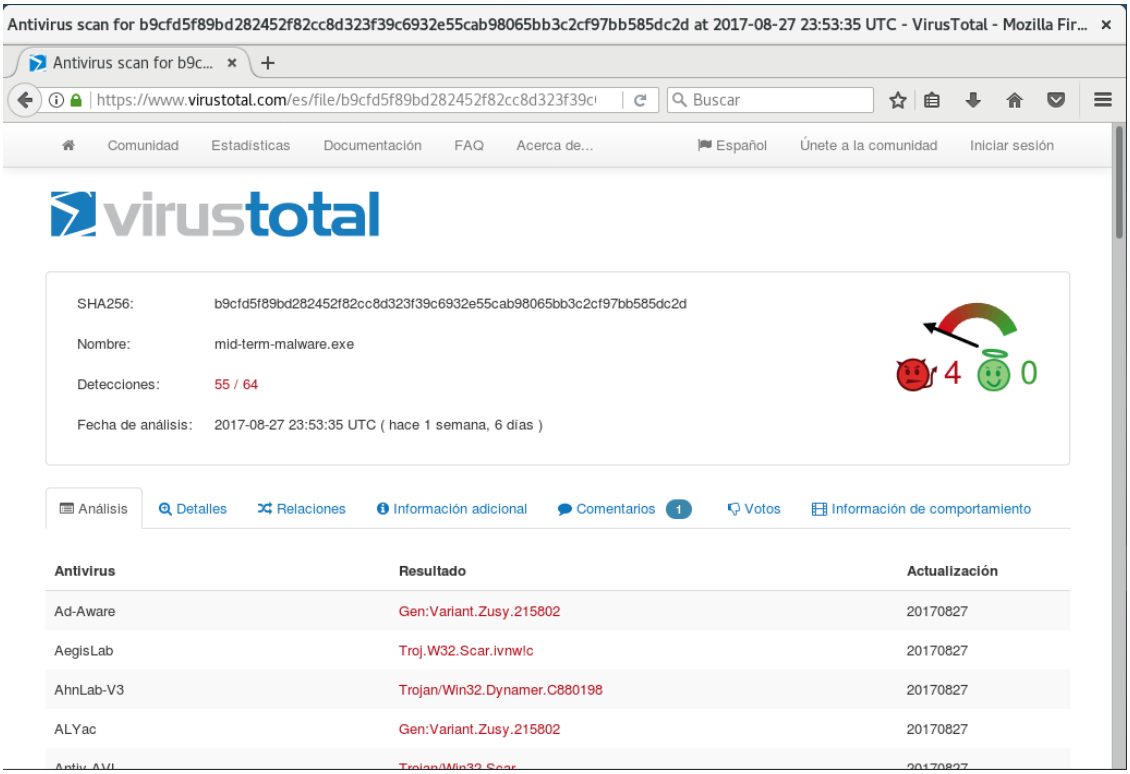


Fig. 5 Resultado del anális

Cuestionario

1. ¿Para qué se usa la herramienta XORsearch? https://blog.didierstevens.com/programs/xorsearch/
2. ¿De cuántos bytes es la cabecera que le agregó el antivirus al malware?
3. ¿Qué son los números mágicos? (relacionado con archivos)
4. ¿Qué es Virus Total?
5. De acuerdo a Virus Total, ¿qué tipo de malware es?

Elementos a calificar

1. Redacte un reporte por equipo, en el que consigne los pasos que considere necesarios para explicar cómo realizó la práctica, incluya capturas de pantalla que justifiquen su trabajo.
2. Incluya en su reporte tanto las respuestas del Cuestionario, como un apartado de conclusiones referentes al trabajo realizado.
3. Puede agregar posibles errores, complicaciones, opiniones, críticas de la práctica o del laboratorio, o cualquier comentario relativo a la misma.
4. Deberá subir el reporte en PDF a Moodle, y el código a un repositorio de GitLab que sea privado, mismo que deberá ser compartido con el profesor y los ayudantes, colocar el link en el reporte.
5. Se puede entregar en equipo de dos personas.

Referencias

- Didier Stevens. *XORSearch & XORStrings*. https://blog.didierstevens.com/programs/xorsearch/
- McAfee. *How to restore a quarantined file not listed in the VSE Quarantine Manager*. https://kc.mcafee.com/corporate/index?page=content&id=KB72755
- Hexacom. *DeXRAY*. http://www.hexacorn.com/blog/2016/03/11/dexray/
- Karspersky Lab. *¿Qué es la Cuarentena? ¿Dónde está su ubicación física en el equipo?* https://support.kaspersky.com/sp/2543

Universidad Nacional Autónoma de México

Paulo Contreras Flores
paulo.contreras.flores@ciencias.unam.mx

Jonathan Banfi Vázquez
jbanfi@ciencias.unam.mx