Ransomware

El ransomware es un tipo de software malicioso (malware) que se utiliza para bloquear el acceso a los archivos o sistemas de una víctima y exigir un rescate para restaurar el acceso. Los atacantes utilizan el ransomware para extorsionar a individuos y empresas mediante el cifrado de archivos o el bloqueo del acceso a sistemas críticos, lo que les impide acceder a sus datos y archivos importantes.

Una vez que el ransomware infecta un sistema, se suele mostrar una pantalla de advertencia que exige un pago en criptomonedas para obtener una clave de cifrado que permita desbloquear los archivos o sistemas afectados. En algunos casos, los atacantes también amenazan con publicar los datos de la víctima si no se paga el rescate.

El ransomware se propaga a menudo mediante técnicas de ingeniería social, como correos electrónicos de phishing, enlaces maliciosos o descargas de software ilegal. Además, algunos tipos de ransomware también pueden propagarse a través de vulnerabilidades en el software o sistemas no actualizados.

Es importante destacar que no se recomienda pagar el rescate exigido por los atacantes ya que no hay garantía de que los archivos o sistemas afectados sean restaurados, además de que esto puede animar a los ciberdelincuentes a continuar con sus actividades ilícitas. En lugar de pagar el rescate, es recomendable tomar medidas preventivas para evitar la infección por ransomware, como mantener el software actualizado, utilizar software de seguridad y educar a los empleados en técnicas de seguridad informática.

Intentar recuperar "shadow copy"

Listar si existen "shadow copies"

```
vssadmin list shadows
```

En caso que hubiera copias, usar ShadowExplorer.exe (portable) para recuperar archivos.

Determinar la forma de infección

- Información básica del sistema

```
systeminfo
```

- Información de red

```
ipconfig/all
```

- Identificar con que equipos se comunicó

```
arp -a
```

- Extraer el historial de navegación (Ejecutar como el usuario que infecto el equipo)
  - Chrome History View (AGAVE)
  - Mozilla History View (AGAVE)
  - IE History View (AGAVE)
- Registro de actividades (Necesita permisos de administrador)
  - LastActiivityView
  - MyEventViewer
  - RecentFileView
  - USBDBView

Nota: Transformar los archivos a UTF-8 con el comando dos2unix.

Análisis forense

- Realizar el apagado brusco del equipo. Desconectar el cable (PC de escritorio), Usar el boton de apagado (Laptop)
- Realizar copia bit a bit del disco duro

```
dd if=/dev/sdc of=/media/parrot/disk600Gb/backup.img bs=64M conv=sync,noerror status=progress
```

Si fuera necesario convertir la imagen forense en disco virtual

```
qemu-img convert -O vmdk -o compat6 backup.img vmdkname.vmdk
qemu-img convert -f raw -O vmdk rawdisk200gb.img vdisk200gb.vmdk
```

Herramientas útiles

- Identificar exactamente que variante de ransomware infecto al host
  - https://id-ransomware.malwarehunterteam.com/index.php
  - https://www.nomoreransom.org/crypto-sheriff.php?lang=en
  - Buscar IoC (IPs, dominios, etc) en los logs del firewall/proxy

Identificar si el ransomware usa llave simetrica (AES) o asimetrica (RSA). Si el ransomware usa una llave simetrica buscar la llave de encriptación en la copia de la memoria RAM.

Buscar herramientas para desencirptar

- https://docs.google.com/spreadsheets/d/1TWS238xacAto-fLKh1n5uTsdijWdCEsGIM0Y0Hvmc5g/pub?output=html
- https://heimdalsecurity.com/blog/ransomware-decryption-tools/
- https://www.nomoreransom.org/en/decryption-tools.html
- https://www.avast.com/ransomware-decryption-tools
- https://decrypter.emsisoft.com/
- https://support.kaspersky.com/viruses/utility
- https://noransom.kaspersky.com/?tool=. [EXTENSION ARCHIVOS CIFRADOS]
- https://malpedia.caad.fkie.fraunhofer.de/

Intentar recuperar archivos de la copia forense

- Usar Autopsy con la copia forense
- Usar FTK para montar la imagen forense y usar el software de recuperacion “recuva”

Anexos

- Links de descarga:
  - https://www.shadowexplorer.com/downloads.html
  - http://devcdn.avanquest.com/rw/WindowsDataRecovery.exe
- Extracción de llave de cifrada estático (AES) de memoria RAM
  - https://medium.com/@0xINT3/jigsaw-ransomware-analysis-using-volatility-2047fc3d9be9
- Posibles vectores:
  - pop-ups
  - facebook messenger
  - mail
  - Cracks

Revision #6
Created 7 marzo 2023 15:30:02 by Franz Rojas
Updated 3 abril 2025 12:30:23 by Vladimir Urquiola