GUIAS DE SEGURIDAD UJA

Ransomware

1. Qué es el *ransomware*

Podemos definir el *ransomware* como un tipo de *malware* (software malicioso) que bloquea el uso de un dispositivo (ordenador, tablet, smartphone…) o la información que contiene, para después pedir un **rescate** a cambio de su recuperación.

El método más habitual de propagación es a través del envío de correos electrónicos maliciosos a las víctimas. Los cibercriminales las engañan para que abran un archivo adjunto infectado o hagan clic en un enlace que les lleva al sitio web del atacante, dónde se infectan. Una vez infectados, mediante un mensaje, que suele ser intimidante, avisan a la víctima de que la única forma en que puede descifrar sus archivos o recuperar el sistema es pagar al cibercriminal.

Es habitual que incluyan un límite de tiempo para pagar el rescate o amenacen con la destrucción total de los archivos secuestrados o con incrementar el valor del rescate si no se paga a tiempo. El rescate suele variar entre cientos y miles de euros y es habitual que se solicite a través de alguna moneda virtual como *Bitcoins.* A cambio del pago, los ciberdelincuentes prometen facilitarnos el mecanismo para desbloquear el ordenador y descifrar los ficheros. Pero, en cualquier caso, **nunca tenemos garantías de que esto sea así, por lo que siempre se recomienda no pagar el rescate**.

2. Cómo nos podemos infectar

Las vías más habituales de infección por *ransomware* suelen ser las siguientes:

- Aprovechar **agujeros de seguridad (vulnerabilidades) del software** de los equipos, sus sistemas operativos y sus aplicaciones. Ciertas variedades de *ransomware* hacen uso de **servidores web desactualizados** como

vía de acceso para instalarse. También se aprovechan de sistemas industriales SCADA conectados a Internet sin las medidas básicas de seguridad.

- **Conseguir cuentas con privilegios de administrador** de acceso a los equipos mediante engaños (*phishing* y sus variantes), debilidades como no cambiar el usuario y contraseña por defecto, o vulnerabilidades del software.

- Engañar a los usuarios, mediante **técnicas de ingeniería social**, **para que instalen el malware**.

- Mediante **SPAM (correo basura)** que contiene enlaces web maliciosos o ficheros adjuntos que descargan el malware.

- Otro método, conocido como ***drive-by-download,*** consiste en dirigir a las víctimas a sitios web infectados, descargando el malware sin que ellas sean conscientes, aprovechando las vulnerabilidades de su navegador. También utilizan técnicas de ***malwertising*** (incrustan anuncios maliciosos en sitios web legítimos). El anuncio contiene código que infecta al usuario sin que este ni siquiera tenga que hacer clic en él.

3. Prevenir la infección por ransomware

3.1. Prevenir ataques de ingeniería social

Gran parte de las infecciones por *ransomware* tiene lugar mediante **ingeniería social**. Es una técnica psicológica que consiste en engañar a los usuarios suplantando la identidad de personas importantes o conocidas de la organización, intentando que las víctimas les den acceso para instalar el malware o para conseguir las contraseñas de acceso con las que entrar e instalarlo.

Es fundamental estar formado para ser capaz de reconocer estas situaciones y saber cómo actuar.

Reconocer y evitar un ataque de ingeniería social

- Desconfía de cualquier mensaje recibido por correo electrónico, SMS, Whatsapp o redes sociales en el que se te coaccione o apremie a hacer una acción amenazando con una posible sanción si no se hace.

- No abras correos de usuarios desconocidos o que no hayas solicitado: elimínalos directamente. No contestes nunca a estos correos.

- Revisa los enlaces antes hacer clic, aunque sean de contactos conocidos. Desconfía de los enlaces acortados.

- Desconfía de los ficheros adjuntos, aunque sean de contactos conocidos.

- Asegúrate de que en todas tus cuentas de usuario usas contraseñas robustas.

- Tenga siempre actualizado el sistema operativo y el software antivirus y/o antimalware. El Servicio de Informática de la Universidad de Jaén ofrece recomendaciones prácticas para mantener al día las actualizaciones del sistema operativo en el siguiente enlace:

http://www10.ujaen.es/conocenos/servicios-unidades/sinformatica/guias/seguridad/generales

3.2. Copias de seguridad

Si somos víctimas de un ataque de *ransomware*, la principal medida de seguridad (y puede que la única) que va a permitirnos recuperar nuestra actividad en poco tiempo, son las copias de seguridad o *backups*.

Recomendaciones básicas:

- Haz y conserva al menos **dos copias de seguridad** actualizadas.
- Guarda las copias de seguridad **en un lugar diferente** al del ordenador. Lo ideal es almacenar las copias de seguridad en discos físicos o en soportes externos no conectados a nuestra red (en otra ubicación física).
- Comprueba que las copias de seguridad que tienes funcionan correctamente y que puedes y sabes recuperarlas.

  El Servicio de Informática de la Universidad de Jaén ofrece recomendaciones prácticas para la realización de copias de seguridad en el siguiente enlace:

  http://www10.ujaen.es/conocenos/servicios-unidades/sau/guias/microinformatica/copia_seguridad

3.3. Navegación segura

- **Utiliza redes privadas virtuales (VPN)** siempre que sea posible. Las redes privadas virtuales son un tipo de conexión de red en el que el tráfico viaja cifrado y en el que los atacantes no pueden fisgar.
- **Evita visitar sitios web de contenido dudoso**. Siempre se recomienda mantener actualizados los navegadores web, y al mismo tiempo tener prudencia en nuestras actividades online.

3.4. Actualizaciones

Cuanto más actualizados estén los sistemas que utilizas, menos vulnerabilidades tendrán y será más difícil que puedan entrar o infectarte. Asegúrate que los sistemas operativos, aplicaciones y dispositivos tengan habilitados la instalación de actualizaciones de forma automática.

El Servicio de Informática de la Universidad de Jaén ofrece recomendaciones prácticas para mantener al día las actualizaciones del sistema operativo en el siguiente enlace:

http://www10.ujaen.es/conocenos/servicios-unidades/sinformatica/guias/seguridad/generales

4. Recuperar la información cifrada

Recomendaciones fundamentales:

- **NO PAGAR** nunca el rescate.
- Utiliza la última **copia de seguridad** de tu información para recuperar la información perdida.
- Puedes contactar con el Centro de Respuesta a Incidentes CERTSI de INCIBE. Te ayudarán a resolver el incidente y te indicarán cómo actuar y con un poco de suerte, pueden indicarte cómo recuperar tus archivos si existiera ya algún mecanismo probado.

- Aísla inmediatamente los equipos con *ransomware* desconectándolos de la red para evitar que este se expanda y ataque otros equipos o servicios compartidos.

- Si fuera posible recoge y aísla muestras de ficheros cifrados o del propio *ransomware* como el fichero adjunto en el mensaje de correo con el que puedes haberte infectado,

- Cambia lo antes posible todas las contraseñas de red y de cuentas online. Después de eliminado el *ransomware* vuelve a cambiarlas.

- Desinfecta los equipos y recupera los archivos cifrados (si fuera posible).

- Si fuera posible reinstala el equipo con el software original o arranca en modo seguro y recupera la copia de seguridad más reciente si la tuvieras.

4.1. ¿Por qué no debes pagar el rescate?

Si has sido víctima de un ataque de *ransomware* tendrás muchas dudas sobre si pagar el rescate o no. **La recomendación es no pagar nunca**, por los siguientes motivos:

- Pagar no te garantiza que vuelvas a tener acceso a los datos. Recuerda que se trata de delincuentes.

- Si pagas es posible que seas objeto de ataques posteriores pues, ya saben que estás dispuesto a pagar.

- Puede que te soliciten una cifra mayor una vez hayas pagado.

- Pagar fomenta el negocio de los ciberdelincuentes.

5. Herramientas para detectar y prevenir el *ransomware*

Muchos antivirus y herramientas antimalware ya incluyen entre sus funcionalidades la protección frente al *ransomware*. Pero existen numerosas herramientas y aplicaciones específicas que ayudan en la detección y prevención del mismo. Además, muchos fabricantes de antivirus disponen de herramientas específicas de desencriptado ficheros para ciertas variantes de ransomware.

Herramientas interesantes:

- Kaspersky anti-ransomware tool y herramientas de desencriptado:
  https://go.kaspersky.com/Anti-ransomware-tool.html
  https://noransom.kaspersky.com/

- AVAST – herramientas de desencriptado
  https://www.avast.com/ransomware-decryption-tools

- TrendMicro Ransomware File Decryptor
  https://success.trendmicro.com/solution/1114221-downloading-and-using-the-trend-micro-ransomware-file-decryptor

- AVG: herramientas de desencriptado
  https://www.avg.com/en-ww/ransomware-decryption-tools

- McAfee herramientas gratuitas anti-ransomware:
  https://www.mcafee.com/us/downloads/free-tools/index.aspx

- Ransomfree Cybereason:
  https://ransomfree.cybereason.com/

- GS Antiransomware: https://anti-ransomware.gridinsoft.com/
- No more Ransom – Herramientas de desencriptado https://www.nomoreransom.org/es/decryption-tools.html

6. Referencias en Internet

- Kaspersky – Blog: Historia y evolución del ransomware: datos y cifras https://blog.kaspersky.com.mx/ransomware-blocker-to-cryptor/7295
- No-More-Ransom https://www.nomoreransom.org/
- Malware.es Ransomware el virus que secuestra un Sistema http://www.malware.es/ransomware/
- Trendmicro Blog: ¿Por qué funciona el ransomware? Psicología y métodos utilizados para distribuir, infectar y extorsionar http://blog.trendmicro.es/?p=3033
- Segu-Info Blog: 22 consejos para prevenir el Ransomware http://blog.segu-info.com.ar/2016/03/22-consejos-para-prevenir-el-ransomware.html
- Navegación Segura http://www.navegacionsegura.es/
- CCN-CERT Informe sobre medidas de seguridad contra el ransomware https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/4251-actualizacion-del-informe-de-medidas-de-seguridad-contra-el-ransomware.html
- CCN-CERT – Información sobre *rasomware* https://www.ccn-cert.cni.es/component/tags/tag/ransomware.html?limitstart=0
- INCIBE - Enfrentándonos al ransomware https://www.incibe.es/protege-tu-empresa/blog/enfrentandonos-ransomware
- INCIBE - Servicio Antiransomware https://www.incibe.es/protege-tu-empresa/herramientas/servicio-antiransomware
- Microsoft Malware protection center – Ransomware https://www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx
- Segu-Info Blog: Herramientas para detectar ransomware en Windows y Linux http://blog.segu-info.com.ar/2016/03/herramientas-para-detectar-ransomware.html
- Guardia Civil - Grupo de Delitos Telemáticos: https://www.gdt.guardiacivil.es
- Policía Nacional – Brigada de Investigación Tecnológica http://www.policia.es/org_central/judicial/udef/bit_alertas.html