GUIAS DE SEGURIDAD UJA

Ransomware

Servicio de Informática
Vicerrectorado de Tecnologías de la Información
y la Comunicación y Universidad Digital
Universidad de Jaén

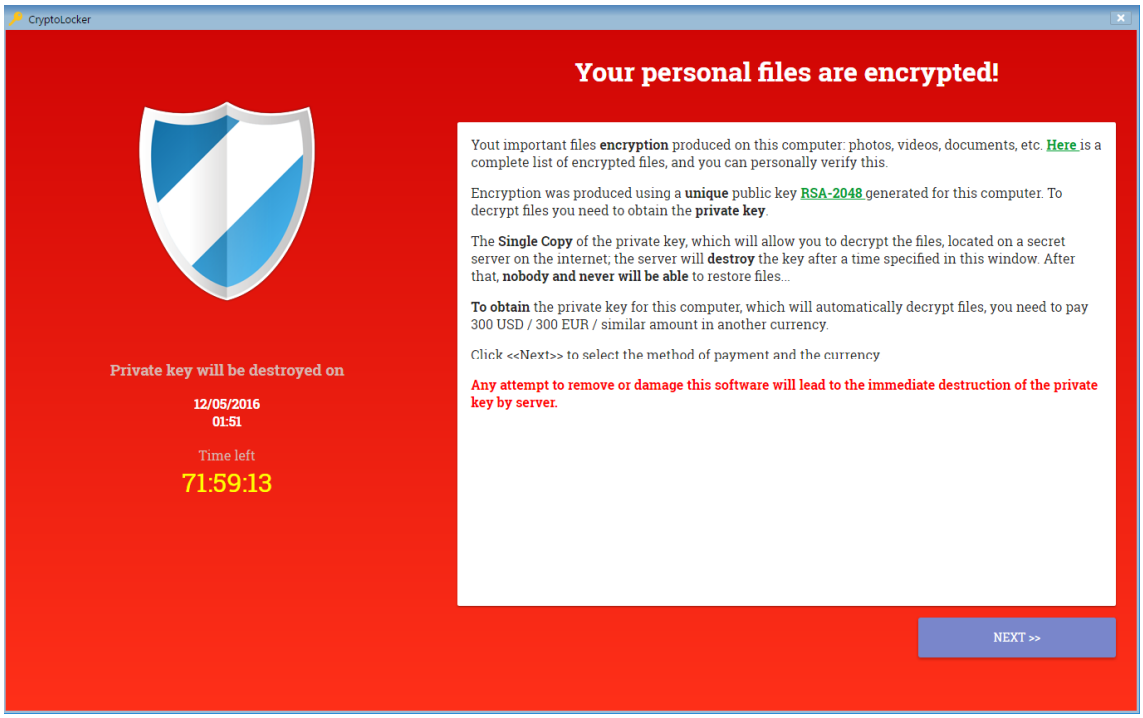
Edición: **febrero 2018**

Contenidos

1. ¿Qué es el *ransomware*?

Dentro del mundo digital actual en el que proliferan todo tipo de dispositivos, cada día estamos más expuestos a una amplia variedad de amenazas y peligros virtuales. Dentro de estas actividades maliciosas, hay una que se está desarrollando con gran rapidez en los últimos años, causando un gran impacto tanto en empresas como en usuarios particulares, al tiempo que está teniendo un gran impacto en los medios de comunicación. Se trata de un tipo de extorsión digital denominada genéricamente ***ransomware***.

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



Ejemplo de aviso de amenaza en un equipo infectado por *ransomware*

La palabra *ransomware* resulta de la unión de las palabras *ransom* (rescate, en inglés) y *malware*. Se trata de un malware que pide un **rescate** (*ransom*) a la víctima, a través de un mensaje o una ventana emergente. Es un "secuestro virtual" de nuestros recursos digitales por el que nos piden un rescate.

La causa del gran avance que ha experimentado el *ransomware* es que permite a los ciberdelincuentes obtener una gran rentabilidad económica en poco tiempo, a la vez que les facilita sistemas de pago que les permite el anonimato, como las *Bitcoins* y otro tipo de criptomonedas. Esto, junto con los avances en criptografía y la proliferación de dispositivos móviles e inteligentes ha provocado la aparición cada vez mayor de grupos especializados en el desarrollo de *ransomware*, así como el aumento de los recursos que los ciberdelincuentes destinan a su creación.

El *ransomware* se propaga como otros tipos de malware. El método más habitual 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

Existen numerosas formas en las que podemos infectarnos con algún tipo de malware de tipo *ransomware*. Las vías más habituales para infectar a la víctima suelen ser las siguientes:

- Aprovechar **agujeros de seguridad (vulnerabilidades) del software** de los equipos, sus sistemas operativos y sus aplicaciones. Los desarrolladores de malware disponen de herramientas para detectar y a averiguar dónde están estos agujeros de seguridad e introducir así el malware en los equipos.

  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

  - 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. Por ejemplo, cada vez más equipos de aire acondicionado, impresoras de red, equipos médicos, etc. son conectados a redes corporativas o Internet sin las mínimas medidas 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**. Esta es la más frecuente y la más fácil para el ciberdelincuente. Por ejemplo, mediante un correo falso con un enlace o un fichero adjunto con una supuesta actualización de software que en realidad instala el malware. O con un mensaje suplantando a un amigo o conocido con un enlace a un sitio que aloja el malware. También se utilizan estas técnicas a través de redes sociales o servicios de mensajería instantánea.

- Mediante **SPAM (correo basura)** que contiene enlaces web maliciosos o ficheros adjuntos como documentos de Microsoft Office o ficheros

comprimidos (.rar, .zip) que contienen macros o ficheros JavaScript 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*

La prevención contra este tipo de amenazas se puede llevar a cabo a diferentes niveles, que veremos a continuación:

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.

Las técnicas para conseguir la confianza y manipular a la víctima son diversas y se aprovechan:

- **Del respeto a la autoridad**, cuando el atacante se hace pasar por un responsable o por un policía, por ejemplo.
- **De nuestra disposición a ayudar y colaborar** especialmente en entornos laborales y comerciales.
- **Del miedo a perder algo**, como es el caso de los mensajes en los que tienes que hacer un ingreso para obtener un trabajo, una recompensa, un premio, etc.
- **De la vanidad,** cuando adulan a la víctima por sus conocimientos, su posición o sus influencias.
- **Creando situaciones de urgencia** y consiguiendo sus objetivos como fruto de la pereza, el desconocimiento o la ingenuidad de la víctima.

Consejos importantes para 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 en ningún caso 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.

NOTA: 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

En caso de que seamos 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*.

Como primera medida básica, es recomendable hacer copias de seguridad a diario (de forma programada o automatizada a ser posible), y que estas copias de seguridad están almacenadas en una ubicación física diferente.

Se pueden hacer copias de seguridad con aplicaciones como las siguientes:

- Syncback free
  https://www.2brightsparks.com/freeware/freeware-hub.html
- Cobian backup
  http://www.cobiansoft.com/index.htm

O en la nube, usando servicios como:

- Google Drive
  https://www.google.com/intl/es_ALL/drive/

- Dropbox
  https://www.dropbox.com/es_ES/

- Microsoft OneDrive
  https://account.microsoft.com/account/onedrive

Estas son las recomendaciones básicas en cuanto a las copias de seguridad:

- Haz y conserva al menos **dos copias de seguridad** actualizadas. En el caso de que hayamos sufrido un ataque por *ransomware* tenemos tres opciones:
  - Pagar el rescate
  - Recuperar la información desde una copia de seguridad
  - O asumir que hemos perdido nuestros datos

  De estas tres opciones, la mejor, sin lugar a dudas, es recuperar nuestra información desde una copia de seguridad. Y como las copias también pueden fallar, se recomienda mantener al menos dos copias actualizadas en todo momento.

- Guarda las copias de seguridad **en un lugar diferente** al del ordenador. Hay tipos de *ransomware* que infectan y cifran la información (incluidos los ficheros de las copias de seguridad) de discos duros o sistemas de almacenamiento de red distintos al equipo infectado. Por lo tanto, lo ideal es almacenar las copias de seguridad, siempre que sea posible, en discos físicos (DVD o similar) o en soportes externos no conectados a nuestra red (en otra ubicación física, a ser posible).

- Si haces la copia de seguridad en la nube *(cloud)* y se sincroniza continuamente, recuerda que algunas familias de *ransomware* también cifran y bloquean los *backups* en *la nube* Desactiva la sincronización persistente siempre que sea posible.

- **Comprueba que las copias de seguridad que tienes funcionan correctamente y que puedes y sabes recuperarlas**. Las copias de seguridad también pueden corromperse. Por eso es necesario una comprobación periódica de esa copia de respaldo. Para ello hay que probar a restaurar algunos ficheros cada cierto tiempo.

NOTA: 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. Este tipo de conexiones se suelen utilizar cuando estamos fuera de la organización y queremos acceder a cualquier documento interno de nuestra red corporativa. De esta forma tendremos acceso a todos nuestros documentos y a la vez navegaremos seguros.

- **Evita visitar sitios web de contenido dudoso**. Existen páginas web que, aun aparentando ser buenas y legítimas, esconden los llamados *exploit kits* que detectan las vulnerabilidades de nuestro navegador web y las aprovechan para instalar *ransomware* en nuestro equipo. Para evitar esto, siempre se recomienda **mantener actualizados los navegadores web**, y al mismo tiempo tener prudencia en nuestras actividades online.

4. Recuperar la información cifrada

Si has tenido una infección por *ransomware* y te están extorsionando para pagar un rescate hay que saber cómo actuar. En cualquier caso, debes seguir estas 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. Aísla o apaga los equipos que no estén aún del todo afectados para minimizar los daños.
- 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*

Aunque muchos antivirus y herramientas antimalware ya incluyen entre sus funcionalidades la protección frente al *ransomware*, existen numerosas herramientas y aplicaciones específicas que ayudan en la detección y prevención del mismo.

Además, muchos de los principales fabricantes de antivirus disponen de herramientas específicas de desencriptado de ficheros para aquellas variantes de *ransomware* cuyas organizaciones cibercriminales responsables han sido desarticuladas o se han podido encontrar de algún modo las claves necesarias para desencriptar los ficheros.

A continuación, se indica una relación de las herramientas más 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