Ransomware: una guía de aproximación para el empresario

INSTITUTO NACIONAL DE CIBERSEGURIDAD

SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe_

Índice

1 Introducción

La evolución de la tecnología con la irrupción de Internet, los dispositivos móviles, la nube y más recientemente la Internet de las cosas (IoT), están provocando una verdadera invasión de dispositivos, redes y aplicaciones en todos los ámbitos de la empresa. Como era de esperar, esta irrupción no está exenta de riesgos ya que las mismas ventajas de inmediatez, miniaturización, movilidad, facilidad de pago, comunicación, etc. de las que se benefician las empresas, gobiernos y usuarios, son también aprovechadas por los que se dedican a realizar actividades maliciosas.

Dentro de estas actividades maliciosas, hay una que se está desarrollando con rapidez y causando un gran impacto tanto en empresas como en ciudadanos. Es un tipo de extorsión denominada genéricamente **ransomware**.

Por definirlo de forma sencilla, el ransomware es un tipo de malware (software malintencionado) que tiene como objetivo bloquear el uso del ordenador o parte de la información que contiene, para después poder pedir un **rescate** a cambio de su liberación.

Su aparición data de los años 80 pero es ahora cuando está creciendo de forma exponencial. Las razones de la proliferación de este tipo de malware tienen que ver con la difusión y desarrollo de la tecnología que permite a los delincuentes obtener una **gran rentabilidad económica**, les proporciona **facilidad para ocultarse** y les facilita sistemas de pago internacionales que permiten el anonimato, como *Bitcoin* [1]. Esto, junto con los avances en criptografía y a la proliferación de dispositivos móviles y los *smartdevices* (*smartTV*, *smartwatches*, vehículos inteligentes...) de la IoT, está provocando tanto la aparición de grupos especializados en su desarrollo como el aumento de los recursos que los ciberdelincuentes destinan a su creación.

El ransomware afecta a cualquier usuario, negocio o actividad que pueda pagar a cambio de la devolución de su información. Este malware está afectando a usuarios domésticos, negocios, gobiernos e incluso servicios críticos como hospitales o centrales energéticas, causando pérdidas temporales o permanentes de información, interrumpiendo la actividad normal, ocasionando pérdidas económicas para restaurar los sistemas y ficheros, y en algunos casos daños de reputación. En esta guía os proponemos actuaciones para conocer, prevenir y mitigar esta amenaza.

2 ¿Qué es el ransomware?

El ransomware es un tipo de malware que hoy en día se está propagando de forma muy activa por internet. Este malware impide el acceso y amenaza con destruir los documentos y otros activos de las víctimas si estas no acceden a pagar un rescate.

Recordamos que el malware (virus, troyanos,...) es un software que si llega a los ordenadores de las víctimas, los infecta, manipulando el sistema y provocando mal funcionamiento o que realice acciones maliciosas. En el caso del ransomware, es un malware que cifra ciertos archivos o bien todo el disco duro de la víctima, bloqueándolo para impedir que el usuario acceda a sus ficheros y solicitando un rescate para recuperar el acceso al sistema y los ficheros.

El ransomware se propaga como otros tipos de malware; el método más común es mediante el envío de correos electrónicos maliciosos a las víctimas, los cibercriminales las engañan para que abran un archivo adjunto infectado o hagan clic en un vínculo que les lleva al sitio web del atacante, dónde se infectan.

2.1 ¿Por qué se llama así?

Ransomware se forma al unir *ransom* (rescate, en inglés) con *ware* (producto o mercancía, en inglés). Ya que en este caso el malware pide un **rescate** (*ransom*) a la víctima, a través de un mensaje o una ventana emergente, de ahí el nombre. Es un «secuestro virtual» de nuestros recursos por el que nos piden un rescate.

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.

> "Su página web está bloqueada.Transfiera 1,4 BitCoin a la dirección WWWWWWWh8Q6d2j1B4XXXXXXXXXT4vTDbSM9 para desbloquearla."

Es común que el rescate se solicite a través de alguna moneda virtual como *Bitcoins* o que se utilicen muleros, que son intermediarios que transfieren el dinero procedente de estas actividades ilícitas (de forma voluntaria o involuntaria). Tanto las monedas virtuales como los muleros permiten al ciberdelincuente ocultarse. El rescate suele variar entre cientos y miles de euros.

A cambio del pago, los ciberdelincuentes prometen el mecanismo para desbloquear el ordenador y descifrar los ficheros. Como tratamos con delincuentes no tenemos garantías, por lo que **se recomienda no pagar el rescate**. Además, para acceder al mecanismo de desbloqueo dirigen a la víctima a un enlace que podría a su vez contener malware y causar otra infección. Es muy frecuente que los ordenadores infectados por ransomware estén también infectados con otro tipo de malware.

"Están proliferando redes de ciberdelincuentes especializadas en ransomware."

2.2 ¿Quién está detrás del ransomware?

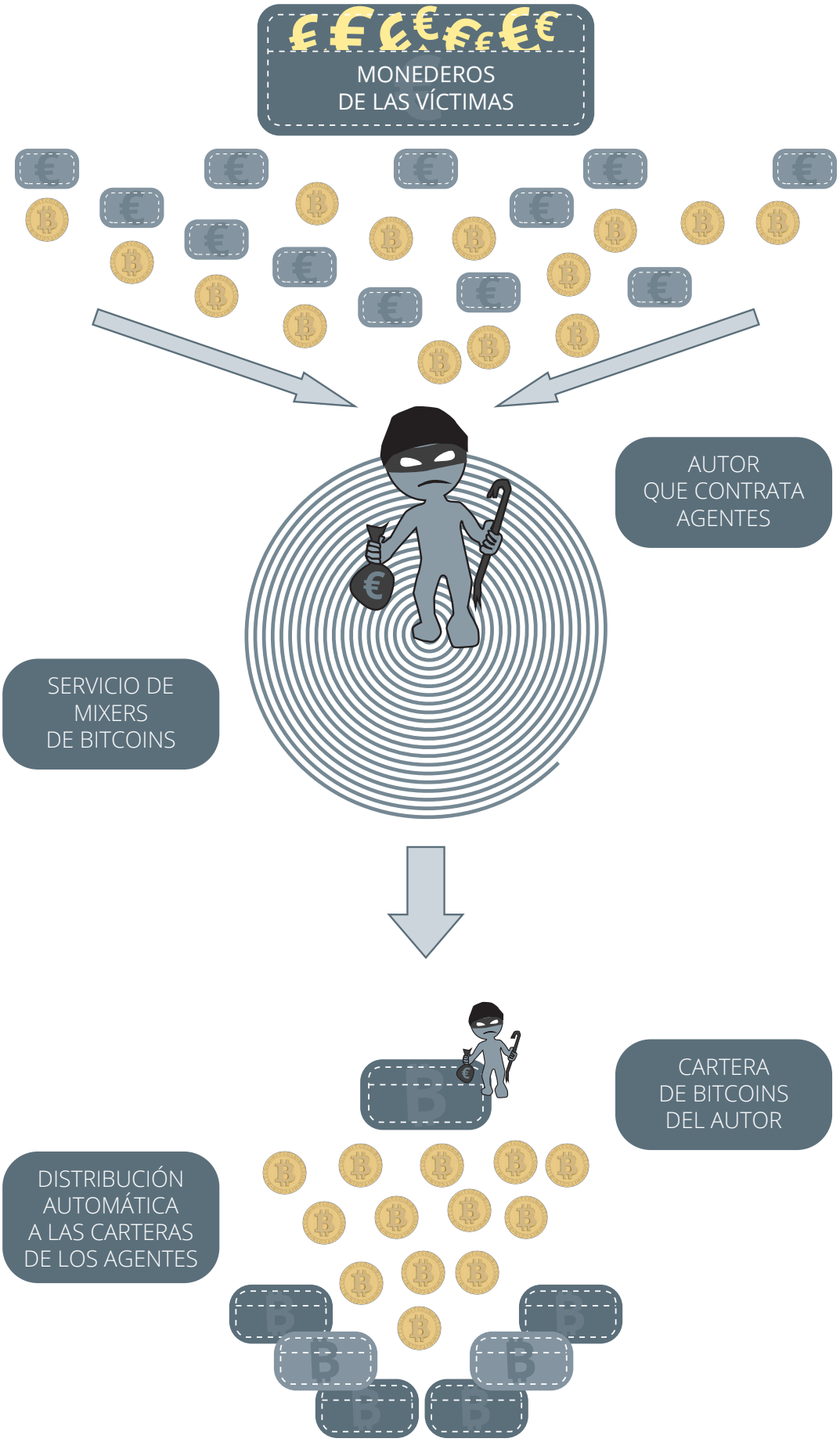
El ransomware, como otros tipos de malware, es un negocio, ilícito, pero un negocio. Además, no es muy costoso ponerlo en marcha y los beneficios son importantes. Están proliferando redes de ciberdelincuentes especializadas en ransomware. En este negocio participan además del creador del ransomware, los que alquilan la infraestructura para su distribución o los agentes que lo distribuyen y los servicios para recaudar el rescate. Aprovechando las ventajas de la tecnología, los ciberdelincuentes utilizan los modelos de negocio que proporciona internet (P2P, *crowdsourcing*, redes de afiliados o piramidales, inserción de publicidad, SaaS o *software as a service*,...), para obtener beneficio y ocultar su actividad maliciosa. Funcionan como un ecosistema del cibercrimen: los desarrolladores del malware se llevan una parte; otra parte los que desarrollan y gestionan los kit de *exploits* [2] para, aprovechando las vulnerabilidades de los equipos de las víctimas, poder difundirlo; lo mismo que los que alojan los servidores de correo o las páginas maliciosas con el malware y los agentes que cobran el rescate.

Algunas familias de ransomware funcionan como un servicio: *Ransomware as a Service* [3]. El delincuente contacta con agentes para distribuir el ransomware. Los agentes, al igual que los muleros que cobran los rescates, pueden ser cualquier persona con conocimientos de internet y algo de tiempo. Los agentes distribuyen el malware (alojándolo en sitios legítimos, mediante correos electrónicos, con ataques tipo abrevadero o *waterhole*,...) y si consiguen que alguien pague el rescate obtendrán una parte del mismo.

2.3 ¿Por qué piden el rescate en bitcoins?

Los *bitcoins* son monedas virtuales o criptomonedas, que permiten el pago anónimo entre particulares. Este anonimato es posible gracias a los servicios de *mixing* o *tumbling* de bitcoins [4], accesibles desde la red anónima Tor [5], que mezclan los fondos de distintas carteras, realizando una especie de lavado de la criptomoneda que dificulta que se pueda seguir el rastro de las transacciones. Esto facilita que los cibercriminales puedan extorsionar a sus víctimas sin que la policía pueda seguirles la pista.

El siguiente gráfico explica cómo funciona:


MONEDEROS
DE LAS VÍCTIMAS
AUTOR
QUE CONTRATA
AGENTES
SERVICIO DE
MIXERS
DE BITCOINS
CARTERA
DE BITCOINS
DEL AUTOR
DISTRIBUCIÓN
AUTOMÁTICA
A LAS CARTERAS
DE LOS AGENTES

2.4 ¿Cómo te infecta?

"El ransomware utiliza agujeros de seguridad del software y técnicas de ingenieria social para instalar el malware."

Como pasa en el caso de otros tipos de malware, los ciberdelincuentes van utilizar una o varias de estas vías para infectar a la víctima:

Aprovechar **agujeros de seguridad (vulnerabilidades) del software** de los equipos, sus sistemas operativos y sus aplicaciones. Los desarrolladores de malware disponen de herramientas que les permiten reconocer dónde están estos agujeros de seguridad e introducir así el malware en los equipos.

- Recientemente, algunas variedades de ransomware utilizan **servidores web desactualizados** como vía de acceso para instalar el ransomware.

- También se están aprovechando 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. que no estaban conectados a ninguna red informática, son conectados a redes corporativas o internet sin las mínimas medidas de seguridad.

Conseguir las cuentas con privilegios de administrador de acceso a los equipos mediante engaños (*phishing* y sus variantes), debilidades de procedimiento (por ejemplo no cambiar el usuario y contraseña por defecto) o vulnerabilidades del software. Con estas cuentas podrán instalar software, en este caso malware en los equipos.

- Muchos de los equipos los antiguos equipos SCADA o IoT que se están conectando últimamente a internet, conservan las mismas credenciales genéricas de acceso y administración.

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 adjunto con una supuesta actualización de software de uso común 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** que contiene enlaces web maliciosos o ficheros adjuntos como un documento de Microsoft Office o un fichero comprimido (.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 se aperciban aprovechando las vulnerabilidades de su navegador. También utilizan técnicas de ***malvertising*** o *malvertizing* que consiste en incrustar anuncios maliciosos en sitios web legítimos. El anuncio contiene código que infecta al usuario sin que este haga clic en él.

2.5 Variedades de ransomware

"El ransomware es una actividad criminal que tiene muchas formas siendo cada vez más sofisticado y destructivo."

El ransomware es una actividad criminal que tiene muchas formas. Desde sus comienzos este tipo de malware se ha ido haciendo cada vez más sofisticado y destructivo. Algunos vienen asociados a otros tipos de malware que roban información (cuentas de bancos, credenciales de acceso...), abren puertas traseras o instalan *botnets* [6]. También personalizan sus mensajes al idioma de las víctimas. Inicialmente bloqueaban el acceso al sistema operativo o al navegador a cambio de un rescate no muy elevado que se cobraba mediante el envío de un SMS a un número corto (como los de información de las compañías de telefonía o las campañas de ayuda en desastres) o con una transferencia a un monedero electrónico. Cuando la policía desmanteló esta forma de pago tuvieron que evolucionar.

Las mejoras en el cifrado hicieron posible la aparición de las criptomonedas que les garantizaba un sistema de pago anónimo de los rescates. Por otra parte también la evolución de las técnicas de cifrado permitió que mejoraran su mecanismo de extorsión (antes utilizaban programas que bloqueaban el sistema), cifrando la valiosa información que se encuentra en los discos duros y otros sistemas de almacenamiento de sus víctimas, lo que les permitió aumentar el valor del rescate. En el último año, según datos de Kaspersky [7] el número de ataques se quintuplicó. También se duplicaron los ataques a usuarios corporativos.

Se expanden internacionalmente. Algunas variedades cifran, además del equipo infectado, los dispositivos de almacenamiento conectados, los dispositivos de almacenamiento en red compartidos que tengan asociados o los servicios en la nube que estén mapeados en el ordenador infectado. Aparecen nuevas variantes para dispositivos móviles y dispositivos de la IoT.

En los seis primeros meses de 2016 [8] han aparecido varias decenas de nuevas familias que han causado a las empresas pérdidas de varios cientos de millones de euros. Algunos ataques iban dirigidos a sectores específicos como los videojuegos o el sector sanitario. Variantes de estas familias han aparecido en las noticias recientemente: CriptXXX, Crysis, BlackShades, Jigsaw, Apocalypse, FLocker, RAA, GOOPIC, Kozy.Jozy, MIRCOP, Locky, TeslaCrypt, MSIL o Samas (SAMSAM), Xorist, CryptorBit, Criptowall y CTB-Locker.

3 ¿Cómo puedo protegerme?

Para protegerse ante el ransomware es necesario adoptar una serie de buenas prácticas con dos propósitos:

- por una parte, evitar caer víctimas de engaños conociendo las técnicas de ingeniería social;
- por otra parte, configurar y mantener los sistemas evitando que sean técnicamente vulnerables.

3.1 Concienciación y formación

Más de la mitad de las infecciones con ransomware tienen lugar por medio de ataques de ingeniería social. Es decir, engañan a los usuarios bien para que les den acceso bien para instalar el malware o para conseguir las contraseñas de acceso con las que entrar e instalarlo.

Es esencial que formemos y concienciemos a nuestros empleados enseñándoles a reconocer estas situaciones y cómo actuar en consecuencia.

Los usuarios han de conocer las políticas de la empresa en materia de ciberseguridad, por ejemplo las relativas al uso permitido de aplicaciones y dispositivos, el uso de wifis públicas, la seguridad en el puesto de trabajo y en movilidad, y la política de contraseñas.

3.1.1 ¿Cómo funciona un ataque de ingeniería social?

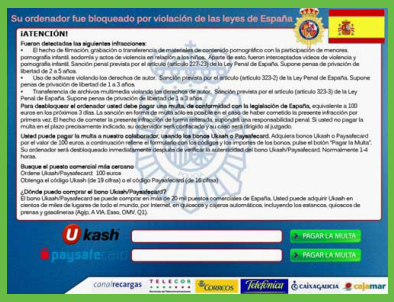
Los ataques de ingeniería social no son muy distintos de los clásicos timos. El ciberdelincuente sigue los mismos pasos que el timador «presencial»: reconocimiento, establecimiento, contacto y confianza, manipulación para obtener su objetivo y marcharse sin levantar sospechas.

El primer paso va a ser intentar reunir toda la información posible sobre la empresa que le pueda ser útil para conocer a su víctima, información como listados de empleados y teléfonos, departamentos, ubicación, proveedores,...

A continuación seleccionará una víctima (generalmente un empleado o algún colaborador de la empresa) y tratará de establecer alguna relación que le permita ganarse su confianza utilizando la información obtenida: su banco de confianza, la empresa de mantenimiento informático, una situación particular, etc.

Una vez se ha ganado su confianza, manipula a su víctima para obtener la información que necesita (credenciales, información confidencial,...) o conseguir que realice alguna acción por él (instalar un programa, enviar algunos correos, hacer algún ingreso...).

3 ¿Cómo puedo protegerme?



"Como norma, desconfíe de todos los mensajes recibidos en los que se le coaccione a hacer una acción ante una posible sanción."

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;
- de la voluntad de ser útil, ayudar o colaborar que se aprecia en entornos laborales y comerciales;
- del temor a perder algo, como en los mensajes 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;
- apelando al ego de los individuos al decirles que ha ganado un premio o ha conseguido algo y que para obtenerlo tienen que realizar una acción que en otro caso no harían;
- creando situaciones de urgencia y consiguiendo los objetivos por pereza, desconocimiento o ingenuidad de la víctima.

Por último, tras conseguir su objetivo, tienen que apartarse sin levantar sospechas. En ocasiones destruyen las pruebas que puedan vincularles con alguna actividad delictiva posterior que ejecuten con la información obtenida (por ejemplo: accesos no autorizados si obtiene credenciales, publicación de información,...)

3.1.2 ¿Cómo reconocer un ataque de ingeniería social?

Para evitar el ransomware, o cualquier tipo similar de ataque realizado mediante ingeniería social, desconfíe de cualquier mensaje recibido por correo electrónico, SMS, Whatsapp o redes sociales en el que se le coaccione o apremie a hacer una acción ante una posible sanción.

Como pautas generales, para evitar ser víctima de fraudes de tipo ransomware:

- No abra correos de usuarios desconocidos o que lo haya solicitado: elimínelos directamente. No conteste en ningún caso a estos correos.
- Revise los enlaces antes hacer clic aunque sean de contactos conocidos. Desconfíe de los enlaces acortados o utilice algún servicio para expandirlos antes de visitarlos.
- Desconfíe de los ficheros adjuntos aunque sean de contactos conocidos.

"Para evitar ser infectado es imprescindible concienciarse y adoptar medidas técnicas y de procedimiento."

- Tenga siempre actualizado el sistema operativo y el antimalware. En el caso del antimalware compruebe que está activo.
- Asegúrese de que las cuentas de usuario de sus empleados utilizan contraseñas robustas y no tienen permisos de administrador.

Para entrenarse ante este tipo de técnicas, Incibe pone a disposición de las empresas un kit de concienciación [9].

3.2 Prevención

Para evitar ser infectado, además de ser imprescindible las medidas de concienciación, se deben tomar una serie de **medidas técnicas y de procedimiento**.

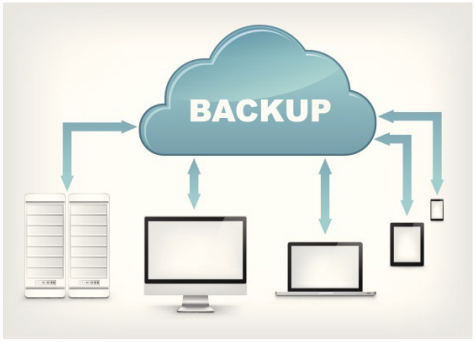
Las medidas técnicas van a permitir que nuestros sistemas no tengan agujeros de seguridad, manteniéndolos actualizados y bien configurados. También tendremos que adoptar un buen diseño de nuestra red para evitar que expongamos servicios internos al exterior, de manera que sea más difícil para el ciberdelincuente infectarnos.

Por otra parte, los procedimientos han de describir las actuaciones para: tener actualizado todo el software, hacer copias de seguridad periódicas, controlar los accesos, restringir el uso de aplicaciones o equipos no permitidos, actuar en caso de incidente, etc.

Por último la vigilancia y las auditorías van a mantenernos alerta ante cualquier sospecha.

3.2.1 Copias de seguridad

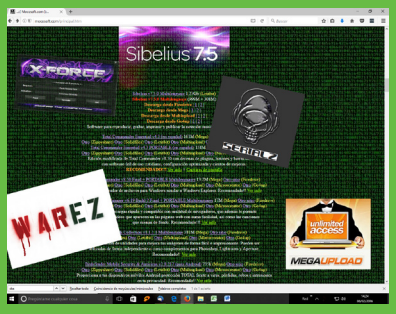
En caso de que seamos objeto de un ataque de ransomware, la principal medida de seguridad (y puede que la única) que va a permitirnos recuperar la actividad de nuestra empresa en poco tiempo, son las copias de seguridad o backups.



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 desde una copia de seguridad o asumir que hemos perdido nuestros datos. De estas tres opciones, la mejor, sin lugar a dudas, es recuperar nuestros contenidos desde un *backup*. Y como los *backups* también pueden fallar, se recomienda mantener al menos dos copias actualizadas en todo momento.

3 ¿Cómo puedo protegerme?



"Evita visitar sitios web de contenido dudoso."

- Guarda las copias de seguridad **en un lugar diferente** al del servidor de ficheros. Dado que existen especímenes de ransomware que infectan y cifran la información (incluido los ficheros de las copias de seguridad) de discos duros o sistemas de almacenamiento de red distintos al equipo infectado, lo ideal es almacenarlos, siempre que sea posible, en discos físicos (DVD o Blu-Ray) o en soportes externos no conectados a nuestra red (en otro edificio, a ser posible).

- Si haces el *backup* en *cloud* y se sincroniza continuamente, recuerda que algunas familias de ransomware también cifran y bloquean los *backups* en *cloud* con esta funcionalidad. Desactiva la sincronización persistente.

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

3.2.2 Navega seguro

Utiliza **redes privadas virtuales** 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 empresa y queremos acceder a cualquier documento que tengamos en la intranet o en nuestro equipo corporativo. De esta forma tendremos acceso a todos nuestros documentos y a la vez navegaremos seguros.

Evita visitar sitios web de contenido dudoso. Ya hemos comentado que existen páginas web que, aparentando ser buenas y legítimas, esconden los llamados *exploit kits* que detectan las vulnerabilidades de nuestro navegador de internet y las aprovechan para instalar ransomware en nuestro ordenador. Para evitar esto, como siempre, es recomendable **mantener actualizados los navegadores web**, pero también es sensato tener un poco de prudencia en nuestras actividades online.

3.2.3 Actualiza

Los ciberdelincuentes se aprovechan de las vulnerabilidades o agujeros de seguridad en el software, los sistemas operativos o el firmware, incluso de forma automatizada (*exploit kits*). Por ello 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 y centralizada**.

Si utilizas software a medida, asegúrate que en su diseño se han tenido en cuenta requisitos de seguridad. Solicita la asistencia de expertos en auditorias del software para evitar las vulnerabilidades de este tipo de software.

"Hay que evitar que los usuarios y grupos tengan más privilegios de los que necesitan."

3.2.4 Mínimos privilegios

Un principio básico de seguridad es mantener los privilegios de seguridad de usuarios y grupos al mínimo, es decir, evitar que los usuarios y grupos de usuarios tengan más privilegios de los que necesitan. Esto es posible gestionando los privilegios de las cuentas de los usuarios y los permisos para acceder a la información o para instalar software.

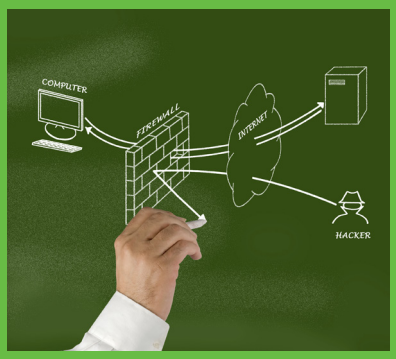
Para los usuarios generales se han de utilizar **cuentas que tengan privilegios limitados**, en lugar de las cuentas con privilegios de «administrador». Así evitamos que los usuarios generales tengan acceso a servicios, información o procedimientos que no necesitan para su actividad. Esto proporciona una protección adicional al prevenir que se instalen distintos tipos de malware, por error o si perdieran o les robaran sus credenciales. Las cuentas con privilegios deben ser sólo utilizadas por los administradores. Estos son algunos consejos básicos en cuanto al uso de cuentas de usuario:

- **Utiliza contraseñas robustas y políticas de bloqueo de cuentas ante un número determinado de intentos de acceso**. Los atacantes generalmente llegan a nuestro sistema a través de otros servicios nuestros más desprotegidos (redes sociales, servicios abiertos de la compañía...). Una vez acceden a esos servicios se quedan a la espera para obtener más información y poder engañarnos de una forma más creíble para que acabemos ejecutando el ransomware que cifrará nuestro sistema. Para proteger nuestros servicios utilizaremos siempre contraseñas robustas y políticas de bloqueo en caso de que se realicen un número de intentos de acceso sin éxito en el sistema de control de acceso.

- **No utilices cuentas con permisos de administrador**. Si usamos este tipo de usuario y nuestra contraseña llega a manos del atacante, este tendrá un control total sobre nuestro equipo. Si, en cambio, usamos cuentas de usuario con permisos limitados, hacemos que el atacante lo tenga más difícil para llegar a datos críticos.

- **Elimina o deshabilita aquellas cuentas de usuario que no sean necesarias**. Cualquier cuenta que tenga acceso a nuestro equipo es una posible fuente de acceso al mismo. No hace falta tener una cuenta de «invitado». Si no usamos algo, mejor quitarlo. También debemos eliminar las cuentas que ya no se utilicen y la de los empleados que no pertenezcan ya a nuestra empresa.

A la hora de configurar las cuentas de usuario, perfiles y permisos relativos a los **controles de acceso**, se ha de hacer con este principio de mínimos privilegios en mente. Así el acceso a ficheros, directorios y espacios de almacenamiento compartido, en particular con permi-



"Se recomienda utilizar programas que eviten que los empleados instalen aplicaciones no permitidas."

sos de escritura y para compartirlos, será exclusivo de aquellos que realmente lo necesitan.

Es también una buena práctica **clasificar los datos** según su valor para la empresa, en qué parte de la organización se utilizan y la seguridad que necesitan. Así se podrán aplicar medidas para **separar física y lógicamente** los lugares donde se ubica la información y aplicar controles de acceso por perfiles (los de contabilidad acceden a los programas y datos de contabilidad, pero no a otros) o medidas de protección especiales (como cifrado) en casos de información más sensible o confidencial. Una forma de separar aplicaciones o sistemas críticos es utilizar **entornos virtualizados**.

Por otra parte también es recomendable utilizar programas para **evitar que los empleados instalen aplicaciones no permitidas**. Es lo que se conoce políticas de restricción de software. De forma automática puede implementarse con software basado en listas blancas de aplicaciones. Este software impedirá que se instale y ejecute software no permitido.

Las políticas de restricción del uso del software pueden incluir controles para evitar que se ejecute malware desde carpetas temporales de los navegadores o desde programas de compresión/descompresión de ficheros o en las carpetas ocultas del sistema.

3.2.5 Mínima exposición

Otro principio básico de seguridad es el de **mínima exposición**, es decir, evitar la exposición al exterior de la red interna de la empresa o de aquella información o servicio que no necesita ser accedida desde el exterior de la misma.

Las empresas necesitan ofrecer algunos servicios a través de Internet a sus clientes o trabajadores: correo electrónico, página web corporativa, aplicaciones remotas o repositorios de ficheros. Algunas empresas optan por la subcontratación de estos servicios. Otras prefieren hacerlo internamente y asumen la instalación y gestión de los servidores y equipos en sus propios locales, de forma que pueden ahorrar costes y aumentar el control sobre su información.

En este caso es necesario separar los servidores accesibles desde el exterior de los servidores privados de nuestra organización.

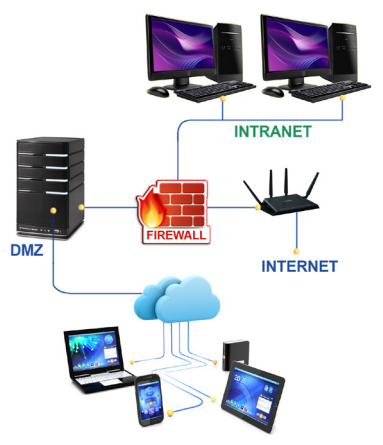
Para hacer que aquellos servidores que queremos sean accesibles desde Internet, es necesario abrir una parte de nuestra red, evitando siempre que el resto de la misma quede desprotegida: esto se consigue mediante el uso de cortafuegos.

Un **cortafuegos (o *firewall*)** es un sistema de seguridad capaz de establecer reglas para bloquear o permitir conexiones de entrada o salida de nuestra red.

Para que el cortafuegos «sepa» lo que está permitido y lo que no, deberemos configurar:

- Qué tipo de conexiones permitimos (web, correo, chat, descargas P2P, etc.).

3 ¿Cómo puedo protegerme?



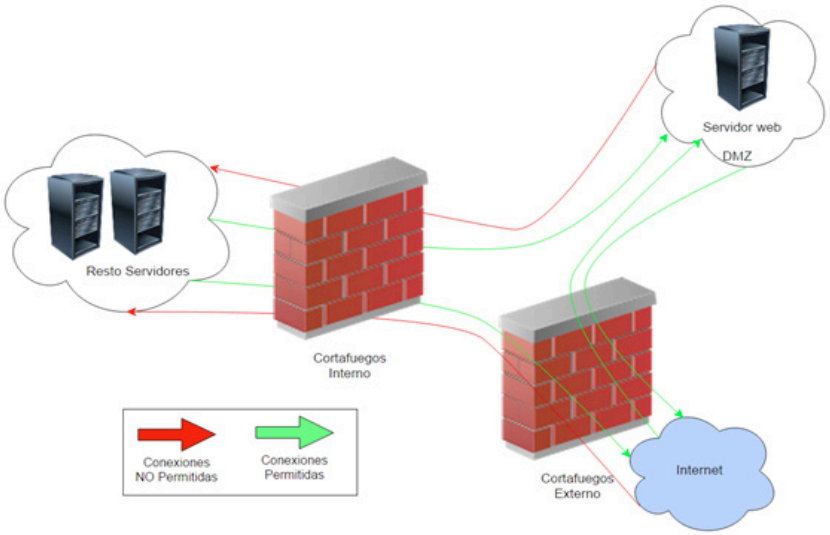
"Si necesitamos contar con un servidor accesible desde internet es fundamental montarlo en una DMZ."

- En qué sentido las permitimos (hacia Internet o desde Internet).
- A qué equipos afecta (todos los equipos, solo uno o un conjunto ellos).
- Qué direcciones IP están bloqueadas (por estar en listados de IP maliciosas).

Además, una medida básica de seguridad, es deshabilitar el protocolo de acceso remoto (RDP o escritorio remoto en Windows) a los sistemas si no se está utilizando.

Pero un cortafuegos no es suficiente para proteger nuestros servidores internos. Una vez hemos permitido el acceso a nuestra red, un posible atacante podría aprovechar una vulnerabilidad de nuestro servidor para comprometerlo y desde ahí intentar atacar a otros servidores a los que en un principio no tiene acceso desde el exterior de la red.

Para evitar esta posible brecha de seguridad existe una configuración denominada **zona (o red) desmilitarizada (DMZ).**



Una red DMZ es una red aislada del resto de la red interna, donde se ubican únicamente los servidores que deben ser accesibles desde Internet. De esta forma, si se ataca y compromete uno de estos servidores, el resto de la red estará protegida.

Así pues, esta red DMZ, por el hecho de estar expuesta a ataques desde Internet, deberá estar especialmente controlada y monitorizada, siendo muy recomendable **instalar detectores de intrusos**, tener especial cuidado a la hora de proteger sus servidores y considerarlos prioritarios a la hora de instalar actualizaciones y parches de seguridad críticos.

Algunos ejemplos de equipos candidatos a estar dentro de una DMZ serían:

- servidores de correo y *webmail;*
- servidores de VPN (Redes Privadas Virtuales);
- servidores DNS (Servidor de Nombres de Dominio).

"El correo electrónico es una de las principales vias de entrada de malware en nuestro ordenador."

Si contratamos servicios tecnológicos o externalizamos alguno de ellos sobre las instalaciones de proveedores hemos de incluir en **los acuerdos de nivel de servicio** las cláusulas que nos permitan verificar que toman estas medidas de mínima exposición y el resto de medidas técnicas de este apartado.

3.2.6 Configurar el correo electrónico

El correo electrónico es una de las principales vías de entrada de correos de *phishing* con los que intentarán robarnos las contraseñas de acceso a nuestros servicios, y otros con engaños para que instalemos malware o visitemos páginas dónde infectarnos. Por ello los servidores de correo electrónico deben:

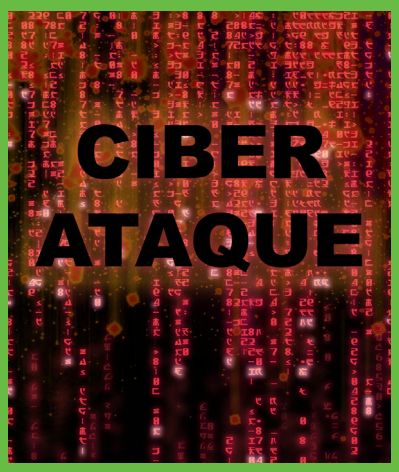
- Contar con **filtros de spam** para evitar que los emails de phishing lleguen al buzón de los empleados. Este filtro debe estar activado y configurado, y revisarse de forma continua. De esta manera, se evita que el empleado tome la decisión de abrir ficheros adjuntos o que haga clic en enlaces potencialmente peligrosos para él y para la empresa.

- Evitar el email *spoofing* o suplantación de correo electrónico utilizando **autenticación de correos entrantes** (existen distintas tecnologías: *Sender Policy Framework* o SPF, *Domain Message Authentication Reporting and Conformance* o DMARC, y *DomainKeys Identified Mail* o DKIM).

- **Escanear los correos entrantes y salientes** para detectar amenazas y filtrar ficheros ejecutables o los comprimidos para evitar que alcancen al empleado. Igualmente configura el sistema operativo para que te deje ver las extensiones de los archivos.

- **Deshabilitar las macros** de los ficheros de Office transmitidos por correo electrónico o bien utilizar un Office Viewer en lugar de abrir los ficheros directamente con los programas de la suite de Microsoft Office.

- **Desactivar el HTML** en las cuentas de correo críticas. Este formato permite incluir un lenguaje de programación denominado JavaScript, muy utilizado para funcionalidades que nos ofrece el correo electrónico. Esta funcionalidad puede hacer que los *spammers* verifiquen que la dirección de correo electrónico es válida o redirigir el navegador web del usuario a una página web maliciosa que acabe infectando nuestro ordenador. Es recomendable la desactivación del formato HTML en el correo electrónico, al menos en las cuentas de correo críticas o que se encuentren a disposición del público para contactar con nuestra empresa. De esta manera no sería posible la visualización de correos electrónicos atractivos, pero este sería mucho más seguro.



"En caso de ataque hay que apagar el equipo y aislarlo de la red de inmediato."

3.2.7 Plan de respuesta a incidentes

Otra acción de carácter preventivo es tener un plan de actuación o respuesta ante incidentes. Esta es una representación esquemática de las fases que ha de tener este plan:

- En la fase de **preparación** se ha de fijar:
  - Quién ha de realizar la gestión de los incidentes dentro de la empresa.
  - Dónde está la documentación necesaria sobre los sistemas y redes que se usan en la empresa. Definir cuál es la actividad «normal» que nos permita detectar actividades sospechosas que sean indicios de incidentes.
  - Con quién tendremos que contactar en caso de incidencia. Por ejemplo en caso de servicios externalizados el responsable en el proveedor. También es útil tener a mano la forma de contacto con algún Centro de respuesta ante incidentes, como el CSIRT [10] de INCIBE, que pueden indicarnos cómo recuperar nuestros archivos si existiera ya algún mecanismo probado.
  - En la fase de **detección y análisis** se ha de **clasificar el incidente** para determinar que es un ransomware, su origen, la criticidad de los sistemas afectados, etc. También en esta fase se ha de escalar el incidente en caso de que no tengamos recursos propios para resolverlo o necesitemos contar con expertos externos para su resolución.

- En la fase de **contención, resolución y recuperación**, se han de seguir los siguientes pasos:
  - **Aislar los equipos** con ransomware.
  - **Clonar los discos duros** de los equipos infectados.
  - **Aislar muestras de ficheros cifrados o del propio ransomware**.
  - **Denunciar el incidente**.
  - **Cambiar todas las contraseñas** de red y de cuentas online.

"Para protegerse hay que mantener los equipos actualizados, con antivirus, antispam, etc."

- **Desinfectar los equipos y recuperar los archivos cifrados**.
- **Restaurar los equipos** para continuar con la actividad.

Después de cerrado el incidente, se han de registrar todos los datos necesarios sobre el mismo, usuarios afectados, equipos, qué acciones se han tomado, resultados, etc. Con esto se pueden detectar mejoras para actuar en caso de que se repita un incidente similar.

3.2.8 Audita

Una buena práctica básica es **escanear los equipos con un antimalware** y programarlo para que se ejecute periódicamente. El software antimalware ha de estar actualizado y activo.

También recomendable realizar periódicamente una **auditoría** a nuestros sistemas tanto para poner a prueba nuestros mecanismos de seguridad o para comprender nuestra capacidad para defendernos de los ataques. En la actualidad esta tarea se está simplificado de forma significativa pues existen productos y servicios para automatizarla. No obstante, sigue siendo necesario que las realice personal especializado o contratar un servicio externalizado.

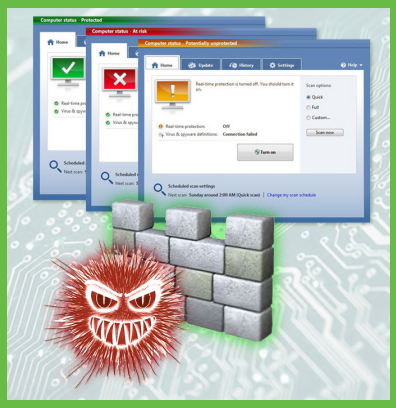
Estos son los aspectos que deben considerarse, para prevención del ransomware, cuando solicitamos una auditoría:

- protección **antivirus, antispam** y de filtrado de contenidos;
- administración de **permisos** de usuarios y **accesos** a servicios;
- seguridad de los **dispositivos móviles**;
- gestión automatizada de **actualizaciones y parches**;
- detección de **vulnerabilidades**;
- monitorización del **uso de los recursos** informáticos y de red;
- monitorización y análisis de **eventos de seguridad** en tiempo real (SIEM);

Estos son los distintos tipos de pruebas que puedes solicitar:

- **Test de penetración:** es un tipo de auditoría técnica que consiste en un conjunto de pruebas a las que se somete a una aplicación, servicio o sistema, con el objetivo de encontrar huecos o fallos a través de los cuales sería posible conseguir acceso no autorizado a información de la empresa.

3 ¿Cómo puedo protegerme?



"Una buena práctica es escanear los equipos con un antimalware y un antivirus periódicamente."

- **Auditoría de red**: permiten analizar la red de la empresa en busca de puertos abiertos, recursos compartidos, servicios o electrónica de red (*router*, *switch*, etc.). Además, en estas auditorías se emplean herramientas que permiten realizar la catalogación de las infraestructuras conectadas a la red o incluso detectar versiones de dispositivos inseguros, versiones de software o la necesidad de instalar actualizaciones o parches.

- **Auditoría de seguridad perimetral**: se trata de un proceso destinado a determinar el nivel de seguridad de las barreras que protegen la red de comunicaciones de una organización de los riesgos que provienen del exterior y del interior. Podríamos englobarla dentro de la auditoría de red, aunque está más especializada en detectar fallos de seguridad desde el punto de vista de exterior.

- **Auditoría web**: analiza los fallos de seguridad o vulnerabilidades que afectan al funcionamiento de una página web.

- **Auditoría forense:** son auditorías posteriores a un incidente de seguridad para identificar las causas que lo produjeron. Tiene como objetivo recabar y preservar las pruebas o evidencias de un incidente para, tras su posterior análisis, saber qué y como ha ocurrido, aprender de ello y depurar las posibles consecuencias legales.

4 ¿Qué hacer si me afecta?

Si has tenido un incidente de seguridad en el que te están extorsionando para pagar un rescate has de conocer cómo actuar. En todos los casos, debes seguir estas dos recomendaciones:

- **NO PAGAR** nunca el rescate.
- Si contamos con un **plan de respuesta a incidentes**, lo aplicaremos para que poder minimizar en lo posible los daños causados y poder recuperar la actividad corporativa lo antes posible. Este plan de respuesta, nos marcará las pautas a seguir para la obtención de evidencias para una posible denuncia de la acción delictiva.
- Si no tienes Plan de respuesta ante incidentes utiliza la última **copia de seguridad** de tu información para recuperar la información perdida.

4.1 ¿Cómo recupero mi actividad y mis datos?

Has de seguir los siguientes pasos:

- Contacta con el Centro de Respuesta a Incidentes CERTSI de INCIBE [10]. Te ayudarán a resolver el incidente y te indicarán cómo actuar y que pueden indicarnos cómo recuperar nuestros archivos si existiera ya algún mecanismo probado.
- Aísla los equipos con ransomware inmediatamente 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 contener los daños.
- Clona los discos duros de los equipos infectados, pues pueden servir de evidencia si vamos a denunciar. Este es un procedimiento que debe realizar técnicos experimentados. Esta copia también puede servirnos para recuperar nuestros datos en caso de que no exista aún forma de descifrarlos.
- Si fuera posible recoge y aísla muestras de ficheros cifrados o del propio ransomware como el fichero adjunto en el mensaje desde el que nos infectamos, por ejemplo.
- Denuncia el incidente [11 y 12]:
  - Guardia civil – Grupo de delitos telemáticos
  - Policía nacional – Brigada de Investigación Tecnológica (BIT)
- Si fuera posible cambia todas las contraseñas de red y de cuentas online. Después de eliminado el ransomware volver a cambiarlas.
- Desinfecta los equipos y recuperar los archivos cifrados (si fuera posible).
- Restaura los equipos para continuar con la actividad. Si fuera posible reinstala el equipo con el software original o arranca en modo seguro y recupera un *backup* previo si lo tuvieras.

4.2 ¿Por qué no has de pagar el rescate?

"Pagar el rescate no garantiza que los delincuentes nos den la clave de descifrado para recuperar nuestros documentos."

Si te ha ocurrido un incidente tendrás muchas dudas sobre si acceder a pagar el rescate o no. Nuestra recomendación es que no lo pagues y estos son los motivos:

- Pagar no te garantiza que volverás 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 Referencias

[1]. Bitcoin Wiki
https://es.bitcoin.it/wiki/Pagina_principal

[2]. Channebiz – Blog: Exploit Kits o conviértete en un hacker
http://www.channelbiz.es/2015/07/21/exploit-kits-o-conviertete-en-un-hacker/

[3]. Trendmicro Trendlabs: Economics Behind Ransomware as a Service: A Look at Stampado's Pricing Model
http://blog.trendmicro.com/trendlabs-security-intelligence/the-economics-behind-ransomware-prices/

[4]. Criptonoticias – Blog: Mixers, el servicio para lavar bitcoins
http://criptonoticias.com/colecciones/mixers-el-servicio-para-lavar-bitcoins/#axzz4J-5SuTYXe

[5]. The Tor Project
https://www.torproject.org/

[6]. INCIBE – Protege tu empresa – Herramientas – Servicio antibotnet
https://www.incibe.es/protege-tu-empresa/herramientas/servicio-antibotnet

[7]. Kaspersky – Blog: Historia y evolución del ransomware: datos y cifras
https://blog.kaspersky.com.mx/ransomware-blocker-to-cryptor/7295/

[8]. US-CERT Alert 31-03-2016 Ransomware and Recent Variants
https://www.us-cert.gov/ncas/alerts/TA16-091A

[9]. INCIBE – Protege tu empresa – Kit de Concienciación
https://www.incibe.es/protege-tu-empresa/kit-concienciacion

[10]. INCIBE – CERSI – Centro de Respuesta a incidentes
https://www.certsi.es/respuesta-incidentes/ciudadanos-y-empresas

[11]. Guardia Civil Grupo de Delitos Telemáticos
https://www.gdt.guardiacivil.es/webgdt/home_alerta.php

[12]. Policía Nacional – Brigada de Investigación Tecnológica
http://www.policia.es/org_central/judicial/udef/bit_alertas.html

[13]. Europol [et. al] No-More-Ransom
https://www.nomoreransom.org/

[14]. CCN-CERT Actualizado el Informe sobre medidas de seguridad contra el ransomware (13/02/2017)
https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/4251-actualizacion-del-informe-de-medidas-de-seguridad-contra-el-ransomware.html

[15]. INCIBE – CERTSI – Blog: Ransomware, herramienta de la ciberextorsión
https://www.certsi.es/blog/ransomware

[16]. INCIBE – Protege tu empresa – Blog: Enfrentándonos al Ransomware
https://www.incibe.es/protege-tu-empresa/blog/enfrentandonos-ransomware

5 Referencias

[17]. INCIBE – CERTSI – Blog: RANSOMWARE II: Malware de cifrado
https://www.certsi.es/blog/ransomware-de-cifrado

[18]. INICIBE - Protege tu empresa - Blog: Me han atacado... ¿y ahora qué? ¿Qué pasos se deben de dar para poner una denuncia?
https://www.incibe.es/protege-tu-empresa/blog/respuesta-juridica-incidente-ciberseguridad

[19]. INCIBE - Protege tu empresa - Blog: Que no te secuestren el ordenador: medidas para evitarlo (Infografía)
https://www.incibe.es/protege-tu-empresa/blog/que-no-te-secuestren-el-ordenador-medidas-para-evitarlo

[20]. INCIBE - Protege tu empresa - Blog: Historias reales: «¡Me han cifrado el disco duro!»
https://www.incibe.es/protege-tu-empresa/blog/historias-reales-me-han-cifrado-disco-duro

[21]. INCIBE - Protege tu empresa - Blog: Historias reales: «Hola, he cifrado todos los datos importantes de tu empresa»
https://www.incibe.es/protege-tu-empresa/blog/cifrado-datos-importantes-empresa-ransomware

[22]. INCIBE - Protege tu empresa - Blog: Descubre cómo proteger tu empresa del malware»
https://www.incibe.es/protege-tu-empresa/blog/descubre-proteger-tu-empresa-del-malware

[23]. Malware.es Ransomware el virus que secuestra un Sistema
http://www.malware.es/ransomware/

[24]. Dell.com – Portátiles – Ransomware: qué es y cómo eliminarlo
http://es.community.dell.com/support_forums/laptops_general_hardware/w/wiki/86.ransomware-que-es-y-como-eliminarlo

[25]. Microsoft Malware protection center – Ransomware
https://www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx

[26]. Trendmicro Blog: ¿Por qué funciona el ransomware? Psicología y métodos utilizados para distribuir, infectar y extorsionar
http://blog.trendmicro.es/?p=3033

[27]. Kaspersky anti-ransomware tool
https://go.kaspersky.com/Anti-ransomware-tool.html

[28]. Segu-Info Blog: Herramientas para detectar ransomware en Windows y Linux
http://blog.segu-info.com.ar/2016/03/herramientas-para-detectar-ransomware.html

[29]. Segu-Info Blog: 22 consejos para prevenir el #Ransomware
http://blog.segu-info.com.ar/2016/03/22-consejos-para-prevenir-el-ransomware.html

[30]. SANS Security Awareness Blog - OUCH
https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201608_sp.pdf

5 Referencias

[31]. ENISA – Glossary: Ransomware
https://www.enisa.europa.eu/topics/national-csirt-network/glossary/ransomware

[32]. Microsoft Technet blog: The 5Ws and 1H of Ransomware
https://blogs.technet.microsoft.com/mmpc/2016/05/18/the-5ws-and-1h-of-ransomware/

[33]. Servicio Antiransomware
https://www.incibe.es/protege-tu-empresa/herramientas/servicio-antiransomware

[34]. Juego de Rol
https://www.incibe.es/protege-tu-empresa/juego-rol-pyme-seguridad


GOBIERNO
DE ESPAÑA
MINISTERIO
DE ENERGÍA, TURISMO
Y AGENDA DIGITAL


incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD