Universidad Católica
Nuestra Señora de la Asunción

Facultad de Ciencias y Tecnología

Ingeniería Informática

Ransomware
El virus de hoy

Versión 1.0

Orlando Martínez
Estudiante de Ingenieria
orlando.martinez@uc.edu.py

Asunción - Paraguay

Para más información, póngase en contacto :

- **Springer-Asunción Paraguay**
  Facultad de Ciencias y Tecnologias Universidad Católica "Nuestra Señora de la Asunción"
  Teléfono: (0 21)441 044
  (+ 595)982 901951
  Eorreo Electrónico: orlando.martinez@uc.edu.py

Índice general

1. Introducción

Ransomware (del inglés ransom, 'rescate', y ware, por software) es un tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema infectado, y pide un rescate a cambio de quitar esta restricción. Algunos tipos de ransomware cifran los archivos del sistema operativo inutilizando el dispositivo y coaccionando al usuario a pagar el rescate

2. ¿Qué es el ransomware?

En lineas generales;

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. Tipos de Ransomware

CryptoLocker
En septiembre de 2013 hizo su reaparición el ransomware basado en el cifrado de archivos también conocido como CryptoLocker, el cual genera un par de claves de 2048-bit del tipo RSA con las que se controla el servidor y se cifran archivos de un tipo de extensión específica. El virus elimina la clave privada a través del pago de un bitcoin o un bono prepago en efectivo dentro de los tres días tras la infección. Debido al largo de la clave utilizada, se considera que es extremadamente difícil reparar la infección de un sistema.

En caso de que el pago se retrase más allá de los tres días, el precio se incrementa a 10 bitcoins, lo que equivalía, aproximadamente, a 2300 dólares, en noviembre de 2013.

CryptoLocker fue aislado gracias a que incautaron la red GameoverZeuS, tal como fue anunciado oficialmente por el Departamento de Justicia de los Estados

Unidos el 2 de junio de 2014.

El Departamento de Justicia emitió una acusación en contra del ciberdelincuente ruso Evgeniy Bogachev alegando su participación en la red Gameover-ZeuS. Se estima que consiguió al menos tres millones de dólares hasta que el malware fue desactivado.

CryptoLocker.F y TorrentLocker

En septiembre de 2014, una ola de ransomware llegó a sus primeros objetivos en Australia, denominados ÇryptoWallƶ ÇryptoLocker". Las infecciones se propagaban a través de una cuenta de correo australiana falsa, la cual enviaba un correo electrónico notificando entregas fallidas de paquetes. De este modo evitaba los filtros antispam y conseguía llegar a los destinatarios. Esta variante requería que los usuarios ingresaran en una página web y, previa comprobación mediante un código CAPTCHA, accedieran a la misma, antes de que el malware fuese descargado, de esta manera se evitó que procesos automáticos puedan escanear el malware en el correo o en los enlaces insertados.

Symantec determinó la aparición de nuevas variantes conocidas como CryptoLocker.F, el cual no tenía ninguna relación al original debido a sus diferencias en el funcionamiento. La Corporación Australiana de Broadcasting fue víctima de este malware tuvo que interrumpir su programa de noticias ABC News 24 durante media hora, trasladarse a los estudios de Melbourne y abandonar las computadoras pertenecientes al estudio de Sídney debido a CryptoWall.

TorrentLocker es otro tipo de infección con un defecto, ya que usaba el mismo flujo de claves para cada uno de los computadores que infectaba, el cifrado pasó a ser trivial pero antes de descubrirse ya habían sido 9000 los infectados en Australia y 11 700 en Turquía.

CryptoWall

CryptoWall es una variedad de ransomware que surgió a principios de 2014 bajo el nombre de CryptoDefense dirigida a los sistemas operativos Microsoft Windows. Se propaga a través del correo electrónico con suplantación de identidad, en el cual se utiliza software de explotación como Fiesta o Magnitud para tomar el control del sistema, cifrar archivos y así pedir el pago del rescate del computador. El rango de precios se encuentra entre los 500 y 1000 dólares.

En marzo de 2014, José Vildoza, un programador argentino, desarrolló una herramienta para recuperar los archivos de las víctimas de manera gratuita. La recuperación de archivos fue posible gracias a una falla en el programa malicioso por el cual las claves de cifrado quedaban guardadas en el equipo afectado.

Cuando los autores se percataron del error, actualizaron el criptovirus nombrándolo CryptoWall, pasando luego por distintas actualizaciones hasta llegar a la ver-

sión 3.0.

CryptoWall 3.0 ha sido reportado desde enero de 2015 como una infección que surge donde hackers rusos se encuentran detrás de esta extorsión.

Mamba

Un grupo de investigadores de seguridad de Brasil, llamado Morphus Labs, acaba de descubrir un nuevo ransomware de cifrado de disco completo (FDE - Full Disk Encryption) esta misma semana, llamado "Mamba". Mamba, como lo llamaron, utiliza una estrategia de cifrado a nivel de disco en lugar de uno basado en archivos convencionales. Para obtener la clave de descifrado, es necesario ponerse en contacto con alguien a través de la dirección de correo electrónico proporcionada. Sin eso, el sistema no arranca.

El ransomware Mamba se ha identificado el 7 de septiembre durante un procedimiento de respuesta a incidentes por parte de Renato Marinho, un experto en seguridad de Morphus laboratorios. Esta amenaza de malware utiliza el cifrado a nivel de disco que causa mucho más daño que los ataques basados en archivos individuales. Los desarrolladores criminales han utilizado el DiskCryptor para cifrar la información, una herramienta de código abierto.

Se hizo una comparación con el virus Petya que también utiliza disco cifrado. Sin embargo, Petya cifra solamente la tabla maestra de archivos (MFT) con lo que no afectan a los datos en sí.

Tras la exitosa infiltración, Mamba crea su carpeta titulada DC22 en la unidad C del equipo donde coloca sus archivos binarios. Un servicio del sistema se crea y alberga el proceso del ransomware. Un nuevo usuario llamado MythBusters se crea asociado con la contraseña 123456.

También sobrescribe el registro de inicio maestro (MBR) del disco del sistema que contiene el gestor de arranque para el sistema operativo. Esto prohíbe efectivamente al usuario de incluso cargar el sistema operativo sin ingresar el código de descifrado.

WannaCry

WanaCryptor o también conocido como "WannaCry.^{es} un ransomware .^{a}ctivo"que apareció el 12 de mayo de 2017 con origen en el arsenal estadounidense de malware Vault 7 revelado por Wikileaks pocas semanas antes, el código malicioso ataca una vulnerabilidad descrita en el boletín MS17-010 en sistemas Windows que no estén actualizados de una manera adecuada. Provocó el cifrado de datos en más de 75 mil ordenadores por todo el mundo afectando, entre otros, a:

- Rusia: red semafórica, metro e incluso el Ministerio del Interior.

- Reino Unido: gran parte de los centros hospitalarios.
- Estados Unidos.
- España: empresas tales como: Telefónica, Gas Natural e Iberdrola.

El ransomware cifra los datos que, para poder recuperarse, pide que se pague una cantidad determinada, en un tiempo determinado. Si el pago no se hace en el tiempo determinado, el usuario no podrá tener acceso a los datos cifrados por la infección. WannaCry se ha ido expandiendo por Estados Unidos, China, Rusia, Italia, Taiwán, Reino Unido y España, al igual de que se señala que los sistemas operativos más vulnerables ante el ransomware son Windows Vista, Windows 7, Windows Server 2012, Windows 10 y Windows Server 2016.

Un ordenador infectado que se conecte a una red puede contagiar el ransomware a otros dispositivos conectados a la misma, pudiendo infectar a dispositivos móviles. A su inicio, WanaCrypt0r comienza a cifrar los archivos de la víctima de una manera muy rápida.

Afortunadamente en la actualidad se pudo detener su expansión gracias a un programador de Reino Unido.
Cominezos (Ransomware-WannaCry)

El primer virus ransonware conocido, apodado como troyano SIDA, ocurrió en 1989, según Symantec (Norton antivirus). El pago demandado en ese entonces fue de 189 dólares.
En diciembre de 1989, cuando aún no había nacido la primera página web, 20.000 disquetes de 5,25 pulgadas (los populares 'cinco y cuarto') se enviaron desde Londres a empresas tanto británicas como de otros países, a los suscriptores de la revista 'PC Business World' e incluso a participantes de un congreso sobre el sida organizado por la Organización Mundial de la Salud.
'AIDS Information Introductory Diskette' (Disquete de Información Introductoria sobre el sida), rezaba su pegatina, que decía provenir de la PC Cyborg Corporation. En realidad no era más que un engaño: cifraba el disco duro de los ordenadores y pedía un rescate. Un 'ransomware' más rudimentario y mucho menos dañino que su tristemente famoso descendiente WannaCry pero que también se difundió a escala global: llegó a unos 90 países por correo postal.
Al final, no fue exitoso porque pocas personas usaban computadores personales en ese momento e internet era usado sobre todo por científicos y expertos de la tecnología. Los pagos internacionales no eran tampoco tan comunes en ese entonces.

El ransomware ha sido el sello favorito de los cibercriminales desde hace algún tiempo, ya que les permite obtener beneficios rápidamente tras una infección. Pueden cobrar rápidamente gracias al uso de la moneda virtual bitcoin, que es difícil de rastrear. La competencia entre distintas bandas de ransomware las ha

llevado a buscar maneras más eficaces de extender sus códigos maliciosos.
WannaCry parece haber sido creado para explotar un fallo detectado por la Agencia Nacional de Seguridad de EU, (NSA, por sus siglas en inglés).
Cuando se filtraron detalles del error, muchos investigadores de seguridad predijeron que esto llevaría a la creación de gusanos de ransomware automáticos.
En ese caso, puede ser que los hackers sólo hayan necesitado unos meses para hacer realidad esa predicción.

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 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. 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. Métodos de Propagación

Normalmente un ransomware se transmite como un troyano o como un gusano, infectando el sistema operativo, por ejemplo, con un archivo descargado o explotando una vulnerabilidad de software. En este punto, el ransomware se iniciará, cifrará los archivos del usuario con una determinada clave, que sólo el creador del ransomware conoce, e instará al usuario a que la reclame a cambio de un pago.

2.4. ¿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, accesibles desde la red anónima Tor, 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.

3. Metodo de infección

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 malwertising 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.

4. Protección contra ransomware

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.

4.1. 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.

4.2. ¿Cómo funciona un ataque de ingeniería social?

Los ataques deingeniería socialno son muy distintos de los clásicos timos. Elciberdelincuente 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).
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 lavoluntad de ser útil, ayudar o colaborarque 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 alegode 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 deurgenciay 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)

4.3. 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 lecoaccione 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 losenlaces anteshacer 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.

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

5. 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.

5.1. 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 doscopias de seguridadactualizadas. En el caso de que hayamos sufrido un ataque porransomware 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 unbackup. Y como los backups también pueden fallar, se recomienda mantener al menos dos copias actualizadas en todo momento.
"Para evitar ser infectado es imprescindible concienciarse y adoptar medidas técnicas y de procedimiento."
¿Cómo puedo protegerme?
Guarda las copias de seguridad en un lugar diferente al del servidor de ficheros. Dado que existen especímenes deransomware 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.

5.2. Navega seguro

Utiliza redes privadas virtuales siempre que sea posible. Lasredes privadas virtualesson 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 laintraneto 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 llamadosexploit kitsque detectan las vulnerabilidades de nuestro navegador de internet y las aprovechan para instalarransomwareen 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.

5.3. 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.

6. ¿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.

6.1. ¿Cómo recupero mi actividad y mis datos?

Has de seguir los siguientes pasos:
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 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.

6.2. ¿Por qué no has de pagar el rescate?

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.

7. Conceptos

Malware o Software Malicioso
También llamado badware, código maligno, software malicioso, software dañino o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario. El término malware es muy utilizado por profesionales de la informática para referirse a una variedad de software hostil, intrusivo o molesto.

Troyano
Se denomina caballo de Troya, o troyano, a un software malicioso que se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero que, al ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado. El término troyano proviene de la historia del caballo de Troya mencionado en la Odisea de Homero.
Bitcoin
Criptomoneda concebida en 2009; divisa electrónica que presenta novedosas características y destaca por su eficiencia, seguridad y facilidad de intercambio.
Cibercriminales
Personas que con basto conocimiento de informatica, atacan víctimas a través de códigos maliciosos y complejos ciberataques.
Delito Informático, Ciberdelito o Ciberataques
Acción anti jurídica y culpable, que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet. Debido a que la informática se mueve más rápido que la legislación, existen conductas criminales por vías informáticas que no pueden considerarse como delito.
Ingeniería social
Consiste en engañar a la gente para que cedan su información personal como contraseñas o datos bancarios o para que permitan el acceso a un equipo con el fin de instalar software malicioso de forma inadvertida. Los ladrones y estafadores utilizan la ingeniería social porque es más fácil engañar a alguien para que revele su contraseña que vulnerar su seguridad.

8. Referencias

Bitcoin Wiki
https://es.bitcoin.it/wiki/Pagina$_p$*rincipal*
Channebiz – Blog: Exploit Kits o conviértete en un hacker
http : *//www.channelbiz.es*/2015/07/21/*exploit* − *kits* − *o* − *conviertete* − *en* − *un* − *hacker/*
Trendmicro Trendlabs: Economics Behind Ransomware as a Service: A Look at Stampado's Pricing Model
http : *//blog.trendmicro.com/trendlabs*−*security*−*intelligence/the*−*economicsbehind*−*ransomware* − *prices/*
Criptonoticias – Blog: Mixers, el servicio para lavar bitcoins
http : *//criptonoticias.com/colecciones/mixers* − *el* − *servicio* − *para* − *lavar* − *bitcoins/axzz*4*J* − 5*SuTY Xe*
The Tor Project
https : *//www.torproject.org/*
INCIBE – Protege tu empresa – Herramientas – Servicio antibotnet
https : *//www.incibe.es/protege*−*tu*−*empresa/herramientas/servicio*−*antibotnet*
Kaspersky – Blog: Historia y evolución del ransomware: datos y cifras
https : *//blog.kaspersky.com.mx/ransomware* − *blocker* − *to* − *cryptor*/7295/

US-CERT Alert 31-03-2016 Ransomware and Recent Variants
https : *//www.us* − *cert.gov/ncas/alerts/TA*16 − 091*A*
INCIBE – Protege tu empresa – Kit de Concienciación
https : *//www.incibe.es/protege* − *tu* − *empresa/kit* − *concienciacion*