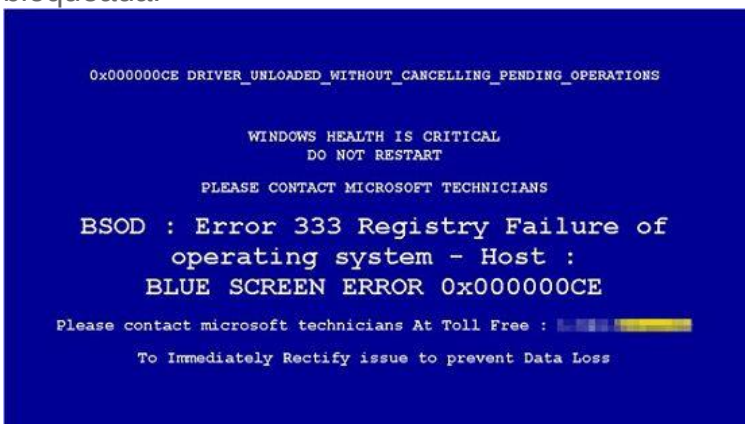
¿QUÉ ES RANSOMWARE?

Dentro de las diversas amenazas que existen actualmente en torno a los equipos informáticos y sobre todo ligadas al uso de Internet, **desde hace tiempo ya ha comenzado a generar interés en los usuarios el término Ransomware,** que es uno de los peligros a los cuales estamos expuestos quienes solemos navegar por Internet.

En líneas generales, Ransomware es un tipo de malware desarrollado para cometer un determinado tipo de estafa, **que se centra en tomar de rehén nuestra computadora y los archivos que se encuentran almacenados en ella,** para luego exigirnos un pago por el rescate de los mismos.

Como lo indica su nombre en inglés, **proveniente de las palabras anglosajonas "ransom", que significa rescate, y "ware" de abreviatura de software,** el malware Ransomware se concentra en el secuestro de datos personales de su víctima durante la exploración que realiza en su PC, luego de ello cifra los datos y es por ello que el usuario ya no puede acceder a sus archivos, y en muchos casos al encender su computadora se encuentra que la misma está bloqueada.

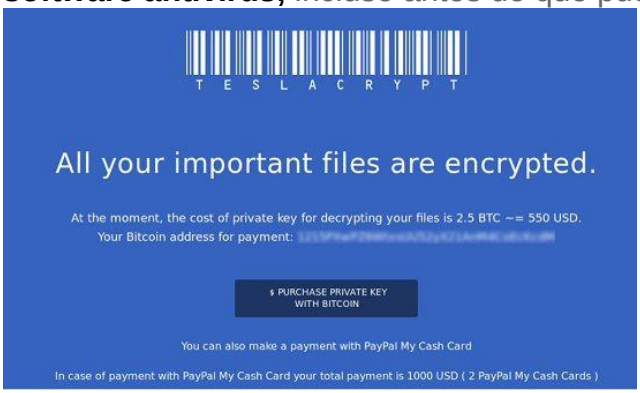


Muchos de los Ransomware que circulan hoy entre los equipos informáticos, cuando infectan una PC y el usuario necesita abrir un archivo, no permite ejecutarlo **y en su lugar muestra un cuadro de diálogo en el cual solicita el pago de dinero para que el usuario pueda volver a utilizar su computadora normalmente.**

¿QUÉ ES RANSOMWARE?

Por lo general, los malware del tipo Ransomware suelen propagarse a través de archivos adjuntos a correos electrónicos, programas descargados de Internet, **como así también sitios web que se encuentran infectados.**

Por tal motivo es sumamente importante que tomemos los recaudos necesarios para evitar ser víctimas de este tipo de estafas. Además, debemos tener en cuenta también en la mayoría de los casos, **los Ransomware pueden ser detectados por las tradicionales herramientas de software antivirus,** incluso antes de que puedan llegar a infectar nuestro equipo.



Asimismo, debido a lo dañino que pueden llegar a ser este tipo de malware, **es aconsejable realizar copias de seguridad de nuestros archivos de forma frecuente,** ya que si somos víctimas de un Ransomware y no disponemos de copias de nuestros archivos ni estamos protegidos, quizás deberemos tener que terminar pagando por ellos.

Cuando un equipo es infectado con un Ransomware, los delincuentes detrás de este malware pueden utilizar diferentes enfoques para extorsionar a sus víctimas, **por ejemplo enviando una nota de rescate a través de un correo electrónico, donde se nos informa que si entregamos el dinero solicitado se nos enviará la clave que nos permitirá desencriptar los archivos,** y al mismo tiempo el atacante advierte que si el rescate no es pagado en una fecha determinada, la clave privada será destruida y los datos se perderán para siempre.

Otro de los modus operandi se centra en engañar a la víctima haciéndole creer que es objeto de una investigación policial debido a la descarga de software ilegal o bien de contenido web ilegal, **el cual ha sido encontrado en su PC, y en este caso lo que se le solicita a la víctima es el pago de una supuesta multa electrónica.**

Así funciona el ransomware

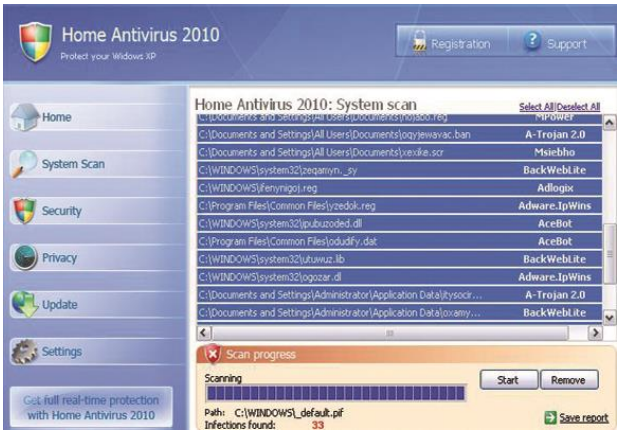
La clave para evitar ser infectados por este tipo de malware, es conocer cómo actúa exactamente este tipo de amenaza. Así sabrás cómo eludirlo, o cómo reaccionar si ha conseguido superar las barreras de tu ordenador. El ciclo de vida del ransomware se compone de varios pasos:

Infección

Este tipo de malware no puede considerarse un virus, porque no se propaga de un ordenador a otro. Hay que instalarlo manual o automáticamente, mediante un engaño de la víctima. El ransomware se camufla dentro de un programa con un gancho muy apetecible para hacer que la víctima lo instale o entre en contacto con él de forma voluntaria. Por ejemplo, un juego erótico, una web para ver vídeos, un programa para descargar películas o juegos... Incluso se hace pasar por un antivirus o herramientas que aceleran la velocidad de funcionamiento de tu PC.

A veces se camuflan como actualizaciones del sistema Windows o de Adobe Flash, o incluso como codecs para poder ver ciertos vídeos. De esta forma la víctima piensa que está instalando un antivirus o una actualización de Windows.

Hay casos en los que se cuela automáticamente, por ejemplo, al entrar en ciertas webs de dudosa reputación o al abrir ciertos emails con ficheros adjuntos o enlaces, pero eso sólo suele ocurrir si no tienes el navegador o el propio Windows actualizado.



El chantaje

Una vez ha penetrado en el ordenador, el malware se activa, produciendo un bloqueo del sistema operativo. Entonces en pantalla aparecerá un mensaje con la amenaza y el importe del chantaje. Para asustar todavía más, se muestra tu dirección IP, tu ciudad y el nombre de tu proveedor de Internet. En realidad, estos datos son públicos y es fácil acceder a ellos.

Existen muchos tipos de ransomware. Estos son los más populares:

- ***Contenido pirateado***: En pantalla aparece un mensaje de una falsa agencia de copyright, y te informa que ha realizado un rastreo en tu ordenador y ha encontrado material pirateado: películas, juegos, o música. Si no pagas la multa, procederán a denunciarte. En España se hizo muy popular el "virus de la SGAE".

- ***Falsos virus***: En muchos casos, el mensaje te informa que has sido infectado por un virus muy potente, y debes descargar un antivirus pagando con un SMS o similar, para obtenerlo. Casi siempre, aunque pagues, este supuesto "antivirus" es un gusano que infectará tu PC con un verdadero virus, difícil de eliminar.

- ***Software caducado***: Otras versiones de ransomware se camuflan como un aviso de Microsoft, o de un antivirus o programa de pago que tengas instalado, indicando que la versión ha caducado, y por tanto debes pagar por la nueva actualización.

- ***Contenido embarazoso***: Una amenaza muy popular consiste en mostrar imágenes pornográficas en la pantalla, que no desaparecerán hasta que no pagues. Mucha gente, para evitar que las vean su familia y se cree un situación embarazosa, acaba sucumbiendo al chantaje.

- ***Contenido ilegal***: Una variante más agresiva, muy popular en España, es la del "Virus de la Policía". Un supuesto aviso de la Policía Española, el FBI, u otra agencia de seguridad, te informa que has accedido a una web con pornografía infantil. La denuncia será inmediata si no pagas una multa. La web de seguridad **InfoSpyware** ha creado una **página web en Facebook** en donde recogen imágenes de todas las variantes de Virus de la Policía que se han distribuido en España.

Tipos de bloqueos

Para proceder al secuestro, el ransomware utiliza diferentes métodos de “captura” de tu ordenador. Es la clave para saber si podrás rescatarlo.

• ***Bloqueo sin encriptación***: Se produce una toma de control del sistema sin encriptar los datos. Por regla general, el malware desactiva el Administrador de tareas, blinda el acceso al registro e infecta el fichero EXPLORER.EXE para hacer desaparecer los iconos del escritorio y así impedir que uses programas. Los más sofisticados también impiden arrancar en Modo Seguro. Pese a que no son fáciles de quitar, al no existir encriptación de datos es posible recuperar el equipo instalando un antivirus.

• ***Bloqueo con encriptación****:* Esta variante encripta los datos del disco duro con códigos de encriptación que son casi imposibles de desencriptar, si no conoces la clave. Si la encriptación sólo afecta a archivos del sistema, un antivirus puede recuperar el control reinstalándolos. Pero si está encriptado todo el sistema operativo o, aún peor, los datos del usuario, la única solución es formatear el disco duro, con la inevitable pérdida de datos.

El pago

Todos estos chantajes de ransomware ofrecen una alternativa a la víctima: pagar una determinada cantidad de dinero para eliminar la amenaza, ya sea una multa a “la policía”, a la agencia de copyright, o al creador del supuesto antivirus que desbloqueará tu equipo.

La cantidad nunca suele ser muy elevada, para que no merezca la pena realizar la denuncia. Los chantajes más habituales varían entre los 10 y los 50 euros, pero hay variantes que te exigen más de 100 euros.

Los sistemas de pago a través del ransomware son muy variados:

- Los más comunes te exigen que envíes un SMS de pago.
- Otros te obligan a llamar a un número con tarifas de pago muy altas. Permanecerá descolgado unos minutos hasta que crean que has pagado lo suficiente.
- El ransomware más sofisticado usan sistemas de pago online con tarjeta de crédito anónimas o tarjetas canjeables tipo PaySafeCard o uKash.

En pocos casos, al pagar sí se produce el desbloqueo del PC, especialmente en el caso de los datos encriptados, pues te envían la clave. Pero la mayoría de las veces la liberación nunca se produce.

Consejos para evitar el ransomware

Hemos visto los mecanismos que utiliza el ransomware para secuestrar un ordenador y pedir rescate. Sabiendo cómo funciona, resulta más sencillo evitar sus trampas.

Con este tipo de software maligno hay que prestar más atención que con un virus estándar, porque en muchos casos eres tú mismo el que abres las puertas al ransomware. Ya hemos visto cuales son las artimañas, pero a veces van un paso más allá, y cuando se disfrazan de virus o actualización de Windows incluso piden a la víctima que desactive el antivirus o el cortafuegos porque “van a instalar una actualización muy delicada”. Si quieres evitar el ransomware, pon en marcha estas medidas:

- Instala todos los parches y actualizaciones del sistema.
- Usa un navegador de Internet moderno, y actualizado.
- Instala todas las actualizaciones de Java, Adobe Flash, y otras librerías de Internet, en el mismo momento en que se produce la actualización.
- Ten siempre funcionando en segundo plano un antivirus y un cortafuego actualizado.
- Un par de veces al mes, realiza un chequeo con algún programa especializado en troyanos y gusanos, tipo Malwarebytes Anti-Malware.
- No abras correos de fuentes desconocidas ni entres en webs de mala reputación, llenas de publicidad con ventanas emergentes, que ofrecen contenido sospechosamente atractivo.
- Si descargas algún archivo dudoso, antes de usarlo chequéalo con un antivirus. Medidas para eliminarlo

Medidas para eliminarlo

A pesar de tomar todas las precauciones posibles, o quizá porque has llegado demasiado tarde, es posible que alguna versión de ransomware se instale en tu equipo. Ante todo, lo importante es que no cunda el pánico. Tienes la tranquilidad de saber que los chantajes son falsos: ni la policía ni el FBI han analizado tu ordenador, ni tienes un potente virus que requiere comprar un antídoto. Ahora ya sólo queda confiar en los antivirus de verdad...

Si detecta un comportamiento extraño o sospecha que ha sido víctima de infección, por favor contacte al departamento técnico inmediatamente: http://helpdesk.magnum.com.co/magnum

En la mayoría de los casos el técnico tendrá que crear un disco de rescate. El antivirus se instalará en memoria antes que el sistema operativo e intentará retomar el control. Es posible que se deba arrancar en Modo Seguro. Si el ransomware no ha encriptado los ficheros del disco duro, las posibilidades de eliminarlo son bastante altas. Si hay encriptación, será necesario formatear (**borrar los datos**)... Seguro que tienes hecha una copia de seguridad, ¿verdad?...

Cualquier malware es un hueso duro de roer, pero con las precauciones y las herramientas adecuadas, conseguirás bloquear la amenaza antes de que entre en tu PC.

También en android

Al tratarse de un sistema operativo abierto, Android permite instalar apps de terceros a través de servicios de descarga alternativos a Google Play, o incluso de forma manual. Esto es aprovechado por el malware para disfrazarse de apps con algún tipo de gancho -juegos, apuestas, vídeos eróticos- e “invitarte” a que las instales desde fuera de Google Play, y así introducir el virus en tu smartphone.

Por ejemplo, Fakedefender, se camufla como una app que detecta software maligno, pero en realidad bloquea el acceso al smartphone y pide una cantidad de dinero para desbloquearlo. La única forma de recuperarlo sin pagar es regresar a los valores de fábrica, lo que significa perder todos los datos. Para evitar este tipo de ataques es imprescindible instalar un buen antivirus para Android.

Fuente: http://tecnologia-facil.com

Marzo 2017