¿PODRÍA SOBREVIVIR TU NEGOCIO AL CRYPTO-RANSOMWARE?

Aprende a defenderte frente al crypto-ransomware

http://www.kaspersky.es/business-security/

¿QUÉ ES EL RANSOMWARE?

Ya pasaron los días en los que los aficionados desarrollaban *software* malicioso simplemente como una travesura. El crimen organizado está detrás de gran parte del *malware* actual, y el principal objetivo es ganar dinero.

Como su nombre indica, el *ransomware* es un tipo concreto de malware que intenta obtener una recompensa monetaria a cambio de desbloquear el acceso a un recurso que pertenece a la víctima.

En el caso del *crypto-ransomware*, los recursos "secuestrados" son los archivos y los datos que se almacenan en un dispositivo infectado. El *crypto-ransomware* cifra los datos de la víctima en un formato ilegible, y los datos solo se pueden descifrar utilizando una clave de descifrado concreta. Sin embargo, el criminal solo proporciona la clave una vez que la víctima haya pagado el rescate exigido.

El *crypto-ransomware* a menudo muestra un cuadro de diálogo que indica que el cifrado se ha llevado a cabo como resultado de un acto ilegal por parte de la víctima. El mensaje parece estar enviado por la policía o el FBI.

ATAQUES DE CRYPTO-RANSOMWARE: DAÑANDO A LAS EMPRESAS Y A LOS CONSUMIDORES

Aunque los consumidores se enfrentan a demandas de rescate de 250 a 500 euros, los cibercriminales piden rescates mucho más elevados a las empresas, cuyos datos son muy valiosos.

Si se infecta uno de tus dispositivos, el criminal te dará un plazo de 48 a 72 horas para pagar el rescate. Si no lo pagas en el plazo indicado, el precio para el descifrado aumentará. Una vez cumplido el segundo plazo, si el pago siguiera sin realizarse, es probable que la clave de descifrado sea eliminada. Llegados a este punto, puede ser imposible que recuperes tus archivos de forma legible.

Sin embargo, aunque pagues el rescate, no tendrás la garantía de que tus datos sean descifrados. Algunos *crypto-ransomware* contienen *bugs* en su *software* que pueden causar daños en el proceso de descifrado. En otros casos, la variante de *ransomware* no cuenta con la función de descifrado. En cambio, en vez de proporcionar las claves de descifrado, los criminales tan solo tratan de quedarse con el dinero de sus víctimas.

El 40% de las víctimas de CryptoLocker aceptaron pagar la recompensa, según una encuesta realizada por el Centro Interdisciplinario de Investigaciones de la Universidad de Kent.

"Un *crypto-ransomware* moderno llevará a cabo una serie de acciones adicionales que impiden la recuperación de los datos cifrados, incluyendo la eliminación o el cifrado de las copias ocultas utilizadas en el almacenamiento del sistema de puntos de restauración y copias de seguridad periódicas de Windows".

– Andrey Pozhogin, experto en ciberseguridad, Kaspersky Lab

SOLUCIÓN KASPERSKY

Nuestro subsistema de contramedidas System Watcher anula las consecuencias de los ataques de *crypto-malware* al hacer copias de seguridad, locales y protegidas, de los archivos de datos del usuario en cuanto los abre un programa sospechoso.

ALTOS COSTES PARA LAS EMPRESAS: EL PAGO DEL RESCATE ES SOLO EL PRINCIPIO

Aunque los criminales suelen exigir el pago de mayores recompensas a los negocios que son víctimas de sus ataques, esta recompensa puede suponer el menor de los costes a los que se enfrente la empresa. Estos ataques pueden provocar pérdidas financieras mucho mayores.

Imagina perder el acceso a todos tus registros de ventas, archivos de clientes, contabilidad, información de productos y datos de diseño. ¿Cómo puede esto afectar a tu negocio? ¿Cuántos ingresos se pierden mientras tu equipo intenta que todo vuelva a la normalidad?

En la actual "era de la información", la pérdida temporal de datos puede interrumpir totalmente los procesos críticos de un negocio, lo que lleva a:

- Pérdida de ventas
- Reducción de la productividad
- Grandes costes invertidos en la recuperación del sistema

Sin embargo, la pérdida permanente de los datos puede tener consecuencias mucho más graves:

- Dañar permanentemente la posición competitiva de la empresa
- La reducción de los ingresos por ventas a largo plazo
- Impedir el acceso permanente a la propiedad intelectual y los datos de diseño

Esto puede poner en peligro todo el negocio.

CONSEJO PRINCIPAL

Si tu negocio sufre un ataque, ten precaución con los falsos remedios que circulan por Internet. Estos solo pueden darte más problemas.

1. No suelen funcionar y suelen costar más dinero a la víctima.
2. Algunos "remedios" incluso pueden descargar *malware* adicional en la red de la víctima.

SE PRODUCEN MÁS ATAQUES DE CRYPTO-RANSOMWARE QUE NUNCA

En los primeros seis meses de 2015, el número de ataques de crypto-ransomware igualó la cifra de todo el 2014.

Fuente: Red de Seguridad Kaspersky

Algunos ejemplos recientes de *crypto-ransomware*:

CoinVault–utiliza un cifrado AES 256-bit para cifrar los archivos de sus víctimas.

CryptoLocker–Ha infectado decenas de miles de equipos y generado millones de dólares en beneficio de los criminales

CryptoWall–suele duplicar el valor de la recompensa si el pago de esta no se realiza en el periodo de tiempo inicial

TorLocker–cifra los datos y utiliza la red Tor para ponerse en contacto con los criminales responsables del ataque

A pesar del aumento de los ataques de ransomware, una reciente investigación afirma que el 40 % de las empresas no considera que el ransomware sea una seria amenaza.

Obviamente, esta actitud supone una debilidad de seguridad que los cibercriminales pueden aprovechar.

Fuente: Encuesta de Kaspersky Lab sobre los Riesgos Globales de la Seguridad Informática 2015

CÓMO ATACAN LOS *CRYPTO-RANSOMWARE*

Como muchos otros muchos tipos de *malware*, hay muchas formas en las que un *crypto-ransomware* puede acceder a los ordenadores y otros dispositivos.

Sin embargo, dos de las formas más comunes son mediante:

***Phishing* enviado a través de *spam*:** la víctima recibe un correo electrónico que contiene un documento adjunto que está infectado o el correo electrónico incluye un enlace que lleva al usuario a una página web de *phishing*.

***Water holing*:** la visita a una conocida página web legítima con un tipo de usuario o un puesto de trabajo específicos puede llevar a la infección del dispositivo del empleado. En estos casos de infección "de paso", la página web habrá sido previamente infectada con un malware listo para explotar las vulnerabilidades existentes en los dispositivos de los visitantes.

¿A QUÉ DISPOSITIVOS ATACAN?

Debemos recordar que el crypto-ransomware puede atacar a una gran variedad de dispositivos entre los que se incluyen:

- PCs
- Ordenadores Mac
- Tablets y smartphones Android
- Infraestructura de escritorios virtuales (VDI)

Además, si el dispositivo atacado está conectado a una unidad de red, los archivos corporativos compartidos también pueden llegar a estar comprometidos. Los archivos compartidos también podrán quedar cifrados, sin importar el sistema operativo que utiliza el servidor.

No importa qué dispositivo esté siendo atacado, el *crypto-ransomware* no necesita los derechos de administrador para llevar a cabo sus acciones maliciosas.

EL CRYPTO-RANSOMWARE ACTUAL ES MÁS PELIGROSO

LOS PRIMEROS *CRYPTO-RANSOMWARE*

Cuando se descubrieron los primeros crypto-ransomware, era posible invertir sus efectos.

A veces, la clave de descifrado estaba simplemente oculta dentro del dispositivo infectado. Se solucionaba simplemente con encontrar la clave y descifrar los datos.

En otros ataques, los expertos en seguridad podían invertir el diseño del malware y encontrar la forma de descifrar los datos.

EL *CRYPTO-RANSOMWARE* HA EVOLUCIONADO

Los cibercriminales actuales ya no cometen errores básicos. Utilizan técnicas mucho más complejas que pueden ser muy difíciles de invertir. Incluso en los casos en que es posible el uso de la ingeniería inversa, la probabilidad de encontrar la clave de descifrado en el dispositivo atacado es muy baja.

DESCIFRADO DE UN DISPOSITIVO

La mayoría de los *crypto-ransomware* actuales generan una clave de descifrado única para cada dispositivo atacado. Por lo tanto, incluso si se consigue acceder a una clave de descifrado, no se podrá utilizar para descifrar los archivos en el caso de otros dispositivos.

Estas técnicas de cifrado son cada vez más sofisticadas y hacen que sea prácticamente imposible descifrar los datos. Entre ellas se incluyen:

- El método combinado RSA/AES que permite el cifrado de alta velocidad, usando el algoritmo AES, y después cifra la clave AES con el potente algoritmo RSA
- Algoritmos de curvas elípticas que permiten niveles de cifrado aún más profundos manteniendo la velocidad

CUBRIENDO SUS HUELLAS

Los cibercriminales que lanzan crypto-ransomware también están dedicando más recursos en intentar obstaculizar los esfuerzos de los organismos policiales, por lo que es cada vez más difícil localizar y parar las crypto-operaciones modernas:

- Normalmente se solicita realizar el pago en Bitcoin u otras monedas digitales, por lo que se dificulta el rastreo del pago
- El uso de los mecanismos de anonimato, como la red Tor, hacen prácticamente imposible rastrear la ubicación de los criminales

CÓMO PROTEGER TU NEGOCIO

Cuando se trata de evitar el riesgo de un ataque de crypto-ransomware, tienes dos opciones:

1. Esperar a no ser atacado. Pero con el creciente número de crypto-ransomware, no es realmente una opción viable.
2. Seguir una serie de reglas de fácil aplicación para mantener la seguridad de tus datos y tu negocio en marcha.

FORMA A TUS EMPLEADOS

Las personas suelen ser el elemento más vulnerable de cualquier negocio. Forma a tus empleados sobre los conceptos básicos de seguridad informática, incluyendo:

- El conocimiento del *phishing* y sus riesgos
- Las implicaciones de seguridad que tiene abrir el archivo adjunto de un correo electrónico que parece sospechoso, incluso aunque parezca provenir de una fuente fiable

REALIZA CON FRECUENCIA COPIAS DE SEGURIDAD DE TUS DATOS Y COMPRUEBA LA RESTAURACIÓN DE TUS COPIAS DE SEGURIDAD

Casi todas las empresas cuentan con políticas de copia de seguridad de sus datos. Sin embargo, es importante hacer una copia de seguridad de los datos en un subsistema de seguridad sin conexión, en lugar de copiar simplemente los archivos a otro sistema "autónomo" en tu red corporativa. De lo contrario, el *crypto-ransomware* podrá cifrar tus archivos de copia de seguridad.

Establece una política de "copia de seguridad sin conexión", así no solo copiarás los datos en un servidor de archivos de conexión fija.

PROTEGE TODOS TUS DISPOSITIVOS Y SISTEMAS

Como el *crypto-ransomware* no solo ataca a los ordenadores, también tendrás que considerar si tu *software* de seguridad protege a los ordenadores Mac, o a las máquinas virtuales y los dispositivos móviles de Android.

También es conveniente comprobar que tu sistema de correo electrónico cuente con las suficientes medidas de protección.

IMPLEMENTA Y MANTÉN ACTUALIZADO TU *SOFTWARE* DE SEGURIDAD

Además de tener en cuenta todas las medidas de prevención contra el malware, tu lema debe ser "actualiza pronto y a menudo" por lo que debes:

- Actualizar todas las aplicaciones y los sistemas operativos para eliminar las vulnerabilidades recientes
- Actualizar la aplicación de seguridad y sus bases de datos para contar con las medidas de protección más recientes.

Elige una solución de seguridad que incluya herramientas que te permitan:

- Gestionar el uso de Internet, por ejemplo, según el puesto de trabajo
- Controlar el acceso a los datos corporativos, según el departamento o el puesto de trabajo
- Gestionar los privilegios de acceso y activación mediante tecnologías de control de aplicaciones que ayudan a denegar o permitir el uso de ciertos programas.

"Los cibercriminales son cada vez más hábiles en el desarrollo de ransomware que pase desapercibido mientras esté en funcionamiento, y cuentan con una gran cantidad de técnicas y herramientas a su alcance para garantizar que la víctima no descubra el ransomware".

- Andrey Pozhogin, experto en ciberseguridad, Kaspersky Lab.

ELIGE UN SOFTWARE DE SEGURIDAD RECONOCIDO

Los productos de Kaspersky Lab ofrecen soluciones de seguridad multicapa que protegen tu negocio contra las amenazas conocidas, desconocidas y más avanzadas, entre las que se incluye a los *crypto-ransomware*.

Proporcionamos actualizaciones para las bases de datos de nuestras soluciones de seguridad y *antimalware* con mucha más frecuencia que la mayoría de los proveedores de seguridad informática. Además, Kaspersky Endpoint Security for Business cuenta con una tecnología proactiva y heurística, además de usar tanto técnicas de comportamiento como tecnologías asistidas en la nube para responder rápidamente a las nuevas amenazas.

Muchos de nuestros productos también ofrecen una gran variedad de tecnologías y herramientas de seguridad adicionales.[1]

SYSTEM WATCHER INCLUYE MEDIDAS CONTRA EL CRYPTOMALWARE

System Watcher monitoriza el comportamiento de todos los programas que se ejecutan en tus sistemas y compara el comportamiento de cada programa con el típico modelo de comportamiento del *malware*.[2]

Si se detecta cualquier comportamiento sospechoso, System Watcher pondrá el programa en cuarentena automáticamente. Ya que System Watcher guarda un registro dinámico del sistema operativo, el registro, etc., esto le proporciona información para poder invertir las acciones maliciosas que se llevaron a cabo antes de que se identificara el *malware*.

Además, System Watcher supervisa constantemente el acceso a ciertos tipos de archivo, entre los que se incluyen los documentos de Microsoft Office, y almacena temporalmente copias de los mismos en caso de que cualquiera de estos archivos se modifique o elimine. Si System Watcher detecta un proceso sospechoso, como el acceso de un *crypto-ransomware* a un archivo, las "copias de seguridad" temporales se pueden utilizar para devolver el archivo a su forma no cifrada. Aunque las copias de seguridad temporales generadas por System Watcher no pretenden sustituir el funcionamiento de una estrategia de copias de seguridad completa, pueden resultar de ayuda en la protección contra los efectos de un ataque de *crypto-ransomware*.

Trabajando en conjunto con el System Watcher, el Control de privilegios de las aplicaciones también permite a los administradores limitar el acceso que tienen las aplicaciones a los recursos críticos del sistema, incluido el acceso al disco duro.

EVALUACIÓN DE LAS VULNERABILIDADES Y GESTIÓN DE PARCHES [3]

Las vulnerabilidades o los *bugs* que se encuentran en cualquiera de las aplicaciones y los sistemas operativos que se ejecutan en un dispositivo pueden convertirse en puntos de entrada de ataques de *malware*, como en el caso del *crypto-ransomware*.

Nuestras herramientas automatizadas de evaluación de las vulnerabilidades y gestión de parches pueden escanear tus sistemas, identificar las vulnerabilidades conocidas y ayudarte a gestionar los parches y las actualizaciones necesarias para que las vulnerabilidades de seguridad conocidas puedan ser eliminadas.

PREVENCIÓN AUTOMÁTICA DE EXPLOITS (AEP) [4]

Nuestra tecnología AEP también ayuda a detener la explotación de las vulnerabilidades de *malware* de los sistemas operativos y las aplicaciones. Monitoriza específicamente las aplicaciones más frecuentes, incluyendo Adobe Reader (una de las más atacadas), Internet Explorer, Microsoft Office y Java, para proporcionar una poderosa capa de seguridad adicional.

Los expertos en seguridad, en ocasiones, son capaces de encontrar una vulnerabilidad dentro del crypto-ransomware y aprovecharla para ayudar a las víctimas a recuperar sus archivos.

Kaspersky Lab se asoció recientemente con la *Unidad Nacional* contra *Delitos de Alta Tecnología* (NHTCU) de la policía holandesa para crear un repositorio de claves de descifrado y una aplicación de descifrado para las víctimas de CoinVault.

1. Las características de seguridad varían en los diferentes sistemas/plataformas. Para más información, consulta www.kaspersky.es/business.

2. System Watcher está disponible en Kaspersky Endpoint Security for Business (Select, Advanced y Total) y KSV|Light Agent.
   Solo para los sistemas con un sistema operativo basado en Windows, las plataformas de servidor no son compatibles.
   No disponible para Mac y dispositivos Android.

3. Las funciones de evaluación de las vulnerabilidades y de gestión de parches están incluidas en Kaspersky Total Security for Business, Kaspersky Endpoint Security for Business Advanced y Kaspersky Systems Management.

4. AEP es parte de las funcionalidades de System Watcher.

Los innovadores productos y tecnologías de seguridad de Kaspersky Lab han sido galardonados en muchas más ocasiones que otros proveedores de seguridad.

En 2014, nuestros productos alcanzaron el primer lugar en 51 de los 93 ensayos y pruebas independientes realizados.

Kaspersky Lab | 2014
#1 in 51 independent tests

*usa.kaspersky.com/awards

CONTROL DE APLICACIONES Y LISTAS BLANCAS

Las herramientas flexibles de control de aplicaciones, además de las listas blancas dinámicas, incluyen una serie de categorías que permiten el control flexible de la puesta en marcha. Además, también se puede obtener un control privilegiado que te da la opción de limitar el acceso de ciertas aplicaciones restringidas a los datos específicos en un ordenador, al tiempo que les permite iniciar.

Además de bloquear los programas de la lista negra, se puede aplicar la política de denegación predeterminada para algunas de las equipos y servidores, de manera que solo se consienta la ejecución de las aplicaciones que están en la lista blanca. Por lo tanto, el crypto-ransomware se bloqueará automáticamente.

CONTROL WEB

Las herramientas sencillas de utilizar te ofrecen flexibilidad para establecer políticas de acceso a Internet y controlar el uso de este, de acuerdo a tus propias especificaciones. Puedes prohibir o permitir la actividad de ciertos usuarios a páginas web individuales o a ciertas categorías, como las redes sociales, jo páginas de juego online. Por lo tanto, se reduce la probabilidad de que los usuarios visiten una web infectada con crypto-ransomware.

ANTIPHISHING

Nuestra herramienta *antiphishing* te ayuda a evitar que tus empleados sean víctimas de campañas *phishing* y *spearphishing* que puedan conducir a infecciones de *crypto-ransomware*.

SISTEMA DE SEGURIDAD DEL CORREO ELECTRÓNICO

Kaspersky Security para el servidor de correo electrónico analiza el correo entrante, saliente y almacenado en Microsoft Exchange, Linux Mail y los servidores de correo electrónico de Lotus Domino.

Nuestro motor *antispam* y *antiphishing* te ayuda a eliminar las distracciones y te protege contra el crypto-ransomware y otras amenazas.

AYUDÁNDOTE A PROTEGER TODOS TUS DISPOSITIVOS ENDPOINT...Y MÁS

Ofrecemos soluciones para la protección de una amplia gama de:

- PC`s
- Mac
- Servidores de archivos
- Teléfonos móviles y tablets
- Servidores virtuales
- Infraestructura de escritorios virtuales (VDI)

Además de seguridad para los portales de Internet y servidores de colaboración.

PRUEBA KASPERSKY LAB

Descubre la seguridad premium de Kaspersky Lab para proteger tu negocio del *malware* y el cibercrimen instalando la versión de prueba sin ningún compromiso. Regístrate hoy y descarga las versiones completas de nuestros productos y disfruta de la protección de toda tu infraestructura informática, tu negocio y tus datos confidenciales.

ÚNETE A LA CONVERSACIÓN >

ÚNETE A LA CONVERSACIÓN

Suscríbete a nuestro canal de YouTube

Síguenos en Facebook

Sigue nuestro blog

Síguenos en Twitter

Síguenos en LinkedIn

ACERCA DE KASPERSKY LAB

Kaspersky Lab es una de las compañías de seguridad cibernética de mayor crecimiento en el mundo y la más grande de propiedad privada. La empresa se encuentra entre los cuatro principales proveedores mundiales de soluciones de seguridad informática (IDC, 2014). Desde 1997, Kaspersky Lab es una compañía innovadora en el sector de la seguridad cibernética y ofrece soluciones de seguridad digital eficaces y proporciona información sobre las amenazas a grandes, pequeñas y medianas empresas y a al público en general. Kaspersky Lab es una empresa internacional, presente en casi 200 países y territorios de todo el mundo, proporcionando protección a más de 400 millones de usuarios en todo a nivel mundial. Más información en: http://www.kaspersky.es/

KASPERSKY lab
EL PODER DE PROTECCIÓN