¿Cómo sobrevivir al ransomware de cifrado?

KASPERSKY lab

Junio 2017

Este es un documento producido por

www.ituser.es
www.itreseller.es

Accede a nuestras publicaciones digitales

CÓMO USAR ESTE DOCUMENTO

Con el fin de obtener la mejor experiencia de uso de esta revista, es **imprescindible** seguir estos sencillos pasos que te indicamos a continuación:

Paso 1. Asegúrate de disponer de las versiones más actualizadas de Adobe Reader y Flash Player. Si no las tienes instaladas, puedes descargarlas aquí:

Adobe Acrobat Reader y Adobe Flash Player

Paso 2. Accede al enlace de descarga y la publicación se abre en el visor del navegador.

Paso 3. Busca la opción guardar como que, dependiendo del navegador que utilices, podrá ser un icono o estar incluída en la barra de menú, y guarda la revista en la carpeta donde almacenes los documentos en tu equipo.

Paso 4. Accede a dicha carpeta y usa el botón derecho del ratón para hacer clic en el fichero de la revista.

Paso 5. Selecciona Adobe Reader como aplicación predeterminada para abrir este tipo de documentos.

Paso 6. Una vez abierta la revista, habilita la visualización a pantalla completa, y puedes iniciar la lectura de la revista con todas las capacidades interactivas disponibles.

¿Cómo sobrevivir al ransomware de cifrado?

Recientemente, todos los medios de comunicación hemos llevado a nuestras portadas o a nuestros sumarios el ataque sufrido por una larguísima lista de empresas y entidades que han convertido en protagonista al ransomware WannaCry. A partir de ahí, surgen una serie de preguntas, ¿estamos seguros? ¿Qué ha provocado esta incidencia? ¿Cómo protegerse? ¿Qué hacer ahora? Y, sobre todo, ¿podría haberme afectado a mí? En las páginas siguientes trataremos de responder a todas ellas.

En primer lugar, vayamos a lo más genérico: ¿qué es el ransomware? El crimen organizado está detrás de gran parte del malware actual y su intención es ganar dinero. Como su propio nombre indica, el ransomware es un tipo específico de malware cuyo objetivo es lograr el pago de un rescate a cambio de desbloquear el acceso a un recurso que pertenece a la víctima.

En el caso del ransomware de cifrado, o cryptors, los activos "secuestrados" son los archivos y los datos que se almacenan en el dispositivo infectado. El cryptor cifra los datos de la víctima en un formato ilegible y los datos solo se pueden descifrar mediante la clave de descifrado necesaria, pero dicha clave solo la proporcionará el criminal cuando la víctima pague el rescate.

Mientras que los usuarios se enfrentan a exigencias de rescate de 300 a 500 dólares, los cibercriminales saben que los datos pueden ser muy valiosos para una empresa, por lo que la suma del rescate es mucho mayor. Si uno de los dispositivos está infectado, el atacante suele ofrecer un margen de 48 a 72 horas para pagar el rescate.

Si no paga dentro del plazo, es probable que el precio del descifrado aumente. Si vence el segundo plazo y el pago no se ha realizado todavía, es probable que la clave de descifrado se elimine. En ese punto cabe la posibilidad de que sea imposible recuperar sus archivos en un formato legible. Incluso, si paga el rescate, no hay garantía de que sus datos se descifren. Algunos cryptors incluyen errores de software que pueden hacer que no funcione, por lo que el proceso de descifrado fallará. En otros casos, es posible que el criminal

RANSOMWARE EN ATAQUES DIRIGIDOS

CLICAR PARA VER EL VÍDEO

no tenga la intención de descifrar nada y solo quiera obtener el dinero de la víctima.

Pero, como siempre, la realidad no es la misma para un usuario en su domicilio que para una empresa y, en este caso, los efectos perniciosos son todavía mayores. A pesar de que los criminales suelen exigir cantidades más elevadas a víctimas de empresas, el rescate solo representa una pequeña parte de los costes totales para la empresa. Este ataque puede dar lugar a pérdidas económicas mucho mayores.

En la "era de la información" actual, cualquier pérdida temporal de datos puede interrumpir totalmente los procesos fundamentales para la empresa, lo que se traduce en pérdida de ventas, reducción de la productividad, costes más que significativos para recuperar el sistema y revertir la situación al momento anterior al problema.

Según un informe de Interdisciplinary Research Center in Cyber Security de la Universidad de Kent en febrero de 2014, más del 40% de las víctimas de CryptoLocker cedió a pagar el rescate

Sin embargo, la permanente pérdida de datos puede tener consecuencias mucho más graves, como un efecto negativo en la posibilidad de la empresa de competir en el mercado, una reducción de las ventas a largo plazo, o imposibilidad de acceder a datos y recursos necesarios para el día a día de la empresa.

Incluso, se puede poner en peligro a toda la empresa, si, por ejemplo, se pierde la posibilidad de acceder a todos sus registros de ventas, archivos de clientes, datos contables, información de productos y datos de diseño.

El tristemente famoso WannaCry

El más famoso incidente de seguridad informática en las últimas semanas ha sido WannaCry, que ha infectado a más de 200.000 ordenadores. Durante el primer día del ataque, descubrimos que WannaCry estaba en 74 países, incluido el nuestro, si bien, aunque en Espa-

NO MORE RANSOM!

Las fuerzas y cuerpos de seguridad y las compañías tecnológicas han unido fuerzas para interrumpir las operaciones de los cibercriminales que hacen uso del ransomware. El portal No More Ransom, puesto en marcha en julio de 2016, es una iniciativa del National High Tech Crime Unit de la policía de Países Bajos, el European Cybercrime Centre de Europol y dos compañías de ciberseguridad, Kaspersky Lab e Intel Security, con el objetivo de ayudar a las víctimas de ransomware a recuperar sus datos cifrados sin tener que pagar a los criminales.

Desde su puesta en marcha, se han adherido a esta iniciativa más de 80 nuevos miembros, entre fuerzas de seguridad, como Guardia Civil, y empresas privadas del mundo de la ciberseguridad.

El proyecto también se dirige a educar a los usuarios sobre cómo funciona el ransomware e informar sobre qué contramedidas se pueden tomar para prevenir eficazmente una infección. Esta iniciativa está accesible en este enlace.

Pero, además de consejos preventivos, los usuarios pueden encontrar en esta página herramientas para el descifrado de archivos, así como los enlaces correspondientes en diferentes jurisdicciones para poder denunciar, en caso de haber sido atacado.

ña la repercusión ha sido muy grande en los medios, no ha sido uno de los países más afectados.

WannaCry tiene dos partes. La primera es un exploit que se encarga de la infección y de la propagación. La segunda es un cifrador que se descarga en un ordenador después de ser infectado.

La primera supone la gran diferencia entre WannaCry y la mayoría de cifradores. Para infectar un ordenador con un cifrador normal, el usuario debe cometer un error, como, por ejemplo, hacer clic en un enlace sospechoso, permitir que Word ejecute macros maliciosas o descargar un adjunto malicioso de un mensaje de correo electrónico. Un sistema puede ser infectado con WannaCry sin que el usuario haga nada.

Los creadores de WannaCry se han aprovechado de un exploit de Windows conocido como EternalBlue y que Windows parcheó con la actualización de software MS17-010 el 14 de marzo del presente año. Mediante el exploit, pudieron obtener acceso remoto a los ordenadores e instalar el cifrador.

Después de hackear con éxito un ordenador, WannaCry intenta distribuirse por toda la red local hacia otros ordenadores del mismo modo en que lo haría un gusano. El cifrador busca la vulnerabilidad EternalBlue

Solo el 40% de las empresas consideran el ransomware un peligro serio

en otros ordenadores y, cuando WannaCry encuentra un dispositivo vulnerable, lo ataca y cifra sus archivos.

Por tanto, al infectar un ordenador, WannaCry puede infectar a toda una red local y cifrar todos los ordenadores de la misma. Por ello, las grandes empresas son las que más han sufrido por el ataque de WannaCry (a más ordenadores en la red, mayor puede ser el daño).

Como cifrador, WannaCry se comporta como cualquier cifrador: cifra los archivos de un ordenador y pide un rescate para descifrarlos. Se parece mucho a una variación de CryptXXX.

WannaCry cifra diferentes tipos de archivos, incluyendo los documentos de Office, imágenes, vídeos y otros tipos de archivos que puedan contener información importante para el usuario. Las extensiones de los archivos cifrados se renombran a .WCRY y el archivo se vuelve del todo inaccesible.

Tras esto, el troyano cambia el fondo de pantalla con una imagen que contiene la información sobre la infección y las acciones que se supone que el usuario debe llevar a cabo para recuperar los archivos. WannaCry deja notificaciones en formato de archivos de texto con la misma información en todas las carpetas del ordenador para asegurarse de que el usuario recibe el mensaje.

Como de costumbre, una de las acciones era transferir cierta cantidad de dinero, en bitcoins, a los malhechores. Tras ello, dicen que descifrarán todos los archivos. En un principio, los ciberdelincuentes pedían 300 dólares, pero luego subieron el rescate a 600 dólares.

En este caso, también intentan intimidar a las víctimas afirmando que la cantidad del rescate se incrementa pasados tres días y, es más, diciendo que pasados siete días es imposible descifrar los archivos.

Y la salida al problema no es el pago, dado que no hay garantías de que los delincuentes vayan a descifrar los archivos tras recibir el mismo. De hecho, en otras ocasiones simplemente borraron los archivos, evitando cualquier opción de los usuarios de recuperarlos.

Formas y efectos del ataque

Más allá del caso de WannaCry, y al igual que la mayoría del resto de tipos de malware, existen muchas maneras en las que un cryptor puede encontrar una vía de entrada a ordenadores y otros dispositivos. Sin embargo, dos de las formas más comunes son las denominadas Phishing spam y Water holing. En el primero de los casos, la víctima recibe un mensaje de correo electrónico con un archivo adjunto infectado o el texto incluye un enlace a un sitio web de phishing, mientras que, en el segundo caso, al visitar un sitio web legítimo que es popular entre un tipo específico de usuarios o función laboral, como un foro de contabilidad o un sitio de asesoramiento empresarial, por ejemplo, el dispositivo del empleado se puede infectar. En estos casos de infección oculta, el sitio web ya se habrá infectado con el malware, que está listo para aprovechar vulnerabilidades en los dispositivos de los visitantes.

Un cryptor puede atacar una amplia gama de dispositivos, desde equipos de sobremesa a infraestructuras de escritorios virtuales, pasando por tabletas y smartphones.

Además, si el dispositivo que está sufriendo un ataque también está conectado a una unidad de red (que permite compartir archivos corporativos), es probable que el cryptor cifre dichos archivos compartidos, con independencia del sistema operativo en el que se está ejecutando el servidor de archivos.

Lamentablemente, sea cual sea el dispositivo que sufra el ataque, no se requieren derechos de administrador para la mayoría de las acciones maliciosas que realizan los cryptors.

Algunos consejos para estar protegidos

Dado que cruzar los dedos y esperar que no nos afecte no parece una solución adecuada para hacer frente a las amenazas, es necesario, además de contar con las herramientas adecuadas, de las que hablaremos a continuación, seguir unos sencillos pasos que nos ayudarán a mantenernos más seguros.

El primero de ellos es la formación a los usuarios que, normalmente, son el eslabón más débil de la cadena. Deben ser conscientes de los riesgos y, sobre todo, de las consecuencias e implicaciones que tiene abrir un mensaje sospechoso o acceder a determinadas páginas o foros.

El segundo, es contar con una copia de seguridad actualizada de forma constante y que estemos seguros de que se puede recuperar.

Y, tercero, mantener actualizado tanto los sistemas operativos y las aplicaciones de la red y de los dispositivos, así como las herramientas de seguridad que protegen toda la infraestructura de la empresa. Además, convendría contar con una herramienta de seguridad que permita administrar el uso de internet en cada puesto de trabajo, controlar quién y desde dónde se accede a los datos corporativos y que administre el lanzamiento de programa, pudiendo bloquear aquellos que sean perjudiciales o, simplemente, sospechosos.

Kaspersky EndPoint Security for Business

Kaspersky Endpoint Security for Business ofrece una seguridad a varios niveles para ayudar a proteger las empresas contra amenazas conocidas, desconocidas y sofisticadas, incluidos los cryptors. Junto con las actualizaciones constantes, incluye técnicas de comportamiento, heurísticas y proactivas, así como tecnologías con asistencia en la nube para una rápida respuesta a las nuevas amenazas.

Un elemento importante de esta solución es System Watcher, que supervisa el comportamiento de todos los programas que se ejecutan en los sistemas y compara cada comportamiento del programa con los modelos de comportamiento de malware típico. Si se detecta cualquier comportamiento sospechoso, System Watcher pone automáticamente la aplicación en cuarentena.

Como mantiene un registro dinámico del sistema operativo o el registro, permite deshacer las acciones maliciosas que se implementaron antes de que el malware se identificara. Además, System Watcher controla constantemente el acceso a determinados tipos de archivos, incluidos documentos de Microsoft Office, y almacena temporalmente copias si se accede a alguno de estos archivos. Si System Watcher detecta que se trata de un proceso sospechoso, como un cryptor, que accedió a los archivos, las copias de seguridad temporales se pueden utilizar para restablecer los archivos al formato sin cifrar. Aunque las copias de seguridad temporales generadas por System Watcher no están diseñadas como reemplazo a una estrategia de

copia de seguridad completa de los datos, pueden ser valiosas para ayudar a la empresa a protegerse contra los efectos de un ataque de cifrado.

Junto con System Watcher, el control de privilegios en las aplicaciones también permite a los administradores limitar los recursos esenciales del sistema a los que se permite acceder a las aplicaciones, incluido el acceso al disco de nivel bajo. Las vulnerabilidades, o errores de software, dentro de cualquiera de las aplicaciones y sistemas operativos que se ejecutan en sus dispositivos pueden proporcionar

puntos de entrada para ataques de malware, incluidos los cryptors.

Estas herramientas de evaluación de vulnerabilidades y gestión de parches automatizadas pueden analizar los sistemas, identificar las vulnerabilidades conocidas y ayudarle a la empresa a distribuir los parches necesarios y las actualizaciones, de manera que las vulnerabilidades de seguridad conocidas se puedan eliminar. Esto también ayuda a evitar que el malware se aproveche de las vulnerabilidades en aplicaciones y sistemas operativos, y controla específicamente las aplicaciones atacadas con más frecuencia, entre las que se incluyen Adobe Reader, Internet Explorer, Microsoft Office y Java, a fin de proporcionar un potente nivel adicional de seguridad.

Las herramientas flexibles de control de aplicaciones, además del marcado en lista blanca dinámico, hacen que sea fácil permitir o impedir el inicio de programas. Además de bloquear los programas incluidos en la lista negra, puede optar por aplicar una política de denegación predeterminada para algunas de sus estaciones de trabajo y servidores, de modo que solo se ejecutarán las aplicaciones que se encuentran en su lista blanca; como resultado los cryptors se bloquearán automáticamente.

Las herramientas fáciles de usar le permiten configurar las políticas de acceso a Internet y supervisar el uso de Internet. Puede prohibir, permitir o inspeccionar las actividades de los usuarios en sitios web individuales o categorías de sitios, como redes sociales, juegos o sitios de apuestas, para reducir las probabilidades de que los usuarios visiten un sitio web infectado por un cryptor.

Por su parte, el motor antiphishing con asistencia en la nube ayuda a evitar que los empleados se conviertan en víctimas de campañas de phishing y spear phishing que pueden llevar a infecciones por cryptors.

Enlaces relacionados

- Herramienta gratuita anti-ransomware
- #nomoreransomware
- Kaspersky Lab Daily
- Kaspersky Endpoint Security for Business
- Soluciones de Kaspersky Lab para la empresa
- Por qué elegir Kaspersky Lab frente al ransomware
- Impacto financiero de la seguridad en el negocio