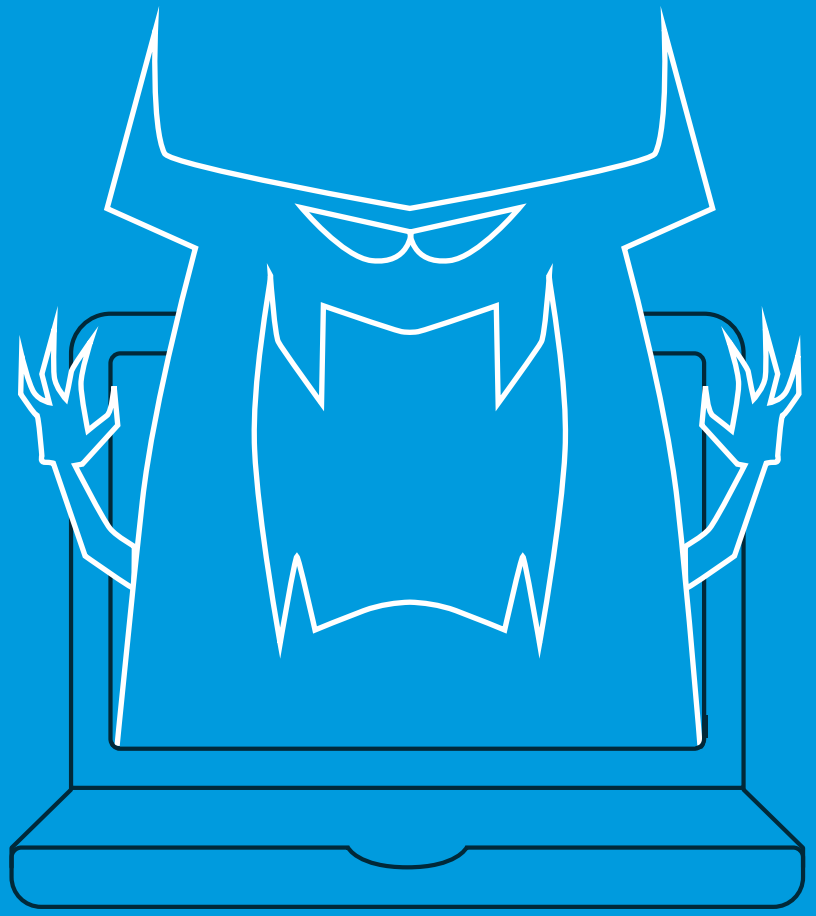
datto

FOLLETO ELECTRÓNICO

GUÍA EMPRESARIAL SOBRE EL RANSOMWARE

Todo lo que necesita saber para mantener su empresa a flote



Índice

INTRODUCCIÓN

Cada vez más, el ransomware supone una amenaza grave para empresas y particulares. El ransomware, un tipo de malware que cifra los datos de los sistemas infectados, se ha convertido en una opción lucrativa para los extorsionistas cibernéticos. Cuando se ejecuta, el malware bloquea los archivos de la víctima y permite a los criminales solicitar un pago para desbloquearlos.

A menos que no esté al día, seguramente sepa que el ransomware es un tema candente de actualidad. Ha afectado a empresas de todos tipos y tamaños, pero las empresas pequeñas son particularmente vulnerables a los ataques. Y el ransomware va en aumento. En un estudio reciente llevado a cabo por el distribuidor de software de seguridad McAfee Labs, los investigadores identificaron más de 4 millones de muestras de ransomware en el segundo trimestre de 2015, incluidos 1,2 millones de muestras nuevas, en comparación con menos de 1,5 millones de muestras en total en el tercer trimestre de 2013 (400 000 nuevas). El ransomware se distribuye de varias maneras y es difícil protegerse contra él ya que, como el virus de la gripe, evoluciona constantemente.

Hay varias maneras en las que puede proteger su empresa de los ataques de ransomware. En este folleto electrónico, descubrirá cómo se propaga el malware, los diferentes tipos de ransomware que existen hoy en día y lo que puede hacer para evitar un ataque o recuperarse de uno. No sirve de nada ignorar el problema, ya que los extorsionistas de hoy en día juegan sucio. Asegúrese de que su organización está preparada.

El exploit kit Angler utiliza HTML y JavaScript para identificar el navegador de la víctima y los complementos instalados, lo que permite al hacker seleccionar el ataque con mayores probabilidades de éxito.
Angler, que utiliza una variedad de técnicas de camuflaje, evoluciona constantemente para evitar ser detectado por los productos de software de seguridad.

EL RANSOMWARE HOY EN DÍA

Existen varios tipos principales, o familias, de ransomware. Cada tipo incluye diversas variedades. Se espera que con el tiempo surjan nuevas familias. En el pasado, los ataques se han dirigido a Microsoft Office, Adobe PDF y archivos de imágenes, pero McAfee prevé que, a medida que el ransomware siga evolucionando, otros tipos de archivos se convertirán también en objetivos.

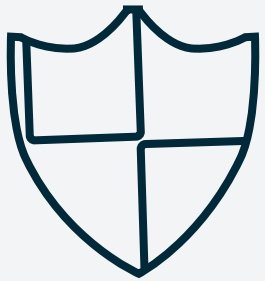
La mayoría del ransomware utiliza el algoritmo AES para cifrar los archivos, aunque también se utilizan otros algoritmos. Para descifrar los archivos, los extorsionistas cibernéticos suelen solicitar un pago en Bitcoin o mediante servicios de cupones de pago en línea, como Ukash o Paysafecard. La tarifa habitual ronda los 400 euros, aunque hemos visto importes muy superiores. Los delincuentes cibernéticos que lanzan campañas de ransomware suelen concentrar sus ataques en países y ciudades de mayor nivel económico en los que las personas y empresas pueden permitirse pagar el rescate. En los últimos meses, hemos visto ataques repetidos en determinados sectores, especialmente en el de la Sanidad.

Cómo se propaga el ransomware

El spam es la vía más común de distribución de ransomware. Por lo general, se propaga mediante algún tipo de ingeniería social. Se engaña a las víctimas, que piensan que están descargando un documento adjunto en un correo o haciendo clic en un enlace. Los mensajes de correo electrónico falsos pueden parecer una nota de un amigo o compañero que solicita al destinatario que consulte el documento adjunto, por ejemplo. El correo también puede proceder de una institución de confianza (como un banco) y pedirle que realice una tarea rutinaria. A veces, el ransomware utiliza tácticas que asustan y coaccionan a la víctima al asegurar que el ordenador se ha utilizado para realizar actividades ilegales. Una vez que el usuario realiza la acción, el malware se instala en el sistema y comienza a cifrar los archivos. Puede pasar en un instante con tan solo hacer un clic.

Otro método común que utiliza el ransomware es un paquete de software denominado "exploit kit". Estos paquetes están diseñados para identificar vulnerabilidades y aprovecharlas a fin de instalar ransomware. En este tipo de ataque, los hackers instalan código en un sitio web legítimo que redirige a los usuarios a un sitio malintencionado. A diferencia del spam, a veces este enfoque no requiere que la víctima realice ninguna acción. Es lo que se conoce como un ataque de "descarga oculta".

El exploit kit más común que se utiliza hoy en día es Angler. Un estudio llevado a cabo en mayo de 2015 por el distribuidor de software de seguridad Sophos demostró que todos los días se crean miles de nuevos sitios web que contienen Angler. El exploit kit Angler utiliza HTML y JavaScript para identificar el navegador de la víctima y los complementos instalados,



También existen opciones para aspirantes a hackers con habilidades informáticas mínimas. De acuerdo con McAfee, existen ofertas de ransomware como servicio en la red Tor, que permiten a prácticamente cualquier persona llevar a cabo estos tipos de ataques.

lo que permite al hacker seleccionar el ataque con mayores probabilidades de éxito. Angler, que utiliza una variedad de técnicas de camuflaje, evoluciona constantemente para evitar ser detectado por los productos de software de seguridad. No obstante, Angler no es más que un exploit kit; hay varios otros en uso.

Los botnets de spam y exploit kits son relativamente sencillos de utilizar, pero requieren ciertos conocimientos técnicos. Sin embargo, también existen opciones para aspirantes a hackers con habilidades informáticas mínimas. De acuerdo con McAfee, existen ofertas de ransomware como servicio en la red Tor, que permiten a prácticamente cualquier persona llevar a cabo estos tipos de ataques.

TIPOS COMUNES DE RANSOMWARE

Como se ha mencionado anteriormente, el ransomware evoluciona constantemente y aparecen nuevas variedades todo el tiempo. Por ello, sería difícil, si no imposible, crear una lista de todos los tipos de ransomware en uso hoy en día. Mientras que la siguiente no es una lista exhaustiva de todos los tipos de ransomware actuales, permite hacerse una buena idea de los programas principales y la gran variedad disponible.

CryptoLocker

El ransomware ha existido en distintos formatos durante las últimas dos décadas, pero cobró fama en 2013 con CryptoLocker. El botnet original de CryptoLocker se deshabilitó en mayo de 2014, pero para entonces ya había extorsionado unos 2,5 millones de euros de sus víctimas. Desde entonces, el método CryptoLocker se ha copiado numerosas veces, aunque las variedades en uso hoy en día no están directamente vinculadas con el original. La palabra CryptoLocker, al igual que las palabras Xerox y Kleenex en sus respectivos sectores, se ha convertido en sinónimo del ransomware.

CryptoLocker se distribuye mediante exploit kits y spam. Cuando se ejecuta el malware, se instala en la carpeta de perfil del usuario de Windows y cifra los archivos en los discos duros locales y las unidades de red asignadas. Solo cifra los archivos con extensiones específicas, como Microsoft Office, OpenDocument, imágenes y AutoCAD. Una vez completado el trabajo sucio, aparece un mensaje en la pantalla del usuario que lo informa de que los archivos han sido cifrados y le solicita un pago en Bitcoin.

CryptoWall

CryptoWall cobró fama tras la caída del CryptoLocker original. Apareció a comienzos de 2014 y, desde entonces, se han creado variedades con distintos nombres: Cryptorbit, CryptoDefense, CryptoWall 2.0 y CryptoWall 3.0, entre otros. Al igual que CryptoLocker, CryptoWall se distribuye a través de spam o exploit kits.

Las campañas de spam que están propagando Locky operan a escala masiva. El malware se distribuye mediante spam, normalmente a través de un mensaje de correo electrónico que parece una factura. Cuando se abre, la factura está codificada y se pide al usuario que active las macros para poder leer el documento.

La versión original de CryptoWall utilizaba una clave de cifrado pública RSA, pero las versiones posteriores (incluida la más reciente, CryptoWall 3.0) utilizan una clave AES, que se oculta como clave AES pública. Cuando se abre el archivo de malware adjunto, el código binario de CryptoWall se copia en la carpeta Temp de Microsoft y comienza a codificar los archivos. CryptoWall cifra más tipos de archivos que CryptoLocker pero, una vez completado el proceso de cifrado, también muestra un mensaje en la pantalla del usuario solicitando un pago.

CTB-Locker

Los criminales que han creado CTB-Locker utilizan un método distinto de distribución del virus. Inspirándose en las empresas Girl Scout Cookies y Mary Kay Cosmetics, estos hackers externalizan el proceso de infección a sus socios a cambio de un porcentaje de los beneficios. Se trata de una estrategia de eficacia demostrada para conseguir grandes volúmenes de infecciones de malware a mayor velocidad.

Cuando se ejecuta CTB-Locker, se copia en el directorio Temp de Microsoft. A diferencia de la mayoría de los tipos de ransomware actuales, CTB-Locker usa la criptografía de curva elíptica (ECC) para cifrar los archivos. CTBLocker afecta a más tipos de archivos que CryptoLocker. Una vez que se han cifrado los archivos, CTB-Locker muestra un mensaje en el que se solicita un pago en, como ya se imaginará, Bitcoin.

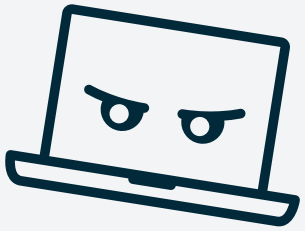
Locky

Locky es un tipo relativamente nuevo de ransomware, pero su método resulta familiar. El malware se distribuye mediante spam, normalmente a través de un mensaje de correo electrónico que parece una factura. Cuando se abre la factura, está codificada y se pide al usuario que active las macros para poder leer el documento. Cuando se activan las macros, Locky comienza a cifrar una gran variedad de tipos de archivos mediante el cifrado AES. Una vez completado el proceso, solicita un pago en Bitcoin. ¿Resulta obvio el patrón?

Las campañas de spam que están propagando Locky operan a escala masiva. Una compañía informó de haber bloqueado cinco millones de correos electrónicos asociados con campañas de Locky en dos días.

TeslaCrypt

TeslaCrypt es otro tipo nuevo de ransomware. Como la mayoría de los demás ejemplos, utiliza un algoritmo AES para cifrar los archivos. Normalmente, se distribuye mediante el exploit kit de Angler y, en particular, detecta las vulnerabilidades de Adobe. Una vez aprovechada la vulnerabilidad, TeslaCrypt se instala en la carpeta Temp de Microsoft. En lo referente al pago, TeslaCrypt ofrece varias opciones: Bitcoin, Paysafecard y Ukash. ¿A quién no le gusta disponer de varias opciones?



Disponer de software de seguridad es algo fundamental, pero no puede quedarse ahí. Una estrategia adecuada de protección contra el ransomware requiere una metodología triple, que se compone de educación, seguridad y copias de seguridad.

TorrentLocker

Por lo general, TorrentLocker se distribuye mediante campañas de spam y está dirigido geográficamente, es decir, los correos electrónicos se envían a regiones específicas. A menudo, se utiliza la palabra CryptoLocker para referirse a TorrentLocker, que utiliza un algoritmo AES para cifrar los archivos. Además de cifrar los archivos, recoge las direcciones de correo electrónico de la agenda de contactos de la víctima para distribuir el malware más allá del ordenador o red infectados, característica exclusiva de TorrentLocker.

TorrentLocker utiliza una técnica denominada vaciado del proceso, mediante la que se inicia un proceso del sistema de Windows en estado suspendido, después se instala código malintencionado y, por último, se reanuda el proceso. Utiliza explorer.exe para el vaciado del proceso. Este malware también elimina las instantáneas de volumen de Microsoft para impedir una restauración con las herramientas de recuperación de Windows. Como es el caso con los demás programas mencionados anteriormente, la divisa de preferencia para el pago es Bitcoin.

KeRanger

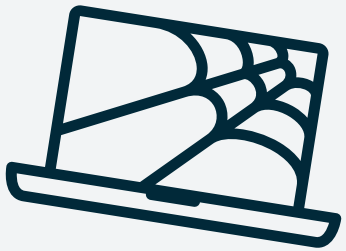
De acuerdo con ArsTechnica, hace poco se detectó el ransomware KeRanger en un cliente popular de BitTorrent. El uso de KeRanger no está muy extendido todavía, pero merece la pena nombrarlo porque es el primer ransomware operativo diseñado para bloquear aplicaciones de Mac OS X.

PROTÉJASE DEL RANSOMWARE

Los delincuentes cibernéticos armados con ransomware son un temible enemigo. Aunque las campañas de ransomware no están específicamente dirigidas a las pymes, estas son más propensas a sufrir un ataque. Con frecuencia, los equipos informáticos de las empresas pequeñas están desbordados y, en algunos casos, utilizan tecnología antigua por motivos de restricciones del presupuesto. En lo referente a la vulnerabilidad ante el ransomware, se trata de la tormenta perfecta. Por suerte, hay varias maneras conocidas y comprobadas de proteger su empresa de los ataques de ransomware. Disponer de software de seguridad es algo fundamental, pero no puede quedarse ahí. Una estrategia adecuada de protección contra el ransomware requiere una metodología triple, que se compone de educación, seguridad y copias de seguridad.

Educación: En primer lugar, la educación es fundamental para proteger a su empresa del ransomware. Es esencial que sus empleados entiendan lo que es el ransomware y la amenaza que supone. Proporcione a su equipo ejemplos específicos de correos sospechosos con instrucciones claras acerca de qué hacer si se encuentran con un posible cebo de ransomware (es decir, no abrir los archivos adjuntos, comunicar lo que han visto, etc.).

Como el ransomware evoluciona constantemente, puede traspasar incluso el mejor software de seguridad. Por eso, es fundamental para las empresas contar con un segundo nivel de defensa que garantice la recuperación en caso de que se produzca un ataque de malware: las copias de seguridad.



Realice cursos de formación dos veces al año para informar a los empleados del riesgo del ransomware y otras amenazas cibernéticas. Cuando se incorporen al equipo nuevos empleados, asegúrese de enviarles un correo electrónico para ponerlos al día sobre las prácticas recomendadas en materia cibernética. Es importante que el mensaje se comunique con claridad a todos los empleados de la empresa, en lugar de transmitirse de boca en boca. Por último, mantenga informados a los empleados cuando aparezca un nuevo tipo de ransomware o cuando modifique su comportamiento.

Seguridad: El software antivirus debería ser considerarse algo fundamental en cualquier empresa como método de protección contra el ransomware y otros riesgos. Asegúrese también de que el software de seguridad está actualizado, de modo que pueda protegerse de amenazas identificadas recientemente. Mantenga las aplicaciones empresariales actualizadas y con los parches pertinentes para minimizar las vulnerabilidades.

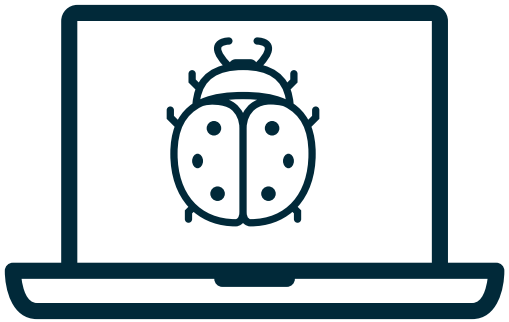
Algunos productos de software antivirus ofrecen funcionalidades específicas de ransomware. Por ejemplo, Sophos incorpora una tecnología que supervisa los sistemas para detectar actividades malintencionadas como cambios a la extensión de los archivos o en el registro. Si se detecta ransomware, el software puede bloquearlo y alertar a los usuarios.

No obstante, como el ransomware evoluciona constantemente, puede traspasar incluso el mejor software de seguridad. Por eso, es fundamental para las empresas contar con un segundo nivel de defensa que garantice la recuperación en caso de que se produzca un ataque de malware: las copias de seguridad.

Copias de seguridad: Las soluciones de protección de datos completas y modernas, como Datto, realizan copias de seguridad incrementales basadas en instantáneas con frecuencias que pueden alcanzar los cinco minutos, a fin de crear una serie de puntos de recuperación. Si su empresa sufre un ataque de ransomware, esta tecnología le permite restaurar los datos a un momento determinado antes de que fueran dañados. En lo referente al ransomware, esto aporta dos ventajas. En primer lugar, no es necesario que pague el rescate para recuperar sus datos. En segundo lugar, como está restaurando los datos a un momento determinado antes de que se produjera la infección de ransomware, puede asegurarse de que todo está en buen estado y de que la infección no se activará y volverá a infectar los datos.

Además, hoy en día, algunos productos de protección de datos permiten a los usuarios ejecutar aplicaciones a partir de copias de seguridad de máquinas virtuales basadas en imágenes. Esta función se denomina con frecuencia "recuperación en el sitio" o "recuperación instantánea". Esta tecnología puede resultar útil para recuperarse de un ataque de ransomware, ya que le permite continuar con las operaciones empresariales mientras se restablecen los sistemas principales, sin apenas experimentar tiempo de

inactividad. La versión de Datto de esta tecnología crucial para las empresas se llama Instant Virtualization y virtualiza los sistemas de forma local o remota en una nube segura en cuestión de segundos. La solución garantiza que las empresas puedan seguir operando cuando ocurre lo peor.



CONCLUSIÓN

Los extorsionistas cibernéticos que utilizan el ransomware constituyen una amenaza real para las empresas de hoy en día, desde la pizzería de la esquina a las empresas de la lista Fortune 500. Sin embargo, un poco de formación y las soluciones adecuadas pueden marcar una gran diferencia. Asegúrese de que sus empleados entienden de lo que deberían estar pendientes y se evitará numerosos dolores de cabeza. Nunca subestime la dedicación y la experiencia de los hackers actuales. Se adaptan constantemente y perfeccionan su arma preferida. Por eso necesita el mejor software de seguridad y de copias de seguridad. Mantenga su empresa a salvo y relájese.

A modo de conclusión, diremos que la distribución de la información y el software de seguridad pueden ayudarle a evitar los ataques cibernéticos. La gestión de parches es fundamental. Asegúrese de que el software está actualizado y es seguro. Al final, cuando todo lo demás falle, será la copia de seguridad la que le ayudará a volver a ponerse en marcha. Considere utilizar un producto de copias de seguridad moderno con características que puedan eliminar permanentemente el tiempo de inactividad.

Tal vez le interese...

FOLLETO ELECTRÓNICO GRATUITO

The 4 Essentials of Business Continuity Planning

Prepare su empresa para todo

DESCARGAR YA