SOPHOS
Security made simple.

CÓMO PROTEGERSE DEL RANSOMWARE

Pequeñas y grandes empresas se enfrentan a la amenaza de ataques de ransomware cada vez más brutales y agresivos. Perder el acceso a archivos críticos y la consiguiente demanda de un pago puede provocar enormes interrupciones en la productividad de una empresa.

¿Pero cómo es un ataque típico? ¿Y qué soluciones de seguridad deben implementarse para contar con la mejor defensa posible?

Este monográfico estudia las tecnologías más utilizadas para distribuir el ransomware, analiza por qué son eficaces estos ataques y proporciona nueve recomendaciones de seguridad para ayudarle a estar protegido. También subraya las tecnologías de seguridad fundamentales que debe incluir cada configuración de TI.

Monográficos de Sophos Febrero de 2018

Ransomware: una breve presentación

El ransomware es una de las amenazas más extendidas y perjudiciales a las que se enfrentan los usuarios de Internet. Desde que se detectó el infame CryptoLocker por primera vez en 2013, hemos visto una nueva generación de variantes de ransomware de cifrado de archivos, que se introduce a través de los mensajes de spam y kits de explotación con el fin de extorsionar tanto a usuarios particulares como a empresas.

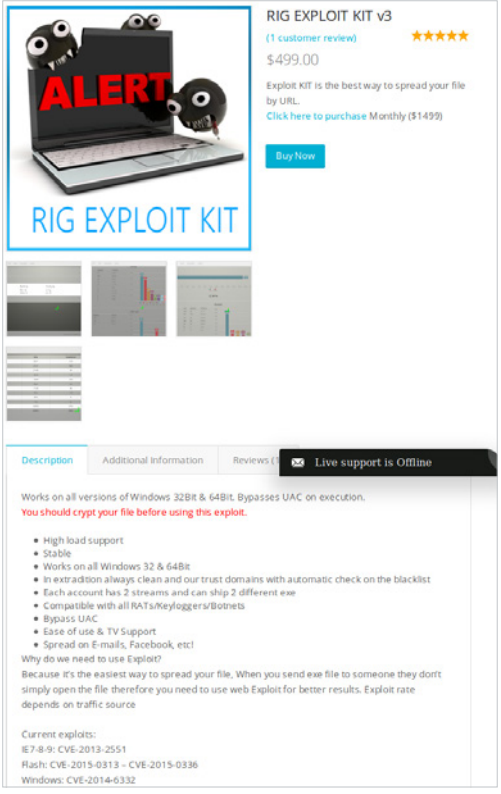
El origen de la actual oleada de familias de ransomware se remonta a los inicios del Fake AV o falso antivirus, pasando por las variantes de «Locker» y, finalmente, hasta las variantes de cifrado de archivos que prevalecen hoy día. Las distintas categorías de malware comparten un objetivo común: extorsionar a las víctimas para sacarles dinero a través de técnicas de ingeniería social y, directamente, intimidación. Y estas demandas económicas se han vuelto cada vez más contundentes.

Una encuesta de Sophos a 2700 empresas reveló que el 54 % de ellas se habían visto afectadas por el ransomware, con una media de dos ataques. De esas empresas afectadas, el 77 % contaba con un antivirus actualizado en el momento del ataque. Y los costes son punitivos: la media del impacto por empresa es de 133 000 USD (100 000 GBP).

¿Por qué son tan eficaces los ataques de ransomware?

La mayoría de las organizaciones tienen implementado al menos algún tipo de seguridad informática. Entonces, ¿por qué se cuelan a través de la red los ataques de ransomware?

1. **Técnicas de ataque sofisticadas e innovación constante**
   - Cada vez es más fácil acceder a programas de «exploit como servicio» (EaaS) ya preparados, con lo que es más sencillo iniciar un ataque, llevarlo a cabo correctamente y beneficiarse de él, incluso para criminales menos expertos en tecnología. A continuación, se muestra un programa EaaS a la venta.



- Se emplean prácticas de ingeniería social muy hábilmente para llevar al usuario a ejecutar la secuencia de instalación del ransomware. Por ejemplo, podría recibir un mensaje como este:

  «En el archivo adjunto se detallan los requisitos de mi empresa. Envíenos un presupuesto.»

- Los creadores del ransomware actúan de forma muy profesional. Esto incluye entregar una herramienta de descifrado operativa una vez pagado el rescate, aunque no hay ninguna garantía al respecto.

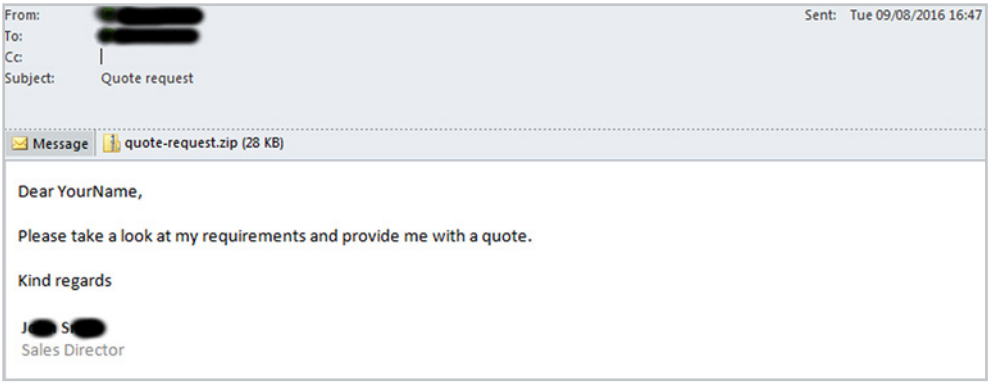
2. **Brechas de seguridad en las empresas afectadas**
   - Estrategia de copias de seguridad inadecuada (sin copias de seguridad en tiempo real, sin copias de seguridad sin conexión/fuera de la red).
   - Las actualizaciones y los parches para el sistema operativo y las aplicaciones no se implementan lo bastante rápido.
   - Permisos de derechos o usuario peligrosos (los usuarios trabajan como administradores o tienen más derechos sobre los archivos de las unidades de red de lo que es necesario para sus tareas).
   - Falta de formación de seguridad de los usuarios («¿Qué documentos puedo abrir y de quién?», «¿Cuál es el procedimiento si un documento parece malicioso?», «¿Cómo reconozco un correo de phishing?»).
   - No se han implementado sistemas de seguridad (programas antivirus, firewalls, IPS y puertas de enlace a Internet o de correo electrónico) o no están configurados correctamente. Aquí también cabe incluir una segmentación de red inadecuada (servidores y estaciones de trabajo en la misma red).
   - Falta de conocimientos de seguridad informática (los archivos .exe pueden estar bloqueados en el correo electrónico, pero no en las macros de Office u otro contenido activo).
   - Conflictos de prioridades («Sabemos que este método no es seguro, pero nuestros empleados tienen que trabajar...»).
3. **Falta de tecnología de prevención avanzada**
   - Muchas organizaciones tienen una forma u otra de protección genérica.
   - El ransomware se está actualizando constantemente para explotar y esquivar esta protección. Por ejemplo, se autoelimina con tal rapidez después de cifrar los archivos que no se puede analizar.
   - Las soluciones deben diseñarse especialmente para combatir las técnicas de ransomware.

¿Cómo se produce un ataque de ransomware?

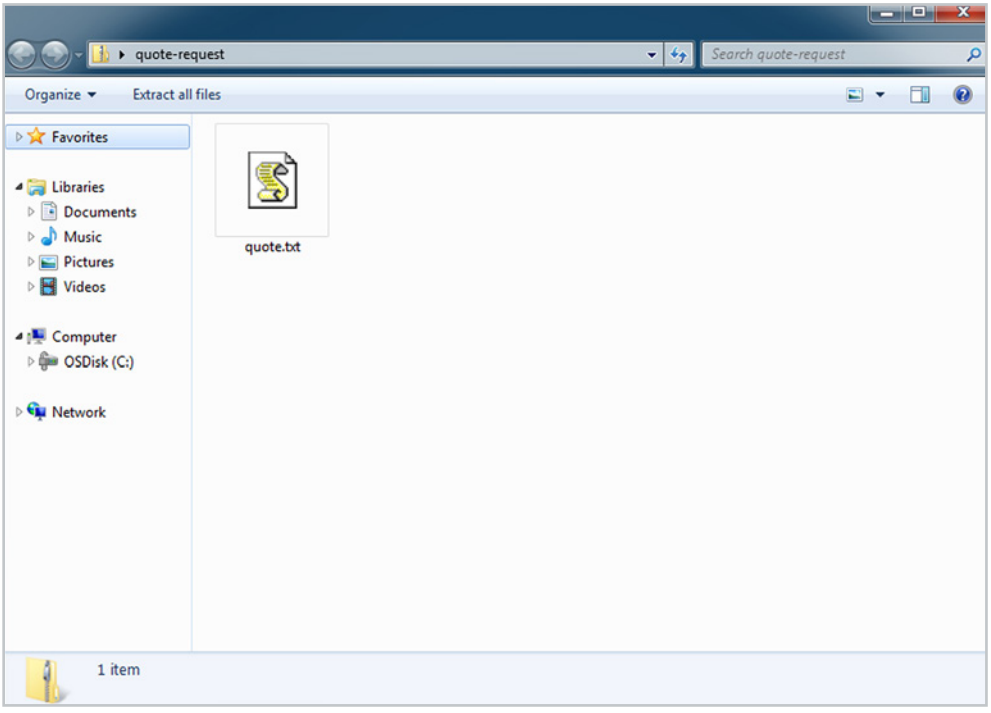
Un ataque de ransomware se inicia principalmente de dos maneras: a través de un correo electrónico con un archivo adjunto malicioso o al visitar un sitio web infectado (a menudo legítimo y de uso generalizado).

Correo electrónico malicioso

Los criminales de hoy en día crean correos electrónicos que son imposibles de distinguir de los mensajes legítimos. Sin errores de gramática ni de ortografía, suelen estar escritos de forma que sean de interés para usted y su negocio.



Al abrirlo, el archivo zip parece contener un archivo .txt normal y corriente.



Sin embargo, al ejecutar el archivo el ransomware se descarga e instala en el equipo. En este ejemplo, el troyano es en realidad un archivo JavaScript camuflado como un archivo .txt, pero existen muchas otras variaciones de este método, como enviar un documento de Word con macros o archivos de acceso directo (.lnk).

Sitios web maliciosos

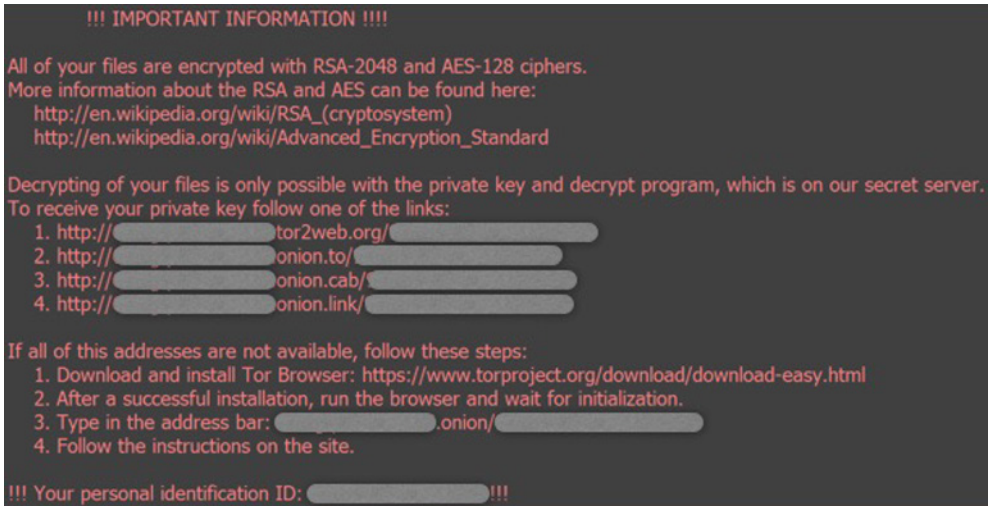
Otra forma habitual de infectarse es visitar un sitio web legítimo que se haya infectado con un kit de explotación. Incluso los sitios web populares pueden verse afectados de forma temporal. Los kits de explotación son herramientas del mercado negro que los criminales utilizan para explotar vulnerabilidades conocidas o desconocidas (como los exploits de día cero).

Uno visita el sitio web pirateado y hace clic en un enlace aparentemente inofensivo, pasa el cursor sobre un anuncio o en muchos casos simplemente consulta la página. Y eso es suficiente para descargar el archivo de ransomware en el equipo y ejecutarlo, a menudo sin signos visibles del ataque hasta después de que el daño ya esté hecho.

Qué pasa después

Después de la exposición inicial, como en los ejemplos de infección por correo electrónico o a través de Internet, el programa de ransomware emprende otras acciones:

- Contacta con el servidor de comando y control del atacante, envía información sobre el ordenador infectado y descarga una clave pública individual para este equipo.
- Los tipos de archivo específicos (que varían en función del tipo de ransomware) como documentos de Office, archivos de base de datos, PDF, documentos CAD, HTML, XML, etc., se cifran en el equipo local, dispositivos extraíbles y todas las unidades de red accesibles.
- Las copias de seguridad automáticas del sistema operativo Windows (las instantáneas) suelen eliminarse para impedir la recuperación de datos.
- Aparece un mensaje en el escritorio que explica que puede pagarse un rescate (normalmente en forma de bitcoines) en un plazo específico.



- Finalmente, el ransomware se elimina, de forma que solo quedan los archivos cifrados y la información del rescate.

Brote del ransomware Wanna Decrypt0r 2.0

Wanna (también conocido como WannaCry, WCry, WanaCrypt, WanaCrypt0r y Wana DeCrypt0r) es un programa de ransomware de rápida propagación que empezó a generar problemas a nivel global el 12 de mayo de 2017.

El análisis parece haber confirmado que el ataque fue lanzado utilizando presunto código de la Agencia de Seguridad Nacional estadounidense (NSA) filtrado por el grupo de hackers Shadow Brokers. Utiliza una variante del exploit EternalBlue (CC-1353) expuesto por los Shadow Brokers y usa un cifrado sólido en archivos como documentos, imágenes y vídeos.

Excepcionalmente, Wanna logró explotar una vulnerabilidad de ejecución de código remoto (RCE) que le permitió infectar equipos desactualizados sin que los usuarios hicieran nada. Es por este motivo por el que Wanna se propagó con rapidez, de forma parecida a los brotes de gusanos como Slammer y Conficker hace más de una década.

La vulnerabilidad de RCE explotada era un fallo en el servicio del bloque de mensaje de servidor (SMB) de Windows, que las estaciones Windows utilizan para compartir archivos e impresoras en redes locales. Microsoft había abordado esta cuestión en su boletín MS17-010 de marzo de 2017, pero los sistemas que no habían instalado la actualización o que tenían versiones de Windows que ya no eran compatibles seguían siendo vulnerables.

En respuesta al brote, Microsoft tomó la insólita decisión de publicar la actualización de seguridad para las plataformas con soporte personalizado (como Windows XP) para todo el mundo. Se recomienda encarecidamente instalar esta actualización lo antes posible.

Para obtener más información, consulte el artículo de la base de conocimiento de Sophos: www.sophos.com/kb/126733

Nueve mejores prácticas de seguridad que aplicar

Protegerse contra el ransomware no solo consiste en contar con las últimas soluciones de seguridad. Las buenas prácticas de seguridad informática, incluida la formación periódica de los empleados, son componentes esenciales de todas y cada una de las estrategias de seguridad. Asegúrese de seguir estas nueve mejores prácticas:

1. **Aplique los parches con prontitud y frecuencia**

El malware que no se introduce a través de un documento aprovecha los errores de seguridad de aplicaciones populares, como Microsoft Office, su navegador, Flash y otras. Cuanto más pronto aplique las revisiones de software, menos agujeros existirán para explotarse.

2. **Realice copias de seguridad periódicamente y guarde una copia de seguridad reciente fuera de la red y sin conexión**

Existen muchísimas razonas aparte del ransomware por las que pueden perderse los archivos de repente, como incendios, inundaciones, robos, accidentes con portátiles e incluso eliminaciones accidentales. Cifre las copias de seguridad para no tener que preocuparse si el dispositivo con las copias acaba en malas manos.

3. **Habilite las extensiones de archivo**

La opción predeterminada de Windows es que las extensiones de archivo no estén habilitadas, lo que significa que dependemos de la miniatura del archivo para identificarlo. Al habilitar las extensiones resulta mucho más fácil detectar los tipos de archivo que usted o sus usuarios no suelen recibir habitualmente, como JavaScript.

4. **Abra los archivos JavaScript (.JS) con el Bloc de notas**

Abrir un archivo JavaScript con el Bloc de notas impide que ejecute código malicioso y le permite examinar su contenido.

5. **No habilite las macros de los documentos adjuntos que reciba por correo electrónico**

Microsoft desactivó la ejecución automática predeterminada de las macros deliberadamente hace muchos años como medida de seguridad. Muchas infecciones dependen de que usted vuelva a activar las macros, así que no se deje convencer.

6. **Tenga cuidado con los archivos adjuntos no solicitados**

Los atacantes confían en el dilema que se le plantea al destinatario de que no debería abrir un documento sin estar seguro de que es el que espera, cosa que no puede saber si no lo abre. Si tiene dudas, no lo haga.

7. **No se conceda más derechos de los que necesita**

No permanezca conectado como administrador más tiempo del que sea estrictamente necesario, y evite explorar y abrir documentos u otras actividades de trabajo común mientras tenga derechos de administrador.

8. **Manténgase al día sobre las nuevas funciones de seguridad en sus aplicaciones empresariales**

Por ejemplo, ahora Office 2016 incluye el control «Bloquear la ejecución de macros en archivos de Office procedentes de Internet», que le ayuda a protegerse contra contenido malicioso externo sin dejar de utilizar macros internamente.

9. **Aplique los parches con prontitud y frecuencia**

Estar al día con los parches de seguridad es tan importante que lo hemos incluido dos veces. No deje que el ransomware explote vulnerabilidades que disponen de parches.

Cómo le ayuda Sophos a protegerse

Para detener el ransomware, debe tener implementada una protección avanzada eficaz en cada fase de un ataque.

Proteja los endpoints

Intercept X utiliza múltiples capas de defensa para detener el ransomware al instante. La tecnología antiexploits detiene la distribución de ransomware, el Deep Learning bloquea el ransomware antes de que se ejecute y CryptoGuard previene el cifrado malicioso de archivos y revierte los cambios en los archivos afectados. Intercept X funciona de forma paralela a la protección antivirus existente, tanto de Sophos como de otros proveedores.

Proteja los servidores

Server Advanced incluye la función CryptoGuard, que evita el cifrado malicioso de archivos y revierte los cambios en los archivos afectados. Las listas blancas y el bloqueo permiten solo las aplicaciones autorizadas e identifican lo que pueden modificar. Todos los demás intentos de realizar cambios se bloquean. La detección de tráfico malicioso impide que el ransomware contacte con los servidores de comando y control y descargue la carga maliciosa.

Detenga los correos de phishing

Sophos Phish Threat envía simulaciones de ataques de phishing a su empresa para poner a prueba la preparación de los empleados frente a los ataques del mundo real. Los mensajes de correo electrónico, localizados a varios idiomas, pueden adaptarse a su empresa y sector. Puede consultar información detallada para saber cuántos usuarios han sido engañados, la predisposición general a los ataques y mucho más.

Asegúrese de utilizar las mejores prácticas de configuración para sus soluciones de Sophos.

www.sophos.com/kb/120797

Pruebe Sophos Intercept X gratis en

es.sophos.com/intercept-x

Más de 100 millones de usuarios en 150 países confían en Sophos para obtener la mejor protección contra amenazas complejas y fugas de datos. Nuestro objetivo es ofrecer soluciones de seguridad completa fáciles de desplegar, administrar y utilizar con el coste total de propiedad más bajo del sector. Sophos ofrece soluciones galardonadas de cifrado y protección para estaciones, Internet, correo electrónico, móviles, servidores y redes con el respaldo de SophosLabs, nuestra red de centros de investigación de amenazas. Infórmese mejor en www.sophos.com/es-es/products.

Ventas en España
Teléfono: (+34) 913 756 756
Correo electrónico: comercialES@sophos.com

Ventas en América Latina
Correo electrónico: Latamsales@sophos.com

2018-02 WP-ES (NP)