SOPHOS

Ransomware: La ciberamenaza que no desaparece

Después de 30 años desde el primer ciberataque de ransomware del mundo, los ciberdelincuentes siguen extorsionando a empresas, cifrando maliciosamente sus archivos y exigiendo sustanciosos rescates por devolver los datos intactos. Si bien los titulares aparecen y desaparecen, el ransomware es más fuerte que nunca, y hoy en día son comunes los rescates de hasta seis y siete cifras.

En este monográfico se exploran las razones tras la longevidad del ransomware, incluidos los factores que le han permitido volverse más rápido, inteligente y letal a lo largo de los años, y lo que debemos aprender de esta historia si hemos de minimizar nuestro riesgo de ataques en el futuro.

También se profundiza en las tres nuevas áreas en que está empezando a asentarse el ransomware, provocado por cambios tecnológicos y sociales acaecidos recientemente. Por último, se examinan las tecnologías y los comportamientos que deben adoptar las empresas para asegurarse de que cuentan con la mejor defensa posible contra el ransomware, y se explica cómo puede ayudar Sophos.

Contenido

El impacto del ransomware 2

La evolución del ransomware 3
- El nacimiento del ransomware 3
- Aprovechar las oportunidades 4
- El juego del gato y el ratón 4
- La evolución del ransomware: Ryuk 5

El futuro del ransomware 6
- Ransomware en la nube pública 6
- Ataques a proveedores de servicios 7
- Ataques sin cifrado 8

Cómo defenderse del ransomware 9
- Una protección contra amenazas que actúe en toda la cadena de ataque 9
  - Sophos Intercept X 10
  - Sophos XG Firewall 10
  - Seguridad sincronizada 10
  - Managed Threat Response (MTR) 10
- Prácticas de seguridad sólidas 11
- Formación continuada del personal 11

Conclusión 12

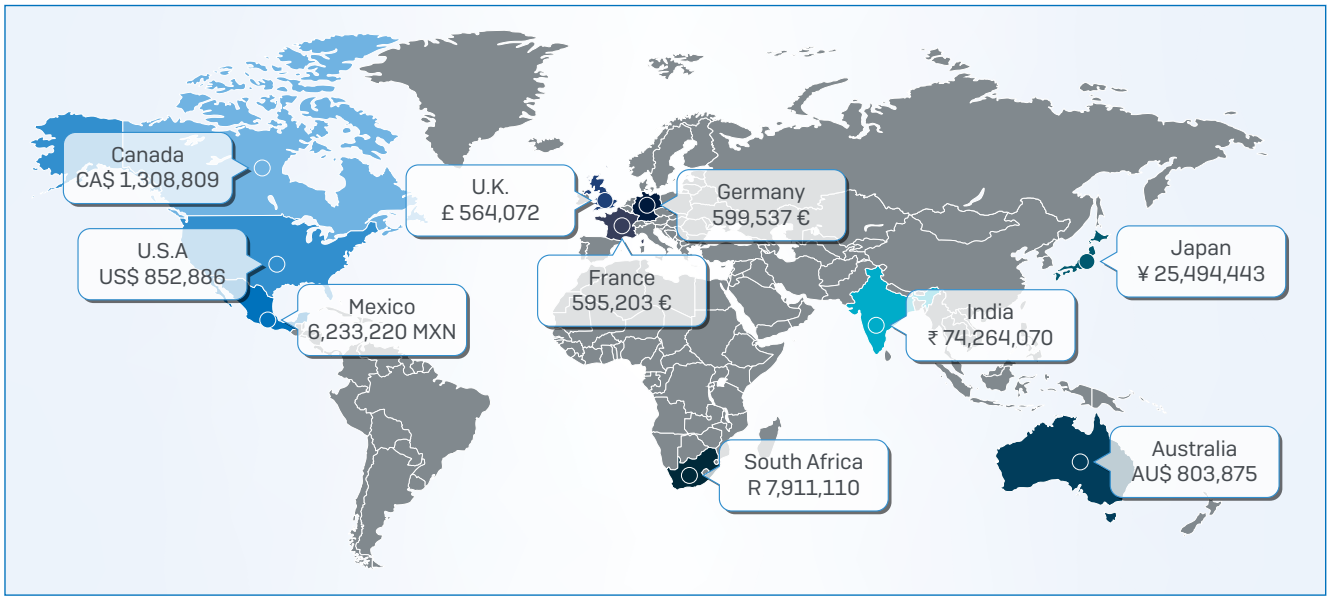
Lecturas recomendadas 12

El impacto del ransomware

El ransomware es una amenaza muy real para las empresas de todo el mundo. Una reciente encuesta independiente a 3100 directores de TI de 12 países encargada por Sophos reveló que el 21 % de las empresas se vieron afectadas por el ransomware en 2018. Y lo que es más, tres de cada 10 (30 %) de las empresas que fueron víctimas de un ciberataque experimentaron el ransomware.

El impacto financiero del ransomware es enorme. Si se suman todos los costes de la remediación, incluidos el tiempo de inactividad, las horas del personal, el coste de los dispositivos, el coste de la red, las oportunidades perdidas y el rescate pagado, las cifras finales por víctima resultan ruinosas.

Coste de rectificar un ataque de ransomware



Fuente: Estado actual de la seguridad para endpoints, Sophos, 2018

Dada la amplitud del alcance del ransomware y el alto coste de los ataques, la pregunta obvia es: ¿por qué es tan persistente? ¿Por qué, a pesar de todos nuestros avances en tecnología, no podemos eliminarlo para siempre? ¿Por qué puede tener un impacto tan devastador?

Para responder a estas preguntas, es necesario comprender cómo hemos llegado a la situación actual. Esto requiere que retrocedamos en el tiempo para ver cómo (y, lo que es fundamental, por qué) ha evolucionado el ransomware a lo largo de los años.

La evolución del ransomware

El nacimiento del ransomware

El ransomware no es nuevo. De hecho, el primer ciberataque de ransomware se lanzó en diciembre de 1989. El Dr. Joseph V. Popp envió 20 000 disquetes infectados con el Troyano de información sobre el sida. Se suponía que el programa era un sistema diseñado para asesorar a las personas sobre su riesgo de contraer el VIH y el sida pero, después de ejecutarlo 90 veces, cifraba el disco duro.

Quienes vivieron esa época recodarán que, en 1989, la gente apagaba el ordenador al final del día, de modo que el 90.º reinicio solía producirse cuatro o cinco meses después de ejecutar el programa por primera vez. El usuario veía una nota de rescate que exigía 189 $ por un año de uso del programa o 378 $ para poder usarlo indefinidamente. El pago debía realizarse mediante cheque bancario a una empresa en Panamá.

Nota de rescate de ransomware del Troyano de información sobre el sida

Por desgracia para el Dr. Popp, el cifrado utilizado era fácil de desentrañar y muy pronto aparecieron herramientas de descifrado gratuitas. Además, la idea de enviar el pago mediante cheque bancario a Panamá fue un fracaso. Como resultado, la iniciativa no llegó a generar ingresos y, en lugar de ello, terminó llevándole ante los tribunales.

Hay tres obstáculos principales que deben superar los ciberdelincuentes para perpetrar un ataque de ransomware satisfactorio: introducir el ransomware en los dispositivos de la víctima, cifrar y descifrar los archivos, y recibir el pago.

Aunque el Dr. Popp había identificado un enfoque efectivo, si bien muy poco escalable, para introducir su amenaza en los dispositivos de las víctimas (tuvo que grabar esos 200 000 disquetes manualmente), falló con las partes del cifrado y del pago del proceso.

☑ Instalar el ransomware

☒ Cifrar y descifrar los archivos

☒ Recibir el pago

Aprovechar las oportunidades

El ataque del Troyano de información sobre el sida sí que tuvo éxito en un aspecto: sacó partido de una oportunidad de un entorno más amplio, concretamente la preocupación generalizada sobre el VIH/sida que existía en aquella época. Desde entonces, los ciberdelincuentes han seguido aprovechando los avances tanto en tecnología como en la sociedad en general para desarrollar y perfeccionar sus ataques de ransomware, como:

- **El auge de los servicios gratuitos de correo electrónico como AOL y Yahoo**. Estos servicios permitieron a los hackers crear un número ilimitado de direcciones de correo electrónico no rastreables por primera vez, lo que llevó a la puesta en marcha de campañas de spam a gran escala utilizadas para propagar el ransomware.
- **El cambio de las conexiones de acceso telefónico al ADSL**, que permitió que muchas más personas utilizaran Internet y durante períodos más largos de tiempo, proporcionó a los delincuentes un área objetivo más amplia para sus ataques.
- **Las capacidades de segmentación geográfica** permitieron a los ciberdelincuentes dirigir sus ataques a un país o región en particular. La segmentación geográfica incrementó las probabilidades de éxito al permitir que los atacantes explotaran temas de actualidad locales en sus ataques por correo electrónico, al tiempo que adaptaban el idioma a su audiencia.
- **Las tarjetas de crédito de prepago** dieron a los delincuentes un método anónimo y accesible para recibir los pagos de los rescates.
- **La disponibilidad de las ciberdivisas**, en especial los bitcoins, facilitó a los delincuentes otra forma fiable y accesible de recibir los pagos.

Como resultado de aprovechar estas (y otras) oportunidades, para 2010, los ciberdelincuentes habían superado los tres principales retos a los que se enfrentaba el ransomware, con lo que se convirtió en una actividad comercial viable.

☑ Instalar el ransomware

☒ Cifrar y descifrar los archivos

☒ Recibir el pago

El juego del gato y el ratón

Una vez que el ransomware se generalizó, los ciberdelincuentes centraron sus esfuerzos en pulir y mejorar sus ataques a fin de incrementar los ingresos. Esto incluía:

- **Desarrollo de marca**. Los astutos ciberdelincuentes se dieron cuenta de que la gente solo pagaría si había una alta probabilidad de que se restauraran sus datos. En consecuencia, era fundamental contar con una herramienta de descifrado fiable para que el ransomware fuera una fuente de ingresos constantes. Al mismo tiempo, no todas las herramientas de descifrado eran iguales. Los responsables del ransomware con una buena herramienta no querían que se les asociara con otras menos eficientes y que eso manchara su reputación. Esto los llevó a utilizar una técnica de marketing que ha sido una práctica común en el mundo comercial durante décadas: el desarrollo de marca. Buscando rápidamente en Internet un nombre de ransomware, la víctima conoce las probabilidades que tiene de recuperar sus datos si paga.
- El **ransomware como servicio**, en que los expertos del ransomware aprovechaban la oportunidad comercial para facilitar "paquetes" de ransomware a otros malhechores que carecían de conocimientos sobre cifrado y de sistemas de pago pero que sabían bien cómo distribuir las amenazas. El servicio incluía el malware y pago en el backend a través de un sitio central a cambio del 30 % de los ingresos recibidos.

- El **ransomware de alto impacto**, que permitía a los responsables del ransomware mejorar su retorno de la inversión (ROI) lanzando devastadores ataques sobre un pequeño número de víctimas. Los ataques dirigidos requerían menos esfuerzo y tenían menos exposición, y al tiempo que incrementaban el impacto de su ataque, también aumentaban la propensión a pagar de la víctima.

Al mismo tiempo, el sector de la ciberseguridad se encontraba ocupado desarrollando sus tecnologías defensivas, identificando cómo detectar y bloquear los ataques de ransomware para anticiparse a los ciberdelincuentes.

La evolución del ransomware: Ryuk

El Ryuk, cuyo nombre procede de un personaje de la serie de manga Death Note, es posiblemente la forma de ransomware más desarrollada que existe en la actualidad. Los responsables del Ryuk suelen atacar a empresas que no pueden permitirse ningún tiempo de inactividad, como periódicos, municipalidades y servicios públicos, para incrementar la probabilidad de pago, y exigen rescates de hasta seis y siete cifras.

Para sortear las tecnologías antiransomware, estos adversarios activos combinan técnicas de ataque avanzadas con el hacking interactivo manual. Los ataques del Ryuk suelen empezar con un correo electrónico de spam que contiene un archivo adjunto malicioso. El adjunto desencadena un ataque del Emotet o el TrickBot, que permite a los ciberdelincuentes introducirse en la red de la víctima.

Una vez dentro de la red, los hackers roban credenciales y aumentan sus privilegios hasta que crean un nuevo usuario administrador. Con sus privilegios de administrador ampliados, los hackers se mueven lateralmente por la red usando múltiples técnicas como el protocolo de escritorio remoto (RDP), la inspección del servicio de Active Directory y la eliminación de las copias de seguridad.

Una vez desmantelada la red de seguridad de la víctima, tratan de desactivar los productos de ciberseguridad antes de liberar finalmente el ransomware Ryuk, que cifra los archivos y exige ingentes sumas de rescate.

Típica cadena de ataque del ransomare Ryuk

El futuro del ransomware

La gran lección que se puede extraer de la historia del ransomware es **que los ciberdelincuentes continúan explotando los cambios en la tecnología y la sociedad para perpetrar sus ataques de ransomware**. En pocas palabras, el ransomware seguirá evolucionando. Teniendo esto en cuenta, vamos a explorar las tres nuevas áreas en que está empezando a asentarse el ransomware, impulsado por las oportunidades que presentan los avances tecnológicos.

Ransomware en la nube pública

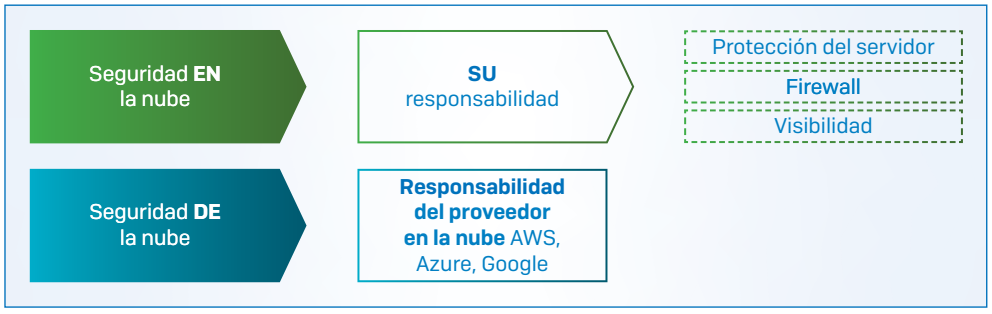
En el primer lugar de la lista está el ransomware en la nube pública, que es el ransomware que ataca y cifra los datos almacenados en servicios en la nube pública como Amazon Web Services (AWS), Microsoft Azure (Azure) y Google Cloud Platform (GCP). La adopción de la nube pública está creciendo y las empresas la utilizan de múltiples formas.

Para muchos, simplemente es un **reemplazo de los servidores locales físicos** que utilizaban para almacenar datos. Mientras que anteriormente los empleados guardaban los archivos en el servidor de la oficina, ahora los guardan en servidores en la nube. Otro caso de uso popular es **ejecutar aplicaciones web**, como ejecutar un sitio web o prestar servicios basados en Internet. El tercer caso de uso de la nube pública es el **desarrollo de software**. Cada vez más, los ingenieros de software escriben código en servidores en la nube pública, porque poner en marcha un servidor en la nube es más fácil y rápido que crear entornos físicos.

La nube pública ofrece muchas ventajas. Sin embargo, en el ámbito de la seguridad, hay mucha incertidumbre y confusión en cuanto a las responsabilidades. Muchas personas desconocen qué partes de la responsabilidad de la seguridad recae sobre los proveedores de la nube pública y qué partes sobre el cliente. No hay duda de que esto conlleva brechas en la protección y proporciona a los ciberdelincuentes del ransomware un tesoro de datos valiosos listos para ser cifrados.

El atractivo de la nube pública no termina ahí. El rápido aumento del volumen y el valor de los datos almacenados en la nube da a los ciberdelincuentes un objetivo mayor que perseguir. Además, la configuración frágil y el acceso público abierto a los recursos de la nube (ya sean buckets de almacenamiento, bases de datos, cuentas de usuario, etc.) se lo ponen más fácil a los delincuentes para penetrar en las bases de datos.

El primer paso para protegerse del ransomware en la nube pública es entender el modelo de responsabilidad compartida de la nube pública. En pocas palabras, significa que usted es responsable de proteger todo lo que ponga en la nube, lo que incluye todos sus datos, además del acceso a la nube pública. Los proveedores de la nube pública son responsables de la seguridad de la nube. Esto incluye la seguridad de las instalaciones físicas donde se encuentran los centros de datos.



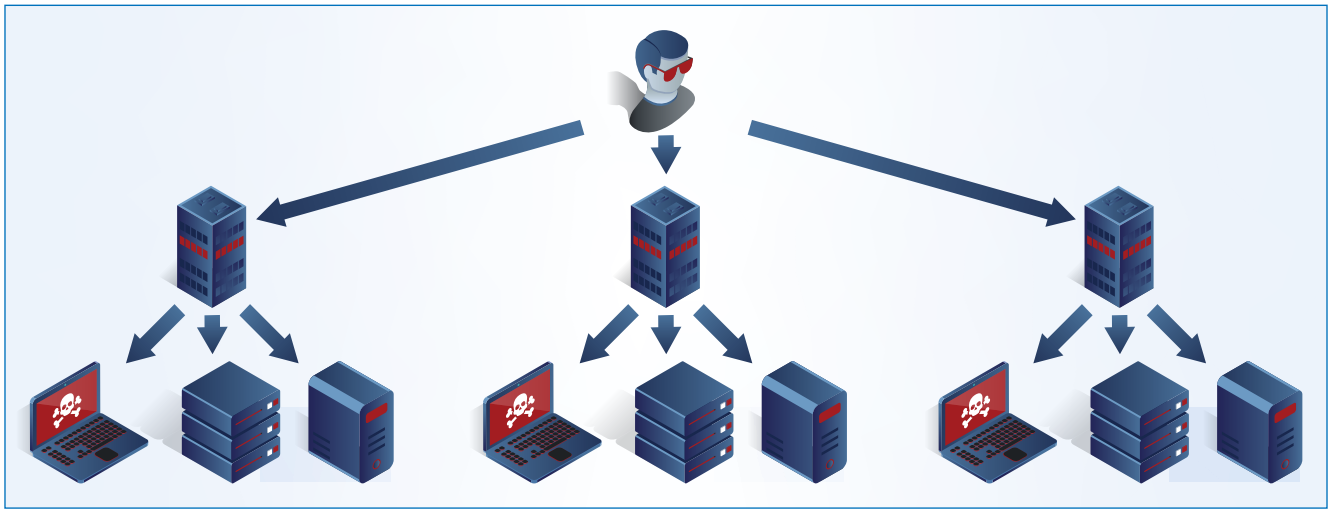
Debe aplicar a sus datos en la nube los mismos principios básicos que a sus datos locales. Igual que utiliza protección de servidores y un firewall localmente, debe utilizar protección de servidores y un firewall para proteger datos en la nube pública. Además, debe saber qué contenido tiene en la nube pública, para que pueda asegurarse de que está protegido.

Ataques a proveedores de servicios

La segunda área en que esperamos ver un crecimiento del ransomware es los ataques a proveedores de servicios. A medida que la tecnología y las amenazas se vuelven más complejas, las empresas subcontratan cada vez más sus servicios de TI a proveedores de servicios administrados (MSP). Estos MSP gestionan todos los aspectos de las TI para sus clientes, desde las impresoras hasta la seguridad. Para ello, necesitan tener acceso directo a las redes de sus clientes.

Tradicionalmente, los responsables del ransomware atacan las empresas de una en una. Una víctima, un rescate. Sin embargo, los ciberdelincuentes, siempre alerta a nuevas oportunidades de incrementar su ROI, se han percatado de que atacar a los MSP les permite secuestrar los datos de varias empresas en un único ataque. Un ataque, muchos rescates.

Modelo de ataque a proveedores de servicios



La respuesta en este caso es no mantener su seguridad en la empresa. Los MSP especializados en seguridad ofrecen un nivel de experiencia muy alto que es difícil de igualar para muchas empresas. En lugar de ello, convierta **la seguridad en uno de sus criterios de selección** a la hora de elegir su MSP. Pregúnteles sobre los productos y las prácticas de seguridad que utilizan en su propia empresa. Un buen MSP no tendrá ningún problema en compartirlo.

Y **pregúntese cuáles son sus prioridades**. ¿Es la protección la primera? Evidentemente, el coste es un factor para casi cualquier empresa, pero no es buena idea sacrificar la protección a largo plazo por el ahorro a corto plazo. Como hemos visto al principio, el coste de hacer frente a un ataque de ransomware pesa más que muchos otros gastos.

Ataques sin cifrado

El ransomware ha cerrado el círculo. La posibilidad de cifrar archivos era una de las capacidades básicas necesarias para convertir el ransomware en un ciberdelito viable. Sin embargo, los ciberdelincuentes ya no necesitan cifrar sus archivos para imponerle un rescate. ¿Por qué? Porque creen que pagará simplemente por evitar que sus datos se hagan públicos.

Hay dos tipos de datos que son objetivos específicos de este tipo de ataque. El primero son los datos personales, la información sobre una persona, también denominada información de identificación personal (PII). En los últimos años, la legislación para proteger los datos personales se ha reforzado significativamente con la implementación de leyes internacionales (como el RGPD), nacionales, regionales y específicas del sector para salvaguardar la información.

Estas leyes contemplan sanciones económicas muy sustanciosas para quien sufra una filtración de datos relevante (la multa máxima según el RGPD es de hasta el 4 % de la facturación anual mundial o 20 millones de euros, lo que sea mayor, para las empresas que incumplan sus requisitos). Los ciberdelincuentes pueden extorsionar a las empresas con la amenaza de divulgar la información personal, con lo que expondrían a la víctima a las consecuencias de una filtración de datos.

En octubre de 2019, la ciudad de Johanesburgo en Sudáfrica sufrió un ataque de ransomware sin cifrado. El grupo de atacantes en cuestión se hacía llamar Shadow Kill Hackers. Según una nota compartida en Twitter, no cifraron los datos. En lugar de ello, los robaron y amenazaron con subirlos a Internet si la ciudad no pagaba. La nota decía:

> *Todos vuestros servidores y datos han sido hackeados. Tenemos decenas de puertas traseras a vuestra ciudad. Tenemos control total de todo en vuestra ciudad. También hemos interceptado todas las contraseñas y datos confidenciales como información personal y financiera de la población.*

El grupo supuestamente exigió un pago de cuatro bitcoins (30 347 £), aunque, a fecha de hoy, parece que aún no se ha pagado el rescate.

El otro tipo de datos especialmente vulnerable a estos ataques es la propiedad intelectual o IP. Esta suele ser el origen del éxito de una empresa, ya sea una receta secreta, una tecnología patentada o unos datos únicos. Si esta propiedad intelectual se hace pública, podría constituir una sentencia de muerte para la empresa.

El ejemplo más público de este tipo de ataque de ransomware fue el que sufrió la banda Radiohead a mediados de 2019. El archivo del líder Thom Yorke fue hackeado, y los delincuentes le robaron 18 horas de música inédita de la época en que se lanzó el álbum de 1997 "OK Computer". Los extorsionadores amenazaron con hacer pública la música a menos que la banda pagara un rescate de 150 000 $, solicitud que Radiohead ignoró, y la banda prefirió hacerla pública ella misma a cambio de una donación de 18 £ (unos 23 $) para ayudar a la organización en defensa del clima Extinction Rebellion.

Detener los ataques sin cifrado significa impedir que los hackers se hagan con sus datos. Requiere muchas de las mismas tecnologías y comportamientos que necesita para el ransomware que cifra datos, lo que enlaza muy oportunamente con nuestra siguiente sección.

Cómo defenderse del ransomware

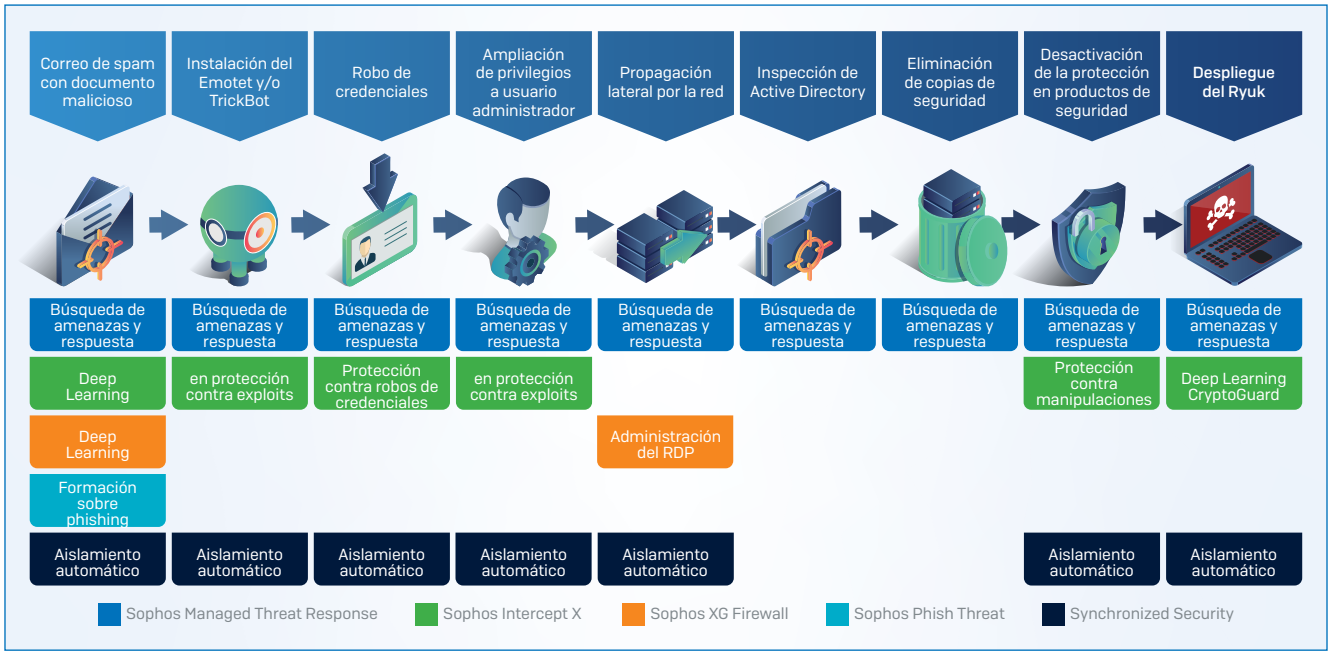
El ransomware ha evolucionado hasta convertirse en una amenaza sumamente compleja, y no va a hacer más que seguir evolucionando. Teniendo esto en mente, ¿cómo puede minimizar su riesgo de sufrir un ataque de ransomware? La respuesta es que debe ponérselo tan difícil como pueda a los implicados en el ransomware para desplegar sus complejos ataques y sacar partido de las oportunidades que presentan los cambios en la tecnología y la sociedad. Para conseguirlo, recomendamos:

- Usar la mejor tecnología de ciberseguridad, centrándose en que actúe en toda la cadena de ataque y no solo en una parte del malware.
- Aplicar las prácticas de seguridad recomendadas en todo momento.
- Informar al personal acerca de los riesgos y los comportamientos requeridos a través de formación periódica de concienciación sobre seguridad.

Una protección contra amenazas que actúe en toda la cadena de ataque

La mejor protección requiere las mejores defensas, tanto para los datos guardados localmente como para los datos guardados en la nube pública.

Si miramos el ejemplo del Ryuk, podemos ver cómo las distintas tecnologías actúan en distintas fases de la cadena de ataque.



Sophos Intercept X
Sophos Intercept X incluye tecnologías de protección avanzadas que detienen el ransomware en sus endpoints y servidores en varias fases de la cadena de ataque.

- La protección contra amenazas con IA detecta las amenazas en los correos electrónicos maliciosos.
- La protección contra exploits detecta y bloquea más de una veintena de técnicas de explotación, incluidas las que se utilizan para distribuir e instalar ransomware y aumentar privilegios.
- La protección contra el robo de credenciales impide que los hackers se hagan con sus valiosas credenciales, bloqueando los accesos no autorizados al sistema y el aumento de privilegios de administrador.
- La protección contra manipulaciones impide que el ransomware desactive la protección de sus endpoints.
- El Deep Learning examina el "ADN" del archivo para determinar si se trata de ransomware y, en caso afirmativo, impide que el ransomware se ejecute.
- La detección de comportamientos de CryptoGuard bloquea el cifrado no autorizado de archivos y los revierte a su estado seguro en segundos.

Sophos XG Firewall
Sophos XG Firewall cuenta con numerosas funciones de protección avanzada para detectar y bloquear los ataques de ransomware e impedir a los hackers moverse lateralmente en su red para aumentar privilegios.

- La protección contra amenazas con IA, incluidos los espacios seguros, detecta el ransomware en la puerta de enlace.
- Las herramientas de administración del RDP le ofrecen una forma simple y elegante de administrar su protocolo de escritorio remoto para impedir que los hackers lo utilicen para moverse lateralmente por su red.
- Los sistemas de prevención de intrusiones (IPS) pueden detectar cualquier intento de explotar vulnerabilidades de la red, como las del RDP o cualquier otra parte de la pila de red.

Seguridad sincronizada
Intercept X y XG Firewall son excelentes por separado, pero juntos son aún mejores con la Seguridad Sincronizada. Si algún evento activa una detección en cualquiera de los dos productos, XG Firewall e Intercept X se ponen a trabajar de forma conjunta para aislar los dispositivos afectados y evitar así que se propague más la amenaza.

Managed Threat Response (MTR)
Muchas empresas no cuentan con la experiencia, los recursos ni el deseo de supervisar su red a todas horas. El servicio Sophos MTR ofrece un equipo dedicado de cazadores de amenazas y expertos en respuesta disponible las 24 horas que busca y procesa continuamente cualquier actividad sospechosa.

Prácticas de seguridad sólidas

Además de contar con tecnologías potentes para frustrar los ataques, también hay varias prácticas recomendadas que debe aplicar para fortalecer su escudo defensivo:

- Utilice la autenticación multifactor (2FA).
- Utilice contraseñas complejas, administradas mediante un gestor de contraseñas.
- Limite los derechos de acceso: dé a las cuentas de usuario y a los administradores solo aquellos derechos de acceso que necesiten y ninguno más.
- Realice copias de seguridad periódicamente y manténgalas fuera de la red y en ubicaciones externas donde los atacantes no puedan encontrarlas: podría ser su última línea de defensa ante una demanda de rescate de seis cifras.
- Aplique los parches con prontitud y frecuencia: ransomware como el WannaCry y el NotPetya dependía de las vulnerabilidades sin corregir para poder propagarse por el mundo.
- Bloquee su RDP: desactive el RDP si no lo necesita y utilice limitación de velocidad, 2FA o una VPN si lo necesita.
- Asegúrese de que la protección contra manipulaciones está activada: el Ryuk y otras variantes de ransomware intentan desactivar la protección de sus endpoints, y la protección contra manipulaciones está diseñada para evitarlo.

Formación continuada del personal

Las personas son siempre el eslabón más débil en la ciberseguridad, y los ciberdelincuentes son expertos en explotar comportamientos humanos normales para su vil beneficio. La mayoría de ataques del Ryuk llegan por correo electrónico con un archivo adjunto malicioso. Si puede evitar que la gente haga clic en el archivo adjunto desde el principio, impedirá que la amenaza penetre en su red. Por lo tanto, le recomendamos que invierta (y que siga invirtiendo) en formar al personal. Para ayudarle con esto, el kit de herramientas antiphishing gratuito de Sophos pone a su disposición una serie de prácticos recursos para formar a su equipo sobre el phishing, entre ellos:

- Póster informativo para su oficina
- Ejemplos de correos electrónicos de phishing
- Los mejores consejos para detectar el phishing
- Presentación de PowerPoint para sesiones de formación interna
- Diagrama de phishing para ayudar a identificar los correos electrónicos de phishing

Descárguelo gratis en www.sophos.com/es-es/phishing.

Conclusión

El ransomware es la ciberamenaza que no desaparece. ¿Por qué? Porque los delincuentes siguen sacando partido de los nuevos avances en la tecnología y la sociedad para pulir y mejorar sus ataques de ransomware. Si tuviéramos que extraer una lección de nuestros 30 años de historia luchando contra el ransomware, sería que el ransomware va a seguir evolucionando.

La mejor defensa contra el ransomware es una combinación de la protección por capas en el endpoint y la puerta de enlace para desmontar la cadena de ataque, la aplicación a conciencia de las prácticas de seguridad recomendadas en todo momento, y la formación continuada de los usuarios.

☑ Una protección contra amenazas que actúe en toda la cadena de ataque

☑ Prácticas de seguridad sólidas

☑ Formación continuada del personal

Lecturas recomendadas

Para acceder a una descripción detallada de los patrones de comportamiento de las diez familias de ransomware más comunes, dañinas y persistentes, lea Cómo ataca el ransomware de Mark Loman, director de ingeniería de Sophos.

Para obtener más información sobre las soluciones de Sophos que le ayudan a luchar contra el ransomware, visite:

- Sophos Intercept X
- Sophos XG Firewall
- Servicio Sophos MTR
- Kit de herramientas antiphishing gratuito

Para mantenerse al día con las noticias más recientes sobre el ransomware, siga **Naked Security**, el servicio de noticias de seguridad de Sophos.

- Boletín diario por correo electrónico. Regístrese en nakedsecurity.sophos.com
- Podcast semanal. Disponible a través de su fuente de podcasts habitual.
- Publicaciones periódicas en redes sociales. Síganos en Twitter, Facebook, Instagram y YouTube

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

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

© Copyright 2019. Sophos Ltd. Todos los derechos reservados.
Constituida en Inglaterra y Gales N.º 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, Reino Unido
Sophos es la marca registrada de Sophos Ltd. Todos los demás productos y empresas mencionados son marcas comerciales o registradas de sus respectivos propietarios.

05-12-19 WP-ES (DD)

SOPHOS