SOPHOS
Cybersecurity evolved.

Prácticas recomendadas con firewalls para bloquear el ransomware

Monográficos de Sophos. Junio 2021

Prácticas recomendadas con firewalls para bloquear el ransomware

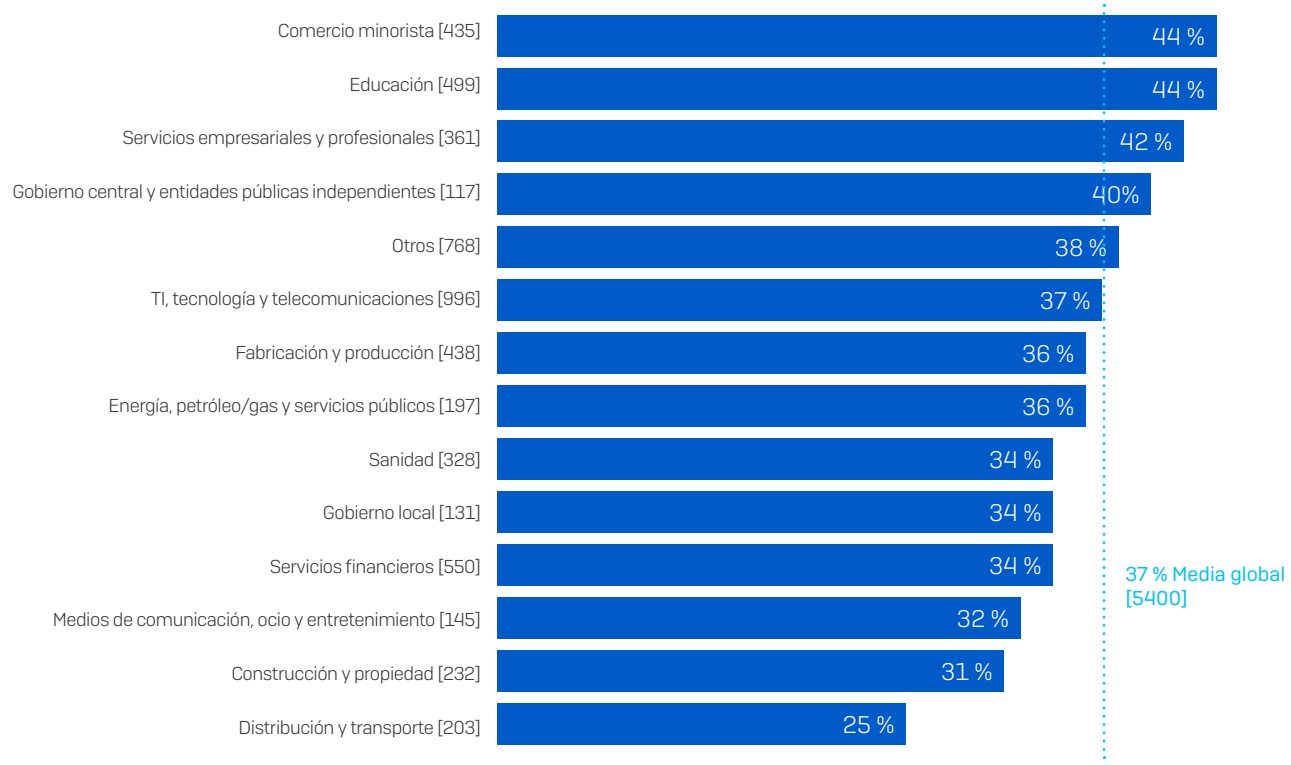
El ransomware continúa asediando a las organizaciones: más de un tercio de las empresas encuestadas en 30 países distintos revelan que se han visto afectadas por el ransomware en el último año*. Estos ataques son cada vez más complejos, y los adversarios se están volviendo más eficientes a la hora de explotar vulnerabilidades de la red y del sistema, lo que conlleva importantes costes de limpieza para las organizaciones: una desorbitada media global de 1,85 millones USD, más del doble del coste registrado el año anterior.

Los firewalls modernos son sumamente efectivos a la hora de proteger contra este tipo de ataques, pero es necesario darles la oportunidad de cumplir su función. En este monográfico explicamos cómo funcionan estos ataques, cómo pueden detenerse y las prácticas recomendadas para configurar los firewalls y las redes a fin de contar con la mejor protección posible.

Quiénes son el objetivo de los hackers

¿Quiénes son el objetivo de los hackers? La respuesta corta es todo el mundo. En una encuesta reciente a 5400 organizaciones medianas de 30 países, el 37 % de los encuestados afirmaron que se habían visto afectados por el ransomware en el último año. No hay ningún país, sector ni segmento vertical que esté a salvo.

Porcentaje de empresas afectadas por el ransomware en el último año



En el último año, ¿se ha visto afectada por el ransomware su empresa? Sí [números base en el gráfico], omitiendo algunas opciones de respuesta, divididas por sector

Si busca "ataque de ransomware" en las noticias, encontrará varios nuevos ataques que logran su propósito todas las semanas. Los efectos son devastadores: ingentes sumas de rescate, prolongados tiempos de inactividad e interrupciones del negocio, perjuicios para la reputación, pérdidas de datos y, en un número de casos cada vez mayor, datos confidenciales de empresas subastados por los atacantes.

*El estado del ransomware 2021, una encuesta independiente a 5400 directores de TI de 30 países encargada por Sophos y realizada por Vanson Bourne.

Cómo penetran en la red los ataques de ransomware

Los responsables del ransomware utilizan una amplia gama de tácticas, técnicas y procedimientos (TTP) para penetrar en las redes de sus víctimas. SophosLabs y el equipo de Sophos Managed Threat Response han observado un aumento de los ataques en que los adversarios intentan varios enfoques hasta que dan con una brecha en las defensas de la organización.

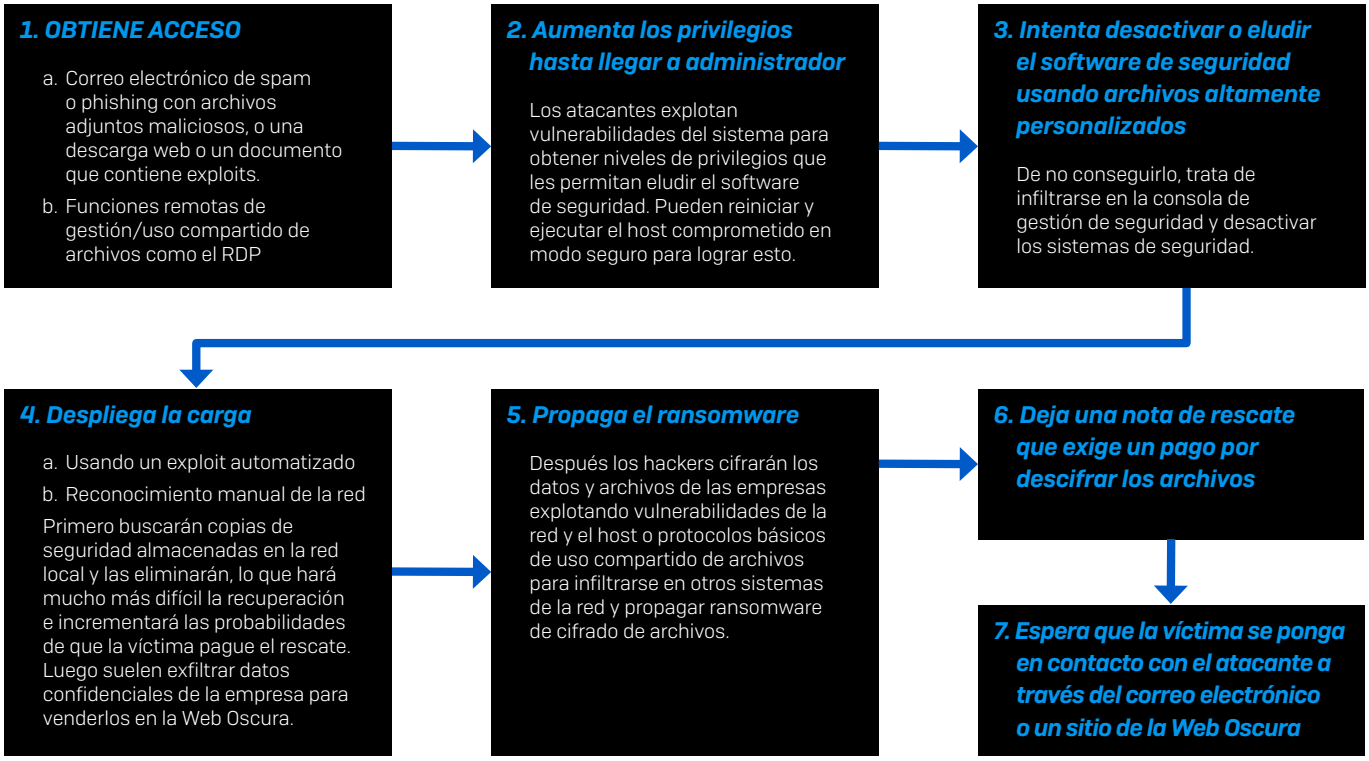
Cómo entró el ransomware en la empresa	% de incidentes
A través de una descarga de archivos/correo electrónico con un enlace malicioso	29%
A través de un ataque remoto al servidor	21%
A través de correo electrónico con un adjunto malicioso	16%
Instancias en la nube pública mal configuradas	9%
A través de nuestro protocolo de escritorio remoto (RDP)	9%
A través de un proveedor que trabaja en nuestra empresa	9%
A través de un dispositivo USB/de medios extraíbles	7%
Total	100%

¿Cómo entró en su empresa el ataque de ransomware? Pregunta realizada a los encuestados cuya empresa se ha visto afectada por el ransomware en el último año. Base: 2538 encuestados. El estado del ransomware 2020, Sophos

Como puede ver por las respuestas a la encuesta de la tabla anterior, el principal punto de entrada para el ransomware son los archivos descargados o enviados a los usuarios en ataques de spam o phishing. No deje la seguridad en manos de sus usuarios. Para estos tipos de ataque, lo mejor es blindar su empresa con una protección sólida para firewalls.

Cómo funciona un ataque de ransomware

El ataque de ransomware dirigido típico funciona del siguiente modo:



RDP - ¿Protocolo de escritorio remoto o protocolo de despliegue de ransomware?

El Protocolo de escritorio remoto (RDP) y otras herramientas de uso compartido del escritorio como Computación virtual en red (VNC) son funciones inocuas y sumamente útiles de la mayoría de sistemas operativos que permiten al personal acceder y gestionar sistemas de forma remota. Desafortunadamente, sin las medidas de protección adecuadas, también sirven como puertas de entrada ideales para los atacantes, por lo que suelen ser explotadas por el ransomware dirigido.

Si no protege el protocolo RDP y otros protocolos de gestión remota similares con una red privada virtual (VPN) o por lo menos limita las direcciones IP que pueden conectarse mediante herramientas remotas, puede estar dejando la puerta abierta de par en par a los atacantes. Estos utilizan a menudo herramientas de hacking por fuerza bruta que prueban cientos de miles de combinaciones de nombres de usuario y contraseñas hasta que dan con la correcta.

Cómo protegerse del ransomware

Para proteger su empresa del ransomware correctamente, hay tres principales iniciativas que debe tomar.

1. Actualice su seguridad TI

Su solución de seguridad para firewalls y endpoints puede impedir ya de entrada que los ataques accedan a la red, de modo que, si un ataque llega a penetrar en su red de alguna manera, impedirá que se propague e infecte otros sistemas. Pero no todas las soluciones de seguridad para firewalls y endpoints pueden hacer esto de forma efectiva, por lo que debe asegurarse de que cuenta con un sistema de seguridad TI que sí lo consiga.

Asegúrese de disponer de:

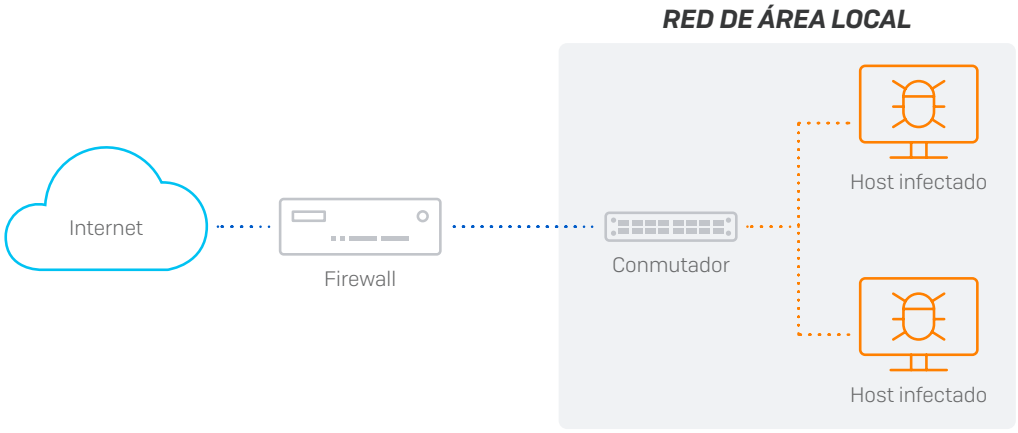
- Espacios seguros asequibles para analizar el comportamiento de los archivos cuando se ejecutan antes de que lleguen a su red
- La tecnología de Machine Learning más reciente para identificar las nuevas variantes de día cero en cualquier archivo que atraviese su firewall
- IPS de firewall con actualización de firmas en tiempo real para bloquear exploits de red
- VPN de acceso remoto sencilla y gratuita para permitir la administración de su red de forma remota sin comprometer la seguridad
- Protección para endpoints con funciones antiransomware

2. Bloquee el acceso y la administración remotos

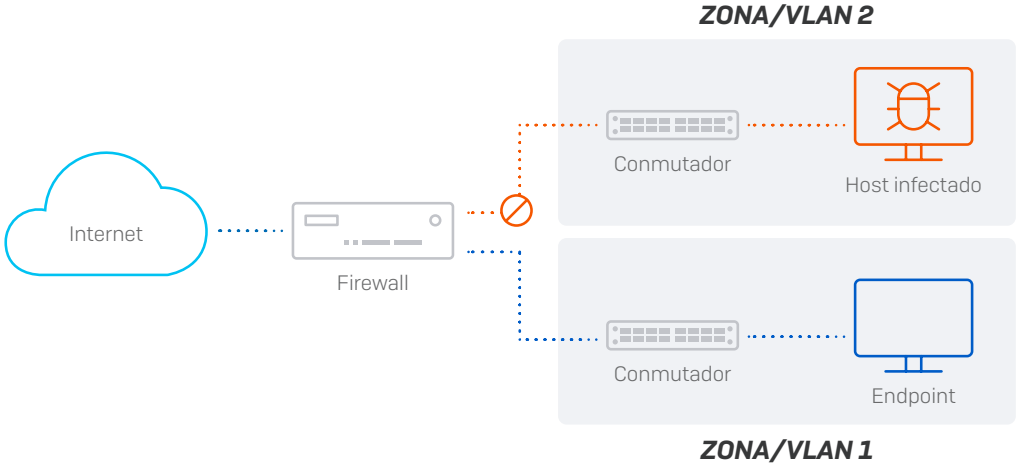
En lo que a redes se refiere, cualquier apertura al mundo exterior es una posible vulnerabilidad esperando a ser explotada por un ataque de ransomware. Bloquear el acceso al Protocolo de escritorio remoto, los puertos abiertos y otros protocolos de administración de su empresa es una de las medidas más efectivas que puede tomar para protegerse contra los ataques de ransomware dirigido. Puede hacerlo de muchas formas. Un método popular es obligar a todos los usuarios a utilizar una VPN para poder acceder a recursos como el RDP y restringir el acceso a la VPN a direcciones IP conocidas. Asimismo, debe proteger y endurecer sus servidores, utilizar contraseñas complejas que se cambien con frecuencia y servirse de la autenticación multifactor.

3. Segmente su red

Desafortunadamente, muchas empresas funcionan con una topología de red plana: todos sus endpoints se conectan a una matriz de conmutación común. Esta topología compromete la protección, ya que permite que los ataques se desplacen o propaguen lateralmente con facilidad dentro de la red local, puesto que el firewall no tiene visibilidad ni control sobre el tráfico que fluye a través del conmutador.



La práctica recomendada es segmentar la LAN en subredes más pequeñas utilizando zonas o redes VLAN y conectarlas después a través del firewall, a fin de permitir la aplicación de una protección IPS y antimalware entre los segmentos. Esto puede identificar y bloquear de forma efectiva las amenazas que intenten propagarse lateralmente en la red.



Se utilizan zonas o redes VLAN en función de la estrategia y el alcance de la segmentación de red, pero ambas ofrecen unas funciones de seguridad similares y la opción de aplicar una seguridad y un control adecuados sobre el movimiento de tráfico entre segmentos. Las zonas son ideales para estrategias de segmentación más pequeñas o redes con conmutadores no administrados. Las VLAN son el método preferido para segmentar redes internas en la mayoría de casos y ofrecen lo último en flexibilidad y escalabilidad. Si embargo, requieren el uso (y la configuración) de conmutadores de capa 3 administrados.

Si bien segmentar la red es una práctica recomendada, no hay una forma mejor que otra de hacerlo. Puede segmentar la red por tipo de usuario (interno, contratista, invitado), por departamento (ventas, marketing, ingeniería), por tipo de rol, dispositivo o servicio (VoIP, Wi-Fi, IoT, ordenadores, servidores) o cualquier combinación que resulte adecuada para la estructura de su red. Pero, por lo general, es conveniente segmentar las partes menos fiables y más vulnerables de la red del resto. También conviene dividir grandes redes en segmentos más pequeños, todo ello con el objetivo de reducir el riesgo de penetración y propagación de amenazas.

Prácticas recomendadas para la configuración de firewalls y redes

- **Asegúrese de que cuenta con la mejor protección** con un firewall next-gen de alto rendimiento moderno con IPS, inspección TLS, espacios seguros de día cero y protección antiransomware con Machine Learning.
- **Bloquee el RDP y otros servicios** con el firewall. Su firewall debe poder restringir el acceso a los usuarios que utilicen una VPN e incluir en una lista blanca las direcciones IP aprobadas.
- **Reduzca al área de la superficie de ataque** lo máximo posible revisando exhaustivamente todas las reglas de enrutamiento de puertos a fin de eliminar cualquier puerto abierto no esencial. Un puerto abierto representa una posible vía de entrada en su red. Siempre que sea posible, utilice una conexión VPN para acceder a los recursos de la red interna desde el exterior en lugar del enrutamiento de puertos.
- **Asegúrese de proteger debidamente cualquier puerto abierto** aplicando una protección IPS adecuada a las reglas que gestionan el tráfico.
- **Habilite la inspección TLS** con soporte para los estándares TLS 1.3 de tráfico web más recientes a fin de evitar que las amenazas entren en su red a través de flujos de tráfico no cifrado.
- **Minimice el riesgo de propagación lateral** dentro de la red segmentando las redes LAN en zonas aisladas más pequeñas o redes VLAN protegidas y conectadas por el firewall. Asegúrese de aplicar políticas IPS adecuadas a las reglas que gestionan el tráfico que atraviesa estos segmentos de la LAN para evitar que los exploits, gusanos y bots se propaguen entre ellos.
- **Aísle los sistemas infectados automáticamente**. Cuando se produzca una infección, es importante que su solución de seguridad TI pueda identificar rápidamente los sistemas comprometidos y aislarlos automáticamente hasta que se puedan limpiar (mediante la Seguridad Sincronizada de Sophos, por ejemplo).
- **Utilice contraseñas seguras y la autenticación multifactor** para sus herramientas de uso compartido de archivos y gestión remota de modo que las herramientas de hacking por fuerza bruta no puedan comprometerlas fácilmente.

Cómo puede ayudar Sophos

Sophos ofrece la solución de seguridad TI definitiva para defenderse del ransomware más reciente. No solo obtiene la mejor protección en cada punto, sino que además disfruta de años de integración entre el firewall y el endpoint. Esto ofrece enormes ventajas en términos de visibilidad del estado de seguridad de la red, así como la capacidad de responder automáticamente a incidentes de seguridad.

Con nuestro galardonado Sophos Firewall, la primerísima prioridad es impedir que los ataques penetren en la red. Sin embargo, en el caso de que el ransomware llegue a entrar en su red, cuenta con una doble protección. Sophos Firewall puede detener automáticamente el ransomware al instante gracias a la integración con Sophos Intercept X, nuestra plataforma de protección para endpoints líder en el sector. Es como poner su red en piloto automático: un enorme multiplicador de fuerzas para su equipo.

Esta tecnología es lo que llamamos Seguridad Sincronizada de Sophos. La Seguridad Sincronizada fusiona nuestras funciones de protección de redes y endpoints en un potente sistema de ciberseguridad profundamente integrado. Y lo mejor de todo es que es sumamente fácil de administrar, junto con todos sus demás productos de Sophos, desde nuestra consola de administración en la nube Sophos Central.

Tecnologías clave de Sophos Firewall y Sophos diseñadas específicamente para combatir el ransomware

- Los análisis de Machine Learning y de espacios seguros en la nube de Sophos Firewall de los archivos que entran en la red ayudan a impedir que incluso variantes de ransomware, exploits y malware desconocidas se propaguen a través de spam, phishing o descargas web.
- El sistema de prevención de intrusiones de Sophos Firewall atrapa los exploits y los ataques de red más recientes de los que puedan servirse los hackers para encontrar vulnerabilidades en sus defensas.
- Las extensas a la vez que simples opciones de VPN de Sophos Firewall le permiten cerrar todos los agujeros de su red y dejar de depender de conexiones RDP vulnerables, al tiempo que puede seguir ofreciendo un acceso total a su red a los usuarios autorizados.
- Sophos Firewall ofrece inspección TLS 1.3 de Xstream de alto rendimiento con controles de políticas flexibles para que pueda encontrar el equilibrio perfecto entre privacidad, protección y rendimiento, además de impedir que las amenazas entren en su red sin ser detectadas por medio de flujos de tráfico cifrado.
- La Seguridad Sincronizada de Sophos integra Sophos Firewall con nuestra protección para endpoints Intercept X a fin de responder automáticamente a los ataques de ransomware detectando las primeras señales de peligro, deteniéndolas y notificándole.
- La protección para endpoints Sophos Intercept X con CryptoGuard puede detectar un ataque de ransomware en curso, detenerlo y revertirlo automáticamente. Sophos Firewall incluye la tecnología CryptoGuard en el entorno de espacio seguro para detectar el ransomware en plena actividad antes de que se introduzca en su red.

Conclusión

A pesar de ser una ciberamenaza perenne, el ransomware no hará más que seguir evolucionando. Si bien es posible que nunca podamos erradicar completamente el ransomware, si seguimos las prácticas recomendadas para firewalls descritas en este documento, su empresa tendrá más probabilidades de mantenerse protegida contra el ransomware más reciente y otras amenazas maliciosas.

En resumen:

- Asegúrese de que cuenta con la mejor protección.
- Bloquee el RDP y otros servicios con su firewall.
- Reduzca el área de la superficie de ataque tanto como sea posible.
- Proteja cualquier puerto abierto aplicando una protección IPS adecuada.
- Aplique análisis de espacio seguro y Machine Learning a descargas y archivos adjuntos.
- Minimice el riesgo de propagación lateral en la red segmentando las LAN.
- Aísle los sistemas infectados automáticamente.
- Utilice contraseñas seguras y la autenticación multifactor para sus herramientas de uso compartido de archivos y gestión remota.

Pruebe Sophos Firewall gratis en

www.sophos.com/firewall

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

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

15-06-21 ES (DD)