SONICWALL®

8 FORMAS DE PROTEGER SU RED CONTRA EL RANSOMWARE

Medidas para prevenir los ataques de ransomware y ahorrar dinero

A veces, lo antiguo vuelve a ponerse de moda. Eso es precisamente lo que está ocurriendo con los ataques de ransomware. Lanzados por primera vez en 1989, los ataques de malware infectan un sistema y "dejan fuera" al usuario, que no puede acceder al dispositivo ni a los archivos en él almacenados. Solo si la víctima accede a pagar un rescate, normalmente en forma de bitcoins, puede desbloquearse el sistema y el usuario puede volver a acceder a él.

Este libro virtual proporciona ocho maneras de proteger su red contra los ataques de ransomware y evitar así que su dinero acabe en manos de cibercriminales.

Si bien los importes de los rescates varían, suelen oscilar entre $200 y $400.[1]

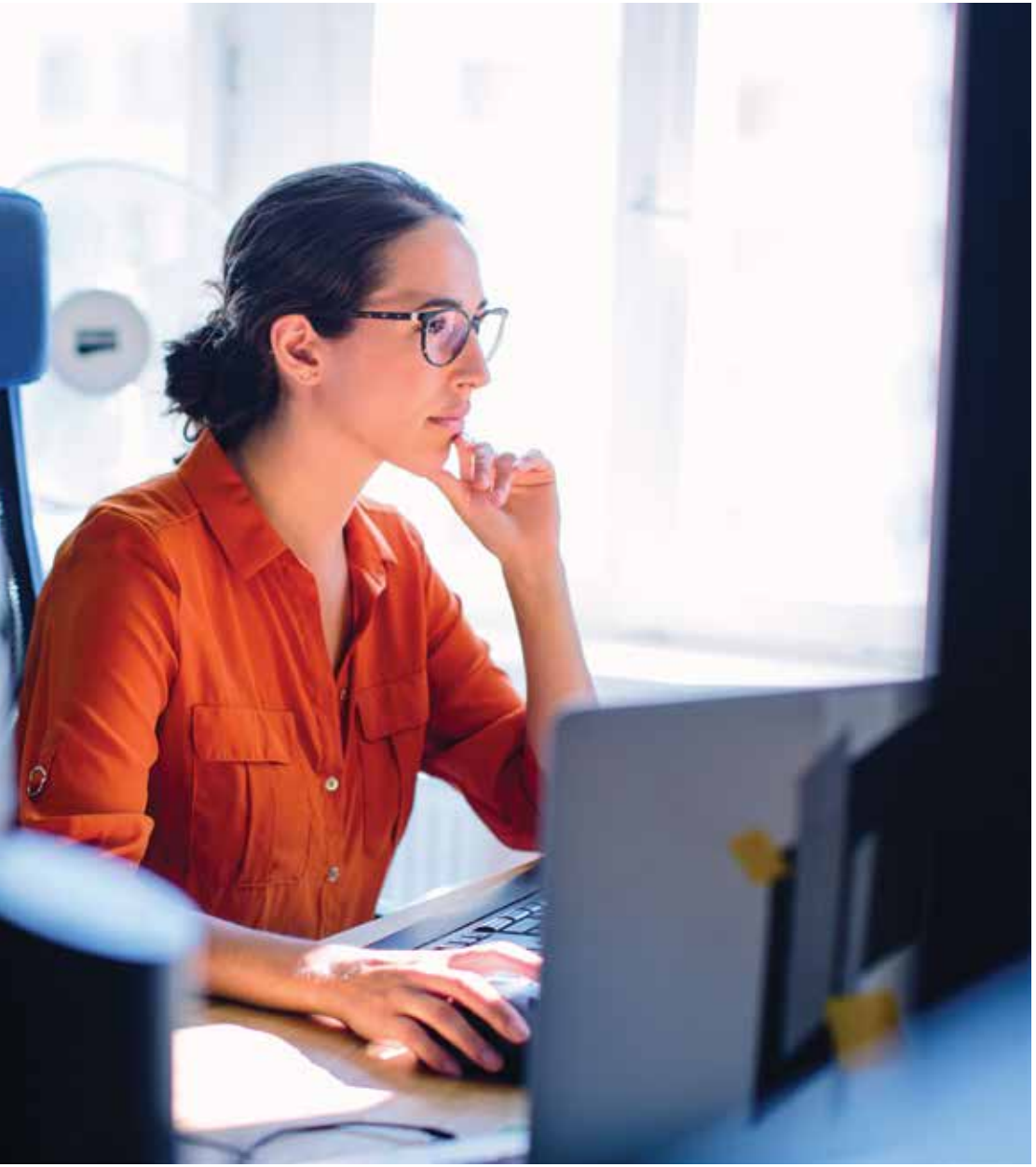
1. Eduque a sus empleados

La educación y la concienciación de los usuarios son fundamentales a la hora de combatir el ransomware. Trate los e-mails sospechosos con precaución Fíjese en el nombre del dominio desde el que se ha enviado el e-mail. Mire si hay faltas de ortografía, revise la definición y la legitimidad de la solicitud. Pase el cursor por encima de los enlaces para ver a dónde conducen.

2. Utilice un enfoque de seguridad de red multicapa

La protección contra el ransomware y otras formas de malware no comienza ni acaba en la pasarela. La ampliación de la seguridad mediante el uso de antivirus, antispyware, prevención de intrusiones y otras tecnologías en dispositivos situados en el perímetro de la red resulta crucial. Adopte un enfoque multicapa para detener el ransomware evitando la existencia de un punto único de fallo en su arquitectura de seguridad.

1 US Computer Emergency Readiness Team Alert (TA16-091A)



3. Realice backups de sus archivos regularmente

Otra forma de evitar el tener que pagar un rescate es utilizar una estrategia robusta de backup y recuperación. Dependiendo de la velocidad con que se detecte el ataque, cuánto se haya propagado y cuál sea el nivel de pérdida de datos aceptable, la recuperación a partir de un backup puede ser una buena opción. Sin embargo, ello requiere una estrategia de backup más inteligente, en consonancia con la importancia de sus datos y con las necesidades de su negocio de objetivos de punto de recuperación (RPO) y objetivos de tiempo de recuperación (RTO).

4. Asegúrese de que sus puntos terminales están protegidos

Puesto que la mayoría de los usuarios interactúan principalmente con dispositivos personales y corporativos, los puntos terminales no gestionados o que no cuentan con una protección antimalware adecuada, están especialmente expuestos. La mayoría de las soluciones antivirus están basadas en definiciones, y pierden su eficacia si no se actualizan regularmente. Las variantes de ransomware más recientes tienen un hash único y por tanto no pueden ser detectadas con técnicas basadas en definiciones. Además, muchos usuarios desactivan las funciones de escaneo antivirus para evitar que ralenticen su sistema.

Implementar una estrategia de seguridad multicapa para aumentar la protección de la red.

5. Aplique parches a sus sistemas y aplicaciones

Muchos ataques se basan en vulnerablidades conocidas de navegadores como Internet Explorer, o de aplicaciones y plug-ins comunes. Por ello, la aplicación rápida y fiable de actualizaciones y parches resulta vital. La elección de una solución que sea capaz de ofrecer parches y actualizaciones de versiones de forma automatizada en un entorno heterogéneo de dispositivos, sistemas operativos y aplicaciones, ayudará en gran medida a combatir una variedad de amenazas cibernéticas, incluido el ransomware.

6. Segmente su red para evitar la propagación

En la mayoría de los casos, el ransomware intentará propagarse desde el punto terminal hasta el servidor/almacén donde se encuentran todos los datos y las aplicaciones de misión crítica. Segmentar la red y mantener las aplicaciones y los dispositivos críticos aislados en una red separada o en una LAN virtual puede limitar la propagación.

7. Ponga en cuarentena y analice los archivos sospechosos

Las tecnologías como el sandboxing permiten poner archivos sospechosos en cuarentena para su análisis antes de que puedan acceder a la red. Los archivos se retienen en la pasarela hasta que se emita un veredicto. Si se detecta un archivo malicioso, puede evitar posibles ataques derivados implementando medidas de protección, como políticas que bloqueen las direcciones de IP o dominios asociados, o bien aplicando definiciones en los dispositivos de seguridad de toda la red.

Segmente su LAN inalámbrica para separar a los usuarios internos de los invitados con el fin de proporcionar un nivel de seguridad adicional.

8. Proteja sus dispositivos Android

Los dispositivos basados en el sistema operativo Google Android se han convertido en los principales blancos de los ataques de ransomware. Tome las siguientes medidas para proteger su teléfono inteligente Android:

- No rootee el dispositivo; los archivos del sistema podrían sufrir modificaciones
- Instale siempre aplicaciones de Google Play store; las aplicaciones de páginas/tiendas desconocidas pueden ser falsas/maliciosas
- Inhabilitar la instalación de aplicaciones de fuentes desconocidas
- Permita a Google escanear el dispositivo en busca de amenazas
- Tenga cuidado al abrir enlaces desconocidos recibidos vía SMS o e-mail
- Instalar aplicaciones de seguridad de terceros que escaneen el dispositivo regularmente en busca de contenido malicioso
- Vigile qué aplicaciones se registran como Administradores de dispositivos
- Cree una lista negra de aplicaciones no autorizadas para dispositivos corporativos

Los ataques de malware contra el ecosistema Android continuaron en aumento en 2015, poniendo en riesgo casi el 85% de los teléfonos inteligentes.

Conclusión

Los ataques de ransomware cada vez son más populares entre los cibercriminales. Por ello, es importante que se asegure de que su red está protegida. SonicWall puede mejorar la protección en toda su organización gracias a la inspección de todos los paquetes y al control de todas las identidades. De este modo, no solo velamos por la seguridad de sus datos allá donde vayan, sino que además utilizamos inteligencia compartida para protegerle contra una gran variedad de amenazas, entre las que se incluye el ransomware.

Visite la página Web de los productos de Seguridad de red de SonicWall.

Acerca de SonicWall

SonicWall lleva más de 25 años combatiendo la industria del crimen cibernético, defendiendo a las empresas pequeñas, medianas y grandes de todo el mundo. Nuestra combinación de productos y partners nos ha permitido crear una solución de defensa cibernética en tiempo real adaptada a las necesidades específicas de más de 500.000 negocios globales en más de 150 países, para que usted pueda centrarse por completo en su negocio sin tener que preocuparse por las amenazas.

Si tiene alguna duda sobre el posible uso de este material, póngase en contacto con nosotros:

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

Para más información, consulte nuestra página Web.
www.sonicwall.com

Ebook-8waysRansomware-EU-IMAG-29271-D1

SONICWALL®