SONICWALL®

CÓMO EL RANSOMWARE PUEDE SECUESTRAR SU NEGOCIO Y UTILIZARLO COMO REHÉN

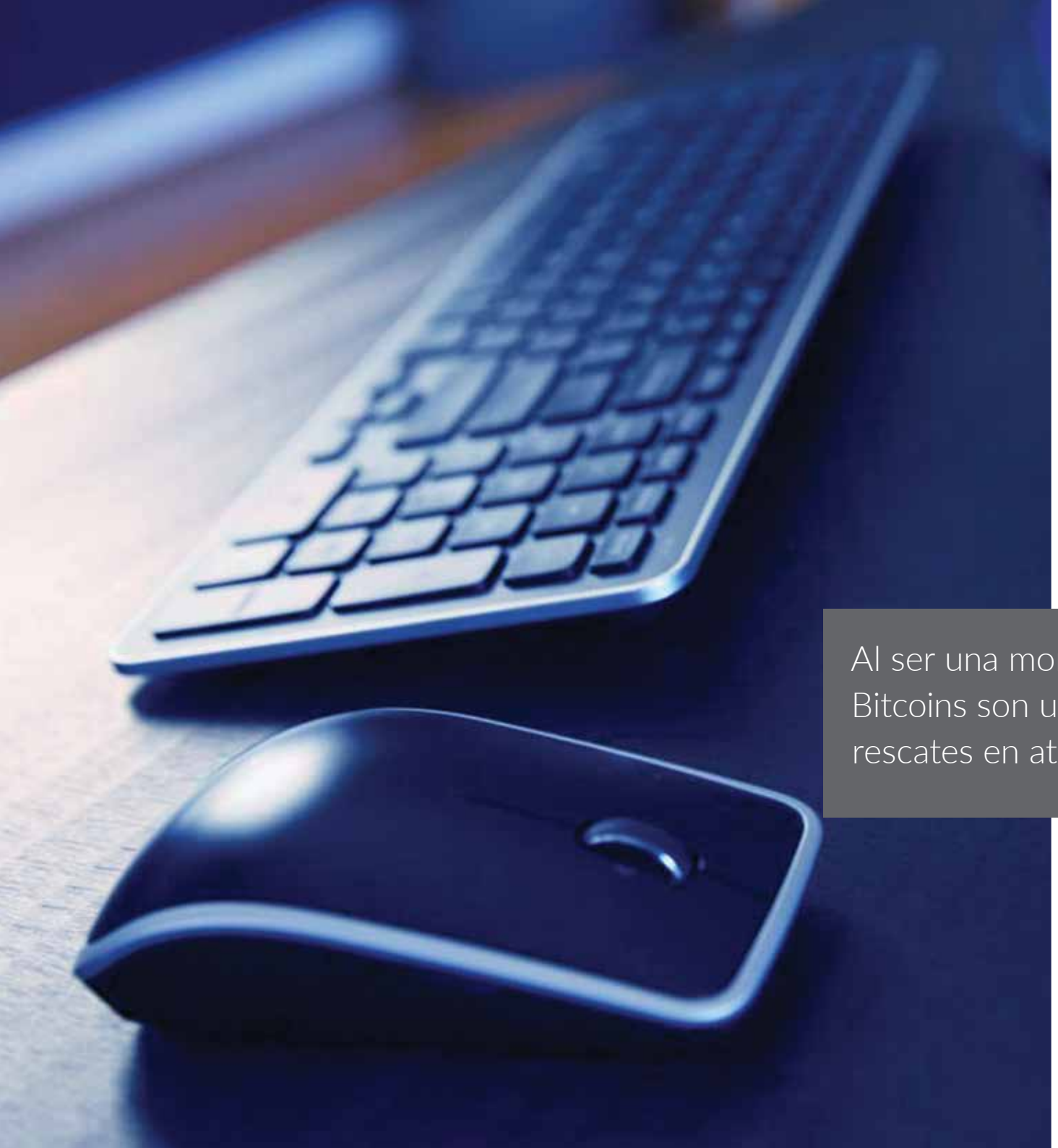
Entienda los ataques de ransomware y cómo se perpetran

Introducción

El ransomware es una forma de malware que deniega el acceso a los datos o sistemas hasta que la víctima pague al cibercriminal un rescate para que retire la restricción. Aunque existe desde hace muchos años, recientemente ha ganado mucho en popularidad y en rentabilidad. CryptoLocker, CryptoWall y RSA4096 son ejemplos de ataques de ransomware conocidos.

Según el FBI, se han pagado más de 209 millones de dólares en rescates solo en los tres primeros meses de 2016[1] en Estados Unidos, en comparación con los 25 millones del año anterior completo.

1 http://sd18.senate.ca.gov/news/4122016-bill-outlawing-ransomware-passes-senate-committee



Cómo funciona el ransomware

El ransomware puede acceder a un sistema a través de muchas vías, haciendo que la víctima descargue e instale una aplicación maliciosa. Una vez en el dispositivo, la aplicación se propaga por todo el sistema y cifra los archivos del disco duro, o simplemente bloquea el sistema. En algunos casos, puede bloquear el acceso al sistema y mostrar imágenes o un mensaje en la pantalla del dispositivo con la intención de forzar al usuario a que pague un rescate al operador del malware a cambio de la clave de cifrado que le permita desbloquear los archivos o el sistema.

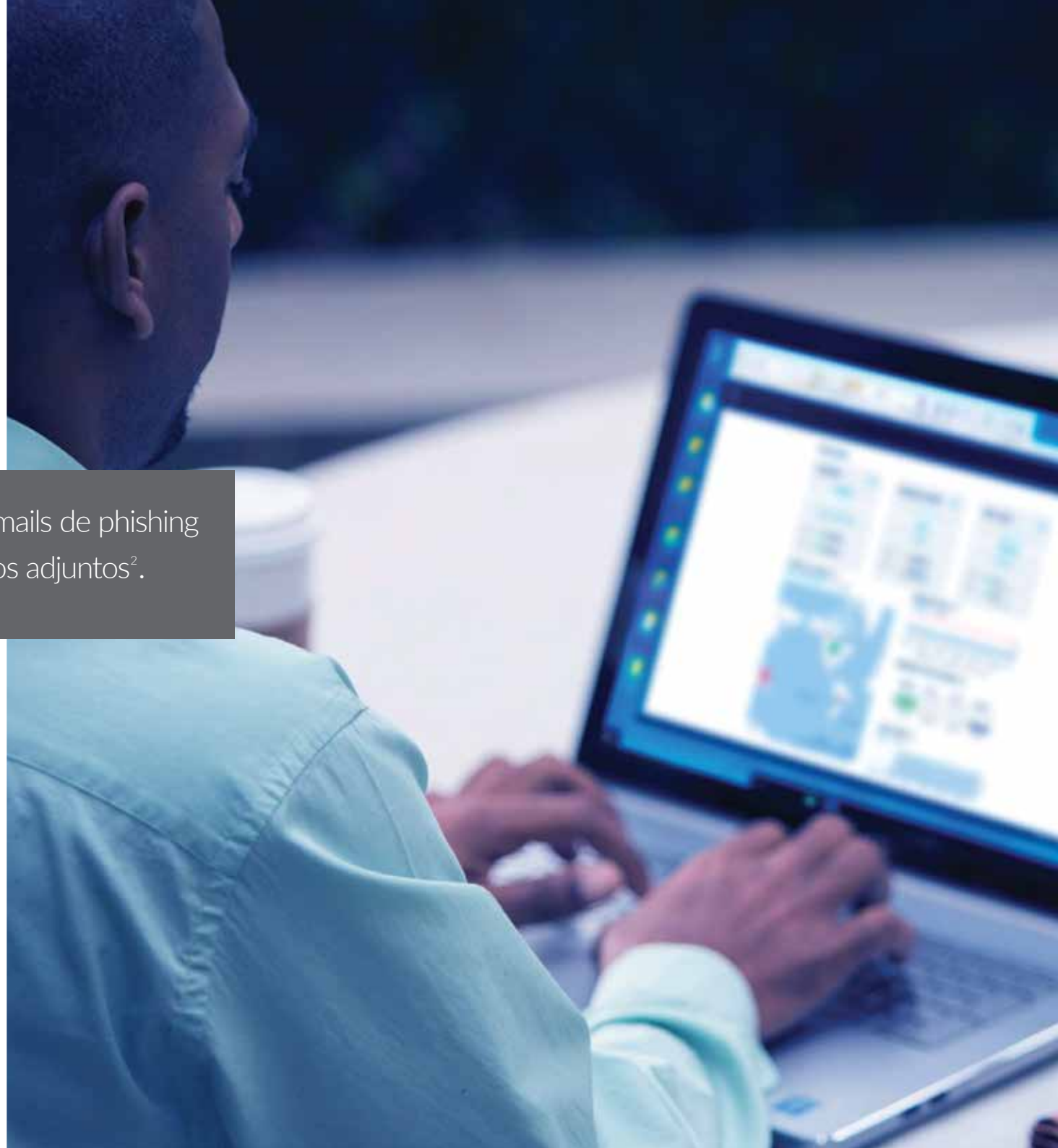
Al ser una moneda digital difícil de rastrear, los Bitcoins son una popular forma de pago de rescates en ataques de ransomware.

SONICWALL®

E-mails de phishing

Uno de los métodos de distribución de ransomware más comunes son los e-mails de phishing. Su objetivo es hacer que los destinatarios abran un e-mail y hagan clic en un enlace a una página Web. Es posible que la página les pida información sensible o que contenga malware, como ransomware, que se descargue en el sistema de la víctima.

El 23% de los destinatarios abren los e-mails de phishing y el 11% incluso hacen clic en los archivos adjuntos[2].

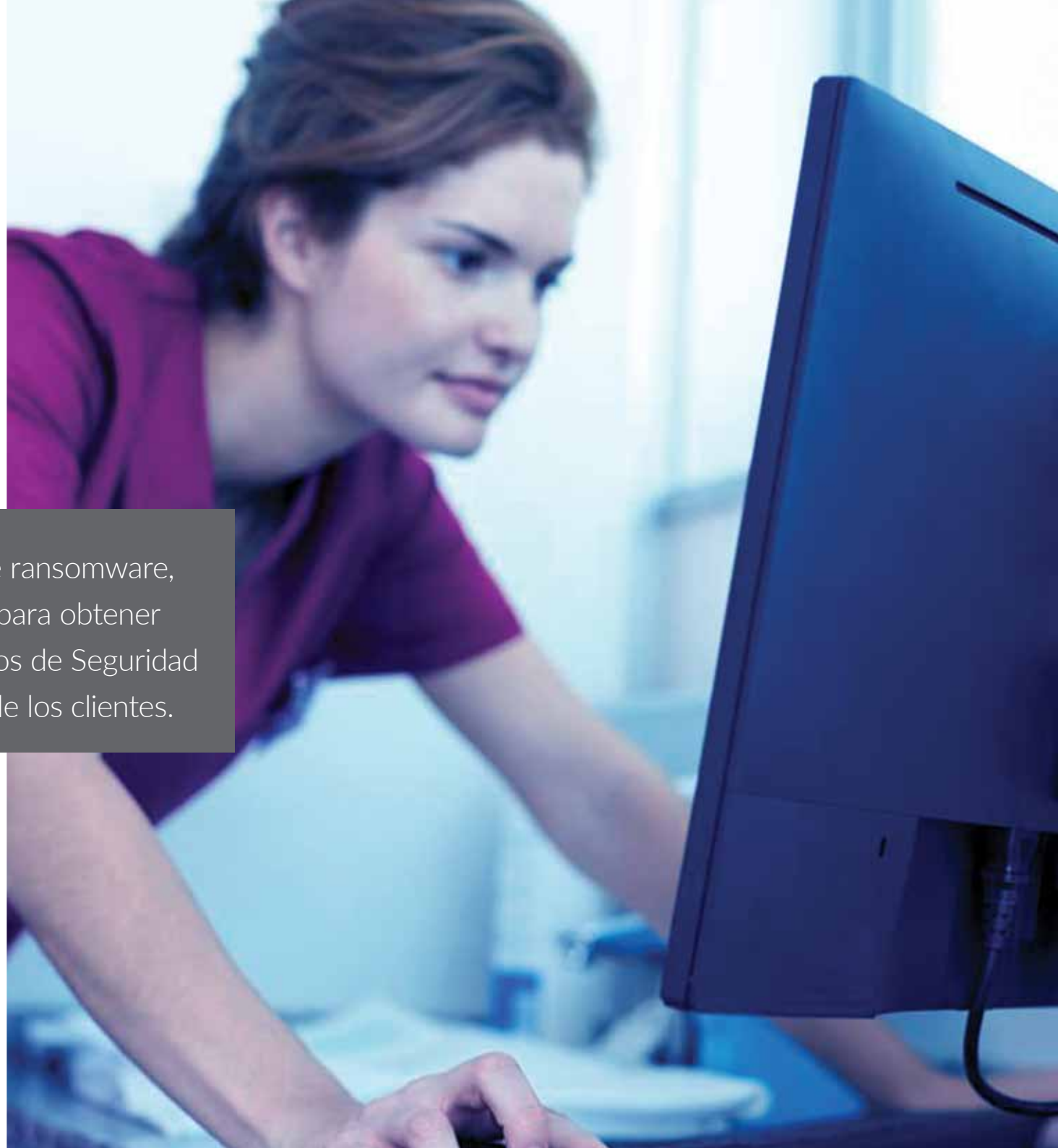


2 Informe de investigación sobre filtración de datos de Verizon

Anuncios maliciosos

Otra forma frecuente de distribuir ransomware es el "malvertising", o la publicidad maliciosa, que utiliza anuncios online para propagar el ataque. El perpetrador del ataque se infiltra en las redes de publicidad, en ocasiones fingiendo ser un anunciante o una agencia, e inserta anuncios contaminados con malware en páginas Web legítimas. Los visitantes desprevenidos ni siquiera tienen que hacer clic en el anuncio para que su sistema se infecte.

Además del lanzamiento de ataques de ransomware, se pueden utilizar anuncios maliciosos para obtener números de tarjetas de crédito, números de Seguridad Social y otra información confidencial de los clientes.

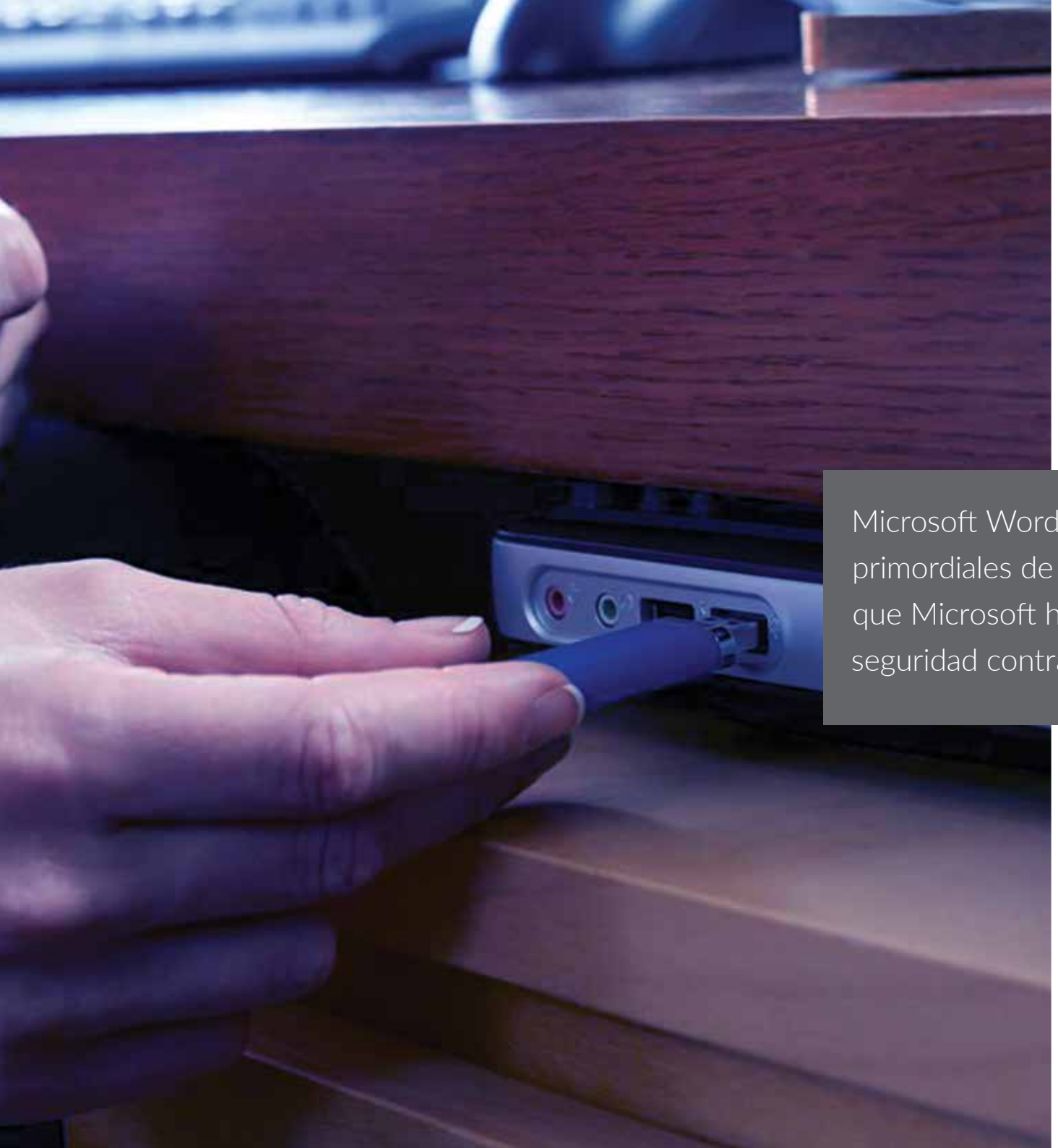


Explotación de sistemas y aplicaciones desprovistos de parches de seguridad

Muchos ataques se basan en vulnerabilidades conocidas de los sistemas operativos, los navegadores y las aplicaciones comunes. Los cibercriminales pueden explotar estas vulnerabilidades para perpetrar sus ataques de ransomware contra sistemas que no cuenten con los más recientes parches de software.

Los sistemas operativos, navegadores y aplicaciones que no cuenten con parches de seguridad pueden contener vulnerablidades que los cibercriminales pueden explotar para perpetrar ataques de ransomware.

SONICWALL®



Dispositivos externos

Los dispositivos externos, como las unidades USB, se utilizan para almacenar y transferir archivos, lo cual los convierte en objetivos interesantes para propagar el ransomware en múltiples sistemas. Algunos de estos archivos contienen una prestación avanzada conocida como macros, que puede ser utilizada por los hackers para ejecutar el ransomware al abrirse el archivo.

Microsoft Word, Excel y PowerPoint son objetivos primordiales de este tipo de ataques, a pesar de que Microsoft ha tomado medidas para mejorar la seguridad contra esta amenaza en Office 2016.

SONICWALL®

Por qué los métodos tradicionales no son capaces de prevenir los ataques de ransomware

Muchos de los controles de seguridad tradicionales a menudo no detectan el ransomware, ya que únicamente buscan comportamientos poco habituales e indicadores estándar de que el sistema ha sido comprometido. Una vez que se ha instalado en el sistema, el ransomware se comporta como una aplicación de seguridad, capaz de denegar el acceso a otros sistemas/programas. Normalmente no afecta a los archivos ni a los sistemas, sino que se limita a restringir el acceso a la interfaz.

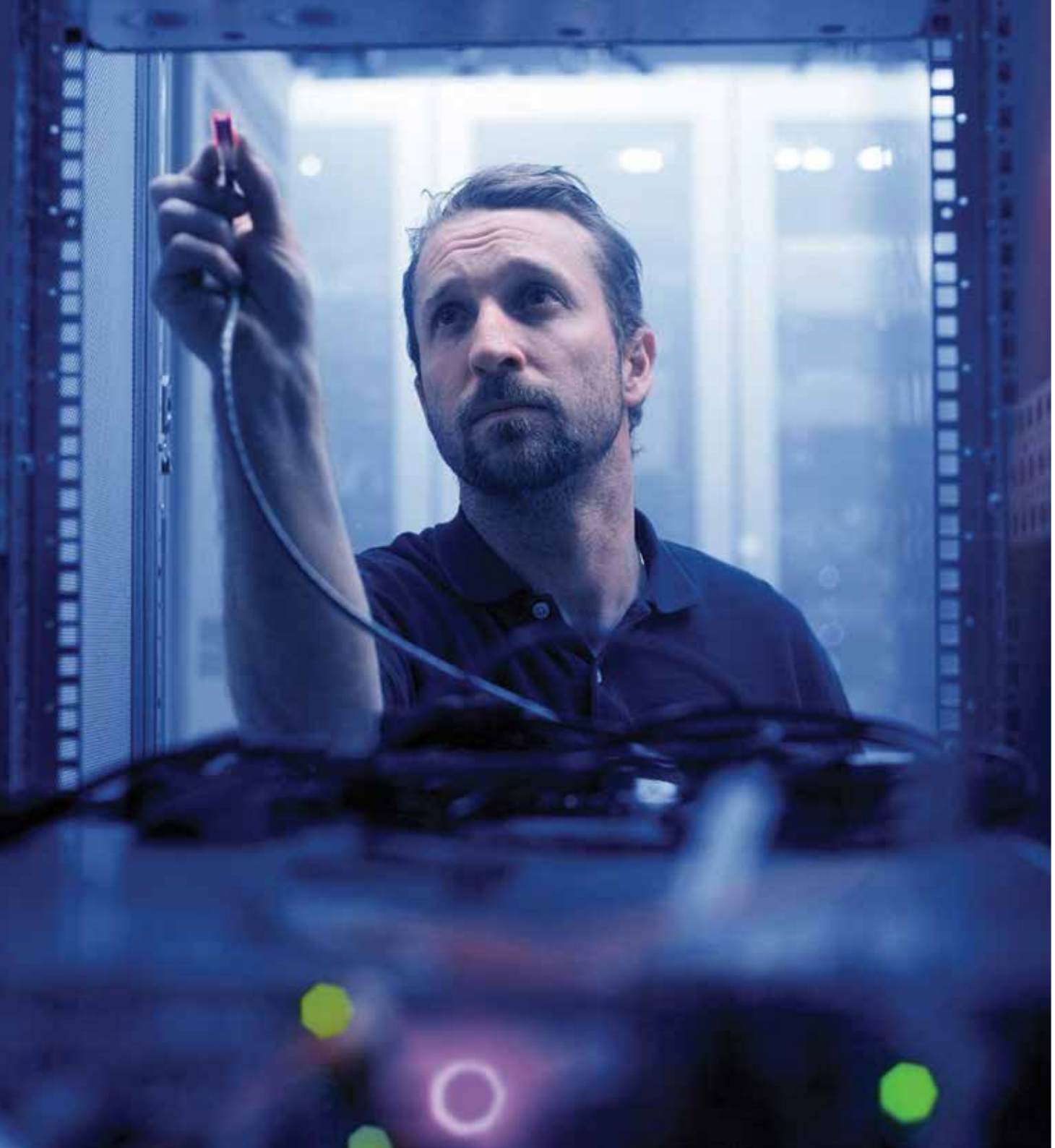
El ransomware, en combinación con la ingeniería social, puede constituir un ataque muy efectivo.

Ransomware oculto

El ransomware también puede pasar desapercibido para los firewalls que no son capaces de descifrar e inspeccionar el tráfico Web cifrado mediante SSL. Las soluciones de seguridad de red anticuadas normalmente o bien no son capaces de inspeccionar el tráfico cifrado mediante SSL/TLS, o bien su rendimiento es tan bajo que no pueden utilizarse mientras se realiza la inspección. Los cibercriminales cada vez saben ocultar mejor el malware en el tráfico cifrado.

El cifrado SSL/TLS (Secure Sockets Layer/Transport Layer Security), cuyo uso continúa en aumento, fue responsable de gran cantidad de ataques no detectados que afectaron por lo menos a 900 millones de usuarios en 2015.[3]

3 Informe anual de amenazas 2016 de SonicWall



Conclusión

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, sus datos estarán seguros allá donde vayan gracias a una red de inteligencia compartida que los protege contra una variedad de amenazas, entre las que se incluye el ransomware.

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

SONICWALL®

Acerca de nosotros

Durante sus 25 años de historia, SonicWall ha sido el partner de seguridad de confianza del sector. Desde la seguridad de red, pasando por la seguridad de acceso, hasta la seguridad del correo electrónico, SonicWall ha desarrollado continuamente su cartera de productos para ayudar a las organizaciones a innovar, a acelerar y a crecer. Con más de un millón de dispositivos de seguridad en casi 200 países y regiones en todo el mundo, SonicWall permite a sus clientes decir "Sí" al futuro con confianza.

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

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

Si desea obtener información sobre nuestras oficinas regionales e internacionales, consulte nuestra página Web.
www.sonicwall.com

Ebook-NS-Ransomware-EU-IMAG-29223 -D1

SONICWALL®