SONICWALL®

SUS DATOS A CAMBIO DE UN RESCATE

Por qué hoy en día el ransomware es el exploit preferido por los cibercriminales

CAPTURE EL RANSOMWARE DE FORMA DEFINITIVA

Los perpetradores de ataques y cibercriminales siempre han tenido gran habilidad para acceder a las redes y robar datos. Sin embargo, a menudo, convertir esos datos en beneficios económicos, resultaba complejo y llevaba mucho tiempo.

Con la introducción del ransomware, se ha eliminado la necesidad de exfiltrar los datos y revenderlos en mercados clandestinos.

En la actualidad, resulta más sencillo acceder a su red, cifrar los datos y tomarlos como rehenes hasta que usted pague un rescate. Sin una estrategia de seguridad cibernética proactiva en tiempo real, las organizaciones tienen pocas opciones.

Este manual le ayudará a entender mejor el ransomware y cómo el sandboxing basado en la nube puede mitigar los ataques antes de que irrumpan en su entorno y tomen sus datos — y su negocio — como rehenes para solicitar un rescate.

Visión general

SONICWALL®

Ransomware: ¿Está usted protegido contra el próximo brote?

¿Será usted la próxima víctima del ransomware? ¿Pueden los perpetradores de ataques cifrar sus datos y tomarlos como rehenes hasta que pague un rescate?

Las organizaciones grandes y pequeñas de todos los sectores y de todo el mundo están expuestas a sufrir un ataque de ransomware. Los medios informan a menudo de los ataques perpetrados contra grandes instituciones, como el Hospital de Hollywood, que estuvo sin datos durante más de una semana en 2016 después de que un ataque de ransomware cifrara sus archivos y pidiera un rescate para descifrar los datos.

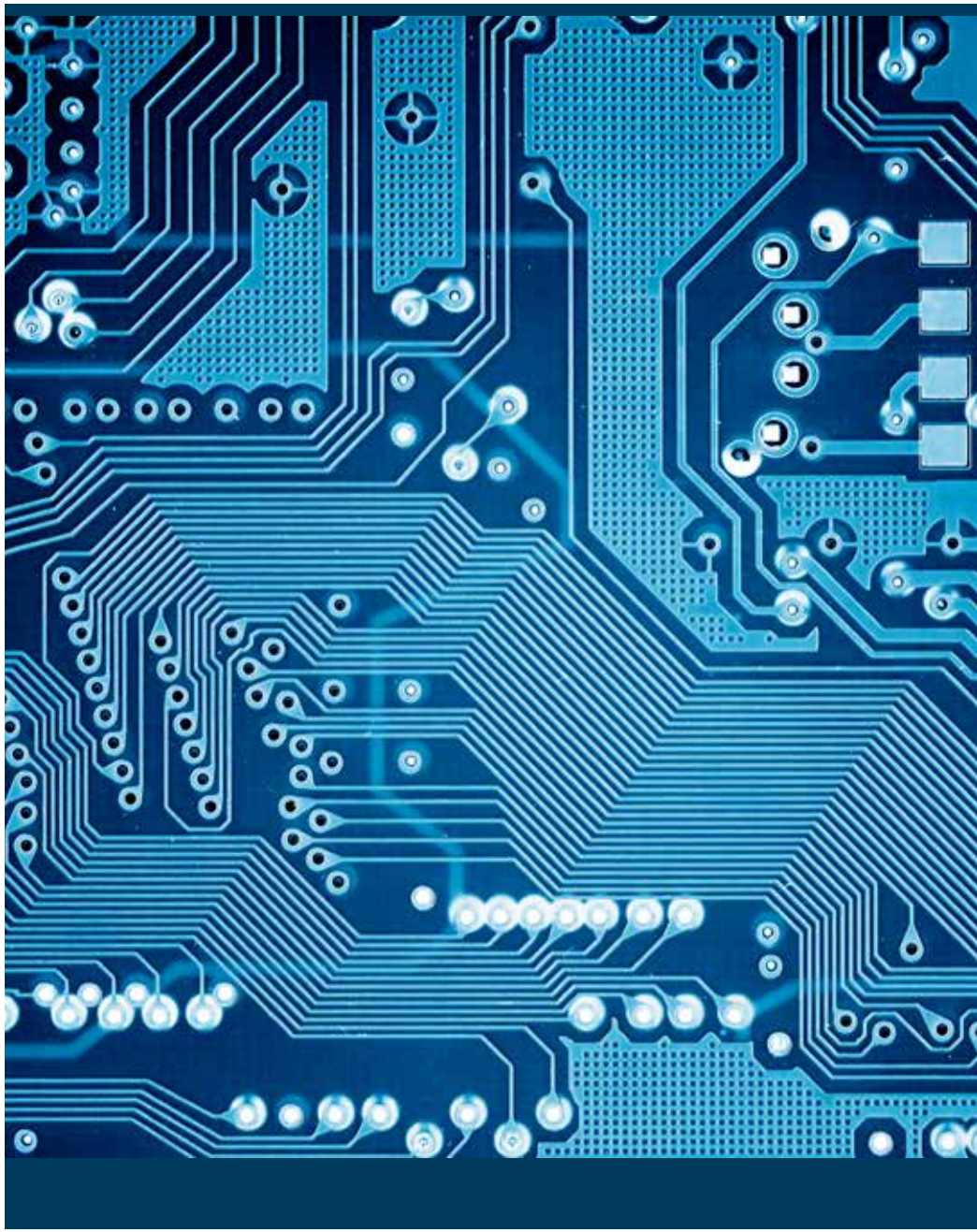
Las empresas pequeñas, sin embargo, también se ven afectadas. De hecho, el equipo de investigación de Kaspersky reveló que las empresas pequeñas y medianas eran las más afectadas. El 42% de ellas habían sido víctima de un ataque de ransomware en un periodo de 12 meses.

De esas empresas afectadas, una de cada tres pagó el rescate, y solo una de cada cinco recuperó sus archivos a pesar de haber pagado. Tanto si forma parte de una organización grande como de una pequeña, está usted en peligro.

TERMINE DE LEER LA HISTORIA >

SONICWALL®

Siete cosas que tienen en común los ataques de ransomware altamente efectivos



En 2016, SonicWall detectó un crecimiento del 600 por ciento de las familias de ransomware. En el Informe anual de amenazas 2017 identificamos una amplia variedad de formas de ransomware y vectores de ataque, algunos de ellos con más éxito, otros con menos.

¿Cuál es, por tanto, la clave del éxito de cualquier ataque? Si entiende los siete componentes de la estrategia de una campaña de ransomware, podrá defenderse mejor contra una de las formas de malware más peligrosas de la historia.

1. Investigación inteligente del blanco

Cualquier buen cibercriminal sabe cómo encontrar a las personas apropiadas de una organización a quienes dirigirse y con qué mensaje debe hacerlo. Los hackers saben que las empresas municipales y sanitarias son blancos beneficiosos.

A pesar de las campañas de concienciación de las organizaciones, la gente sigue haciendo clic en posts de medios sociales y e-mails creados de forma inteligente. Además, los atacantes pueden acceder a cualquier base de datos de generación de oportunidades, donde encuentran un conjunto de víctimas ideales para una campaña de phishing.

2. Entrega efectiva

Puesto que el 65 por ciento de los ataques de ransomware se producen a través del correo electrónico, los perpetradores de ataques pueden enviar un archivo adjunto infectado fácilmente a alguien del departamento de contabilidad afirmando que se trata de una factura impagada. Un ataque de este tipo paralizó a la empresa proveedora de suministros BWL de Lansing, Michigan, EEUU, durante dos semanas, lo cual le costó unos 2,4 millones de dólares.

VEA LA LISTA COMPLETA >

SONICWALL®

El ransomware como servicio (RaaS) es la nueva normalidad

Al desarrollar un modelo de negocio, el empresario tiene que decidirse por un método de distribución y elegir entre la venta directa, a través de un canal de distribuidores, o una mezcla de ambas. Lo mismo ocurre con los desarrolladores de ransomware.

Muchos optan por vender su código exitoso en forma de kit, eliminando así muchos riesgos y la ardua tarea de la distribución — y por supuesto se llevan una parte de los beneficios.

En el transcurso del año pasado (incluso antes de producirse los ataques masivos de WannaCry) se produjeron, a la sombra de los ataques más conocidos, gran cantidad de ataques pequeños y focalizados con kits de exploits adaptados. Tal y cómo descubrió SonicWall, se utilizó una mezcla de malware *amateur*, malware caótico, ransomware readaptado y ransomware RaaS reempaquetado.

- Trumplocker
- AlmaLocker
- Jigsaw
- Lambda
- Derialock
- Shade
- Popcorn
- Jaff

Recientemente, un autor demostró lo fácil que resulta lanzar un ataque de ransomware en una hora... **sin conocimientos de hackeo.**

¿Qué significa esto para una organización como la suya? ¿Debería preocuparle? Dicho de manera simplificada: cuantas más fuentes de ataque haya, más ataques se producen. Pero SonicWall está aquí para protegerle.

CONTINÚE LEYENDO >

SONICWALL®

Por qué el sandboxing de red es necesario para detener el ransomware

Si bien los firewalls de próxima generación utilizan definiciones y métodos heurísticos con gran éxito, éstos ya no son suficientes para ofrecer protección contra los ataques maliciosos de hoy en día. Los retos que plantean los ataques selectivos y las amenazas de día cero hacen que la tecnología de sandboxing sea imprescindible para poder disfrutar de una seguridad efectiva.

El actual crecimiento de las amenazas externas es asombroso. En su esfuerzo por ampliar al máximo el alcance de sus ataques, y evitar al mismo tiempo la detección, los perpetradores de ataques combinan la naturaleza oportunista de la automatización con la mentalidad de un proveedor de software para desarrollar sus amenazas continuamente.

Dado el impacto negativo que sufre cualquier empresa víctima de una filtración de datos o de un ataque de ransomware, para las organizaciones de TI es imprescindible detectar el código malicioso antes de que su red se vea afectada.

El verdadero reto no es el ransomware que ya se ha propagado por Internet, sino los ataques selectivos y las amenazas de día cero.

Los ataques selectivos implican código desconocido hasta el momento y creado específicamente para la organización atacada, mientras que las amenazas de día cero explotan vulnerabilidades recientemente descubiertas para las cuales los proveedores todavía no han creado parches.

Este es el tipo de ataques que más debe preocupar a las organizaciones, ya que suelen tener mucho más éxito que los más antiguos. ¿Cuál es, por tanto, la mejor manera de evitar que emerja una amenaza desde el interior de su red?

Descargue el informe gratuito de IDC y lea cómo el sandboxing ayuda a mitigar las amenazas avanzadas.


IDC

IDC ANALYST CONNECTION

Addressing Advanced Threats Through Multiple Sandbox Options

Informe gratuito de IDC

Addressing Advanced Threats Through Multiple Sandbox Options

DESCARGUE EL INFORME >

SONICWALL®

Detenga el ransomware con Capture ATP

El servicio SonicWall Capture Advanced Threat Protection (ATP) es un sandbox multimotor basado en la nube diseñado para descubrir y detener los ataques de día cero desconocidos (p.ej. el ransomware) en la pasarela, con implementación automática de definiciones.

Se trata del único producto de detección de amenazas avanzadas que combina el sandboxing multicapa, incluida la emulación del sistema completo, con técnicas de virtualización, a fin de analizar comportamientos de código sospechosos.

Gracias a esta eficaz combinación, el servicio SonicWall Capture Advanced Threat Protection detecta más amenazas que las soluciones de sandbox de un solo motor, que son específicas de un entorno de computación y susceptibles a la evasión.

- **Detiene el ransomware en tiempo real**
- **Análisis multimotor de amenazas avanzadas**
- **Informes y alertas**
- **Análisis de gran variedad de tipos de archivos**
- **Rápida implementación de definiciones**
- **Bloqueo hasta que haya un veredicto**

Si desea obtener más información sobre el servicio SonicWall Capture Advanced Threat Protection, descargue la ficha técnica o visite **sonicwall.com/capture**.

¿Cómo funciona Capture ATP?

OBTENGA LA FICHA TÉCNICA >

SONICWALL®

Demostración: SonicWall Capture ATP contra el malware más reciente

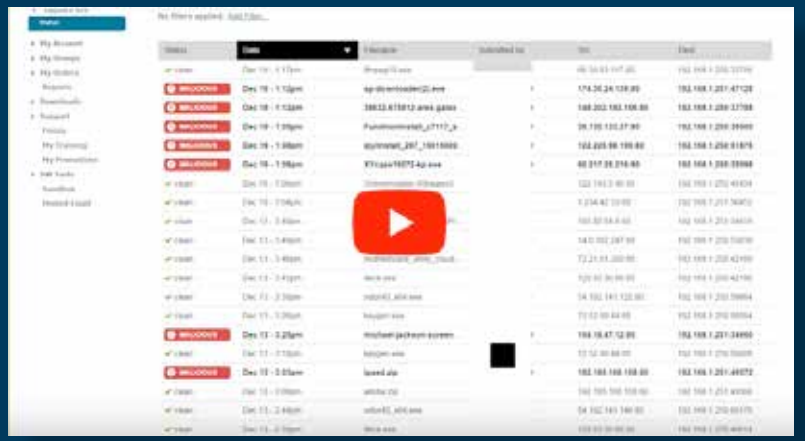
SonicWall Capture Advanced Threat Protection es un servicio basado en la nube y disponible con los firewalls de SonicWall que detecta las amenazas y puede bloquearlas en la pasarela hasta que haya un veredicto. De esta forma, Capture ATP protege a los clientes contra los crecientes peligros de las amenazas de día cero (p. ej. el ransomware).

¿Cómo de eficaz es Capture ATP? Para demostrar que SonicWall es capaz de detener las amenazas avanzadas reales que acechan continuamente a las empresas, hemos tomado el malware más nuevo y peligroso de Internet y hemos realizado un test con nuestra tecnología.

Utilizando solo Gateway Anti-Virus (GAV) y Capture ATP, demostramos cómo se identifica y neutraliza el malware en tiempo real. Capture ATP descubre lo que el malware quiere hacer con la aplicación, el SW, el OS y el hardware.

A partir de ahí, la infraestructura global de inteligencia de amenazas rápidamente implementa las definiciones de las amenazas recién identificadas en todos los dispositivos de seguridad de red de SonicWall, a fin de detener la infiltración.

Los clientes se benefician de una seguridad altamente efectiva, tiempos de respuesta rápidos y un coste total de propiedad reducido.



VEA LA DEMOSTRACIÓN COMPLETA >

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 territorios en todo el mundo, SonicWall permite a sus clientes decir "Sí" al futuro con confianza.

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

SONICWALL®