



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 irruman en su entorno y tomen sus datos – y su negocio – como rehenes para solicitar un rescate.

Visión general

Pág. 3 - Ransomware: ¿Está usted protegido contra el próximo brote?

Pág. 4 - Siete cosas que tienen en común los ataques de ransomware altamente efectivos.

Pág. 5 - El ransomware como servicio (RaaS) es la nueva normalidad

Pág. 6 - Por qué el sandboxing de red es necesario para detener el ransomware

Pág. 7 - Detenga el ransomware con Capture ATP

Pág. 8 - SonicWall Capture ATP contra el malware más reciente

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 >



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

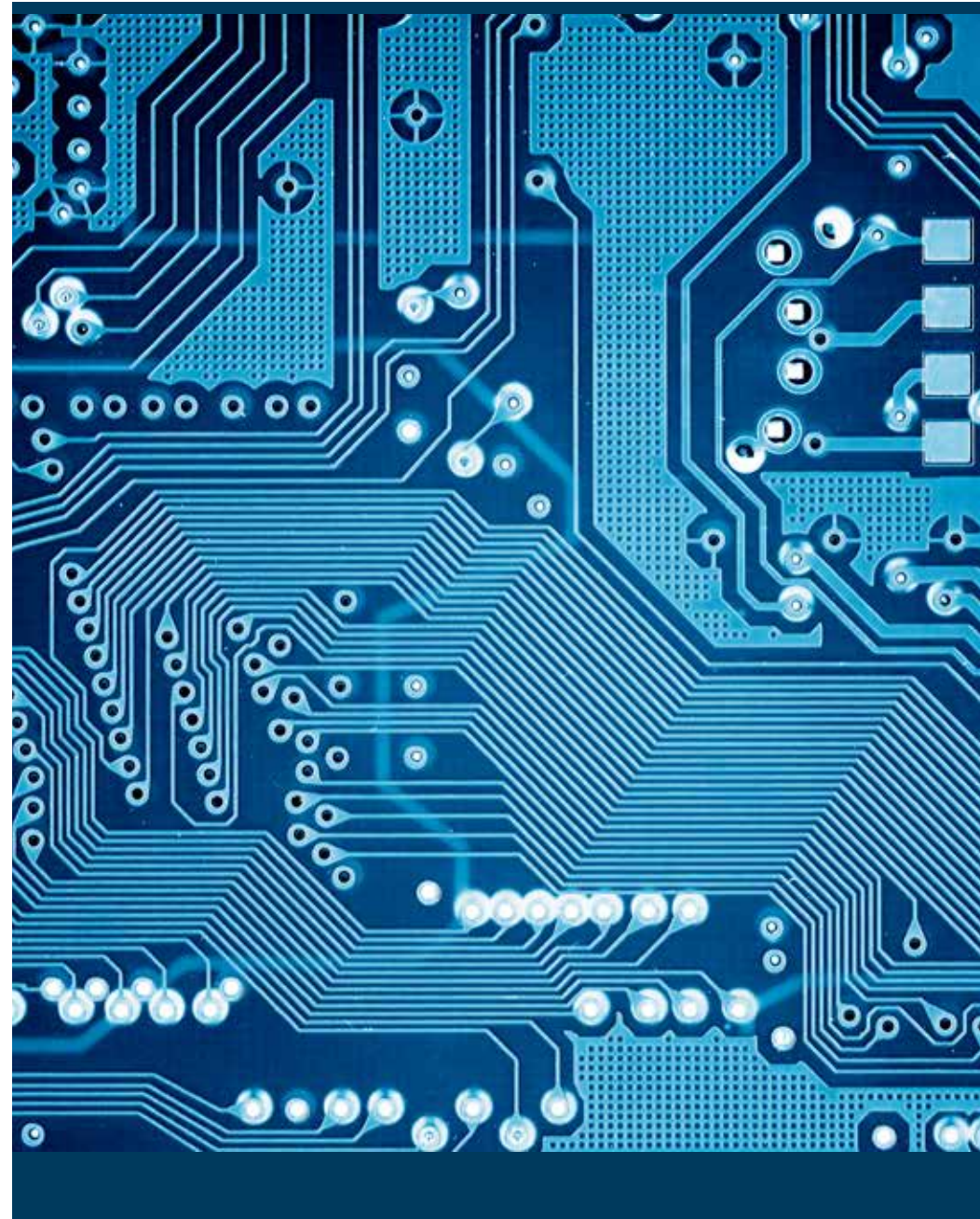
Cualquier buen cibercriminal sabe cómo encontrar a las personas apropiadas de una organización a quienes dirigirse y con qué mensaje debe hacerlo. Los hackers saben que las empresas municipales y sanitarias son blancos beneficiosos.

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 >



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 >



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.



Informe gratuito de IDC

Addressing Advanced Threats Through Multiple Sandbox Options


DESCARGUE EL INFORME >

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 de gran variedad de tipos de archivos**

 **Análisis multimotor de amenazas avanzadas**

 **Rápida implementación de definiciones**

 **Informes y alertas**

 **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 >

Demostración: SonicWall Capture ATP contra el malware más reciente

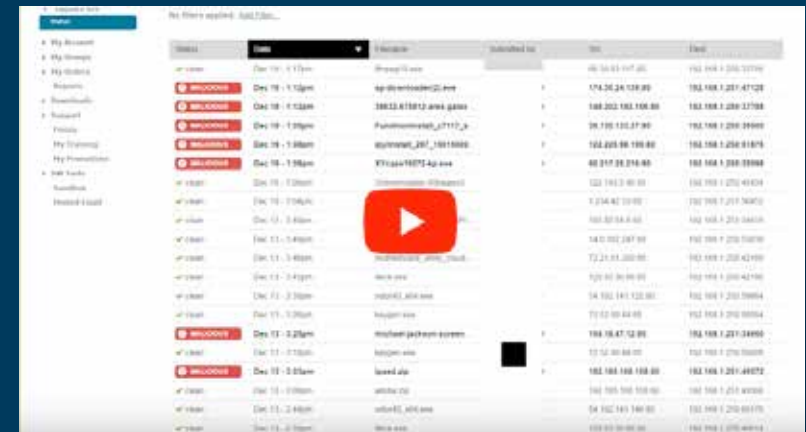
SonicWall Capture Advanced Threat Protection es un servicio basado en la nube y disponible con los firewalls de SonicWall que detecta las amenazas y puede bloquearlas en la pasarela hasta que haya un veredicto. De esta forma, Capture ATP protege a los clientes contra los crecientes peligros de las amenazas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



Threat	Date	Source	Subscribed to	Size	Cost
ap-000000	Dec 18 - 1:13pm	ap-00000002.exe		48 56 83 147 26	162 168 1 201 20170
ap-000000	Dec 18 - 1:12pm	ap-00000002.exe		174 26 24 138 80	162 168 1 201 47128
ap-000000	Dec 18 - 1:12pm	38832.61812.apk.gate		188 202 183 168 88	162 168 1 201 17188
ap-000000	Dec 18 - 1:10pm	Funmmmmmmmm_07117_p		38 190 130 87 90	162 168 1 201 04900
ap-000000	Dec 18 - 1:08pm	WUWUWU_007_18118888		162 205 88 188 88	162 168 1 201 81818
ap-000000	Dec 18 - 1:08pm	X716647072.App.exe		88 017 28 276 88	162 168 1 201 03888
ap-000000	Dec 18 - 1:02pm			122 142 3 88 88	162 168 1 201 48818
ap-000000	Dec 18 - 1:04pm			1 234 42 13 88	162 168 1 201 76872
ap-000000	Dec 17 - 3:48pm			168 88 16 8 88	162 168 1 201 04888
ap-000000	Dec 17 - 1:48pm			34 0 102 187 88	162 168 1 201 10888
ap-000000	Dec 17 - 3:48pm			72 21 81 188 88	162 168 1 201 42188
ap-000000	Dec 18 - 3:48pm	Web.exe		120 88 88 88 88	162 168 1 201 42188
ap-000000	Dec 17 - 3:38pm	38832.61812.apk.gate		188 202 183 168 88	162 168 1 201 76872
ap-000000	Dec 17 - 3:38pm	Web.exe		120 88 88 88 88	162 168 1 201 42188
ap-000000	Dec 17 - 3:25pm	Malware (packet stream)		188 16 47 12 88	162 168 1 201 04888
ap-000000	Dec 17 - 3:18pm	Web.exe		120 88 88 88 88	162 168 1 201 42188
ap-000000	Dec 18 - 3:05pm	Web.exe		162 168 168 168 88	162 168 1 201 48872
ap-000000	Dec 18 - 1:08pm	Web.exe		162 168 168 168 88	162 168 1 201 48872
ap-000000	Dec 17 - 2:48pm	Web.exe		120 88 88 88 88	162 168 1 201 42188
ap-000000	Dec 18 - 1:08pm	Web.exe		162 168 168 168 88	162 168 1 201 48872

VEA LA DEMOSTRACIÓN
COMPLETA >

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

© 2017 SonicWall Inc. TODOS LOS DERECHOS RESERVADOS.

SonicWall es una marca comercial o marca comercial registrada de SonicWall Inc. y/o sus filiales en EEUU y/u otros países. Las demás marcas comerciales y marcas comerciales registradas son propiedad de sus respectivos propietarios.

La información incluida en este documento se proporciona en relación con los productos de SonicWall Inc. y/o sus filiales. No se otorga mediante este documento, ni en relación con la venta de productos SonicWall, ninguna licencia, expresa ni implícita, por doctrina de los propios actos ni de ningún otro modo, sobre ningún derecho de propiedad intelectual. A EXCEPCIÓN DE LO ESTABLECIDO EN LOS TÉRMINOS Y CONDICIONES TAL Y COMO SE ESPECIFICAN EN EL CONTRATO DE LICENCIA DE ESTE PRODUCTO, SONICWALL Y/O SUS FILIALES NO ASUMEN NINGUNA RESPONSABILIDAD Y RECHAZAN CUALQUIER GARANTÍA EXPRESA, IMPLÍCITA O LEGAL EN RELACIÓN CON SUS PRODUCTOS, INCLUIDAS, ENTRE OTRAS, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN, ADECUACIÓN PARA UN DETERMINADO PROPÓSITO O NO VIOLACIÓN DE DERECHOS DE TERCEROS. SONICWALL Y/O SUS FILIALES NO SE HARÁN RESPONSABLES EN NINGÚN CASO DE DAÑOS DIRECTOS, INDIRECTOS, CONSECUENTES, PUNITIVOS, ESPECIALES NI INCIDENTALES (INCLUIDOS, SIN LIMITACIÓN, LOS DAÑOS RELACIONADOS CON LA PÉRDIDA DE BENEFICIOS, LA INTERRUPCIÓN DEL NEGOCIO O LA PÉRDIDA DE INFORMACIÓN) DERIVADOS DEL USO O DE LA INCAPACIDAD DE UTILIZAR EL PRESENTE DOCUMENTO, INCLUSO SI SE HA ADVERTIDO A SONICWALL Y/O SUS FILIALES DE LA POSIBILIDAD DE QUE SE PRODUZCAN TALES DAÑOS. SonicWall y/o sus filiales no ofrecen declaración ni garantía alguna con respecto a la precisión ni a la integridad de la información contenida en el presente documento y se reservan el derecho de modificar las especificaciones y las descripciones de productos en cualquier momento y sin previo aviso. SonicWall Inc. y/o sus filiales no se comprometen a actualizar la información contenida en el presente documento.