
SONICWALL®
Tipos de estrategias de ciberataque y cómo combatirlas
LIBRO VIRTUAL

Introducción

Los cibercriminales de hoy en día han perfeccionado sus técnicas –de por sí ya complejas– para evitar ser detectados y acceder de forma desapercibida a las redes con diversos fines, a menudo lucrativos. Su intención es robar propiedad intelectual, espiar, interrumpir procesos o secuestrar archivos, entre otros muchos delitos. Utilizan las últimas técnicas para evadir la detección, con el fin de mantener su acceso y llevar a cabo sus actividades maliciosas de forma inadvertida.

Una vez que consiguen acceder a la red, los atacantes intentan descargar e instalar malware en el sistema comprometido. En muchos casos, utilizan nuevas variantes de malware que las soluciones antivirus tradicionales todavía no conocen.

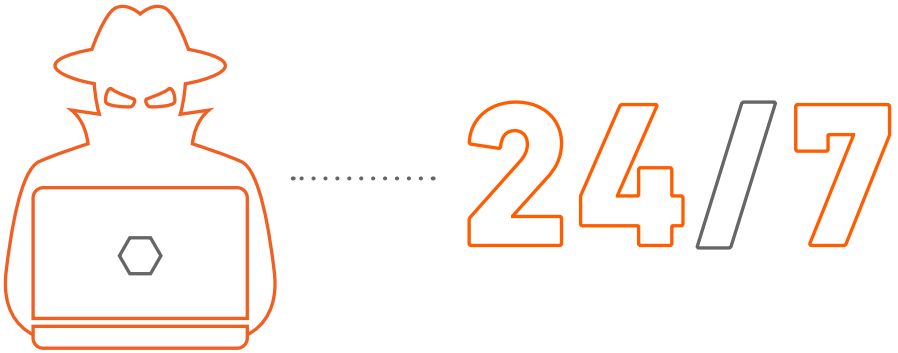
En este eBook recogemos las estrategias y herramientas de ciberataque utilizadas por los ciberdelincuentes para infiltrarse en su red, y explicamos en detalle cómo puede contrarrestar estas estrategias para detener a los cibercriminales.

Los cibercriminales trabajan a todas horas, los siete días de la semana, para explotar sus debilidades.

Estrategia de ciberataque n.º 1 El bombardeo incesante de las redes con malware

El volumen total de malware va en aumento, y en algunos países se está observando un récord de intentos con cifras multimillonarias. Los ataques pueden llegar de todos los vectores para comprometer su red. Se dirigen contra el correo electrónico, los dispositivos móviles, el tráfico Web, etc. y los hackers incluso pueden comprometer su sistema mediante exploits automatizados. Además, el tamaño de su empresa no importa. Para un hacker, usted no es más que una dirección IP, una dirección de e-mail o un posible blanco para un ataque "watering hole". Los perpetradores de ataques utilizan herramientas automáticas para ejecutar exploits o lanzar e-mails de phishing día y noche.

El problema al que se enfrentan muchas organizaciones es que no cuentan con las herramientas adecuadas para protegerse contra estos ataques. Muchas carecen de herramientas automáticas que les ayuden a examinar el tráfico, proteger los endpoints y filtrar el correo electrónico para expulsar los mensajes maliciosos. Otras utilizan firewalls que no pueden ver el interior del tráfico cifrado para detectar amenazas ocultas, o bien cuentan con una memoria del sistema integrada limitada para almacenar las definiciones de malware.



Contraataque n.º 1
Proteja la red cada minuto, de cada día

Puesto que cada hora se desarrollan cientos de variantes de malware nunca antes vistas, las organizaciones necesitan una protección en tiempo real actualizada al minuto contra estas nuevas amenazas. Una solución de seguridad efectiva debe contar con la última tecnología para detectar el peligro en tiempo real, protegiendo su organización las 24 horas del día, los siete días de la semana. Con la gran oleada de tipos y variantes de malware, se excede la memoria disponible de cualquier firewall. Una solución de servicios de seguridad que incluye tecnología como Real-Time Deep Memory Inspection (RTDMI™) detecta y bloquea de forma proactiva las amenazas de día cero del mercado de masas y las variantes de malware desconocidas.

Los firewalls deberían utilizar un sandbox basado en la nube con el fin de proporcionar la más amplia visión del malware y descubrir e identificar nuevas variantes. Asimismo, resulta esencial asegurarse de que su solución de seguridad ofrezca soporte dinámico para una protección actualizada no solo en la pasarela del firewall, sino también en los endpoints móviles y remotos, ya que los dispositivos del Internet de las cosas (IoT) pueden servir como puntos de entrada para los perpetradores de ataques.

Insista en una plataforma de seguridad que aproveche las ventajas de la nube y ofrezca detección y prevención de brechas en tiempo real automatizada para contrarrestar las últimas amenazas de malware.

Los ciberdelincuentes utilizan diferentes tipos de malware para pillarle desprevenido.

Estrategia de ciberataque n.º 2 La infección de las redes con diferentes tipos de malware

Los cibercriminales utilizan múltiples vectores de ataque y variantes de malware para comprometer las redes. Los cinco más comunes son los virus, los gusanos, los troyanos, el spyware y el ransomware.

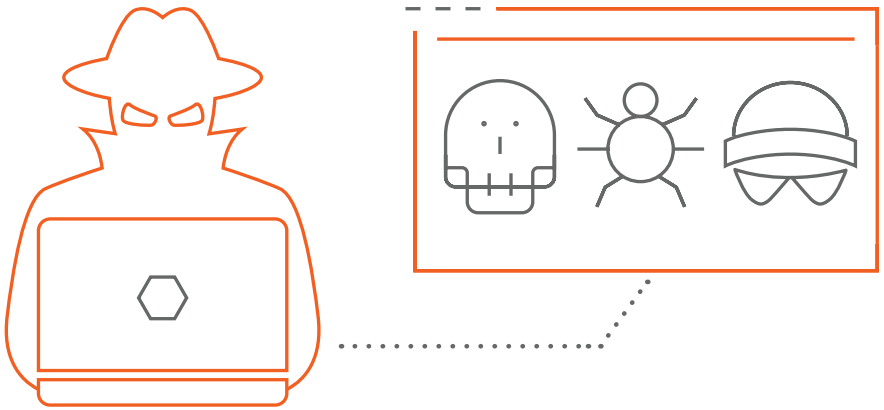
Originalmente, los virus informáticos se propagaban a través de medios infectados compartidos. Conforme la tecnología ha evolucionado, los métodos de distribución también han ido cambiando. En la actualidad, los virus normalmente se transmiten a través de programas legítimos, archivos compartidos, descargas Web y archivos adjuntos de los mensajes de correo electrónico. Pueden cometer diversas acciones maliciosas: desde la corrupción de datos hasta la caída del sistema cuando se abren o ejecutan.

A pesar de que existen desde finales de los años 80, los gusanos informáticos no se convirtieron en una amenaza común hasta que se generalizó el uso de infraestructuras de red en las organizaciones. A diferencia de los virus informáticos, los gusanos se autorreplican y pueden reptar por las redes sin interacción humana. Pueden causar infecciones rápidamente y sobrecargar las redes con tráfico.

Los troyanos son programas maliciosos que se hacen pasar por software o archivos legítimos y están diseñados específicamente para extraer datos sensibles de la red. Muchos tipos de troyanos se hacen con el control del sistema infectado y abren una puerta trasera por la que el atacante accede más tarde. Los troyanos también se utilizan a menudo en la creación de redes de robots informáticos (botnets).

El spyware no es, en sí, un elemento malicioso, pero puede causar graves trastornos, ya que suele infectar los navegadores Web e inutilizarlos casi por completo. A veces, el spyware se hace pasar por aplicaciones legítimas que ofrecen ventajas al usuario, mientras que registra de forma inadvertida las teclas pulsadas y el historial de navegación, robando datos personales o haciendo un seguimiento del comportamiento de los usuarios y de los patrones de uso. Los datos robados se envían al perpetrador del ataque, comprometiendo la privacidad y la seguridad del usuario.

El ransomware es un ataque que a menudo cifra los archivos de un endpoint o de un servidor completo, haciéndolos inaccesibles. Los cibercriminales exigen un rescate a la organización, habitualmente en Bitcoin, a cambio de la clave de cifrado. Cuando se propaga a sistemas críticos de negocio, el coste del ransomware puede ascender a cientos de miles de dólares o más.



Para adelantarse a las amenazas, considere implantar múltiples capas de protección antimalware.

Contraataque n.º 2
Asegúrese de proteger su red contra todos los tipos de malware

Los firewalls deberían proteger a las organizaciones contra todos los tipos de ciberamenazas. La mejor forma de conseguirlo consiste en integrar estas protecciones en un enfoque de un solo paso y baja latencia que bloquee los vectores de ataque no solo en la pasarela, sino también en los endpoints, más allá del perímetro tradicional. Busque las siguientes prestaciones:

- Protección contra malware basada en red para impedir que los atacantes descarguen o transmitan el malware a un sistema comprometido
- Actualizaciones continuas y puntuales para proteger las redes permanentemente contra los millones de nuevas variantes de malware tan pronto se descubran
- Servicio de prevención de intrusiones (IPS) para evitar que los atacantes exploten las vulnerabilidades
- Sandboxing para enviar el código sospechoso a un entorno aislado basado en la nube para su detonación y análisis con el fin de detectar variantes de malware desconocidas hasta el momento
- Seguridad de acceso para aplicar contramedidas de control del acceso de los usuarios en los endpoints móviles y remotos, tanto dentro como fuera del perímetro de la red
- Seguridad de correo electrónico para bloquear los ataques de phishing, spam, troyanos e ingeniería social transmitidos vía e-mail

Asegúrese de que cualquier dispositivo con acceso a su red cuente con un software de protección antivirus actualizado. De esta forma, podrá disfrutar de una capa adicional de protección antimalware. Al combinar un antivirus completo en los PCs y firewalls en la red, las organizaciones pueden bloquear muchas de las herramientas que usan los cibercriminales para comprometer la red.

Estrategia de ciberataque n.º 3 Encontrar y comprometer las redes más débiles

> Los cibercriminales a menudo escogen a sus víctimas en función de los puntos débiles que descubren en la red.

Aunque muchos proveedores de firewalls afirman ofrecer una excelente protección antiamenazas, son muy pocos los que pueden demostrar la eficacia de sus soluciones. Las organizaciones que utilizan firewalls antiguos quizá crean que sus redes están protegidas. Sin embargo, los cibercriminales más hábiles pueden burlar los firewalls que carecen de las medidas de seguridad oportunas utilizando algoritmos complicados que eluden la detección y comprometen la red.

Algunos firewalls ofrecen seguridad a costa del rendimiento, lo cual hace que las organizaciones que los utilizan puedan caer en la tentación de desactivarlos o limitar las medidas de seguridad para conseguir el alto rendimiento de red que requieren. Esta es una práctica arriesgada que debe evitarse.

Otra vulnerabilidad de la seguridad de red se basa en el factor humano. Los cibercriminales se suelen aprovechar de las acciones o conductas humanas que comprometen sin querer la integridad, la confidencialidad y la disponibilidad de una red. Las acciones que pueden conllevar riesgos y debilitar las medidas de seguridad incluyen las estafas de phishing, la ingeniería social, los sistemas mal configurados, el software sin parchear, las políticas de seguridad ignoradas, etc. Los cibercriminales utilizan estas tácticas para acceder a datos de inicio de sesión y otra información de autorización, con la intención de sortear las protecciones del firewall instigando ataques desde el interior. Además, a veces, los empleados se conectan a la red corporativa con dispositivos personales que no cuentan con medidas de seguridad apropiadas. Esto puede dar lugar a un acceso no autorizado si un dispositivo personal se pierde o se deja descuidado, exponiendo a la organización a una brecha cuando se encuentran fuera del perímetro de seguridad de la red.

> Todos los firewalls necesitan un motor que proteja las redes de los ataques internos y externos sin sacrificar el rendimiento.

Contraataque n.º 3
Elija una plataforma de seguridad completa que ofrezca una protección contra las amenazas de nivel superior, alto rendimiento y gestión centralizada.

Busque soluciones de seguridad con protección antimalware basada en la red, probadas y certificadas de forma independiente.

Plantéese un diseño de plataforma multinúcleo capaz de escanear archivos de cualquier tamaño y de cualquier tipo para poder reaccionar sin problemas a los cambiantes flujos de tráfico. Todos los firewalls necesitan un motor que proteja las redes de los ataques internos y externos sin sacrificar el rendimiento.

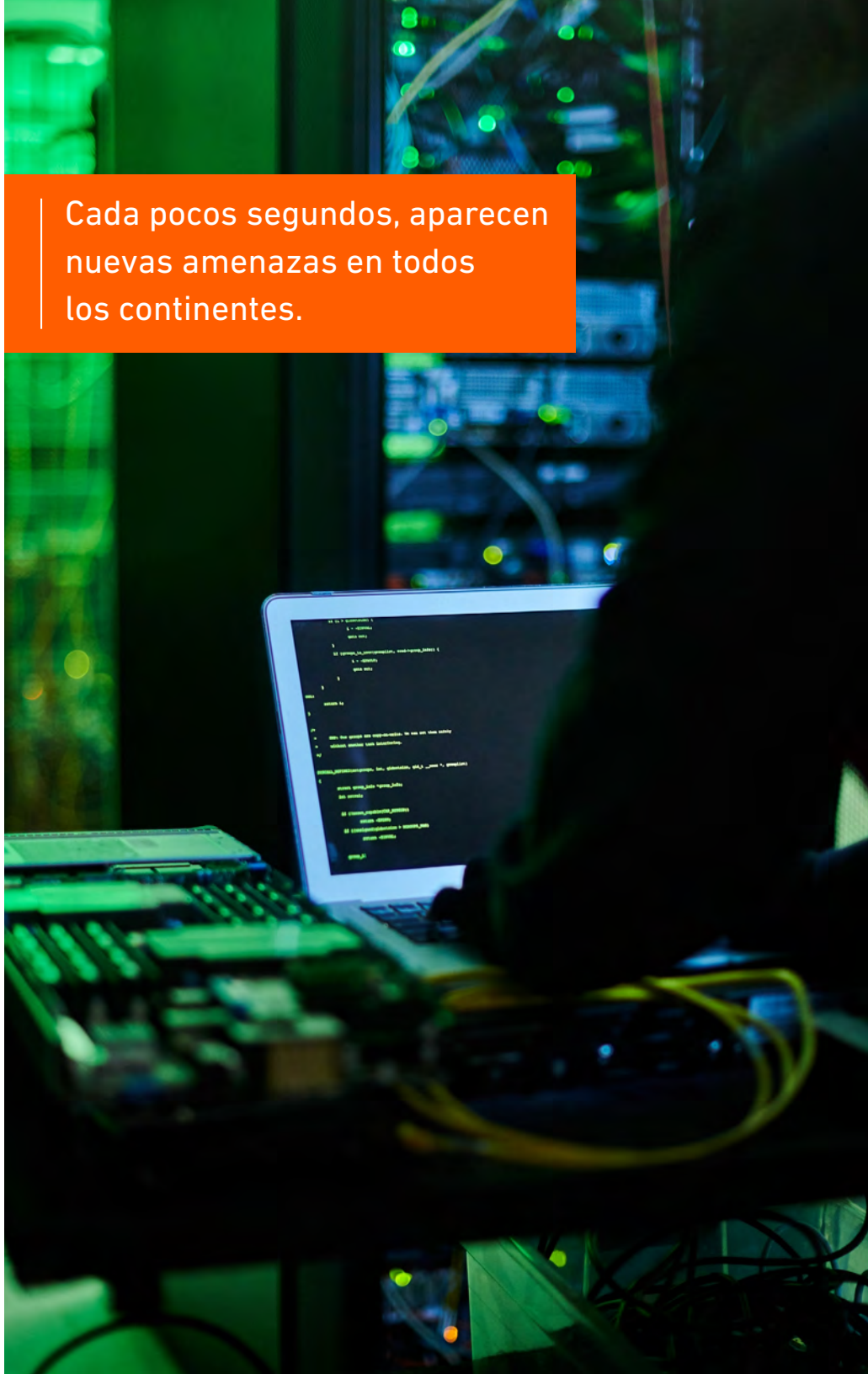
Busque un firewall que ofrezca un sandbox basado en la nube para ayudarle a descubrir nuevas variantes de malware que posiblemente tengan su entorno en el punto de mira. Estos detalles podrían marcar la diferencia entre un día de trabajo normal y el día que los cibercriminales secuestran sus recursos digitales.

Para disfrutar de un acceso móvil seguro, su estrategia de seguridad debe incluir la protección de los endpoints móviles y remotos tanto dentro como fuera del perímetro.

Asimismo, necesita seguridad de correo electrónico que le proteja contra los ataques de phishing, spam, virus, ingeniería social y otras amenazas transmitidas vía e-mail. Utilice herramientas como el test de phishing gratuito de SonicWall para formar a su organización.

Estrategia de ciberataque n.º 4 Transformación constante y ataques a escala global

Muchos cibercriminales logran sus propósitos porque no cesan de inventar nuevo malware ni de compartirlo con otros atacantes por todo el mundo. Esto significa que aparecen nuevas amenazas cada pocos segundos en todos los continentes. Muchos cibercriminales utilizan tácticas de ataque relámpago: realizan la incursión, saquean todo lo que pueden y se marchan antes de que nadie pueda dar la voz de alarma. Pueden entrar y salir incluso antes de que usted sepa lo que ha ocurrido. Otros, proceden más lentamente para intentar acceder a más datos durante un periodo de tiempo más largo. Algunos ataques se perpetran a través de la Web, mientras que otros nos llegan vía e-mail o acceden directamente a la red por medio de dispositivos infectados que han sido utilizados fuera del perímetro de seguridad de la red.



> Cada pocos segundos, aparecen nuevas amenazas en todos los continentes.

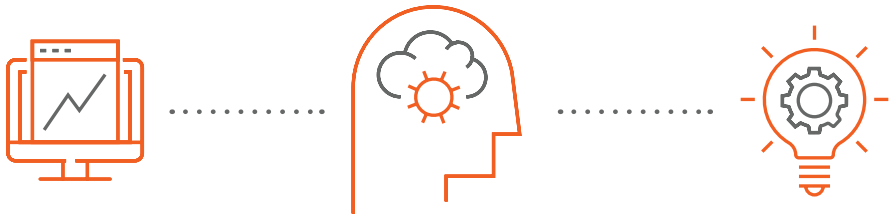
Para bloquear las amenazas globales más recientes, invierta en una solución de seguridad con inteligencia de amenazas global.

Contraataque n.º 4
Elija un firewall que le proteja contra las amenazas globales

Reaccionar rápidamente a las amenazas es esencial para maximizar la protección. Si quiere implementar lo más rápidamente posible medidas contra las amenazas emergentes, recurra a un proveedor de soluciones de seguridad que cuente con un equipo interno de inteligencia de amenazas, investigación y contramedidas. Ese equipo, además, debería colaborar con la comunidad de seguridad global para ampliar el alcance de sus actuaciones, como hace SonicWall con su Informe de Ciberamenazas.

Una solución de amplio espectro utiliza un catálogo de malware global basado en la nube que suplementa el análisis del firewall local.

Finalmente, mientras que un firewall básico puede identificar y bloquear las amenazas por zona geográfica, los firewalls de nueva generación más sofisticados incorporarán funciones de filtrado de redes de robots informáticos con el fin de reducir la exposición a las amenazas globales conocidas mediante el bloqueo del tráfico procedente de dominios peligrosos o de las conexiones establecidas en ambas direcciones con una ubicación maliciosa.



Conclusión

Al diseñar sus estrategias de defensa contra los ciberataques basados en la red, debería implementar un enfoque holístico que incorpore prácticas de seguridad robustas y el uso de herramientas de seguridad efectivas capaces de detectar comportamientos anómalos de la red y tomar las correspondientes medidas sin que el rendimiento se vea comprometido. Proteja su seguridad y la de su organización contra las amenazas desconocidas adaptándose a las cambiantes amenazas con un enfoque proactivo.

Cuando esté preparado para evaluar soluciones de contraataque que se ajusten a las necesidades únicas de su organización, póngase en contacto con su representante de SonicWall o visite nuestra página Web para obtener más información sobre los Firewalls de nueva generación (NGFWs) de SonicWall.

¿Cómo puedo obtener más información?

Póngase en contacto con nosotros y hable con un experto en seguridad de SonicWall.

Vea las demostraciones en directo de nuestra línea de productos SonicWall

Visite nuestra página Web, Firewalls de nueva generación

Vea dónde se están produciendo los últimos ataques en nuestro Capture Labs Security Center.

SONICWALL

Acerca de SonicWall

SonicWall proporciona una Ciberseguridad sin límites, sin perímetro, para la era hiperdistribuida y una realidad laboral caracterizada por la movilidad, el teletrabajo y la inseguridad. Al detectar amenazas desconocidas, proporcionar visibilidad en tiempo real y ofrecer una alta rentabilidad, SonicWall cierra la brecha de la ciberseguridad para empresas, gobiernos y pymes en todo el mundo. Si desea obtener más información, visite www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Si desea obtener más información, consulte nuestra página Web.
www.sonicwall.com

SONICWALL®

Ebook-TypesofCyberattacks-JK-8854