SONICWALL®

TIPOS DE CIBERATAQUES Y CÓMO PREVENIRLOS

Hoy en día, los ciberdelincuentes utilizan diversas técnicas complejas para evitar ser detectados mientras tratan de colarse en las redes corporativas para robar propiedad intelectual o secuestrar archivos y tomarlos como rehenes. A menudo, sus amenazas están cifradas para evadir la detección.

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.

Este ebook explica en detalle las estrategias y herramientas que los cibercriminales utilizan para infiltrar su red y cómo puede detenerlos.

Los ciberdelincuentes trabajan a todas horas, todos los días, para explotar sus debilidades.

Estrategia de ciberataque nº 1

El bombardeo incesante de las redes con malware

Los ataques llegan por todos los vectores: vía e-mail, a través de los dispositivos móviles, en el tráfico Web, y por medio de exploits automáticos. 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 puntos terminales 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.

SONICWALL®

Contraataque nº 1

Proteja la red cada minuto, de cada día

Cada hora se desarrollan cientos de nuevas variantes de malware. Por eso, las organizaciones necesitan una protección en tiempo real actualizada al minuto que les blinde ante las últimas amenazas. Una solución de seguridad solo es eficaz si se actualiza continuamente, las 24 horas del día, los 7 días de la semana. Además, puesto que el número de variantes y de tipos de malware es tan elevado, la memoria disponible de cualquier firewall resulta insuficiente.

Los firewalls deberían utilizar un sandbox de red, así como recurrir a la nube, para contar con las máximas opciones de visualización del malware, descubrir las nuevas variantes e identificarlas mejor. Asegúrese, además, de que su solución de seguridad soporte una protección actualizada de forma dinámica no solo en la pasarela del firewall, sino también en los puntos terminales móviles y remotos, así como para su correo electrónico.

Insista en una plataforma de seguridad que aproveche las ventajas de la nube y ofrezca protección en tiempo real contra las últimas amenazas de malware.

Estrategia de ciberataque nº 2

La infección de las redes con diferentes tipos de malware

Los ciberdelincuentes utilizan diferentes tipos de vectores de ataque para comprometer las redes. Los cinco más comunes son los virus, los gusanos, los troyanos, el spyware y el ransomware.

Los virus informáticos, en los inicios, se propagaban a través de los disquetes que se compartían. Conforme la tecnología ha evolucionado, los métodos de distribución también han ido cambiando. En la actualidad, los virus se transmiten a través de los archivos compartidos, las descargas web y los archivos adjuntos de los mensajes de correo electrónico.

Los gusanos informáticos existen desde finales de los años ochenta, pero no se extendieron hasta que las infraestructuras de red de las organizaciones se generalizaron. A diferencia de los virus informáticos, los gusanos pueden reptar por las redes sin interacción humana.

Los troyanos están diseñados específicamente para extraer información sensible 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 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. Algunas veces, el spyware aparenta ser una aplicación legítima que proporciona al usuario ciertas ventajas, pero, a su vez, registra secretamente el comportamiento y los patrones de uso.

El ransomware es un ataque que a menudo cifra los archivos de un punto terminal o un servidor y exige al usuario final el pago de un rescate en bitcoins a cambio de la clave de cifrado. Cuando se propaga a sistemas críticos de negocio, el coste del rescate puede ascender a cientos de miles de dólares.

Los ciberdelincuentes utilizan diferentes tipos de malware para pillarle desprevenido.

Contraataque nº 2

Asegúrese de proteger su red contra todos los tipos de malware

Todos los firewalls deberían mantener a las organizaciones a salvo de virus, gusanos, troyanos, spyware y ransomware. 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 puntos terminales, 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 se aprovechen de las vulnerabilidades de la red
- **Sandboxing de red** 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 seguridad en los puntos terminales 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 que disponga de acceso a su red cuente con un software de protección antivirus actualizado. De esta forma podrá disfrutar de una capa adicional de protección antimalware. Mediante la combinación de antivirus en los PCs y firewalls en la red, las organizaciones podrán bloquear muchas de las herramientas que utilizan los ciberdelincuentes para poner en peligro la red.

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

Estrategia de ciberataque nº 3

La búsqueda de las redes más débiles para convertirlas en blanco de sus ataques

Aunque muchos proveedores de firewalls afirman ofrecer una excelente protección antiamenazas, son muy pocos los que han podido demostrar la eficacia de sus soluciones. Las organizaciones que utilizan firewalls de calidad inferior quizá crean que sus redes están protegidas, pero la realidad es que los delincuentes más hábiles pueden burlar el sistema de prevención de intrusiones con complicados algoritmos que eluden la detección y suponen un riesgo para el sistema.

Dado que algunos firewalls ofrecen protección a costa del rendimiento, las organizaciones que los usan pueden caer en la tentación de desactivarlos o de limitar las medidas de seguridad para conseguir el alto rendimiento de red que requieren. Esta es una práctica arriesgada que debe evitarse.

Otro punto débil de la seguridad de red es el factor humano. Los criminales utilizan ataques phishing 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. Por otra parte, los empleados pueden perder sus dispositivos móviles o exponerlos a filtraciones de datos al utilizarlos fuera del perímetro de seguridad de la red.

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

Contraataque nº 3

Elija una plataforma de seguridad completa y de alto rendimiento que ofrezca una protección contra amenazas de nivel superior

Busque soluciones de seguridad con protección contra malware basada en la red, probada y certificada por la asociación independiente ICSA Labs.

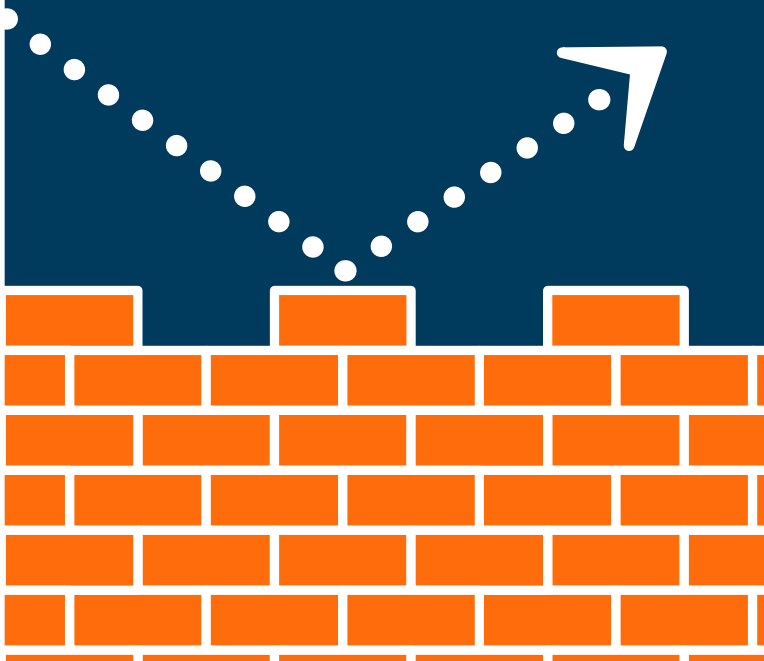
Plantéese un diseño de plataforma multinúcleo capaz de escanear archivos de cualquier tamaño y de cualquier tipo para poder reaccionar sin problemas a los cambiantes flujos de tráfico. Todos los firewalls necesitan un motor que proteja las redes contra los ataques tanto internos como externos sin sacrificar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

Busque un firewall que ofrezca un sandbox de red capaz de ayudarle a descubrir nuevas variantes de malware que posiblemente tengan su entorno en el punto de mira. Esto puede suponer la diferencia entre un día de trabajo normal y uno que recordará como el día en que sus archivos fueron secuestrados.

Su estrategia de seguridad debe incluir la protección de los puntos terminales 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.

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



Cada hora surgen nuevas amenazas en todos los continentes.

Estrategia de ciberataque nº 4

Transformación constante y ataques a escala global

Muchos ciberdelincuentes logran sus propósitos porque no cesan de reinventar nuevo malware ni de compartirlo con otros atacantes por todo el mundo. Esto significa que surgen nuevas amenazas cada hora en todos los continentes. Muchos de estos ciberdelincuentes 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. Luego repiten el ataque en otro sitio.

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 a la red por medio de dispositivos infectados que han sido utilizados fuera del perímetro de seguridad de la red.

SONICWALL®

Contraataque nº 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 los más rápidamente posible medidas contra las amenazas emergentes en el firewall, recurra a un proveedor de soluciones de seguridad que cuente con un equipo interno de expertos en métodos de respuesta rápida para contrarrestar los ataques. Además, ese equipo debería ampliar el alcance de sus actuaciones colaborando con la comunidad de seguridad global.

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 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 concreta.

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

Conclusión

Si bien los ciberataques aumentan exponencialmente, afortunadamente existen métodos de protección eficaces. Si desea evaluar las diferentes soluciones de contraataque disponibles a fin de hallar la que mejor se ajuste a su entorno de red, descargue el libro blanco Achieving Deeper Network Security (Claves para intensificar la seguridad de la red).

Acerca de nosotros

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-TypesOfCyberAttacks-EU-IMAG-24644

SONICWALL®