SONICWALL

RESUMEN EJECUTIVO: CÓMO LOS CIBERCRIMINALES PUEDEN ELUDIR SU GESTIÓN DE LA REPUTACIÓN

La evolución de la gestión de la reputación para la seguridad del correo electrónico

Resumen

A medida que avanza la tecnología, los cibercriminales desarrollan tácticas innovadoras para perpetrar nuevos ataques. Desarrollada en 1997, la lista negra en tiempo real RBL (Real-time Blackhole list) constituye la base del formato de la actual lista negra basada en DNS (DNSBL, DNS-based Blackhole List). No obstante, los cibercrminales perpetran ataques que minan y eluden los sistemas de gestión de la reputación de IP. Por ello, es importante que los profesionales de la seguridad evolucionen y se anticipen a este tipo de ataques para prevenirlos.

Cómo eluden los cibercriminales la gestión de la reputación basada en la IP

A medida que los sistemas de reputación de IP han ganado en popularidad, los hackers han centrado cada vez más recursos en socavarlos. Cada vez utilizan más e-mails de phishing en lugar de ataques de spam con el fin de camuflarse y hacerse pasar por fuentes fiables para utilizar su sistema de correo electrónico corporativo y sus empleados en su contra. Los phishers se hacen pasar por un partner o amigo de confianza, y los e-mails de phishing se centran o bien en comprometer servidores de correo electrónico legítimos de empresas con buena reputación o en violar cuentas de correo Web de ISPs o ASPs como Yahoo® o Gmail®. Esto permite a los criminales cibernéticos evitar o retrasar su inclusión en listas de sistemas de reputación de IP al enviar correo electrónico malicioso mezclado con mensajes inofensivos desde los servidores comprometidos de empresas legítimas.

Si bien los hackers manipulan sus direcciones de IP, no manipulan todos los aspectos de un mensaje de phishing o spam de forma uniforme. Al igual que otras entidades con ánimo de lucro, los cibercriminales reducen la complejidad para recortar

Para estar preparado frente a las amenazas de correo electrónico del futuro, debe aprender del pasado.

costes generales. Tienden a reutilizar direcciones de IP, así como contenidos, diseños, hiperenlaces e imágenes. Esto brinda la oportunidad de contar con una capa de defensa adicional basada en la identificación y gestión de la reputación más allá de las direcciones de IP.

¿Cómo hemos llegado hasta aquí? Evolución de la gestión de la reputación

El sistema original de gestión de la reputación del correo electrónico comenzó con la lista negra en tiempo real RBL. La primera RBL fue desarrollada en 1997 por Paul Vixie para el sistema de prevención de abuso del correo (MAPS, Mail Abuse Prevention System). Igual que un enlace de red que bloquea el tráfico entrante en lugar de reenviarlo, con el "blackhole" Vixie pretendía rechazar el tráfico de correo electrónico de las páginas que envían directamente o permiten el spam. La RBL original consistía en una lista de sitios sospechosos que se transmitía a los administradores de sistemas suscritos a través del protocolo BGP (Border Gateway protocol). Los suscriptores podían aplicar la lista para bloquear el tráfico TCP/IP procedente de esas páginas.

Mientras que las reputaciones de la RBL representaban un importante avance en la gestión del spam, también planteaba retos inherentes. El sistema MAPS verificaba meticulosamente los sitios antes de publicarlos en la lista. Si bien este método reducía los falsos positivos, al mismo tiempo mermaba considerablemente la capacidad de los suscriptores de responder con rapidez a los ataques. Con el tiempo, el MAPS desarrolló clientes RBL que se integraban con el software de correo electrónico para permitir a los administradores personalizar su propia RBL a fin de rechazar el correo electrónico entrante en base al servidor.

La RBL de MAPS sentó las bases para el desarrollo del formato DNSBL (Lista negra basada en DNS). El servicio de Internet de sistema de nombres de dominio (DNS) traduce los nombres de dominios/nombre de host a direcciones de IP (DNS directo) y las direcciones de IP a sus nombres de dominio/nombre de host (DNS inverso) con la ayuda de un servidor DNS. En lugar de ser sencillamente una lista aislada, una DNSBL añadía múltiples estándares para incluir y excluir direcciones de IP de forma dinámica. De este modo, los proveedores de servicios DNSBL podían distribuir listas actualizadas a través del servicio de nombres de dominio de Internet (IDNS) utilizando un formato estandarizado. Los primeros desarrolladores de DNSLBs añadieron criterios como si un servidor de correo electrónico remitente utilizaba proxies o relés abiertos potencialmente explotables, o si un servidor de correo enviaba spam a un sistema "honey pot" diseñado para atraer y recopilar spam para su identificación y análisis.

Actualmente, hay docenas de servicios DNSBL disponibles y la mayoría de servidores de correo electrónico pueden consultar estos servicios para verificar las reputaciones de las direcciones de IP. Sin embargo, estos servicios aplican diferentes estándares para añadir, eliminar o mantener direcciones de IP en sus listas. Por tanto, es posible que algunas listas no contengan direcciones de IP potencialmente peligrosas, o incluyan erróneamente direcciones válidas.

Conclusión

Los e-mails constituyen un vector de amenazas crítico que los cibercriminales utilizan constantemente para perpetrar sus ataques. Se ha comprobado que los e-mails de phishing son la zona cero de la mayoría de los ataques perpetrados con éxito contra redes de organizaciones. Con el aumento de los ataques de spear-phishing y whaling, cada vez es más difícil distinguir entre los e-mails maliciosos y las comunicaciones de negocio legítimas. Por tanto, es esencial que evalúe su gestión de la reputación y se asegure de que proporciona una defensa efectiva contra las amenazas de correo electrónico emergentes.

Obtenga más información. Lea nuestro resumen de la solución Gestión avanzada de la reputación para combatir las amenazas de correo electrónico.

Acerca de SonicWall

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