SONICWALL®

RESUMEN EJECUTIVO: 5 POSIBLES FALLOS DE LOS SANDBOXES DE SU FIREWALL

Lo que necesita saber para mantenerse un paso por delante de las amenazas persistentes avanzadas (APTs)

Una amenaza persistente avanzada (APT) es un conjunto de procesos continuos y sigilosos de hackeo informático, a menudo orquestados por criminales y dirigidos contra un blanco específico. Muchas veces, estas amenazas incluyen malware desconocido e indocumentado, como amenazas de día cero. Están diseñadas para ser cambiantes, polimorfas y dinámicas. Su objetivo consiste en extraer o comprometer datos sensibles, como información sobre identidades, accesos y controles. Si bien estos tipos de ataques son menos comunes que las amenazas estándar o las amenazas automatizadas, cuyos blancos son más amplios, las APTs suponen una amenaza importante.

Para poder detectar las APTs con mayor eficacia, los profesionales de seguridad están implementando tecnologías de detección de amenazas avanzadas, que a menudo incluyen sandboxes virtuales que analizan el comportamiento de los archivos sospechosos y descubren amenazas de malware ocultas, y hasta el momento desconocidas. Sin embargo, las amenazas cada vez son más inteligentes, y muchos proveedores no han logrado mantener sus técnicas de sanboxing a la altura. Este documento examina cinco ámbitos en los que las técnicas de sandboxing anticuadas no dan la talla, y explica qué necesita su empresa para mantenerse un paso por delante de las APTs.

Las tecnologías actuales de detección de amenazas avanzadas a menudo solo informan de la presencia y del comportamiento del malware.

1. Infiltración antes del análisis

En primer lugar, algunas soluciones de sandboxing solamente son capaces de emitir un veredicto del análisis después de que un archivo potencialmente peligroso haya invadido el perímetro de la red. Esto aumenta los posibles vectores que un archivo de malware ejecutado puede utilizar para infiltrar la red detrás del perímetro.

2. Análisis de archivos limitados

En segundo lugar, algunas soluciones de sandboxing en la pasarela están limitadas por el tamaño y el tipo de archivos o por el entorno operativo que pueden analizar. Es posible que solo sean capaces de analizar amenazas dirigidas contra un único entorno informático. Hoy en día, sin embargo, las empresas utilizan múltiples sistemas operativos, como Windows, Android y Mac OSX.

Por otra parte, el aumento de la adopción de dispositivos móviles y conectados ha ampliado la superficie de ataque para las amenazas. En 2015, Dell SonicWALL observó una amplia variedad de nuevas técnicas ofensivas y defensivas destinadas a reforzar los ataques contra el ecosistema Android, que representa casi el 85% de los teléfonos inteligentes de todo el mundo. Las tecnologías actuales de detección de amenazas avanzadas a menudo solo analizan y detectan amenazas dirigidas contra aplicaciones y sistemas operativos de oficina anticuados. Esto puede exponer a las organizaciones a ataques dirigidos contra entornos modernos con dispositivos móviles y conectados.

Además, es posible que no sean capaces de procesar una amplia variedad de tipos de archivos de negocio estándar, como los programas ejecutables (PE), DLL, PDFs, documentos MS Office, archivos, JAR y APK. El resultado de estas limitaciones puede ser la introducción de amenazas de día cero desconocidas en la red sin que hayan sido analizadas ni identificadas.

3. Motores de sandboxing basados en silos

Las soluciones de sandboxing individuales de terceros de un solo motor ya no son apropiadas.

Actualmente, el malware se diseña para detectar la presencia de un sandbox virtual y evadir la detección, lo cual limita la efectividad de las tecnologías de sandbox de primera generación. Las soluciones de sandboxing de un solo motor constituyen un blanco especialmente fácil para las técnicas de evasión.

Es más, las técnicas de un solo motor crean brechas en los análisis. Por ejemplo, los análisis que examinan las llamadas entre aplicaciones y sistemas operativos pueden ser menos granulares que los que se fijan en las llamadas entre el hardware y los sistemas operativos, ya que muchas de estas llamadas quedan ocultas de las capas de aplicación.

Resultaría más efectivo integrar capas de múltiples motores de sandboxing. Aún así, las soluciones de sandboxing de hoy en día a menudo son dispositivos independientes de un solo motor y basados en silos o servicios basados en la nube. La implementación de múltiples tecnologías de sandboxing, en el caso de que fuera viable, aumentaría considerablemente la complejidad de la configuración, la carga administrativa y los costes.

4. Amenazas cifradas

Desde hace muchos años, las instituciones financieras y otras empresas con acceso a información sensible optan por el protocolo seguro HTTPS para

cifrar la información que comparten. Ahora, otras páginas, como Google, Facebook y Twitter, también están adoptando esta práctica en respuesta a la creciente demanda de privacidad y seguridad de los usuarios. A pesar de que el mayor uso de tecnología de cifrado en Internet ofrece numerosas ventajas, también ha traído consigo otra tendencia emergente menos positiva, y es que los hackers están utilizando este cifrado para "ocultar" el malware de los firewalls corporativos.

Con el cifrado SSL/TLS (Capa de conexión segura/Seguridad de la capa de transporte), o el tráfico HTTPS, los perpetradores de ataques expertos pueden cifrar comunicaciones de comando y control y código malicioso para evadir los sistemas de prevención de intrusiones (IPS) y los sistemas de inspección antimalware. Estos ataques pueden ser extremadamente efectivos, simplemente porque la mayoría de las empresas no cuenta con una infraestructura apropiada para detectarlos. Las soluciones de seguridad de red anticuadas normalmente o bien no son capaces de inspeccionar el tráfico cifrado mediante SSL/TLS, o bien su rendimiento es tan bajo que no pueden utilizarse mientras se realiza la inspección.

5. Resolución complicada

Además, las tecnologías actuales de detección de amenazas avanzadas a menudo solo informan de la presencia y del comportamiento del malware. Incluso si la técnica de sandboxing identifica correctamente una variante reciente de una amenaza en un punto terminal específico, las organizaciones no disponen de una forma clara de resolver la amenaza. Carecen de un método sencillo y eficaz para actualizar las definiciones de los firewalls en una red global distribuida.

Una vez descubierto el malware — probablemente después de que se haya infectado el sistema— la resolución recae sobre el departamento de TI, que deberá dedicar una cantidad de tiempo considerable a localizar y erradicar el malware y reparar el daño resultante en los sistemas infectados. Asimismo, el equipo de TI deberá crear e implementar rápidamente nuevas definiciones de malware en toda la organización para prevenir que se produzcan más ataques.

¿Qué se necesita?

Si bien los sandboxes anticuados pueden tener sus defectos, el principio en que se basan es correcto. Sin embargo, para que el sandboxing pueda ser efectivo, deben subsanarse estos fallos. Para ello, su solución de sandboxing debería:

- Aplicar análisis basados en la nube a los archivos sospechosos para detectar y bloquear las amenazas desconocidas fuera de la pasarela hasta que se emita un veredicto
- Analizar una amplia variedad de tipos de archivos y entornos operativos, independientemente del tamaño de los archivos o del cifrado
- Actualizar las definiciones de forma rápida y automática
- Integrar múltiples motores de sandboxing para combatir mejor las técnicas de evasión, mejorar la visibilidad de los comportamientos maliciosos y aumentar la detección de amenazas
- Reducir los costes y la complejidad

Obtenga más información.

Descubra cómo el sandboxing multicapa detecta más amenazas de día cero. Vea el webcast a demanda.

Resultaría más efectivo integrar capas de múltiples motores de sandboxing.

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