SONICWALL

INFORME EJECUTIVO: EL LADO OSCURO DEL CIFRADO

Por qué su seguridad de red necesita descifrar el tráfico para detener las amenazas ocultas

Resumen

Actualmente, la mayoría de las sesiones web de los usuarios se cifran con cifrado Secure Sockets Layer/Transport Layer Security (SSL/TLS) o HTTPS, porque existe una enorme tendencia en el sector actual que desea moverse hacia una Internet cifrada para lograr dos objetivos clave:

- Dificultar la tarea de los delincuentes cibernéticos de ocultarse en las conexiones web
- Mantener la seguridad y la privacidad de la información personal

Mientras que estos delincuentes aumentan el uso del protocolo de cifrado, el cifrado se ha convertido en un vector de amenazas favorito para los hackers, ya que ocultan sus ataques, evaden los sistemas de defensa y, finalmente, abren puertas traseras directamente en su red. Después de todo, sus controles de seguridad no pueden detener lo que no pueden detectar. Si no se tratan, los ataques que utilizan SSL/TLS tendrán una tasa de éxito del 100 % en lo que respecta a poner en riesgo su red, lo que producirá pérdida de datos clasificados, direcciones IP y reputación.

El cifrado está en todas partes

Por lo general, SSL/TLS se utiliza para todo, desde el comercio electrónico hasta la banca en línea. El cifrado SSL/TLS se utiliza para proteger una cantidad cada vez mayor de tráfico empresarial y conforma la mayor parte del tráfico de red en algunos mercados verticales. A través de SSL se protegen los datos en movimiento ya que se crea un canal cifrado en las redes privadas o Internet pública, con lo cual se evita que los datos sean capturados o se vean afectados.

Además, SSL verifica que el destino final de los datos no quede en manos de un hacker que ataque el destino confiable. Los datos sensibles y fundamentales, como la información sobre tarjetas de crédito, nombres de usuarios y contraseñas, se transmiten de manera tal que a cualquier persona, excepto al destinatario previsto, le resulte difícil acceder a los datos. Si bien los sitios web y los servidores de FTP y telnet fueron los usuarios originales de SSL, hoy en día una amplia variedad de aplicaciones usan el protocolo, entre ellas, las aplicaciones basadas en Java, los servicios de administración de aplicaciones y los servicios basados en la nube. Facebook y Twitter son

Las soluciones de seguridad de red heredadas generalmente no tienen la capacidad para inspeccionar el tráfico con cifrado SSL/TLS o su rendimiento es tan bajo que se vuelven inutilizables cuando se lleva a cabo la inspección.

dos de las aplicaciones más populares con SSL habilitado. También están disponibles las funciones adicionales del navegador que pueden forzar el uso de SSL a través de HTTPS.

En el cuarto trimestre de 2015, las conexiones HTTPS (SSL/TLS) conformaron un promedio del 64,6 % de las conexiones web, lo que superó el crecimiento de HTTP a lo largo de la mayor parte del año. En enero de 2015, las conexiones HTTPS fueron el 109 % más que en el mes de enero de 2014. Además, cada mes a lo largo de 2015 tuvo un promedio de aumento del 53 % en comparación con el mismo mes del año 2014.

Los firewalls pueden verse afectados al inspeccionar el tráfico cifrado

Con SSL/TLS, los atacantes habilidosos 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 sumamente eficaces, simplemente porque la mayoría de las empresas no cuentan con la infraestructura adecuada para detectarlos. Las soluciones de seguridad de red heredadas generalmente no tienen la capacidad para inspeccionar el tráfico con cifrado SSL/TLS o su rendimiento es tan bajo que se vuelven inutilizables cuando se lleva a cabo la inspección. La inspección de tráfico HTTPS mediante un firewall de próxima generación (NGFW) requiere seis procesos de ejecución adicionales en comparación con la inspección de tráfico de texto sin formato.

Los dos procesos que más afectan al rendimiento son los siguientes:

- Establecer una conexión segura
- Descifrar y volver a cifrar el tráfico para un intercambio de datos seguro

La disminución del rendimiento puede ser elevada en algunos casos, por lo que, efectivamente, se prohíbe la inspección SSL/TLS para las empresas que operan con sistemas de seguridad heredados.

Gran parte de los ataques cibernéticos son oportunistas y, en su mayoría, se realizan por motivos económicos. Esto significa que todas las empresas corren el riesgo de verse afectadas.

Qué puede significar esto para su empresa

A lo largo del año, los atacantes aprovecharon al máximo esta falta de visibilidad, junto con el crecimiento del tráfico HTTPS. Mediante un ataque realizado precisamente de esta manera, a través de un anuncio en Yahoo, hasta 900 millones de usuarios se vieron expuestos al malware. Esta campaña redirigía a los visitantes de Yahoo a un sitio infectado con el conjunto de vulnerabilidades Angler. Probablemente, 10 millones de usuarios más se vieron afectados en las semanas previas a través del acceso a anuncios publicados por una empresa de marketing llamada E-planning.

Conclusión

El cifrado está en todas partes y, actualmente, es un vector de amenazas favorito para los hackers. Su seguridad de red necesita descifrar el tráfico para detener las amenazas ocultas.

Acerca de nosotros

Durante más de 25 años, SonicWall ha sido el socio de seguridad confiable del sector. Desde la seguridad de red y la seguridad de acceso hasta la seguridad en el correo electrónico, SonicWall ha evolucionado de manera continua su portafolio de productos a fin de posibilitar la innovación, la aceleración y el crecimiento de las empresas. Con más de un millón de dispositivos de seguridad en alrededor de 200 países y territorios en todo el mundo, SonicWall permite a sus clientes decir sí al futuro con confianza.

Si tiene alguna pregunta sobre el posible uso de este material, comuníquese con:

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

Visite nuestro sitio web para obtener más información.
www.sonicwall.com

SolutionBrief-DarkSideOfEncryption-EU-IMAG-22649