SONICWALL®

EL LADO OSCURO DEL CIFRADO

Los hackers han ampliado sus habilidades. Ahora son capaces de utilizar el tráfico SSL para ocultar sus ataques y el malware a fin de eludir los sistemas de seguridad.

97% de las empresas encuestadas están observando un aumento del tráfico Web cifrado[1]

130% de aumento de las amenazas que utilizan conexiones TLS/SSL desde 2014 hasta 2016[1]

80% de los encuestados han sido víctima de un ataque cibernético[2]

41% de los ataques están ocultos en tráfico SSL[2]

[1] *Research Study, NSS Labs, junio de 2016*
[2] *Research Study, Ponemon Study 2016*

Ataques que utilizan tráfico SSL para evadir la detección

Ataque oculto en tráfico "normal" del puerto 443

- El 78% piensa que es probable que sus organizaciones sean el blanco de un ataque de este tipo.
- Menos de un tercio (30%) de las organizaciones confían en su capacidad de resolver la situación.

Phishing

- El 79% cree que es altamente probable que su organización sufra un ataque de phishing.
- Solo el 17% afirma que su organización es capaz de mitigar un ataque de este tipo.

Malware que oculta datos salientes en el tráfico cifrado

- El 74% reconoce que se trata de un vector de ataque altamente probable.
- Tan solo el 16% afirma que su organización podría identificar y mitigar el ataque de malware cifrado mediante SSL antes de que se produzca la exfiltración de datos.

El perpetrador de un ataque podría ocultar el envío de datos salientes y/o robados a un servidor de comando y control

- El 66% afirma que la probabilidad de un evento de este tipo es elevada.
- El 26% cree que su organización podría detectar este comportamiento y prevenir la pérdida de datos.

Research Study, Ponemon Study 2016

Comprender el uso malicioso del cifrado

Solicitud de página: El equipo de un usuario (víctima A) visita una página legítima comprometida.

Ejecución del kit de exploits: Mientras se sirve el contenido Web al cliente, se descarga una pequeña pieza de software en el dispositivo del usuario, donde se ejecuta una secuencia de comandos para explotar las vulnerabilidades de software en el dispositivo cliente.

Solicitud de malware: Una vez que el operador del kit de exploits toma el control del equipo, se cursa un comando de solicitud a una página Web que hospeda malware y lo entrega.

Infección de malware: Ahora, la víctima A tiene malware instalado.

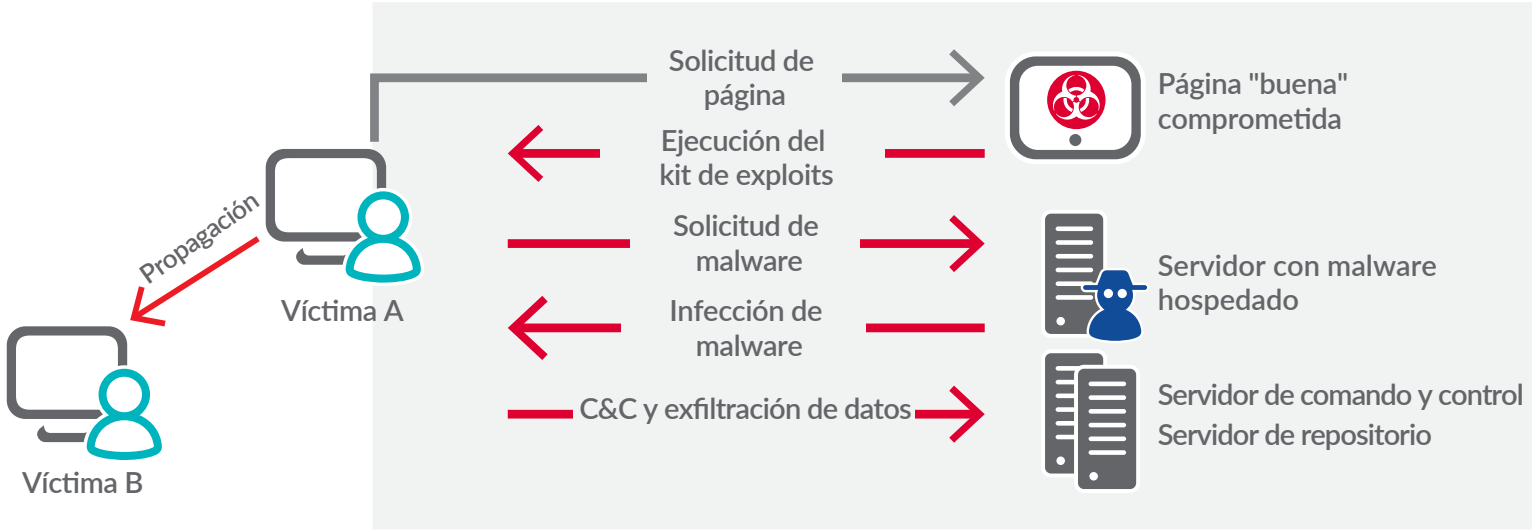
C&C: El malware se comunica con una infraestructura de comando y control para obtener más instrucciones.

Exfiltración de datos: Los datos del equipo de la víctima A se copian a un servidor externo para su procesamiento.

Víctima B: En este punto, los perpetradores de ataques a menudo amplían sus derechos de acceso, lo cual les permite moverse lateralmente por la red e infectar otros puntos terminales.

Cifrado: La nueva realidad es que el cifrado puede implementarse en cualquier fase del ataque para evadir la detección.

El cifrado puede implementarse en cualquier fase de un ataque



SONICWALL®

Tres barreras comunes para la inspección del tráfico SSL

Falta de herramientas de seguridad eficaces

Recursos insuficientes

Degradación del rendimiento

Fuente: Research Study, Ponemon Study 2016

SONICWALL®

El impacto sobre el rendimiento es una preocupación importante

- **El 61%** de los encuestados afirma que la falta de rendimiento es una preocupación para las organizaciones que no descifran el tráfico SSL*

- **El 83%** afirma que el descifrado deriva en algún tipo de degradación en las organizaciones que actualmente descifran e inspeccionan el tráfico SSL*

**Fuente: Research Study, Ponemon Study 2016*

Haga preguntas difíciles

- ¿Sabe si el firewall de su organización inspecciona o no el tráfico HTTPS?
- ¿Su organización ha experimentado interrupciones del servicio de la red o periodos de inactividad frecuentes como resultado del colapso total del rendimiento de su firewall al inspeccionar el tráfico HTTPS?
- ¿Cómo escala la protección del firewall para prevenir la degradación del rendimiento y el retraso y la latencia de su red al inspeccionar el tráfico HTTPS?

Recomendaciones

- Si no ha realizado una auditoría de seguridad recientemente, ahora es un buen momento para hacer una evaluación exhaustiva de la seguridad de la red a fin de identificar sus riesgos y necesidades.
- Actualice sus políticas de seguridad para defenderse contra un mayor espectro de vectores de amenazas y establezca múltiples métodos de seguridad para responder a ataques HTTP y HTTPS.
- Implemente un firewall de próxima generación con funciones de inspección SSL/TLS (Capa de conexión segura/Seguridad de la capa de transporte) de alto rendimiento. Asegúrese de poder inspeccionar todo el tráfico, independientemente de los puertos, protocolos y tamaños de los archivos, descomprimiendo y descifrando cada paquete y examinando cada byte para identificar las amenazas rápidamente.
- Las soluciones de sandboxing estándar no detectan el malware oculto en el tráfico cifrado. La inspección SSL/TLS es una necesidad, ya que se trata de un sandbox de red que bloquea el tráfico hasta que se emita un veredicto y no solo detecta los ataques de día cero, sino que también los previene automáticamente.
- Añada filtrado de contenido para evitar que los usuarios visiten páginas sospechosas, y utilice un antivirus de pasarela y un sistema de prevención de intrusiones para protegerles contra las páginas "buenas" comprometidas.
- Implemente cursos de formación continuos para que su personal sea consciente del peligro de los medios sociales, la ingeniería social, las páginas Web y descargas sospechosas y diversas amenazas de spam y phishing. Y, lo que es más importante, advierta a los usuarios de que nunca deben aceptar un certificado autofirmado e inválido.
- Proporcione una buena higiene cibernética, por ejemplo, asegurándose de que todo su software cuente con todas las actualizaciones de seguridad. Esto le ayudará a proteger todos los equipos contra exploits SSL más antiguos que ya hayan sido neutralizados.
- Establezca y ensaye su respuesta y su plan de resolución. Ponga su plan a prueba regularmente, realice simulaciones como si de un simulacro de incendio se tratara, mejore el proceso y aumente la eficacia y la preparación del personal que debe responder inmediatamente para que ejecuten los planes de resolución tal y como se han diseñado.

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