DETENGA LOS ATAQUES DIRIGIDOS SIN DESCIFRAR EL TRÁFICO

Resumen Ejecutivo

Los atacantes son astutos. Emplean una variedad de técnicas para ocultar sus ataques y evadir la detección. Ahora que el tráfico HTTPS representa dos tercios de todo el tráfico web,[1] el cifrado se ha convertido en su método elegido para eludir las defensas corporativas. El cifrado es solo una de las tantas tácticas colectivas de evasión que tienen los atacantes en la manga; también codifican contenidos del tráfico, comprimen y empaquetan archivos e implementan muchas otras técnicas para esquivar los controles de seguridad.

Los análisis de comportamiento de Magnifier™, una aplicación basada en la nube del Application Framework de Palo Alto Networks®, empodera a las organizaciones para detectar y detener los ataques. Magnifier genera un perfil con el comportamiento del usuario y del dispositivo al analizar los metadatos de la red para descubrir las señales que delaten una intrusión. Sin embargo, al no necesitar inspeccionar el contenido del tráfico, es inmune a las técnicas de cifrado y de ofuscación.

Este documento describe cómo Magnifier detecta los ataques en curso y cómo trabaja en concordancia con la Security Operating Platform de Palo Alto Networks para erradicar las amenazas en el tráfico cifrado.

1. Let's Encrypt with Firefox telemetry, https://letsencrypt.org/stats

El Ascenso del Cifrado SSL

El uso de Secure Sockets Layer (Capa de Sockets Seguros), o cifrado SSL[2], se ha disparado a lo largo de la última década: creció de aproximadamente un 26 % de todo el tráfico de Internet en enero del 2014 al 69 % en febrero del 2018[3]. La creciente preocupación por la privacidad y estímulos de la industria por adoptar el cifrado han motivado a los propietarios de las aplicaciones de todos los tamaños a cifrar el acceso a sus sitios web. Además, la rápida proliferación de certificados SSL gratuitos, o de bajo costo, hizo que el cifrado sea accesible prácticamente para todos los desarrolladores web.

Si bien la adopción de SSL potencia la privacidad y la seguridad, también permite que los atacantes oculten su actividad maliciosa en el tráfico cifrado. Para proteger los recursos corporativos, las organizaciones necesitan métodos robustos de detección y bloqueo de amenazas ocultas en las comunicaciones SSL.

Enfoque de Seguridad del Tráfico Cifrado de Palo Alto Networks

Para garantizar que ningún ataque quede sin ser detectado, Palo Alto Networks desarrolló múltiples tecnologías para inspeccionar y proteger todas las comunicaciones, incluso el tráfico cifrado. Estas tecnologías incluyen:

Analítica de Comportamiento

Una vez que los atacantes se infiltraron en una red, deben ejecutar una serie de pasos para encontrar y robar o destruir datos. La analítica de comportamiento Magnifier monitorea la actividad de red para generar perfiles de comportamiento y detectar anomalías que indiquen que ha ocurrido una intrusión.

Como Magnifier analiza los metadatos de la red, en lugar del contenido real, puede detectar los ataques avanzados sin necesidad de descifrado.

Descifrado SSL de Alto Rendimiento

Para inspeccionar cada paquete, los firewall de nueva generación pueden descifrar el tráfico HTTPS a alta velocidad. Al ser compatible con opciones flexibles de implementación, los firewalls de nueva generación pueden descifrar tráfico SSL entrante o saliente o actuar como intermediario de descifrado SSL.

Al utilizar firewalls de nueva generación, las organizaciones pueden descifrar el tráfico de forma selectiva por aplicación, categoría o usuario.

Advanced Endpoint Protection

Los ataques escondidos en el tráfico HTTPS finalmente se dirigen a los endpoints y sus datos.

Traps™ advanced endpoint protection utiliza múltiples métodos de prevención para detener a los exploits y al malware antes de que puedan poner en peligro a los equipos corporativos. Se integra con la seguridad de la red y de la nube para realizar análisis de amenazas, información compartida y contención automatizada.

La Security Operating Platform de Palo Alto Networks provee una protección blindada contra los ciberataques al mismo tiempo que elimina los puntos ciegos que pueda introducir el tráfico cifrado.

Detección de Amenazas Internas Sin Descifrado de Tráfico

Cuando los atacantes acceden a la red de una de sus víctimas, pueden utilizar cualquier cantidad de técnicas de evasión para eludir los controles de seguridad. En lugar de confiar en el malware, ellos pueden aprovechar las herramientas comunes, como PowerShell® o un sistema de herramientas nativo, para explorar una red comprometida y transferir los datos. Los atacantes pueden robar las credenciales y transferirlas de endpoint a endpoint sin cometer infracciones a las políticas de seguridad o activar alarmas internas necesariamente.

Sin embargo, los atacantes se traicionarán a sí mismos inevitablemente al realizar actividades de reconocimiento y dejar su huella a través de la red porque sus acciones se distinguirán del comportamiento anterior y del comportamiento de otros usuarios o dispositivos en la red. Cuando intenten explorar la red y controlar otros dispositivos, ellos van a acceder a nuevos destinos, usar nuevos protocolos, ingresar a los sistemas con cuentas de usuario inusuales y mostrar otros cambios en su comportamiento que revelarán su intención maliciosa.

La analítica de comportamiento de Magnifier, una aplicación basada en la nube del Application Framework de Palo Alto Networks, detecta automáticamente las anomalías en el comportamiento que indican que existen ataques activos. Magnifier examina abundantes datos de la red, los endpoints y la nube almacenados en el Logging Service de Palo Alto Networks para identificar ataques dirigidos, amenazas internas maliciosas y endpoints comprometidos con una precisión sin igual (ver Figura 1). También optimiza las investigaciones al proporcionar un número reducido de alertas accionables, con el contexto que necesitan los analistas de seguridad para confirmar y responder a los ataques.

2. Las referencias en este documento sobre el cifrado SSL también aplican al Transport Layer Security o TLS, el sucesor de SSL.
3. Let's Encrypt with Firefox telemetry, https://letsencrypt.org/stats/

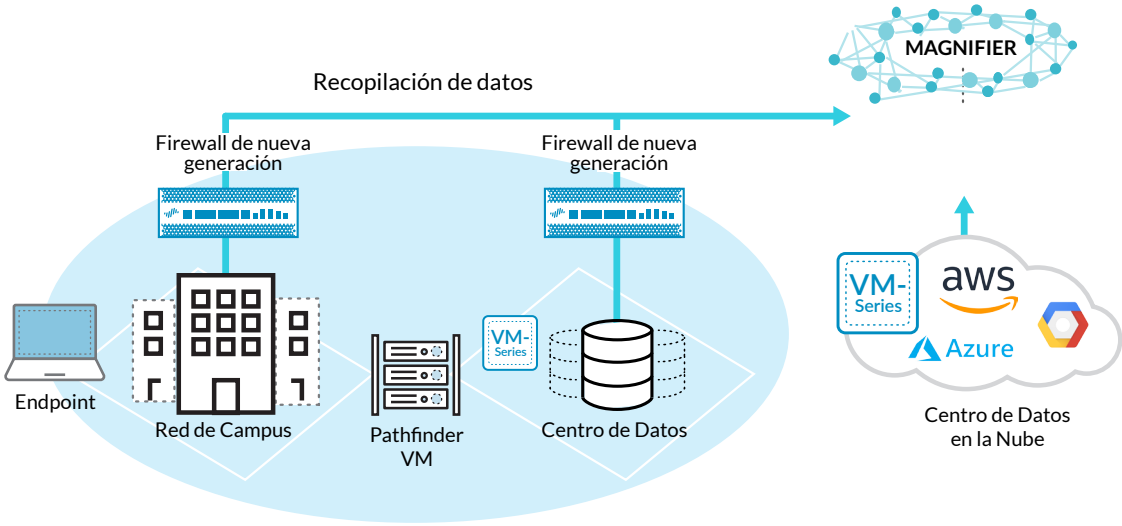


Figura 1: Magnifier analiza los datos almacenados en el Logging Service de Palo Alto Networks desde la Security Operating Platform para generar perfiles de comportamiento y detectar ataques

Diseño Resistente a Evasiones

En lugar de buscar las firmas de un ataque, Magnifier genera perfiles de comportamiento de los usuarios y los dispositivos para detectar anomalías que indiquen la presencia de un ataque. Su robusto sistema de detección de ataques no está basado en el contenido transferido sino en los atributos de la comunicación que incluye qué usuario y host iniciaron la conexión, qué destino accedieron y qué protocolo usaron.

Dado que Magnifier no está diseñado para detectar patrones predefinidos de la red (por ejemplo, el comportamiento específico de las familias de malware), los atacantes no pueden evadir tan fácilmente los algoritmos de detección de Magnifier con solo cambiar la longitud de los paquetes o los códigos de exploits. Mediante el aprendizaje dinámico del comportamiento de los usuarios y los dispositivos en la red, Magnifier detecta los cambios de comportamiento que los atacantes no pueden ocultar. Por ejemplo, cuando un atacante se traslada lateralmente de un host a otro, no puede evitar la comunicación entre ambas máquinas.

Magnifier detecta los comportamientos de los ataques basados en la red que son imposibles de esconder, incluso dentro del tráfico cifrado.

Al generar perfiles de tantas diferentes dimensiones de comportamiento, Magnifier puede detectar las irregularidades que sugieren que hay un ataque en curso, por ejemplo cuando un usuario estándar se conecta a múltiples sistemas a los que rara vez se accede o intenta administrar computadoras remotas.

Como Magnifier analiza los metadatos de la red, y no el contenido o las cargas transferidas, puede descubrir las amenazas de la red, incluso en aquellos entornos donde el tráfico está cifrado.

Detecte Cada Paso de un Ataque en Curso con Analítica de Comportamiento

Una vez que el atacante se infiltró en una red, puede aprovechar el acceso vigente para explorar su entorno y expandir su campo de control hasta alcanzar su objetivo final: robar, manipular o destruir datos confidenciales.

Magnifier detecta cada paso que da el atacante una vez que este logra un punto de apoyo en la red:

Movimiento lateral: para encontrar datos confidenciales y mantener una presencia peristente en la red, los atacantes roban credenciales, realizan tareas de reconocimiento y toman control de múltiples endpoints. Magnifier monitorea el tráfico de red para establecer un modelo del comportamiento esperado y detectar las desviaciones que sugieren la presencia de un ataque. Magnifier genera perfiles de comportamiento de usuarios y dispositivos mediante el análisis de los metadatos a nivel de protocolo recopilados por los firewalls de nueva generación de Palo Alto Networks.

Al analizar los datos de red recopilados por los firewalls de nueva generación (incluidos los registros de aplicaciones y los registros de tráfico optimizados con datos de las tecnologías User-ID™ y App-ID™), Magnifier puede detectar el movimiento lateral y las tareas de reconocimiento que los atacantes no pueden evitar ni ocultar.

Actividad de Comando y Control: Magnifier reconoce el comportamiento de red asociado a las actividades de comando y control, o C2, como las conexiones repetidas a sitios a los que raramente se accede o varias búsquedas fallidas de DNS. Como resultado, Magnifier puede detectar ataques sin inspeccionar el contenido transferido.

Además, como los firewalls de nueva generación de Palo Alto Networks pueden extraer la Indicación del Nombre del Servidor y demás datos pertinentes del tráfico cifrado y presentar estos datos en registros optimizados de aplicaciones, Magnifier puede detectar el tráfico C2 incluso cuando las conexiones a los servidores C2 están cifradas.

Exfiltración de Datos: Luego de obtener datos confidenciales, los atacantes necesitan transferirla fuera de la red. Magnifier examina las conexiones salientes y detecta las cargas grandes subidas a aquellos sitios a los que rara vez se accede o aquellas que utilizan protocolos poco frecuentes.

Como Magnifier pone el foco en la cantidad de datos enviados, el número de puerto, la popularidad y demás atributos del sitio de destino, puede detectar la exfiltración incluso cuando el tráfico de carga está cifrado o el contenido camuflado.

Endpoints comprometidos: Al utilizar Pathfinder, el servicio de análisis de endpoints, Magnifier puede descubrir malware que se ejecute en los endpoints.

Dado que Pathfinder escanea la ejecución de procesos directamente en los endpoints y luego los examina con WildFire®, el servicio de análisis de amenazas en la nube, el cifrado a nivel de la red no lo afecta.

Cómo Genera Magnifier los Perfiles de Comportamiento Cuando el Tráfico está Cifrado

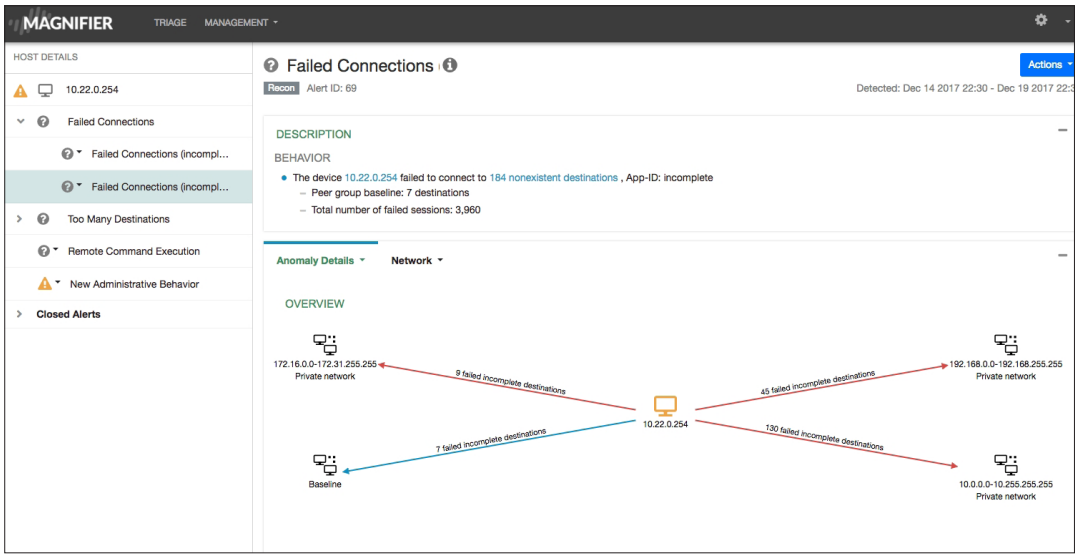
Magnifier detecta los ataques incluso cuando los atacantes intentan usar cifrado o técnicas de ofuscación para evadir la detección. El cifrado a nivel de las aplicaciones no afecta la precisión de los algoritmos de detección de ataques de Magnifier por las razones que se exponen a continuación.

Analiza la Información a Nivel de la Red

Magnifier analiza, en primer lugar, la información a nivel de la red (por ejemplo, la fuente de tráfico, destino, dominio, protocolo, número puerto y volumen), que se puede obtener de los encabezados de paquetes incluso cuando el contenido a nivel de la aplicación está cifrado. Es decir, si un atacante intenta trazar un mapa de la red para encontrar servidores con datos valiosos, no podrá evitar las conexiones de red anormales.

Magnifier analiza los datos recopilados por los firewall de nueva generación para rastrear el comportamiento normal de usuarios y dispositivos, incluidos los sistemas a los que acceden, los protocolos que usan, la cantidad de tráfico que envían y reciben, y muchas otras dimensiones de comportamiento. Si Magnifier detecta una actividad inusual (como solicitudes a muchos puertos en un solo host, incluso puertos anómalos para este usuario individual y sus pares) generará una alerta. Magnifier puede detectar ataques sin inspeccionar el contenido de las aplicaciones, es decir, el cifrado a nivel de aplicación no lo afecta (ver Figura 2).

Figura 2: Magnifier detecta los escaneos de puerto en la red incluso si las solicitudes individuales están cifradas



Optimiza los Esfuerzos de Detección de Amenazas

Magnifier fue diseñado desde el principio para optimizar los esfuerzos de detección de amenazas. Con ese fin, genera una pequeña cantidad de alertas precisas y accionables con contexto de usuario, endpoint y aplicación. Si bien el cifrado no afecta la capacidad de detección de Magnifier, sí puede, en algunos casos, afectar la cantidad de información grabada en las alertas. Aun cuando el tráfico está cifrado, las alertas de Magnifier incluirán la información sobre el dispositivo, el usuario, el número de puerto y el proceso del endpoint o el archivo ejecutable relacionado con el ataque, así como la información sobre el dominio. Sin embargo, es posible que las alertas no enumeren la URL, el agente del navegador o el sitio de referencia de los ataques basados en HTTPS. Incluso en estos casos, Magnifier detectará los ataques, pero no proporcionará la información detallada de la aplicación que incluye usualmente en las alertas.

Incluye Detalles Completos de las Aplicaciones en las Alertas

Magnifier incluye los detalles completos de las aplicaciones en las alertas cuando las organizaciones configuran sus firewalls de nueva generación para descifrar el tráfico HTTPS. Con la configuración adecuada, los firewalls registrarán todos los metadatos de la red en las alertas (incluso agentes de navegación web, sitios de referencia y nombres de

archivos) para optimizar las investigaciones. Al configurar sus firewalls para descifrar el tráfico, las organizaciones también pueden aprovechar las políticas basadas en aplicaciones, usuarios y contenido de sus firewalls así como las capacidades de prevención de amenazas para bloquear accesos no autorizados, exploits y malware.

Cuando un atacante penetra una red, la organización a la que dirige su ataque cuenta con la ventaja de ser local. Sus equipos de TI y de ciberseguridad controlan los derechos de dispositivos, aplicaciones y usuarios; pueden monitorear la actividad de red para detectar comportamientos anómalos. Magnifier proporciona una visibilidad sin precedentes en el tráfico interno de la red y habilita a las organizaciones para descubrir las amenazas internas, incluso cuando el tráfico está cifrado.

Datos de Red Inspeccionados por Magnifier

Magnifier analiza los metadatos a nivel de protocolo en los registros de tráfico, en los registros optimizados de las aplicaciones y los registros de amenazas que recopilan los firewalls de nueva generación de Palo Alto Networks. No necesita inspeccionar el contenido transferido ni las cargas. Al crear un perfil basado en más de 1000 dimensiones de comportamiento que incluyen frecuencia de conexión, fuente y destino del tráfico, protocolos utilizados y más, Magnifier puede aprender el comportamiento esperado de usuarios y dispositivos. Magnifier también monitorea el tráfico interno así como el tráfico externo de clientes y servidores hacia Internet.

Datos a Nivel de Sesión

Los firewalls de nueva generación de Palo Alto Networks extraen los metadatos necesarios para generar los perfiles de comportamiento de usuarios y dispositivos, incluso:

- IP de origen, IP de destino, puerto de origen, puerto de destino;
- Bytes enviados y recibidos;
- Duración de conexión;
- Registros optimizados de aplicaciones con datos a nivel de transacciones en DNS, HTTP, DHCP, RPC, ARP, ICMP, y más;
- Detalles de aplicaciones con App-ID.

Información de Usuarios

Magnifier analiza el tráfico de la red y los datos de los endpoints y extrae el contexto del usuario, por ejemplo:

- Usuario registrado;
- Usuario típico de la máquina;
- Usuario generador del proceso que inició la comunicación.

Información del Host

Magnifier identifica las máquinas al rastrear:

- Nombre de host;
- Dirección MAC.

Encuentre los Ataques en el Tráfico Cifrado con Palo Alto Networks

Los atacantes pueden desarrollar técnicas nunca antes vistas para engañar a los usuarios y comprometer a los endpoints. Con la rápida adopción del cifrado SSL, pueden esconder sus ataques en el tráfico HTTPS para evadir los controles de seguridad. Una vez que se infiltraron en la red, sin embargo, deben llevar a cabo un proceso escalonado de reconocimiento y de movimiento lateral para lograr acceder a los recursos valiosos.

Palo Alto Networks brinda defensas poderosas contra los ciberataques, especialmente aquellos que acechan en el tráfico cifrado. Los firewalls de nueva generación de Palo Alto Networks pueden descifrar el tráfico para inspeccionar y bloquear los ataques en la red. Traps advanced endpoint protection protege los objetivos finales de los ataques (incluso laptops, computadoras personales, servidores y dispositivos IoT) de las amenazas más sofisticadas.

Muchas veces los adversarios humanos que operan dentro de la red, como los atacantes externos o actores internos maliciosos, pueden evitar el uso de exploits tradicionales para no ser detectados. Al generar de perfiles de comportamiento de usuarios y dispositivos, las organizaciones pueden detectar los cambios de comportamiento que revelan la presencia de un ataque activo. Magnifier se centra en los metadatos de la red, y no en el contenido de las aplicaciones, para generar perfiles de comportamiento de usuarios y dispositivos aun cuando el tráfico esté cifrado. Al monitorear la actividad interna en busca de comportamiento anómalo, Magnifier puede detectar los ataques automáticamente y dar a las organizaciones el poder de evitar costosas brechas de datos.

3000 Tannery Way
Santa Clara, CA 95054

Línea principal: +1.408.753.4000
Ventas: +1.866.320.4788
Soporte técnico: +1.866.898.9087

www.paloaltonetworks.com