THREAT PREVENTION

Protección completa de comando y control, exploits y malware para su red

Las organizaciones se enfrentan a un torrente de ataques por parte de los autores de las amenazas en todo el mundo, cuyo objetivo es enriquecerse. Hoy en día, los atacantes cuentan con un buen equipamiento y una buena financiación. Utilizan tácticas evasivas para conseguir un punto de apoyo en su red y lanzan ataques sofisticados y de gran volumen mientras permanecen desapercibidos frente a las defensas tradicionales de las organizaciones, aplicando técnicas que van desde el cifrado, el malware polimórfico y la ofuscación de paquetes, hasta las cargas de varias fases y el DNS de flujo rápido.

El servicio Threat Prevention, especialmente diseñado dentro de la plataforma de seguridad de nueva generación de Palo Alto Networks®, protege las redes en diferentes fases del ataque:

- Analiza todo el tráfico en pleno contexto de aplicaciones y usuarios.
- Previene las amenazas en cualquier fase del ciclo de vida del ciberataque.
- Su arquitectura de análisis de un único paso permite un gran rendimiento sin poner en peligro la seguridad.
- Posibilita las actualizaciones diarias automáticas para detectar amenazas recién descubiertas, con prevenciones disponibles en 300 segundos en el caso de los exploits y el malware de día cero, a través del servicio de análisis de amenazas basado en la nube de WildFire™.
- Utiliza una automatización revolucionaria que permite generar firmas de comando y control a velocidad y escala industriales.

Por si fuera poco, los productos de seguridad de la red todavía usan las mismas estrategias de defensa que se empleaban antes de que evolucionara el panorama de amenazas. El tráfico solo se inspecciona en algunos puertos y, aunque incorporar dispositivos de función única a la pila de defensa podría ayudar a resolver parcialmente un problema en concreto, genera poca visibilidad y un nivel de rendimiento bajo. Esto ha llevado a una situación peligrosa, donde existen fisuras en la defensa de la red porque las soluciones de seguridad están fracturadas y son difíciles de gestionar, mientras que los atacantes son cada vez más hábiles a la hora de penetrar en ellas.

Habilite la aplicación y evite la amenaza

Las aplicaciones son una parte integral de la forma en que las empresas desarrollan sus negocios. Por este motivo, están a entera disposición de los usuarios, ya que se han incorporado a la red a través de canales cifrados, mediante puertos no estándares y pasando de un puerto abierto a otro para garantizar que siempre puedan acceder a ellas.

Desafortunadamente, las amenazas avanzadas se aprovechan de la forma en que las aplicaciones quedan a disposición de los usuarios y las utilizan para penetrar en la red sin ser detectadas. Se camuflan en las aplicaciones, se ocultan en el tráfico cifrado de SSL y se aprovechan de los usuarios desprevenidos para penetrar en la red y ejecutar su actividad maliciosa.

Nosotros protegemos su red frente a estas amenazas proporcionando varias capas de prevención y enfrentándonos a las amenazas en cada frase del ataque. Además de estas capacidades de prevención de intrusiones tradicionales, proporcionamos la capacidad exclusiva de detectar y bloquear amenazas en cualquiera de los puertos, en lugar de invocar a las firmas a partir de un conjunto limitado de puertos predefinidos. Utilizando la tecnología de identificación de aplicaciones App-ID™ y la tecnología de identificación de usuarios User-ID™ con nuestro cortafuegos de nueva generación, que identifica todo el tráfico en todos los puertos y lo enmarca en un contexto, el motor Threat Prevention nunca pierde de vista la amenaza, sea cual sea la técnica de evasión que utilice.

La suscripción a Threat Prevention incluye sistemas de prevención de intrusiones, de protección de red antimalware y de comando y control (CnC).

Elimine amenazas en todas las fases

En prácticamente todas las brechas que han ocurrido recientemente, las organizaciones objetivo tenían una herramienta de defensa de función única en funcionamiento que consiguió evitarse durante el ataque.

- El análisis heurístico, que detecta paquetes y patrones de tráfico anómalos como exploraciones de puertos, limpiezas de host y ataques de saturación por denegación de servicio (DDoS).
- Otras funciones de protección contra ataques, como el bloqueo de paquetes no válidos o malformados, la desfragmentación de IP y el reensamblaje de TCP, se emplean como formas de protección contra los métodos de evasión y ofuscación que utilizan los atacantes.
- Las firmas fáciles de configurar y de vulnerabilidad personalizada le permiten adaptar las capacidades de prevención de intrusiones a las necesidades exclusivas de su red.

Palo Alto Networks utiliza tecnologías de defensa integradas de forma nativa para garantizar que, cuando una amenaza consigue zafarse de una tecnología, otro sistema la detecte. La clave para una protección eficaz consiste en utilizar las funciones de seguridad diseñadas específicamente para compartir información y proporcionar contexto acerca del tráfico que se está analizando y las amenazas que se están identificando y bloqueando.

Intrusion Prevention (IPS)

Las protecciones basadas en amenazas detectan y bloquean intentos de exploit y técnicas evasivas tanto en las capas de red como en la de aplicación, incluidos análisis de puertos, desbordamientos de búfer, ejecución de códigos remotos, fragmentación de protocolos y métodos de ofuscación. Estas protecciones están fundamentadas en la comparación de firmas y la detección de anomalías. Mediante estos dos procedimientos, se descifran y analizan protocolos, y se emplea la información obtenida para enviar alertas al sistema y bloquear los patrones de tráfico malicioso. La comparación de patrones de estado detecta los ataques entre varios paquetes, teniendo en cuenta el orden y la secuencia de llegada y asegurándose de que todo el tráfico permitido sea bienintencionado y no emplee técnicas de evasión.

- El análisis de descodificador de protocolo, que descifra mediante estados el protocolo y aplica de forma inteligente firmas para detectar exploits de aplicación y redes.
- Debido a que existen varias formas de aprovechar una única vulnerabilidad, nuestras firmas de prevención de intrusión se crean a partir de la vulnerabilidad en sí, proporcionando una protección más completa frente a una amplia gama de exploits. Una única firma puede detener varios intentos de exploit en una vulnerabilidad de aplicación o sistema conocida.
- La protección de anomalías de protocolo, que detecta el uso del protocolo que no cumple con el RFC, como los inicios de sesión a URI o FTP excesivamente prolongados.
- Las firmas fáciles de configurar y de vulnerabilidad personalizada nos permiten adaptar las capacidades de prevención de intrusiones a las necesidades exclusivas de su red.

Protección de malware

La protección de malware en línea bloquea el malware antes de que llegue al host objetivo a través de firmas basadas en cargas y no en hash. Las protecciones de malware de Palo Alto Networks bloquean el malware conocido y las futuras variantes de dicho malware, incluidas aquellas que no se hayan visto nunca antes. Nuestro motor de análisis basado en flujos de datos protege la red sin introducir un grado de latencia significativo, que es precisamente uno de los principales inconvenientes de las ofertas de antivirus de red, que dependen de los motores de análisis basados en proxy. El análisis de malware basado en flujo de datos inspecciona el tráfico en cuanto se reciben los primeros paquetes de un archivo. De esta forma, se eliminan las amenazas, así como los problemas de rendimiento relacionados con soluciones independientes tradicionales. Entre las capacidades antimalware clave se incluyen las siguientes:

- Detección en línea basada en flujo de datos y prevención del malware oculto en archivos comprimidos y el contenido web.
- Protección frente a cargas ocultas en tipos de archivos comunes, como documentos de Microsoft® Office y archivos PDF.
- Actualizaciones de WildFire, que garantizan la protección frente al malware de día cero.

Palo Alto Networks recopila miles de millones de muestras activas y genera, a partir de estas, firmas de todos los tipos de malware. Entre estas, se incluye el malware anteriormente desconocido enviado a WildFire, al equipo de investigación de amenazas Unit 42 y a otros socios de tecnología e investigación externos de todo el mundo.

Protección de sistemas de comando y control (spyware)

Sabemos que no existe ninguna cura milagrosa que permita que su red quede totalmente blindada frente a las amenazas. Una vez que se ha producido la infección inicial, los atacantes se comunican con la máquina del host a través de un canal de comando y control (CnC), que utilizan para obtener más malware, emitir instrucciones y robar datos. Nuestros sistemas de protección de CnC se centran en esos canales de comunicación no autorizados y proceden a su cierre bloqueando las solicitudes salientes a dominios maliciosos y de kits de herramientas de CnC conocidos instalados en los dispositivos infectados. Palo Alto Networks no se limita a la automatización estándar de firmas CnC basada en URL y dominios, sino que también genera, de forma automática, firmas CnC basadas en patrones, lo que se traduce en el suministro de firmas CnC de investigador a escala y velocidad industriales.

Firmas basadas en cargas frente a firmas basadas en hash

Las firmas basadas en cargas detectan patrones en el cuerpo de los archivos que después se utilizan para identificar variaciones futuras en ellos, pese a que su contenido se haya modificado ligeramente. Este procedimiento permite identificar y bloquear de forma inmediata malware polimórfico que, de otro modo, se habría considerado como un archivo desconocido nuevo.

Las firmas basadas en hash se comparan con la codificación fija específica de cada archivo. Ya que un archivo hash se modifica fácilmente, las firmas basadas en hash no son muy eficaces a la hora de detectar un malware polimórfico o las variantes de un mismo archivo.

Analizar todas las amenazas en un único paso

El motor de Threat Prevention de Palo Alto Networks representa una primicia en el sector, puesto que, además de inspeccionar y clasificar el tráfico, detecta y bloquea exploits de vulnerabilidad y malware en un único paso. Las tecnologías de prevención de amenazas tradicionales exigen dos o más motores de análisis, lo que supone un nivel de latencia adicional en el sistema y ralentiza el rendimiento drásticamente. Utilizamos un formato de firma

uniforme para todas las amenazas, lo que permite garantizar un proceso más rápido al llevar a cabo todos los análisis en un único sistema integrado. Esto elimina los procesos redundantes comunes a las soluciones que utilizan varios motores de análisis.

La tecnología Threat Prevention analiza cuidadosamente cada paquete a medida que penetra en la plataforma, revisando detalladamente las secuencias de bytes del encabezado del paquete y de la carga. A partir de este análisis, podemos identificar detalles importantes del paquete, incluida la aplicación utilizada, el origen y el destino, si el protocolo cumple con RFC y si la carga contiene un exploit o código malicioso. Además de los paquetes individuales, también analizamos el contexto proporcionado por el orden de llegada y la secuencia de los distintos paquetes para detectar y evitar las técnicas de evasión. Todo este procedimiento de análisis y comparación de firmas ocurre en una sola exploración, por lo que el tráfico de red mantendrá la velocidad de rendimiento que necesita.

Integración de la suscripción a Threat Prevention con WildFire

Las organizaciones pueden ampliar su protección de exploits y malware de día cero con el servicio WildFire. WildFire es el motor de análisis y prevención más avanzado del sector para hacer frente a exploits y malware de día cero especialmente evasivos. El servicio basado en la nube adopta un exclusivo enfoque de varias técnicas en el que confluyen los análisis dinámico y estático, innovadores mecanismos de aprendizaje automático y un entorno de análisis pionero basado en hardware para detectar y prevenir incluso las amenazas más escurridizas.

Reducción de la superficie de ataque

Descifrado SSL

Prácticamente un 40 % del tráfico de red de una empresa se cifra mediante SSL, lo que provoca fisuras en las defensas de red si este no se descifra y se analiza en busca de amenazas. Nuestra plataforma tiene un descifrado SSL integrado, que puede utilizarse de forma selectiva para descifrar el tráfico SSL entrante y saliente. Una vez que todo el tráfico se ha descifrado y se confirma que es seguro, se vuelve a cifrar y se reanuda la transferencia hasta su destino.

Bloqueo de archivos

Alrededor del 90 % de los archivos maliciosos que se utilizan en los ataques de spear phishing son ejecutables. Este hecho, combinado con la afirmación de que casi el 60 % de los incidentes de seguridad son el resultado de una negligencia por parte del empleado, implica que es posible que sus usuarios no sepan qué elementos son seguros y cuáles no. Para reducir las probabilidades de que ocurra una infección de malware, deberá evitar que los tipos de archivos peligrosos que ocultan malware, como los ejecutables, penetren en su red. La funcionalidad de bloqueo de archivos puede combinarse con User-ID para bloquear los archivos innecesarios según las funciones de los puestos de cada usuario, lo que le garantizará que todos los usuarios tengan acceso a los archivos que necesitan y, a la vez, le proporcionará un procedimiento exhaustivo para reducir su exposición a riesgos que sea acorde a los distintos requisitos de su organización. Y, si todavía desea reducir aún más el número de oportunidades de ataque, puede enviar todos los archivos permitidos a WildFire para que se analicen y determinar si contienen malware de día cero.

Protección frente a descargas ocultas

Los usuarios confiados pueden descargar involuntariamente malware simplemente visitando su página web favorita. A menudo, es posible que incluso el usuario o el propietario del sitio web no sean conscientes de que el sitio está dañado. Nuestra tecnología Threat Prevention identifica las descargas potencialmente peligrosas y envía una advertencia al usuario para garantizar que la descarga es intencionada y está autorizada por este. Evite ataques de dominios nuevos y que cambian constantemente asociando esta función a las políticas de bloqueo de archivos y filtrado de URL.

Sistema de mitigación fácil y preciso

DNS Sinkhole

Nuestro servicio de protección CnC da un paso más allá proporcionando capacidades sinkhole para las solicitudes salientes a entradas DNS maliciosas, evitando la exfiltración de datos e identificando a la víctima con precisión. Configure el sinkhole para que cualquier solicitud saliente a un dominio malicioso o a una dirección IP se redireccione a una de las direcciones IP internas de su red. Esta estrategia bloquea de forma eficaz la comunicación de CnC, lo que evita que estas solicitudes lleguen a abandonar la red. Se elabora un informe de los hosts de su red que realizan dichas solicitudes, incluso aunque estén detrás del servidor DNS. Los equipos de respuesta a incidentes tienen una lista diaria de máquinas dañadas en las que deben actuar, sin la presión añadida de tener que corregir el problema en un tiempo determinado porque la comunicación con el atacante se haya interrumpido.

Objetos de correlación automatizada

Nuestra tecnología Threat Prevention incluye la capacidad de identificar la presencia de amenazas avanzadas a través de la supervisión y correlación del tráfico de redes y los logs de amenazas, de forma que pueda identificar rápidamente a los usuarios infectados y analizar los patrones de comportamiento sospechosos. Los objetos de correlación aprovechan la investigación de amenazas de Unit 42 y el análisis de amenazas desconocidas de WildFire en combinación con User-ID para relacionar las anomalías de tráfico y los indicadores de compromiso. De esta forma, se identifican de manera rápida y precisa los dispositivos de su red que están dañados.

Aproveche la inteligencia global sobre amenazas para evitar ataques

Los logs detallados de todas las amenazas no solo se encuentran en la misma interfaz de gestión, sino que se comparten entre todos los mecanismos de prevención para proporcionar contexto. Aprovechamos la inteligencia global sobre amenazas a través de WildFire con el fin de detectar automáticamente el malware desconocido y brindar protecciones para toda la base de datos de nuestros clientes. De este modo, contarán con protección frente a las amenazas avanzadas más recientes.

Red de DNS pasivo

Modelo	Capacidad de prevención de amenazas
PA-200	50 Mbps
PA-500	100 Mbps
PA-2020	200 Mbps
PA-2050	500 Mbps
PA-3020	1 Gbps
PA-3050	2 Gbps
PA-3060	2 Gbps
PA-5020	2 Gbps
PA-5050	5 Gbps
PA-5060	10 Gbps
PA-7050	100 Gbps*
PA-7080	160 Gbps*

* Habilitado para DSRI

Proteja su organización frente a los sitios web maliciosos y a las redes de malware que evolucionan a toda velocidad aprovechando los análisis basados en DNS de Palo Alto Networks. Disfrute de las ventajas de una amplia red de inteligencia habilitando la supervisión de DNS pasivo, que transfiere la información a nuestra base de datos de dominios maliciosos y que se utiliza para generar sistemas de protección en nuestra base de clientes global.

Investigación de amenazas de Unit 42

El equipo de investigación de amenazas de Palo Alto Networks, Unit 42, aplica la inteligencia humana para identificar vulnerabilidades de día cero graves en ecosistemas de Microsoft®, Adobe®, Apple® y Android™, entre otros. Con la identificación proactiva de dichas vulnerabilidades, el desarrollo de protecciones para nuestros clientes y el uso compartido de la información con la comunidad de seguridad, eliminamos las armas que utilizan los atacantes para amenazar a los usuarios y poner en peligro las redes empresariales, gubernamentales y de los proveedores de servicios.

4401, Great America Parkway
Santa Clara, CA 95054 (EE. UU.)

Línea principal: +1 408 753 4000
Ventas: +1 408 753 4000
Asistencia técnica: +1 408 753 4000

www.paloaltonetworks.com

threat-prevention-ds-020617