5 Pasos para Prevenir APTs y Ataques Avanzados

No es novedad que los ataques modernos basados en obtención de información son cada vez más sofisticados y comunes y este tipo de amenazas avanzadas representan uno de los más importantes retos que enfrentan las áreas de seguridad hoy en día.

Los atacantes han aprendido a personalizar y modificar el malware con la finalidad de traspasar los controles de seguridad tradicionales y posteriormente emplearlo como un punto de control para dirigir ataques de red sofisticados y persistentes. Es por ello, que las áreas de seguridad deben adaptar y encontrar nuevas tecnologías de seguridad que puedan **identificar** e incluso **prevenir** infecciones de malware que tal vez nunca han sido vistas "in the wild".
Este documento describe algunos de los puntos clave que hay que considerar cuando se está diseñando una arquitectura de defensa contra ataques avanzados y malware moderno.
Al seguir estos sencillos pasos nuestra organización estará protegida.

#1- Encontrar y Detener Nuevos Códigos Maliciosos y sus Variantes

El malware comúnmente es "habilitador" de los ataques avanzados, ya que fácilmente se puede personalizar, reempaquetar y re-codificar, de tal manera que no se tengan coincidencias con firmas de malware o valores hash conocidos. Debido a esto, los equipos de seguridad deben contar con herramientas que prueben activamente los archivos desconocidos para determinar si son maliciosos, aún si el archivo no coincide con una firma conocida. Adicionalmente, el malware cambia continuamente de nombre de archivo, dominio e inclusive su valor hash para evadir firmas basadas en éstas características comunes. Sin embargo, una solución de malware moderno debe detectar identificadores únicos internos dentro del código malicioso, o se correrá el riesgo de estar en un circuito interminable donde variantes simples de malware constantemente se "re-analizarán", sin que sigan siendo bloqueadas.

#2- Analizar todo el tráfico- De Entrada y Salida

Es importante señalar que cualquier tipo de tráfico que no esté siendo analizado puede causar un riesgo y en especial cuando se trata de ataques avanzados. Los ataques avanzados frecuentemente emplean código malicioso para obtener acceso interno y después ejecutar acciones para comprometer la red interna donde los detectores de intrusos (IPS) y otras medidas de seguridad tal vez no estén analizando cómo deberían de estarlo haciendo. Es por esto que es fundamental buscar amenazas y anomalías dentro del tráfico interno que pueda revelar un ataque. Adicionalmente, los atacantes tienen una variedad de técnicas a su disposición para ocultar sus ataques, por ejemplo, emplearán el protocolo SSL para mantener el tráfico de malware y de "command-and-control" lejos de las miradas indiscretas de los equipos de seguridad. Igualmente, el tráfico de comando y control, y los payloads o carga útil de los códigos maliciosos comúnmente emplean puertos no estándar o túneles personalizados con el fin de evadir la seguridad tradicional, así como el uso de una gran variedad de proxies, anonymizers y aplicaciones tuneleadas y cifradas para ocultar aún más su comunicación. Si una solución de malware moderno falla en controlar este tipo de mecanismos, entonces cada análisis avanzado subsecuente será en vano, ya que los atacantes están evadiendo toda la solución.

#3- Emplear una solución en línea de inspección de todo el tráfico

Con el fin de que las soluciones de seguridad realicen su trabajo, tienen que ser implementadas en línea para asegurarse que puedan bloquear directamente riesgos y amenazas que viajan a través del tráfico. Esto aplica generalmente para la mayoría de las soluciones de seguridad como firewalls, IPSs e incluso web-proxies, así como para las soluciones que particularmente controlan malware moderno y ataques avanzados. Dado que, por definición, este tipo de ataques suelen ser ignorados en el momento del ataque, todo el tráfico debe ser monitoreado para este tipo de amenazas. Así mismo, cuando se bloquea malware o tráfico de malware, es importante que la solución de seguridad esté en línea y pueda descartar todo el tráfico malicioso en lugar de confiar en factores como “TCP resets”.
El código malicioso es comúnmente muy pequeño, y puede resultar en una condición de carrera donde el malware es liberado antes de que el reset surta efecto. Igualmente, la aplicación de TCP resets no es confiable cuando se intentan controlar las comunicaciones de malware, dado que ambos puntos finales (cliente y servidor) son maliciosos y pueden simplemente ignorar o filtrar los mensajes de reinicio. Debido a ello, es primordial que las soluciones de malware moderno sean evaluadas por la taza de bloqueos, desempeño y fiabilidad que el resto de las soluciones de seguridad.

#4- Adaptarse a las Nuevas Técnicas de Malware de forma rápida

A la mayoría de los atacantes les gusta cambiar las firmas del código malicioso que crean, así como actualizar siempre sus tácticas para evadir las medidas de detección y análisis. Ahora que los análisis activos de malware han llegado a incrementarse, los autores de malware han comenzado a acelerar el desarrollo de varias técnicas anti-análisis y sistemas virtuales de detección para prevenir que su malware sea detectado. Las soluciones de malware moderno, por lo tanto, deben ser flexibles y continuamente actualizadas para seguir el ritmo de éstas técnicas de evasión. Sin embargo, esto es un reto mucho mayor que el de actualizar firmas en las soluciones de seguridad tradicionales. Las técnicas de anti-análisis comúnmente tiene como objetivo el SO virtual, equipos o introducen nuevas técnicas de conexión que requieren cambios en el ambiente virtual propiamente. Sin la capacidad de actualizar fácilmente la lógica interna, un malware moderno puede regresar a ser un elemento estático en los intentos del área de seguridad para controlar una amenaza más dinámica.

#5- Ejecutar todo lo Anterior a Escala

Además de evaluar aspectos de escalabilidad de una solución de seguridad, tales como throughput, sesiones y latencia; los equipos de seguridad también deben analizar la escalabilidad del ambiente virtual en sí. Es importante recordar que cada archivo desconocido que requiera un análisis activo o en tiempo real requerirá uno o más sistemas virtuales, el cual puede saturar el hardware local dependiendo del tráfico que va a ser analizado. Sin embargo, esto puede conducir a un problema que es significativamente más grande que el simple dimensionamiento de hardware y problemas de costos. Si el análisis virtual está limitado sólo al hardware local, entonces los atacantes simplemente saturan las soluciones con archivos a analizar, permitiendo que archivos con código malicioso vulneren la seguridad.

Aprende más acerca de la solución de Wildfire y cómo hoy puedes comenzar a proteger tu red de malware moderno.

http://www.paloaltonetworks.com/products/technologies/wildfire---analysis.html