INFORMACIÓN SOBRE EL PRODUCTO DE AKAMAI

Secure Internet Access ThreatAvert

Proteja los activos de red vitales e identifique el malware que afecta a los suscriptores

Los proveedores de servicios reconocen que la seguridad de la red refuerza la imagen de la marca, ya que afecta directamente a la satisfacción de los suscriptores. La mayoría de las amenazas actúan a través de DNS, y se han desarrollado nuevas amenazas que apuntan específicamente a la infraestructura de DNS esencial. Los proveedores deben replantearse cómo proteger los recursos de red y a los suscriptores, sobre todo teniendo en cuenta que las amenazas son cada vez más dinámicas y diversas en un mundo donde todo está conectado.

Akamai Secure Internet Access ThreatAvert evalúa las búsquedas de DNS en tiempo real para detectar y bloquear la actividad maliciosa. Secure Internet Access ThreatAvert tiene como objetivo las amenazas que causan interrupciones o ralentizaciones en la red, afectan negativamente a la experiencia de los suscriptores o subvierten otras protecciones de la red. Algunos ejemplos de estas amenazas son:

- ataques DDoS basados en DNS que desbordan los componentes de resolución con volúmenes masivos de consultas;
- malware de bots que roba valiosos datos personales o compromete dispositivos del consumidor;
- túneles DNS que roban servicios transportando otros protocolos dentro del DNS.

Secure Internet Access ThreatAvert tiene como base el componente de resolución de DNS CacheServe de Akamai, equipado con las fuentes de amenazas dinámicas de Akamai. CacheServe es el modelo de referencia en cuanto a fiabilidad: años de inversión para optimizar el rendimiento y numerosas mejoras de software garantizan su resistencia y disponibilidad, incluso frente a picos masivos en el tráfico de DNS. La inteligencia de Akamai contra amenazas la ha desarrollado el equipo de ciencia de datos de la empresa, que procesa más de 100 000 millones de consultas de DNS, transmitidas en streaming en directo cada día por todo el mundo.

La seguridad de DNS corresponde a los servidores DNS

Las consultas de DNS son uno de los principales indicadores de actividad maliciosa, ya que resolver la dirección de un recurso nocivo —servidor de mando y control, descarga de malware, sitio de exfiltración, etc.— es el primer paso para habilitar la mayoría de las formas de este tipo de actividad. Los componentes de resolución de DNS son el lugar ideal para incrustar inteligencia contra las amenazas objetivo, porque ven todas las consultas en la red del proveedor. Es posible detectar la actividad maliciosa comparando las consultas entrantes con las entradas de listas de amenazas dinámicas.

VENTAJAS PARA SU EMPRESA

- Solución ligera y escalable a millones de suscriptores que cubre todos los dispositivos
- Ciencia de datos líder que ofrece una cobertura frente a amenazas más amplia y profunda
- Fuentes de amenazas continuamente actualizadas para mantener la protección a medida que cambian los ataques
- Informes en tiempo real fáciles de leer que muestran el estado de la amenaza de un vistazo y enlazan con los detalles
- Recopilación eficaz y gestión escalable de los datos de amenazas y de telemetría

Akamai

Secure Internet Access ThreatAvert se incrusta en el plano de control de DNS con un coste, esfuerzo operativo e impacto en la red menores que las soluciones de procesamiento de paquetes dedicadas, que se incrustan en el tráfico del plano de datos.

Es ligero y eficaz, y el tráfico de la red no produce latencia adicional. Dado que se basa en la red, todos los dispositivos están cubiertos, y los clientes y hosts no requieren la instalación de software de seguridad ni actualizaciones.

Mayor precisión, profundidad y cobertura frente a amenazas

Los desarrolladores de malware innovan continuamente para elevar al máximo el retorno de la inversión de sus ataques. Esto significa que la mayoría de las amenazas están cuidadosamente diseñadas para evadir la detección y cambian rápidamente para poder mantenerse. La superficie de ataque también se ha ampliado y ahora incluye una asombrosa variedad de dispositivos de Internet de las cosas conectados, por lo que hay una considerable diversidad de métodos que los atacantes pueden utilizar para lograr sus objetivos.

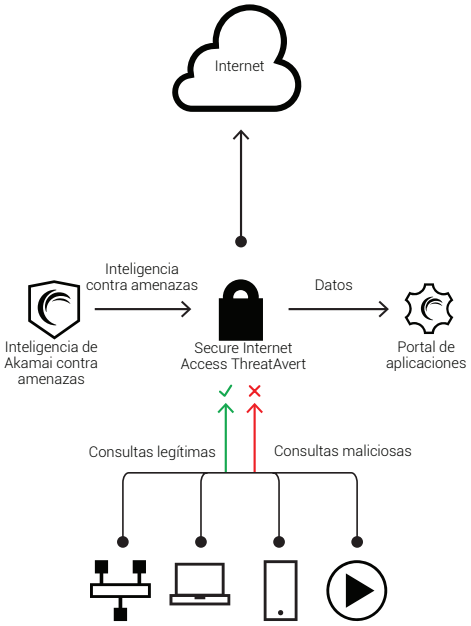
Reconociendo la sutileza y diversidad del panorama de amenazas, el equipo de ciencia de datos de Akamai ha desarrollado, implementado e integrado sistemas clave para analizar las consultas de DNS transmitidas en streaming en directo. Al proceso se han incorporado datos de amenazas de listas de reputación, cebos y otras fuentes de terceros. La mayor amplitud y profundidad de la cobertura frente a amenazas, la precisión y la agilidad provienen de inversiones en:

- algoritmos pendientes de patentar que detectan instantáneamente comportamientos anómalos (como DNS-DDoS), correlacionan amenazas dispares e identifican nuevos algoritmos de generación de dominios bot;
- técnicas avanzadas para permitir automáticamente nombres que garantizan que las consultas de DNS legítimas siempre estén protegidas;
- personal de investigación con años de experiencia en seguridad y una profunda comprensión del malware y los datos de DNS;
- una red mundial y centros de datos para el procesamiento en tiempo real de transmisiones en streaming de datos en directo.

Políticas de precisión que bloquean el tráfico dañino y protegen el legítimo

Se han incorporado políticas de precisión a las fuentes de inteligencia de Akamai contra amenazas para gestionar el tráfico de DNS no deseado. Un conjunto de características amplio y profundo permite filtrar de forma detallada para detectar las consultas maliciosas y proteger (responder a) las consultas legítimas:

- las políticas de precisión pueden aplicarse a las consultas entrantes o a las respuestas salientes;
- los filtros o los límites de frecuencia pueden establecerse en función de los parámetros IP, QTYPE, FQDN u otros muchos parámetros de consulta;
- los filtros o límites de frecuencia pueden utilizar diversos parámetros de consulta, además de operadores lógicos: QTYPE AND FQDN, IP AND FQDN, etc.;
- los filtros o límites de frecuencia pueden emparejarse con listas de amenazas dinámicas de la inteligencia de Akamai contra amenazas o con listas suministradas por el operador;



El gran flujo de datos procesado por los expertos de Akamai ofrece una imagen completa de la actividad maliciosa en Internet, así como de ataques localizados.

- es posible combinar políticas y listas de amenazas: MATCH frente a BLOCKLIST y NOT en ALLOWLIST;
- diversas acciones de política determinan cómo se manejan las consultas: descartar, sintetizar respuesta, responder de forma limitada, NXD, NOERROR, etc.;
- las políticas se pueden combinar y anidar, lo que las hace aún más potentes.

Las políticas de precisión también se pueden configurar manualmente para resolver problemas localizados en la red de un proveedor.

Gestión de datos escalable, telemetría enriquecida e informes

Secure Internet Access ThreatAvert incorpora una arquitectura de gestión de datos basada en soluciones abiertas que han sido probadas en las redes más grandes del mundo y ofrecen excelencia operativa a escala web y velocidad. Los datos transmitidos en streaming en directo desde los sistemas Secure Internet Access ThreatAvert en toda la red se agregan y quedan disponibles para informes (descritos a continuación) y otros sistemas. La resistente arquitectura ofrece una disponibilidad permanente, que es la base de una experiencia sin interrupciones para el cliente. Se pueden utilizar conectores opcionales para abrir sistemas big data (como Splunk o Hadoop) o aplicaciones específicas, a fin de obtener información adicional sobre operaciones, seguridad y negocios.

Los informes de Secure Internet Access ThreatAvert ofrecen una evaluación instantánea de la situación de la seguridad con un panel ejecutivo que cubre las consultas de DNS bloqueadas, el ancho de banda de DNS máximo guardado, el principal malware en la red, los suscriptores infectados y las actualizaciones de la inteligencia contra amenazas. Un panel de seguridad adicional proporciona gráficos de DDoS y detalles del malware. También se pueden obtener, con un solo clic, capas sucesivas de detalles sobre el malware y los clientes infectados. Es posible crear paneles e informes personalizados en minutos para mostrar datos de seguridad en un formato definido por el usuario, a fin de satisfacer sus propios requisitos operativos. Los informes con etiquetas permiten que el personal de operaciones configure vistas de la topología de Secure Internet Access ThreatAvert que se ajusten a sus propios requisitos.