INFORMACIÓN SOBRE EL PRODUCTO DE AKAMAI

Content Protector

Proteja sus ingresos de los ataques cada vez más sofisticados de los scrapers

Mediante el scraping de su contenido, los atacantes ganan dinero y usted lo pierde. Aunque compartir contenido públicamente es una decisión estratégica, es crucial diferenciar entre lo que supone que los consumidores participen y las actividades perjudiciales de scraping. Tanto la competencia como los atacantes pueden aprovechar los datos extraídos, lo que puede afectar a su estrategia de precios y ser perjudicial para sus clientes. Content Protector de Akamai identifica y detiene a los scrapers desde el primer momento mediante mecanismos de detección adaptados a las herramientas y técnicas específicas de los ataques de scraping. Proteja su negocio y sus ingresos sin que esto afecte a la velocidad ni al rendimiento.

Los ataques de scraping suponen un reto continuo para las empresas que operan online. A diferencia de las ciberamenazas habituales que tienen un momento claro de inicio y finalización, los scrapers pueden acceder de forma constante a su sitio, lo que podría tener importantes repercusiones si no se toman las medidas necesarias. Entre ellas se incluyen las siguientes:

- **Efecto en el rendimiento del sitio web:** las actividades de scraping persistentes pueden ralentizar su sitio, lo que provoca frustración entre los usuarios y reducción de las tasas de conversión.
- **Desventajas competitivas:** la competencia puede utilizar el scraping para conocer sus precios y vender más barato que usted, lo que afecta a sus ingresos.
- **Riesgos para la reputación de la marca:** los falsificadores podrían usar el contenido extraído y vender productos falsos haciéndose pasar por su marca.

Es cierto que los scrapers llevan muchos años entre nosotros. Pero, ¿por qué ahora son más peligrosos? La necesidad urgente de combatir a los scrapers se ha intensificado recientemente. Los acontecimientos ocurridos en 2020, entre ellos la pandemia y las posteriores interrupciones en la cadena de suministro, han supuesto un aumento de los incentivos económicos para el scraping. Los artículos con una fuerte demanda, que pueden ir desde productos básicos para el día a día hasta artículos de lujo y servicios relacionados con los viajes, se han convertido en objetivos primordiales para operaciones de scraping sofisticadas.

Ante la perspectiva de obtener más dinero, los operadores de bots comenzaron a innovar sin parar, especializándose en partes de las herramientas (como la telemetría) y, a continuación, a encadenarlas con partes fabricadas por otros operadores de bots, con el fin de crear bots con un gran nivel de especialización y específicos para los ataques de scraping. Esto hace que los scrapers sean más peligrosos y más difíciles de detectar. Y lo que es peor, el scraping también se puede producir mediante otros métodos como los complementos, por lo que con la gestión de bots no será suficiente para detener a los scrapers.

Sin embargo, no se puede limitar a bloquear a todos los scrapers: los bots de búsqueda detectan contenido nuevo que desee que aparezca en las búsquedas públicas, algunos bots de compras de consumidores pueden resaltar sus productos en sitios de comparación y los partners pueden conseguir recopilar la información más reciente sobre los productos para compartirla con sus clientes.

VENTAJAS PARA SU EMPRESA

Aumento de las tasas de conversión
Elimine los bots que ralentizan su sitio y sus aplicaciones, consiguiendo que haya más clientes en su sitio y mejorando las ventas

Reducción de los costes
No pague por distribuir el tráfico de bots

Frustración de los scrapers
Evite que los scrapers hagan ping a su sitio para ver cuándo está disponible el inventario nuevo, lo que permite reducir la posibilidad de que los operadores de bots puedan llevar a cabo el siguiente paso en una cadena de ataques de acaparamiento de inventario

Frustración de la competencia
Detenga el scraping automatizado que permite a su competencia ofrecer precios más bajos que los suyos y reducir sus ventas

Mitigación de las falsificaciones
Detenga el incesante scraping que usan los falsificadores para captar su contenido y, a continuación, hacerse pasar por usted

Mejora de su comercialización
Elimine el tráfico de bots de los análisis de su sitio para garantizar que los usuarios reales puedan disfrutar de las mejoras

Akamai

Content Protector de Akamai ofrece mecanismos de detección especialmente diseñados para identificar a los scrapers y detenerlos. Y lo hace al mismo tiempo que aprovecha la visibilidad de la red de Akamai, nuestro principal aval en la gestión de bots y el desarrollo continuo de los sistemas de detección más avanzados. Al adaptar la protección a las nuevas amenazas que van surgiendo, incorporamos automáticamente la información de nuestros investigadores de inteligencia sobre amenazas y especialistas en datos, motivo por el que Content Protector sigue siendo líder en detecciones personalizadas de scrapers.

Cuando detenga a los scrapers, podrá centrarse en sacar el máximo partido a su presencia digital, por ejemplo, con una mejora del rendimiento del sitio y de las tasas de conversión, y reducir el efecto de la competencia.

Funciones clave

- **Detecciones:** conjunto de métodos de detección basados en aprendizaje automático (ML) que evalúa los datos recopilados del cliente y del servidor.
  - » **Evaluación a nivel de protocolo:** el reconocimiento de huella de protocolo evalúa cómo el cliente establece la conexión con el servidor en las diferentes capas del modelo de interconexión de sistemas abiertos (OSI), TCP, TLS y HTTP, al verificar que los parámetros negociados coinciden con los que esperan los navegadores web y las aplicaciones móviles más habituales.
  - » **Evaluación a nivel de aplicación:** determina si el cliente puede ejecutar alguna lógica empresarial escrita en JavaScript. Cuando el cliente ejecuta JavaScript, Content Protector recopila las características del dispositivo y del navegador, así como las preferencias del usuario (reconocimiento de huella). Estos puntos de datos diferentes se compararán con los datos a nivel de protocolo para verificar la coherencia.
  - » **Interacción del usuario:** las métricas sobre el comportamiento evalúan que una persona interactúe con el cliente a través de periféricos estándar como pantallas táctiles, teclados y ratones. La falta de interacción o la interacción anómala suele estar asociada al tráfico de bots.
  - » **Comportamiento del usuario:** analiza el recorrido del usuario por el sitio web. Las botnets suelen perseguir contenido específico, lo que da lugar a un comportamiento significativamente diferente al del tráfico legítimo.
  - » **Detección de navegador sin interfaz:** un JavaScript personalizado que se ejecuta en el cliente busca indicadores que dejan los navegadores sin interfaz, incluso cuando se ejecutan en modo oculto.
- **Clasificación de riesgos:** proporciona una clasificación determinista y procesable del tráfico en niveles de riesgo bajo, medio o alto, basada en las anomalías encontradas durante la evaluación.
- **Acciones de respuesta:** conjunto de estrategias de respuesta, incluida la sencilla acción de supervisión y denegación, así como otras más avanzadas, como cebos, que simula un servidor colgado o distintos tipos de acciones de desafío. Los desafíos criptográficos suelen ser más fáciles de usar que los desafíos de tipo CAPTCHA a la hora de lidiar con los posibles falsos positivos.

Base de Content Protector: ecosistema de Akamai

Akamai proporciona un servicio de Internet más rápido, inteligente y seguro. Nuestras completas soluciones se construyen en torno a la solución globalmente distribuida Connected Cloud de Akamai, y se gestionan a través de la herramienta unificada y personalizable Akamai Control Center para ofrecerle una mejor visibilidad y un mayor control. Además, cuenta con el soporte de los expertos de Servicios Profesionales de Akamai, que le ayudarán a ponerse en marcha con facilidad y a impulsar la innovación a medida que sus estrategias evolucionen.

Solicite una demostración o póngase en contacto con el equipo de ventas de Akamai.