AKAMAI-PRODUKTBESCHREIBUNG

Content Protector

Schützen Sie Ihre Einnahmen vor immer ausgefeilteren Scraper-Angriffen

Es steht viel Geld auf dem Spiel: Wenn Ihre Daten abgegriffen werden, haben Angreifer viel zu gewinnen und Sie viel zu verlieren. Auch wenn das öffentliche Teilen von Inhalten eine strategische Wahl ist, sollte dennoch zwischen Kundenbindung und schädlichen Scraping-Aktivitäten unterschieden werden. Wettbewerber und Angreifer können gestohlene Daten ausnutzen, um Ihre Preise zu unterbieten und Ihre Kunden zu schädigen. Akamai Content Protector entdeckt und stoppt Scraper sofort auf den ersten Blick. Dabei kommen Erkennungsmethoden zum Einsatz, die auf die einzigartigen Tools und Techniken von Scraper-Angriffen zugeschnitten sind. Schützen Sie Ihr Unternehmen und Ihre Einnahmen, ohne dabei Geschwindigkeit oder Performance zu beeinträchtigen.

Scraping-Angriffe stellen für Onlineunternehmen eine ständige Herausforderung dar. Im Gegensatz zu typischen Cyberbedrohungen mit klaren Start- und Endpunkten können Scraper dauerhaft auf Ihre Website zugreifen. Dies kann weitreichende Auswirkungen haben, wenn nichts dagegen unternommen wird. Dazu gehören:

- **Auswirkung auf die Websiteperformance:** Anhaltende Scraping-Aktivitäten können Ihre Website verlangsamen, was wiederum zu frustrierten Nutzern und reduzierten Konversionsraten führen kann.
- **Wettbewerbsnachteile:** Mitbewerber nutzen Scraping möglicherweise, um Ihre Preise zu beobachten und zu unterbieten. Dies wird sich dann auf Ihren Umsatz auswirken.
- **Risiken für die Reputation der Marke:** Fälscher könnten gestohlene Inhalte missbrauchen und gefälschte Produkte unter dem Namen Ihrer Marke verkaufen.

Natürlich gibt es Scraper schon seit vielen Jahren. Warum sind sie jetzt also schlimmer? Die Dringlichkeit, Scraper zu bekämpfen, hat in letzter Zeit zugenommen. Die Ereignisse des Jahres 2020, einschließlich der Pandemie und der anschließenden Unterbrechungen der Lieferkette, haben die finanziellen Anreize für Scraping erhöht. Stark nachgefragte Artikel, die von Alltagsgegenständen bis hin zu Luxusgütern und Reisedienstleistungen reichen, sind zu den wichtigsten Zielen für anspruchsvolle Scraper geworden.

Da die Aussicht auf mehr Geld lockte, begannen die Bot-Betreiber fieberhaft aufzurüsten und sich auf bestimmte Teile der Tools (wie Telemetrie) zu konzentrieren. Diese kombinierten sie dann mit Teilen anderer Bot-Betreiber. So entstanden hochspezialisierte Bots, die auf Scraping-Angriffe zugeschnitten sind. Dadurch sind die Scraper gefährlicher und zudem schwieriger zu erkennen. Und schlimmer noch: Scraping kann auch mit anderen Methoden wie Plug-ins erfolgen. Es erfordert also mehr als nur Bot-Management, um Scraper zu stoppen.

Aber Sie können nicht einfach alle Scraper blockieren – Such-Bots beispielsweise durchforsten das Internet nach neuen Inhalten, die Sie in öffentlichen Suchanfragen anzeigen möchten, einige für Verbraucher relevante Shopping-Bots können Ihre Produkte auf Vergleichsseiten hervorheben und Partner können effizient die neuesten Produktinformationen sammeln, um sie mit ihren Kunden zu teilen.

VORTEILE FÜR IHR UNTERNEHMEN

Höhere Konversionsraten
Entfernen Sie die Bots, die Ihre Website und Anwendungen verlangsamen, sodass mehr Kunden auf Ihrer Website bleiben und Ihre Umsätze gesteigert werden

Kostensenkung
Zahlen Sie nicht für Bot-Traffic

Scalper verhindern
Verhindern Sie, dass Scraper Ihre Website anpingen, um zu sehen, wann stark nachgefragte Artikel verfügbar sind, und erschweren Sie es Bot-Betreibern, zum nächsten Schritt in einer Inventory-Hoarding-Angriffskette zu gelangen

Mitbewerber in Schach halten
Beenden Sie das automatisierte Scraping, mit dem Ihre Mitbewerber Ihre Preise unterbieten und Ihre Umsätze senken können

Bekämpfung von Fälschungen
Stoppen Sie die hartnäckigen Fälscher, die Ihre Inhalte per Scraping schnappen und sich dann als legitime Eigentümer ausgeben

Bessere Vermarktung
Entfernen Sie Bot-Traffic aus Ihrer Websiteanalyse, um die Optimierung für echte Nutzer sicherzustellen

Akamai

Akamai Content Protector verfügt über Erkennungsmethoden, die speziell darauf ausgelegt sind, Scraper zu finden und zu stoppen. Und dabei profitieren sie von der Transparenz des Akamai-Netzwerks, unserer globalen Stärke im Bot-Management und der kontinuierlichen Weiterentwicklung von modernsten Erkennungsmethoden. Wir aktualisieren Ihren Schutz, wenn sich Bedrohungen weiterentwickeln, und integrieren automatisch die Threat Intelligence unserer Forscher und Data Scientists. Daher nimmt Content Protector weiterhin eine führende Rolle bei der maßgeschneiderten Erkennung von Scrapern ein.

Sobald Sie die Scraper aufgehalten haben, können Sie sich darauf konzentrieren, Ihre digitale Präsenz optimal zu nutzen, z. B. die Verbesserung der Websiteperformance und der Konversionsraten sowie die Reduzierung der Auswirkungen von Mitbewerbern.

Wichtige Funktionen

- **Erkennungen:** Eine Reihe von ML-basierten Erkennungsmethoden, die die erhobenen client- und serverseitigen Daten bewerten.
  - » **Bewertung auf Protokollebene:** Das Protokoll-Fingerprinting wertet aus, wie der Client die Verbindung zum Server auf den verschiedenen Ebenen des OSI-Modells herstellt: TCP, TLS und HTTP – so wird überprüft, ob die ausgehandelten Parameter mit denen übereinstimmen, die von den gängigsten Webbrowsern und mobilen Anwendungen erwartet werden.
  - » **Bewertung auf Anwendungsebene:** Beurteilt, ob der Client eine in JavaScript geschriebene Geschäftslogik ausführen kann. Wenn der Client JavaScript ausführt, erfasst Content Protector die Geräte- und Browsereigenschaften sowie Nutzereinstellungen. Diese verschiedenen Datenpunkte werden verglichen und zur Überprüfung der Konsistenz mit den Daten auf Protokollebene referenziert.
  - » **Nutzerinteraktion:** Anhand von Verhaltensmetriken wird über Standard-Peripherie wie Touchscreen, Tastatur und Maus ermittelt, ob ein Mensch mit dem Client interagiert. Mangelnde Interaktion oder anormale Interaktion ist typischerweise ein Hinweis auf Bot-Traffic.
  - » **Nutzerverhalten:** Analysiert die User Journey auf der Website. Botnets suchen in der Regel nach bestimmten Inhalten, wodurch sich ihr Verhalten signifikant von legitimem Traffic unterscheidet.
  - » **Erkennung von Browsern ohne Header:** Ein nutzerdefiniertes JavaScript, das clientseitig ausgeführt wird und nach Indikatoren sucht, die von Browsern ohne Header hinterlassen werden, selbst wenn sie im Stealth-Modus ausgeführt werden.
- **Risikoklassifizierung:** Bietet eine deterministische und umsetzbare Traffic-Klassifizierung mit niedrigem, mittlerem oder hohem Risiko, die auf den bei der Bewertung festgestellten Anomalien basiert.
- **Maßnahmen:** Eine Reihe von Reaktionsstrategien wie z. B. einfaches Überwachen und Blockieren sowie fortgeschrittenere Strategien wie Tarpit. Dabei werden ein hängender Server oder verschiedene Arten von Challenge-Aktionen simuliert. Krypto-Challenges sind beim Umgang mit möglichen False Positives im Allgemeinen nutzerfreundlicher als CAPTCHA-Sicherheitsfragen.

Das Fundament von Content Protector: Das Akamai-Ökosystem

Akamai macht das Internet schnell, intelligent und sicher. Unsere umfassenden Lösungen bauen auf der global verteilten Akamai Connected Cloud auf. Sie wird durch das einheitliche, individuell anpassbare Akamai Control Center verwaltet, das für Transparenz und Kontrolle sorgt. Und unsere Professional-Services-Experten unterstützen Sie bei der Einrichtung und zeigen Ihnen Innovationsmöglichkeiten auf.

Melden Sie sich für eine Demo an, oder wenden Sie sich an das Akamai-Vertriebsteam.