DESCRIZIONE DEL PRODOTTO AKAMAI

Content Protector

Proteggete i vostri profitti da attacchi di scraping sempre più sofisticati

Lo scraping dei contenuti è una miniera d'oro per gli autori degli attacchi ma può causare gravi perdite agli utenti. Sebbene la condivisione pubblica dei contenuti sia una scelta strategica, è fondamentale distinguere tra engagement dei consumatori e attività di scraping dannose. Aziende concorrenti e utenti malintenzionati possono sfruttare i dati acquisiti illegalmente, mettendo a repentaglio la vostra strategia di determinazione dei prezzi e danneggiando i vostri clienti. Akamai Content Protector identifica e arresta tempestivamente gli scraper, utilizzando metodi di rilevamento personalizzati in base alle tecniche e agli strumenti impiegati negli attacchi di scraping. Proteggete il business e il fatturato senza rinunciare alla velocità e alle performance.

Gli attacchi di scraping rappresentano una sfida continua per le aziende che operano online. A differenza delle minacce informatiche più comuni, per cui è possibile individuare un inizio e una fine, gli scraper sono in grado di accedere al vostro sito in maniera persistente. Per tale ragione è necessario bloccarli con rapidità, onde evitare significative ripercussioni sull'azienda, ad esempio:

- **Impatto sulle performance dei siti web:** le continue attività di scraping possono rallentare il vostro sito, causando frustrazione negli utenti e tassi di conversione ridotti.
- **Svantaggi rispetto alla concorrenza:** le aziende concorrenti possono utilizzare lo scraping per monitorare e influenzare i vostri prezzi, riducendo i profitti che potete generare.
- **Rischi per la reputazione del brand:** gli autori di atti di contraffazione possono utilizzare in modo improprio i contenuti sottratti, vendendo prodotti falsi a nome del vostro brand.

Ovviamente gli attacchi di scaping non sono minacce nuove, ma esistono già da diversi anni. Cosa li rende più pericolosi adesso? La necessità di combattere gli scraper è diventata più urgente negli ultimi anni. Gli eventi del 2020, tra cui la pandemia e le conseguenti difficoltà di approvvigionamento, hanno reso gli attacchi di scraping più allettanti dal punto di vista finanziario. Alcuni articoli molto richiesti, che spaziano dai prodotti d'uso quotidiano ai beni di lusso fino ai servizi di viaggio, sono diventati obiettivi primari per le attività di scraping più sofisticate.

Spinti da un maggiore potenziale di guadagno, gli operatori di bot hanno iniziato a perfezionare la tecnologia adottata, specializzandosi nella realizzazione in alcuni componenti (come la telemetria) che si integrano con quelli realizzati da altri operatori per creare bot altamente specifici e perfetti per gli attacchi di scraping. Tutto ciò rende gli scraper più pericolosi e anche più difficili da identificare. A peggiorare la situazione, il fatto che lo scraping può essere condotto anche utilizzando metodi alternativi, come i plug-in, quindi una gestione attenta dei bot non è più sufficiente per arrestare gli scraper.

Infine, bisogna considerare che non è possibile bloccare tutti gli scraper: i bot di ricerca sono utili per trovare nuovi contenuti da visualizzare nelle ricerche pubbliche, alcuni bot commerciali possono evidenziare i prodotti nei siti di comparazione e i partner possono voler raccogliere in modo efficiente le informazioni più recenti sui prodotti per condividerle con i clienti.

VANTAGGI PER LA VOSTRA AZIENDA

Aumento dei tassi di conversione
Rimuovete i bot che rallentano il sito e le app, fidelizzando più clienti e incrementando le vendite

Riduzione dei costi
Riducete le spese legate alla gestione del traffico di bot

Blocco degli speculatori
Impedite agli attacchi di scraping di monitorare il vostro sito e di capire quando alcuni articoli diventano disponibili, limitando in questo modo la capacità di alcuni operatori di bot di perpetrare una catena di attacchi mirati al furto dell'inventario

Blocco della concorrenza sleale
Arrestate gli attacchi di scraping automatico che consentono alla concorrenza di incidere sui vostri prezzi e ridurre le vostre vendite

Mitigazione della contraffazione
Bloccate gli instancabili autori di atti di contraffazione, che mirano ad acquisire i vostri contenuti e a sottrarre la vostra identità

Analisi di marketing migliorate
Rimuovete il traffico di bot dalle analisi del vostro sito, in modo da garantire una visione accurata degli utenti reali

Akamai

Akamai Content Protector è dotato di tecniche di rilevamento progettate appositamente per rilevare gli scraper e arrestarli. Riesce a farlo sfruttando la visibilità della rete Akamai, la nostra potenza in termini di gestione dei bot e lo sviluppo continuo delle nostre innovative tecniche di rilevamento. Aggiornando la protezione con l'evolversi delle minacce, siamo in grado di integrare automaticamente le informazioni ricevute dai nostri ricercatori di intelligence sulle minacce e dagli analisti di dati in modo che Content Protector possa continuare a condurre rilevamenti personalizzati sugli scraper.

Una volta bloccati gli attacchi di scraping, potrete concentrarvi su come sfruttare al meglio la vostra presenza digitale, ad esempio migliorando le performance e i tassi di conversione del vostro sito e contrastando le offerte della concorrenza.

Funzionalità principali

- **Tecniche di rilevamento:** una serie di metodi basati su ML (Machine Learning) in grado di valutare i dati raccolti lato client e lato server.
  - **Valutazione a livello di protocollo:** attraverso l'impronta digitale del protocollo si valuta in che modo il client stabilisce la connessione con il server ai vari livelli del modello OSI (TCP, TLS e HTTP) verificando che i parametri negoziati siano allineati con quelli previsti dai più comuni browser web e applicazioni mobili.
  - **Valutazione a livello di applicazione:** viene valutata l'eventuale esecuzione della logica aziendale scritta in JavaScript da parte del client. Se il client esegue JavaScript, Content Protector identifica le caratteristiche di browser e dispositivi, oltre alle preferenze degli utenti (impronta digitale). Questi vari punti dati vengono quindi confrontati e verificati sulla base dei dati a livello di protocollo per valutarne la coerenza.
  - **Interazione dell'utente:** attraverso le metriche comportamentali viene analizzata l'interazione dell'utente con il client tramite periferiche standard, come touchscreen, tastiera e mouse. La mancanza di interazione o un'interazione anomala è, solitamente, associata al traffico di bot.
  - **Comportamento dell'utente:** viene analizzato il comportamento dell'utente sul sito web. Le botnet, di solito, prendono di mira contenuti specifici, causando un comportamento molto diverso rispetto al traffico legittimo.
  - **Rilevamento dei browser headless:** viene eseguito un JavaScript personalizzato lato client alla ricerca di indicatori lasciati dai browser headless, anche in modalità invisibile.
- **Classificazione dei rischi:** viene fornita una classificazione del traffico a basso, medio o alto rischio di tipo deterministico e utilizzabile, sulla base delle anomalie rilevate durante la valutazione.
- **Azioni di risposta:** una serie di strategie di risposta, tra cui semplici azioni di monitoraggio e rifiuto oppure azioni più avanzate, ad esempio il tarpit, che simula un blocco del server o varie azioni di sfida. Le sfide crittografiche sono generalmente più facili da usare rispetto alle sfide CAPTCHA nella gestione di possibili falsi positivi.

Alla base di Content Protector c'è l'ecosistema Akamai

Akamai rende Internet veloce, intelligente e sicuro. Le nostre soluzioni complete sono basate su Akamai Connected Cloud, distribuito su scala globale, vengono gestite tramite il portale unificato e personalizzabile Akamai Control Center, che garantisce visibilità e controllo, e sono supportate dagli esperti del team Professional Services, che aiutano i clienti a essere subito operativi proponendo loro soluzioni sempre nuove, in linea con l'evoluzione delle strategie aziendali.

Registratevi per una demo o contattate il team di vendita Akamai.