BOARDROOM
INSIDER COMMUNITY

La protezione di brand e ricavi

con la riduzione di bot e abusi nel percorso d'acquisto dei clienti

RETAIL GAZETTE

IN COLLABORAZIONE CON Akamai

Introduzione

Vi sembra che gli scraper siano diventati recentemente un problema di vaste proporzioni? Non è frutto della vostra immaginazione. Dopo la pandemia di COVID, i bot scraper che prendono di mira i retailer sono diventati più elusivi *e sofisticati* poiché raccolgono dati da poter sfruttare e monetizzare a discapito dei brand.

Tuttavia, molti dirigenti non sono consapevoli (o sottovalutano) l'impatto devastante che i bot scraper possono esercitare sulle performance dei siti web, sulla sicurezza dei dati e sui profitti aziendali. Anche se i bot scraper SEO possono risultare vantaggiosi per migliorare l'individuazione e il posizionamento nei motori di ricerca, vengono utilizzati con intenzioni più dannose per tagliare i prezzi, effettuare lo scalping degli inventari limitati e creare siti contraffatti allo scopo di rubare le informazioni dei clienti. Ecco perché un maggior livello di consapevolezza (e collaborazione tra i vari team addetti al digitale, al marketing, alle frodi e alla sicurezza) è necessario non solo per proteggere i brand, ma anche il fatturato.

Questo rapporto evidenzia il motivo per cui la rimozione degli scraper dal vostro sito web influirà positivamente sui molti aspetti della vostra società di retail. È impossibile difendersi da ciò che non si vede. Con la rimozione degli scraper, sarete maggiormente preparati per massimizzare il vostro potenziale di profitto e ottimizzare il percorso d'acquisto dei clienti.

Susan McReynolds
Global Industry Strategist per il commercio di Akamai

Introduzione

Gli attacchi dei bot, come anche le campagne di phishing che prendono di mira i retailer, sono in aumento. Collettivamente, lo scraping, le frodi di tessere fedeltà e carte di pagamento hanno registrato un aumento di oltre il 700% nella seconda metà del 2023. Il 60% delle società di e-commerce e il 53% dei retailer hanno subito un'impennata nel numero di frodi di tutti i livelli. I canali digitali hanno rappresentato il 52% di tutte le perdite dovute a frodi nell'area EMEA, sorpassando per la prima volta le frodi fisiche a causa dell'anonimità delle transazioni digitali.

Il risultato? L'anno scorso, le perdite dovuta ad attività fraudolente nel retail all'interno dell'area EMEA sono aumentate a livello globale, arrivando a 11,3 miliardi di sterline nel Regno Unito e 15 miliardi di euro in Spagna. Il 94% dei negozi online in Germania sono stati interessati dalle frodi, di cui il 20% hanno subito perdite pari a più di 100.000 euro.

Non si tratta solo di una questione di sicurezza, ma di una sfida dell'IT da risolvere per i CTO e i CIO. È un problema di ottimizzazione aziendale. Per i brand del retail e i responsabili del marketing in particolare, gli abusi online possono alterare i dati dei prodotti, i siti web e il traffico relativo all'engagement dei clienti, influendo sulla strategia e sui budget, nonché sulla fiducia e sulla reputazione duramente conquistate dalle aziende. Inoltre, l'impatto sulla crescita aziendale può essere devastante.

Si tratta di una sfida business-critical con lo stesso obiettivo finale di migliorare il percorso d'acquisto dei clienti e aumentare la loro fidelizzazione. In questa nuova epoca delle frodi online, i team devono superare i compartimenti stagni e collaborare con i vari reparti per risolvere questo problema.

Come afferma Susan McReynolds, che svolge il ruolo di Global Industry Strategist per il commercio di Akamai, ***"per gestire e difendere il percorso d'acquisto dei clienti, proteggere i profitti, i brand e i ricavi, è necessario comprendere l'impatto del ciclo di vita degli ordini".***

Questo rapporto descrive:

- Come la pandemia ha cambiato la natura delle minacce digitali nel retail
- Perché i retailer devono agire subito
- Le tendenze nelle frodi attuali ed emergenti
- Il loro impatto sui brand e sui ricavi
- Come affrontare queste sfide

Sezione 1. Come sono cambiati i bot e perché questo aspetto è importante

Durante la pandemia di COVID-19, il fatto di affidarsi maggiormente alle piattaforme digitali (sia da parte delle aziende che dei consumatori) ha introdotto tutta una serie di nuove vulnerabilità, riplasmando, in pratica, lo scenario delle frodi online. Come? I criminali vanno dove sentono odore di denaro e, durante la pandemia, i soldi si sono spostati più che mai online.

L'eccezionale domanda di alcuni prodotti, come carta igienica, igienizzanti, alimenti per bambini e attrezzature per allenarsi a casa, hanno creato opportunità redditizie per gli operatori dei bot che hanno cercato di sfruttare queste condizioni. I bot scraper, ad esempio, hanno acquistato gli articoli più richiesti per rivenderli a prezzi gonfiati allo scopo di capitalizzare sulla carenza di prodotti e sull'elevata domanda dei consumatori.

Fino a quel punto, i bot scraper non avevano causato danni estesi e non si erano fatti praticamente notare, pertanto, era più semplice affrontarli con i tradizionali strumenti di sicurezza. Tuttavia, poiché hanno rappresentato il primo passo che ha condotto ad una razzia degli inventari, risultata sicuramente molto redditizia, gli operatori dei bot hanno deciso di investire un notevole numero di risorse per rendere gli scraper più elusivi.

Nello stesso tempo, i miglioramenti apportati all'apprendimento automatico e all'intelligenza artificiale hanno creato la tempesta perfetta che ha consentito ai criminali di raggiungere il loro obiettivo. È inoltre aumentata la possibilità di sferrare più attacchi contemporaneamente, tramite tecniche di elusione sofisticate, come la rotazione di proxy e indirizzi IP, per bypassare i tradizionali sistemi di rilevamento dei bot. **Come ha dichiarato Richard Meeus, direttore del reparto Security Technology and Strategy per l'area EMEA di Akamai,*"i bot stanno diventando sempre più intelligenti: riescono ad imitare esattamente un essere umano e possono entrare/uscire dai sistemi in modo praticamente invisibile, il che li rende più difficili da rilevare e contrastare. Inoltre, arrivano in enormi quantità, da migliaia di posti diversi, pertanto, nessun retailer può considerarsi immune".***

La crescita astronomica delle transazioni online causata dalla pandemia (le vendite complessive nel retail online sono cresciute, in media, dal 16% al 19% nel 2020) ha anche registrato un aumento di forme di frodi più dirette, come il controllo degli account (ATO) e gli attacchi di phishing sferrati allo scopo di rubare informazioni sensibili. I retailer hanno trovato difficoltà nel distinguere le interazioni di clienti legittimi dalle attività dannose dei bot e i criminali hanno sfruttato questi punti deboli presenti nelle risorse tecnologiche del settore del retail.

Sfortunatamente, queste vulnerabilità rimangono ancora oggi. I retailer faticano a tenere il passo con l'evoluzione degli abusi e delle frodi digitali, che crescono a dismisura più rapidamente che mai. Inoltre, con l'aumento dell'e-commerce a livello globale (circa il 22% delle vendite complessive del retail nel 2024, una percentuale che si prevede salirà fino al 27% entro il 2026), sui retailer ricade l'onere di proteggere il numero crescente di clienti legittimi che effettuano acquisti online.

Sezione 2. Come le attività dannose riducono i ricavi nel retail e minano la fiducia dei consumatori

L'impatto delle attività dannose sui retailer, in pratica, influisce sul loro fatturato. Da uno studio recente, è emerso che ai commercianti, in media, **ogni frode da 1 dollaro costa 3 dollari**. Le ultime cifre del 2023 indicano che il costo totale delle frodi nell'e-commerce in tutto il mondo **supera la cifra di 48 miliardi di dollari**, a cui si è passato **dai 41 miliardi di dollari raggiunti nel 2022**. Le perdite cumulative dovute alle frodi online a livello globale sono salite a **343 miliardi di dollari**, ossia una cifra più di tre volte superiore all'utile netto realizzato da Apple nel 2023.

Qui stiamo parlando solo, ovviamente, dell'impatto finanziario, ma esiste anche un valore incalcolabile (e, senza dubbio, notevolmente più costoso) derivante dalla perdita del vantaggio competitivo e dal fatto che vengano intaccati il brand, la fedeltà e la fiducia dei consumatori. Quindi come e quando tutto ciò si manifesta nelle attività aziendali?

Il ruolo dello scraping nel mirare l'esclusività e le strategie relative ai prezzi

Lo scraping, ossia la pratica di estrarre i dati dai siti web tramite i bot automatizzati, pone una minaccia significativa per i brand, le strategie relative ai prezzi e l'esclusività dei prodotti dei retailer. Inoltre, molte società di retail non sanno neanche di avere un problema di scraping o, ancora peggio, non si rendono conto del reale impatto che questo tipo di attività può esercitare sulle loro aziende.

Ecco sei modi con cui lo scraping può danneggiare le attività aziendali:

1. Monitoraggio e abbassamento dei prezzi

Le aziende concorrenti possono usare i bot di scraping per monitorare costantemente i dati relativi ai prezzi di un retailer. Con queste informazioni a disposizione, possono così influenzare i prezzi del retailer, rendendo difficile mantenere un vantaggio competitivo o implementare in modo efficace strategie dinamiche relative ai prezzi.

2. Svantaggi rispetto alla concorrenza

A questo punto, effettuando analisi più approfondite, lo scraping dei dati su prezzi, prodotti e inventari consente alle aziende concorrenti di ottenere informazioni preziose sulle strategie di un retailer e di adattare, di conseguenza, le proprie tattiche per ottenere un vantaggio sleale sulla concorrenza. Insomma, non si gioca più alla pari.

3. Perdita di esclusività e valore del brand

Siete a conoscenza di tutto l'impegno profuso dal vostro team addetto al marketing per la creazione di descrizioni e immagini relative ai prodotti? Tutte queste informazioni, insieme ad altri contenuti proprietari, possono essere estratte dal sito web di un retailer da parte dei bot di scraping. Quindi, questi contenuti sottratti possono essere usati per creare elenchi contraffatti o non autorizzati sui mercati di terze parti o, persino, su siti web di tipo simile allo scopo di minare l'esclusività e il valore dei brand.

In una visione più ampia, si tratta di un problema di impersonificazione del brand. Alcuni rivenditori non sono dannosi, ma molti lo sono e, quindi, ad esempio, configurano le pagine dei loro siti web esclusivamente per rubare i dati delle carte di credito. Il problema è che i vostri clienti non riusciranno a capire la differenza tra di essi.

4. Furto di inventari

I bot possono esfiltrare i dati degli inventari in tempo reale e bypassare i limiti di acquisto o i sistemi di accodamento, fornendo un vantaggio sleale sui clienti, consentendo così, come già detto in precedenza, ai rivenditori o agli scalper di accaparrarsi gli articoli in edizione limitata o gli oggetti più richiesti, come le PlayStation, i cosmetici o le scarpe di tendenza, impedendo ai clienti legittimi di effettuare gli acquisti desiderati o, se anche possono farlo, molti di questi rivenditori alzeranno i prezzi anche di tre volte, abbassando il livello di soddisfazione dei clienti più fedeli.

5. Livelli degli inventari non accurati

I bot che si accaparrano o acquistano grandi quantità di prodotti possono consumare rapidamente i livelli degli inventari, causando un esaurimento delle scorte (e un maggior numero di clienti insoddisfatti), il che si ripercuote negativamente sulle previsioni di vendita.

6. Metriche di marketing alterate

Questi bot agiscono come gli esseri umani e le loro analisi riflettono questa situazione, andando ad alterare i dati relativi al marketing. Nel caso di un cliente di Akamai, era emerso che il 90% del suo traffico proveniva dai bot e che, quindi, aveva influito notevolmente sulle sue campagne di marketing e sui costi del cloud.

Come ha sottolineato Christine Ross, Product Marketing Director di Akamai: "I clienti ci hanno detto di ricevere in continuazione sui loro siti web il ping di alcuni prodotti, che sembrava fossero molto popolari, ma, in realtà, si trattava di bot, non di esseri umani. Quindi hanno acquistato prodotti particolari perché ritenuti popolari, ma, in realtà, non erano stati acquistati da altre persone e quella pagina in particolare non era mai stata visitata. Questi aspetti influiscono sulle importanti decisioni relative all'ottimizzazione di siti web e inventari. Se, talvolta, non vengono estratti i dati dei bot, l'ottimizzazione viene effettuata a vantaggio dei bot, non dei clienti, eliminando così il ROI derivante dal marketing e ostacolando la crescita aziendale".

Diminuzione delle performance dei siti e relative ripercussioni sull'engagement degli utenti

Un'altra area che ne ha risentito notevolmente è rappresentata dalle performance dei siti web, la "finestra" sul mondo dei retailer. I bot che eseguono lo scraping o che si accaparrano gli inventari possono sovraccaricare l'infrastruttura del sito web di un retailer, facendo rallentare i tempi di caricamento, incrementare i costi dei server e aumentare le interruzioni del sito. Questo peggioramento delle performance influisce direttamente sull'engagement degli utenti in quanto i clienti che riscontrano problemi di caricamento lento delle pagine o di downtime sono più propensi ad abbandonare il sito, passando potenzialmente alla concorrenza.

Considerando il fatto che il numero medio di visualizzazioni di pagine per ogni sessione di acquisto ha superato le 20 pagine nel 2023, a indicare la necessità di aumentare il numero di pagine e i contenuti da convertire, diventa sempre più cruciale garantire elevate performance ai siti web. La frustrazione degli utenti relativamente ai siti di retail è reale e diffusa, poiché riguarda il 40% delle experience degli acquirenti. Questo aspetto è correlato ai tassi di conversione e costa ai retailer quasi 0,60 dollari per ogni visita.

Un nemico della fidelizzazione è rappresentato anche da user experience scarse. I clienti che tornano a visitare un sito mostrano un tasso di conversione quattro volte superiore rispetto a quello dei nuovi clienti e provengono con minore probabilità da canali a pagamento. Per i responsabili del settore marketing con budget limitati, ad esempio, questo è un aspetto di cui tenere particolarmente conto.

Le violazioni degli account e i costi associati in termini economici e di danni alla reputazione

Le campagne di phishing e gli attacchi di credential stuffing sferrati da bot possono condurre a violazioni degli account dei clienti, con danni particolarmente elevati. Le credenziali rubate possono quindi essere usate per il controllo degli account, il furto di identità o, persino, le violazioni di dati, tutti problemi che influiscono sulle finanze e sulla sicurezza dei clienti, e la colpa è solo vostra.

Dal punto di vista di un retailer, gli accessi agli account non autorizzati possono condurre immediatamente a riaddebiti e ordini fraudolenti, furto di punti fedeltà, abuso di coupon/promozioni, rivendita di account e attacchi di convalida CVV, solo per nominarne alcuni. Tra le conseguenze degli attacchi di controllo degli account, figurano la sostituzione delle risorse per i clienti, potenziali sanzioni, la diminuzione della fiducia nei confronti dei brand, l'aumento dei costi per le indagini relative alle frodi e lo stress dei team addetti alle frodi, alla sicurezza e al marketing.

Relativamente alle violazioni di dati, tra i costi necessari per risolvere questi problemi, figurano le seguenti voci:

Aumento dei costi operativi

(ad es., sicurezza, conformità o, persino, come nel caso di Neiman Marcus nel 2021, un call centre dedicato ai reclami dei clienti relativamente al modo con cui avevano riscontrato i problemi).

Servizi di monitoraggio di crediti e rimborsi

per i clienti interessati (ad es., Hudson Bay nel 2018 ha offerto servizi di protezione delle identità dei clienti che avevano subito episodi di violazione).

Soluzioni di controversie e spese legali

Dopo una violazione del 2013 relativamente ai dati delle carte di credito, Target, il gigante del retail, ha dovuto regolare una serie di cause legali, che, in totale, sono costate circa 300 milioni di dollari. L'impatto sulla crescita dell'azienda è stato devastante: i profitti di Target si sono dimezzati nel 4° trimestre dello stesso anno rispetto all'anno precedente e il prezzo delle sue azioni è sceso del 9% nei due mesi successivi.

Indagini e sanzioni normative

Nel caso di Target, il dipartimento di giustizia degli Stati Uniti ha avviato un'indagine. Quando nel 2018 si verificò una violazione dei dati di 14 milioni dei suoi clienti, l'azienda Dixons Carphone venne condannata dall'ICO (Information Commissioner's Office) nel Regno Unito a pagare la massima sanzione, pari a 500.000 sterline.

I costi relativi ai danni alla reputazione in seguito a violazioni di dati e account influiscono anche sulla crescita complessiva delle aziende. Il 54% dei clienti afferma che cambierebbe brand nel caso di una violazione di dati. Dopo una violazione, i prezzi delle azioni per le società quotate in Borsa subiscono, in media, una perdita del 3,5%. Nel caso della Dixons Carphone, la riduzione dei profitti ha portato alla chiusura di 100 negozi di Carphone Warehouse in un anno e dell'intero brand Carphone Warehouse entro il 2020.

La violazione degli account è un fattore significativo nella percezione e nella fidelizzazione dei clienti, che sono al centro degli obiettivi di ogni brand e di ogni responsabile del marketing. Ad esempio, prima della violazione la percezione dei clienti di Target era classificata con un Brand Index Buzz pari a 20,7, che è sceso drasticamente a 9,4 l'anno successivo. Cinque anni dopo, questa valutazione era risalita a 17,3 a indicare la difficoltà a risalire la china per riguadagnare la fiducia da parte dei clienti. Nel nostro mondo connesso e invaso dai social media, la percezione dei brand può essere costruita o demolita in pochi minuti.

Anche il mutevole comportamento dei consumatori insieme al costo della vita ha sovvertito la fedeltà dei clienti. La fiducia dei clienti, che è la porta d'accesso per la fidelizzazione, è la chiave per raggiungere la nuova generazione di consumatori e per promuovere una crescita aziendale sostenibile. I millennial e la generazione Z mostrano i minimi livelli di fiducia nei confronti dei brand, forse perché circa il 20% di essi ha subito una violazione di dati (rispetto al 2% dei consumatori che appartengono alla generazione X e al 10% dei Baby Boomers).

Pertanto, costruire la fiducia dei consumatori richiede user experience rapide, agevoli e senza frodi. Gli acquirenti sono disposti a pagare il 46% in più con un retailer di cui si fidano. E quali sono i fattori principali che consentono di conquistare la fiducia dei clienti? Un processo di pagamento sicuro e la protezione dei dati personali dei clienti. Come emerso in uno studio globale del 2023, quasi il 90% dei consumatori afferma che questi fattori sono essenziali per consentire ai retailer di conseguire questo obiettivo. In cima alla lista, con il 76% degli intervistati, figura anche una solida reputazione dei brand.

Conclusione: contrastare bot e abusi con un allineamento aziendale

Considerando la crescita dilagante di queste tecnologie illecite, potrebbe sembrare un'altra sfida difficile da affrontare. Ma non è necessariamente così. La buona notizia è che esistono metodi efficaci per controllare il proprio brand e migliorare le customer experience. Ma da dove iniziare?

Le strategie per la protezione del brand e del fatturato

Non sorprende che team diversi siano, solitamente, incentrati sulla protezione di aspetti diversi: il team addetto alla sicurezza protegge i dati, il team del marketing protegge i ricavi, l'IT protegge le interruzioni, il team addetto alle CX protegge il percorso d'acquisto dei clienti. Tuttavia, questi team devono affrontare varie sfide:

- *Comunicano tra loro e si scambiano informazioni sugli obiettivi e sui risultati aziendali?*
- *Possono rispondere alla domanda "Le parti interessate sono allineate sugli strumenti e sui requisiti tecnici necessari per proteggere i dati dei clienti, i brand e i ricavi?"*

A questa domanda, ci è stato risposto perlopiù in modo negativo, ma si tratta di una questione fondamentale. Tra le altre domande principali a cui questi team devono essere in grado di rispondere, figurano le seguenti:

- *Quali sono i risultati che stiamo cercando di conseguire (ad es., protezione dei ricavi, dei dati dei clienti, del percorso d'acquisto o dalle frodi)?*
- *Abbiamo bisogno di una sola soluzione o di più soluzioni per risolvere le varie sfide delle parti interessate e per l'applicazione a diversi casi di utilizzo?*
- *L'acquirente non corrisponde all'utente di una soluzione?*
- *Quali sono i fattori per il successo? Abbiamo stabilito dei KPI chiari?*
- *Cosa siamo propensi a tollerare o quali compromessi sono richiesti per bilanciare la sicurezza con la necessità di ottimizzare il percorso d'acquisto?*
- *Stiamo proteggendo tutto il nostro patrimonio (sito web, app mobili, API e infrastrutture)?*
- *In che modo riusciamo a gestire le risorse desiderate/non desiderate e tutta la confusa frontiera che si frappone tra di esse?*

Ogni team deve comprendere questi punti e disporre di un obiettivo condiviso in grado di favorire l'allineamento e gli interventi necessari per raggiungere risultati ottimali per l'azienda.

Le frodi nel retail stanno aumentando ad un ritmo sempre più veloce diffondendosi a macchia d'olio tra i retailer. Come abbiamo descritto, le perdite non si limitano a quanto visibile facilmente su un libro mastro, dalle sanzioni, alle controversie o alle spese legali, ma colpiscono direttamente all'obiettivo finale del retailer che consiste nel favorire i ricavi tramite la fedeltà al brand e la fidelizzazione, che si fondano sulla fiducia e sulle customer experience: tutti fattori che diminuiscono in un batter d'occhio in caso di attività fraudolente.

L'incremento degli abusi, insieme al difficile scenario di acquisto dei consumatori e al costante aumento delle vendite online, implica che per i retailer ora è più importante che mai dare priorità e investire in avanzate misure di sicurezza per proteggere i propri brand e i propri clienti. Le unità aziendali devono, pertanto, collaborare per comprendere e condividere l'impatto degli attacchi, che non sono più soltanto appannaggio dei team addetti alla sicurezza e all'IT.

Per richiedere assistenza, potete contattare il team di Akamai o scoprire ulteriori informazioni sulle soluzioni per il retail e per il settore turistico-alberghiero. Akamai aiuta retailer e brand in tutto il mondo, come Lufthansa, Wagner eCommerce Group, Panasonic e TOUS, ad offrire online experience sicure e coinvolgenti da oltre 25 anni.

Informazioni su Akamai

A sostegno e protezione della vita online c'è sempre Akamai. Le principali aziende al mondo scelgono Akamai per creare, offrire e proteggere le loro experience digitali, aiutando miliardi di persone a vivere, lavorare e giocare ogni giorno. L'Akamai Connected Cloud, una piattaforma edge e cloud ampiamente distribuita, avvicina le app e le experience agli utenti e allontana le minacce. Per ulteriori informazioni sulle soluzioni di cloud computing, sicurezza e delivery dei contenuti di Akamai, visitate il sito akamai.com o akamai.com/blog e seguite Akamai Technologies su X (in precedenza Twitter) e LinkedIn.

Questo articolo viene offerto in collaborazione con Retail Gazette, la maggiore pubblicazione sul retail B2B del Regno Unito.

Visitate il sito **www.retailgazette.co.uk** per unirvi agli altri 300.000 utenti mensili e accedere gratuitamente alle più recenti notizie, interviste, analisi, rapporti approfonditi e white paper.

Data di pubblicazione: 07/24