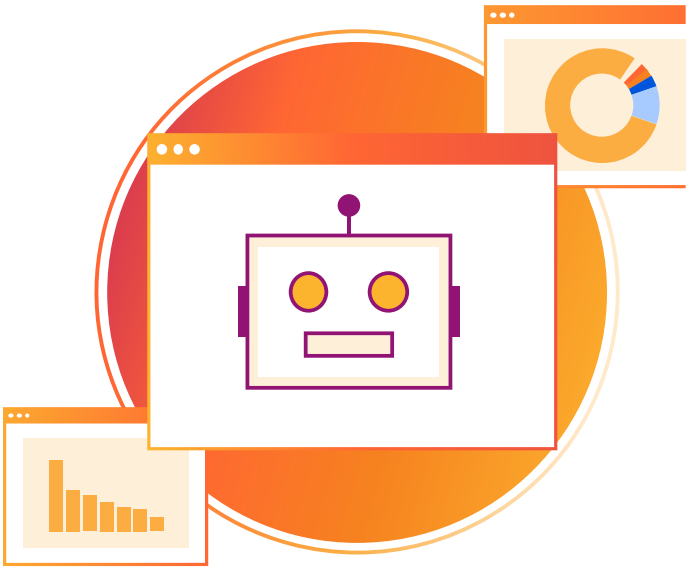
Quattro strategie per gestire i bot dannosi

Come evitare danni costosi e perdite di fatturato causate da bot indesiderati

I bot sono ovunque su Internet

I bot sono comuni nell'Internet moderno perché aiutano ad automatizzare attività importanti. Si stima che il 40-50% del traffico Internet totale sia gestito da bot e molti di questi svolgano funzioni aziendali legittime.

Tuttavia, i bot vengono spesso utilizzati anche dai criminali per attaccare le proprietà Web e causare danni ingenti. I bot dannosi possono rubare dati, violare gli account utente, inviare dati spazzatura tramite moduli online ed eseguire altre attività dannose. Questi bot dannosi sprecano preziose risorse di calcolo e del sito, rubano dati e alterano l'analisi del traffico.



Cos'è la gestione dei bot?

La gestione dei bot si riferisce al blocco del traffico di bot Internet indesiderati o dannosi, consentendo comunque ai bot utili di accedere alle proprietà Web. Ciò avviene rilevando l'attività dei bot, distinguendo tra comportamenti desiderati e indesiderati e identificando le origini delle attività indesiderate.

Perché è importante?

La gestione dei bot è necessaria perché i bot, se non controllati, possono causare problemi enormi e costosi. Le organizzazioni devono assicurarsi di non bloccare i bot necessari, come i bot di scansione dei motori di ricerca, mentre provano a filtrare il traffico di bot dannosi verso le loro proprietà Web.

Cosa si può fare?

Identificare e bloccare i bot dannosi prima che lancino attacchi è una componente fondamentale di qualsiasi buona strategia di sicurezza. Abbiamo condiviso quattro storie di veri clienti Cloudflare che hanno affrontato le loro problematiche di gestione dei bot con quattro diverse strategie utilizzando i prodotti Cloudflare.

Bloccare i bot

Questo approccio richiede molta attenzione perché numerosi processi aziendali legittimi, come l'indicizzazione sui motori di ricerca, richiedono che i bot possano accedere alle risorse aziendali.

Bloccare i bot		
Problema	**Soluzione**	**Risultati**
Una società di iGaming ha riscontrato un aumento significativo dei reclami da parte degli utenti. I loro account sono stati violati e le informazioni delle carte di credito sono state rubate. I malintenzionati utilizzavano bot automatizzati per forzare le credenziali di accesso, ottenendo l'accesso agli account degli utenti e infine prendendone il controllo.	Il team di sicurezza ha applicato la **limitazione della frequenza** e la **gestione dei bot** avanzata per rilevare più tentativi di accesso in breve tempo. Quando veniva rilevato un comportamento insolito, la limitazione della frequenza iniziava a bloccare automaticamente le richieste dannose. Dall'implementazione della funzionalità di limitazione della frequenza, la società di iGaming non ha più subito un singolo attacco di sottrazione e uso illecito delle credenziali.	Tutte le aziende devono trovare il giusto equilibrio tra una sicurezza rigorosa e un'esperienza utente ottimale. Il giusto set di strumenti può aiutare a rilevare e prevenire il traffico di bot dannosi, riducendo al minimo i falsi positivi e gli ostacoli per gli utenti reali.

Rallentare il nemico

Questa tecnica aumenta al massimo il tempo di risposta per tutte le richieste di rete sospette.

Rallentare il nemico		
Problema	**Soluzione**	**Risultati**
Una società di scommesse sportive ha riscontrato una notevole riduzione delle transazioni. Analizzando il problema, ha individuato un'attività bot dannosa che sfruttava le probabilità di successo sul sito Web e utilizzava tali informazioni per ottenere un vantaggio competitivo.	L'azienda non ha bloccato i bot perché i malintenzionati avrebbero aggirato il blocco, invece, ha rallentato l'acquisizione dei dati per le scommesse. Ha utilizzato **Headers Override** per contrassegnare le richieste sospette in base all'analisi di **gestione dei bot**, seguito dagli script **Workers** per reagire a queste intestazioni e rallentare le richieste.	Questo metodo ha consentito all'azienda di ripristinare la normale attività degli utenti. Altri metodi includono l'utilizzo di CAPTCHA per richieste ad alto volume o la modifica del markup HTML a intervalli regolari. Queste azioni interrompono il flusso di lavoro del bot, rendendo più complessa lo scraping di contenuto.

Ingannare i bot

Anche se molte aziende implementano contromisure per i bot, un malintenzionato particolarmente determinato può aggirarle. Invece, alcune aziende decidono di contrattaccare.

Ingannare i bot		
Problema	**Soluzione**	**Risultati**
Una società di scommesse sportive ha cercato di trovare una soluzione al problema dei bot che estraggono le quote dal loro sito Web. Dopo un'attenta riflessione, hanno deciso di lanciare una soluzione alternativa con diversi prodotti Cloudflare che avrebbe consentito loro di fornire ai bot informazioni casuali.	Quando il sistema rilevava che una richiesta era stata generata da un bot dannoso, accettava tale richiesta e avviava un nuovo flusso di lavoro: Richiesta → **WAF** (bot identificato) → **Gestione dei bot** (punteggio della minaccia assegnato) → **Workers** (generazione di dati randomizzati) → **Workers** (restituzione dei dati randomizzati al bot)	Il nuovo flusso di lavoro generava nuovi dati casuali che venivano restituiti ai bot dannosi. Di conseguenza, i bot che si occupavano di raccogliere risorse e infliggere danni se ne andavano con qualcosa di inutile, il che scoraggiava ulteriori abusi.

Eseguire un'analisi dinamica

Man mano che i bot diventano più sofisticati, le aziende devono raccogliere dati su di essi ed eseguire analisi dinamiche prima di agire. Tali obiettivi possono includere l'individuazione di registrazioni errate, quote, richieste di bonus, ecc. Per garantire un'analisi approfondita, i team di sicurezza potrebbero dover combinare più origini dati provenienti da strumenti sia interni che esterni per analizzare i parametri del traffico dei bot.

Eseguire un'analisi dinamica		
Problema	**Soluzione**	**Risultati**
Una società di scommesse ha lanciato una campagna di marketing per attrarre nuovi utenti offrendo premi per la registrazione. Poco dopo il lancio, si sono accorti che dei bot stavano creando registrazioni false. L'azienda disponeva già di alcuni strumenti di analisi interna, che però non fornivano un quadro completo del comportamento dei bot.	Il team ha implementato la **gestione dei bot** avanzata di Cloudflare con firme JA3 per generare i **file non elaborati** di tutto il traffico Internet in arrivo alla pagina di registrazione. Ha arricchito i sistemi interni con punteggi dei bot e firme JA3, che hanno consentito di identificare i bot più distintamente.	Dopo un'analisi approfondita, l'azienda è riuscita ad annullare le registrazioni false ed evitare di gonfiare le statistiche dei nuovi utenti acquisiti. Ha introdotto l'analisi regolare dei bot utilizzando le firme JA3 nelle sue best practice.

Stai sempre un passo avanti rispetto ai bot dannosi

Gestione dei bot con Cloudflare

Implementazione semplice
Nessuna configurazione o manutenzione complessa

Bassa latenza
Latenza mediana inferiore a 0,3 ms

Analisi dettagliata
Correlare i log del traffico con altre origini dati come SIEM o strumenti BI

Controlli precisi
Ottimizzare le regole, usare un generatore di regole visivo o scrivere le proprie regole di corrispondenza dei modelli

Fermare i bot dannosi prima che danneggino la tua attività

I bot diventano ogni giorno più complessi. Esistono limitazioni intrinseche al rilevamento e al blocco dei bot man mano che gli approcci degli aggressori diventano più sofisticati. Le aziende di oggi devono costantemente adattare le proprie strategie per far fronte al continuo rinnovamento degli aggressori, raggiungendo al contempo il giusto equilibrio tra una sicurezza elevata e la riduzione al minimo dell'attrito per l'utente.

Qualunque sia la strategia che decidi di adottare, assicurati che il tuo partner disponga di un set flessibile di strumenti per gestire i bot in modo efficace. Per saperne di più su come Cloudflare può aiutarti ad affrontare le difficoltà legate ai bot, contattaci per una valutazione personalizzata.

Intelligence di cui ti puoi fidare

Cloudflare gestisce circa il 20% di tutto il traffico Internet globale, fornendo un'ampia intelligence in tempo reale sui comportamenti dei bot dannosi nella rete Cloudflare.
Inoltre, Cloudflare collabora con numerosi partner che condividono informazioni sulle credenziali di accesso rubate, semplificando l'individuazione dei tentativi di acquisizione di account prima che si traducano in una vera e propria violazione.

Inizia il tuo viaggio verso una rete più veloce, più affidabile e più sicura

Richiedi una consulenza

Non sei pronto per la valutazione?

Scopri di più su Cloudflare