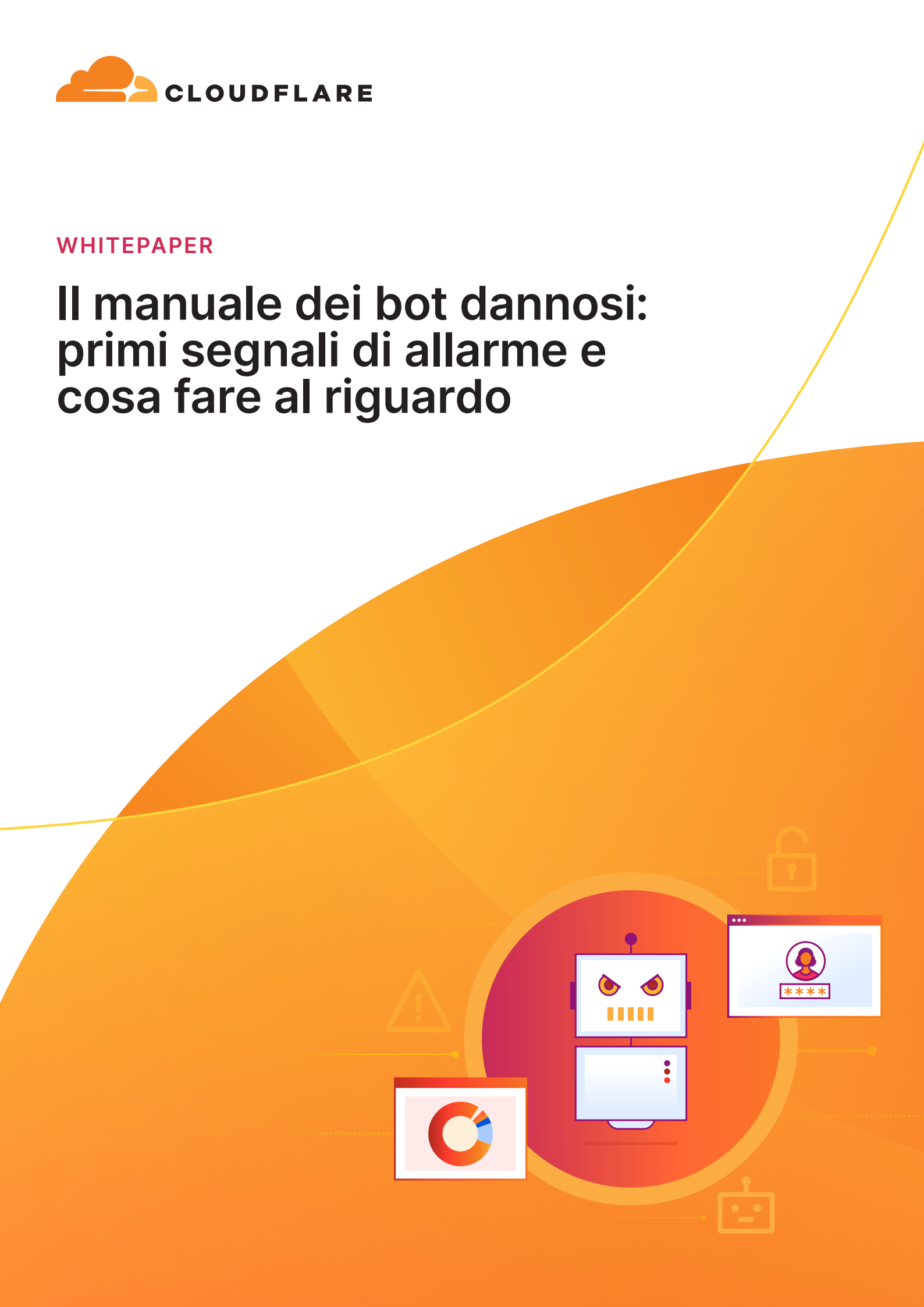
CLOUDFLARE

WHITEPAPER

Il manuale dei bot dannosi: primi segnali di allarme e cosa fare al riguardo



Indice

Introduzione

Oggigiorno i bot rappresentano circa il 30% del traffico online e molti di questi puntano a danneggiare organizzazioni come la tua: si stima che il 93% di questo traffico di bot non sia verificato e potenzialmente dannoso. La diffusione di attacchi di scraping di contenuti e prezzi, acquisizioni di account, furto di credenziali e carte di credito, accaparramento delle scorte e attacchi DDoS (Distributed Denial-of-Service) basati su botnet indica che i bot dannosi diventano ogni anno più complessi e sofisticati.

Inoltre, le tradizionali misure anti-bot, come il blocco della posizione, il blocco degli indirizzi IP e i CAPTCHA tradizionali, sono oggi inefficaci. In effetti, i CAPTCHA sono più facili da risolvere per i bot che per gli esseri umani.[1]

Per questo motivo, non esiste una singola tattica che possa fermare tutti i bot e impedirgli di danneggiare i tuoi utenti e il tuo marchio. L'unico approccio efficace è quello di prestare attenzione a una vasta gamma di segnali di allarme rivelatori di bot e di rispondere a ciascuno di essi raccogliendo dati e quindi implementando risposte mirate, rilevamento di modelli, analisi predittive e altre strategie complementari.

1. https://www.usenix.org/conference/usenixsecurity23/presentation/searles

Segnali di allarme di un problema con un bot

Monitorando una serie di potenziali indicatori, hai ottime possibilità di individuare i bot dannosi prima che possano causare danni gravi. Ecco cosa cercare:

Costi di infrastruttura più elevati senza aumento del business

Tutto il traffico verso il tuo sito Web comporta dei costi. Indipendentemente da chi o cosa accede ai tuoi contenuti, dovrai sostenere i costi di archiviazione e di elaborazione. Ma i bot dannosi possono aumentare i costi legati al traffico senza generare alcun guadagno per la tua attività. Mentre i bot buoni vengono utilizzati dai motori di ricerca per indicizzare i contenuti del tuo sito e quindi supportare il tuo posizionamento SEO, i bot cattivi comportano ogni anno costi di larghezza di banda eccessivi e significativi.

Acquisti insoliti di inventario a basso volume e ad alta domanda

Se ti accorgi di vendere una percentuale sospettosamente alta del tuo inventario a un sottoinsieme sorprendentemente piccolo di acquirenti, i colpevoli potrebbero essere i bot che accaparrano scorte. Mentre alcuni di questi bot si limitano a riempire e abbandonare i carrelli della spesa per bloccare i clienti legittimi, altri acquisteranno effettivamente il tuo inventario con l'obiettivo di rivenderlo a un prezzo più alto su altri siti.

Aumento dei reclami dei clienti

Un aumento dei ticket di supporto relativi a blocchi di account e transazioni fraudolente potrebbe essere il segnale della presenza di bot di sottrazione e uso illecito delle credenziali. Questi bot prendono il controllo degli account degli utenti legittimi con le informazioni raccolte dalle fughe di dati passate. Oltre ad avere un impatto negativo sull'esperienza del cliente, queste transazioni fraudolente sovraccaricheranno i server, allungando i tempi di caricamento delle pagine o addirittura rendendo il sito Web non disponibile.

Aumento dei tentativi di accesso non riusciti

Capita a tutti i clienti di digitare male la propria password, ma se all'improvviso si verifica un'ondata di tentativi di accesso non riusciti, è molto probabile che si tratti di un problema di bot. Mentre alcuni bot di sottrazione e uso illecito delle credenziali provano ad accedere agli account legittimi dei clienti tramite credenziali rubate, una tecnica più semplice e comune è quella di lanciare un attacco di forza bruta, in cui i bot tentano numerosi accessi rapidi utilizzando dizionari di migliaia di nomi utente e password comuni. Quando un bot supera il limite di accessi non riusciti per un determinato account, il vero proprietario umano di quell'account verrà bloccato finché non risolverai il problema: un vero grattacapo per l'esperienza utente.

Basso rendimento della spesa pubblicitaria

La pubblicità digitale può essere uno strumento efficace per aumentare il traffico verso il tuo sito, ma è anche un'arma redditizia per i bot dannosi. Molti bot del traffico imitano il comportamento degli utenti umani: cliccano ripetutamente sui tuoi annunci per aumentare la spesa pay-per-click (PPC), per poi abbandonarli senza effettuare un acquisto. Mentre alcune piattaforme pubblicitarie hanno implementato algoritmi di apprendimento automatico per ridurre le frodi di clic, gran parte di esse rimane inosservata.
Ecco perché è fondamentale essere proattivi e monitorare ogni clic che arriva tramite i tuoi annunci.

Analisi distorta delle visualizzazioni di pagina

Se le visualizzazioni della tua pagina aumentano improvvisamente senza un motivo apparente, la causa potrebbe essere un bot dannoso. Sebbene un picco di traffico possa provenire da utenti umani se hai appena lanciato un nuovo prodotto o la promozione di un evento, gli operatori di bot dannosi stanno diventando più astuti nell'implementare bot di scraping di contenuto proprio in questi momenti, rubando i tuoi contenuti e influenzando negativamente i tuoi dati analitici aggregati.

Aumento improvviso della creazione di account

Quando centinaia o addirittura migliaia di nuovi account utente compaiono all'improvviso, è possibile che dietro a questo afflusso ci siano dei bot. Possono usare questi profili falsi per riempire di spam le tue valutazioni pubbliche e commettere numerose altre forme di frode, minacciando non solo i tuoi ricavi e la fidelizzazione degli utenti, ma anche la credibilità del tuo marchio.

Duplicati dei tuoi contenuti su siti non approvati

Il fatto che altri siti condividano i tuoi contenuti può essere una buona idea, ma un improvviso aumento di contenuti duplicati è un segno distintivo dei bot di scraping di contenuto. Questi bot rubano le informazioni che hai impiegato del tempo per raccogliere e curare, consentendo agli operatori di siti malintenzionati di ospitarle sui domini di loro proprietà, aumentando così il loro traffico mentre il tuo subisce un colpo.

Traffico proveniente da aree geografiche insolite

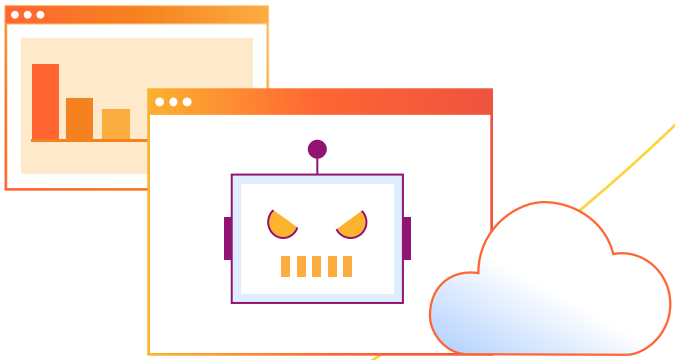
Picchi improvvisi provenienti da luoghi inaspettati potrebbero indicare attività di bot dannosi, soprattutto se questa attività si verifica in cluster, concentrati in regioni in cui i tuoi clienti non vivono o i tuoi servizi non sono disponibili. Tieni d'occhio qualsiasi attività sospetta che non sembra correlata alla tua base di utenti abituali.

Traffico da posizioni tipiche in orari insoliti

Proprio come i picchi di traffico provenienti da luoghi inaspettati possono indicare la presenza di bot dannosi, i picchi provenienti da luoghi normali in orari insoliti possono indicare che bot stanno cercando di camuffarsi da utenti abituali. Ad esempio, se noti un picco di attività in una regione comune nel cuore della notte, potresti voler analizzare più attentamente quel traffico.

Aumento degli errori di verifica delle carte

Un segno particolarmente pericoloso di bot dannosi è un aumento delle transazioni con carta di credito che non vengono convalidate. I bot di sottrazione e uso illecito delle carte di credito testeranno migliaia di numeri di carte di credito rubate nel tentativo di trovarne una che funzioni. Questa operazione viene eseguita effettuando acquisti di basso valore su siti Web meno sicuri, prima di eseguire transazioni più grandi su siti più importanti o vendendo i numeri di carta convalidati sul dark Web. Il tuo sito potrebbe tenere conto di questi piani in qualsiasi punto della catena e se le transazioni non riuscite sono abbastanza gravi, il tuo provider di servizi di pagamento potrebbe multarti.



2. https://www.entrepreneur.com/article/313943

Tattiche per combattere i bot

Poiché non esistono due attacchi di bot uguali, avrai bisogno di una combinazione di più strategie per fermarli tutti sul loro cammino. Considera alcune delle seguenti strategie:

Bloccare i bot dannosi non appena vengono rilevati

La risposta più evidente a un bot è anche una delle più efficaci: bloccare semplicemente tutto il traffico che hai identificato come proveniente da attività dei bot dannosi. Questa tattica da sola può farti risparmiare costi significativi su larghezza di banda e spazio di archiviazione, per non parlare della salvaguardia della fiducia dei consumatori e della reputazione del tuo marchio. Allo stesso tempo, ricorda che se un operatore di bot è particolarmente motivato, potrebbe cambiare tattica e tornare successivamente con una strategia di attacco diversa.

Aggiungi alla lista consentita tutti i bot validi di cui sei a conoscenza

Anche se rilevi e blocchi i bot dannosi, è fondamentale assicurarsi che i bot buoni dei motori di ricerca e dei partner siano ancora in grado di arrivare al tuo sito. Ciò non solo garantisce che il tuo posizionamento SEO rimanga solido, ma gestisce anche il traffico legittimo dei clienti in modo che scorra senza intoppi da servizi di terze parti che indirizzano il traffico a te. L'inserimento in una lista consentita semplifica inoltre notevolmente l'impostazione di regole di blocco dei bot che non influiscano negativamente sull'accesso dei visitatori umani.

Mettere alla prova i bot sospetti che vengono rilevati

Non appena si nota un modello di accessi sospetti, una bassa profondità di pagina o tempo trascorso sulla pagina, convalide di carte di credito non riuscite o qualsiasi altro comportamento di un bot di marchi registrati, è fondamentale implementare un test di sicurezza. In passato, l'uso dei CAPTCHA era considerato una best practice. Tuttavia, molti bot avanzati riescono ora a risolvere questi enigmi in modo ancora più rapido e accurato rispetto agli utenti umani.

Oggigiorno, l'approccio migliore è quello di utilizzare sfide senza CAPTCHA, in cui il software di "sfida" prende in considerazione una serie di fattori per determinare se l'utente è realmente un bot (ad esempio, rete, dispositivo, impronte digitali JavaScript). Le sfide "No CAPTCHA" come questa idealmente vengono integrate con una soluzione completa di gestione dei bot per la massima precisione (vedere Conclusione per maggiori informazioni).

Limitare la frequenza con cui gli utenti possono richiedere informazioni

La limitazione della frequenza può essere una tecnica efficace per tenere a bada i bot meno sofisticati. Impostando limiti rigidi al numero di volte in cui qualsiasi indirizzo IP può inviare richieste al tuo sito, impedirai molti semplicistici attacchi a forza bruta di bot, che provano ad accedere utilizzando migliaia di parole del dizionario e password comuni. Tuttavia, i bot odierni più avanzati possono mantenere il loro numero di richieste appena al di sotto del limite di frequenza rimanendo inosservati mentre continuano a infliggere danni.

Conservare log dettagliati di tutto il traffico del sito

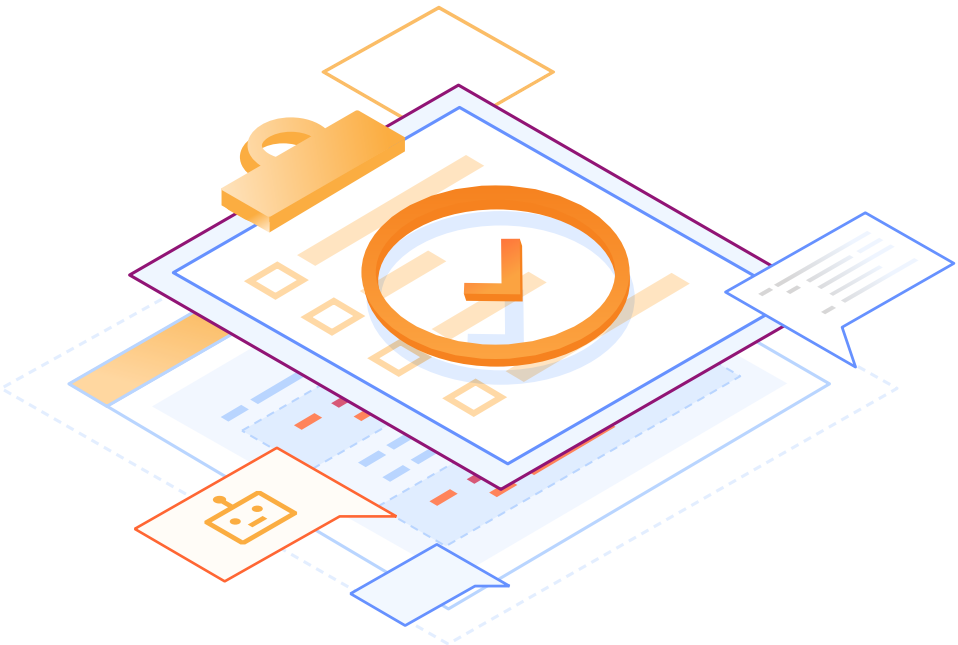
Sebbene sia probabile che tu stia già conservando log giornalieri di visualizzazioni di pagina e accessi all'account, log più dettagliati delle informazioni sugli utenti, come indirizzi IP, browser, dispositivi, sistemi operativi, geolocalizzazione, referrer, reti e visualizzazioni di pagina, possono rivelarsi inestimabili per il rilevamento modelli di attività più sottili. I log possono darti un'idea chiara di come i bot tendono a comportarsi sul tuo sito, consentendoti di impostare criteri di sicurezza più efficaci. Inoltre, i log sono spesso essenziali per la segnalazione e la conformità nel caso in cui si subisca effettivamente una violazione dei dati.

Reindirizzare i bot a contenuti alternativi

Quando sei abbastanza certo che una determinata fonte di traffico sia un bot, forniscigli un contenuto alternativo che ne consumi le risorse di calcolo. È persino possibile fornire dati falsi, come informazioni errate sui prezzi, ai bot di scraping di contenuto, rendendoli inutili per i loro operatori. Tecniche come queste ti permetteranno di guadagnare tempo per osservare il comportamento di ogni bot, comprenderne lo schema di attività e preparare una strategia per affrontarlo una volta per tutte.

Richiedere l'autenticazione aggiuntiva per tutti gli utenti

Man mano che gli attacchi di bot diventano più diffusi, un numero sempre maggiore di siti sta passando a misure di sicurezza rafforzate, anche per accessi umani legittimi. L'autenticazione a due fattori (2FA), ad esempio, richiede agli utenti di confermare la propria identità su più dispositivi o account, mentre le password monouso (OTP) possono scoraggiare i bot che sottraggono le credenziali rendendo gli account più difficili da decifrare. Ma ricorda che queste tecniche possono avere un impatto negativo sulla tua esperienza utente, aggiungendo attrito alla tua procedura di accesso.

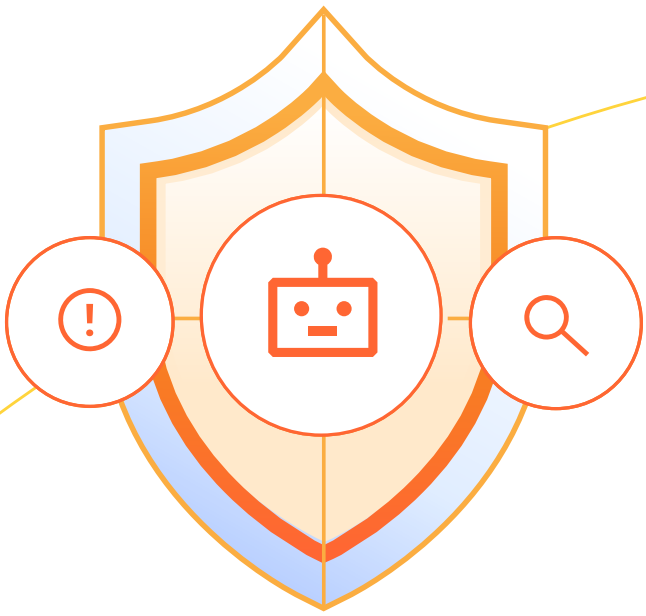


Conclusioni

Mentre esplori queste tattiche, ricorda: nessuna di esse, se utilizzata singolarmente, fermerà tutti i bot. Per proteggere la tua attività, probabilmente dovrai combinare diverse strategie e aggiungere un'analisi avanzata del modello multivariabile. Cloudflare Bot Management può aiutare le organizzazioni di diversi settori ad adottare questo approccio su più fronti. È integrato nella più ampia rete Cloudflare, che supporta milioni di proprietà Internet e si estende in più di 330 città in tutto il mondo.

Grazie all'intelligence continua delle minacce provenienti da tutta la rete, Cloudflare Bot Management offre analisi comportamentale, machine learning automatico e impronte digitali lato client per eliminare gran parte dello sforzo necessario per contrastare i bot dannosi. Inoltre, Cloudflare offre Turnstile, una sfida bot praticamente senza intoppi e senza CAPTCHA che può essere integrata in qualsiasi applicazione web con solo poche righe di codice.

Scopri di più su Cloudflare Bot Management.



+44 20 3514 6970 | enterprise@cloudflare.com | www.cloudflare.com/it-it/

REV:BDES-6333.2024SEPT03