CLOUDFLARE

KURZDARSTELLUNG

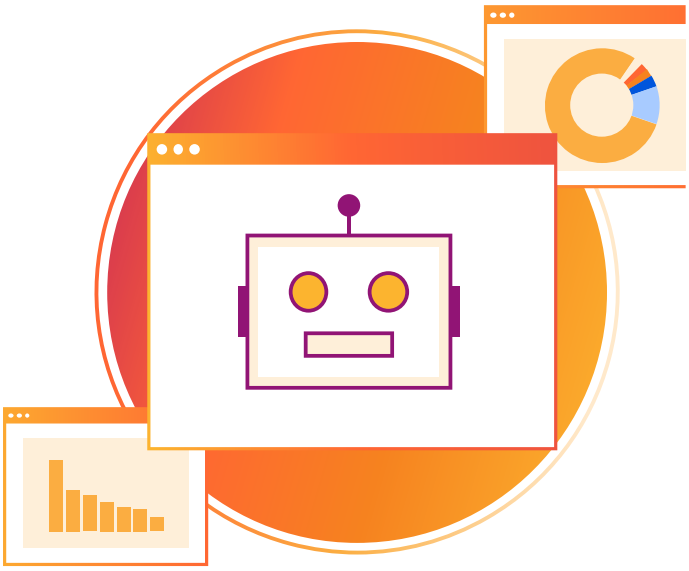
4 Strategien für den Umgang mit bösartigen Bots

Vermeiden Sie kostspielige Schäden und Umsatzeinbußen durch unerwünschte Bots

Bots sind im Internet allgegenwärtig

Bots sind im modernen Internet weit verbreitet, da sie dazu beitragen, wichtige Aufgaben zu automatisieren. Schätzungsweise 40-50 % des gesamten Internet-Traffics wird von Bots gesteuert, und viele dieser Bots führen legitime Geschäftsfunktionen aus.

Bots werden jedoch auch häufig von Kriminellen eingesetzt, um Websites anzugreifen und kostspielige Schäden zu verursachen. Bösartige Bots können Daten stehlen, in Nutzerkonten eindringen, Junk-Daten über Online-Formulare übermitteln und andere bösartige Aktivitäten durchführen. Diese bösartigen Bots verschwenden wertvolle Computer- und Website-Ressourcen, stehlen Daten und verfälschen Traffic-Analysen.



Was ist Bot-Management?

Unter Bot-Management versteht man das Blockieren von unerwünschtem oder bösartigem Bot-Traffic, ohne dass dabei nützlichen Bots der Zugriff auf Websites verwehrt wird. Dies geschieht, indem Bot-Aktivitäten erkannt, zwischen gewünschten und unerwünschten Bot-Verhalten unterschieden und die Ursachen für die unerwünschte Aktivität identifiziert werden

Warum ist das wichtig?

Bot-Management ist notwendig, da unkontrollierte Bots massive und teure Probleme verursachen können. Unternehmen müssen sicherstellen, dass sie notwendige Bots, wie z. B. Suchmaschinen-Crawling-Bots, nicht blockieren, während sie versuchen, jeglichen bösartigen Bot-Traffic zu ihren Websites herauszufiltern.

Was kann getan werden?

Ein wichtiger Aspekt wirksamer Sicherheitsstrategien ist die frühzeitige Erkennung und Blockierung von bösartigen Bots, bevor diese Angriffe starten. Wir haben vier Berichte von echten Cloudflare-Kunden zusammengestellt, die ihre Herausforderungen im Bot-Management mit vier verschiedenen Strategien unter Verwendung von Cloudflare-Produkten bewältigt haben.

Die Bots blockieren

Bei diesem Ansatz ist Vorsicht geboten, da viele legitime Geschäftsprozesse, wie z. B. die Indizierung durch Suchmaschinen, den Zugriff von Bots auf Unternehmensressourcen erfordern.

Die Bots blockieren		
Die Herausforderung	**Die Lösung**	**Ergebnisse**
Ein iGaming-Unternehmen bemerkte eine deutliche Zunahme der Beschwerden von Nutzern. Ihre Konten wurden gehackt und Kreditkarteninformationen gestohlen. Böswillige Akteure setzten automatisierte Bots ein, um mit Brute-Force-Angriffen die korrekten Anmeldedaten zu ermitteln, sich Zugang zu Nutzerkonten zu verschaffen und diese schließlich zu übernehmen.	Das Sicherheitsteam setzte **Rate Limiting** zusammen mit erweitertem **Bot Management** ein, um mehrere Anmeldeversuche innerhalb kurzer Zeit zu erkennen. Als ungewöhnliches Verhalten erkannt wurde, begann das Rate Limiting automatisch, schädliche Anfragen zu blockieren. Seit der Implementierung der Rate-Limiting-Funktion hat das iGaming-Unternehmen keinen einzigen Credential-Stuffing-Angriff mehr erlebt.	Alle Unternehmen müssen strenge Sicherheitsmaßnahmen mit einer optimalen Benutzererfahrung in Einklang bringen. Das richtige Toolset kann helfen, schädlichen Bot-Traffic zu erkennen und zu verhindern, während Fehlalarme und Hürden für echte Nutzer minimiert werden.

Den Feind ausbremsen

Mit dieser Technik wird die Antwortzeit für alle verdächtigen Netzwerkanfragen maximiert.

Den Feind ausbremsen		
Die Herausforderung	**Die Lösung**	**Ergebnisse**
Ein Sportwettenanbieter stellte einen erheblichen Rückgang der Transaktionen fest. Bei der Analyse des Problems wurde schädliche Bot-Aktivität festgestellt, die die Quoten auf ihrer Website abrief und diese Informationen nutzte, um sich einen Wettbewerbsvorteil zu verschaffen.	Das Unternehmen blockierte die Bots nicht, da die böswilligen Akteure die Blockade umgehen würden. Stattdessen verlangsamten sie das Abrufen von Daten für Wetten. **Sie verwendeten** Header Override (Header-Überschreibung), um verdächtige Anfragen auf der Grundlage einer **Bot-Management**-Analyse zu markieren, gefolgt von **Workers**-Skripten, um auf diese Header zu reagieren und die Anfragen zu verlangsamen.	Diese Methode ermöglichte es dem Unternehmen, die normale Aktivität der Nutzer wiederherzustellen. Andere Methoden sind die Verwendung von CAPTCHAs bei einer hohen Anzahl von Anfragen oder die regelmäßige Änderung des HTML-Markup. Diese Aktionen unterbrechen den Workflow des Bots, sodass kontinuierliches Content Scraping erschwert wird.

Die Bots täuschen

Obwohl viele Unternehmen Gegenmaßnahmen gegen Bots einsetzen, kann ein wirklich entschlossener Angreifer diese umgehen. Einige Unternehmen entscheiden sich stattdessen, sich zu wehren.

Die Bots täuschen		
Die Herausforderung	**Die Lösung**	**Ergebnisse**
Ein Sportwettenanbieter versuchte, eine Lösung für Bots zu finden, die Quoten auf seiner Website abrufen. Nach einiger Überlegung beschlossen sie, eine Umgehungslösung mit verschiedenen Cloudflare-Produkten einzuführen, die es ihnen ermöglichen würde, Bots mit zufälligen Informationen zu füttern.	Als das System feststellte, dass eine Anfrage von einem bösartigen Bot gestellt wurde, akzeptierte es diese Anfrage und erstellte einen neuen Workflow: Anfrage → **WAF** (Bot erkannt) → **Bot-Management** (Bedrohungswert zugewiesen) → **Workers** (randomisierte Daten generieren) → **Workers** (randomisierte Daten an Bot ausgeben)	Der neue Workflow generierte neue randomisierte Daten, die an die bösartigen Bots zurückgesendet wurden. Das Ergebnis war, dass Bots, die kamen, um Quoten abzurufen und Schaden anzurichten, mit etwas Nutzlosem verschwanden, was jeden weiteren Missbrauch verhinderte.

Dynamische Analysen durchführen

Da Bots immer ausgefeilter werden, müssen Unternehmen Daten über Bots sammeln und dynamische Analysen durchführen, bevor sie Maßnahmen ergreifen. Ziele können etwa die Erkennung von Falschanmeldungen, Quotenmanipulationen oder Bonusmissbrauch sein. Um eine gründliche Analyse zu gewährleisten, müssen Sicherheitsteams unter Umständen mehrere Datenquellen aus internen und externen Tools kombinieren, um die Parameter des Bot-Traffics zu analysieren.

Dynamische Analysen durchführen		
Die Herausforderung	**Die Lösung**	**Ergebnisse**
Ein Wettanbieter startete eine Marketingkampagne, um neue Nutzer mit Belohnungen für die Registrierung zu gewinnen. Kurz nach dem Start stellten sie fest, dass Bots gefälschte Registrierungen vornahmen. Das Unternehmen verfügte bereits über einige interne Analysetools, die jedoch kein vollständiges Bild des Bot-Verhaltens lieferten.	Das Team implementierte das fortschrittliche **Bot-Management** von Cloudflare mit JA3-Signaturen, um **Rohdatenprotokolle** des gesamten Internet-Traffics zu generieren, der auf die Registrierungsseite gelangt. Sie erweiterten ihre internen Systeme um Bot-Scores und JA3-Signaturen, wodurch sie Bots deutlicher identifizieren konnten.	Nach einer gründlichen Analyse war das Unternehmen in der Lage, gefälschte Registrierungen zu annullieren und eine Aufblähung der Statistik der neu gewonnenen Nutzer zu vermeiden. Die regelmäßige Bot-Analyse mit JA3-Signaturen wurde im Unternehmen in die Best Practices aufgenommen.

Bösartigen Bots stets einen Schritt voraus

Bot-Management von Cloudflare

Einfache Bereitstellung
Keine komplexe Konfiguration oder Wartung

Geringe Latenz
Mittlere Latenz von <0,3 ms

Aufschlussreiche Analysen
Korrelieren Sie Traffic-Protokolle mit anderen Datenquellen wie SIEMs oder BI-Tools

Präzise Steuerung
Regeln anpassen, einen visuellen Regelassistenten verwenden oder eigene Regeln für die Mustererkennung schreiben

Stoppen Sie bösartige Bots, bevor sie Ihrem Unternehmen schaden

Bots werden jeden Tag fortschrittlicher. Da die Angreifer immer raffinierter werden, sind der Bot-Erkennung und -Blockierung zwangsläufig Grenzen gesetzt. Unternehmen müssen ihre Strategien kontinuierlich anpassen, um neuen Angriffsformen standzuhalten und gleichzeitig das richtige Gleichgewicht zwischen hoher Sicherheit und minimaler Beeinträchtigung der Nutzer zu finden.

Unabhängig davon, für welche Strategie Sie sich entscheiden, sollten Sie sicherstellen, dass Ihr Partner über flexible Tools verfügt, um Bots effektiv zu verwalten. Wenn Sie mehr darüber erfahren möchten, wie Cloudflare Ihnen bei Ihren Herausforderungen mit Bots helfen kann, kontaktieren Sie uns, um eine persönliche Analyse zu erhalten.

Daten, denen Sie vertrauen können

Cloudflare wickelt etwa 20 % des gesamten weltweiten Traffics ab, wodurch wir umfangreiche Echtzeitinformationen über das Verhalten bösartiger Bots im Cloudflare-Netzwerk erhalten. Darüber hinaus arbeitet Cloudflare mit mehreren Partnern zusammen, die Informationen über gestohlene Anmeldedaten austauschen, wodurch es einfacher wird, Versuche der Kontoübernahme zu erkennen, bevor sie zu einem Datenverstoß führen.

Wechseln Sie jetzt zu einem schnelleren, zuverlässigeren und sichereren Netzwerk

Beratung anfordern

Sie möchten noch mehr Informationen?

Erfahren Sie noch mehr über Cloudflare