CLOUDFLARE

PRÉSENTATIONDE
SOLUTION

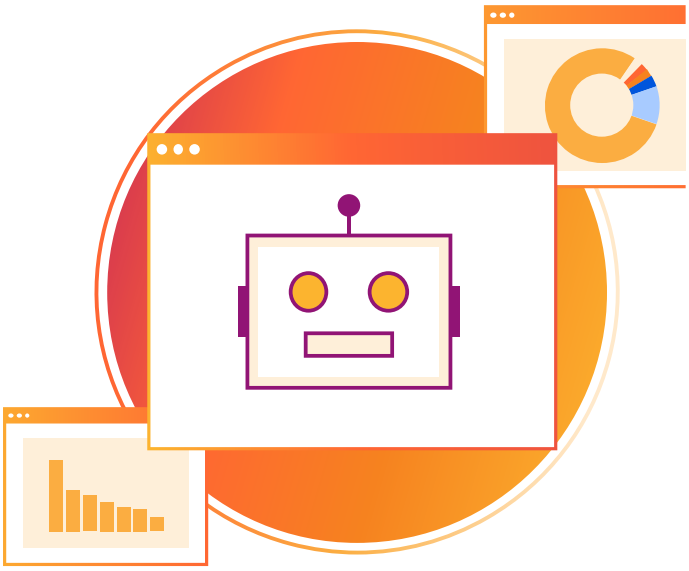
Quatre stratégies de gestion des bots malveillants

Évitez les dommages coûteux et les pertes de revenus dus aux bots indésirables

Les bots sont omniprésents sur Internet

Les bots sont très répandus sur l'Internet moderne, car ils contribuent à l'automatisation de tâches importantes. On estime que 40 à 50 % du trafic Internet total est généré par des bots, dont beaucoup exécutent des fonctions opérationnelles légitimes.

Cependant, les bots sont également souvent employés par des criminels pour lancer des attaques contre des propriétés web et causer des dommages coûteux. Les bots malveillants peuvent voler des données, infiltrer des comptes d'utilisateurs, transmettre des données indésirables via des formulaires en ligne et effectuer d'autres activités malveillantes. Ces bots malveillants consomment de précieuses ressources de sites et de traitement, dérobent des données et faussent les données analytiques concernant le trafic.



Qu'est-ce que la gestion des bots ?

La gestion des bots consiste à bloquer le trafic de bots indésirables ou malveillants, tout en permettant aux bots utiles d'accéder aux propriétés web. Pour cela, la solution de gestion des bots détecte l'activité des bots, distingue le comportement des bots légitimes de celui des bots indésirables et identifie les sources de toute activité malveillante.

Pourquoi est-elle importante ?

La gestion des bots est nécessaire, car s'ils ne sont pas contrôlés, les bots peuvent entraîner de graves et coûteux problèmes. Les entreprises doivent s'assurer qu'elles ne bloquent pas les bots nécessaires, tels que les bots d'indexation des moteurs de recherche, pendant qu'elles essaient de filtrer le trafic de bots malveillants affluant sur leurs propriétés web.

Que permet-elle de faire ?

La capacité d'identifier et de bloquer les bots malveillants avant qu'ils ne lancent des attaques est une composante vitale de toute stratégie de sécurité des applications. Nous avons publié quatre articles consacrés à des clients de Cloudflare, qui ont relevé les défis de la gestion des bots en appliquant quatre stratégies différentes employant les produits Cloudflare.

Bloquer les bots

Cette approche exige de la circonspection, car de nombreux processus opérationnels légitimes, tels que l'indexation par les moteurs de recherche, nécessitent que les bots puissent accéder aux ressources d'une entreprise.

Bloquer les bots		
Problématique	**Solution**	**Résultats**
Une société de jeux de hasard en ligne avait remarqué une augmentation considérable des plaintes d'utilisateurs, dont les comptes avaient été piratés et les informations de carte de paiement dérobées. Des acteurs malveillants utilisaient des bots automatisés pour exécuter des attaques par force brute afin d'obtenir des identifiants de connexion, d'accéder à des comptes d'utilisateurs et d'en prendre le contrôle.	L'équipe de sécurité a mis en oeuvre le service de **contrôle du volume des requêtes**, ainsi qu'un déploiement avancé du service Cloudflare **Bot Management**, afin de détecter les tentatives de connexion fréquemment renouvelées un délai réduit. Lorsqu'un comportement inhabituel était détecté, le service de contrôle du volume des requêtes commençait à bloquer automatiquement les requêtes malveillantes. Depuis la mise en œuvre du contrôle du volume des requêtes, la société de jeux en ligne n'a plus subi aucune attaque par bourrage d'identifiants (Credential Stuffing).	Toutes les entreprises doivent parvenir à équilibrer une sécurité rigoureuse et une expérience utilisateur optimale. Un ensemble d'outils performant peut contribuer à la détection et la prévention du trafic de bots malveillants, tout en minimisant les faux positifs et les désagréments pour les utilisateurs réels.

Ralentir l'ennemi

Cette technique consiste à maximiser les temps de réponse pour toutes les requêtes suspectes transmises au réseau.

Ralentir l'ennemi		
Problématique	**Solution**	**Résultats**
Une société de paris sportifs a constaté une diminution significative du nombre de transactions. Lorsqu'elle a analysé le problème, elle a décelé l'activité de bots malveillants qui récupéraient les cotes sur son site web, puis utilisaient ces informations pour s'arroger un avantage concurrentiel.	La société n'a pas choisi de bloquer les bots, car les acteurs malveillants auraient trouvé un moyen de contourner le blocage. Au lieu de cela, elle a ralenti la récupération des données concernant les paris. Elle a utilisé la fonction de **remplacement des en-têtes** pour identifier les requêtes suspectes en se fiant à l'analyse réalisée par le service Cloudflare **Bot Management**, puis elle a déployé des scripts **Workers** pour réagir à ces en-têtes et ralentir le traitement des requêtes.	Cette méthode a permis à l'entreprise de rétablir une activité normale des utilisateurs. Parmi les autres méthodes figurent l'utilisation de CAPTCHA pour les volumes élevés de requêtes ou la modification des balises HTML à intervalles réguliers. Ces actions interrompent le flux de travail des bots, rendant plus complexe l'extraction de contenus cohérents.

Duper les bots

Bien que de nombreuses entreprises déploient des contre-mesures contre les bots, un acteur malveillant vraiment déterminé peut les contourner. Certaines entreprises décident de riposter.

Duper les bots		
Problématique	**Solution**	**Résultats**
Une société de paris sportifs tentait de trouver une solution aux bots qui récupéraient les cotes sur son site web. Après réflexion, elle a décidé de déployer une solution de contournement reposant sur plusieurs produits Cloudflare, afin de fournir aux bots des informations générées aléatoirement.	Lorsque le système déterminait qu'une requête était générée par un bot malveillant, il acceptait cette requête et générait un nouveau flux de travail : Requête → **Pare-feu WAF** (identification d'un bot) → **Bot Management** (attribution d'un score de menace) → **Workers** (génération de données aléatoires) → **Workers** (envoi de données aléatoires au bot)	Le nouveau flux de travail générait de nouvelles données aléatoires, qui étaient transmises aux bots malveillants. Par conséquent, les bots qui venaient extraire des cotes en causant un préjudice pour le site récupéraient des données inutiles, ce qui a permis de décourager d'éventuels nouveaux abus.

Réaliser une analyse dynamique

À mesure que les bots deviennent toujours plus sophistiqués, les entreprises doivent collecter des données à leur sujet et réaliser une analyse dynamique avant de prendre des dispositions. Ces objectifs peuvent inclure la détection d'enregistrements incorrects, de cotes, de demandes de bonus, etc. Pour garantir une analyse approfondie, les équipes de sécurité peuvent être amenées à réunir plusieurs sources de données provenant d'outils internes et externes, afin d'analyser les paramètres du trafic de bots.

Réaliser une analyse dynamique		
Problématique	**Solution**	**Résultats**
Une société de paris a lancé une campagne de marketing afin d'attirer de nouveaux utilisateurs, en offrant des récompenses lors de l'inscription. Peu après le lancement de la campagne, elle a remarqué que des bots effectuaient de fausses inscriptions. L'entreprise disposait déjà d'outils de données analytiques internes, mais ces derniers ne fournissaient pas une représentation complète du comportement des bots.	L'équipe a mis en oeuvre un déploiement avancé du service Cloudflare **Bot Management** avec des signatures JA3, afin de générer des **journaux bruts** de l'ensemble du Internet affluant sur la page d'inscription. Elle a enrichi ses systèmes internes avec des scores de bots et des signatures JA3, ce qui lui a permis d'identifier plus précisément les bots.	Au terme d'une analyse approfondie, la société a pu annuler les fausses inscriptions et éviter de gonfler les statistiques de nouveaux utilisateurs. Elle a introduit, dans ses bonnes pratiques, une analyse régulière des bots avec les signatures JA3.

Gardez une longueur d'avance sur les bots malveillants

Cloudflare Bot Management

Un déploiement simple
Pas de configuration ou de maintenance complexes

Faible latence
Latence médiane (<0,3 ms)

Données analytiques riches
Corrélez les journaux de trafic avec d'autres sources de données, telles que les plateformes SIEM ou les outils d'information décisionnelle

Contrôles précis
Ajustez les règles, utilisez un générateur de règles visuel ou écrivez vos propres règles de correspondance

Interceptez les bots malveillants avant qu'ils ne causent un préjudice pour votre entreprise

Les bots deviennent plus avancés chaque jour. Il existe des limites inhérentes à la détection et au blocage des bots, car les approches des acteurs malveillants deviennent toujours plus sophistiquées. Les entreprises doivent aujourd'hui adapter continuellement leurs stratégies afin de faire face aux nouveaux outils des acteurs malveillants, tout en atteignant un point d'équilibre entre une sécurité renforcée et des désagréments minimaux pour l'utilisateur.

Quelle que soit la stratégie que vous décidez d'utiliser, assurez-vous que votre partenaire dispose d'un ensemble d'outils flexibles, permettant de gérer efficacement les bots. Pour découvrir comment Cloudflare peut vous aider à relever vos défis concernant les bots, contactez-nous pour bénéficier d'une évaluation personnalisée.

Des informations auxquelles vous pouvez vous fier

Cloudflare traite en proxy environ 20 % de l'ensemble du trafic Internet mondial, ce qui fournit à l'entreprise d'amples connaissances en temps réel concernant les comportements des bots malveillants présents sur le réseau Cloudflare.
Par ailleurs, Cloudflare collabore avec une multitude de partenaires qui partagent des connaissances sur les identifiants de connexion volés, ce qui facilite la détection des tentatives d'usurpation de comptes avant qu'elles n'entraînent une violation de données.

Commencez votre parcours vers un réseau plus rapide, plus fiable et plus sécurisé

Demandez un entretien

Vous n'êtes pas encore prêts pour votre évaluation ?

Continuez à vous informer sur Cloudflare