CLOUDFLARE

LIVRE BLANC

Guide des bots malveillants : les signes d'alerte précoces et les mesures à adopter

Sommaire

Introduction

Les bots représentent aujourd'hui près de 30 % du trafic en ligne, et bon nombre d'entre eux ont été créés dans le but de porter préjudice aux entreprises telles que la vôtre. Environ 93 % du trafic de bots est non vérifié et potentiellement malveillant. La prévalence des campagnes d'extraction de contenu et de prix, des attaques par usurpation de compte et par bourrage d'identifiants et de données de cartes de paiement, des pratiques d'accaparement de stock et des attaques par déni de service distribué (DDoS) pilotées par des botnets indique que les acteurs malveillants utilisant des bots gagnent chaque année en complexité et en sophistication.

En outre, les mesures traditionnelles de lutte contre les bots, telles que le blocage par localisation géographique, le blocage d'adresses IP et les CAPTCHA traditionnels s'avèrent aujourd'hui inefficaces. En réalité, les bots résolvent plus facilement les CAPTCHA que les humains.[1]

C'est pourquoi il n'existe aucune tactique universelle permettant d'arrêter tous les bots et de les empêcher de porter atteinte à vos utilisateurs et à votre réputation. La seule approche viable consiste à prêter attention aux différents signaux d'alerte révélant l'activité de bots et à réagir à chaque occurrence en collectant des données, puis en déployant des réponses ciblées – identification des modèles récurrents, utilisation de données analytiques et d'autres stratégies complémentaires.

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

Signaux d'alerte révélant la présence de bots malveillants

La surveillance de différents indicateurs potentiels offre d'excellentes chances d'identifier les bots malveillants avant qu'ils n'aient le temps de réellement causer des dommages. Voici les signaux auxquels vous devez prêter attention :

Hausse des coûts d'infrastructure sans augmentation de l'activité

Tout le trafic affluant vers votre site web entraîne un coût. Quelle que soit la personne ou l'équipement qui accède à vos contenus, c'est à vous qu'il incombe de payer les coûts de stockage et de traitement. Or, les bots malveillants peuvent augmenter les coûts liés au trafic, sans toutefois générer de revenus pour votre entreprise. Si les moteurs de recherche ont recours à des bots utiles pour indexer les contenus de votre site et ainsi, assurer votre référencement SEO, les bots malveillants peuvent, chaque année, générer des coûts de bande passante excessifs.

Achats inhabituels de produits rares, à forte demande

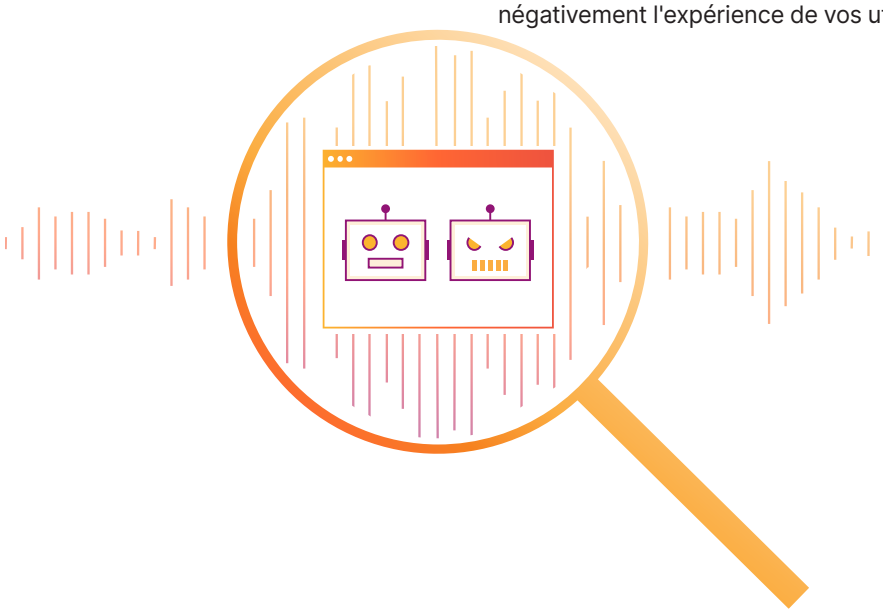
Si vous remarquez que vous vendez un pourcentage anormalement élevé de votre stock à un groupe d'acheteurs étrangement restreint, vous êtes peut-être victime d'une attaque par accaparement de stocks perpétrée par des bots. Si certains de ces bots ne font que remplir, puis abandonner des paniers d'achats dans le but de bloquer les clients légitimes, d'autres achètent vraiment vos produits avec l'objectif des les revendre à un prix plus élevé sur d'autres sites.

Augmentation des plaintes de clients

Une augmentation du nombre de tickets d'assistance liés à des blocages de comptes et des transactions frauduleuses peut révéler la présence de bots de bourrage d'identifiants (Credential Stuffing). Ces bots utilisent des identifiants volés lors de précédentes fuites de données pour prendre le contrôle de comptes d'utilisateurs légitimes. En plus de porter préjudice à l'expérience utilisateur de vos clients, ces transactions frauduleuses peuvent surcharger vos serveurs, augmentant ainsi les temps de chargement de pages, voire rendre votre site web inaccessible.

Augmentation des tentatives de connexion infructueuses

Tous vos clients peuvent parfois se tromper en saisissant leur mot de passe. Toutefois, si vous constatez une augmentation soudaine du nombre de tentatives de connexion infructueuses, vous avez très probablement affaire à des bots. Si certains bots de bourrage d'identifiants (Credential Stuffing) utilisent des identifiants volés pour tenter d'accéder aux comptes de clients légitimes, d'autres adoptent une technique plus simple et plus répandue, consistant à exécuter une tentative de connexion par force brute. Lors de ces attaques, les bots effectuent de nombreuses tentatives de connexion successives en utilisant des dictionnaires contenant des milliers de noms d'utilisateurs et de mots de passe courants. Si un bot dépasse le nombre maximal de tentatives de connexion autorisées par votre site pour un compte donné, le client humain auquel appartient ce compte ne pourra plus se connecter tant que vous n'aurez pas remédié au problème. Ces incidents affectent donc très négativement l'expérience de vos utilisateurs.



Faible rendement des dépenses publicitaires

La publicité numérique peut être un outil efficace pour générer du trafic sur votre site, mais elle est également une arme lucrative pour les bots malveillants. De nombreux bots générateurs de trafic imitent le comportement d'utilisateurs humains : ils cliquent de manière répétée sur vos publicités pour augmenter le montant des paiements par clic (PPC), puis consultent différentes pages, sans jamais effectuer d'achats. De nombreuses plates-formes publicitaires ont mis en place des algorithmes d'apprentissage automatisé pour combattre la fraude au clic, mais ces pratiques restent très rarement détectées.[2]
Il est donc impératif d'adopter des mesures proactives et de surveiller chaque clic généré par vos publicités.

Altération des données analytiques de consultations de pages

Si le nombre de consultations de pages augmente soudainement sans raison particulière, des bots malveillants peuvent en être la cause. Bien que des utilisateurs humains puissent générer un pic d'affluence lors du lancement d'un nouveau produit ou d'une campagne promotionnelle, les opérateurs de bots malveillants savent comment profiter de ces événements pour déployer des bots d'extraction de contenu qui dérobent vos informations et ont un impact négatif sur vos données analytiques globales.

Augmentation soudaine des créations de comptes

Si des centaines, voire des milliers de nouveaux comptes sont créés de manière soudaine et inattendue, il est possible que des bots en soient la cause. Ils peuvent utiliser ces faux profils pour fausser vos avis publics et commettre de nombreux autres types de fraude, nuisant ainsi non seulement à vos revenus et à la fidélité de vos utilisateurs, mais également à la crédibilité de votre marque.

Duplication de vos contenus sur des sites non approuvés

Le partage de vos contenus sur d'autres sites peut être bénéfique, mais une augmentation soudaine de la présence de contenus manifestement dupliqués est caractéristique d'une attaque de bots d'extraction de contenus. Ces bots dérobent les informations que vous avez pris le temps de collecter et d'organiser, permettant aux opérateurs de sites malveillants de les publier sur des domaines qui leur appartiennent – et ainsi, de générer de l'affluence sur leurs sites, au détriment du vôtre.

Trafic provenant de régions géographiques inhabituelles

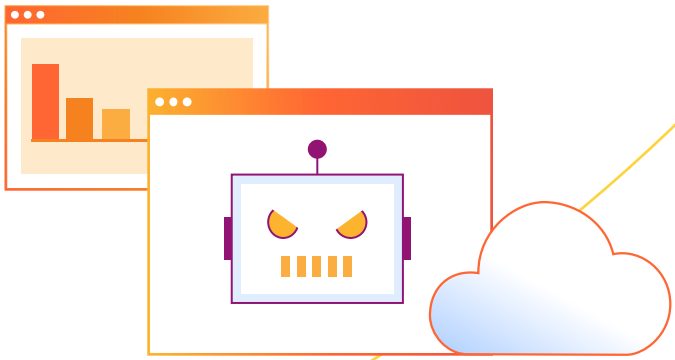
Des pics d'affluence soudains provenant de régions géographiques inattendues peuvent révéler l'activité de bots malveillants, surtout si cette activité se manifeste sous forme de « clusters » centrés dans des régions dans lesquelles vos clients ne résident pas ou vos services ne sont pas disponibles. Surveillez de près toute activité suspecte qui ne semble pas être liée à vos utilisateurs habituels.

Trafic provenant de régions géographiques habituelles, mais à des heures inhabituelles

Tout comme les pics d'affluence provenant de régions géographiques inhabituelles peuvent être symptomatiques d'une attaque de bots malveillants, les pics d'affluence provenant de régions géographiques habituelles à des heures inhabituelles peuvent révéler la présence de bots tentant de se faire passer pour des utilisateurs légitimes. Par exemple, si vous constatez un pic d'activité provenant d'une région géographique habituelle au beau milieu de la nuit, vous devriez peut-être prêter une attention particulière à ce trafic.

Augmentation des échecs de validation de cartes de paiement

L'augmentation du nombre d'échecs de transactions par carte de paiement peut être un symptôme particulièrement alarmant d'une attaque de bots malveillants. Les bots utilisant des numéros de carte de paiement volés testent des milliers de numéros de carte avec l'objectif d'identifier un numéro valide. Pour cela, ils effectuent des achats de faible valeur sur des sites web peu sécurisés avant d'effectuer des achats plus importants sur des sites plus renommés ou de revendre les numéros de carte de paiement valides sur le Dark Web. Votre site peut être exploité à ces fins à n'importe quelle étape du processus, et si le nombre de transactions ayant échoué est particulièrement élevé, votre prestataire de services de paiement peut vous facturer des pénalités.



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

Tactiques pour combattre les bots

Dans la mesure où il n'existe pas deux attaques de bots identiques, vous devrez généralement associer plusieurs stratégies pour les contrer. Voici quelques stratégies que vous pouvez envisager de mettre en œuvre :

Bloquez les bots malveillants dès que vous les identifiez

La réaction la plus évidente à l'attaque d'un bot est également l'une des plus efficaces : bloquez simplement tout le trafic que vous avez associé à l'activité d'un bot malveillant. À elle seule, cette tactique peut vous permettre de réduire considérablement vos coûts de bande passante et de stockage, en plus de préserver la confiance de votre clientèle ainsi que la réputation de votre marque. Cependant, n'oubliez pas que si un opérateur de bots est particulièrement déterminé, il pourra lancer d'autres attaques ultérieurement, en adoptant une autre stratégie.

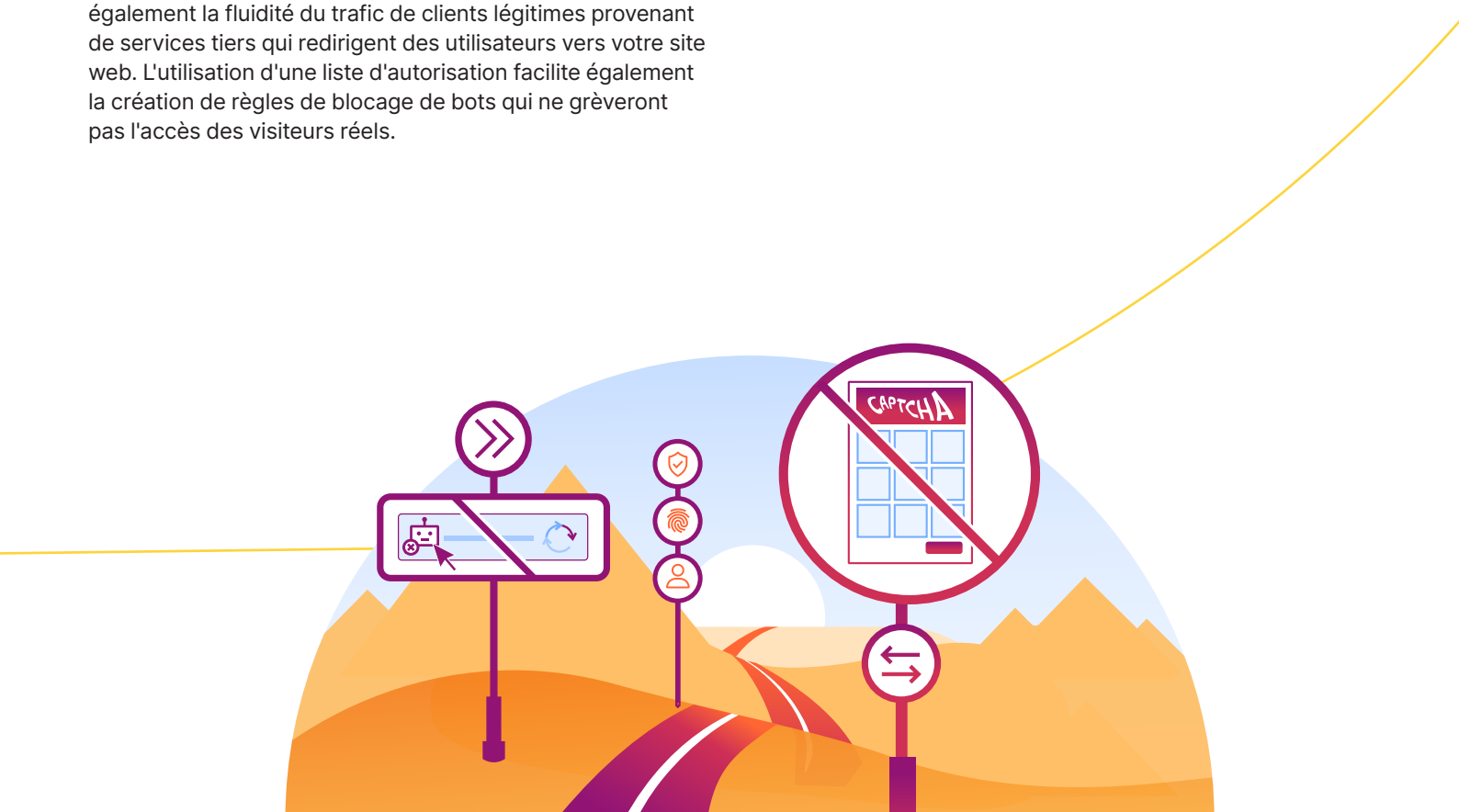
Ajoutez tous les bots légitimes que vous connaissez à une liste d'autorisation

Tout en détectant et en bloquant les bots malveillants, vous devez impérativement vous assurer que les bots légitimes des moteurs de recherche et de vos partenaires puissent continuer à recueillir des données sur votre site. Vous conserverez ainsi votre référencement SEO, et préserverez également la fluidité du trafic de clients légitimes provenant de services tiers qui redirigent des utilisateurs vers votre site web. L'utilisation d'une liste d'autorisation facilite également la création de règles de blocage de bots qui ne grèveront pas l'accès des visiteurs réels.

Testez les bots suspects que vous détectez

Dès que vous remarquez une séquence de connexions suspectes, une faible profondeur ou un faible temps de consultation par page, des échecs de validation de carte de paiement ou tout autre comportement symptomatique de l'activité de bots, il est crucial de mettre en œuvre un test de sécurité. Autrefois, l'affichage de vérifications CAPTCHA était considéré comme une bonne pratique. Cependant, de nombreux bots avancés peuvent désormais résoudre ces énigmes encore plus rapidement et avec plus de précision que les utilisateurs humains.

Aujourd'hui, la meilleure approche consiste à utiliser des vérifications sans CAPTCHA, dans lesquels le logiciel de vérification prend en compte une multitude de facteurs afin de déterminer si l'utilisateur est réellement un bot (par exemple, réseau, appareil, empreintes JavaScript). Idéalement, les vérifications sans CAPTCHA doivent être intégrées à une solution complète de gestion des bots pour offrir une précision maximale (reportez-vous à la conclusion pour plus d'informations).



Limitez la fréquence d'envoi des requêtes d'utilisateurs

Le contrôle du volume des requêtes peut être une technique efficace pour bloquer les bots peu sophistiqués. En limitant de manière stricte le nombre de requêtes que peut envoyer une adresse IP à votre site, vous arrêterez de nombreuses attaques simplistes par force brute lancées par des bots qui tentent de se connecter en utilisant des dictionnaires contenant des milliers de noms d'utilisateur et mots de passe courants. Cependant, les bots plus sophistiqués que l'on rencontre aujourd'hui peuvent maintenir le nombre de requêtes envoyées juste en dessous de la limite que vous avez définie, et ainsi, continuer à causer des dommages sans être détectés.

Conservez des journaux détaillés de tout le trafic affluant sur votre site

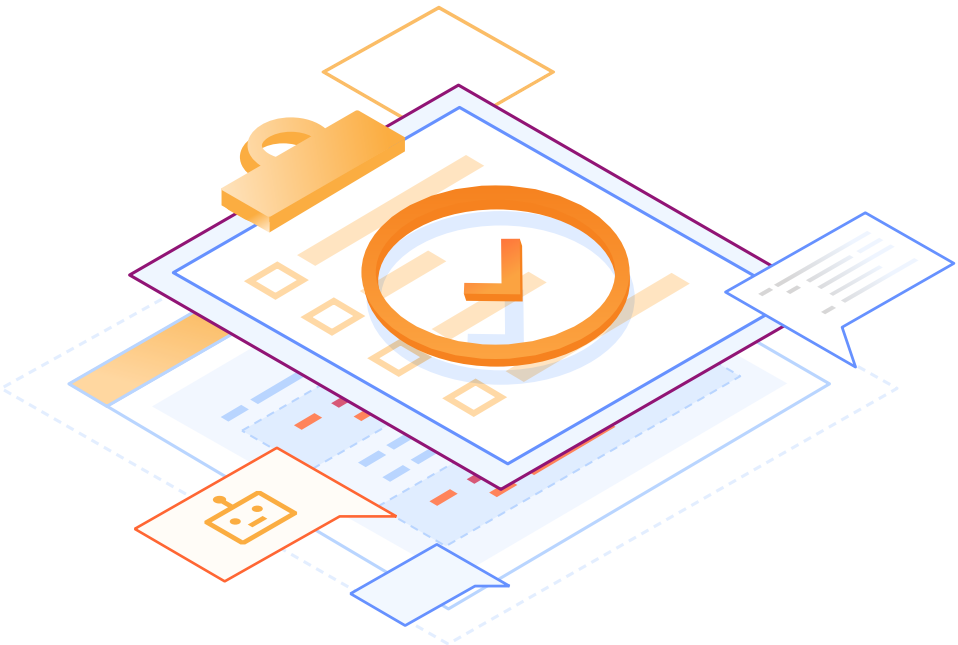
Même si vous conservez probablement déjà des journaux quotidiens des consultations de pages et des connexions de comptes, des journaux plus détaillés contenant des informations sur les utilisateurs (adresses IP, navigateurs, appareils, systèmes d'exploitation, géolocalisation, points d'accès, réseaux et consultations de pages) peuvent être extrêmement utiles pour détecter les activités plus furtives. Ces journaux peuvent vous fournir une idée claire du comportement des bots sur votre site, et ainsi, vous permettre de mettre en œuvre des stratégies de sécurité plus efficaces. Par ailleurs, ils sont souvent indispensables dans le cadre des procédures d'information réglementaire et de conformité, si vous êtes effectivement victime d'une violation de données.

Redirigez les bots vers des contenus de substitution

Si vous avez la certitude qu'un bot est une source de trafic particulier, servez-lui des contenus de substitution qui consomment ses ressources de calcul. Vous pouvez même envoyer des données factices (par exemple, des informations de tarification erronées) aux bots d'extraction de contenus, afin de les rendre inutiles pour leurs opérateurs. Ces techniques vous permettront de gagner du temps afin de mieux observer le comportement de chaque bot, de comprendre son fonctionnement et d'élaborer une stratégie permettant de le bloquer définitivement.

Ajoutez une couche d'authentification pour tous les utilisateurs

Face aux attaques de bots toujours plus fréquentes, les sites sont de plus en plus nombreux à adopter des mesures de sécurité renforcées, même pour les connexions humaines légitimes. L'authentification à deux facteurs (2FA), par exemple, exige des utilisateurs qu'ils confirment leur identité sur plusieurs appareils ou comptes, tandis que les mots de passe à usage unique peuvent décourager les opérateurs de bots de bourrage d'identifiants (Credential Stuffing) utilisant des identifiants volés, en rendant les comptes plus difficiles à pirater. Cependant, souvenez-vous que ces techniques peuvent porter préjudice à l'expérience des utilisateurs en rendant le processus de connexion moins fluide.

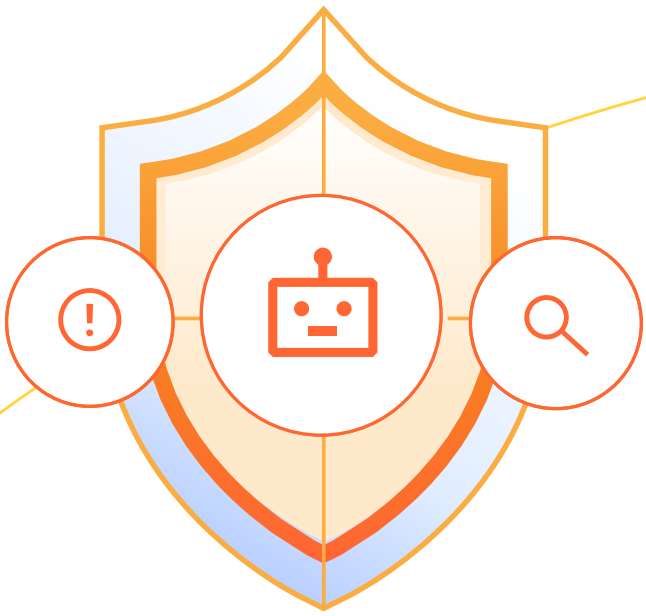


Conclusion

À mesure que vous essayez ces tactiques, souvenez-vous qu'aucune stratégie unique ne suffira, à elle seule, à arrêter tous les bots. Pour protéger votre entreprise, vous devrez associer plusieurs tactiques et ajouter à ces dernières des fonctions avancées d'analyse multivariée des modèles.
Le service Cloudflare Bot Management peut aider les entreprises issues de différents secteurs de l'industrie à adopter cette approche pluridisciplinaire. Cette solution est intégrée au vaste réseau Cloudflare, qui protège plus des millions de propriétés Internet et est présent dans plus de 330 villes à travers le monde.

En s'appuyant sur des informations sur les menaces issues de ce réseau, Cloudflare Bot Management propose des fonctionnalités d'analyse comportementale, d'apprentissage automatique et de collecte d'empreintes numériques, réduisant ainsi considérablement la difficulté de la lutte contre les bots malveillants. En outre, Cloudflare propose Turnstile, une solution de vérification des bots extrêmement fluide, sans CAPTCHA, qui peut être intégrée à n'importe quelle application web avec quelques lignes de code seulement.

En savoir plus sur Cloudflare Bot Management.



01 73 01 52 44 | enterprise@cloudflare.com | www.cloudflare.com/fr-fr/

RÉV. : BDES-6333.2024SEPT03