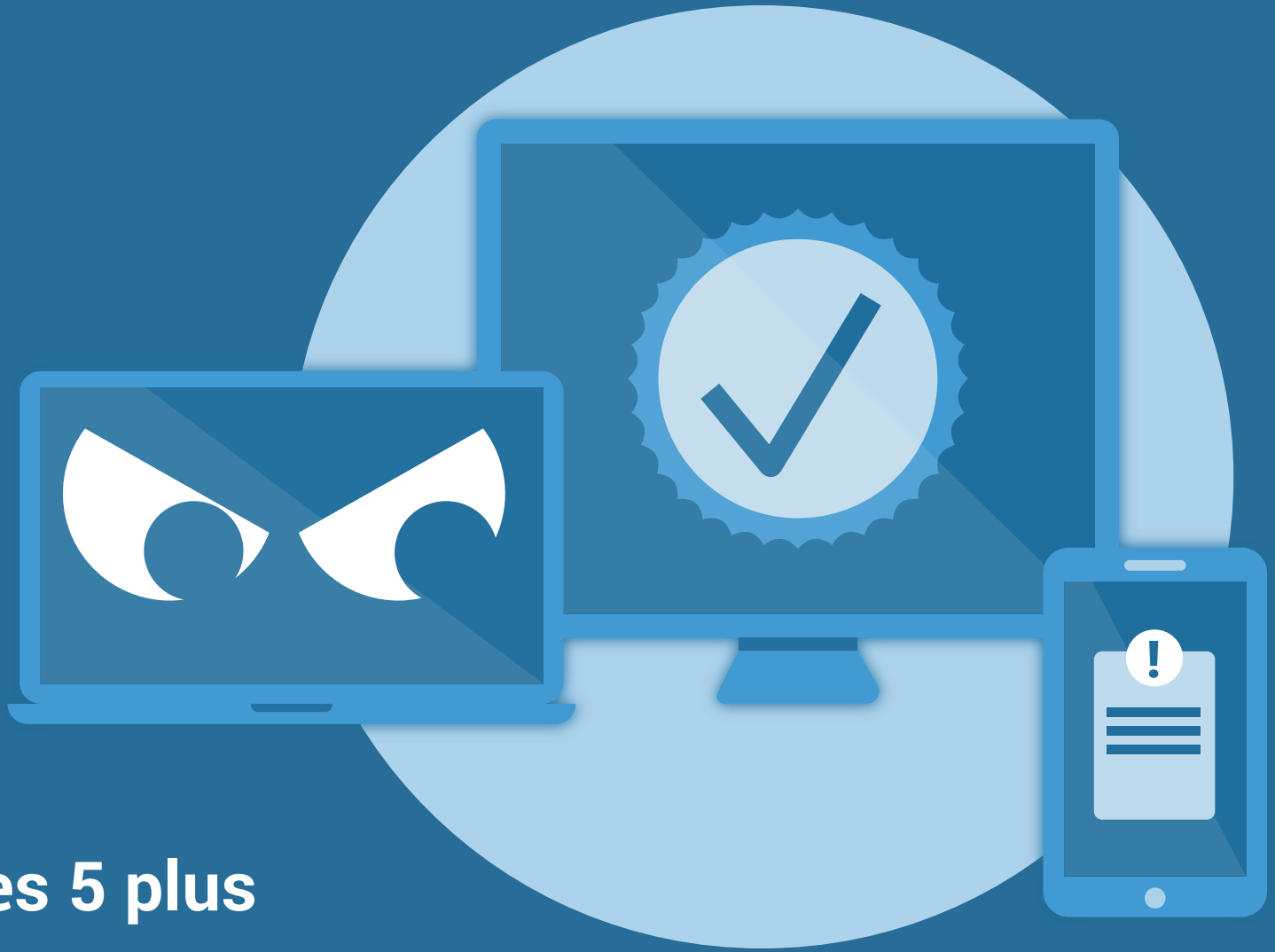


Démystifier les 5 plus grands mythes sur les bots malveillants

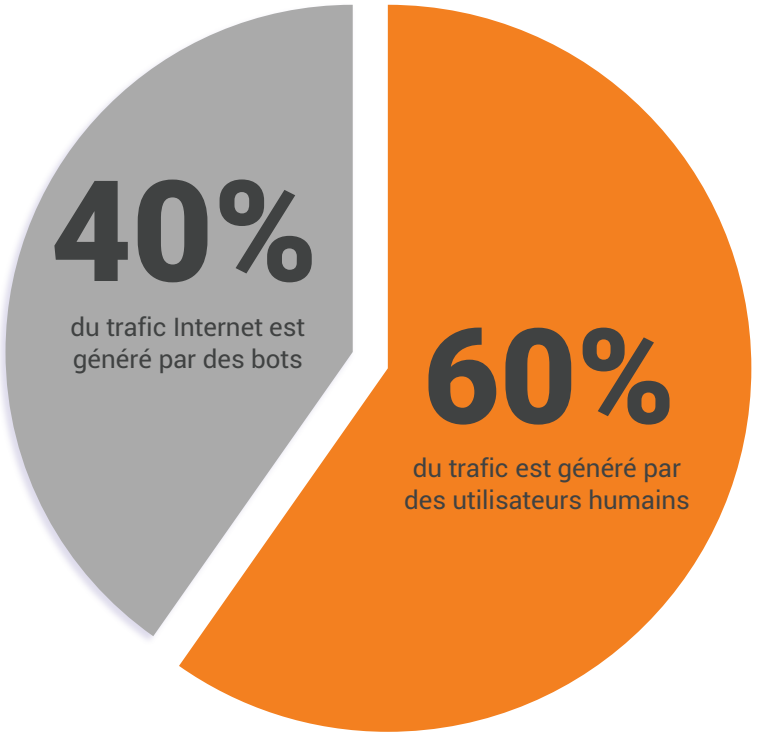
+33 75 7 90 52 73 | enterprise@cloudflare.com | www.cloudflare.com/fr-fr/

CLOUDFLARE®

Sommaire

CLOUDFLARE

Mythes sur le trafic des bots malveillants



Aujourd'hui, jusqu'à 40 % du trafic Internet est généré par des bots, c'est-à-dire des utilisateurs non humains de sites web et d'applications. Regrettablement, une grande partie de ces bots sont malveillants. Et à mesure que les bots malveillants deviennent toujours plus répandus et plus sophistiqués, vérité et fiction se confondent parfois. Il devient alors difficile de comprendre l'impact que peuvent avoir les bots malveillants sur votre organisation – et ce que vous pouvez faire pour les arrêter.

Examinons de plus près certaines des hypothèses erronées les plus courantes au sujet des bots malveillants – et comment votre organisation peut se protéger des bots en adoptant une approche mieux informée de la défense.

MYTHE N° 1 :

Tous les bots vous veulent du mal

Bien que les bots malveillants aient tendance à monopoliser l'attention, les bots légitimes sont presque aussi répandus.

Les bots légitimes jouent des rôles cruciaux dans le bon déroulement des activités numériques. Par exemple, les bots aident les entreprises telles que Google, Bing et Baidu à indexer les milliards de sites qui apparaissent dans vos résultats de recherche. Et chaque fois que vous recherchez un voyage sur Expedia ou Priceline, une équipe de bots partenaires « extrait » (c'est-à-dire, effectue une recherche sur) les contenus des sites web de compagnies aériennes telles que Delta et American Airlines, puis vous présente une liste d'horaires et de prix pour les vols correspondant à vos expressions de recherche.

Suite >>

Le rôle des bots légitimes

Cette distinction est importante, car les bots légitimes sont tellement essentiels au fonctionnement d'Internet aujourd'hui qu'il est problématique d'arrêter les bots malveillants en bloquant simplement tous les utilisateurs non humains.

Les auteurs d'attaques sont bien conscients de ce fait. C'est pourquoi ils conçoivent délibérément leurs robots malveillants pour imiter le comportement de bots légitimes, qui peuvent être bénéfiques à votre organisation. Les bots d'extraction de contenus, par exemple, peuvent collecter des contenus originaux sur votre site et les rediffuser sur des sites frauduleux sans votre autorisation. Toutefois, si vous bloquez tous les bots d'extraction de contenus, vous risquez d'empêcher des partenaires bien intentionnés (par exemple, un partenaire de diffusion ou un site d'avis) d'accéder aux informations dont ils ont besoin pour promouvoir légitimement votre organisation.

> *Avant d'utiliser Cloudflare, nous étions vraiment désorientés. Nous n'avions aucune idée du pourcentage de visites de bots que recevait notre infrastructure, ni des mesures que nous devions prendre pour protéger les intérêts de nos partenaires éditeurs contre le trafic malveillant."*
>
> **Romeo Ju** Président
>
> **Sulvo**

MYTHE N° 2 :

Les bots ciblent seulement certaines industries – l'e-commerce, les voyages et la finance

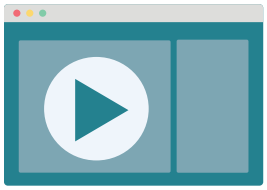
Si de nombreuses attaques de bots très médiatisées ont visé des banques, des compagnies aériennes, des hôtels et des sociétés d'e-commerce, les bots malveillants s'attaquent de plus en plus fréquemment à différentes industries. Ces dernières années, Cloudflare a observé des attaques de bots lancées contre des établissements de santé, des services de billetterie, des établissements d'enseignement, des sociétés de jeux, des firmes publicitaires et de marketing, des maisons d'édition et même des agences gouvernementales.

Ici, les tactiques des opérateurs de bots varient considérablement d'une verticale à l'autre. En réalité, de nombreuses attaques de bots sont ciblées de manière unique pour exploiter des vulnérabilités dans la logique opérationnelle d'une organisation particulière. Par exemple, un site web qui sert des contenus à des millions d'utilisateurs externes peut être victime d'une attaque par extraction de contenus ou par accaparement des stocks, tandis qu'une installation qui conserve des données internes confidentielles peut devenir la cible d'une attaque de cassage de mots de passe par force brute.

La réalité est que tout site web doté d'une page de connexion accessible aux clients peut constituer une cible attrayante pour des bots malveillants. De plus, toute entreprise proposant des services de marketing, informatiques, de webdesign ou d'autres services numériques peut paraître aussi tentante qu'un coffre-fort rempli de billets de banque aux yeux d'un opérateur de bots malveillants.

MYTHE N° 3

La fréquence des attaques de bots augmente pendant la période des fêtes



Il est incontestable que l'on observe un grand nombre d'attaques de bots pendant la période des fêtes de fin d'année.[2] Toutefois, il est également vrai que des attaques de bots peuvent être lancées tout au long de l'année. Elles sont parfois motivées par un événement majeur, tel qu'un lancement de produit, et d'autres fois, par des facteurs beaucoup plus difficiles à anticiper.

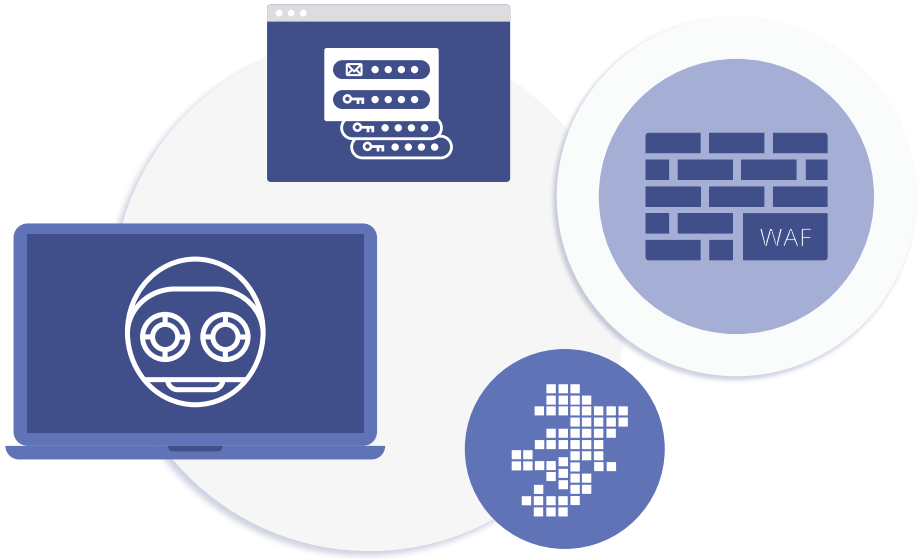
▶ Les attaques de bots ont lieu à longueur d'année l'année

Par exemple, Disney a été la cible d'une attaque de bots tristement célèbre en novembre 2019, qui a coïncidé avec le lancement du nouveau service de streaming de contenu Disney+.[3] Des bots ont perpétré une attaque par « credential stuffing » (c'est-à-dire l'utilisation en masse d'identifiants volés) pour cibler des comptes de clients pendant le lancement du service. Des milliers de ces comptes compromis ont ensuite été mis en vente sur le Dark Web. Les criminels qui ont acheté ces comptes piratés pouvaient potentiellement accéder aux coordonnées bancaires des utilisateurs, ainsi qu'aux informations de connexion à de nombreux autres sites et applications.

Et si l'attaque lancée contre Disney reste l'une des plus grandes catastrophes imputables à des bots de mémoire récente, de nombreuses attaques de moindre ampleur ont lieu tous les mois de l'année. En réalité, l'imprévisibilité pure et simple de l'activité des bots, à l'image de l'attaque par « credential stuffing » lancée contre J.Crew en avril 2019,[4] représente l'un des principaux arguments en faveur de l'adoption d'une solution à plusieurs facettes de défense contre les bots.

MYTHE N° 4

Mon organisation peut arrêter tous les bots malveillants avec un seul outil



On pourrait croire que la mitigation des attaques DDoS, la limitation du débit, un pare-feu d'applications web (« Web Application Firewall », WAF), l'authentification multi-facteurs, les CAPTCHA ou d'autres tactiques à méthode unique suffisent à répondre aux besoins de gestion des bots d'une organisation. Cependant, les attaques de bots gagnent en sophistication et sont désormais capables de contourner les défenses individuelles en imitant les comportements humains. La réalité est que les organisations ont besoin d'une solution exhaustive de gestion des bots.

Suite >>

MYTHE N° 4 Mon organisation peut arrêter tous les bots malveillants avec un seul outil, suite

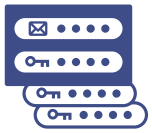
La mitigation des attaques DDoS peut être efficace contre les attaques volumétriques, lors desquelles un botnet perturbe un serveur, un service ou un réseau ciblé en inondant la cible ou l'infrastructure environnante de trafic Internet. Toutefois, la mitigation des attaques DDoS est beaucoup moins apte à détecter les bots individuels qui imitent le comportement d'utilisateurs humains.

Les pare-feu d'applications web peuvent offrir une défense contre les attaques SQL Injection, Cross-Site Scripting (XSS) et Zero Day en appliquant des politiques qui interdisent l'accès depuis des plages d'adresses IP ou des régions géographiques spécifiques. Cependant, les opérateurs de bots actuels peuvent utiliser des millions d'adresses IP dans des centaines de pays.

Les CAPTCHA peut être un élément efficace de la prévention des bots en interceptant les bots malveillants trop évidents. Cependant, certains bots récents peuvent maintenant résoudre les CAPTCHA – et dans tous les cas, les CAPTCHA ont un impact négatif sur votre expérience utilisateur en ralentissant inutilement votre parcours de connexion ou d'achat.

La **limitation du débit** peut permettre de bloquer les attaques de bots simplistes générant un nombre excessif de requêtes. Toutefois, les bots sophistiqués peuvent éviter la détection en réduisant simplement leur nombre de requêtes. De nombreux bots malveillants optent aujourd'hui pour une approche « discrète et lente », c'est-à-dire en effectuant des actions à une fréquence semblable à celle d'un utilisateur humain.

La détection de bots JavaScript peut interdire l'accès depuis des navigateurs non légitimes. Cependant, les tests de bots JavaScript grèvent les performances du site, car l'application doit vérifier chaque requête auprès du serveur d'origine du fournisseur, ce qui crée une expérience désagréable pour les utilisateurs finaux. C'est également un casse-tête de déploiement pour vos équipes informatiques et de sécurité, qui doivent gérer et sécuriser des bibliothèques JavaScript tierces.



L'authentification multi-facteurs peut contribuer à la protection contre les connexions non autorisées lorsque des bots tentent d'utiliser des identifiants d'utilisateur légitimes. Cependant, elle est simplement inefficace dans la majorité des scénarios d'utilisation de bots – et elle ralentit également votre expérience utilisateur.

MYTHE N° 5 :

Les attaques de bots sont tellement variées que je devrais développer mes propres outils de gestion des bots

Compte tenu de la sophistication des bots actuels et du ciblage précis et individualisé de nombreuses attaques de bots, une solution dédiée de gestion des bots pourrait sembler être le choix le plus judicieux. Cependant, si une solution développée en interne peut s'avérer très efficace dans l'immédiat, elle nécessitera une maintenance coûteuse et des mises à jour fastidieuses par des experts internes pour rester efficace.

En outre, les bots malveillants continuent d'évoluer en réagissant à chaque attaque déjouée, en modifiant leurs modèles d'attaque, en perfectionnant leur imitation des utilisateurs humains et en apprenant à se soustraire aux outils de sécurité actuels les plus complexes. Cela signifie que la solution de gestion des bots que vous avez conçue nécessiterait un ajustement continu des règles et des stratégies pour anticiper les menaces posées par les bots de demain.

Et en fin de compte, même la plus élaborée des solutions internes de gestion des bots devrait être autonome. Vos possibilités se limiteraient à la prédiction des attaques de bots à partir de vos données internes et à l'analyse les modèles d'activités suspects avec des algorithmes obsolètes. Par conséquent, votre solution dédiée générerait de nombreux faux positifs, ce qui aurait un impact négatif sur l'expérience que votre site propose à vos utilisateurs légitimes.

Conclusion : attributs de la solution idéale de gestion des bots

Une solution efficace de gestion des bots doit réunir les meilleurs attributs de l'ensemble des outils et approches énumérés ci-dessus. Elle doit tirer parti des connaissances de Global Threat Intelligence à grande échelle et doit utiliser l'apprentissage automatisé pour effectuer une analyse comportementale en temps réel du trafic du site, en bloquant les bots malveillants tout en apprenant à les reconnaître encore plus rapidement à l'avenir.

D'un point de vue pratique, une solution idéale de gestion des bots doit être facile à déployer et à gérer, sans exiger d'expertise interne, de maintenance coûteuse ou d'ajustements manuels continus. Elle doit générer peu de faux positifs et bloquer avec précision les bots malveillants, sans avoir d'impact négatif sur les utilisateurs humains ou les bots utiles. Dans l'ensemble, elle doit améliorer et rationaliser de manière proactive l'expérience que propose votre site.

Cloudflare Bot Management est conforme à toutes ces spécifications. La solution tire parti d'informations concernant les menaces provenant de plus de 25 millions de propriétés en ligne pour analyser le comportement des utilisateurs. Elle utilise par ailleurs l'apprentissage automatisé fondé sur un sous-ensemble géré de centaines de milliards de requêtes par jour, ainsi que des empreintes digitales collectées sur des millions de sites et d'applications. Ceci permet à Cloudflare de détecter de manière proactive toute anomalie dans le trafic des utilisateurs et d'évaluer avec précision la probabilité que chaque requête émane d'un bot malveillant, préservant ainsi l'expérience de vos utilisateurs tout en protégeant votre site contre les bots.

Consultez le site www.cloudflare.com pour découvrir comment accélérer et protéger votre site web.

Notes de bas de page

1 Cloudflare, « What Is Bot Traffic? », Cloudflare Learning Center, consultation le 4 mars 2020

2 Cloudflare, 5 BONNES PRATIQUES : Préparer votre site d'e-commerce pour garantir votre succès pendant les fêtes de fin d'année

3 Barrett, Brian, « The Likely Reason Disney+ Accounts Are Getting Hacked », Wired.com, 20 novembre 2019

4 Alina Bizga, « U.S. retailer J.Crew reveals 2019 security incident to customers », Security Boulevard.