Attaques de bots : principales menaces et tendances

Vol. 1 Septembre 2021

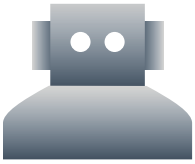
Un aperçu du nombre croissant d'attaques automatisées

Tous les bots ne sont pas équivalents. Bien que certains d'entre eux, tels que les bots d'indexation des moteurs de recherche, soient performants, les mauvais bots sont conçus pour mener des attaques malveillantes à grande échelle. Le trafic provenant de ces mauvais bots explose, et ce rapport détaillé explore les modèles de trafic émergents, des exemples concrets de comportement et de détection des bots, ainsi que les mesures que vous devez prendre pour protéger votre entreprise.»

Barracuda
Your journey, secured.

Table des matières

Résultats clés



Les Bots représentent près des **deux tiers** du trafic Internet

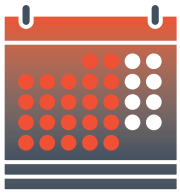
Les applications d'e-commerce et les **portails de connexion** sont les cibles privilégiées **des bots persistants avancés**

L'Amérique du Nord concentre **67 %** du trafic des mauvais bots

aws

Microsoft Azure

La plus grande partie du trafic généré par les bots provient des **deux** principaux **acteurs du cloud public : AWS** et **Microsoft Azure**



Les bots malveillants respectent les **horaires de travail classiques**

Introduction

Au cours des dernières années, le trafic des bots automatisés a connu une croissance rapide. Auparavant principalement utilisés par les moteurs de recherche, les bots ont désormais des utilisations variées, bonnes et mauvaises. Les bots bienveillants sont principalement les bots des moteurs de recherche, les bots des réseaux sociaux, les bots des agrégateurs, les bots de surveillance, etc. Ces bots obéissent aux règles du propriétaire du site Web telles qu'elles sont spécifiées dans le fichier robots.txt, publient des méthodes permettant de les valider comme étant ceux qu'ils sont, et travaillent de manière à ne pas submerger les sites Web et les applications qu'ils visitent.

Les bots malveillants sont conçus pour réaliser diverses activités hostiles : du scraping de base qui vise à extraire certaines données d'une application (action facilement neutralisée) aux bots persistants avancés qui se comportent presque comme des êtres humains et qui tentent d'échapper à la détection. Ces bots lancent des attaques telles que le Web et le price scraping, la mise à mal des inventaires, le piratage de compte, les attaques par déni de service distribué (DDoS), entre autres.

Les bots malveillants représentent aujourd'hui une part significative du trafic sur les sites Web, c'est pourquoi leur détection et leur neutralisation sont incontournables pour les entreprises.

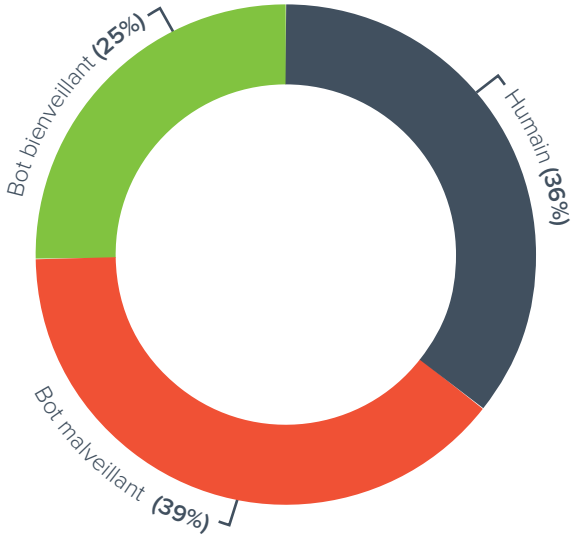
Tendances du trafic

Constat N° 1 : les bots représentent 64 % du trafic Internet.

Le trafic automatisé représente près des deux tiers du trafic Internet, d'après les mesures effectuées à l'aide de la technologie Barracuda au cours des six premiers mois de 2021. Environ 25 % de ce trafic provient de bots bienveillants, comme les bots d'indexation des moteurs de recherche, les bots des réseaux sociaux et les bots de surveillance.

Cependant, d'après nos mesures, presque 40 % du trafic total vient des mauvais bots. Parmi ces mauvais bots figurent les Web scrapers de base et les scripts d'attaque, ainsi que les bots persistants avancés. Ces bots avancés s'efforcent d'échapper aux systèmes de détection classiques et tentent de mener leurs activités malveillantes de manière inaperçue. Dans notre base de données, les bots persistants les plus courants étaient ceux qui s'attaquaient aux applications d'e-commerce et aux portails de connexion.

Répartition du trafic : bots et humains (janvier à juin 2021)



Répartition par mois

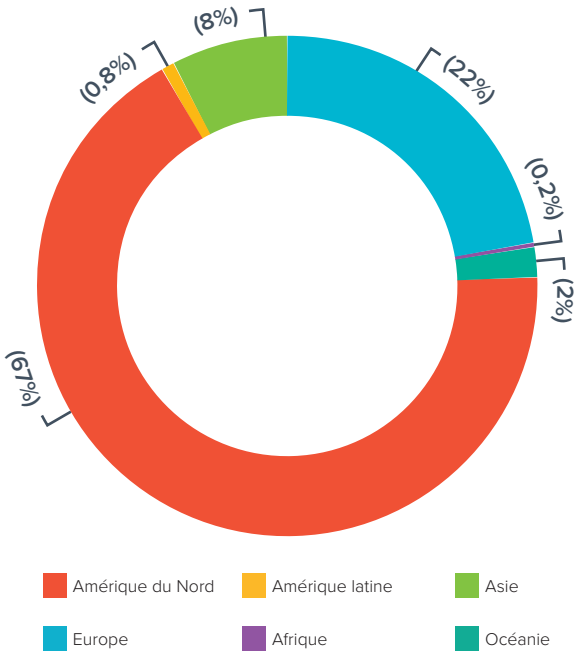
Constat N° 2 : la plus grande partie du trafic généré par les bots malveillants provient d'Amérique du Nord, et notamment de datacenters

La majeure partie du trafic des bots malveillants provient des plages IP des datacenters. Il est donc relativement simple d'identifier et de bloquer ces bots. Si votre application ne s'attend pas à recevoir du trafic provenant d'une plage d'adresses IP d'un datacenter spécifique, vous pouvez envisager de la bloquer, comme vous le feriez grâce au blocage basé sur la géolocalisation.

D'après notre ensemble d'échantillons, la majeure partie du trafic des bots provenait des deux principaux acteurs du cloud public (AWS et Microsoft Azure) selon une proportion pratiquement égale. Cela peut être dû au fait qu'il est facile de créer un compte gratuitement avec l'un ou l'autre des fournisseurs, puis de l'utiliser pour configurer les mauvais bots.

D'après la répartition régionale du trafic, l'Amérique du Nord concentre 67 % du trafic des bots malveillants, suivie de l'Europe et de l'Asie. Il est intéressant de noter que le trafic des bots européens est plus susceptible de provenir de services d'hébergement (VPS) ou d'adresses IP résidentielles que le trafic nord-américain.

Sources géographiques du trafic de mauvais bots

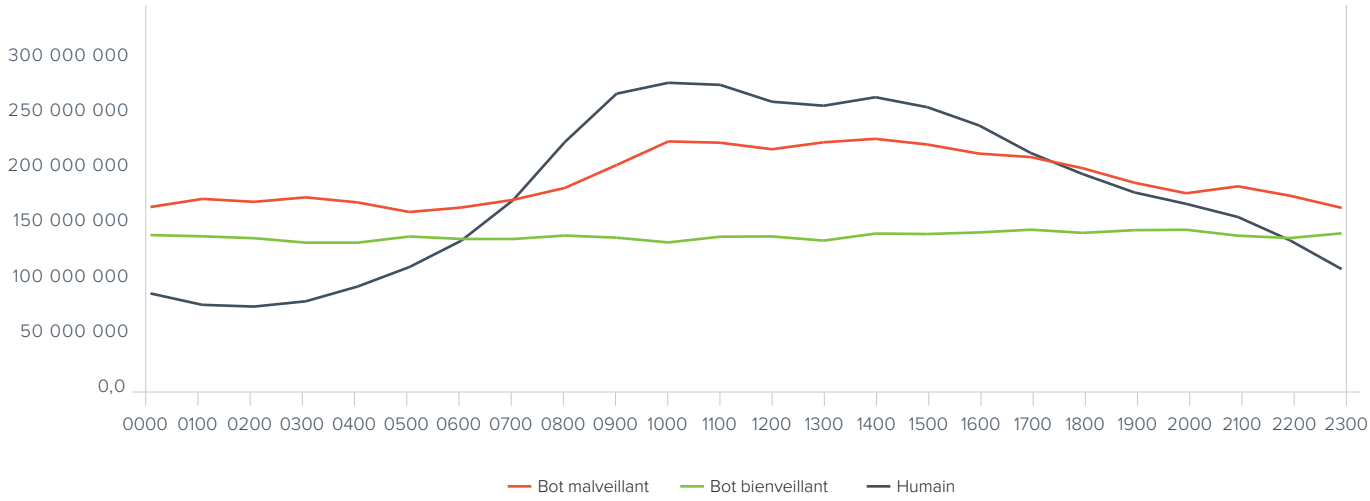


Constat N° 3 : les bots malveillants respectent les horaires de travail classiques

En 2020, nos chercheurs ont constaté que le trafic de bots malveillants respectait les horaires de travail classiques. C'est ce que confirme notre analyse portant sur le premier semestre 2021. Les bots bienveillants suivent une répartition normale, sans grande variation, et le taux de trafic est plutôt constant tout au long de la journée. Au cours des six mois que nous avons analysés, une importante part de ce trafic provient des bots de surveillance, et ce manque de variance est attendu.

Quant aux bots malveillants, ils ont une bonne raison de respecter les horaires de travail classiques. Les pirates qui exécutent ces bots malveillants préfèrent se cacher derrière le flux de trafic humain normal pour ne pas éveiller l'attention. Le stéréotype courant du « pirate » perpétrant ses attaques tard dans la nuit dans une pièce sombre avec des polices vertes sur un écran noir a été remplacé par des personnes qui ont configuré leurs bots pour mener des attaques automatisées pendant la journée.

Trafic des bots sur une journée



Exemples concrets de bots malveillants

Exemple 1 : se faire passer pour un analyseur de vulnérabilités connu

Chaque point représente une URL unique accessible. Le premier groupe montre que de nombreuses requêtes adressées à une URL ont été effectuées en même temps, et à ce stade, le client a été arrêté. Après la première salve, les demandes arrivaient en moindre quantité, mais uniquement vers des URL spécifiques, et le bot a été identifié à l'aide de ses caractéristiques.

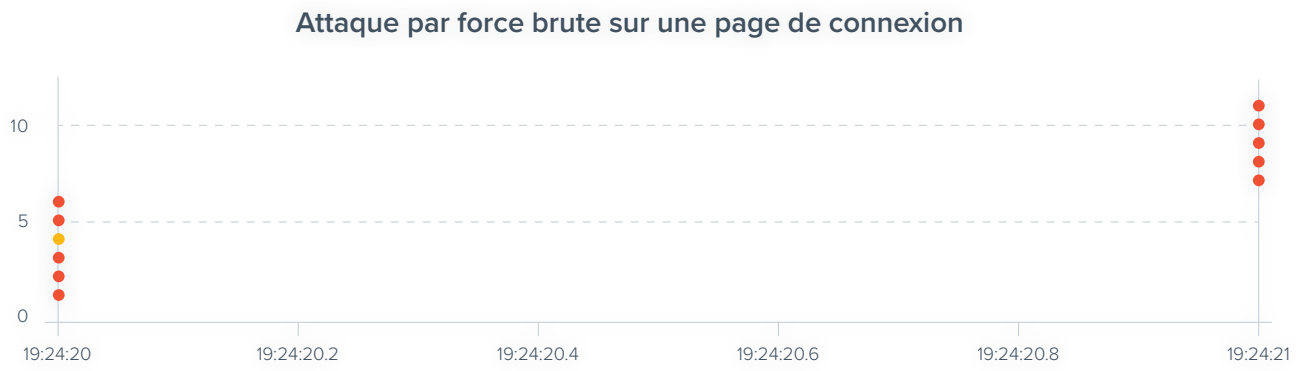
Dans notre analyse, nous avons identifié cet exemple de mauvais bot se faisant passer pour un analyseur de vulnérabilités connu (un bot bienveillant). Le bot malveillant essayait d'effectuer une reconnaissance et de détecter les vulnérabilités à l'aide d'attaques de base. Pour ce faire, le bot utilisait un agent utilisateur de navigateur standard, mais il disposait d'en-têtes HTTP personnalisés supplémentaires qui usurpaient les en-têtes d'un analyseur utilisé par l'organisation victime de l'attaque.

Cependant, le bot a échoué sur plusieurs comptages et a été détecté relativement facilement. Un des signes révélateurs était que l'empreinte du client ne correspondait pas à celle d'un navigateur connu. Alors que les en-têtes personnalisés usurpés étaient corrects, leur ordre envoyé par l'outil ne correspondait pas au profil attendu. Le bot malveillant, qui provenait d'adresses IP résidentielles, visitait également des pages de manière aléatoire. Toutes ces actions combinées ont permis de détecter et de neutraliser assez rapidement ses tentatives répétées.

Exemple 2 : accéder à la page de connexion d'un prestataire de services médicaux

Dans cet exemple que nous avons détecté, le bot accédait à la page de connexion d'un prestataire de services médicaux. Se faisant passé pour Internet Explorer sous Windows 10, ce bot ajoutait également des paramètres UTM aléatoires à l'URL de la page de connexion et venait de plusieurs plages IP AWS.

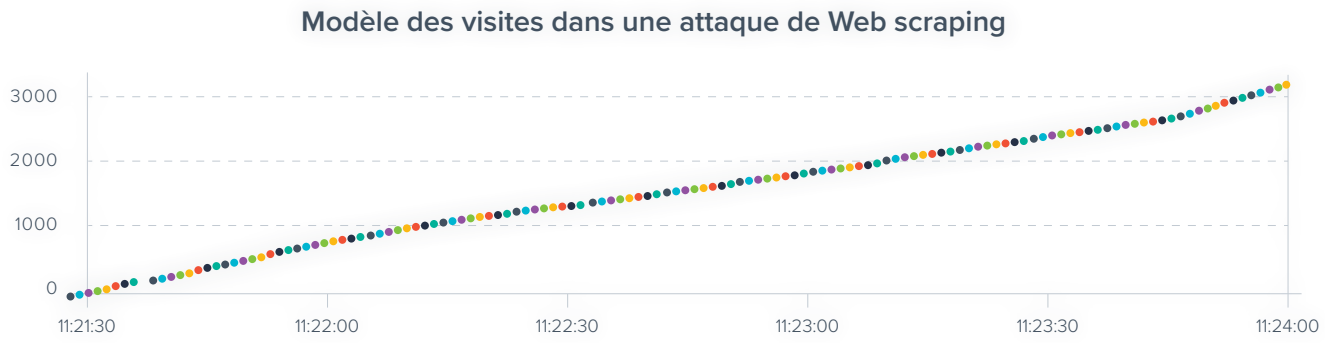
Le bot a été détecté en raison des variations d'en-tête qui différaient de celles d'un navigateur standard. Il a également été démasqué du fait que la même signature de navigateur venait de plusieurs adresses IP AWS, mais celles-ci n'accédaient qu'aux pages de connexion de l'application. Le signe révélateur était une attaque par force brute à l'aide d'identifiants volés. Elle a été détectée grâce à notre base de données d'identifiants et le bot n'a pas pu accéder au site.



Ce graphique montre un extrait des demandes de connexion effectuées par le bot qui tentait en même temps de forcer la page de connexion. Chaque point représente une tentative de connexion.

Exemple 3 : Web scraping d'une boutique d'e-commerce B2B

Ce bot a tenté d'extraire une quantité importante d'informations d'une boutique d'e-commerce B2B au Royaume-Uni. Le bot se faisait passer pour un navigateur standard et avait tous ses en-têtes dans l'ordre. De plus, il opérait depuis une adresse IP résidentielle et c'est précisément ce qui a mis le système en alerte : ce site Web était rarement visité par des clients résidentiels. En outre, il a été détecté que le client utilisait un kit SDK Web, généralement utilisé pour l'automatisation, et ces détections, ainsi que la traversée rapide du site Web, ont été utilisées pour identifier et bloquer le bot.

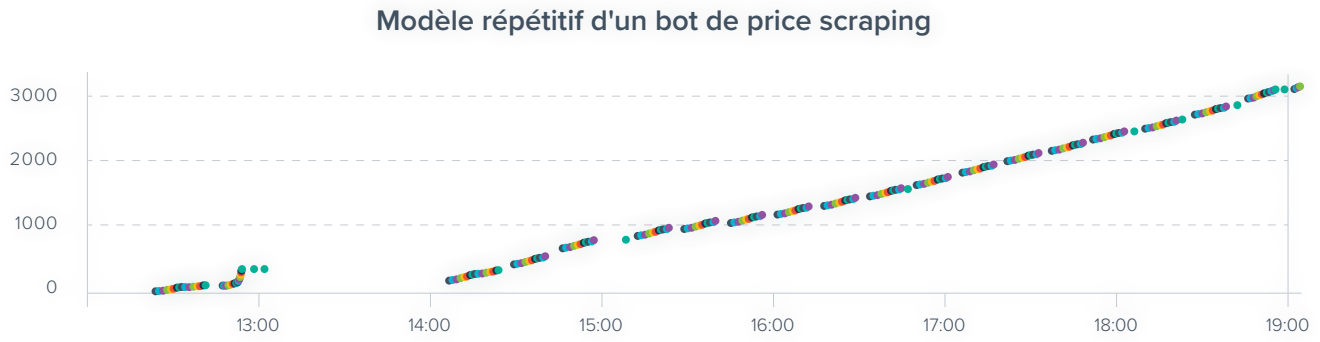


Ce graphique montre que le bot tente d'accéder à la même série d'URL à plusieurs reprises dans un court laps de temps pour récupérer des données. Il va reproduire plusieurs fois ce modèle au cours de la journée.

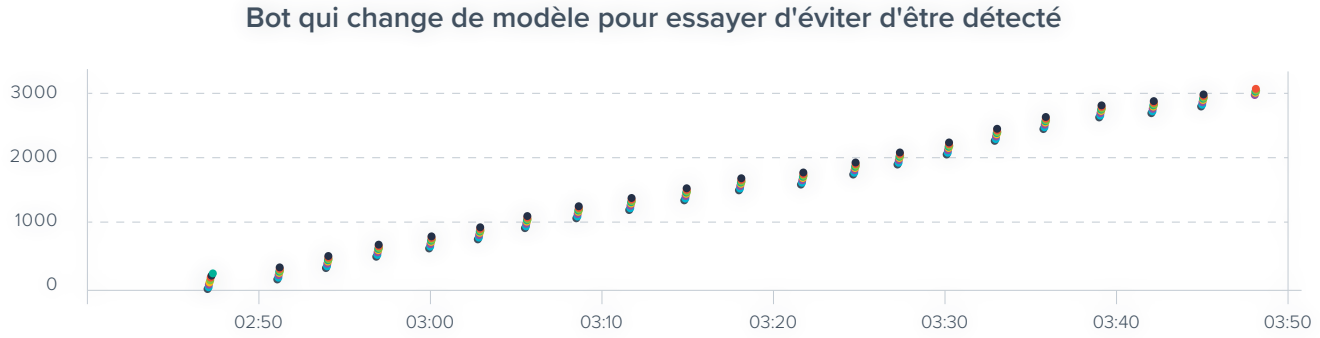
Exemple 4 : price scraping d'une boutique d'e-commerce en Europe de l'Est

Dans cet exemple, une tentative de price scraping était suspectée dans une boutique d'e-commerce basée en Europe de l'Est. La boutique offrait une réduction sur les produits Apple, et des comportements douteux se sont manifestés dans le trafic. Le trafic suspect provenait de clients de navigateurs standard, via plusieurs adresses IP résidentielles locales. Toutefois, ces adresses IP locales provenaient de fournisseurs d'hébergement VPS, et chaque client n'avait accès qu'à un ensemble standard de pages. Après quelques itérations de ces demandes, les modèles de trafic ont été corrélés, identifiés comme des tentatives de price scraping et bloqués.

Une fois que ces bots de scraping ont été neutralisés, les mauvais bots ont commencé à se présenter sous différents modèles de navigateur et avec des adresses IP situées dans des pays voisins. Cette fois, l'activité a été plus facile à identifier car les nouveaux clients utilisaient des en-têtes de navigateur non standard et accédaient aux mêmes pages, ce qui a également permis de les bloquer.



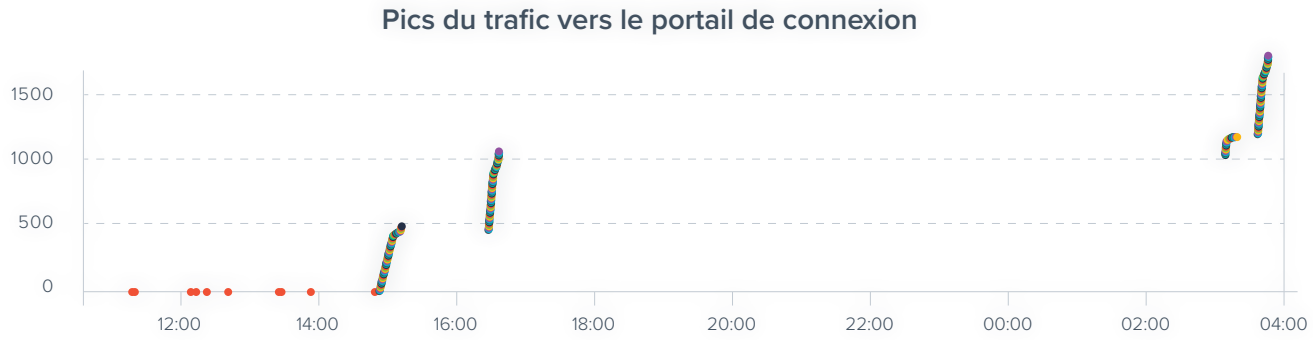
Les bots accédaient à plusieurs reprises au même ensemble d'URL de produits en une heure après le blocage de la première vague.



Les bots tentent d'accéder à un plus petit ensemble de pages de produits selon un modèle de navigation différent plusieurs fois par heure.

Exemple 5 : tentative de saturation du portail de connexion d'une entreprise de fabrication indienne

Dans cet exemple, le portail de connexion d'une entreprise de fabrication indienne connaissait un trafic inhabituellement élevé. Le trafic venait principalement des réseaux mobiles, ce qui était inhabituel, mais pas non plus inattendu pour ce site Web. Après une analyse plus poussée, le système a cependant déterminé que le trafic entrant provenait probablement d'un navigateur de bureau qui usurpait l'identité d'un appareil mobile lorsqu'il était connecté à un point d'accès. Les clients qui tentaient de saturer cette page de connexion ont été bloqués avec succès, et le temps de réponse de la page est revenu à la normale.



Les premiers points correspondaient à un bot se faisant passer pour un humain et distribuant ses identifiants d'accès.
Après cela, des clusters se sont formés et chaque point représente un client distinct tentant d'accéder à la page de connexion.

Bonnes pratiques de protection contre les attaques de bots

Les bots malveillants constituent aujourd'hui un problème majeur pour les propriétaires d'applications Web et API. Ils attaquent les comptes utilisateur, détournent les analyses, extraient des données et détruisent l'expérience client. Pour finir, ils peuvent conduire à une violation de données. Selon The State of Application Security in 2021, les attaques par bots sont les plus susceptibles d'avoir contribué à des violations de sécurité réussies résultant des vulnérabilités des applications au cours des 12 derniers mois.

Lorsqu'il est question de se protéger contre des types d'attaques plus récents, tels que les bots, les systèmes de défense peuvent parfois être submergés en raison du nombre de solutions requises. La bonne nouvelle, c'est que ces solutions sont regroupées dans des offres WAF/ WAF-as-a-Service également connues sous le nom de services de protection des applications Web et API (WAAP).

Pour protéger votre entreprise, ainsi que vos données, analyses et stocks, vous devez investir dans une technologie WAAP qui identifie et bloque les bots malveillants. Cela améliorera l'expérience utilisateur et renforcera la sécurité globale.

- **Mettez en place une sécurité des applications appropriée.** Installez une solution web application firewall ou WAF-as-a-Service et veillez à ce qu'elle soit correctement configurée. Il s'agit-là d'une première étape importante pour garantir le bon fonctionnement de votre solution de sécurité des applications.

- **Investissez dans la protection contre les bots.** Assurez-vous que la solution de sécurité des applications que vous choisissez inclut une protection antibot afin qu'elle puisse détecter et arrêter efficacement les attaques automatisées avancées.

- **Tirez parti du machine learning.** Grâce à une solution qui exploite la puissance du machine learning, vous pouvez détecter et bloquer efficacement les attaques masquées des bots « presque humains ». Assurez-vous également d'activer la protection contre le credential stuffing pour empêcher le piratage de compte.

A propos de Barracuda

Rendre le monde plus sûr est notre objectif chez Barracuda.

Nous pensons que chaque entreprise doit se doter de solutions cloud, faciles à acquérir, à déployer et à utiliser, tout en gardant leur niveau de sécurité. Nous protégeons les e-mails, les réseaux, les données et les applications avec des solutions innovantes et évolutives, qui s'adaptent à la croissance de nos clients.

Plus de 200 000 entreprises à travers le monde font confiance à Barracuda pour les protéger – elles restent sereines face aux risques qui sont toujours là – et peuvent se concentrer sur le développement de leur business.

Pour en savoir plus, rendez-vous sur fr.barracuda.com.

Barracuda®
Your journey, secured.