imperva
a Thales company

#RAPPORTBADBOTS2025

2025

RAPPORT « BAD BOTS » 2025

La multiplication des bots,
un danger sous-estimé par les entreprises

Résumé

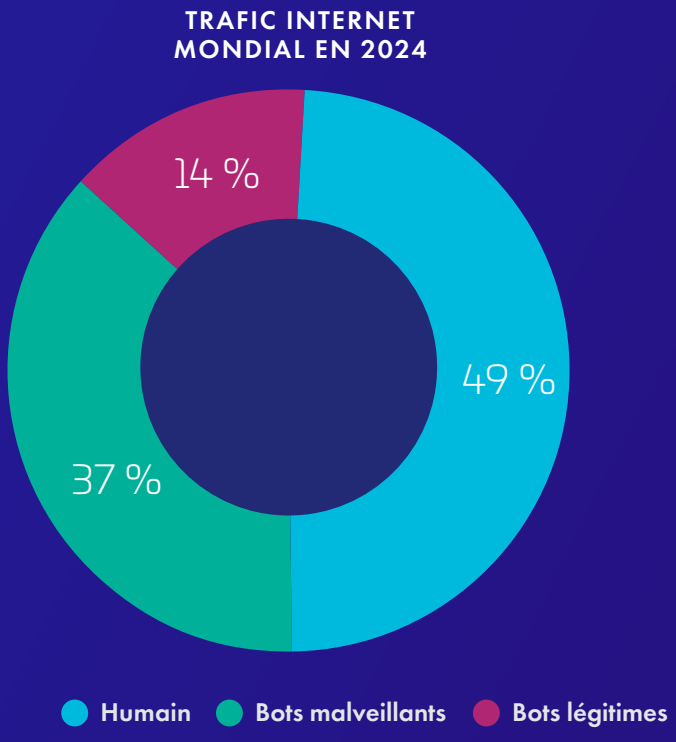
Le rôle de l'IA dans les attaques de bots

Les outils d'intelligence artificielle ont profondément transformé la cybercriminalité. Les menaces automatisées se multiplient, gagnent en complexité et deviennent plus difficiles à détecter. Les bots deviennent plus furtifs, plus adaptatifs, et placent les entreprises dans une position défensive permanente. Grâce à l'IA, les cybercriminels peuvent concevoir, tester et déployer des bots malveillants à grande échelle, avec une rapidité et une efficacité inédites. Ils peuvent aussi analyser les attaques de bots qui ont échoué, affiner leurs tactiques et contourner plus finement les dispositifs de sécurité. Avec l'IA générative, même les cybercriminels les moins qualifiés peuvent créer des bots. Face à une telle situation, les équipes de sécurité doivent repenser leur stratégie de protection applicative et adopter une approche dynamique, capable d'anticiper les attaques.

Le trafic automatisé dépasse le trafic humain

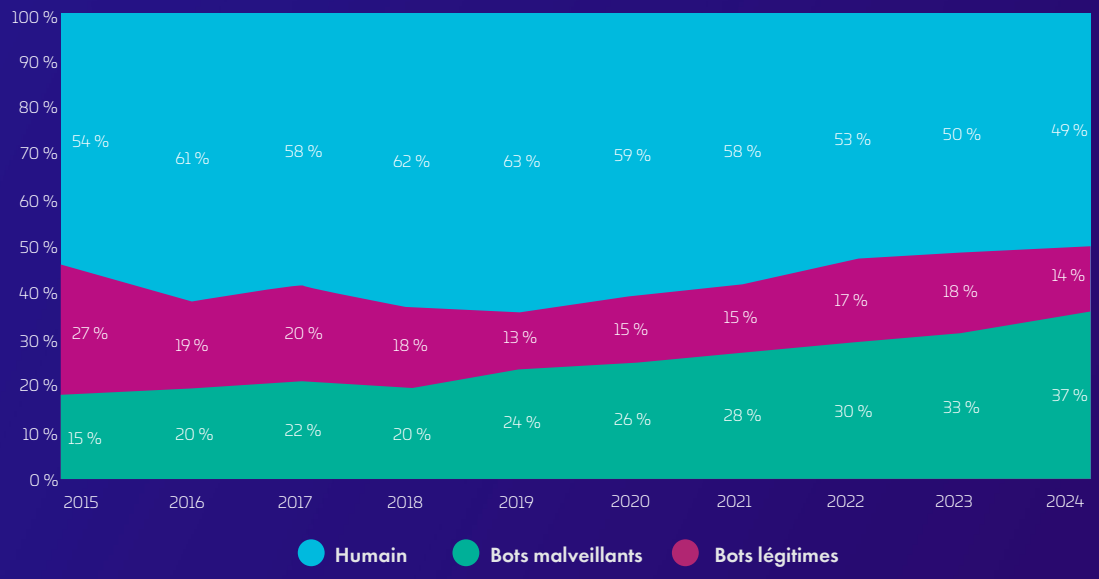
Pour la première fois en dix ans, le trafic automatisé a dépassé l'activité humaine, avec 51 % de l'ensemble du trafic web en 2024. Ce changement s'explique principalement par l'adoption rapide de l'IA et des grands modèles de langage (LLM), qui ont rendu la création de bots beaucoup plus accessible et évolutive.

Parallèlement, l'activité des bots malveillants a augmenté pour la sixième année consécutive : désormais, ils représentent 37 % de l'ensemble du trafic internet, une hausse marquée par rapport aux 32 % observés en 2023.



Le graphique ci-dessous illustre une tendance inquiétante : les bots malveillants gagnent du terrain année après année. En 2015, ils ne constituaient encore que 15 % du trafic. L'explosion de l'activité en ligne liée à la pandémie de COVID-19 a marqué un tournant en 2019. Depuis, leur progression ne faiblit pas, atteignant 37 % du trafic en 2024.

TRAFIC INTERNET MONDIAL DE CES 10 DERNIÈRES ANNÉES



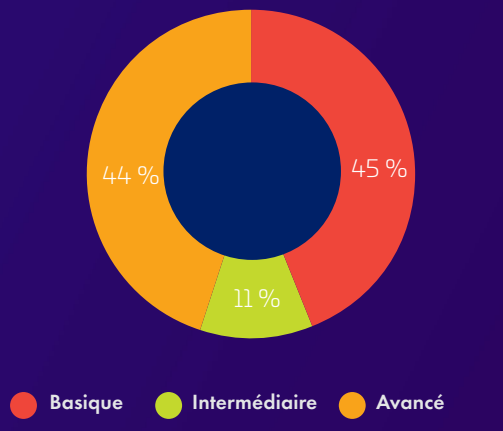
Avec l'essor de l'intelligence artificielle, une question majeure se pose désormais : comment freiner cette prolifération afin de protéger les entreprises et préserver l'équité des marchés numériques ?

Sophistication des attaques de bots

Les attaques simples mais massives progressent rapidement : elles comptent désormais pour 45 % du total, contre 40 % en 2023. Cette évolution s'explique par la démocratisation des outils d'automatisation fondés sur l'IA, qui permettent à des acteurs moins expérimentés de lancer facilement des attaques à grande échelle.

En 2024, les attaques de bots avancées ou intermédiaires ont représenté 55 % de l'ensemble des attaques recensées. Ces attaques emploient désormais des techniques particulièrement élaborées et capables d'imiter le comportement humain, ce qui complique leur détection et leur neutralisation.

NIVEAU DE SOPHISTICATION DES BOTS EN 2024



Les menaces automatisées OWASP représentent près d'un tiers des attaques

Au cours de l'année écoulée, près d'un tiers (31 %) des attaques détectées et bloquées par Imperva étaient menées de manière automatisée. Autrement dit, elles reposaient sur des bots ou des scripts capables d'agir sans intervention humaine. Selon la classification de l'OWASP, ces menaces automatisées regroupent plusieurs types d'attaques exploitant les failles des applications web pour contourner les systèmes de sécurité, collecter des données ou perturber les activités en ligne. Elles figurent aujourd'hui parmi les formes d'attaques les plus fréquentes et les plus préoccupantes pour les organisations.

L'analyse détaillée révèle que 25 % de ces attaques proviennent de bots malveillants sophistiqués conçus pour détourner la logique métier des applications, c'est-à-dire pour exploiter le fonctionnement normal des applications à des fins frauduleuses.

Les API doivent être protégées contre les bad bots

En 2024, l'équipe de recherche sur les menaces d'Imperva a observé une forte hausse des attaques ciblant les API : 44 % du trafic de bots avancés visait désormais directement ces interfaces. Les bots malveillants qui exploitent la logique métier des API représentent aujourd'hui l'une des menaces les plus sérieuses : ils peuvent perturber des processus critiques, compromettre des données sensibles ou détourner des fonctionnalités essentielles. Protéger les API ne relève donc plus seulement de la cybersécurité : il s'agit de préserver les fondations mêmes de l'écosystème numérique des organisations. Le présent rapport consacre une section à la sécurité des API, un enjeu majeur pour les entreprises.

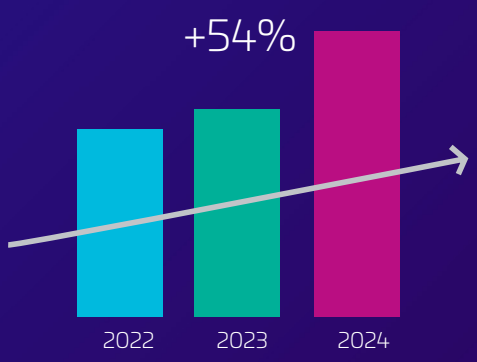
Les proxies résidentiels restent une stratégie d'évasion privilégiée

21 % de l'ensemble des attaques menées via des fournisseurs d'accès à internet (FAI) ont transité par des proxys résidentiels, une tactique d'évasion fréquemment employée par les cybercriminels avancés. Les proxys résidentiels donnent au trafic automatisé des bots l'apparence d'un simple usage domestique du web.

Attaques de prise de contrôle de compte

Le nombre d'attaques par prise de contrôle de comptes (ATO) a fortement augmenté, avec une hausse de 40 % par rapport à l'an dernier et de 54 % depuis 2022. Cette envolée s'explique probablement par l'utilisation accrue de l'IA et du machine learning par les cybercriminels : ces technologies automatisent le bourrage d'identifiants (credential stuffing) et les attaques par force brute. Ces technologies rendent aussi ces attaques plus sophistiquées et difficiles à détecter.

ÉVOLUTION DES ATTAQUES ATO 2022 À 2024

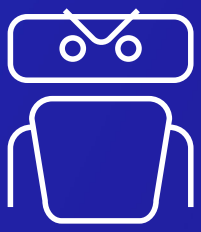


« 25 % des attaques neutralisées proviennent de bots malveillants sophistiqués exploitant spécifiquement la logique métier. »

Sommaire

Chiffres clés

51% DU TRAFIC INTERNET ÉTAIT AUTOMATISÉ EN 2024

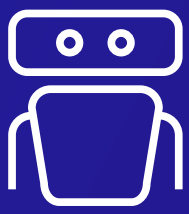


37% DU TRAFIC INTERNET A ÉTÉ ATTRIBUÉ AUX BAD BOTS

14% DU TRAFIC INTERNET A ÉTÉ GÉNÉRÉ PAR DES BOTS LÉGITIMES

55%

DES ATTAQUES DE BOTS ONT ÉTÉ MENÉES PAR DES BOTS INTERMÉDIAIRES OU AVANCÉS EN 2024



45%

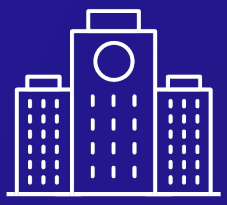
DES ATTAQUES DE BOTS ONT ÉTÉ MENÉES PAR DES BOTS BASIQUES EN 2024

44%

DES CYBERATTAQUES SOPHISTIQUÉES ONT VISÉ LES API

+ 55%

DE FUITES DE DONNÉES API ET DE VIOLATIONS D'API EN 2024



25%

DES ATTAQUES DE BOTS ONT CIBLÉ LES ENTREPRISES

19%

DES ATTAQUES DE PRISE DE CONTRÔLE DE COMPTE ONT CIBLÉ LES API

46% DES ATTAQUES DE BOTS UTILISENT CHROME POUR IMITER UN TRAFIC LÉGITIME

14% DES CONNEXIONS ONT ÉTÉ CIBLÉES PAR DES TENTATIVES DE PRISE DE CONTRÔLE DE COMPTE

31% DES ATTAQUES SONT BASÉES SUR DES MENACES AUTOMATISÉES (OWASP)

2 MILLIONS

D'ATTAQUES QUOTIDIENNES SONT ASSISTÉES PAR L'IA CHAQUE JOUR

27%

DES ATTAQUES DE BOTS ONT CIBLÉ LE SECTEUR DU TOURISME EN 2024

13 MILLE MILLIARDS DE REQUÊTES DE BOTS ONT ÉTÉ BLOQUÉES PAR IMPERVA EN 2024

+40%

DE PRISES DE CONTRÔLE DE COMPTE EN 2024

Les attaques de bots exploitent la logique métier des API

Portées par la transformation numériques et l'intelligence artificielle, les API se multiplient. Ces interfaces sont devenues l'un des piliers du numérique: elles connectent les services, simplifient les opérations et permettent de proposer des expériences client personnalisées à grande échelle. Elles interviennent dans tous les domaines, des paiements en ligne à la gestion logistique, en passant par l'analyse de données ou l'intégration de services tiers, et sont aujourd'hui essentielles à l'efficacité, à l'innovation et à la compétitivité des entreprises. Avec la généralisation du cloud et des architectures à base de microservices, les API forment l'infrastructure technique indispensable pour accroître la performance, accélérer le développement et créer de nouvelles sources de revenus.

La logique propre à chaque API repose sur un ensemble de règles de traitement et de contrôle, qui déterminent comment les données sont manipulées et comment les opérations critiques sont exécutées. Ces mécanismes rendent possibles l'automatisation, les décisions en temps réel et la continuité des échanges entre services. Mais ils constituent aussi une cible privilégiée pour les cybercriminels, qui cherchent à exploiter ces points de passage pour mener des cyberattaques, extraire des données ou contourner les dispositifs de protection.

Les bad bots ne se contentent plus de saturer les points d'accès : ils apprennent à exploiter les règles internes qui régissent le fonctionnement des API. Les cybercriminels automatisent désormais des attaques à grande échelle comme le détournement de comptes, la fraude aux paiements ou le vol de données, en reproduisant le comportement d'utilisateurs légitimes.

La logique de chaque API étant propre à l'organisation qui l'exploite, les approches de sécurité basées sur des signatures connues se révèlent souvent inefficaces : les attaques passent de ce fait inaperçues, provoquant des pertes financières, une dégradation de la confiance et des risques réglementaires accrus.

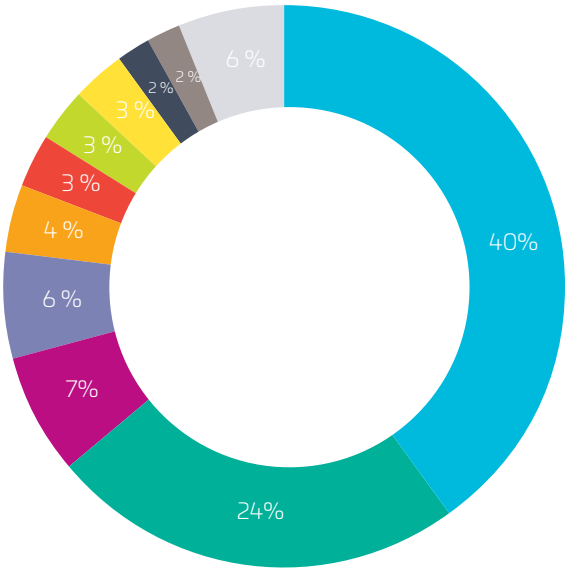
La analyse qui suit a été menée par l'équipe Imperva Threat Research. Elle décrit comment les bots ciblent les API. Elle présente les secteurs les plus vulnérables, les techniques utilisées et les nouvelles formes de cyberattaques.

API vs applications web

En 2024, l'équipe Imperva Threat Research a constaté une forte hausse des attaques dirigées contre les API : 44 % du trafic de bots sophistiqués visait désormais ces interfaces, contre seulement 10 % pour les applications web. Cette évolution traduit une stratégie délibérée des cybercriminels, qui concentrent désormais leurs attaques sur les points d'accès aux données sensibles et à forte valeur.

Principaux secteurs ciblés par les attaques de bots sur les API

Les services financiers, les télécoms, la santé et la commerce de détail font partie des dix secteurs les plus ciblés par les attaques de bots sur les API. Ces secteurs utilisent les API pour des opérations essentielles et pour la gestion de données sensibles, ce qui en fait des cibles privilégiées pour des attaques sophistiquées.

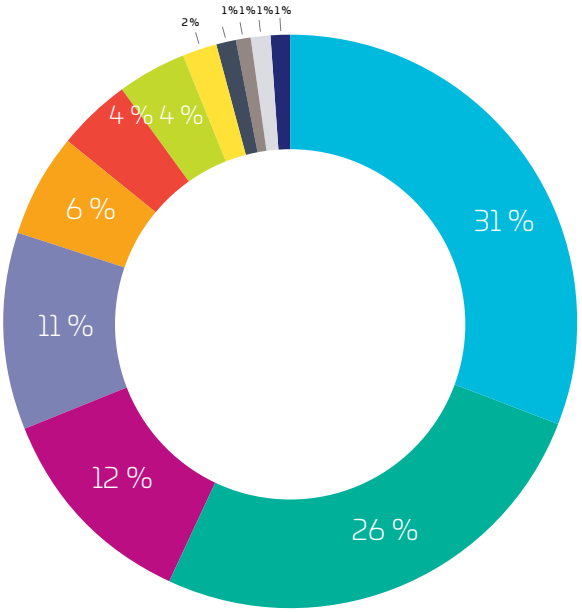


SECTEURS LES PLUS CIBLÉS PAR LES ATTAQUES D'API

- Services financiers
- Business
- Télécommunications & fournisseurs d'accès
- Santé
- Mode de vie
- Éducation
- Commerce de détail
- Informatique
- Société
- Tourisme
- Autres

Techniques et tactiques d'attaque sur les API

Notre analyse 2024 des attaques de bots sur les API révèle une menace multiforme : les cybercriminels utilisent une multitude de méthodes pour exploiter les failles des API :



RÉPARTITION DES ATTAQUES SUR LES API

- Extraction de données
- Fraude au paiement
- Prise de contrôle de compte (ATO)
- Achats en masse (scalping)
- Collecte d'informations utilisateur
- Téléchargement et exécution à distance
- Fraude sur les cartes cadeaux
- Détournement de session
- Fraude à la carte bancaire
- Test automatisé de codes promotionnels
- Accès à l'interface d'administration
- Accès à des données sensibles

Extraction de données

~31 % des attaques API

Certains bots collectent d'importants volumes de données en exploitant des API qui traitent des informations sensibles ou confidentielles. Cette approche permet aux cybercriminels d'automatiser la récupération de données précieuses, comme les informations utilisateurs, les détails produits ou les indicateurs internes, sans rencontrer beaucoup de résistance. Cette extraction de données en masse facilite non seulement d'autres activités illicites, mais elle peut aussi offrir un avantage concurrentiel significatif.

Fraude au paiement

~26% des attaques API

En ciblant les points de transaction financière, les cybercriminels peuvent manipuler les processus de paiement pour commettre des fraudes. Cette méthode représente environ 26 % des attaques. Elle consiste à exploiter les failles des systèmes de paiement ou de validation pour déclencher des transactions non autorisées, ou détourner des mécanismes promotionnels. L'impact financier immédiat, associé à la perte de confiance des clients, fait de la fraude au paiement une cible privilégiée pour les bots malveillants.

Prise de contrôle de compte

~12% des attaques API

Les attaques par prise de contrôle de compte (Account Takeover ou ATO) représentent environ 12 % des attaques recensées. Elles reposent sur l'utilisation d'identifiants volés ou obtenus par force brute afin d'accéder illégalement à des comptes utilisateurs. Une fois le compte compromis, les cybercriminels peuvent consulter des données personnelles ou financières sensibles, ce qui ouvre la voie à des intrusions plus larges et à d'autres formes d'exploitation.

Revente automatisée

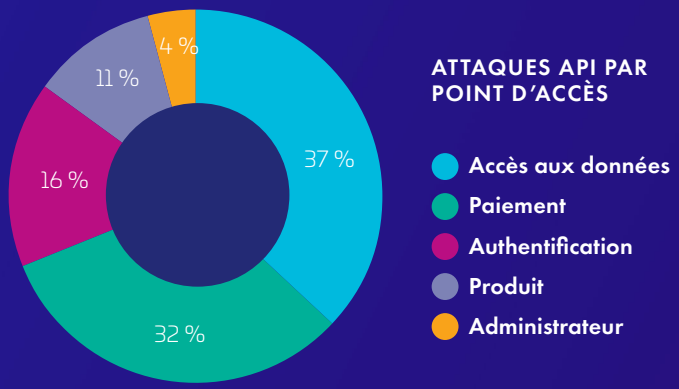
~11 % des attaques sur les API

Les attaques par scalping représentent environ 11 % des cas observés. Elles consistent à utiliser des bots capables d'acheter ou de réserver en quelques secondes de grandes quantités de produits ou de services très demandés. Cette pratique fausse l'accès équitable pour les consommateurs et perturbe le fonctionnement normal du marché, les cybercriminels revendant ensuite ces biens à des prix largement gonflés.

Outre ces principales techniques, Ils recourent aussi à la fraude aux cartes cadeaux (~4 %), à l'exécution de code à distance (Remote Code Execution, ~4 %) et au détournement de session (~2 %). Toutes ces méthodes reposent sur un même principe : l'exploitation des failles propres aux API (erreurs de configuration, limitation de requêtes insuffisante, mécanismes d'authentification trop faibles).

Attaques de bots ciblant les points d'accès

Le graphique ci-dessous montre que les bots malveillants visent en priorité les points d'accès API qui gèrent des opérations sensibles et de grande valeur :



Points d'accès aux données

~37% des attaques API

Ces points d'accès sont chargés de récupérer des informations sensibles ou confidentielles, ce qui en fait une véritable mine d'or pour les cybercriminels. Ce taux de 37% montre à quel point les cybercriminels investissent dans l'extraction et l'exfiltration de données. Les informations dont ils s'emparent servent ensuite à alimenter d'autres activités criminelles ou à constituer une forme d'intelligence concurrentielle. Les points d'accès centralisent d'importants volumes de données sensibles, et ils sont souvent moins bien protégés que les points d'accès transactionnels. Pour minimiser les risques, les équipes de sécurité doivent renforcer la surveillance, appliquer des contrôles d'accès stricts et déployer des systèmes de détection d'anomalies capables d'identifier des comportements inhabituels lors de la consultation ou du transfert de données.

Points d'accès au paiement

~32% des attaques API

Essentiels au traitement des transactions financières, les points d'accès de paiement concentrent environ 32 % de l'ensemble des attaques visant les API. Toute perturbation au niveau de ces points d'accès spécifiques a un impact immédiat sur les revenus et sur la confiance des clients. Les cybercriminels exploitent les failles de ces interfaces pour manipuler les processus de paiement, mener des opérations frauduleuses ou détourner les règles de fonctionnement des systèmes, ce qui provoque des transactions non autorisées. Ces attaques sur les processus de paiement soulignent la nécessité de renforcer la sécurité des transactions, notamment par une surveillance en temps réel, une authentification multiniveaux et des mécanismes proactifs de détection des fraudes.

Points de terminaison d'authentification

~16% des attaques API

Les points d'accès dédiés à l'authentification, qui assurent la vérification de l'identité et le contrôle des accès, représentent 16 % des attaques par bots ciblant les API. Les cybercriminels les visent pour contourner l'authentification multifactorielle, exploiter les systèmes fondés sur des tokens (token-based authentication) ou manipuler la gestion des sessions. Ces points d'accès d'authentification constituent la première ligne de sécurisation de l'accès des utilisateurs : toute compromission à ce niveau peut donc entraîner des prises de contrôle de comptes et, plus largement, des intrusions dans les systèmes. Le renforcement de ces points d'accès repose sur la mise en œuvre de protocoles d'authentification dynamiques, avec des audits réguliers pour limiter les risques d'accès non autorisé.

Globalement, la concentration des attaques sur les interfaces de données, de paiement et d'authentification illustre la volonté des cybercriminels d'exploiter les maillons les plus sensibles de l'écosystème API.

Nouvelles méthodes d'exploitation

Les bots malveillants vont au-delà des approches classiques : ils exploitent désormais les vulnérabilités des API à travers des intégrations tierces mal configurées ou la manipulation de paramètres. Ces méthodes émergentes permettent aux cybercriminels de contourner plus facilement les dispositifs de sécurité en place.

L'essor des attaques assistées par l'IA

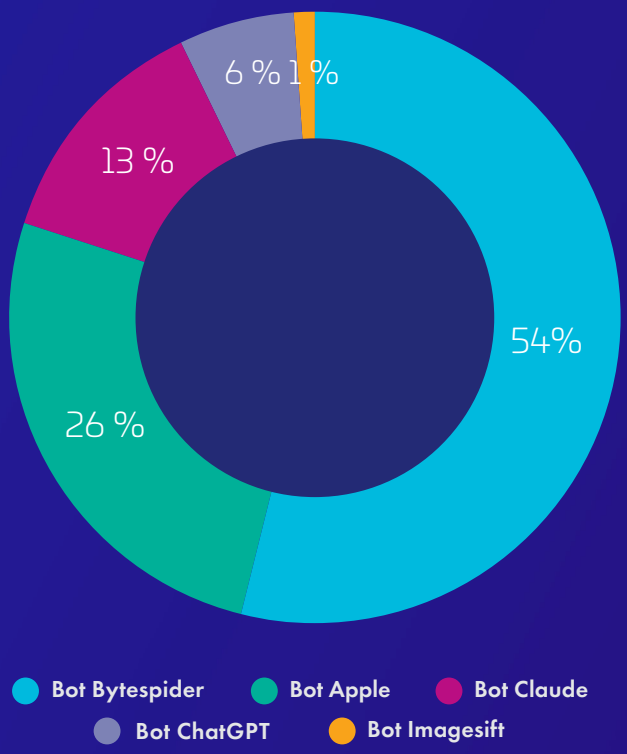
En 2024, l'usage de l'intelligence artificielle dans les cyberattaques s'est fortement accru. Imperva a bloqué en moyenne plus de deux millions d'attaques automatisées par l'IA chaque jour.

Des outils tels que ChatGPT, ByteSpider, Claude, Google Gemini, Perplexity AI, Cohere AI ou Apple Bot transforment profondément la manière dont les utilisateurs interagissent avec les services, comment les étudiants apprennent ou comment les employés produisent du contenu. Mais ces mêmes technologies deviennent aussi de nouveaux vecteurs d'attaque, désormais exploités par les cybercriminels.

Selon une analyse menée par l'équipe Imperva Threat Research, la majorité des outils d'IA actuellement utilisés servent également à mener des cyberattaques. La répartition des attaques de bots assistées par l'IA varie fortement : le bot ByteSpider est à l'origine de 54 % des attaques recensées, suivi des bots d'Apple (26 %) et de Claude (13 %). Le bot ChatGPT, quant à lui, a été utilisé par 6 % des attaques identifiées.

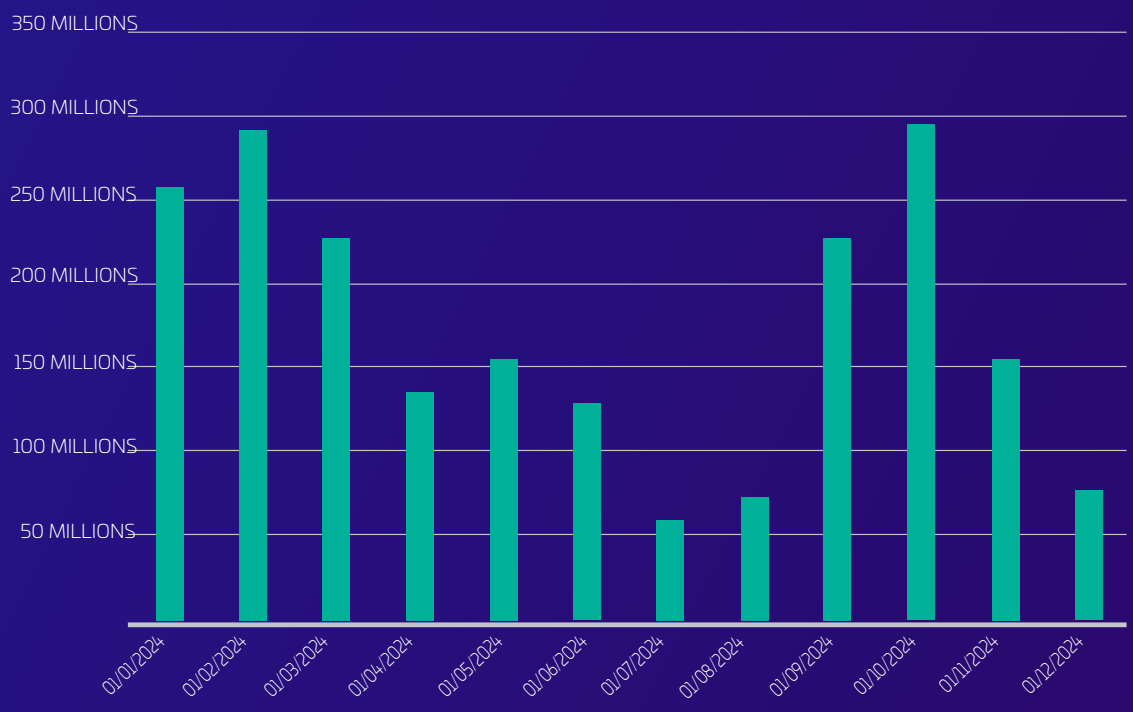
La prédominance de ByteSpider dans les attaques assistées par l'IA s'explique en grande partie par sa réputation de robot d'indexation légitime, ce qui en fait une cible idéale pour l'usurpation d'identité. Les cybercriminels déguisent fréquemment leurs bots malveillants en robots d'exploration web afin d'échapper à la détection et de contourner les protections qui accordent leur confiance aux crawlers connus. À l'inverse, les bots Apple (26 %) et Claude (13 %) semblent moins exploités, probablement en raison de mécanismes de sécurité plus stricts ou d'un potentiel d'usurpation moindre.

ATTAQUES DE BOTS PAR OUTIL D'IA



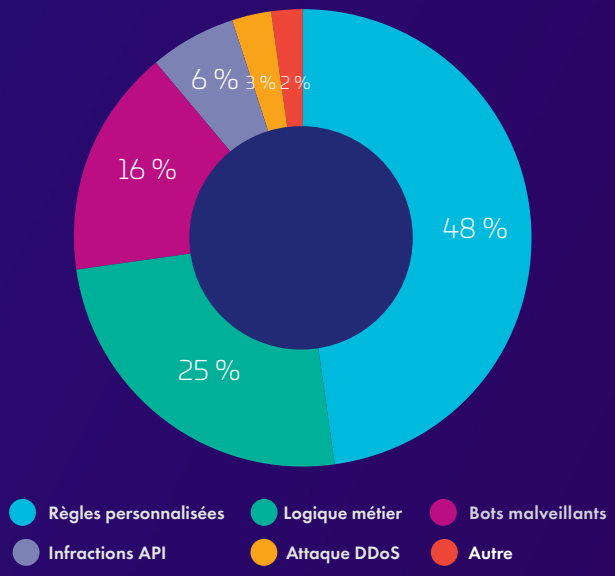
Les variations du volume d'attaques observées tout au long de l'année indiquent que les cybercriminels sont encore dans une phase d'expérimentation : ils affinent leurs méthodes pour tirer le meilleur parti de ces nouveaux outils. À mesure qu'ils s'adaptent, nous prévoyons une expansion de ce vecteur d'attaque dans les années à venir, avec une hausse des menaces automatisées.

Attaques de bots assistées par l'IA en 2024



L'intelligence artificielle offre désormais aux cybercriminels de nouveaux moyens pour mener toutes sortes d'attaques : DDoS, exploitation de règles de sécurité personnalisées, ou encore intrusions via les API. Les attaques ciblant les API sont particulièrement variées : elles peuvent impliquer des bots automatisés, mais aussi des tentatives d'accès non autorisé ou l'exploitation d'erreurs de configuration. Les attaques pilotées par des bots deviennent toutefois de plus en plus sophistiquées et difficiles à détecter. En 2024, les bots malveillants représentaient plus de 16 % des attaques assistées par l'IA. Si l'on y ajoute les attaques de la logique métier, qui utilisent l'automatisation pour mener des reconnaissances discrètes et progressives, cette proportion atteint 41 %. Cette évolution montre comment les cybercriminels s'appuient sur l'IA pour affiner leurs méthodes. Ils s'en servent notamment pour identifier et exploiter les vulnérabilités des API pour extraire des données sensibles. Plus les capacités de l'IA progresseront, plus la lutte contre les attaques de la logique métier deviendra complexe et exigeante.

Types d'attaques assistées par l'IA



Stratégies d'évasion des bots

À mesure que les bots gagnent en sophistication et imitent de plus en plus le comportement humain, les équipes de sécurité rencontrent des difficultés croissantes pour distinguer les menaces automatisées des véritables utilisateurs. Et dans un contexte de préoccupations croissantes quant à la confidentialité des données, les opérateurs de bots recourent de plus en plus à des VPN et à des techniques d'obfuscation pour se fondre dans le trafic légitime et éviter d'être détectés.

Sur la base du travail des experts Imperva de lutte contre les bots et de l'équipe Imperva de recherche sur les menaces, voici un aperçu des tactiques et techniques d'évasion utilisées par les cybercriminels en 2024 :

Usurpation d'identité du navigateur et falsification d'attributs

De nombreux bots malveillants basiques usurpent l'identité d'un navigateur (par exemple, Chrome ou Firefox). Cette technique, assez simple, s'avère très efficace pour contourner les mesures de sécurité élémentaires. Les bots plus sophistiqués vont plus loin : ils falsifient des en-têtes HTTP, simulent l'exécution de JavaScript ou reproduisent d'autres comportements de navigateur afin d'échapper aux outils de détection les plus sophistiqués.

Proxys résidentiels

Les cybercriminels exploitent des adresses IP résidentielles pour se fondre dans le trafic « normal ». Les proxies résidentiels routent le trafic malveillant via de véritables connexions domestiques, ce qui rend l'identification et le blocage fondés uniquement sur la réputation IP beaucoup moins efficaces. Si l'emploi de FAI résidentiels a légèrement reculé (de 26 % en 2023 à 21 % en 2024), cette tactique reste prisée car elle reproduit très bien le comportement d'un utilisateur réel.

Outils de confidentialité

Des services comme iCloud Private Relay masquent une partie de l'identité des utilisateurs, ce qui complique la distinction entre trafic humain légitime et activité automatisée.

Abus d'API

Les cybercriminels exploitent des API exposées ou insuffisamment protégées pour extraire des données, automatiser des attaques ou contourner les contrôles front-end.

Piratage d'applications mobiles

Les bots ciblent les applications mobiles obsolètes qui n'imposent pas de mises à jour obligatoires, les exposant ainsi à l'ingénierie inverse, au bourrage d'identifiants (credential stuffing) et à des modifications non autorisées.

Contournement des CAPTCHA

Les bots pilotés par l'IA résolvent les défis CAPTCHA avec une grande précision, rendant de nombreuses défenses classiques inefficaces.

Changement dynamique de propriétés

L'IA permet de modifier rapidement les adresses IP, les agents utilisateurs et les paramètres du navigateur pour échapper aux détections.

Navigateurs sans interface graphique

Les outils optimisés par l'IA tels que Puppeteer, Playwright et Selenium, contournent les systèmes de détection et permettent d'interagir avec les sites web comme le ferait un utilisateur réel (exécution de JavaScript, résolution de CAPTCHA, navigation dynamique sur les pages).

Scripts assistés par l'intelligence artificielle

Les scripts de bots générés par l'IA augmentent le volume d'attaques et potentialise l'efficacité de l'automatisation.

Extraction de contenus et navigateurs anti-détection

Des services d'extraction de données tels que Browser.ai permettent de collecter des informations à grande échelle, tandis que les navigateurs anti-détection comme Multilogin, GoLogin et AdsPower facilitent la neutralisation des mécanismes de sécurité.

Génération cohérente de jetons

Les bots produisent des jetons (tokens) cohérents, ce qui limite l'activation des protections anti-bot lors des processus de postback.

Bots polymorphes

Ces bots auto-apprenants modifient leurs caractéristiques en temps réel pour passer inaperçus.

Bots « as a service » (BaaS)

Les services de bots commercialisés se développent et entraînent une explosion sans précédent des menaces automatisées dans tous les secteurs.

Usurpation de navigateurs par des bots malveillants

Pour échapper aux systèmes de détection, les cybercriminels configurent leurs bots de façon à imiter les navigateurs web ou mobiles les plus utilisés par les internautes. Cette imitation, rendue possible grâce à des outils d'automatisation, reproduit le comportement d'un navigateur légitime afin de tromper les défenses en place. Autrefois considérée comme une méthode d'évasion sophistiquée, cette pratique est aujourd'hui courante et largement employée dans les attaques automatisées. Afin de rester indétectables, ces navigateurs simulés évoluent au fil du temps pour correspondre aux habitudes réelles des utilisateurs. Ainsi, Internet Explorer, autrefois largement exploité par ces outils d'automatisation, a progressivement disparu au profit de navigateurs plus récents.

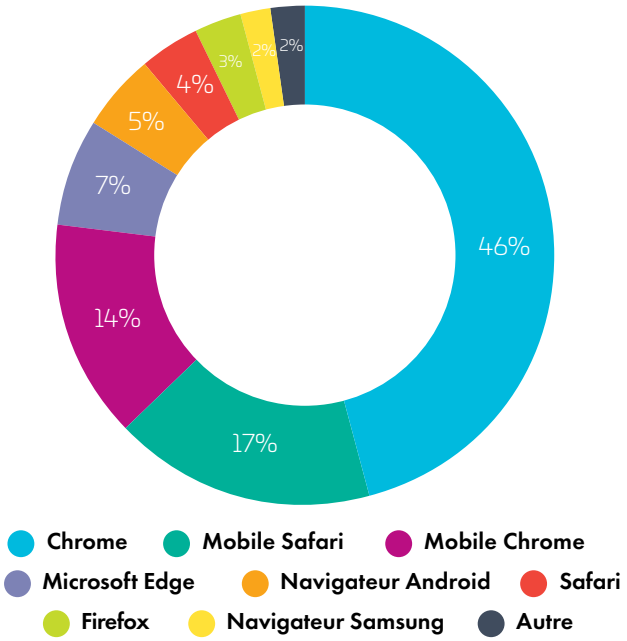
Chrome demeure, pour la dixième année consécutive, le navigateur le plus imité par les cybercriminels. En 2024, il était associé à 46 % des attaques automatisées, contre 40 % l'année précédente. Le choix de Chrome s'explique par plusieurs facteurs bien identifiés :

Une adoption massive. Chrome reste le navigateur le plus utilisé dans le monde. En se présentant comme du trafic Chrome, les bots se fondent plus facilement dans le flux global des utilisateurs réels, ce qui réduit leurs chances d'être repérés.

Un niveau de confiance élevé. De nombreux sites et systèmes de sécurité considèrent par défaut le trafic émanant de navigateurs connus comme légitime. Comme Chrome bénéficie d'une forte réputation de fiabilité, ce type de camouflage permet de contourner plusieurs filtrage de base.

Fonctionnalités avancées. Chrome prend en charge un large éventail de technologies web modernes (JavaScript, HTML5, etc.), sur lesquelles reposent la plupart des sites. En imitant ce navigateur, les bots peuvent interagir avec des contenus dynamiques et exécuter des attaques plus complexes — telles que le credential stuffing ou l'extraction automatisée de données — tout en paraissant légitimes.

NAVIGATEURS LES PLUS IMITÉS PAR LES BOTS MALVEILLANTS EN 2024



Safari mobile est le deuxième navigateur le plus imité, avec 17 % des attaques. Safari est installé par défaut sur les appareils Apple comme les iPhones et iPads. Il est donc très répandus. En imitant Mobile Safari, les cybercriminels peuvent viser une large part du trafic web mobile.

Pour des raisons similaires, **Chrome mobile** est la troisième option favorisée par les cybercriminels, avec une part stable de 14 % d'année en année.

Attaques ATO : prises de contrôle de compte

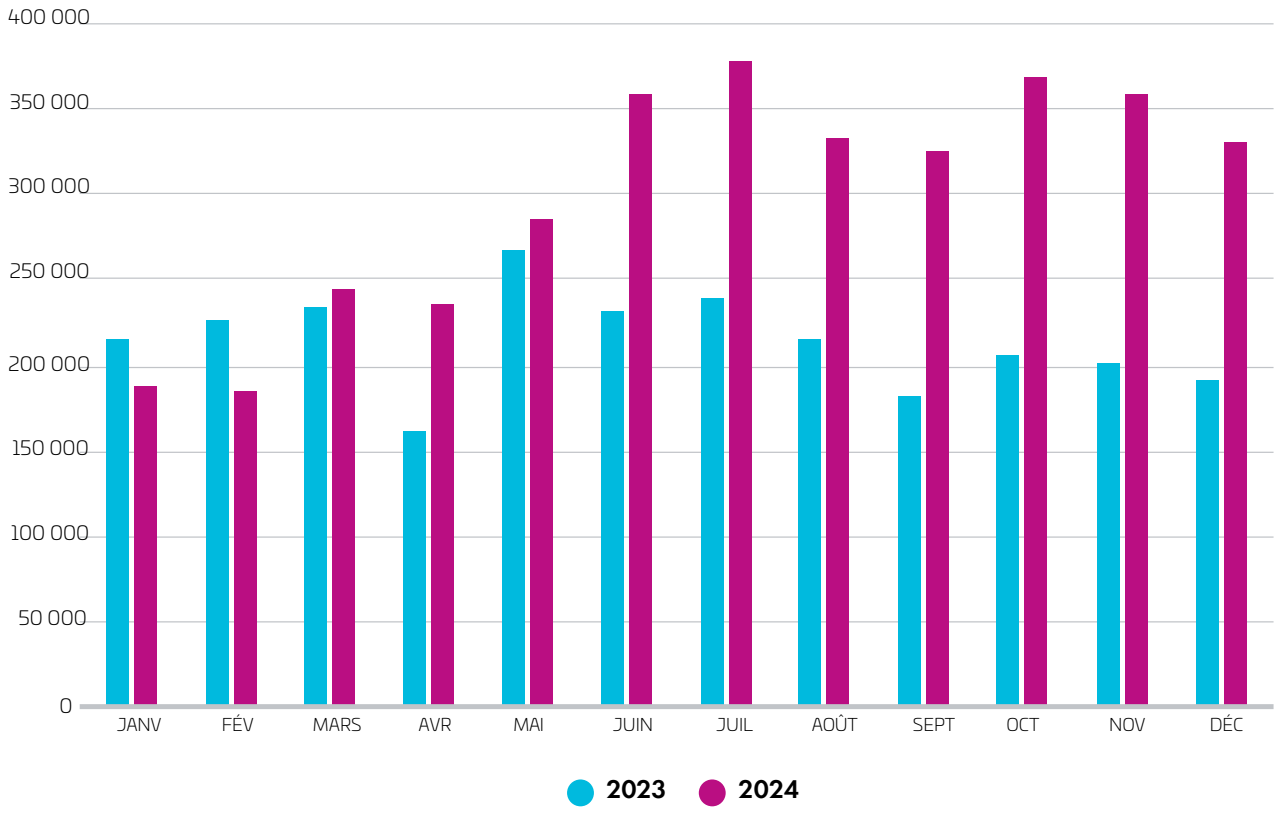
Les attaques par prise de contrôle de compte (Account Takeover, ou ATO) utilisent des bots automatisés pour obtenir un accès illégal à des comptes en ligne.

Elles s'appuient sur des techniques telles que le credential stuffing (réutilisation d'identifiants volés) ou le credential cracking (tests systématiques de combinaisons d'identifiants et de mots de passe). Ces attaques entraînent des usurpations d'identité numérique et des pertes financières importantes pour les organisations ciblées.

Les attaques ATO figurent aujourd'hui parmi les menaces les plus critiques pour les entreprises opérant en ligne. Une intrusion réussie peut provoquer des pertes financières directes, le vol de données sensibles, l'exploitation d'informations personnelles, et une atteinte durable à la réputation.

Le graphique ci-dessous montre une forte progression de ces attaques au fil des mois. Depuis juin, leur volume a augmenté de manière marquée avec une accélération nette à l'automne : entre septembre et novembre, le nombre d'attaques ATO a bondi de 79 % par rapport à la même période l'année précédente.

PRISES DE CONTRÔLE DE COMPTE PAR MOIS 2023 vs 2024



Quelques raisons viennent expliquer l'augmentation marquée des attaques ATO depuis juin dernier :

Événements e-commerce saisonniers et périodes de soldes

Les grands événements d'e-commerce — Black Friday, soldes de fin d'année et autres campagnes promotionnelles — atteignent leur pic au second semestre. Ces périodes concentrent un volume massif de transactions et d'ouvertures de comptes, ce qui attire particulièrement les cybercriminels. Les comptes à forte valeur deviennent alors des cibles privilégiées et les attaques ATO explosent.

Augmentation des violations de données

Les violations de données alimentent les bases de données d'identifiants piratés. Chaque attaque vient grossir les longues listes d'adresses e-mail et de mots de passe volés. Les cybercriminels les réutilisent ensuite pour accéder à d'autres services, via le credential stuffing. Selon le Identity Theft Resource Center (ITRC), plus d'1,7 milliard de violations ont été recensées aux États-Unis en 2024, soit une hausse de 312% par rapport aux 419 millions enregistrées en 2023.

Méthodes d'attaque plus sophistiquées

Les cybercriminels recourent désormais à des outils plus avancés, notamment des bots et systèmes d'automatisation pilotés par l'IA : ces derniers sont capables de contourner les mécanismes de sécurité traditionnels tels que les CAPTCHA ou l'authentification multifactorielle (MFA). L'émergence de ces nouveaux outils a conduit à une hausse significative du nombre d'attaques ATO réussies.

Les secteurs les plus visés par les attaques ATO

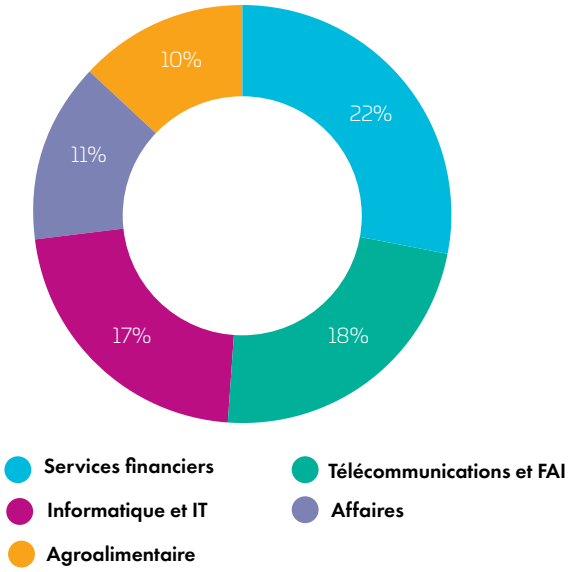
Le graphique de droite présente les cinq secteurs les plus ciblés par les attaques de prise de contrôle de comptes en 2024. Ensemble, ils représentent 78 % de l'ensemble des attaques

Le secteur le plus visé est celui des services financiers, avec 22 % de toutes les attaques ATO, suivi des télécoms et FAI avec 18 %, et de l'informatique, avec 17 %.

Le secteur des services financiers reste une cible privilégiée pour ce type d'attaque. Banques, sociétés de cartes de crédit et plateformes fintech détiennent une quantité considérable d'informations personnelles identifiables (PII) : coordonnées bancaires, numéros de carte, données d'identité. Ces informations se revendent facilement sur le dark web, où elles constituent une ressource lucrative pour les cybercriminels. L'essor des API dans ce secteur a ouvert de nouvelles perspectives pour les cybercriminels : ils exploitent désormais les failles liées à une authentification insuffisante ou à des droits d'accès mal configurés pour s'emparer de comptes et dérober des données.

Le **secteur des télécommunications** figure également parmi les principales cibles des attaques ATO, mais les motivations y dépassent la simple recherche de profit. Certes, l'accès à des données clients sensibles peut rapporter un gain financier, mais ce secteur contrôle aussi une part essentielle de l'infrastructure internet mondiale. En compromettant les comptes ou les systèmes d'un fournisseur d'accès internet (FAI), les cybercriminels peuvent intercepter ou rediriger le trafic (attaques de type man-in-the-middle), déployer des logiciels malveillants, voire perturber des services. Dans certains cas, notamment lors de tensions géopolitiques, certains acteurs étatiques ciblent les entreprises de télécommunication à des fins d'espionnage ou de surveillance.

Cinq secteurs concentrent 78 % des attaques par prise de contrôle de compte



Conséquences d'une compromission de compte

Une attaque par prise de contrôle de compte peut déboucher sur des fuites importantes de données et donc avoir de lourdes conséquences : amendes réglementaires, frais juridiques, demandes d'indemnisation, atteinte à la réputation et pertes financières durables. La gravité de l'impact dépend de plusieurs facteurs : la nature de la violation, le cadre réglementaire applicable et la réactivité de l'entreprise concernée.

RÉGLEMENTATION	SANCTIONS	CONSÉQUENCES SUPPLÉMENTAIRES
RGPD (Règlement général sur la protection des données)	Sanctions pouvant aller jusqu'à 20 millions € ou 4 % du chiffre d'affaires mondial annuel en cas de non-protection des données personnelles	Pénalités supplémentaires en cas de non-déclaration aux autorités dans les 72 heures
CCPA (California Consumer Privacy Act)	Amendes pouvant atteindre 2 500$ par infraction ou 7 500$ en cas de violation intentionnelle	Recours juridiques des utilisateurs pour la divulgation de données personnelles, avec notamment des actions collectives
HIPAA (Loi sur la portabilité et la responsabilité en matière d'assurance maladie)	Sanctions allant de 100$ à 50 000$ par infraction, avec un plafond annuel de $1,5 million	Sanctions lourdes en cas de divulgation d'informations de santé protégées (PHI)

Les bots malveillants : un fléau mondial

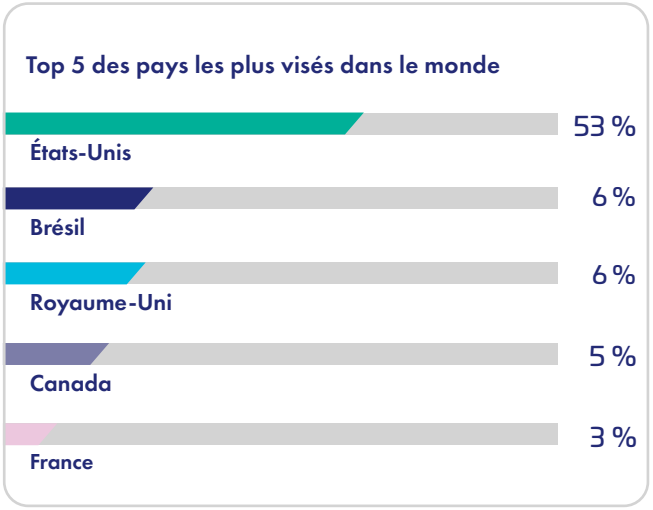
Plus de la moitié des attaques de bots ont visé les États-Unis

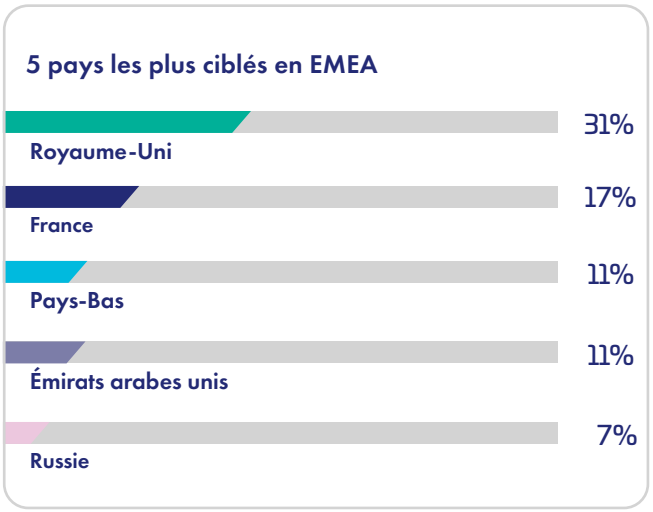
Les États-Unis restent le pays le plus ciblé par les attaques de bots, avec 53 % de toutes les attaques en 2024. Le Brésil et le Royaume-Uni arrivent ex æquo en deuxième position, chacun étant la cible de 6 % des attaques.

Les États-Unis possèdent la plus grande économie numérique au monde, avec des millions de transactions en ligne chaque jour. Grâce à une forte concentration de richesse mondiale, d'institutions financières majeures et de géants de la tech, ce pays attire tout particulièrement les cybercriminels en quête de profits.

Près d'un tiers des attaques de bots en région EMEA ont visé des sites britanniques

En 2024, le Royaume-Uni a été le pays le plus ciblé dans la région EMEA (Europe, Moyen-Orient et Afrique), avec 31 % des attaques de bots. À l'image des États-Unis, le Royaume-Uni est un centre financier majeur de la région, avec une forte présence de banques, de sociétés fintech et une importante concentration de richesse à Londres. Cela en fait une cible privilégiée pour les cybercriminels désireux d'exploiter des transactions financières, de prendre le contrôle de comptes ou de lancer des attaques de bots frauduleuses.





Les facteurs géopolitiques continuent d'influencer en profondeur le paysage de la cybersécurité. La Russie et l'Ukraine figurent toutes deux parmi les dix pays les plus ciblés de la région EMEA. Les attaques observées dans ces pays sont variées : opérations soutenues par des États, actions de hacktivisme ou encore campagnes à motivation financière. Cette situation montre toute la complexité des cyber-risques dans la région.

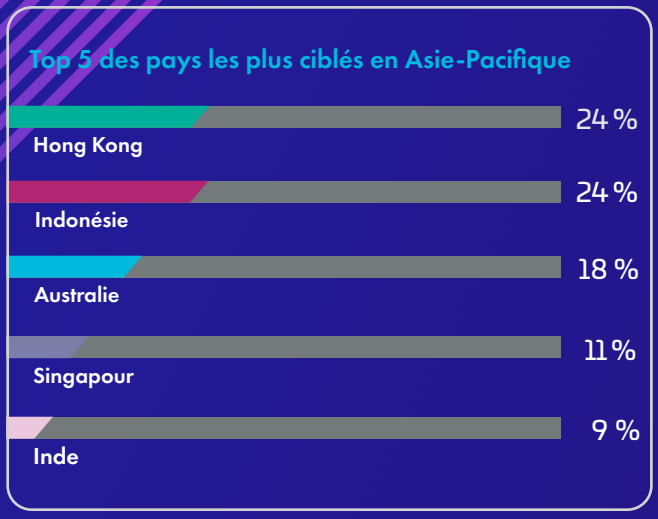
Pays les plus ciblés dans la région APAC

En 2024, les attaques par bots dans la région Asie-Pacifique (APAC) se sont concentrées principalement à Hong Kong et en Indonésie, chacun représentant 24 % du total.

À elles deux, ces économies totalisent donc près de la moitié de l'activité malveillante recensée dans la région. La position de Hong Kong, à la fois centre financier mondial et porte d'entrée vers la Chine, en fait une cible privilégiée pour les cybercriminels qui cherchent à exploiter le secteur bancaire, la fintech et le commerce en ligne. En Indonésie, la croissance rapide de l'économie numérique, combinée à des infrastructures de cybersécurité encore fragiles, favorise la multiplication des fraudes automatisées et des attaques par credential stuffing.

L'Australie arrive en troisième position, avec 18 % des attaques. Économie développée, dotée d'un secteur financier solide, d'un marché e-commerce dynamique et d'infrastructures critiques, elle reste une cible fréquente pour les cybercriminels qui utilisent des bots pour mener des campagnes de vol d'identifiants ou de fraudes automatisées.

Ainsi, en région APAC, la croissance économique, l'expansion numérique et les tensions géopolitiques se conjuguent pour redessiner les risques liés à la cybersécurité.



Pays les plus ciblés en Amériques

En 2024, les États-Unis sont restés la principale cible des attaques par bots sur le continent américain, concentrant à eux seuls 76 % des incidents recensés. Derrière eux, le Brésil (9 %) et le Canada (7 %) figurent parmi les pays les plus touchés de la région.

La place du Brésil s'explique par plusieurs facteurs : une économie numérique en forte expansion, l'adoption massive des services bancaires mobiles et un niveau élevé de fraude en ligne. Les cybercriminels y exploitent les failles des secteurs financier et du e-commerce, notamment à travers des attaques de credential stuffing et des fraudes aux paiements. La taille de la population et le taux élevé de connexion à internet renforcent l'attractivité du pays pour les attaques automatisées.

Le Canada, troisième du classement, demeure une cible régulière en raison de la solidité de son secteur bancaire, du développement du commerce en ligne et de la numérisation croissante des services publics.
Les attaques y prennent souvent la forme de prises de contrôle de comptes, de fraudes automatisées ou de collectes illicites de données sensibles. Sa proximité économique et numérique avec les États-Unis en fait par ailleurs une cible évidente pour les cybercriminels, qui cherchent à exploiter les échanges transfrontaliers et les infrastructures numériques communes.

Analyse sectorielle

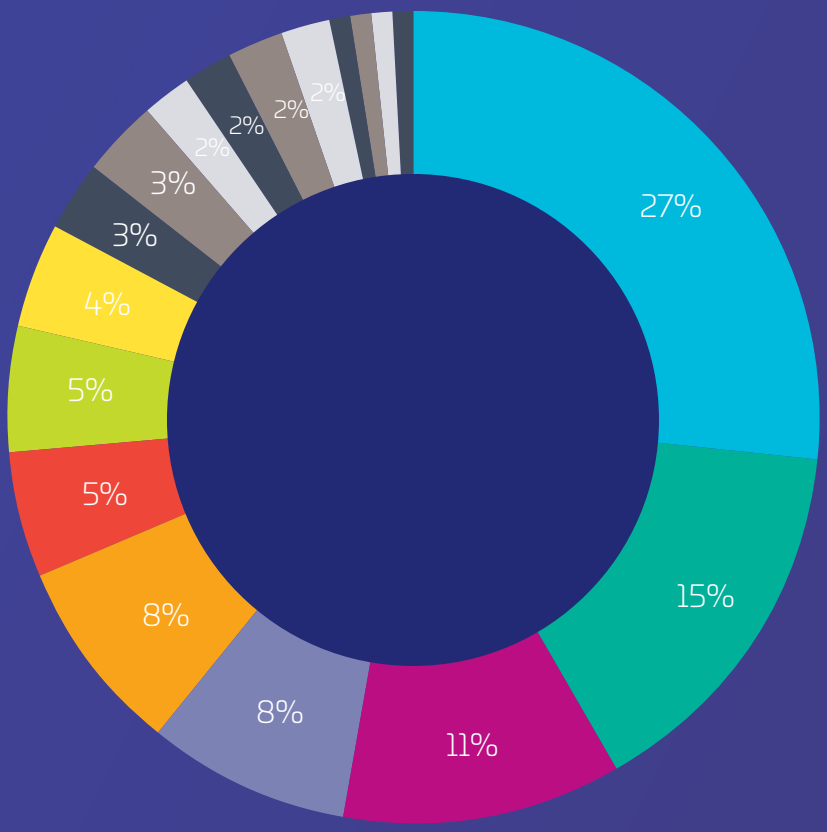
Principaux secteurs ciblés par les attaques de bot

En 2024, le secteur du tourisme a pris la tête du classement. Il concentre désormais 27 % de l'ensemble des attaques par bots, soit plus d'un quart du total. Le commerce de détail, pour sa part, recule nettement : il ne représente plus que 15 % des attaques, contre 24 % l'année précédente.

Les bots malveillants constituent 41 % du trafic dans le tourisme et 59 % dans le commerce de détail. Dans la suite de ce rapport, nous analyserons les raisons qui expliquent la présence accrue des bots dans ces secteurs.

L'éducation occupe désormais la troisième place, avec 11 % du trafic de bots malveillants dirigé vers ses plateformes. Fait marquant : il s'agit du secteur où la proportion de bots simples est la plus élevée (92 %). Ce phénomène suggère que certaines attaques proviennent d'acteurs moins expérimentés, voire d'étudiants exploitant des outils d'IA générative pour mener des expérimentations.

Enfin, la part du trafic malveillant dirigé vers les services financiers a été divisée par deux en un an, passant de 16 % à 8 %.



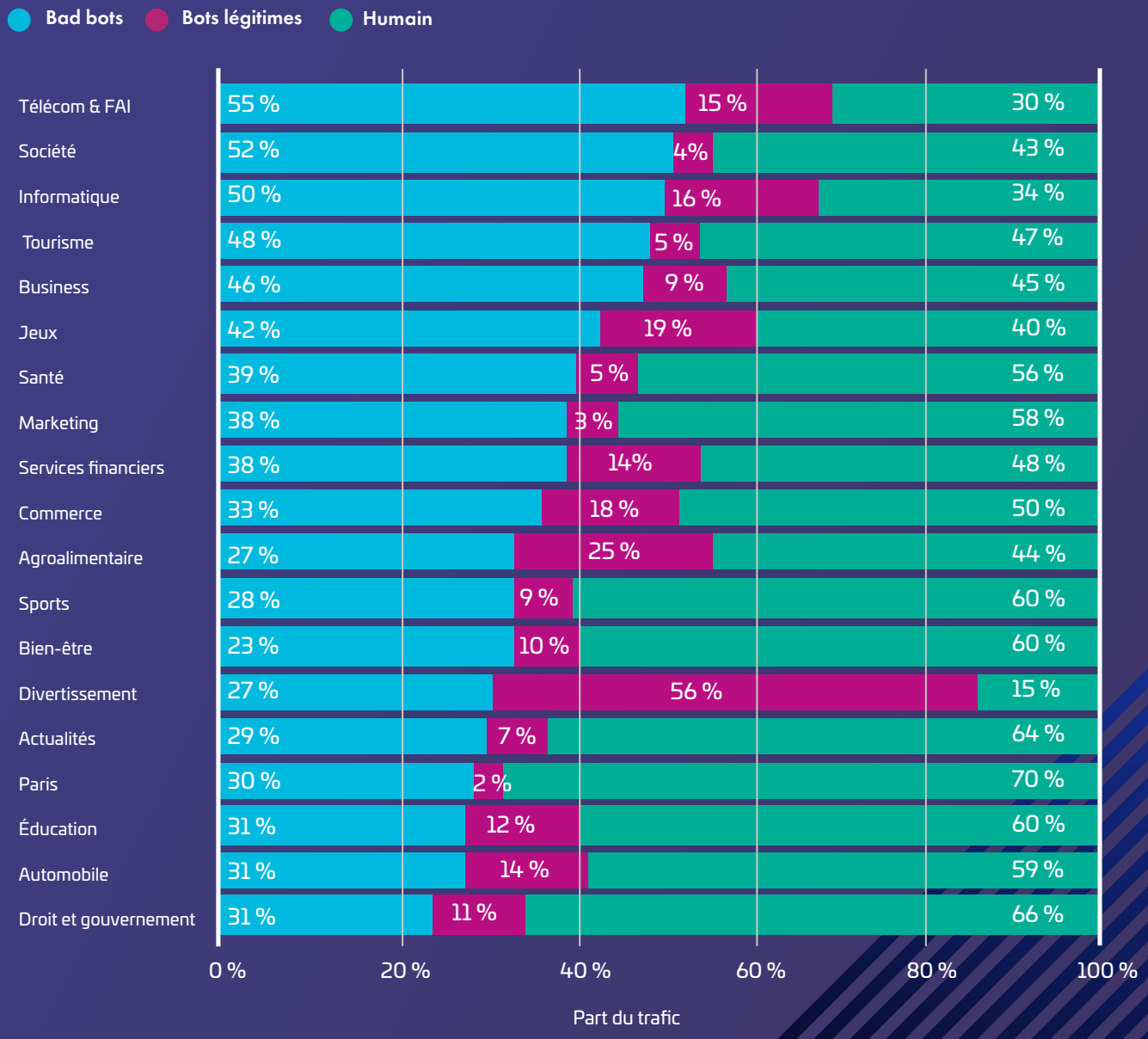
PRINCIPAUX SECTEURS CIBLÉS

- Tourisme
- Commerce
- Éducation
- Services financiers
- Business
- Informatique et IT
- Santé
- Droit et gouvernement
- Télécom et FAI
- Jeu
- Automobile
- Bien-être
- Société
- Agroalimentaire
- Divertissement
- Jeu
- Sports
- Actualité

Bad bot, bot légitime et humains

Le graphique ci-dessous présente la répartition du trafic des bots légitimes, des bad bots et des humains, selon les différents secteurs. Le secteur Télécom et FAI affiche le plus fort taux de trafic automatisé avec 56 %. La catégorie Société arrive juste derrière, avec 52 %, suivie par le secteur Informatique, avec 50 %.

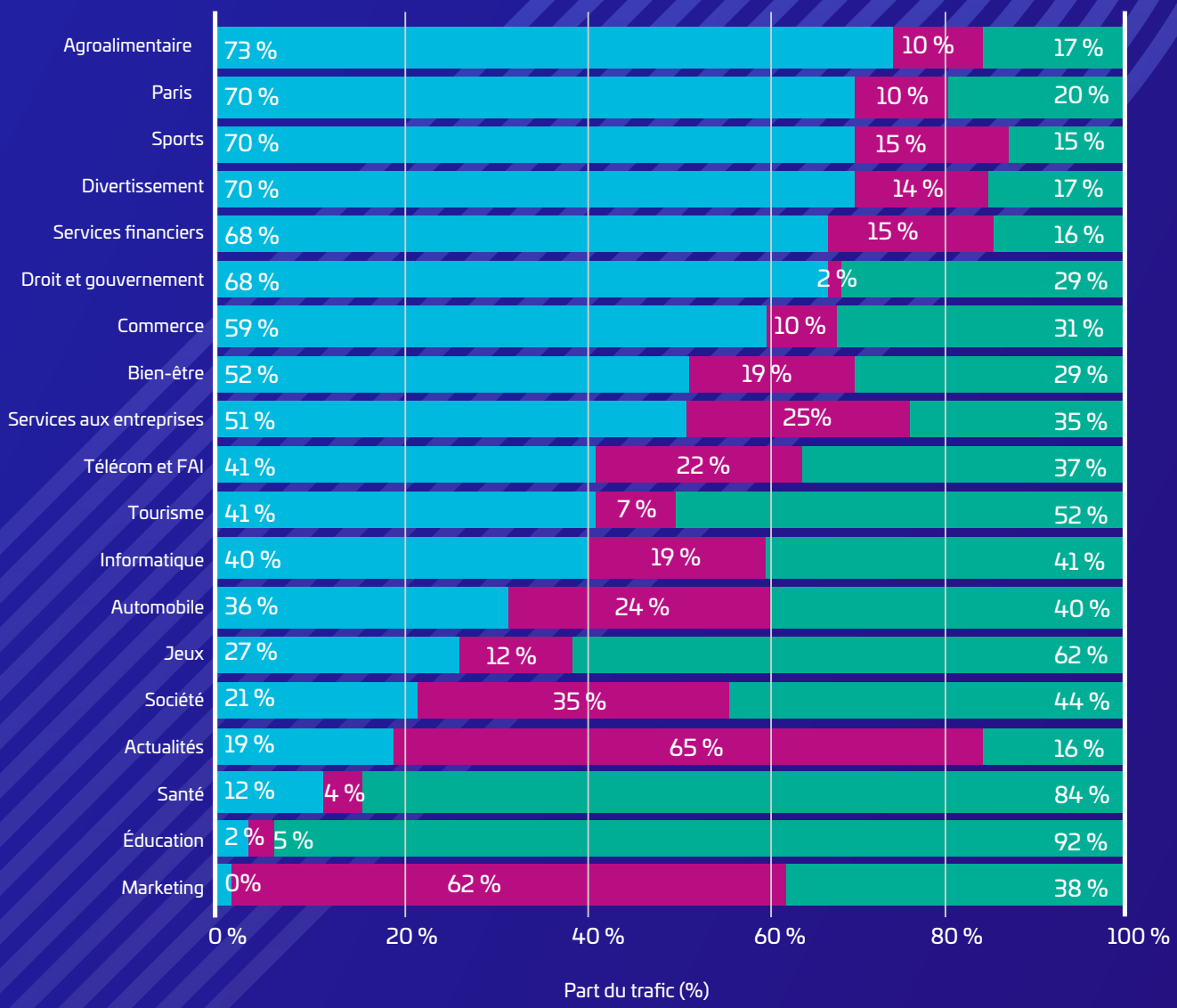
Profil du trafic par secteur en 2024



Niveau de sophistication des bots par secteur

Le graphique précédent présentait le taux de bad bots par secteur, mais cela ne suffit pas à rendre compte du risque. Prenons un exemple : 31 % du trafic dans le secteur de l'agroalimentaire provient de bad bots. Le graphique suivant révèle que 73 % des attaques de bots dans ce secteur sont menées par des bots avancés. En 2023, la part des bots avancés dans ce secteur était de 50 %. Cette progression témoigne de la complexification du problème. Les cyberattaques ciblant les enseignes alimentaires passent notamment par des fraudes aux cartes cadeaux et par l'achat massif de stocks.

Degré de sophistication des bots par secteur en 2024



Les bots et l'industrie du tourisme

En 2024, le secteur du voyage est devenu la cible la plus prisée des attaques de bots, avec 27 % de l'ensemble des attaques, contre 21 % en 2023, soit une hausse de 6 %. Deux changements marquent l'année 2024 : la baisse des attaques de bots sophistiqués visant ce secteur (41 %, contre 61 % en 2023) et la forte augmentation des attaques de bots simples (52 %, contre 34 %). Cette évolution montre que les outils d'automatisation assistés par l'IA ont facilité l'accès à la cybercriminalité : des hackers moins expérimentés ont ainsi pu lancer des attaques plus basiques. Plutôt que de miser uniquement sur des techniques avancées, les cybercriminels déploient désormais de grands volumes de bots élémentaires pour submerger les sites de voyages, rendant les attaques plus fréquentes et plus étendues.

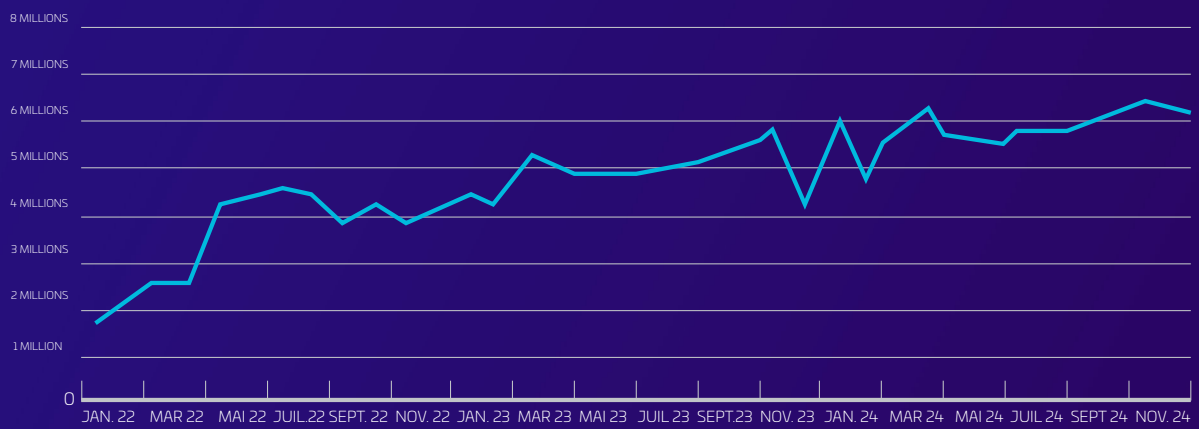
Principales menaces pour l'industrie du tourisme

Les compagnies aériennes, notamment, doivent faire face à de nombreuses menaces automatisées qui perturbent leur activité et impactent leurs revenus :

- **Les bots « Seat Spinning »** simulent la réservation jusqu'à l'étape du paiement, bloquant des billets sans jamais finaliser l'achat, privant les véritables clients de leur accès à ces billets et les poussant à chercher ailleurs.
- **Déséquilibre du ratio consultation/réservation :** un trafic excessif de bots gonfle artificiellement ce ratio, faussant l'évaluation de la demande et des tarifs, ce qui désavantage les compagnies aériennes face à la concurrence.
- **Extraction non autorisée de données :** les concurrents et fraudeurs collectent massivement des tarifs, ce qui perturbe les stratégies de tarification et la gestion des revenus.
- **Fraude aux programmes de fidélité :** Les bots de fraude aux programmes de fidélité mènent des attaques de credential stuffing pour s'emparer de comptes clients et utiliser les points ou avantages volés.
- **Scalping de billets :** les cybercriminels utilisent des bots pour réserver en masse des billets sur des vols très demandés, qu'ils revendent ensuite à des prix majorés.

Le graphique ci-dessous montre la hausse du nombre d'attaques de bots ciblant le secteur du tourisme au cours des 3 dernières années, avec une augmentation de 280 % entre janvier 2022 et décembre 2024, révélant la vulnérabilité croissante du secteur.

Croissance fulgurante des attaques de bots ciblant le secteur du tourisme



Les bad bots, un cauchemar pour le commerce

Les cybercriminels n'attendent plus la saison des achats de fin d'année

En 2024, le commerce de détail est resté le deuxième secteur le plus ciblé, totalisant 15 % de l'ensemble des attaques de bots. Les bots malveillants représentent désormais 33 % du trafic sur les sites marchands, contre 26 % en 2023. La hausse des attaques sophistiquées (59 %, contre 52 % l'année précédente) témoigne d'un raffinement croissant des méthodes employées, tandis que les attaques simples (31 %) et intermédiaires (10 %) reculent légèrement.

Les détaillants sont confrontés à de nombreuses menaces : scalping, credential stuffing, fraude aux cartes cadeaux, aspiration de prix (price scraping) ou encore attaques DDoS. Ces attaques atteignent leur pic pendant les périodes de forte activité commerciale, comme les soldes ou les fêtes de fin d'année. Elles perturbent les opérations, entraînent des pertes de chiffre d'affaires, une érosion de la confiance client et une hausse des coûts d'infrastructure.

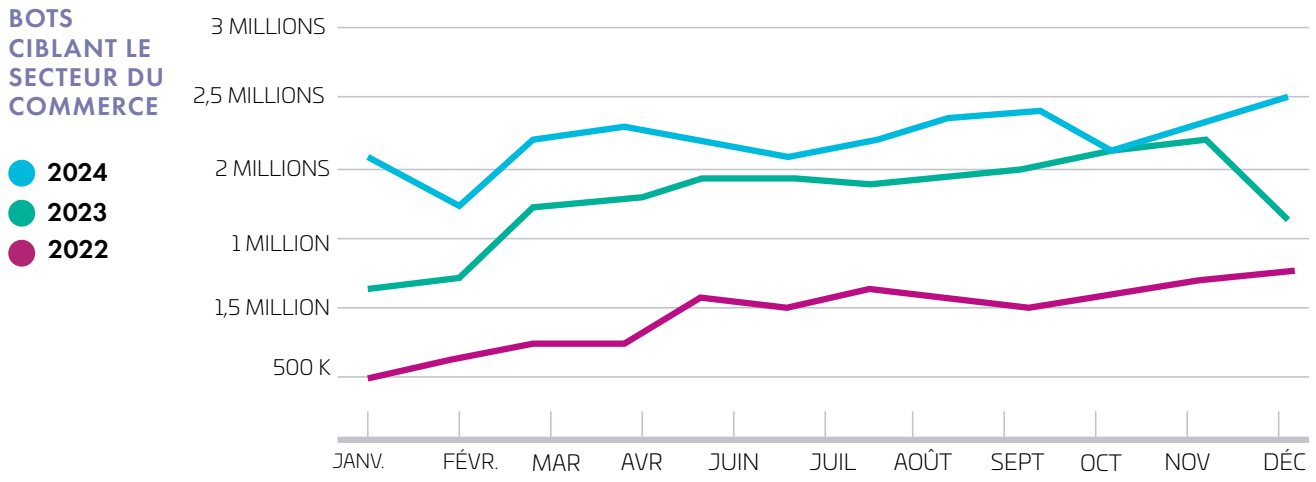
Les campagnes promotionnelles et les lancements de produits attirent les cybercriminels et donnent lieu à des pics d'activité des bots. Cela provoque des ruptures de stock artificielles et faussent les niveaux de disponibilité affichés. Résultat : l'expérience d'achat se dégrade et les clients légitimes peinent à finaliser leurs commandes.

Selon l'équipe Imperva Security Analyst Services, le trafic des bots peut être multiplié par deux à trois fois lors des grands événements commerciaux, ce qui accentue la pression sur les infrastructures et les équipes opérationnelles. Certains bots d'abandon de panier ajoutent massivement des articles sans jamais valider l'achat, créant une fausse pénurie et perturbant la gestion des stocks et les prévisions de la demande.

Tendances des attaques de bots dans le secteur du commerce

Le graphique ci-dessous illustre l'évolution des attaques de bots contre le secteur du commerce de détail au cours des trois dernières années. En 2022 et 2023, ces attaques ont connu une hausse entre mars et avril, puis une progression régulière jusqu'en novembre, le mois qui marque le début des grandes périodes d'achats en ligne comme le Black Friday et le Cyber Monday.

En 2024, toutefois, le schéma a changé. Le trafic de bots a enregistré un premier pic autour d'avril, puis un second en septembre, avant de repartir à la hausse à l'approche de la fin d'année. Ce changement suggère que les bots ne se concentrent plus uniquement sur la saison des achats de fin d'année : ils ciblent désormais les enseignes tout au long de l'année, au gré des opportunités.



Cette évolution pourrait également être liée aux outils d'automatisation pilotés par l'intelligence artificielle, qui rendent les attaques plus accessibles et permettent aux cybercriminels d'agir plus fréquemment et de manière plus opportuniste, sans attendre les pics commerciaux traditionnels.

Focus sur le secteur aérien

Indicateurs de conversion faussés : le cauchemar des compagnies aériennes

Les compagnies aériennes font face à un problème bien connu, mais de plus en plus préoccupant : la manipulation du taux de conversion recherche/réservation (look-to-book ratio), un indicateur clé qui mesure le rapport entre les recherches de vols et les billets effectivement achetés.

Les bots de scraping en sont la cause principale. En multipliant les requêtes automatiques sans finaliser de réservation, ils gonflent artificiellement le volume de recherche. Résultat : les prévisions de demande deviennent erronées, les modèles de tarification dynamique se dérèglent et les coûts opérationnels augmentent.

Ce phénomène, appelé fraude au look-to-book, touche aujourd'hui les compagnies aériennes du monde entier. Et pourtant, il est encore souvent perçu comme un problème opérationnel plutôt que comme une véritable menace de sécurité.

En mettant en place des systèmes avancés de détection et de contrôle des bots, ainsi qu'une surveillance continue du trafic, les compagnies aériennes peuvent rétablir la fiabilité des modèles tarifaires, réduire la charge sur les infrastructures informatiques et protéger leurs revenus.

Ignorer les bad bots revient à se placer en situation de désavantage concurrentiel, surtout lorsque certaines entreprises utilisent elles-mêmes ces bots pour aspirer les tarifs et proposer des prix inférieurs.

> « Les bots adorent fausser les données de tarification et les indicateurs marketing ! »

Si vous ne maîtrisez pas le trafic de votre site, quelqu'un d'autre le fera à votre place.

Qu'est-ce qu'un bot ?

Un bot est un programme informatique automatisé qui effectue différentes tâches en ligne. Il existe des bots utiles, comme ceux des moteurs de recherche, qui répertorient le contenu, et des bots nuisibles, utilisés à des fins malveillantes.

Qu'est-ce qu'un bad bot ?

Les bad bots, ou bots malveillants, sont des programmes automatisés créés pour accomplir des actions nuisibles, comme l'extraction de données, l'envoi de spams ou la réalisation d'attaques par déni de service. Ils peuvent imiter le comportement humain, ce qui les rend difficiles à repérer et à bloquer.

ÉTUDE DE CAS

Fraude marketing

Les bad bots perturbent une campagne marketing mondiale

Une grande agence mondiale de recrutement faisait face à un problème majeur dans ses campagnes de marketing digital. Malgré des investissements considérables (plusieurs centaines de milliers de dollars en annonces, publicités ciblées et actions sur les réseaux sociaux), les retombées restaient quasi nulles. Les outils d'analyse affichaient un trafic très élevé sur le site, mais les résultats ne suivaient pas.

Une analyse approfondie menée par Imperva a révélé l'origine du problème : 83 % du trafic provenait de bots malveillants. Ce trafic artificiel faussait complètement les données, rendant impossible toute évaluation fiable de la performance des campagnes. Le volume d'activité automatisée, notamment sur les recherches et publications d'offres d'emploi, figurait parmi les plus élevés du secteur (où la moyenne observée était de 53 %).

Ainsi, les bots sabotaient les campagnes marketing, détournaient les ressources publicitaires et produisaient des indicateurs trompeurs.

En moins de quatre jours, la solution Advanced Bot Protection (ABP) d'Imperva a permis de bloquer intégralement le trafic frauduleux. L'agence a ainsi pu reprendre le contrôle de ses données et retrouver la fiabilité de ses analyses. Les bots ont tenté de s'adapter mais la solution d'Imperva est restée particulièrement efficace : elle a supprimé 100 % du trafic automatisé, sécurisé le contenu et rétabli la valeur réelle des campagnes marketing.

Résultat : l'agence a constaté une amélioration nette de son retour sur investissement (ROI) et dispose désormais d'indicateurs fiables pour piloter ses futures stratégies.

> « Les bots malveillants ruinent les efforts marketing et plombent le ROI »

Recommandations

Les entreprises doivent désormais prendre des mesures concrètes pour se protéger des bots et des fraudes en ligne. Chaque site présente ses propres vulnérabilités et ses points d'entrée potentiels, ce qui rend difficile la mise en place d'une solution unique et universelle. En revanche, une approche proactive, combinant plusieurs dispositifs de sécurité, permet de réduire considérablement les risques. Elle doit notamment recourir à des outils avancés de détection de bots et à des solutions de cybersécurité efficaces. Ensemble, ces systèmes constituent une défense solide et adaptable face aux cybermenaces en constante évolution.

Les API représentent aujourd'hui une surface d'attaque critique dans les infrastructures numériques modernes. Elles sont régulièrement la cible d'attaques par credential stuffing, aspiration de données (data scraping) ou exploitation automatisée. Vous trouverez ci-dessous des recommandations spécifiques à la sécurisation des API.

1. Identification des risques

Pour bloquer les bad bots, la première étape consiste à identifier les risques potentiels :

A. Les campagnes marketing et e-commerce attirent inévitablement une hausse du trafic automatisé, surtout lors du lancement de produits très attendus en quantité limitée (baskets en édition spéciale, consoles de nouvelle génération, objets de collection, etc.). L'annonce d'une date de mise en vente agit comme un signal d'alerte pour les bots, qui cherchent à accaparer les stocks avant les véritables clients, faussant ainsi les ventes et nuisant à l'image de la marque. Pour éviter cela, il est essentiel de renforcer la sécurité du site et de distinguer le trafic légitime de l'activité automatisée. Le recours à une analyse fine du trafic, à des mécanismes de détection en temps réel et à des protocoles d'authentification robustes permet de garantir un accès équitable pour les acheteurs réels, tout en protégeant l'intégrité du lancement.

B. Une gestion efficace des bots commence par l'identification des fonctionnalités à risque sur votre site ou vos applications. Certaines pages attirent particulièrement les activités malveillantes. Par exemple, les espaces de connexion sont la cible d'attaques de type credential stuffing ou credential cracking, où les cybercriminels utilisent des identifiants volés pour accéder à des comptes. Les formulaires de paiement, quant à eux, exposent les entreprises aux fraudes à la carte bancaire (carding, card cracking). Les cartes cadeaux ou bons promotionnels peuvent, eux aussi, être exploités pour commettre des fraudes automatisées.

Pour réduire ces risques, il convient d'activer l'authentification multifactorielle (MFA), de déployer des CAPTCHA adaptatifs, d'assurer une surveillance continue des activités suspectes, et de recourir à des systèmes de détection pilotés par l'IA, capables d'identifier les comportements anormaux en temps réel. Les mécanismes de limitation dynamique du trafic (rate limiting) se révèlent également efficaces pour neutraliser les bots qui tentent de contourner les défenses classiques.

C. Il est aussi essentiel d'identifier les éléments les plus exposés (pages de connexion, tunnels d'achat, API) et d'y appliquer des mesures de protection ciblées : limitation du nombre de requêtes, surveillance des adresses IP à fort volume et sécurisation de l'ensemble de la hiérarchie des pages et services concernés. Les API constituent une surface d'attaque particulièrement convoitée. Elles sont souvent visées par des attaques automatisées de credential stuffing ou de data scraping. Pour les protéger efficacement, il est essentiel de mettre en œuvre une authentification renforcée, une limitation spécifique du trafic API, et des systèmes de détection d'anomalies capables de repérer les accès non autorisés ou abusifs.

2. Réduction des vulnérabilités

Les API et les applications mobiles constituent souvent des portes d'entrée vers des données sensibles. Mettre en œuvre des mesures de protection cohérentes sur toutes les plateformes et bloquer les flux suspects entre systèmes permet de réduire les vulnérabilités et de garantir une défense unifiée contre les accès non autorisés. La sécurisation des API et des applications mobiles est tout aussi essentielle que celle des sites web. Il est en effet nécessaire d'adopter une stratégie de cybersécurité globale, couvrant l'ensemble des points de contact numériques.

La sécurité des API doit s'appuyer sur les bonnes pratiques d'authentification et sur des contrôles d'accès stricts, afin d'éviter les abus liés aux jetons (tokens) et le data scraping non autorisé. En complément, des mécanismes de défense multicouches, tels que les systèmes de preuve de travail (proof of work) ou les stratégies de ralentissement contrôlé (tarpit), permettent de freiner les bots sans nuire à la fluidité de l'expérience utilisateur.

3. Réduction des menaces : chaînes d'identification

De nombreux outils et scripts de bots utilisent encore des chaînes d'identification (user-agent) associées à des versions obsolètes de navigateurs. À l'inverse, les utilisateurs humains mettent automatiquement leurs navigateurs à jour vers les versions les plus récentes. Il est donc recommandé de bloquer les versions de navigateurs obsolètes, afin de limiter le trafic automatisé et de renforcer la fiabilité des accès.

	BLOCAGE Fin de vie depuis plus de trois ans	**CAPTCHA Fin de vie depuis plus de deux ans**
VERSION DE CHROME	<100	<110
VERSION DE FIREFOX	<95	<105
VERSION DE SAFARI	<13	<14
VERSION D'INTERNET EXPLORER	<11	<13

Il est aussi essentiel d'imposer des règles d'accès claires, par exemple en limitant les régions géographiques autorisées, les types de requêtes ou les versions d'application acceptées, afin d'empêcher les abus provenant de sources de trafic douteuses ou dépassées.

4. Réduction des menaces : Proxies

Les cybercriminels recourent de plus en plus aux proxies pour permettre à leurs bots malveillants d'imiter le comportement d'utilisateurs légitimes. Grâce à la rotation d'adresses IP via des services spécialisés, ils parviennent à dissimuler leur véritable origine et à contourner les mécanismes de détection. Pour contrer cette menace, il est essentiel de restreindre l'accès depuis les centres de données qui fournissent massivement des adresses IP. Cette mesure réduit significativement les risques d'infiltration liés au trafic de bots. Plusieurs grands fournisseurs sont concernés, parmi lesquels Host Europe GmbH, Dedibox SAS, Digital Ocean, OVH SAS ou encore Choopa LLC. La mise en place de contrôles d'accès et la surveillance du trafic en provenance de ces acteurs permettent de renforcer la sécurité, en détectant et en bloquant de manière proactive le trafic généré par les bots.

5. Réduction des menaces : Automatisation

Des outils comme Puppeteer, Selenium ou WebDriver sont de plus en plus souvent détournés pour simuler des comportements humains en ligne. Ces programmes permettent d'automatiser la création de comptes, l'extraction de données ou d'autres actions malveillantes à grande échelle. Pour contrer ces abus, il est essentiel de repérer les signes d'activité automatisée comme des vitesses d'exécution anormales, une navigation répétitive ou des interactions trop régulières. Cette approche permet de détecter et bloquer les attaques automatisées sans perturber l'expérience des véritables utilisateurs.

Les API sont particulièrement vulnérables : les cybercriminels y ont recours pour exploiter directement les points d'accès via des navigateurs sans interface ou des scripts automatisés. Une surveillance ciblée du trafic API peut donc aider à distinguer les requêtes légitimes du trafic malveillant.

Enfin, il est essentiel de neutraliser en priorité les bots les plus simples, tels que les outils d'automatisation ou les navigateurs headless, afin de réduire rapidement la charge d'attaques et d'alléger la pression sur les systèmes de détection.

6. Évaluation du trafic – détection générale des bots et établissement d'un trafic de référence

Identifier les bots reste difficile, mais certains indices caractéristiques permettent souvent de les repérer. Un taux de rebond élevé, un faible taux de conversion ou des pics soudains et inexpliqués de trafic sur une même URL sont autant de signaux pouvant indiquer une activité non humaine. En surveillant ces anomalies, les organisations peuvent détecter rapidement un trafic suspect, l'analyser et mettre en place les mesures adaptées pour limiter son impact.

Il est recommandé de définir les comportements de trafic normalement attendus, puis de guetter toute déviation inhabituelle pouvant révéler une activité automatisée. Une hausse soudaine du trafic vers un point d'accès précis peut, par exemple, signaler une attaque ciblée sur un événement ou une opération spécifique. Dans ce cas, il convient d'analyser l'origine du trafic pour en déterminer la cause.

Certains phénomènes doivent attirer l'attention : un volume anormalement élevé de requêtes provenant d'une même adresse IP, d'un fournisseur d'accès unique ou d'une URL spécifique constitue par exemple un indice fort d'accès automatisé. Ces informations sont essentielles pour déployer des contre-mesures ciblées et protéger efficacement les actifs numériques contre les attaques de bots.

7. Surveillance du trafic API en temps réel

Définissez d'abord un seuil de référence pour les tentatives de connexion échouées sur vos pages de login, puis surveillez toute anomalie ou pic d'activité. Configurez des alertes automatiques afin d'être immédiatement averti en cas d'écart. Les attaques dites « low and slow » (discrètes et étalées dans le temps) ne déclenchent généralement pas d'alerte au niveau de l'utilisateur ou de la session : il est donc essentiel de définir des seuils globaux pour détecter ces comportements.

Sur les pages de paiement ou de validation de cartes cadeaux, une augmentation du nombre d'échecs, voire du trafic global, peut révéler une attaque de type carding, ou la présence de bots comme GiftGhostBot cherchant à dérober des soldes de cartes.

Les entreprises doivent aussi surveiller en continu l'activité de leurs API : la fréquence des requêtes, l'apparition de pics soudains et les comportements d'accès inhabituels peuvent révéler une automatisation malveillante.

8. Sensibilisation et authentification multifactorielle (MFA)

Il est essentiel de rester vigilant face aux fuites et violations de données. Les cybercriminels peuvent aujourd'hui se procurer très facilement des identifiants compromis issus de ces fuites et louer des infrastructures de bots pour automatiser leurs attaques. Les menaces deviennent de ce fait particulièrement difficiles à contenir. Des identifiants récemment volés sont souvent utilisés pour lancer des attaques de credential stuffing ou de prise de contrôle de comptes (Account Takeover), les mots de passe étant généralement encore valides au moment de leur exploitation. Pour réduire ce risque, il est crucial de monitorer les violations de données connues. Cette veille permet de renforcer les défenses proactives et de contrer les cybercriminels. La mise en place d'une authentification multifactorielle (MFA) constitue par ailleurs un rempart essentiel contre les accès non autorisés. Elle doit être appliquée non seulement aux connexions, mais aussi aux paiements et aux réinitialisations de mot de passe, afin d'ajouter un niveau de sécurité supplémentaire.

Enfin, du côté des API, l'adoption de mécanismes d'authentification renforcés contribue à limiter les risques de credential stuffing et d'abus de tokens, deux techniques couramment utilisées dans ce type d'attaque.

9. Évaluation des solutions de protection contre les bots

Face à toutes ces évolutions, les solutions de protection en place doivent être évaluées. Les mesures simples qui suffisaient autrefois à bloquer les bots malveillants ne sont plus efficaces aujourd'hui. Les données présentées dans ce rapport montrent à quel point la sophistication et la capacité d'adaptation des bots actuels ont atteint un niveau inédit. Leur facilité d'utilisation et leur efficacité redoutable en font désormais un outil privilégié des cybercriminels. Ils évoluent rapidement et imitent de plus en plus fidèlement le comportement humain, ce qui complique considérablement leur identification et leur neutralisation. Dans un tel contexte, tenter de contrer ces menaces sans assistance spécialisée relève presque de l'impossible.

Il devient désormais capital d'opter pour une stratégie évolutive de défense : les organisations doivent non seulement identifier les bots malveillants, mais aussi les distinguer des bots légitimes dans des environnements de plus en plus complexes.

Cette situation appelle à une solution complète de protection contre les bots, avec une approche de défense multiniveaux combinant l'analyse du comportement des utilisateurs, le profilage et le fingerprinting. L'intégration d'outils fondés sur l'intelligence artificielle (IA) et l'apprentissage automatique (ML) est également essentielle pour améliorer la précision de la détection et adapter en continu les défenses.

En maintenant une vigilance permanente, en réalisant des audits réguliers et en renforçant l'intégration de l'IA et du ML, les organisations peuvent protéger de manière proactive leurs actifs critiques tout en réduisant les faux positifs et faux négatifs. Une telle approche exige cependant une expertise dédiée, capable de faire évoluer les mécanismes de défense en rythme avec l'émergence des menaces.

10. Ne dévoilez pas toute votre stratégie d'un coup

En déployant simultanément l'ensemble de votre stratégie de mitigation sur toute la plateforme, vous risquez, paradoxalement, de révéler la structure complète de vos défenses. Les cybercriminels risquent alors de prendre le temps d'analyser vos mesures de protection, pour mieux les contourner.
Mieux vaut adopter une approche ciblée et adaptative. Certaines mesures doivent être réservées aux moments spécifiques, comme par exemple lors d'un lancement de produit, d'une grande opération commerciale ou d'une période de forte affluence, c'est-à-dire lorsque l'activité des bots atteint généralement son pic. Une fois l'événement terminé, ces dispositifs peuvent être désactivés ou ajustés pour éviter que les cybercriminels n'en étudient le fonctionnement. Du côté des API, les organisations doivent veiller à moduler dynamiquement les seuils de limitation de requêtes, les contrôles d'accès et les mécanismes de détection des bots. Ces variables doivent pouvoir s'adapter au trafic et au niveau de risque. En considérant la protection contre les bots non pas comme un ensemble figé de règles, mais comme une stratégie en constante évolution, les organisations peuvent garder une longueur d'avance dans la lutte contre les menaces automatisées.

Annexe

Définitions

Qu'est-ce qu'un bot ?

Sur internet, un bot désigne un programme informatique capable d'exécuter automatiquement différentes tâches. Ces tâches peuvent aller de la simple saisie d'un formulaire à des opérations plus avancées, comme l'extraction de données d'un site web.

Qu'est-ce qu'un bot malveillant ou « bad bot » ?

Les mauvais bots sont des logiciels qui accomplissent des actions automatisées à des fins nuisibles. Ils peuvent, par exemple, collecter illégalement des données sur des sites web pour les réutiliser ou pour en tirer un avantage concurrentiel. Ils servent souvent à l'achat massif d'articles rares pour les revendre plus cher (scalping). Ils peuvent aussi être utilisés pour lancer des attaques par déni de service distribué (DDoS) contre des applications. Certains bad bots commettent même des actes délictueux (fraudes, vols). Par exemple, les bots spécialisés dans le credential stuffing figurent parmi les attaques les plus répandues. Le projet Open Web Application Security Project (OWASP) recense 21 attaques de bots dans son guide Automated Threat Handbook1.

Quelle est la différence entre bot malveillant et bot légitime ?

Les bots présents sur internet ne sont pas tous nuisibles. Certains remplissent des fonctions utiles, comme l'indexation des sites web pour les moteurs de recherche ou la surveillance des performances d'un site. Googlebot et Bingbot, par exemple, sont des robots d'exploration qui contribuent à actualiser un index consultable des pages web. En indexant ces pages, ces bots aident les internautes à trouver facilement les sites web les plus pertinents pour leurs recherches. Ces bots jouent un rôle clé pour les entreprises en ligne, car ils permettent aux clients potentiels de repérer et d'accéder aisément à leurs sites, produits et services.

Même les bots « bienveillants » peuvent poser problème

Les bots légitimes peuvent fausser considérablement les rapports d'analyse web en rendant certaines pages artificiellement populaires. Par exemple, un bot utile peut générer une impression sur une page que vous mettez en avant, sans que cela ne débouche sur un véritable parcours d'achat. Cette situation peut nuire aux performances des annonceurs, fausser les analyses marketing et conduire à de mauvaises décisions commerciales. Il est donc essentiel de distinguer avec précision le trafic issu des utilisateurs humains, des bots utiles et des bad bots, pour prendre des décisions éclairées.

Qu'est-ce qu'un bot boosté par l'IA ?

Un bot boosté par l'intelligence artificielle utilise l'apprentissage automatique et l'IA pour imiter les comportements humains. Il peut s'adapter et affiner ses stratégies au fil du temps. Il peut analyser des données, apprendre lors des interactions et contourner les méthodes de détection classiques en se faisant passer pour de véritables utilisateurs.

Qu'est-ce qu'un bot polymorphe ?

Un bot polymorphe est conçu pour modifier en permanence son apparence et son comportement afin de passer inaperçu, par exemple en changeant régulièrement son code, son user-agent ou son adresse IP. Cette capacité à se transformer lui permet de déjouer les mesures de sécurité en imitant différents types de trafic légitime.

Classification des bots malveillants

Imperva a mis en place le système de classification suivant qui répartit les bots malveillants selon leur niveau de sophistication :

- **Basique** - Ces bots se connectent depuis une seule adresse IP attribuée par un fournisseur d'accès. Ils visitent les sites grâce à des scripts automatisés. Ces bots ne se font pas passer pour des navigateurs.

- **Intermédiaire** - Ces bots utilisent des navigateurs sans interface (headless browsers) capables de simuler le comportement d'un véritable navigateur web, y compris l'exécution de JavaScript. Ils sont donc plus difficiles à repérer que les scripts basiques, car ils se comportent comme de réels visiteurs.

- **Avancé** - Ces bots, les plus évolués, reproduisent le comportement humain, comme les mouvements de souris et les clics, pour tromper les systèmes de détection. Ils utilisent des outils d'automatisation du navigateur ou des malwares intégrés dans de véritables navigateurs pour accéder aux sites.

- **Furtif** - Les cybercriminels qui opèrent des bots sophistiqués font preuve d'une grande persévérance. Si une solution anti-bots les bloque, ils peuvent chercher à comprendre comment et revenir ensuite avec une nouvelle méthode capable de contourner la technique de détection utilisée. Ces cybercriminels utilisent des bots avancés de plus en plus difficiles à repérer. Ils combinent souvent des stratégies intermédiaires et avancées.
  Les bots furtifs mettent en œuvre des tactiques complexes : rotation d'adresses IP aléatoires, utilisation de proxies anonymes ou résidentiels, changement d'identité, imitation du comportement humain, temporisation des requêtes ou contournement des CAPTCHA. Ils adoptent une approche dite « lente et discrète » : elle leur permet d'éviter d'être repérés tout en menant des attaques de grande ampleur avec un nombre limité de requêtes. Ce mode opératoire rend leur détection beaucoup plus difficile et leur permet de mener des attaques significatives tout en passant inaperçus.

Usage des bots malveillants

PROBLÈME	DE QUOI S'AGIT-IL ?	IMPACT SUR L'ENTREPRISE	SYMPTÔMES	SECTEURS CIBLÉS
Extraction de prix	Utilisation de bots pour surveiller et collecter illégalement les tarifs, souvent dans le but de proposer des prix plus bas que la concurrence	Perte de ventes au profit de concurrents qui aspirent vos données tarifaires (price scraping), ajustent leurs prix à la baisse et prennent l'avantage sur le marché. Atteinte à la réputation lorsque les données extraites sont réutilisées de manière trompeuse Diminution de la valeur à vie des clients Performances du site web impactées	Baisse du taux de conversion, recul du référencement SEO, ralentissements et interruptions inexpliquées du site (généralement à cause de scrapers trop agressifs)	Toutes les entreprises affichant des tarifs : • Commerce de détail • Jeux vidéo • Compagnies aériennes • Tourisme
Extraction de contenu	Utilisation de bots pour collecter des contenus et des données sur un site web	Perte de revenus liée à la republication non autorisée de vos contenus ou de vos données sur d'autres sites, entraînant une baisse du trafic vers votre site d'origine et une diminution des ventes de vos produits ou services. Contenu dupliqué, qui détériore le référencement naturel (SEO) de votre site. Atteinte à la réputation de la marque.	Votre contenu se retrouve sur d'autres sites, recul du référencement SEO, ralentissements, interruptions inexpliquées du site (généralement à cause de scrapers trop agressifs)	Similaire à la collecte de prix, mais concerne aussi : • Sites d'emploi • Petites annonces • Places de marché • Finance • Billetterie
Prise de contrôle de compte (Account Takeover), aussi appelée Credential Stuffing ou Credential Cracking	Utilisation de bots pour obtenir illégalement l'accès aux comptes d'utilisateurs : techniques de connexion forcée : credential stuffing (réutilisation automatisée d'identifiants volés) ou credential cracking (essais multiples pour deviner des identifiants valides).	Atteinte à la réputation et à la fidélité client, couverture médiatique négative. Frustration des utilisateurs confrontés à des blocages de compte, des vols de données ou des transactions frauduleuses. Dégradation des performances et de la fiabilité du site web lors d'attaques massives. Risque de non-conformité aux réglementations sur la protection des données (RGPD, etc.). Hausse des coûts liés à l'assistance client et à la gestion des fraudes.	Augmentation du taux d'échecs de connexion. Multiplication des blocages de comptes et des demandes d'assistance. Hausse des fraudes : vols de points de fidélité, détournement de cartes bancaires, achats non autorisés. Augmentation du nombre de rétrocessions de paiement (chargebacks).	Toute entreprise proposant une page de connexion
Création frauduleuse de comptes (aussi appelée agrégation de comptes)	Utilisation des bots pour automatiser la création massive de comptes à des fins diverses : fraude, diffusion de contenus indésirables (spam), manipulation d'opinions ou propagation de messages de propagande.	Perte de crédibilité du site envahi par des comptes automatisés diffusant du spam ou amplifiant artificiellement certains messages. Pertes financières liées aux bots qui détournent les crédits de bienvenue ou les offres promotionnelles (somme d'argent, points, essais gratuits, etc.). Statistiques gonflées par les bots : mesures de performance faussées, orientant les décisions dans la mauvaise direction.	Hausse anormale du nombre de nouveaux comptes créés. Augmentation du volume de commentaires ou messages indésirables. Baisse du taux de conversion des nouveaux comptes en utilisateurs payants.	Plateformes de messagerie • Réseaux sociaux • Sites de rencontres • Communautés Abus des promotions aux nouveaux inscrits : • Jeux en ligne • Secteur financier

PROBLÈME	DE QUOI S'AGIT-IL ?	IMPACT SUR L'ENTREPRISE	SYMPTÔMES	SECTEURS CIBLÉS
Fraude à la carte bancaire (appelée aussi Carding, Card Cracking)	Recours à des bots pour vérifier massivement la validité de numéros de cartes bancaires volées ou deviner les informations manquantes (CVV, date d'expiration, etc.)	Pertes financières (remboursements coûteux), perte de chiffre d'affaires due à la baisse de confiance des consommateurs. Atteinte à la réputation de la marque. Dégradation du score de risque de fraude de l'entreprise. Hausse des coûts du service client (réclamations) Non-conformité aux réglementations (RGPD, etc.).	Augmentation des fraudes par carte bancaire Hausse des appels au service client Augmentation du nombre de rétrofacturations traitées	Toute plateforme acceptant les paiements : • Commerce • Associations/ONG • Compagnies aériennes • Tourisme • Billetterie • Finance • Jeux
Attaque par déni de service	Utilisation de bots pour saturer un site web de requêtes : épuisement des ressources (système de fichiers), mémoire, processus, threads, CPU et même les ressources humaines ou financières	Ralentissement du site, avec risques de coupure ou d'indisponibilité Perte de chiffre d'affaires due à l'inaccessibilité du site Image de marque dégradée Risque de perte de clients	Pics de trafic inhabituels et inexpliqués sur certaines ressources (connexion, inscription, pages produits, etc.) Hausse des réclamations au service client	Tous les secteurs d'activité
Vérification et abus de solde sur cartes cadeaux	Automatisation : utilisation de bots pour tester et repérer les numéros de cartes cadeaux sur les pages de vérification de solde, afin de dérober les fonds disponibles	Comme pour la fraude bancaire, la fraude sur les cartes cadeaux entraîne des pertes financières liées au vol de fonds par des bots. Augmentation des coûts du service client pour traiter les litiges Réputation affectée et baisse des ventes futures Image de marque détériorée	Pics d'accès à la page de consultation des soldes de cartes-cadeaux Hausse des appels au service client concernant la perte de soldes	Toute entreprise proposant les cartes-cadeaux comme moyen de paiement, principalement dans le commerce de détail
Indisponibilité artificielle des stocks	Utilisation de bots pour garder des articles dans les paniers sans jamais finaliser l'achat, empêchant ainsi les vrais clients d'y accéder	Perte de revenus liée aux articles non vendus, bloqués dans les paniers d'achat par des bots. Baisse des taux de conversion. Hausse du taux d'abandon de panier. Atteinte à l'image de l'entreprise lorsque des intermédiaires peu scrupuleux accaparent les stocks pour les revendre ailleurs à un prix supérieur.	Augmentation du nombre d'articles abandonnés dans les paniers Baisse du taux de conversion Hausse des réclamations sur l'indisponibilité des stocks	Entreprises proposant des articles rares ou à durée limitée : • Compagnies aériennes • Billetterie • Commerce de détail • Santé

Usage des bad bots

PROBLÈME	DE QUOI S'AGIT-IL ?	IMPACT SUR L'ENTREPRISE	SYMPTÔMES	SECTEURS CIBLÉS
Scalping	Utilisation de bots pour obtenir un avantage injuste sur les vrais clients et acquérir des produits ou services rares ou convoités	Réputation dégradée. Ralentissement du site pouvant entraîner des interruptions ou des pannes et une perte de chiffre d'affaires. Valeur vie client (LTV) réduite, car un bot ne revient pas régulièrement pour de nouveaux achats. Panier moyen (ABV) plus faible, les bots ciblant un seul produit alors que les clients légitimes achètent plusieurs articles.	Ralentissements et indisponibilités du site sans explication (souvent à cause de bots de scalping agressifs) Baisse du taux de conversion Hausse des plaintes des clients concernant des ruptures de stock	Comparable à une indisponibilité artificielle des stocks : • Transport aérien • Billetterie • Commerce de détail (ex. : baskets, consoles, matériel informatique, éditions limitées) • Secteur de la santé
Réservation de sièges sans achat	Les bots bloquent des sièges sans paiement, parfois jusqu'à 24 heures	Perte de chiffre d'affaires liée aux sièges invendus Image de marque ternie car les vrais clients ne peuvent pas réserver les vols qu'ils souhaitent	À l'approche du départ, des vols affichés complets révèlent soudain de plus en plus de sièges libres	Compagnies aériennes

Mauvais bots par secteur d'activité

SECTEUR D'ACTIVITÉ	QUELS TYPES D'ENTREPRISES SONT CONCERNÉS ?	QUE FONT LES MAUVAIS BOTS ?
Automobile	Location de voitures, constructeurs, concessionnaires, plateformes de vente de véhicules	Extraction de prix, collecte de données, inventaire
Services aux entreprises	Immobilier, prestataires/plateformes de distribution, systèmes CRM, indicateurs de performance	Attaques ciblant les API, collectes de données, prises de contrôle de comptes
Informatique	Services informatiques, fournisseurs IT, entreprises et prestataires technologiques	Usurpation de compte, collecte de données
Éducation	Plateformes d'apprentissage en ligne, établissements scolaires, universités, grandes écoles	Usurpation de compte étudiant ou enseignant, vérification de disponibilité des cours, extraction de données et de publications scientifiques exclusives
Divertissement	Services de streaming, billetterie en ligne, sociétés de production, salles de spectacle	Piratage de comptes, collecte de prix, analyse de stocks, achats automatisés
Services financiers	Banques, assurances, investissements, cryptomonnaies	Détournement de comptes, fraude à la carte bancaire, piratage, collecte de contenus personnalisés
Agroalimentaire	Services de livraison de repas, courses en ligne, sites de marques alimentaires, sites de boissons	Fraude à la CB, piratage de comptes, abus de cartes cadeaux et de codes promotionnels
Jeux d'argent	Casinos, paris sportifs	Détournement de comptes, récupération de cotes, création de comptes pour profiter de promotions

SECTEUR	QUELS TYPES D'ENTREPRISES SONT CONCERNÉS ?	QUELLES SONT LES ACTIONS DES MAUVAIS BOTS ?
Jeux vidéo	Jeux en ligne, jeux vidéo	Usurpation de comptes, création de comptes pour abus promotionnels, triche, automatisation du jeu, attaques par déni de service
Administration	Sites institutionnels, services aux citoyens, États, municipalités, métropoles	Usurpation de comptes, extraction de données sur les immatriculations d'entreprises, enregistrements de votes, récupération et planification de rendez-vous
Santé	Services de santé, pharmacies	Usurpation de comptes, extraction de contenus, bots « utiles » récupérant les disponibilités de rendez-vous
Mode de vie	Magazines de vie, blogs	Extraction de contenus exclusifs
Marketing	Agences de marketing, agences publicitaires	Extraction de contenus exclusifs, fraude publicitaire, attaques par déni de service, manipulation des données
Actualités	Sites d'actualités, magazines en ligne	Extraction de contenus exclusifs, fraude publicitaire, spam dans les commentaires
Commerce	Sites e-commerce, places de marché, petites annonces	Usurpation de comptes, revente massive, rupture de stock, fraude à la CB, fraude aux cartes cadeaux, extraction de données et de prix, manipulation des analyses
Société	Associations, religions et croyances, relations amoureuses, communautés en ligne, LGBTQ, généalogie	Extraction de contenus et de données, prise de contrôle de comptes, création de comptes, tests de cartes bancaires volées sur les pages de dons
Sports	Actualités sportives, mises à jour, résultats en direct	Collecte de données (scores en direct, cotes, etc.)
Télécoms et FAI	Opérateurs télécom, fournisseurs mobiles, hébergeurs	Prise de contrôle de comptes, collecte de prix concurrents
Voyage	Compagnies aériennes, hôtels, réservations de séjours	Extraction de prix, manipulation du ratio consultation/réservation, déni de service, collecte de prix, prise de contrôle ATO, rotation de sièges

À propos de ce rapport

Cette douzième édition du Bad Bot Report d'Imperva explore l'évolution rapide du trafic automatisé sur internet et l'impact croissant des bots malveillants. Ce rapport s'appuie sur les analyses des équipes Threat Research et Security Analyst Services (SAS) d'Imperva. Il présente les tactiques, techniques et procédés (TTP) les plus récents utilisés par ces bots pour contourner les défenses des entreprises.

L'analyse repose sur les données 2024 collectées à travers le réseau mondial Imperva, avec le blocage de 13 000 milliards de requêtes malveillantes sur des milliers de domaines. Ce volume d'informations offre une vision unique du comportement des bots et permet d'aider les organisations à mieux comprendre et anticiper les risques liés aux attaques automatisées.

Grâce à l'IA, les attaques de bots gagnent en ampleur, en accessibilité et en sophistication. Les bots sont désormais capables d'imiter des comportements humains, de contourner les mécanismes de détection et de mener des opérations ciblées à grande échelle. Ils exploitent les failles des systèmes pour extraire des données, détourner des comptes ou manipuler des inventaires, souvent à des fins lucratives. Ces attaques ont aussi un impact direct sur la relation client : elles dégradent la qualité du service en ligne, faussent les prix et limitent l'accès aux produits, sapant ainsi la confiance et la fidélité des utilisateurs.

Face à ces évolutions, les entreprises doivent renforcer leurs dispositifs de protection et adopter des stratégies de défense plus avancées afin de se prémunir contre la fraude, les pertes financières et les atteintes à la réputation. Ce rapport Bad Bots 2025 propose une série de recommandations concrètes pour aider les organisations à identifier, prévenir et neutraliser les menaces liées à l'automatisation malveillante, un enjeu devenu central pour la sécurité numérique des entreprises.

À propos de la sécurité des applications Imperva

Imperva, acteur de référence dans le domaine de la cybersécurité, protège les applications, les API et les données des organisations, sur tous les environnements : cloud, hybride et on premise. La plateforme de sécurité applicative Imperva combine performance et fiabilité : elle permet aux entreprises de sécuriser leurs actifs numériques à grande échelle, tout en optimisant leurs coûts et en limitant les faux positifs. Grâce à l'équipe Imperva Threat Research et à une communauté mondiale d'experts, Imperva anticipe en permanence l'évolution des menaces et intègre les dernières avancées en matière de sécurité, de protection des données et de conformité réglementaire.

La plateforme Imperva Application Security réunit les meilleures technologies du marché pour offrir une protection multiniveaux sur tous les environnements cloud, hybrides et on premise :

- Web Application Firewall (WAF) — solutions sur site et dans le cloud pour bloquer les principales menaces ciblant les applications web.
- Sécurité des API — protection continue grâce à l'indexation et à la classification approfondies des API.
- Protection avancée contre les bots — défense des sites web, applications mobiles et API face aux attaques automatisées les plus sophistiquées.
- Protection côté client — sécurisation des sites web contre les attaques côté navigateur et simplification de la conformité PCI DSS 4.0
- Protection DDoS — garantie de la continuité opérationnelle pour les sites, réseaux et DNS grâce à une disponibilité assurée
- Réseau de diffusion de contenu (CDN) — distribution sécurisée et optimisée des applications, partout dans le monde.

Lancez dès aujourd'hui votre essai gratuit pour protéger vos applications contre les bots malveillants.

imperva
a Thales company

Contactez-nous

Pour nous contacter, rendez-vous sur
imperva.com/contact-us

imperva.com