Avril 2022

Le nouvel ABC de la sécurité des applications

Des vulnérabilités des API aux bots en passant par la protection côté client

Barracuda

Sommaire

Introduction – Des vecteurs d'attaque plus récents et plus dangereux

En permettant aux entreprises numériques de communiquer avec leurs utilisateurs et leurs clients, les applications se sont rapidement imposées comme un outil indispensable. L'adoption massive du télétravail en 2020 a accentué l'importance des applications sur le Web, poussant les entreprises à mettre à niveau leurs services Web existants, à exposer leurs anciennes applications sur Internet ou encore à déployer de toutes nouvelles applications. Ces nouvelles applications ont été créées rapidement à l'aide d'API et de logiciels open source et, une fois de plus, la sécurité a été négligée au profit de la croissance de l'entreprise.

Barracuda

Les entreprises sont confrontées depuis toujours à une multitude de défis liés à la sécurité des applications. En effet, ces dernières comptent parmi les principaux vecteurs de violation de données comme l'indique le Rapport Verizon sur les violations de données depuis quelques années, et représentent l'une des deux principales raisons pour lesquelles les violations de données se produisent. Après les attaques traditionnelles contre les applications sur le Web telles que l'injection SQL, le cross-site scripting et l'injection de commandes, on s'en prend désormais aux API et aux applications mobiles.

Depuis quelques années, les menaces qui pèsent sur les applications ne cessent de se multiplier et de nouveaux vecteurs d'attaque, plus dangereux, sont apparus. Parmi ces derniers, les plus répandus sont les vulnérabilités des API, les bots automatiques et les vulnérabilités côté client. En effet, selon les personnes interrogées par Barracuda dans le cadre de son rapport La sécurité des applications : état des lieux en 2021, les violations de données au sein de leur entreprise étaient principalement imputables aux attaques par bots, aux vulnérabilités des applications sur le web, aux attaques contre les chaînes logistiques logicielles et aux failles de sécurité API.

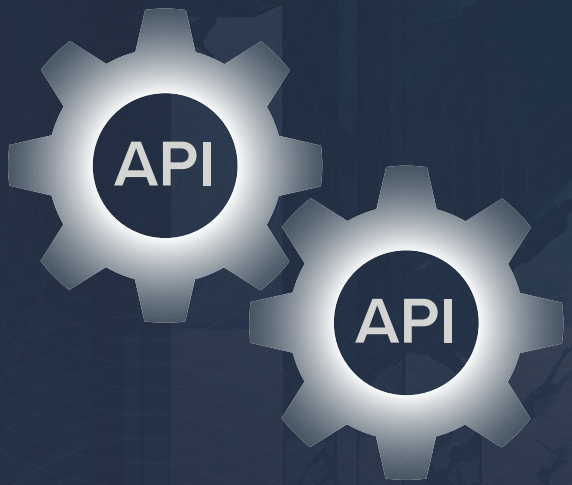
Le nombre de vulnérabilités et de failles imputables aux API et aux attaques côté client a augmenté de manière exponentielle. Certaines violations de données comme celles de T-Mobile et de British Airways ont tristement fait la une. Les attaques côté client, également appelées attaques de la chaîne logistique, ont été découvertes aux alentours de 2018 et baptisées Magecart car elles ciblaient principalement les boutiques en ligne qui utilisaient la technologie Magento. Les pirates informatiques avaient commencé par identifier le JavaScript tiers couramment utilisé pour les pages de paiement. Ils en ont ensuite piraté les fichiers source et inséré leur code de skimming. Lorsqu'un utilisateur se connectait au site, le JavaScript, désormais malveillant, se chargeait et dérobait ses identifiants.

Les attaques de bots affectent différemment les entreprises. À titre d'exemple, l'un des principaux types d'attaques consiste à automatiser l'achat d'articles en édition limitée afin de les revendre. Connue sous le nom de « scalping », cette pratique entraîne des pénuries, comme celle de la PlayStation 5. Cela fait un moment que l'on emploie également les bots pour lancer d'autres types d'attaques dont les plus dommageables sont le piratage de compte et les attaques DDoS.

Cet e-book vous propose une analyse approfondie de ces trois vecteurs d'attaque, à savoir les vulnérabilités des API, les attaques de bots et les attaques côté client, ainsi que nos conseils pour renforcer la sécurité de vos applications et protéger votre entreprise contre ces menaces en constante évolution.

« A » comme API

Longtemps, les API étaient principalement utilisées en arrière-plan des applications métier pour assurer la communication entre machines. Aujourd'hui, on les trouve partout, notamment dans les applications que nous utilisons au quotidien.
La plupart des applications mobiles et Web que nous utilisons au travail ou en dehors reposent sur des API. Elles sont au cœur des entreprises, alimentent les plateformes numériques modernes et contribuent à la transformation numérique.



Barracuda

Les entreprises se sont massivement tournées vers le développement d'applications orientées API, une méthode qui leur permet d'innover et de se lancer rapidement sur le marché. Associées à des pratiques agiles et DevOps, les API permettent aux développeurs de créer et de publier rapidement de nouvelles fonctionnalités pour les applications sur le Web et mobiles, accélérant ainsi les délais de livraison. Alors que leur usage est en hausse, les API, qui servent désormais de socle aux principaux services des applications qu'elles alimentent, ont vu leur accès aux données stratégiques augmenter de manière exponentielle.

La croissance des API et leur accès direct aux données stratégiques en font la cible privilégiée des pirates informatiques. Étant donné que les API reposent sur l'automatisation, la recherche et l'exploitation d'API non sécurisées s'avèrent très rentables pour les cybercriminels. Les attaques automatisées rendent l'exfiltration des données plus rapide et plus facile que dans le cas des applications sur le Web. Contrairement aux applications traditionnelles, qui cachent la logique métier sur le serveur backend, les applications basées sur API encodent cette logique sur elles-mêmes. Cela signifie que les pirates peuvent facilement intercepter le trafic des applications concernées afin d'identifier les points de terminaison des API et de mener des attaques contre eux.

Les API constituent une cible privilégiée des cybercriminels, comme l'indique le rapport PriorityOne publié par BugCrowd en 2021. Ce dernier révèle que les vulnérabilités des API ont doublé en un an et ne cesseront d'évoluer et de se multiplier au cours des années à venir pour devenir l'un des principaux vecteurs d'attaque contre les applications.

les vulnérabilités des API

ont doublé

en un an

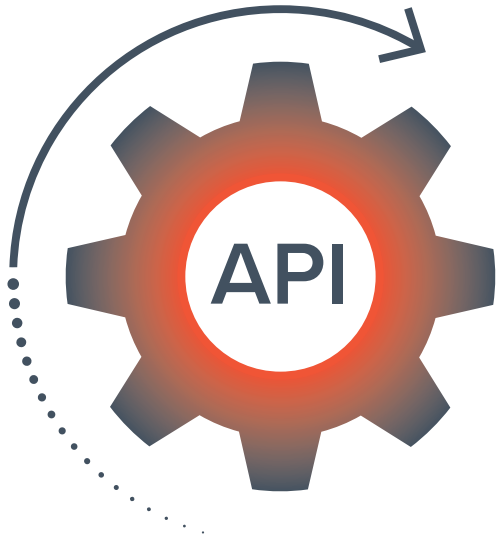
Exemple : l'API Experian expose les notes financières de dettes d'entreprise

Pendant qu'il étudiait les offres de prêt étudiant en ligne, un chercheur a récemment découvert une importante vulnérabilité d'API. Sur le site de l'organisme prêteur, il suffisait de renseigner son nom, son adresse et sa date de naissance pour vérifier son éligibilité. En bon chercheur, il a examiné le code derrière cette recherche pour découvrir qu'il s'agissait d'un appel d'API vers Experian. L'API utilisée permettait aux prêteurs d'envoyer des requêtes automatisées et d'obtenir les scores FICO auprès du bureau de crédit.

Le chercheur a constaté que l'accès à l'API d'Experian n'était pas sécurisé, et qu'il suffisait de saisir des zéros dans le champ de la date de naissance pour connaître la note financière des personnes souhaitées. Il a alors décidé de créer un outil pratique pour automatiser les recherches. L'API communiquait également les quatre « facteurs de risque » pris en compte dans le calcul des notes financières.

Contactée à ce sujet, la société Experian s'est contentée de supprimer l'accès API à partir de ce point de terminaison.

Le danger de ce type d'exposition est démontré par l'outil que le chercheur a créé. Ce dernier a fait le choix de signaler le problème à Experian. En revanche, s'il avait été découvert par un acteur malveillant, le point de terminaison aurait pu être utilisé pour recueillir la note financière des utilisateurs dont le nom et l'adresse sont affichés publiquement et les conséquences auraient pu être désastreuses. Impossible d'évaluer le type d'extraction entraîné par l'appel API et la manière dont cette visualisation a affecté la note financière de la personne.



Barracuda

Exemple : mots de passe des réunions privées Zoom déchiffrés par force brute

Par défaut, les réunions Zoom étaient protégées par un mot de passe à six caractères numériques, ce qui correspond à 1 million de combinaisons possibles. Un chercheur a découvert que ces mots de passe pouvaient être déchiffrés par force brute, ouvrant ainsi la voie aux bombardements de Zoom ainsi qu'à d'autres types d'attaques.

À l'époque où les mots de passe Zoom comportaient uniquement des caractères numériques, les utilisateurs pouvaient cliquer sur le lien des réunions pour ouvrir une page Web les invitant à saisir leur mot de passe. Après avoir rempli les champs obligatoires et cliqué sur Entrée, l'utilisateur a pu observer les interactions dorsales de l'API et découvrir la faille.

Une faille importante a été identifiée lors de ce processus : le nombre de tentatives de connexion était illimité. Par conséquent, le chercheur a pu essayer différents mots de passe ; environ 29 minutes et 43 164 tentatives plus tard, soit 25 mots de passe par seconde, il a fini par trouver le bon identifiant. Si plusieurs machines avaient été utilisées en parallèle lors d'une attaque, le mot de passe aurait été identifié très rapidement.

Les implications de ce type de piratage étaient considérables. En effet, cette faille aurait pu s'avérer fort dommageable si des acteurs malveillants avaient espionné les réunions des innombrables institutions publiques et organismes similaires qui font appel à Zoom. Le chercheur en a informé Zoom qui a pris les mesures nécessaires pour résoudre le problème.

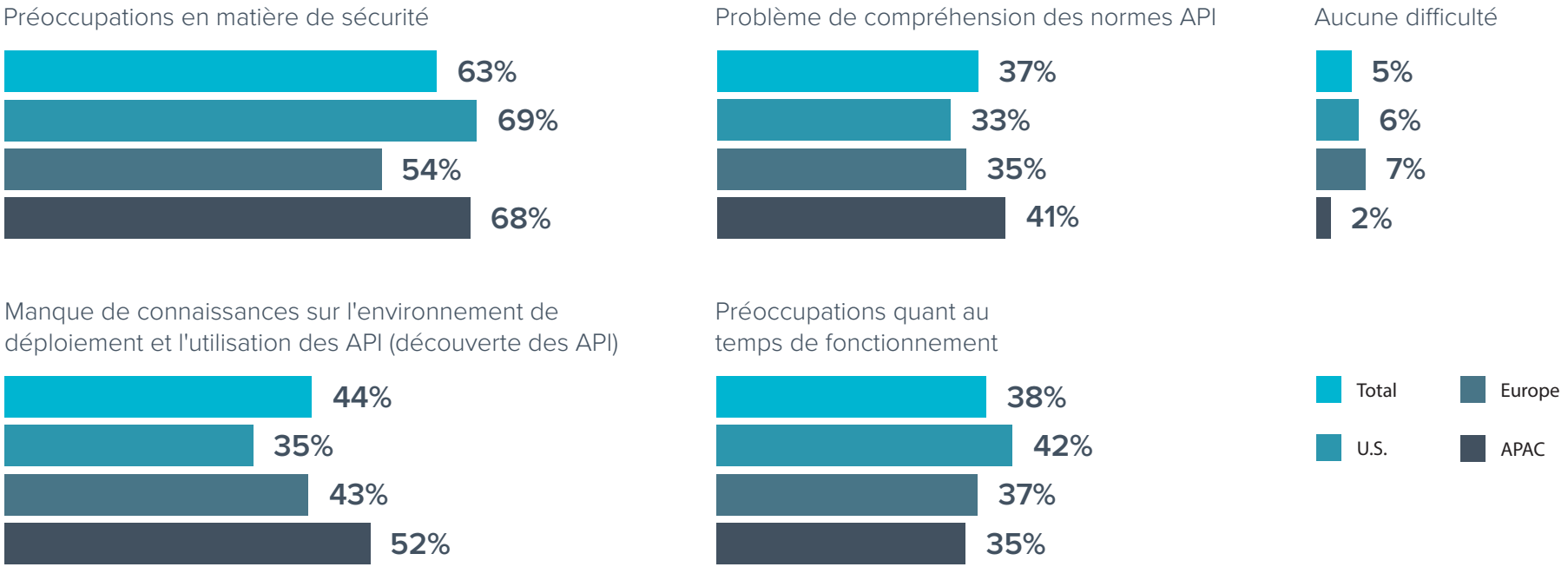
Outre le nombre de tentatives illimité, un autre problème que l'on a pu constater était le manque de surveillance et de consignation, mesures qui auraient permis à l'équipe de Zoom de détecter ces tentatives.

Ce qu'en disent les spécialistes en sécurité des applications

Étant donné l'impact considérable des violations d'API, la sécurité de ces dernières est, sans surprise, au cœur des préoccupations des équipes de défense. Lors d'une récente enquête, nous avons demandé aux spécialistes en sécurité des applications de préciser les principaux défis qu'ils rencontraient lors du déploiement des API et la sécurité est arrivée en tête de liste. Cela est confirmé par l'OWASP (Open Web Application Security Project), qui vient de publier son Top 10 des failles API qui répertorie les principaux risques de sécurité et les vulnérabilités spécifiques aux API.

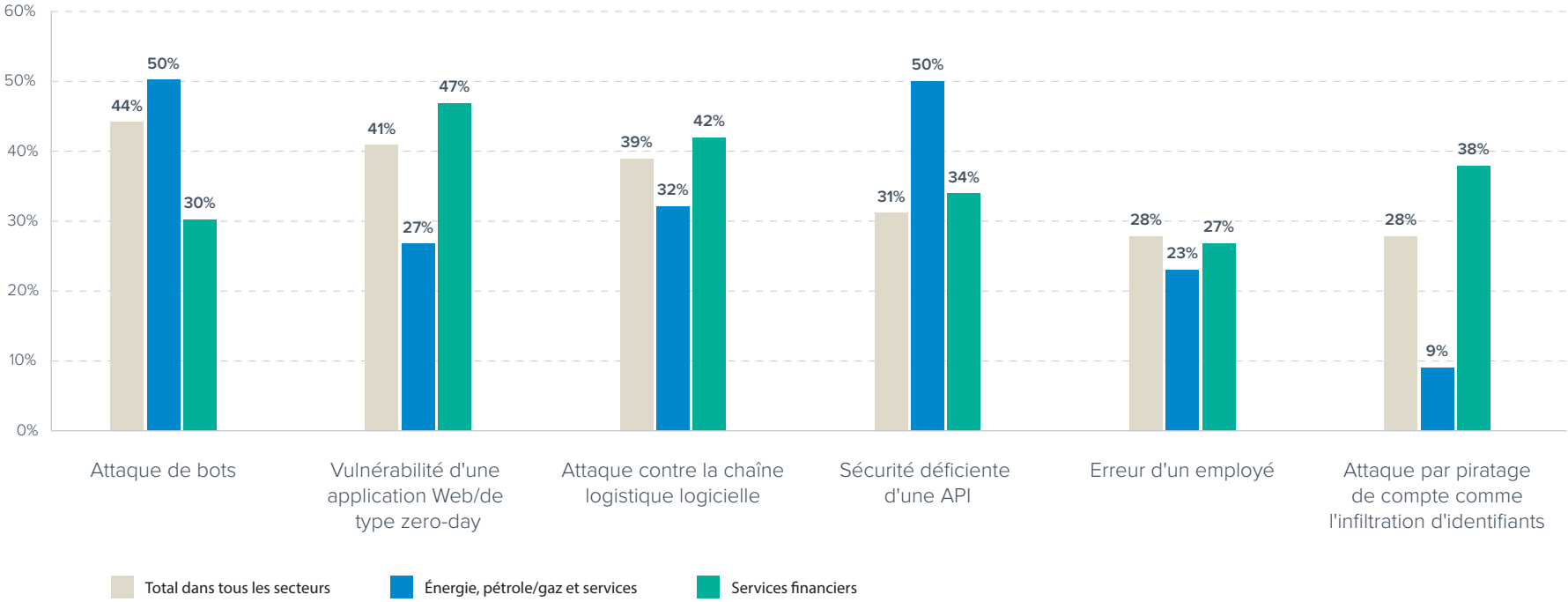
Quelles principales difficultés votre entreprise rencontre-t-elle lors du déploiement d'API ?

(n=728)



Parmi les éléments suivants, lesquels ont contribué à la réussite de la violation de sécurité ayant touché l'une des applications de votre entreprise au cours des 12 derniers mois ?

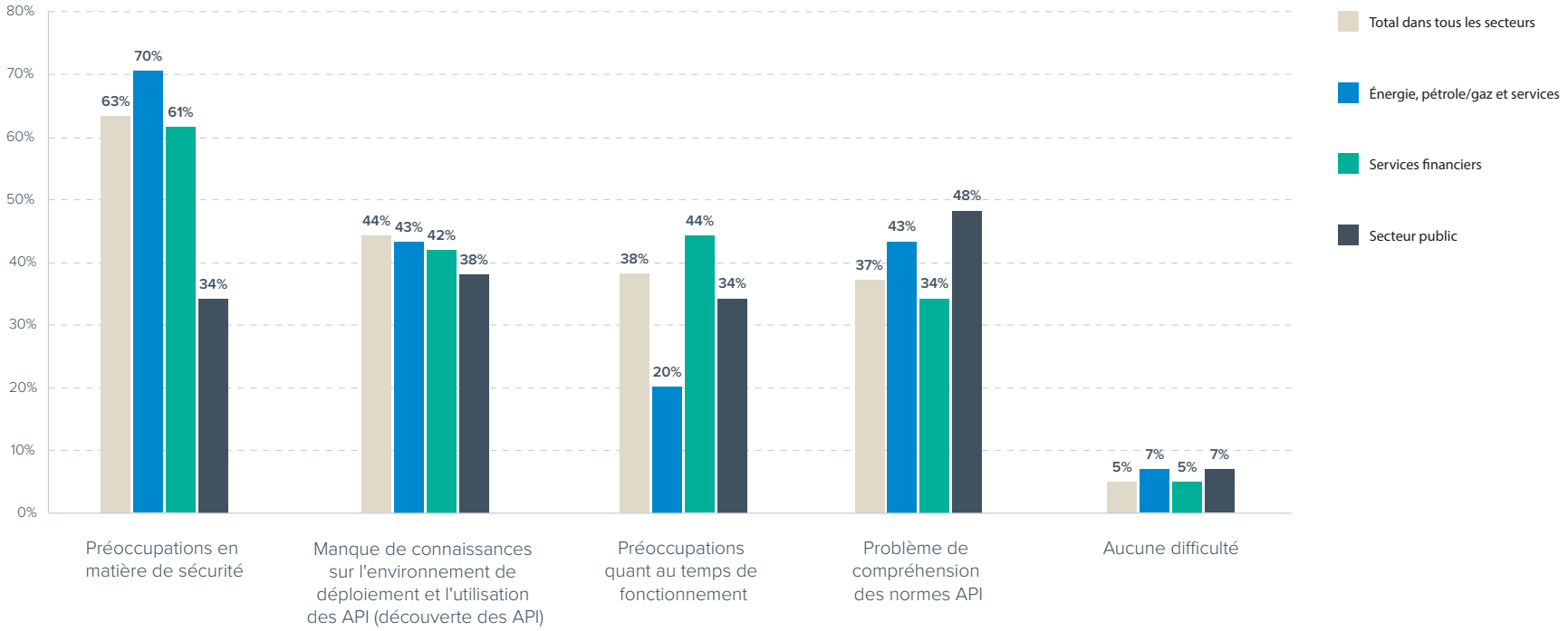
(n=541)



Selon les résultats de l'enquête, les secteurs les plus susceptibles de subir une violation de données en raison d'une vulnérabilité d'API sont ceux de l'énergie, du pétrole et du gaz ainsi que les services. Bien que ces secteurs fassent la une surtout en raison des attaques ciblées par ransomware et des attaques menées sur les objets connectés, leurs API, dont beaucoup sont destinées au public, sont également menacées. Les personnes interrogées dans le secteur financier, dont les transactions reposent essentiellement sur des API, ont également cité les failles API en haut du classement.

Quelles principales difficultés votre entreprise rencontre-t-elle lors du déploiement d'API ?

(n=728)

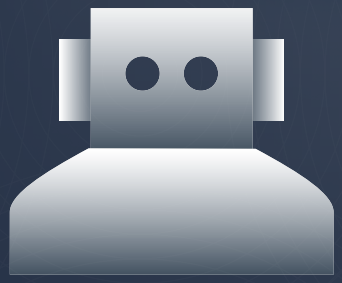


Selon les personnes interrogées, le secteur des services est le moins susceptible de rencontrer des difficultés lors du déploiement des API. Il est intéressant de noter qu'ici, le principal défi est la « mauvaise compréhension des normes API ». La sécurité des API n'arrive qu'en troisième position, alors que les autres secteurs se disent presque tous profondément préoccupés par cette dernière. Ce sont les secteurs de l'énergie, du pétrole, du gaz mais aussi les services et les industries manufacturières qui sont les plus préoccupés par la sécurité des API.

Les entreprises du secteur financier sont, sans surprise, les plus préoccupées par le temps de bon fonctionnement. Les secteurs les moins préoccupés par la question de conformité sont ceux de l'énergie, du pétrole, du gaz, et des services, ce qui est d'une certaine manière inquiétant étant donné que la conformité des API contribue à renforcer leur sécurité.

« B » comme bots

Au cours des dernières années, nous avons assisté à une montée en flèche du trafic généré par les bots automatisés. Autrefois utilisés principalement par les moteurs de recherche, les bots sont désormais utilisés à des fins différentes, bonnes ou mauvaises. Parmi les « bons » bots, citons notamment les robots d'indexation utilisés par les moteurs de recherche, les bots employés par les réseaux sociaux et les agrégateurs ou encore les robots de surveillance. Ces bots respectent les règles définies par le propriétaire du site Web dans le fichier robots.txt, publient des méthodes permettant de les valider en tant que tels et évitent de submerger les sites Web et les applications qu'ils visitent.

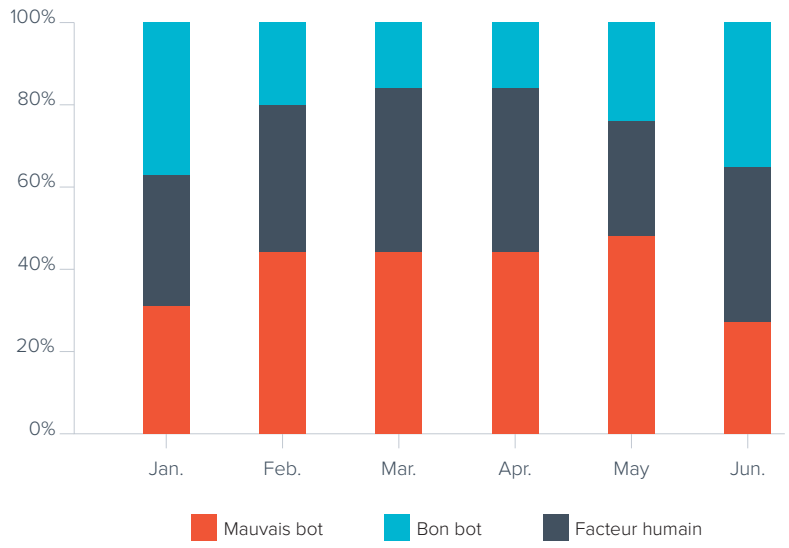


Barracuda

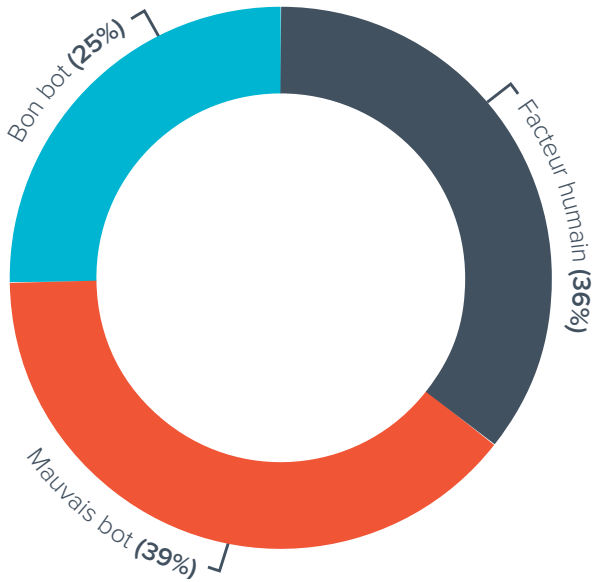
Conçus pour nuire, les bots malveillants peuvent être utilisés à des fins différentes et se déclinent en plusieurs catégories, des simples bots de scraping, qui visent à dérober des données à partir d'une application (et qui sont faciles à bloquer), aux bots persistants avancés qui imitent le comportement humain et tentent d'échapper à la détection autant que possible. Ces derniers lancent différents types attaques, notamment le web scraping et le price scraping, le piratage des inventaires, les tentatives de piratage de compte et les attaques par déni de service distribué (DDoS). Sachant qu'une part importante du trafic web actuel provient des bots malveillants, il est impératif que les entreprises soient à même de les identifier et les neutraliser.

Le trafic automatisé représente près des deux tiers du trafic Internet, selon les mesures effectuées par Barracuda au cours du premier semestre 2021. Environ 25 % de ce trafic provient de bons bots connus, comme les robots d'indexation utilisés par les moteurs de recherche, les bots employés par les réseaux sociaux et les robots de surveillance.

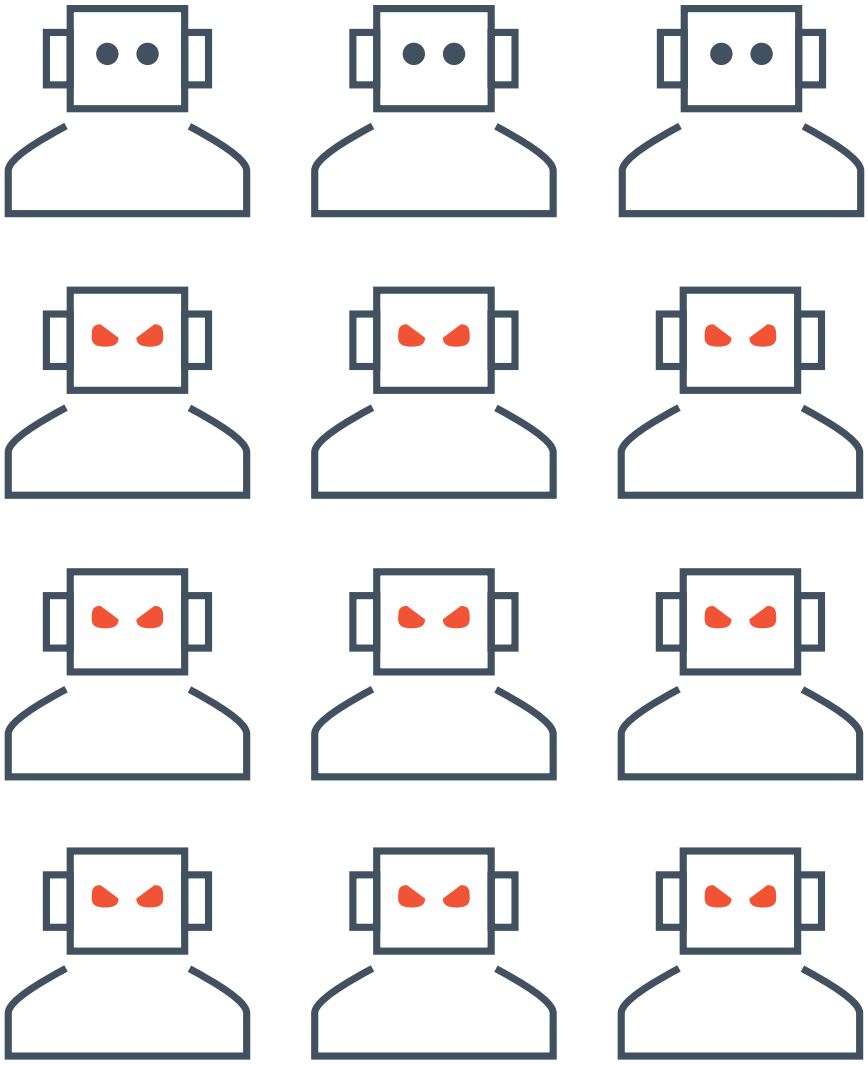
Répartition par mois



Distribution du trafic : bots et humains (janvier – juin 2021)



Hautement sophistiqués, les bots d'aujourd'hui sont conçus pour imiter au mieux le comportement humain et contourner la plupart des systèmes de défense. Les mesures classiques mises en places pour les bloquer, notamment Google reCAPTCHA, ne leur posent aucun problème. Bien au contraire, les CATPCHA à base d'images sont plus faciles à résoudre pour les bots que pour les humains. Autour des bots s'est construit tout un écosystème englobant les personnes qui les ont créés, les services proposant des comptes Google « à réputation élevée » pour contourner la vérification CAPTCHA, les services proposant des adresses IP résidentielles (ou Resis) pour contourner le filtrage de réputation IP ou encore les services d'entiercement qui protègent les acheteurs contre les arnaques. Le recours de plus en plus fréquent aux bots pour gagner de l'argent rapidement, comme le scalping de PlayStation 5 en décembre 2020, en font un problème majeur.

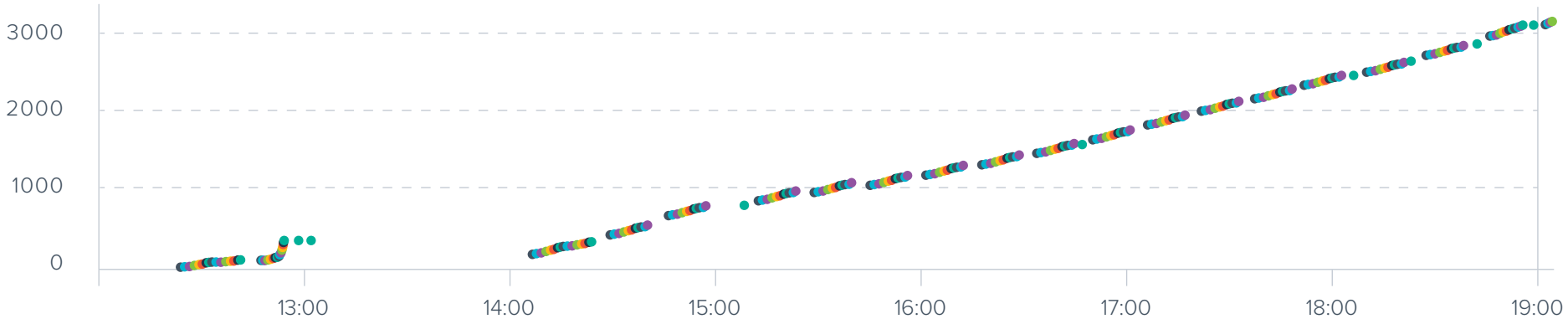


Exemple : price scraping d'une boutique de e-commerce en Europe de l'Est

Barracuda a détecté et arrêté une tentative de price scraping visant une boutique e-commerce en Europe de l'Est. La boutique proposait une réduction sur les produits Apple et le trafic présentait des comportements suspects. Ces derniers étaient associés à des clients de navigateurs standard et à plusieurs adresses IP résidentielles locales. Cependant, ces adresses IP locales provenaient de fournisseurs d'hébergement VPS et l'accès de chaque client était limité à un ensemble de pages standard.

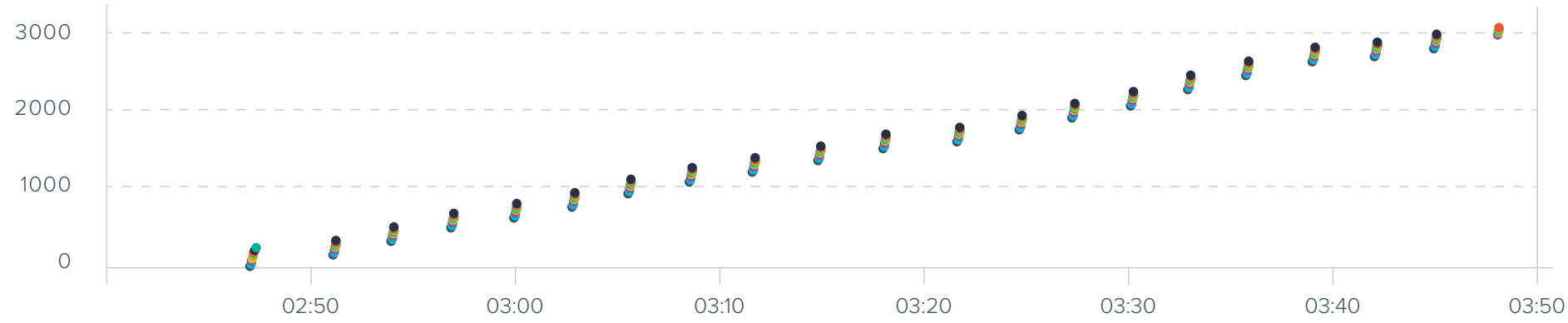
C'est cette corrélation qui a permis de démasquer les pirates et d'arrêter la tentative de price scraping.

Reproduire le modèle d'un bot de récupération de prix



Les bots accédaient au même ensemble d'URL de produits plusieurs fois par heure après le blocage de la salve initiale.

Changement de modèle de robot pour tenter d'éviter la détection

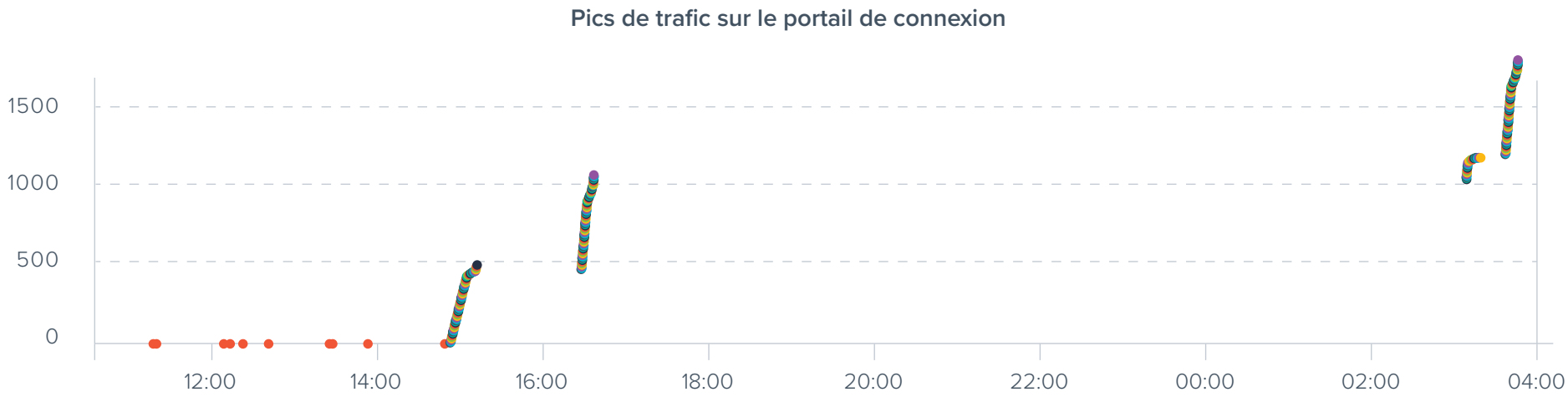


Les bots tentent d'accéder à un plus petit ensemble de pages de produits dans un modèle de navigation différent plusieurs fois par heure.

Barracuda

Exemple : tentative de submerger le portail de connexion d'un fabricant indien

Le portail de connexion d'un fabricant indien enregistrait un trafic particulièrement élevé. Ce dernier provenait principalement de réseaux mobiles, ce qui est inhabituel mais pas inattendu pour ce site Web. Grâce à une analyse approfondie, le système a toutefois déterminé que le trafic entrant provenait très probablement d'un navigateur de bureau qui agissait comme un appareil mobile connecté à un hotspot. Les clients qui tentaient de submerger cette page de connexion ont pu être bloqués et le temps de réponse est redevenu normal.



Les premiers points étaient un robot qui prétend être humain et répandre ses accès. Par la suite, des agrégats s'affichent et chaque point représente un client différent tentant d'accéder à la page de connexion.

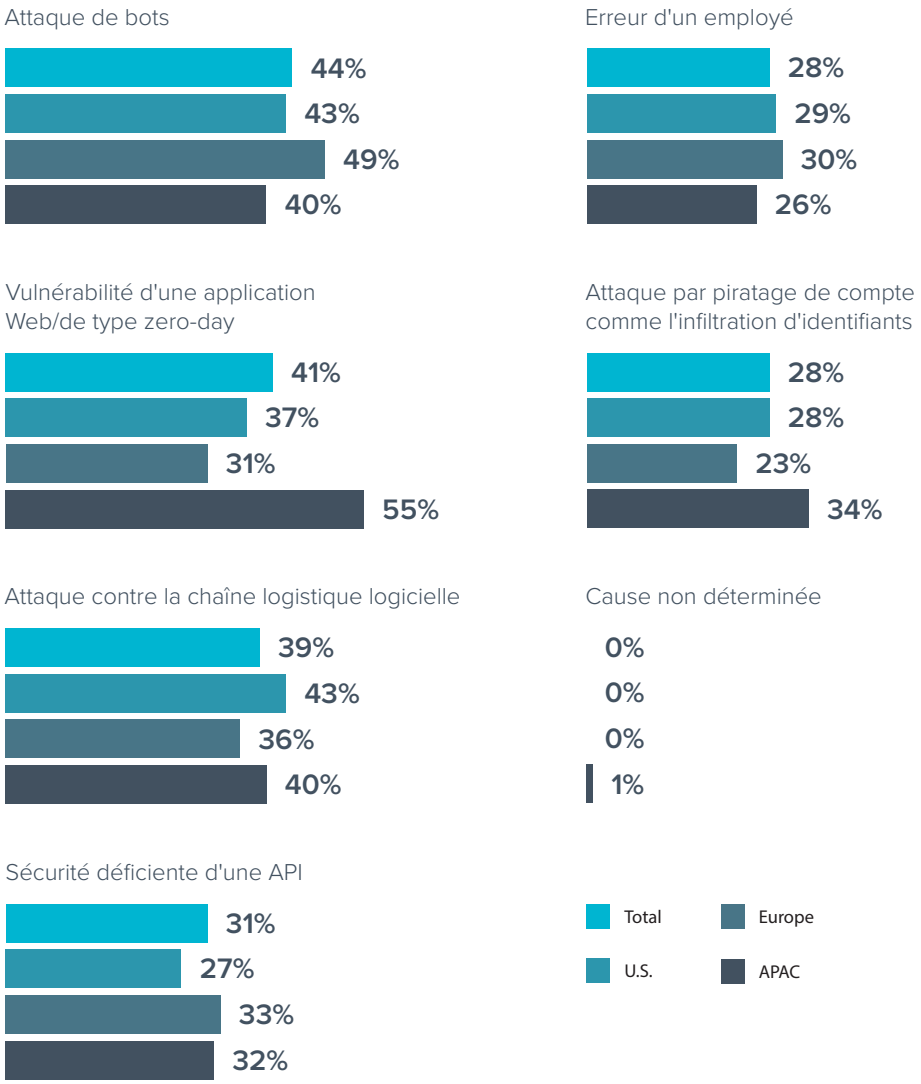
Ce qu'en disent les spécialistes en sécurité des applications

Les attaques de bots se sont multipliées ces dernières années et elles ont entraîné des compromissions d'une ampleur considérable. Il y a deux ans, les principales menaces liées aux bots étaient le piratage de compte et le credential stuffing. Par ailleurs, les attaques étaient souvent médiatisées et le « dumping d'identifiants » provenant de sites comme LinkedIn était rendu public.

Selon une récente étude menée par Barracuda auprès des spécialistes en sécurité des applications, ce sont les attaques de bots qui ont su exploiter au mieux les vulnérabilités des applications au cours des 12 derniers mois.

Parmi les éléments suivants, lesquels ont contribué à la réussite de la violation de sécurité ayant touché l'une des applications de votre entreprise au cours des 12 derniers mois ?

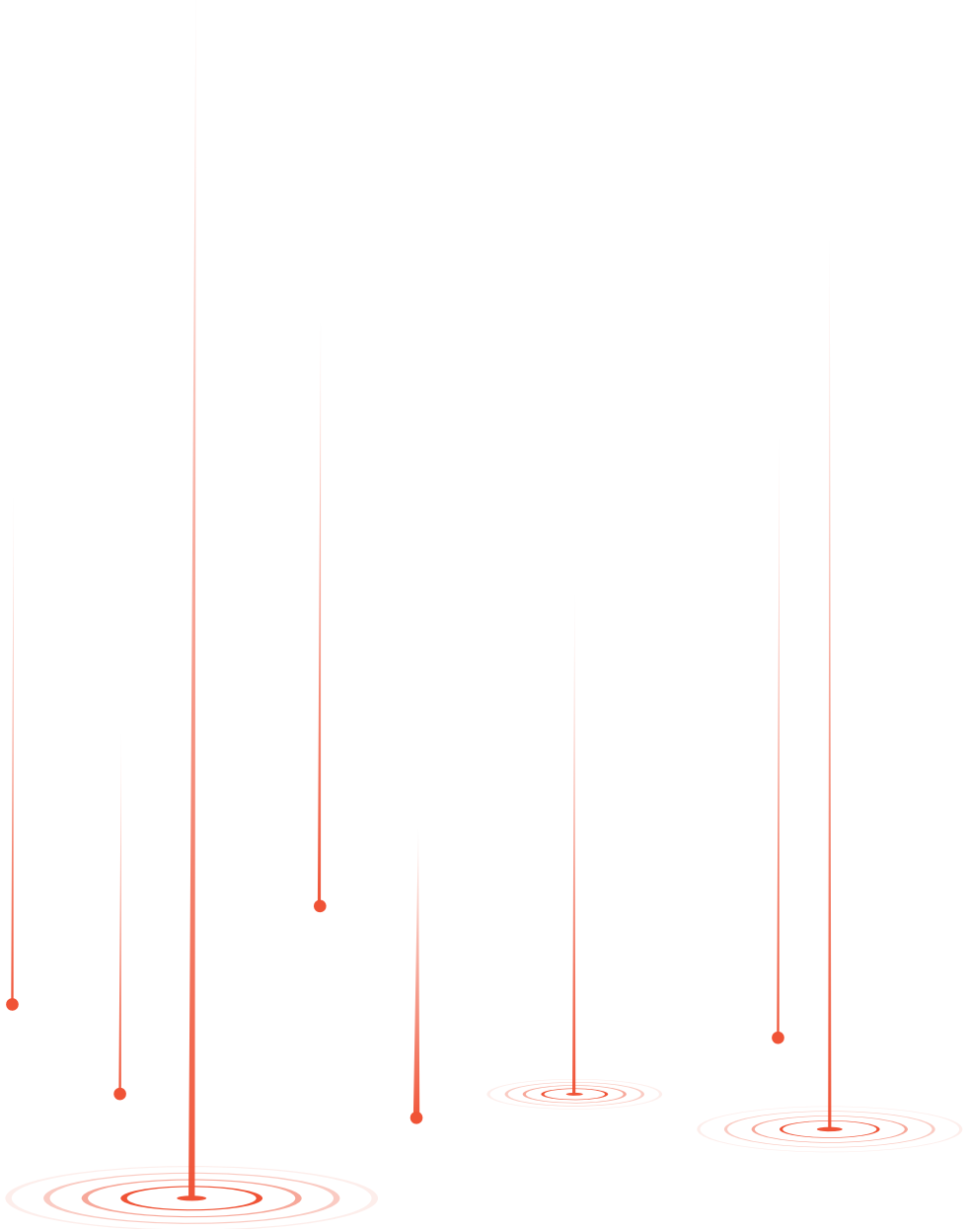
(n=541)



La diversité des attaques de bots visant les applications les rend difficiles à neutraliser et donne du fil à retordre aux équipes de défense.

Face à une telle multiplicité, la plupart des entreprises peinent, sans surprise, à protéger leurs applications contre ces bots. Alors que le spam provenant de bots constitue plutôt une nuisance, il est souvent utilisé pour dissimuler une activité plus malveillante d'où la nécessité de s'en occuper avec attention et non de l'ignorer. En fonction de sa fréquence et de son origine, ce spam peut vite prendre des proportions inquiétantes et facilement mettre en péril les activités de l'entreprise.

Les bots qui se font passer pour un navigateur ou une application constituent également un problème majeur. Plus ou moins complexes, ces usurpations revêtent diverses formes, de l'utilisateur qui tente de dissimuler son navigateur aux bots exécutant la version compromise d'une application au sein d'une ferme à clics à des fins malveillantes comme la fraude publicitaire.

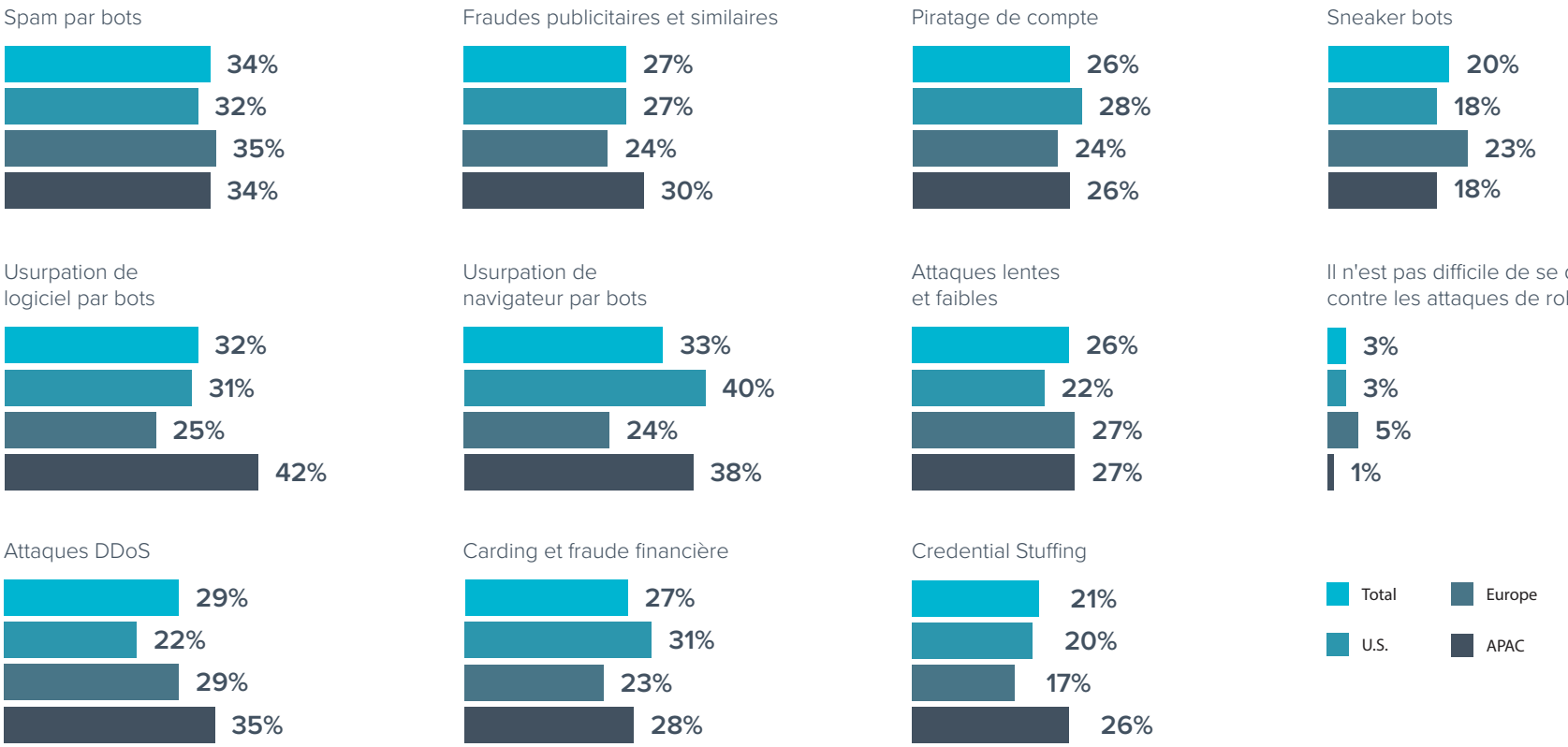


Barracuda

Or la combinaison de ces bots augmente leurs chances de réussite. Les attaques de bots multivecteurs de type « low-and-slow » constituent le cœur du problème et ont très probablement contribué à certaines violations réussies l'an dernier.

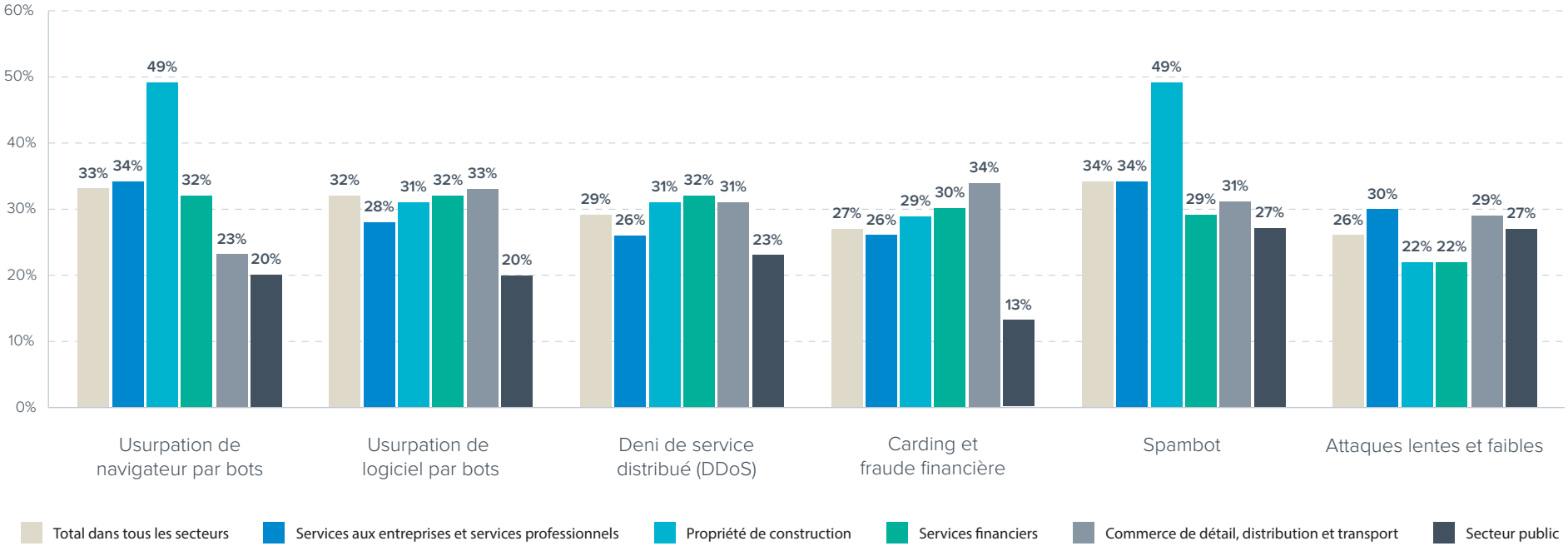
Contre quels types d'attaques de bots visant les applications votre entreprise peine-t-elle à se défendre ?

(n=750)



Parmi les types suivants d'attaque par bots ciblés par les applications de votre organisation, quels types de bots avez-vous du mal à se défendre ?

(n=750)



Selon les personnes interrogées, le secteur financier peine à se protéger contre trois principaux types d'attaques de bots : les attaques DDoS, les bots se faisant passer pour un logiciel et les bots se faisant passer pour un navigateur. Ces types d'usurpation constituent une réelle menace pour les applications financières. En effet, les cybercriminels utilisent des versions piratées pour mener des actions malveillantes contre ces entreprises. Les attaques DDoS entraînent des pertes financières considérables puisqu'elles rendent ces systèmes indisponibles. Il est également intéressant de noter que les fraudes à la carte bancaire et les fraudes financières arrivent en deuxième position, et non en première, comme on aurait pu l'imaginer. Cela démontre l'importance toujours croissante des services d'accès par application ou navigateur pour les entreprises financières.

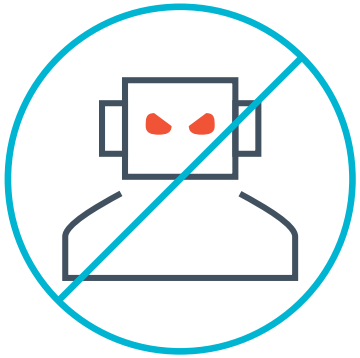
Les bots se faisant passer pour un logiciel ou un navigateur arrivent dans le top 5 des préoccupations, tous secteurs confondus. Autre détail intéressant, les secteurs de la construction et de l'immobilier, ainsi que le secteur public, se disent très préoccupés par les spambots. Nous pouvons en conclure que les sites immobiliers recensent un nombre important d'annonces frauduleuses. Le spam représente également une préoccupation majeure pour le secteur public. Par exemple, il y a quelques années, le nombre d'entrées de type « spam » dans les discussions de la FCC autour de la neutralité du Net était particulièrement préoccupant.

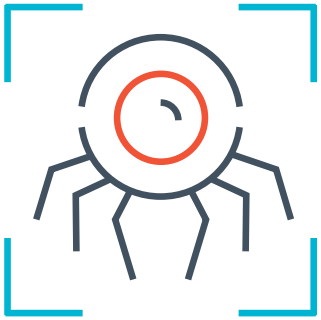
Les entreprises publiques, les secteurs du commerce de détail, des services aux entreprises et des services professionnels citent les bots de type « low and slow » comme principal sujet de préoccupation. Les entreprises publiques, qui ont souvent un grand nombre de téléchargements non protégés, deviennent une cible privilégiée des attaques DDoS applicatives. Le secteur du commerce de détail est également grandement menacé par les attaques dites « low and slow », comme le piratage de compte, le price scraping, le scalping, etc.

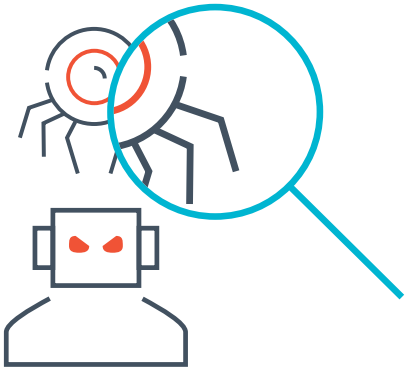
Les fournisseurs proposant une protection contre ces types d'attaques devront impérativement intégrer à leur solution des fonctionnalités telles que la prévention, la détection et l'identification des bots.

Les fournisseurs proposant une protection contre ces types d'attaques devront impérativement intégrer à leur solution des fonctionnalités telles que la prévention, la détection et l'identification des bots.

Il est impératif que les entreprises renforcent leurs défenses contre les attaques de bots, qu'ils soient frauduleux, de type spam ou conçus pour usurper les logiciels et les navigateurs. Après tout, les bots étaient responsables de la plupart des attaques réussies visant les applications au cours de l'année écoulée. Selon les personnes interrogées dans le cadre de notre enquête, le choix des solutions de sécurité se fait sur trois critères : la protection contre la fraude, la détection du spam et l'identification des bots.



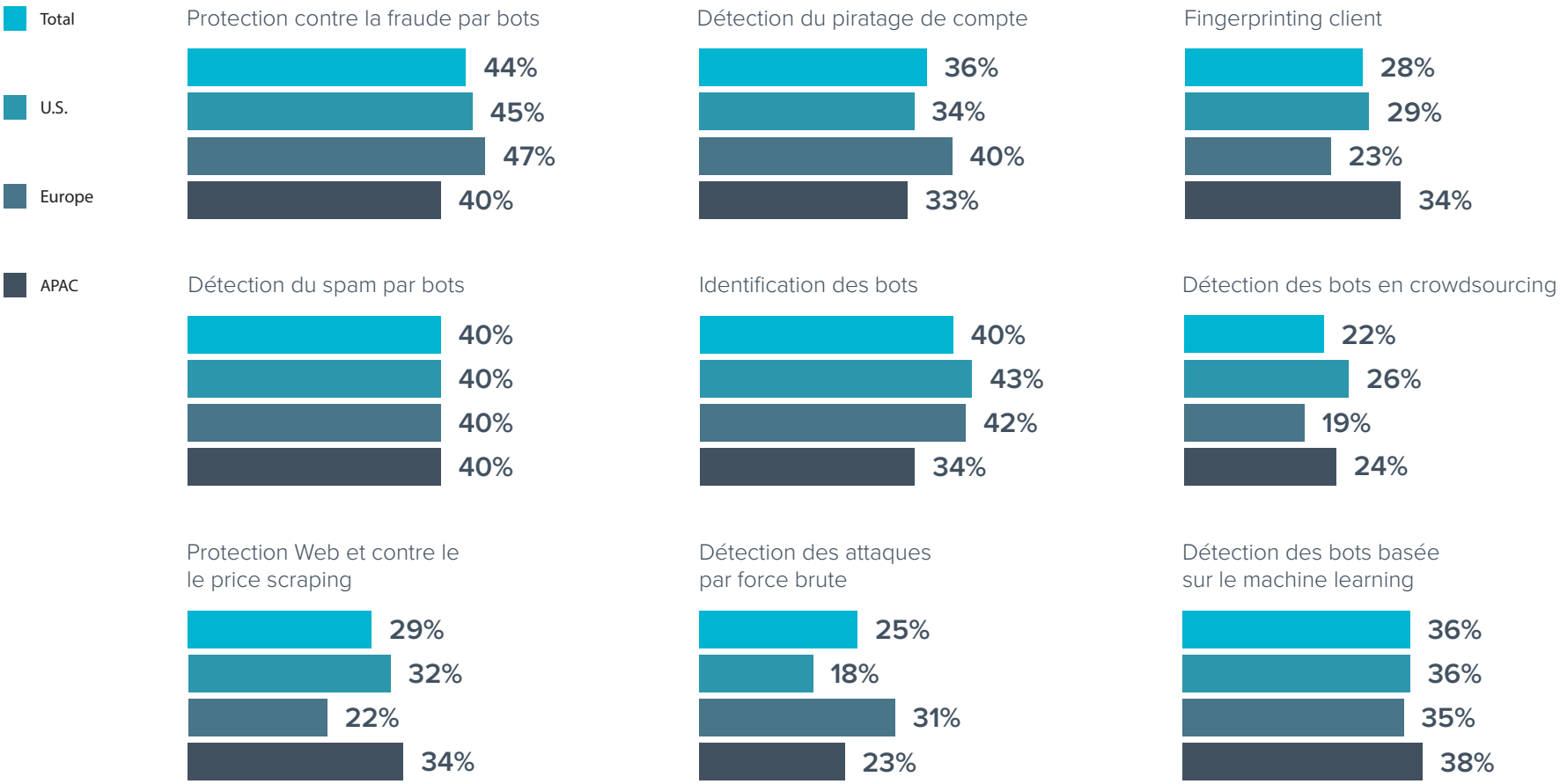




Ces fonctionnalités sont essentielles pour se défendre contre la plupart des attaques, quelle que soit leur nature. Tout fournisseur capable de les réunir au sein d'une seule et même solution saura protéger efficacement les entreprises contre ces bots.

Quelles fonctionnalités votre entreprise juge-t-elle les plus importantes dans le choix d'une solution de sécurité afin de protéger ses applications contre les attaques de bots ?

(n=750)



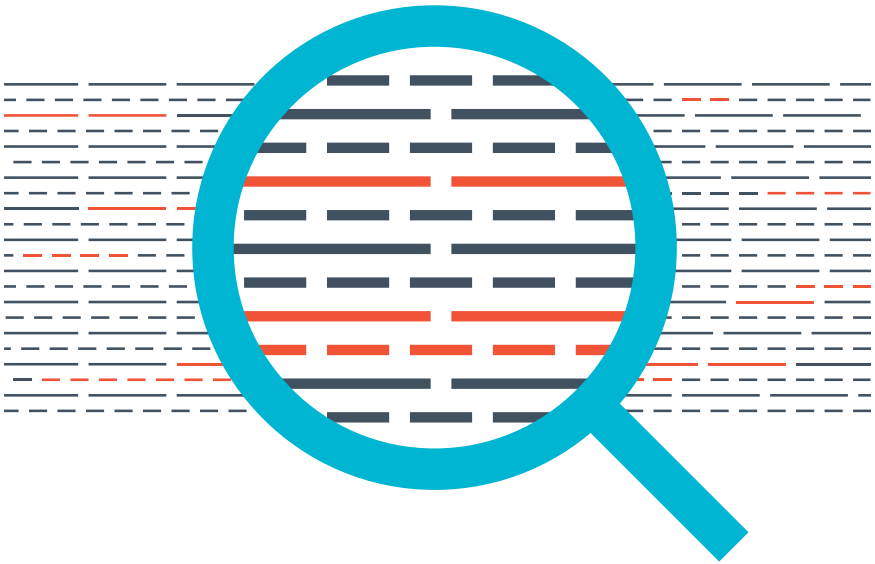
« C » comme protection côté client

Depuis quelques années, nous assistons à l'émergence de nouvelles vulnerabilités sur le Web telles que le clickjacking et le cross-site scripting (XSS), dont beaucoup se manifestent côté client. Par ailleurs, les vulnérabilités de type injection, qui ont fait leur apparition il y a une dizaine d'années, y sont toujours bel et bien présentes.

Les attaques côté client, également appelées attaques de la chaîne logistique ou attaques Magecart (baptisées d'après Magento, l'application de gestion commerciale initialement ciblée) sont difficiles à détecter et à bloquer.

Barracuda

Depuis la fin des années 1980, quand l'Internet a vu le jour, les applications n'ont cessé d'évoluer pour satisfaire notre appétit insatiable pour le Web. Ce changement s'est produit non seulement du côté serveur mais aussi du côté client (c'est-à-dire du navigateur). Tout comme le contenu dynamique a remplacé le contenu statique, les applications à page unique ont remplacé le simple rendu JavaScript par une expérience plus adaptée aux téléphones et aux tablettes. La logique applicative étant progressivement déplacée côté client, les pirates informatiques ont commencé à s'y intéresser également. Cette logique côté client est majoritairement mise en œuvre à l'aide d'un code open source ou d'un autre code tiers et ce au détriment de la sécurité.



Alors pourquoi les développeurs utilisent-ils du code tiers ? Pour simplifier, disons que le Web moderne ne serait pas possible autrement. Les pages Web modernes comprennent des dizaines, voire des centaines de scripts externes tiers. Les outils tels que webpagetest.org permettent de découvrir le nombre impressionnant de scripts tiers présents sur une page Web. Si cette approche du développement Web est retenue, c'est parce que l'autre solution, à savoir réinventer des milliers de lignes de code, est impensable. Le fond du problème est la confiance : un script jugé bon aujourd'hui peut être piraté le lendemain. Les acteurs malveillants ciblent les sources hébergeant ce code tiers pour pouvoir atteindre toutes les applications qui l'utilisent.

Comme c'est le code tiers qui est malicieusement modifié, la plupart des propriétaires d'applications ne détectent la compromission des scripts que bien plus tard. Chargés à partir d'autres sources comme les CDN et les référentiels de code, les scripts ne sont généralement pas envoyés directement du site Web vers le navigateur, ce qui les rend difficiles à détecter et à arrêter avec les outils et les pratiques actuels.

Exemple : attaque contre la chaîne logistique de British Airways

En 2018, une attaque sur la chaîne logistique de British Airways s'est soldée par le vol des données de 380 000 à 500 000 clients. Les personnes concernées se sont vu dérober leurs informations personnelles et leurs informations de paiement.

C'était l'une des attaques Magecart les plus importantes à avoir jamais eu lieu. Spécialisé dans le vol de données bancaires en ligne, le groupe Magecart s'était fait connaître en 2016. Ses membres injectaient des scripts conçus pour dérober les données des formulaires de paiement en ligne, qu'ils utilisaient eux-mêmes ou qu'ils vendaient à d'autres cybercriminels par la suite.

Dans le cas de British Airways, le groupe Magecart a modifié un morceau de code JavaScript appelé Modernizr, utilisé dans les applications sur le Web et mobiles de l'entreprise. Dans ce script, ils ont incorporé une petite fonctionnalité qui s'exécutait à la fin du script. Une fois exécutée, cette fonctionnalité collectait les données saisies dans le formulaire de paiement et les transmettait à un site Web tiers exploité par le groupe criminel. Cette opération a entraîné une exfiltration de données massive et a valu à British Airways une amende de 20 millions de livres sterling, la plus lourde infligée jusque-là au Royaume-Uni (minorée par rapport au montant initial de 183,39 millions de livres sterling, en raison de l'impact économique de la pandémie sur les compagnies aériennes et le secteur du tourisme).

Clients touchés par **la violation de données**

380-500K

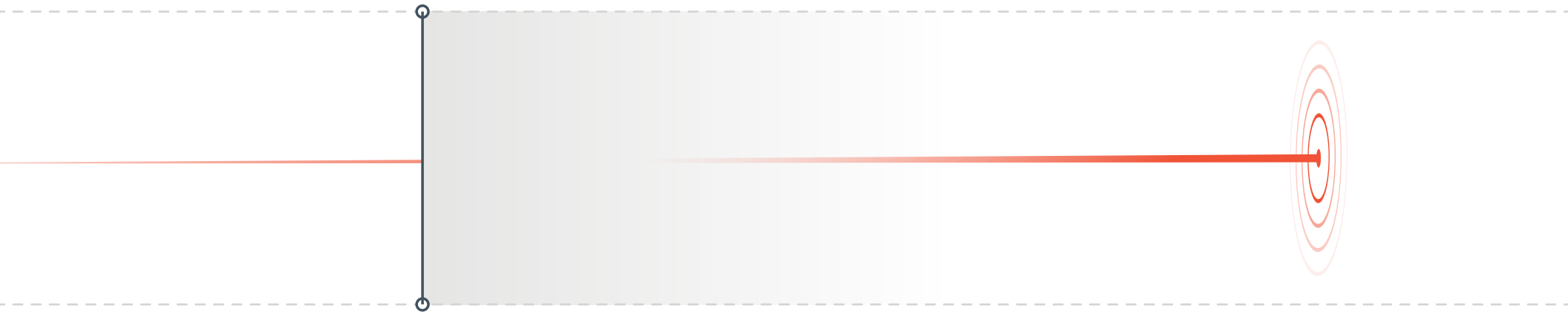
British Airways condamné **à une amende de**

20M de livres sterling

Exemple : Visa met en garde contre un skimmer en ligne

En septembre 2020, Visa mettait en garde contre Baka, un nouveau skimmer en ligne conçu pour mener des attaques côté client et doté de mécanismes intéressants pour éviter la détection. Le skimmer se chargeait dynamiquement dans la mémoire de la machine client au moment de l'exécution, ce qui le rendait indétectable par un balayage ou une inspection de page classique. Conçu pour s'exécuter uniquement en mémoire, il ne laissait aucune trace dans le stockage du navigateur. Ses créateurs ont tout mis en œuvre pour le chiffrer entièrement et empêcher sa détection lorsqu'il s'exécutait sur un site Web ou une application.

Au moment de la notification, le skimmer, manifestement conçu pour échapper à la détection aussi longtemps que possible, était utilisé activement dans de nombreuses boutiques en ligne.



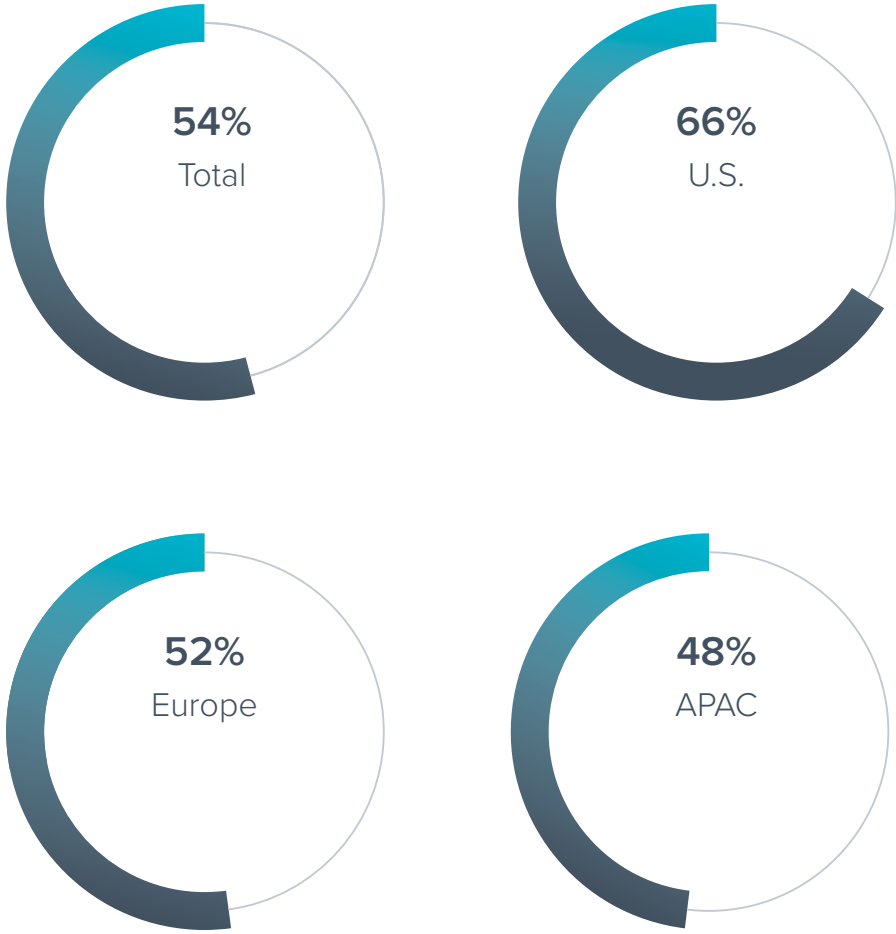
Ce qu'en disent les spécialistes en sécurité des applications

L'intégration de scripts tiers dans une application Web est monnaie courante et les méthodes utilisées par les entreprises pour les délivrer aux navigateurs varient.

Une fois de plus, rester efficace est primordial dans le développement d'applications, comme l'indique l'étude menée récemment par Barracuda auprès des spécialistes en sécurité des applications. En effet, plus de la moitié des entreprises utilisent des scripts tiers prêts à l'emploi pour créer leurs applications sur le Web. L'utilisation de code tiers peut poser de véritables problèmes de sécurité, surtout lorsque le code est transmis directement au navigateur depuis une plateforme source comme GitHub. Si le code a été altéré, il se peut qu'une attaque sur la chaîne logistique logicielle, comme Magecart, se prépare. Les entreprises ont tout intérêt à rester vigilantes face aux risques inhérents à cette approche du développement d'applications.

De manière approximative, quel pourcentage des applications Web de votre entreprise a recours à des scripts tiers ?

(n=750)

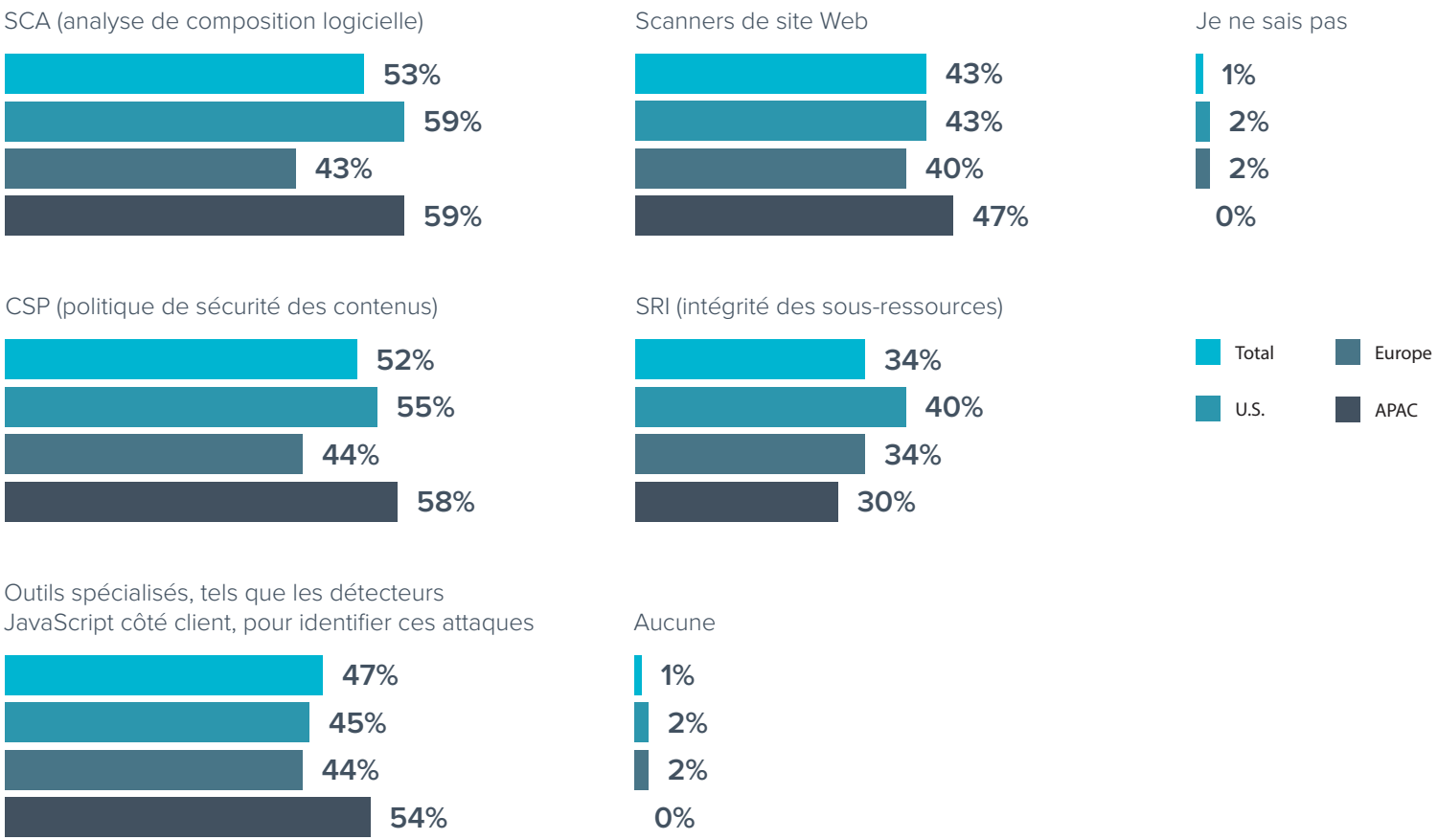


Barracuda

Des mesures de protection relativement standard sont en place pour réduire les attaques contre les chaînes logistiques. Selon les personnes interrogées, la région APAC a davantage recours à des outils spécialisés, comme les écouteurs JS côté client, pour identifier des attaques. Ces écouteurs s'avèrent plus efficaces que les scanners de site Web pour détecter les attaques avancées. En effet, même si les scanners de site Web représentent la quatrième technologie la plus utilisée sur cette liste, ils sont facilement déjoués comme le prouve le skimmer Baka détecté par Visa. La technologie SRI (intégrité des sous-ressources) est quant à elle compliquée à configurer et à entretenir, ce qui pourrait expliquer sa faible popularité.

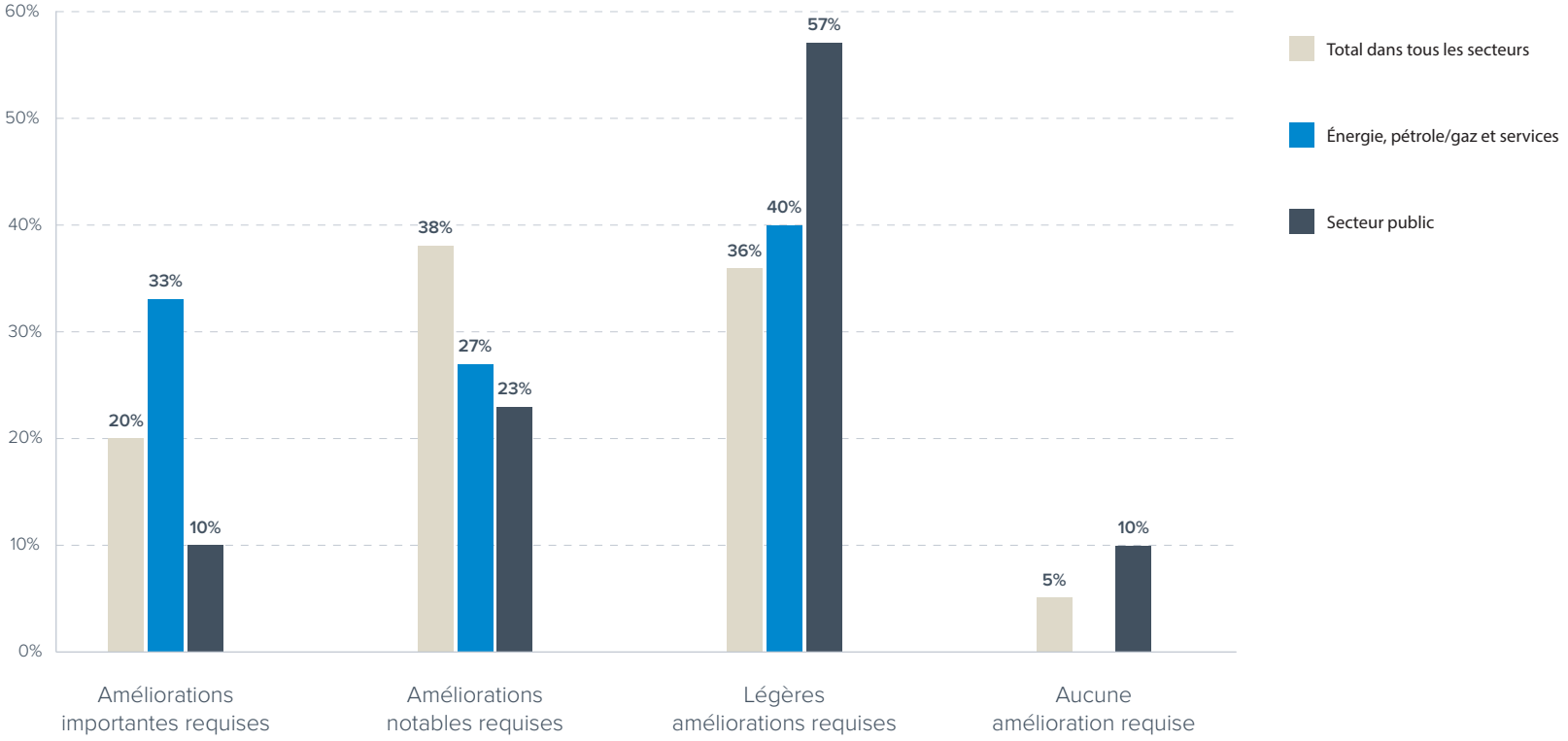
Quelles technologies votre entreprise utilise-t-elle pour se protéger des attaques contre la chaîne logistique logicielle ?

(n=750)



Selon vous, quel niveau d'amélioration est nécessaire dans votre entreprise en matière de défense contre les attaques de la chaîne logistique logicielle ?

(n=728)



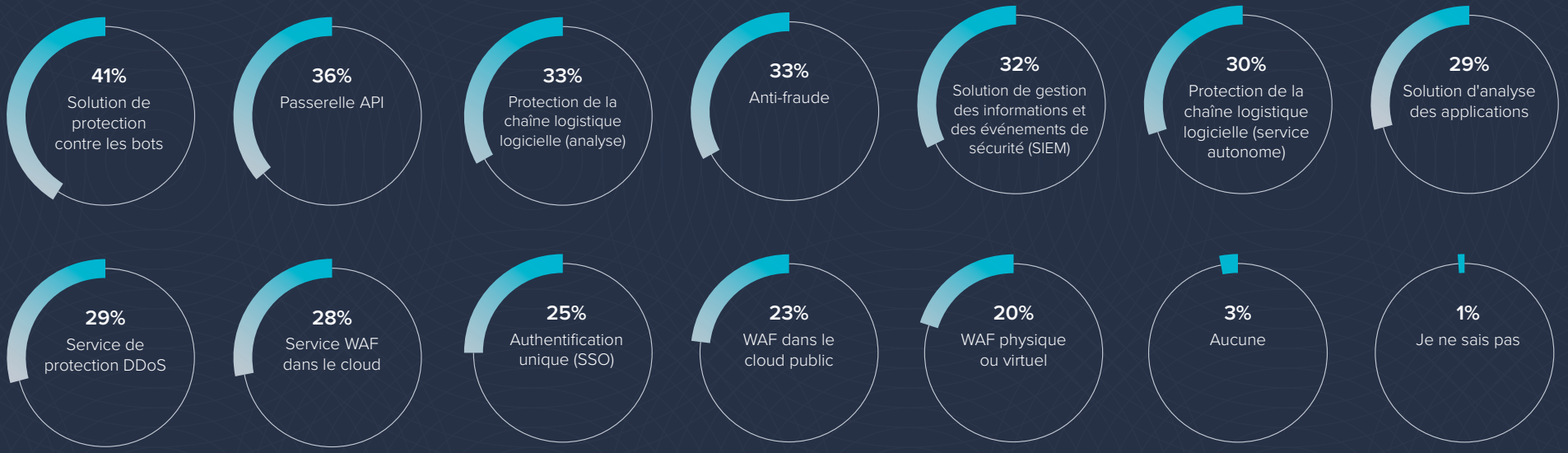
La plupart des entreprises sont partagées en ce qui concerne les améliorations à apporter à leur chaîne logistique Web. Les personnes interrogées au sein du secteur public semblent convaincues que peu d'améliorations (voire aucune) sont nécessaires pour renforcer leur protection. Seuls les secteurs de l'énergie, du pétrole, du gaz et des services estiment que d'importantes améliorations sont nécessaires. Cela s'explique par l'apparition relativement récente de ce vecteur d'attaque ainsi que par une sous-estimation de son impact. Plus ces attaques seront dévoilées au grand jour, plus on comprendra le danger qu'elles représentent.

Conclusion : se préparer aux nouvelles règles ABC de sécurité des applications

Les entreprises se font de plus en plus attaquer par le biais de leurs applications Web et de leurs API. Face au développement foisonnant des nouvelles technologies, les acteurs malveillants cherchent sans cesse à contourner les mesures de sécurité. Les API, les attaques de bots et les attaques côté client font partie des tactiques les plus récentes mises au point afin de pirater les applications pour le plaisir et le profit.

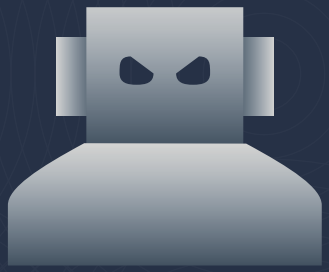
Parmi les solutions suivantes, laquelle sera déployée par votre entreprise l'année prochaine ?

(n=750)



Notre étude laisse penser que les entreprises en ont pris conscience, puisqu'elles sont nombreuses à envisager le déploiement de nouvelles solutions au cours de l'année à venir : protection contre les bots (41 %), passerelle API (36 %) et protection de la chaîne logistique logicielle (analyse) (33 %).

La volonté de combler ces lacunes est en soi une bonne nouvelle mais plus les entreprises multiplient les solutions, plus la sécurité de leurs applications devient un enjeu complexe. Seule une plateforme conçue pour protéger les clients contre tous ces vecteurs d'attaques constitue une solution de sécurité des applications efficace. En effet, cette approche garantit une protection maximale contre les menaces, qu'elles soient classiques ou émergentes, tout en restant simple à utiliser et à gérer.



Barracuda en quelques mots

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 plus d'informations, visitez le site barracuda.com

Barracuda