SOTI

V10 NUMÉRO 01

10 YEARS
OF SECURITY INSIGHT

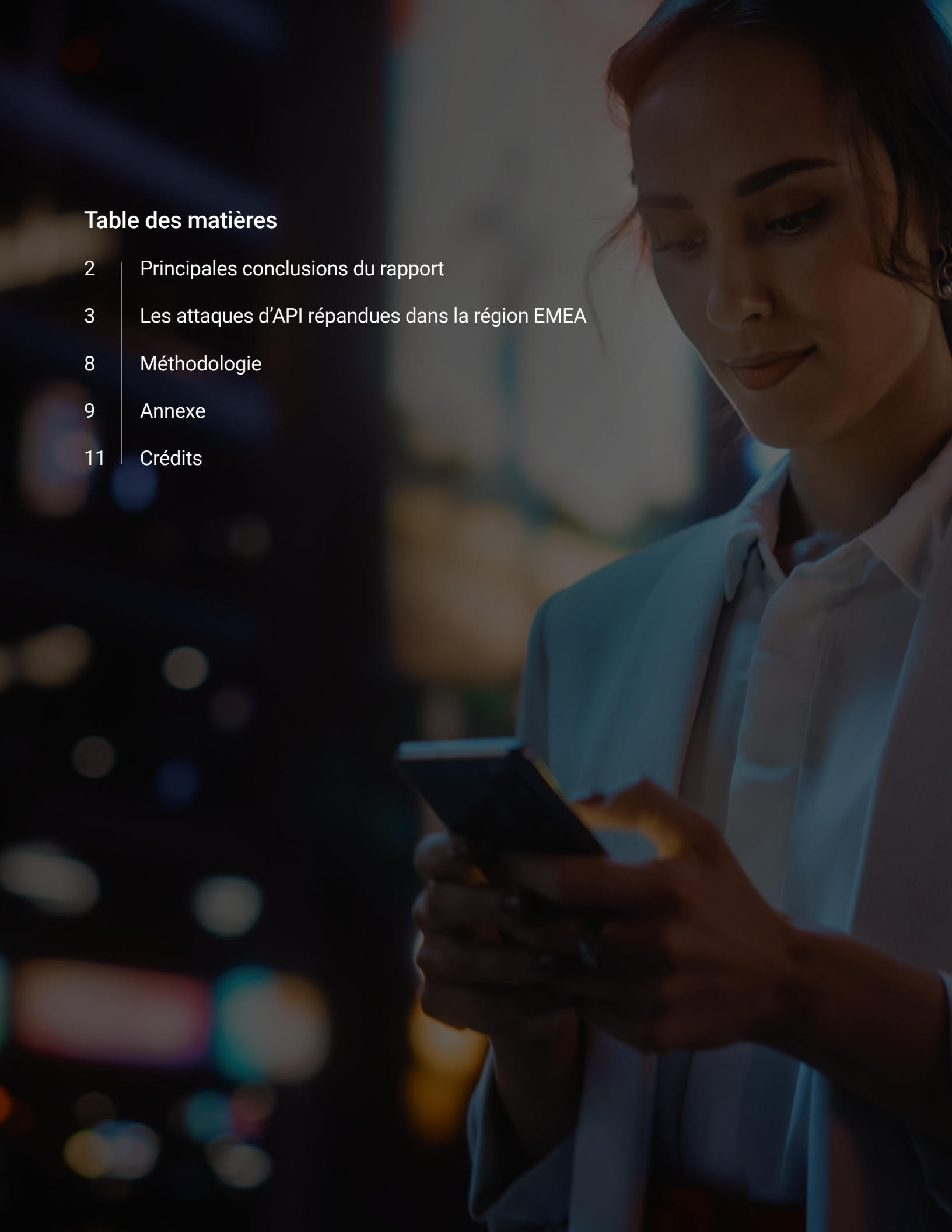
Coup de projecteur sur les menaces ciblant les API

Vue d'ensemble de la zone EMEA

Akamai

État des lieux d'Internet/Sécurité

Table des matières



Principales conclusions du rapport

La vue d'ensemble de la zone EMEA vient compléter notre rapport État des lieux d'Internet plus général sur la sécurité des API, intitulé De l'ombre à la lumière : coup de projecteur sur les menaces ciblant les API (disponible en anglais uniquement). Consultez ce rapport pour savoir comment les pirates exploitent les vecteurs d'attaque évoqués dans cette vue d'ensemble, obtenir des recommandations afin de protéger votre entreprise, et comprendre nos méthodologies de recherche ainsi que notre nouvel ensemble de données.

Présentation

À mesure que l'innovation digitale et l'économie des API améliorent l'expérience des collaborateurs et des clients, elles offrent également aux cybercriminels de nouvelles opportunités d'exploitation. Les attaques ciblant les API peuvent porter atteinte aux résultats financiers, à l'image de marque et à la réputation d'une entreprise. Elles peuvent également lui faire perdre des données confidentielles et la confiance des clients. Les API étant de plus en plus utilisées pour échanger des informations financières sensibles, le volume d'attaques d'API va augmenter fortement, de même que les contrôles réglementaires et les exigences en matière de déclaration. La sécurité des API est donc plus importante que jamais.

Pour mieux comprendre l'écosystème des menaces ciblant les API, au lieu d'examiner les attaques d'applications Web et d'API dans leur ensemble, nous utilisons en 2024 un nouvel ensemble de données qui permet aux chercheurs d'Akamai de distinguer ces deux types d'attaques et de se concentrer sur le pourcentage d'attaques ciblant les API. Dans cette vue d'ensemble de la zone EMEA, qui couvre les 12 mois de janvier à décembre 2023, nous analysons les tendances des attaques et leurs conséquences pour vous.

- À l'échelle mondiale, la région Europe, Moyen-Orient et Afrique (EMEA) affichait le pourcentage le plus élevé d'attaques Web ciblant les API (47,5 %), nettement supérieur à la région classée en 2ème position, l'Amérique du Nord (27,1 %).
- Conformément à la tendance mondiale, les attaques par protocole HTTP et injection SQL (SQLi) ont été les principaux vecteurs d'attaque d'API dans la zone EMEA au cours des 12 derniers mois.
- Les requêtes de bots sont également un sujet de préoccupation : 40 % des près de 4 000 milliards de requêtes de bots suspectes ciblaient les API.
- Dans le secteur du commerce, près des trois quarts (74,6 %) de toutes les attaques Web ayant touché les entreprises étaient des attaques d'API, soit plus de deux fois le pourcentage du secteur le plus proche, la haute technologie (35,5 %).

Les attaques d'API répandues dans la région EMEA

En exploitant un nouvel ensemble de données qui suit spécifiquement le trafic des attaques d'API, une étude d'Akamai a révélé que la région EMEA affichait le pourcentage le plus élevé d'attaques d'API au niveau mondial, soit 47,5 %, dépassant de loin la région classée en 2ème position, l'Amérique du Nord, avec 27,1 % (Figure 1 zone EMEA). Ces chiffres reposent sur le nombre total d'attaques Web dans chaque région et montrent que les API sont plus en danger dans la zone EMEA que dans d'autres régions.

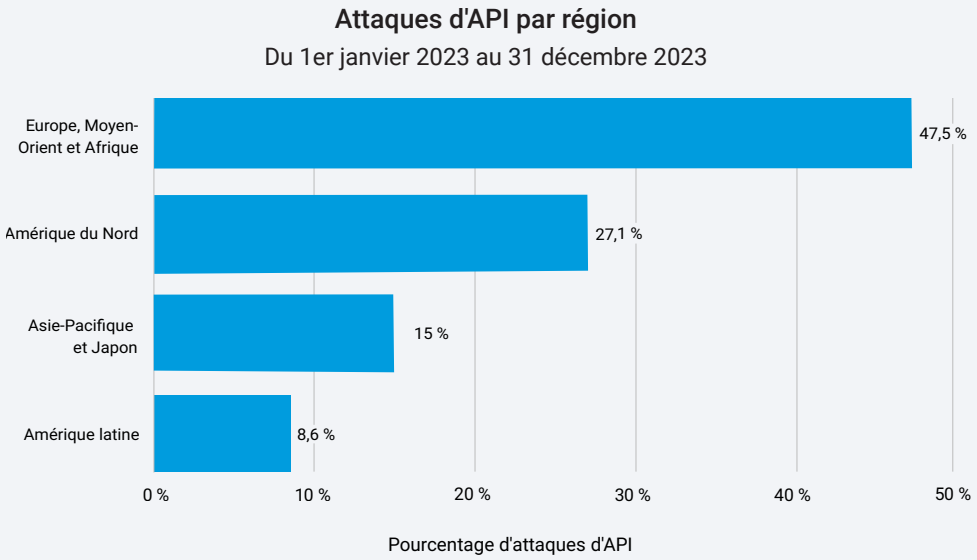


Fig. 1 zone EMEA : Les attaques Web sont nettement plus susceptibles de cibler les API dans la zone EMEA que dans toute autre région

Ce pourcentage relativement élevé d'attaques dans la zone EMEA (comparé au pourcentage d'attaques dans d'autres régions) peut être en partie attribué à l'importance du marché des API ouvertes par rapport à l'Amérique du Nord et à la région Asie-Pacifique, avec un taux d'adoption des API plus élevé dans la zone EMEA, ainsi qu'à l'ouverture des opérations bancaires et à la norme de sécurité de l'industrie des cartes de paiement (Payment Card Industry Data Security Standard ou PCI DSS) v4.0, qui stimulent l'utilisation des API et peuvent introduire les risques de sécurité mentionnés dans le rapport mondial.

Au sein de la zone EMEA, les pays affichant le pourcentage le plus élevé d'attaques Web ciblant les API sont l'Espagne (94,8 %), le Portugal (84,5 %), les Pays-Bas (71,9 %) et Israël (67,1 %). Cela ne signifie pas que le nombre d'attaques Web est globalement plus élevé dans ces pays que dans d'autres de la zone EMEA, mais plutôt que ces pays sont confrontés à un risque beaucoup plus concentré d'exploitations d'API en raison de l'importance que les pirates accordent à ce vecteur.

Les tendances mensuelles observées entre janvier et décembre 2023 montrent que les attaques Web ciblant les API dans la zone EMEA ont augmenté de manière assez régulière, passant de 34 % en janvier à 41 % à la fin de l'année (Figure 2 zone EMEA). Des exceptions ont eu lieu en mars et avril, où les chercheurs d'Akamai ont constaté un pic d'attaques d'API alors que le secteur du commerce en Espagne, un pays où la concentration d'attaques d'API était déjà importante, a connu des attaques ciblées à grande échelle. Ce pic montre à quelle vitesse les attaquants peuvent se concentrer sur des régions et des secteurs spécifiques. Il est donc utile de suivre les tendances plus globales.

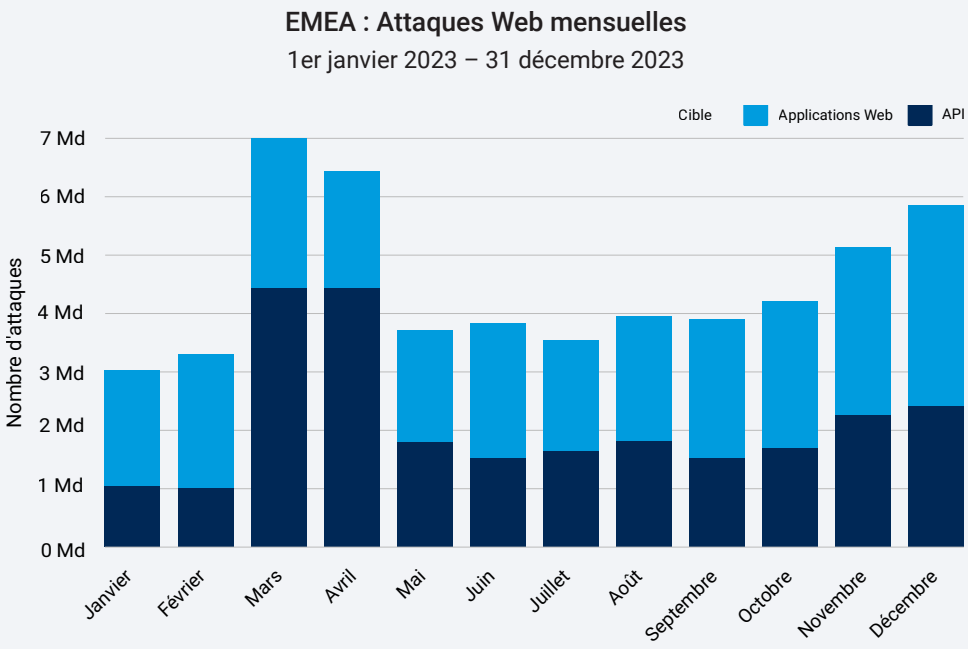


Fig. 2 zone EMEA : À l'exception des mois de mars et d'avril, où les attaques d'API ont connu un pic, les attaques d'API ont augmenté lentement tout au long de 2023, atteignant 41 % de l'ensemble des attaques à la fin de l'année

Attaques d'API dans les autres secteurs

Au cours de la période de référence, les chercheurs d'Akamai ont constaté que le secteur du commerce affichait le pourcentage le plus élevé d'attaques Web ciblant les entreprises (74,6 %), soit plus de deux fois le pourcentage du deuxième secteur le plus touché, le secteur des hautes technologies (35,5 %). Arrivent ensuite les jeux vidéo, à 28,7 %, les services aux entreprises, à 24,5 % et les autres médias digitaux, à 19,7 % (Figure 3 zone EMEA).

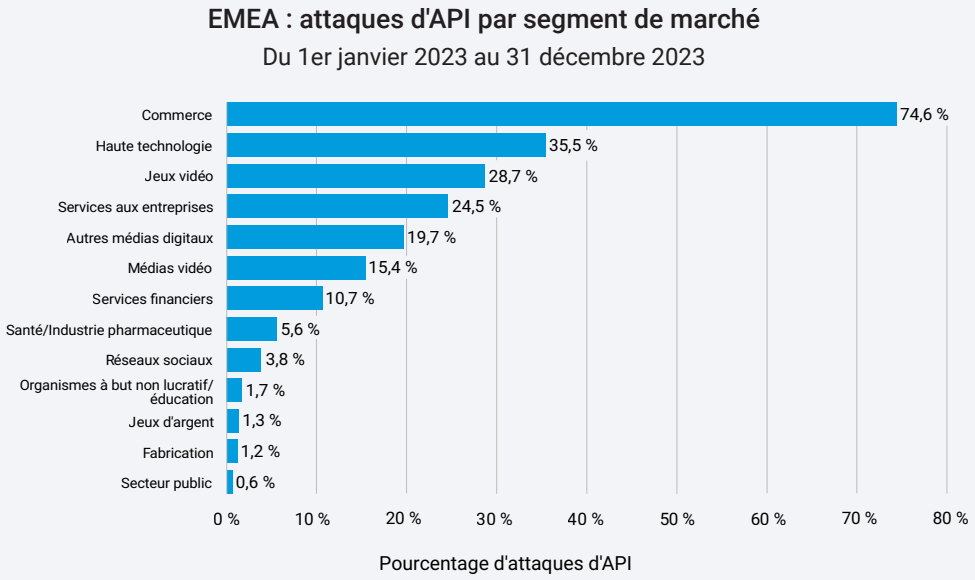


Fig. 3 zone EMEA : Le segment de marché du commerce a connu le pourcentage le plus élevé d'attaques d'API, en partie en raison de la nature complexe de son écosystème, de sa forte dépendance aux API et des données précieuses que les entreprises de ce secteur possèdent

API attaquées : analyse du trafic

Conformément à la tendance mondiale, les vecteurs HTTP et SQLi ont été les principaux moyens par lesquels les pirates ont ciblé les API dans la zone EMEA au cours des 12 derniers mois, et l'inclusion de fichiers locaux (LFI) est descendue dans la liste par rapport à sa prédominance dans les attaques d'applications Web (Figure 4 zone EMEA).

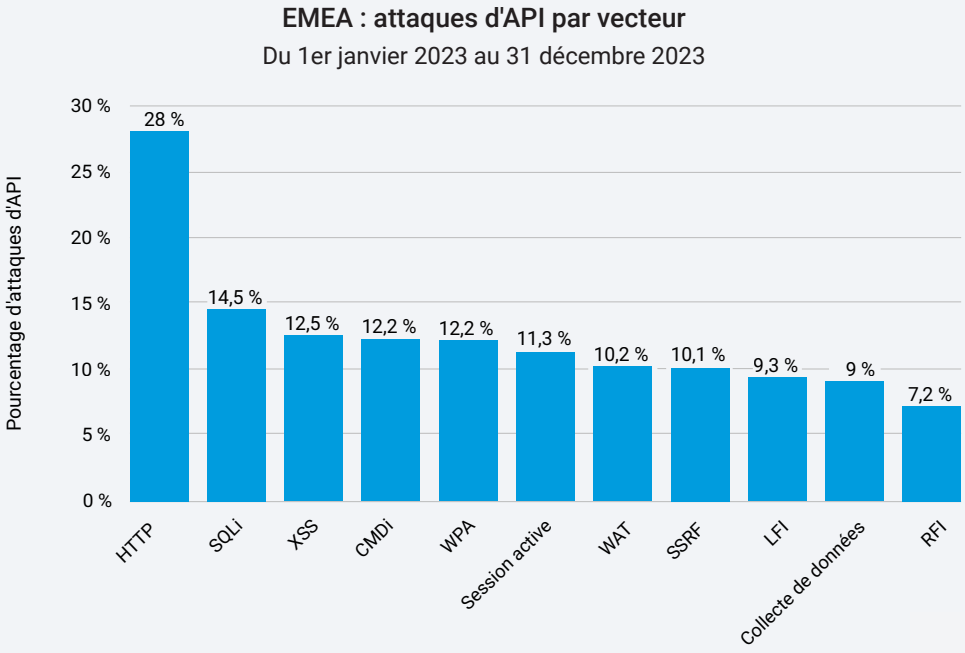


Fig. 4 zone EMEA : Les vecteurs HTTP, SQLi et XSS sont les plus pertinents pour les attaques d'API. La LFI est moins répandue pour les attaques d'API, mais toujours activement utilisée pour les attaques contre les applications Web

Dans la région EMEA, le cross-site scripting (XSS) reste une technique privilégiée même pour les attaques d'API, tout comme l'injection de commande (CMDi). Notre nouvel ensemble de données nous permet de surveiller des vecteurs d'attaque supplémentaires pour les API. Par exemple, la falsification des requêtes côté serveur (SSRF, que nous avons évoquée dans notre rapport 2023) est aujourd'hui un vecteur prometteur. (Voir l'annexe pour une liste complète des définitions de vecteurs d'attaque.)

Nos recherches ont également révélé que les requêtes de bots étaient une source de préoccupation. Sur la même période de 12 mois, 40 % des près de quatre mille milliards de requêtes de bots suspectes ont visé des API.

Conclusion

Défendre les API est une nécessité absolue du point de vue de la sécurité et de la gestion des risques. En outre, les lois et réglementations existantes, ainsi que les réformes à venir visant à adapter la législation en matière de cybersécurité à l'écosystème des menaces rendent également la protection des API indispensable.

Par exemple, le Règlement général sur la protection des données (RGPD) de l'Union européenne privilégie la protection des données personnelles, et les API sont désormais le principal moyen par lequel ces données sont utilisées et partagées. En outre, la nouvelle directive sur la sécurité des réseaux et de l'information (NIS2) appelle spécifiquement à la mise en place d'un solide programme de sécurité des API. En dehors de l'UE, des pays tels que l'Arabie saoudite ont quant à eux adopté des lois sur la protection des données similaires au RGPD de l'UE, qui impose des obligations aux entités traitant des données personnelles. De plus, l'article 6 de la norme de sécurité de l'industrie des cartes de paiement (PCI DSS) v4.0 inclut spécifiquement de nouvelles normes sur l'utilisation des API dans le développement et la maintenance des systèmes et des logiciels, afin de réduire le risque de compromission des données.

Alors que les régulateurs adoptent des initiatives et des politiques visant à renforcer les normes de cybersécurité pour les API, il est important de comprendre les meilleures pratiques et les directives afin d'intégrer les API à votre programme de sécurité pour améliorer la visibilité, renforcer les défenses et respecter les exigences de conformité.

Pour en savoir plus, nous vous invitons à consulter notre rapport État des lieux d'Internet sur la sécurité des API intitulé « De l'ombre à la lumière : coup de projecteur sur les menaces ciblant les API ».

Méthodologie

Attaques des applications Web et par bots

Ces données décrivent les alertes de la couche applicative sur le trafic vu à travers notre pare-feu d'application Web (WAF) et notre outil de gestion des bots. Les alertes d'attaque des applications Web sont déclenchées lorsque nous détectons une charge utile malveillante dans une requête adressée à un site Web, à une application ou à une API protégée. Les alertes de bots sont déclenchées lorsque nous détectons une charge utile de bot dans une requête adressée à un site Web, à une application ou à une API protégé(e). Ces alertes de bot peuvent être déclenchées par des bots malveillants et inoffensifs. En revanche, elles n'indiquent pas si ces attaques sont fructueuses. Bien que ces produits permettent un haut niveau de personnalisation, nous avons recueilli les données présentées ici d'une manière qui ne tient pas compte des configurations personnalisées des propriétés protégées. Les données sont issues d'un outil interne d'analyse des événements de sécurité détectés sur Akamai Connected Cloud, un réseau mondial s'étendant sur plus de 4 000 points de terminaison dans plus de 130 pays. Nos équipes de sécurité utilisent ces données, qui se mesurent en pétaoctets par mois, pour étudier les attaques, signaler des comportements malveillants et fournir des informations supplémentaires aux solutions Akamai.

Les données de ce rapport couvrent une période de 12 mois, du 1er janvier 2023 au 31 décembre 2023.

Mise à jour des données 2024

Nous sommes heureux d'annoncer plusieurs mises à jour de nos ensembles de données pour notre 10e anniversaire ! Nos ensembles de données sur les attaques d'applications Web et de bots ont reçu plusieurs mises à jour. Leur méthode de collecte a été repensée, simplifiée et optimisée. La diversité et le niveau de détails de nos informations ont été améliorés. Des classifications pour d'autres vecteurs d'attaque, tels que la SSRF, ont été ajoutées. L'identification des attaques ciblant les points de terminaison API a également été ajoutée à chaque ensemble de données. Nous sommes ravis de présenter certaines de ces nouvelles améliorations dans ce rapport, et continuerons à partager ces mises à jour avec nos lecteurs tout au long de l'année (et au-delà), qui marque les dix ans de notre série de rapports État des lieux d'Internet/Sécurité.

Informations d'API Security

Nous remercions tout particulièrement notre équipe Akamai API Security Solution Engineering pour ses informations concrètes sur les risques liés aux API et leur impact potentiel d'après nos alertes de sécurité d'API.

Annexe

Vecteur d'attaque	Définition
Session active	Un trafic d'attaques a récemment été signalé pour le client et les requêtes répétées seront bloquées pendant la durée de la session.
Injection de commande (CMDi)	Un pirate injecte de nouveaux éléments dans une commande existante pour en modifier l'interprétation prévue et accomplir les actions de son choix.
Cross-site scripting (XSS)	Un pirate intègre des scripts malveillants au contenu de sorte que le logiciel cible exécute les scripts avec les niveaux de privilège des utilisateurs lorsque le contenu est distribué aux navigateurs Web.
Collecte de données	Un pirate exploite les failles de conception ou de configuration de la cible et de ses communications pour lui faire révéler plus d'informations que prévu. Cette opération vise souvent à collecter des données pour préparer un autre type d'attaque, mais l'accès aux informations peut également être l'objectif final du pirate.
Protocole HTTP (HTTP)	Un pirate profite des faiblesses du protocole de communication entre un client et un serveur pour effectuer des actions inattendues. L'exploitation de différents types de protocoles peut mener à des objectifs finaux différents pour les attaques.
Inclusion de fichiers locaux (LFI)	Un pirate manipule des entrées dans le logiciel cible pour accéder à, voire modifier, des zones du système de fichiers qui n'étaient pas censées être accessibles.

Vecteur d'attaque	Définition
Inclusion de fichiers distants (RFI)	Le pirate charge et exécute du code arbitraire à distance, détournant ensuite l'application ciblée et la forçant à exécuter ses propres instructions.
Falsification de requête côté serveur (SSRF)	Le pirate abuse des fonctionnalités du serveur pour lire ou mettre à jour des ressources internes.
Injection SQL (Structured Query Language, SQLi)	Un attaquant crée des chaînes d'entrée de sorte que, lorsque le logiciel cible tente de construire des instructions SQL basées sur les entrées des utilisateurs, l'instruction SQL résultante exécute les actions souhaitées par l'attaquant. En cas de réussite, l'injection peut entraîner la divulgation d'informations, ainsi que la possibilité d'ajouter ou de modifier des données dans la base de données.
Outil d'attaque Web (WAT)	Le pirate sonde activement la cible de manière à solliciter des renseignements qui pourraient être exploités à des fins malveillantes. Grâce à ces sondes, il peut obtenir des informations sur la cible qui lui permettent de tirer des conclusions sur sa sécurité, sa configuration ou ses vulnérabilités potentielles.
Attaque de plateforme Web (WPA)	Attaque contre une plateforme logicielle (couche cloud, Web ou applicative) n'étant pas classée dans un autre groupe d'attaques.

Crédits

Édition et rédaction

Badette Tribbey – Rédactrice en chef
Charlotte Pelliccia – Rédactrice principale (régions)

Contributeurs éditoriaux

James Casey
Edward Roberts
Steve Winterfeld

Révision et expertise

Tom Emmons
Reuben Koh
Rob Lester
Richard Meeus
Abigail Ojeda
Menachem Perlman
Yariv Shivek

Analyse des données

Chelsea Tuttle

Marketing et publication

Georgina Morales Hampe
Emily Spinks

Autres rapports État des lieux d'Internet/Sécurité

Lisez les numéros précédents et surveillez les prochaines parutions du célèbre rapport État des lieux d'Internet/Sécurité d'Akamai, **akamai.com/soti**

D'autres recherches sur les menaces d'Akamai

Tenez-vous au courant des dernières analyses d'informations sur les menaces, des rapports de sécurité et des recherches sur la cybersécurité sur **akamai.com/threatresearch**

Accéder aux données de ce rapport

Consultez des versions de haute qualité des graphiques et des tableaux référencés dans ce rapport. Ces images sont libres d'utilisation et de référence, à condition qu'Akamai soit dûment crédité en tant que source et que le logo Akamai soit conservé. **akamai.com/sotidata**

En savoir plus sur les solutions Akamai

Pour en savoir plus sur les solutions Akamai contre les attaques d'API, visitez notre **page sur la sécurité des applications et des API**.

Akamai protège votre expérience client, votre personnel, vos systèmes et vos données en vous aidant à intégrer la sécurité dans tout ce que vous créez, dans toutes vos conceptions et diffusions. La visibilité de notre plateforme sur les menaces mondiales nous aide à adapter et à faire évoluer votre stratégie de sécurité (activer Zero Trust, bloquer les ransomwares, sécuriser les applications et les API, ou lutter contre les attaques DDoS), vous donnant ainsi la confiance nécessaire pour innover, prospérer et ouvrir le champ des possibles. Pour en savoir plus sur les solutions de Cloud Computing, de sécurité et de diffusion de contenu, rendez-vous sur akamai.com et akamai.com/blog, ou abonnez-vous à Akamai Technologies sur X (anciennement Twitter) et LinkedIn.
Publication : 03/24.