V11 NUMÉRO 02

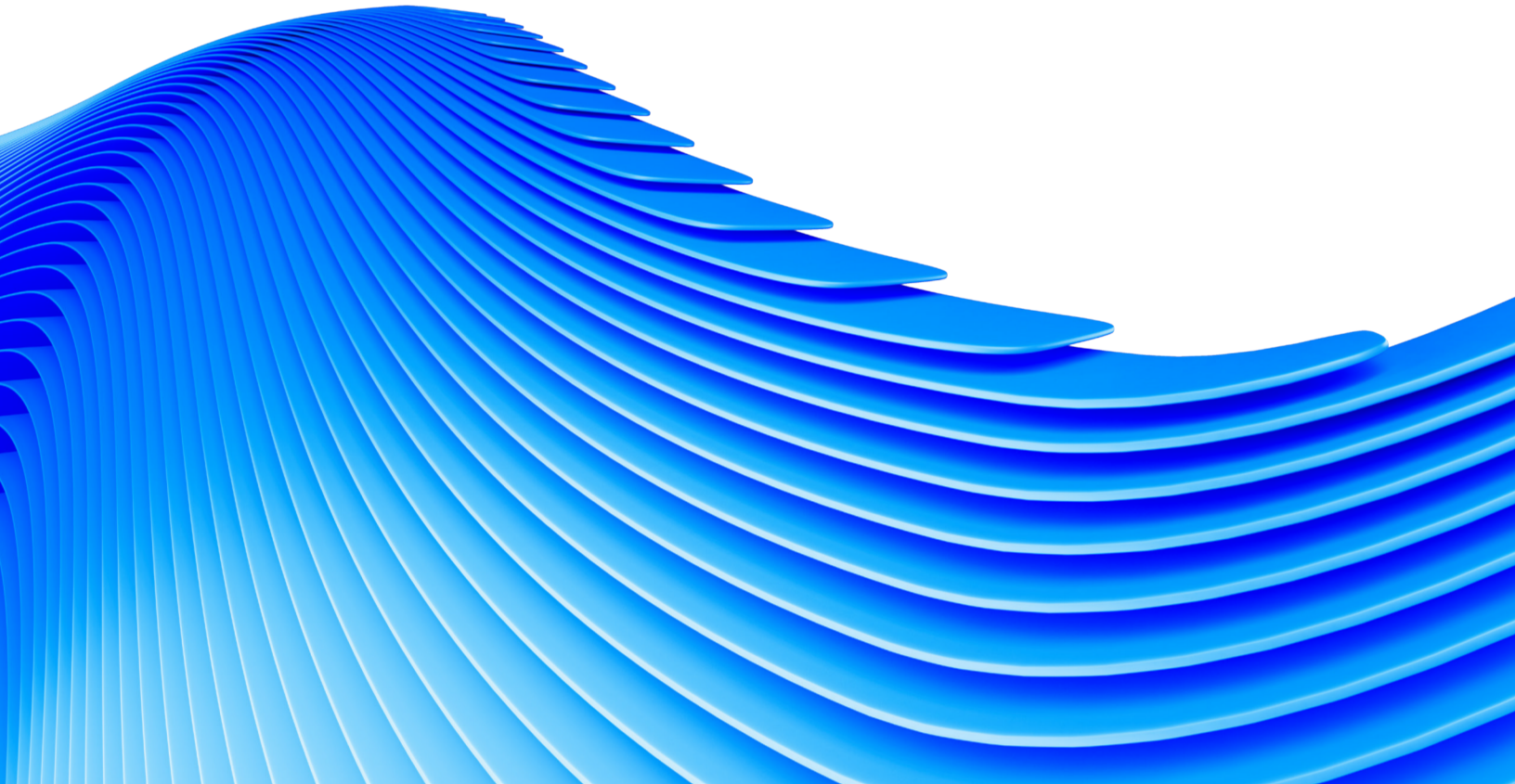
État des lieux de la sécurité des applications et des API en 2025

L'impact de l'IA sur le paysage digital

Akamai

État des lieux d'Internet/**Sécurité**

Contenu



Introduction

Au début de l'année 2025, le paysage de la sécurité des applications Web reflète une complexité et une sophistication sans précédent au niveau des vecteurs de menace. Les entreprises sont confrontées à une forte augmentation des attaques ciblant les applications Web. En 2024, Akamai a observé plus de 311 milliards d'attaques ciblant les applications Web et les API, ce qui représente une augmentation de 33 % par rapport à l'année précédente. Cette hausse est directement liée à l'adoption accélérée des services cloud, des architectures de microservices et des applications basées sur l'intelligence artificielle (IA). Les facteurs géopolitiques ont accentué d'autant plus cette tendance. En effet, les secteurs des hautes technologies, du commerce et des réseaux sociaux enregistrent le plus grand nombre d'attaques par déni de service distribué (DDoS) de couche 7 (couche applicative). Plus particulièrement, les cybercriminels déploient désormais des chaînes d'attaque générées par l'IA qui automatisent l'ensemble du cycle de vie des attaques.

Dans le même temps, les API sont devenues les cibles principales : entre janvier 2023 et décembre 2024, Akamai a dénombré plus de 150 milliards d'attaques ciblant les API. L'intégration d'outils SaaS (logiciel en tant que service) basés sur l'IA aux plateformes principales, via des API, a considérablement étendu la surface d'attaque. Cette situation soulève de lourdes implications financières : les problèmes liés à la sécurité des API coûtent actuellement aux entreprises près de 87 milliards de dollars par an, et, en l'absence de mesure adéquate, les analystes estiment que ce chiffre pourrait dépasser 100 milliards de dollars d'ici 2026. Dans des écosystèmes d'API de plus en plus complexes, les API fantômes et zombies constituent des vecteurs d'attaque particulièrement vulnérables.

Le rôle de l'IA dans la sécurité des applications Web et des API

L'IA transforme à la fois les environnements de sécurité des applications Web et des API en améliorant les capacités de détection et de réponse aux menaces, tout en introduisant de nouveaux défis. Dans les applications Web, l'IA est utilisée pour automatiser la détection des menaces, prédire les violations potentielles et améliorer les temps de réponse aux incidents. Cependant, l'intelligence artificielle permet également aux pirates de générer des logiciels malveillants pilotés par l'IA, d'élaborer des méthodes d'extraction Web sophistiquées et d'automatiser le cycle de vie des attaques à l'aide de méthodes d'attaque dynamiques.

En ce qui concerne les API, l'IA joue un rôle crucial dans la gestion et la sécurisation d'un très grand nombre d'interactions. Les outils optimisés par l'IA sont essentiels pour détecter les anomalies, identifier les schémas d'utilisation abusive et automatiser les réponses aux menaces en temps réel. La gestion des API basée sur l'IA continuera d'évoluer en intégrant des analyses prédictives et des mesures de sécurité automatisées pour se protéger contre des attaques de plus en plus sophistiquées. Malgré ces progrès, les attaques pilotées par l'IA visant les API, telles que le « credential stuffing » et les attaques de logique métier, restent une préoccupation majeure qui nécessite des cadres de sécurité robustes pour contrer efficacement ces menaces.

Des stratégies différentes mais interdépendantes pour contrer les attaques ciblant les applications Web et les API

Bien qu'elles soient liées, les attaques d'applications Web et les attaques d'API ciblent différents aspects de l'infrastructure applicative :

- **Les attaques d'applications Web** ciblent les composants d'applications Web liés à l'expérience utilisateur, tels que les pages de connexion, et elles recourent souvent à des techniques moins élaborées.
- **Les attaques d'API** visent à exploiter les vulnérabilités présentes dans les points de terminaison API et la logique back-end d'une application, ce qui nécessite une compréhension plus approfondie de la structure et du comportement de l'API.

Les principales différences résident dans leur surface d'attaque et leur complexité. Les attaques d'applications Web ciblent généralement les parties visibles d'une application, tandis que les attaques d'API exploitent les canaux de communication entre les différents composants logiciels. Cependant, si elles arrivent à leurs fins, ces deux attaques peuvent fournir un accès non autorisé aux données sensibles et aux ressources système.

Il est essentiel de comprendre les mesures de cybersécurité applicables à la fois aux attaques ciblant les applications Web et les attaques ciblant les API, car les fonctionnalités des applications actuelles s'appuient de plus en plus sur les API. Les entreprises s'attendent à une augmentation de 39 % du nombre d'applications Web d'ici deux ans, ce qui explique pourquoi l'interdépendance entre la sécurité Web et la sécurité des API est de plus en plus forte. Négliger l'un des deux aspects peut exposer une entreprise à des attaques sophistiquées et multivectorielles qui exploitent les vulnérabilités du front-end et du back-end des applications.

La perspective unique d'Akamai : découvrir les modèles de menaces

Pour relever ces défis complexes, Akamai bénéficie de son infrastructure réseau, qui traite plus d'un tiers du trafic Web mondial, offrant ainsi une visibilité inégalée sur les modèles de menaces. Cette perspective, combinée aux informations rassemblées par ses équipes de recherche et de science des données, permet à Akamai de fournir des renseignements complets et exploitables. Les conclusions de ces recherches offrent aux responsables de la sécurité les informations stratégiques nécessaires pour prendre les bonnes décisions. Elles leur permettent de se concentrer sur les domaines où il convient de réduire les risques afin d'optimiser le retour sur investissement en matière de sécurité.

Principales conclusions du rapport

Les API basées sur l'IA sont moins sécurisées que leurs homologues.

La majorité des API basées sur l'intelligence artificielle (IA) sont accessibles en externe et beaucoup dépendent de mécanismes d'authentification inadaptés, une faille aggravée par le nombre croissant d'attaques pilotées par l'IA qui visent ces API.

L'IA alimente les avancées techniques des acteurs malveillants.

Cela inclut des progrès tels que les logiciels malveillants pilotés par l'IA, l'analyse des vulnérabilités, les attaques sur les systèmes intégrant l'IA et les capacités sophistiquées d'extraction Web.

32 %

Pourcentage d'augmentation du nombre d'incidents liés aux 10 principaux risques pour la sécurité des API selon l'OWASP

Les risques pour la sécurité des API ne cessent de se multiplier. En effet, la liste des 10 principaux risques pour la sécurité des API dressée par l'Open Worldwide Application Security Project (OWASP) révèle des failles d'authentification et d'autorisation qui exposent les fonctionnalités et données sensibles.

30 %

Hausse des alertes de sécurité liées au cadre de sécurité MITRE

Les pirates utilisent des techniques sophistiquées, notamment l'automatisation et l'IA, pour exploiter les API. Le cadre de sécurité MITRE permet d'identifier plus rapidement et plus précisément ces attaques.

33 %

Pourcentage d'augmentation des attaques Web d'une année sur l'autre, à l'échelle mondiale

L'augmentation des attaques est directement liée à l'adoption rapide des services cloud, des microservices et des applications d'IA, qui élargissent les surfaces d'attaque et posent de nouveaux défis en matière de sécurité.

+ de 230 milliards

Nombre d'attaques Web qui ciblent les entreprises commerciales, ce qui en fait le secteur d'activité le plus touché, avec près de trois fois plus d'attaques que le secteur des hautes technologies (qui arrive en deuxième position).

73 %

Augmentation du nombre total d'attaques Web d'une année sur l'autre dans la région APJ,

passant de 29 milliards en 2023 à 51 milliards en 2024.

37 %

Pourcentage d'attaques Web dans la région EMEA (Europe, Moyen-Orient et Afrique) qui ont ciblé des API,

ce qui représente la plus forte concentration de ces attaques parmi toutes les régions.

94 %

Croissance trimestrielle des attaques par déni de service distribué (DDoS) de couche 7

entre le premier trimestre 2023 et le quatrième trimestre 2024.

11 900 milliards

Nombre d'attaques DDoS de couche 7 qui ont ciblé l'Amérique du Nord

pendant une période de deux, entre le premier trimestre 2023 et le quatrième trimestre 2024.

7 000 milliards

Nombre d'attaques DDoS de couche 7 qui ont ciblé le secteur des hautes technologies

entre janvier 2023 et décembre 2024, ce qui en fait le secteur d'activité le plus touché.

7 400 milliards

Nombre d'attaques DDoS de couche 7 qui ont ciblé la région APJ

pendant une période de deux ans, entre le premier trimestre 2023 et le quatrième trimestre 2024.

20 %

Pourcentage d'attaques DDoS de couche 7 ciblant les API dans la région EMEA,

ce qui représente la plus forte concentration de ces attaques parmi toutes les régions.

Améliorer nos renseignements sur les menaces ciblant les API

Grâce à l'intégration de Noname Security, Akamai a considérablement amélioré nos capacités de recherche et de création de rapports sur les menaces ciblant les API, ce qui nous a permis de porter un tout nouveau regard sur les risques propres aux API. Akamai utilise ce nouvel ensemble de données (en phase initiale d'intégration des données) pour améliorer nos renseignements sur les menaces et élargir notre champ de vision sur les problèmes de sécurité des API.

Établir une correspondance entre les alertes et les cadres de sécurité

Au fil du temps, ce nouvel ensemble de données s'enrichira d'informations sur les alertes de sécurité, qui seront ensuite rapprochées des cadres de cybersécurité et normes de conformité essentielles, notamment :

- MITRE ATT&CK Framework (Adversarial Tactics, Techniques, and Common Knowledge)
- Règlement général sur la protection des données (RGPD)
- Normes de sécurité de l'industrie des cartes de paiement (PCI DSS)
- Organisation internationale de normalisation (ISO)
- Open Worldwide Application Security Project (OWASP)

Ces améliorations renforcent considérablement la capacité d'Akamai à fournir aux clients une protection robuste. En s'alignant sur ces cadres de sécurité, les entreprises peuvent mieux comprendre leur stratégie de sécurité, répondre aux exigences réglementaires et hiérarchiser efficacement leurs efforts en matière de sécurité. Cette approche complète permet aux entreprises d'allouer des ressources de manière stratégique et de développer des stratégies ciblées pour protéger leurs API et leurs données sensibles.

Analyse d'un échantillon de données sur 30 jours

Pour ce rapport, nous avons analysé un échantillon de données sur 30 jours afin de mettre en évidence l'activité générale des acteurs malveillants pour chaque cadre de cybersécurité et chaque norme de conformité (Figure 1). Nous fournissons également une perspective plus approfondie sur les alertes MITRE et OWASP. Nous cherchons enfin à évaluer l'impact potentiel de ces risques et incidents de sécurité sur les normes de conformité.

	Activité sur 30 jours	Augmentation mensuelle
OWASP	**5 907 000**	**32 %**
MITRE	**2 817 000**	**30 %**
ISO	**832 000**	**22 %**
RGPD	**669 000**	**21 %**
PCI DSS	**881 000**	**16 %**

Fig. 1 : Répartition des alertes de sécurité selon les cadres de sécurité et les normes de conformité

Alertes MITRE

Sur une période de 30 jours, nous avons observé une augmentation de 30 % des incidents liés aux techniques MITRE parmi nos clients. En particulier, les pirates ont fréquemment utilisé des comptes valides (T1078), en exploitant des identifiants légitimes pour obtenir un accès non autorisé aux systèmes ou aux réseaux. Étant donné que les API s'appuient souvent sur des jetons pour les autorisations, les cybercriminels qui obtiennent ces jetons peuvent accéder à des données sensibles sans être détectés.

Nous avons également identifié la technique T1566 (hameçonnage), qui consiste à lancer des campagnes d'hameçonnage pour voler des jetons d'API ou des identifiants en vue de futures attaques. Comme les API élargissent la surface d'attaque, les acteurs malveillants les utilisent de plus en plus pour obtenir un accès non autorisé. En outre, les alertes associées à la technique T1190 (exploitation des applications publiques) ont révélé que des attaquants utilisent des failles d'application pour infiltrer les réseaux. La technique T1580 (détection de l'infrastructure cloud) a également été observée. Elle consiste à utiliser des API pour effectuer une reconnaissance en sondant les points de terminaison cloud exposés via des appels d'API.

Bien que MITRE ne dispose pas d'une matrice de sécurité d'API dédiée, son cadre reste essentiel pour les équipes de sécurité et les organisations qui recherchent des informations sur les techniques des pirates ciblant les API. En mappant les tactiques des cybercriminels aux comportements propres aux API, les équipes de sécurité peuvent améliorer la réponse aux incidents et la détection des menaces en identifiant les étapes de l'attaque et les tactiques, techniques et procédures associées. Cette approche permet aux gardiens de la sécurité d'atténuer les risques plus efficacement.

Alertes OWASP

La liste des 10 principaux risques pour la sécurité des API selon l'OWASP est une ressource essentielle qui fournit des informations exploitables sur l'impact et la gravité des vulnérabilités. Elle permet aux développeurs et aux équipes de sécurité de hiérarchiser efficacement les initiatives, grâce à des mises à jour qui assurent la pertinence des informations dans un écosystème de menaces en constante évolution.

Au cours de la période de test de 30 jours, notre analyse a révélé une hausse de 32 % des incidents liés aux risques identifiés par l'OWASP. Il convient de noter que l'autorisation défaillante au niveau de la propriété de l'objet (BOPLA), l'autorisation défaillante au niveau de la fonction et la violation d'authentification exposent des données sensibles ou des fonctions critiques qui peuvent être exploitées directement par les cybercriminels. Les mécanismes d'autorisation insuffisants permettent aux acteurs malveillants d'élever les privilèges, de prendre le contrôle des comptes et d'accéder à des informations confidentielles, ce qui en fait l'un des vecteurs d'attaque les plus dangereux au niveau des API.

L'autorisation défaillante au niveau de l'objet (BOLA) reste une vulnérabilité critique de la sécurité des API, mais sa détection est difficile car elle dépend des failles de la logique métier. Cela entraîne souvent des signalements insuffisants ou de faibles taux de détection. Pour résoudre ce problème, les entreprises doivent utiliser des solutions de sécurité des API, l'objectif étant d'établir des relations claires entre les utilisateurs et les ressources auxquelles ils accèdent habituellement. Pour y parvenir, il est nécessaire de définir des références comportementales à l'aide d'algorithmes sophistiqués d'apprentissage automatique, capables de reconnaître les modèles d'accès anormaux.

La menace BOPLA exploite les problèmes d'accès granulaires au niveau des champs dans les API, qui sont souvent négligés lors des tests de sécurité. Contrairement aux vulnérabilités BOLA, qui nécessitent de modifier les identifiants d'objets entiers, les attaques BOPLA ciblent des propriétés spécifiques au sein des objets. Par exemple, un appel d'API « DELETE » qui expose des informations personnelles sensibles (PII) dans sa réponse constitue une vulnérabilité BOPLA. Cette subtilité rend les menaces BOPLA plus répandues que les attaques BOLA.

Exemple concret : une demande de désabonnement qui utilise uniquement une adresse e-mail et où la réponse de l'API inclut par inadvertance le nom complet et l'adresse de l'utilisateur. Les données sensibles sont ainsi exposées à des tiers non autorisés, car les tests de sécurité se concentrent généralement sur des objets entiers plutôt que sur des propriétés individuelles. Cette négligence explique pourquoi les vulnérabilités BOPLA ont été davantage détectées dans les évaluations de sécurité des API.

La consommation illimitée des ressources est une autre vulnérabilité critique, que les pirates peuvent exploiter pour provoquer des interruptions de service par un épuisement des ressources ou par des attaques de type DDoS. Cette vulnérabilité présente des risques dont l'impact ne se limite pas aux services : elle entraîne notamment une augmentation des coûts opérationnels suite à l'utilisation excessive des ressources cloud, mais aussi des risques accrus d'attaques par force brute. Sans une limitation adéquate du débit, les pirates peuvent rapidement sonder les API, ce qui peut potentiellement compromettre la sécurité. Par ailleurs, ces attaques génèrent un trafic important, ce qui entraîne une forte hausse des coûts pour les entreprises.

La consommation d'API non sécurisée, qui découle d'une validation inadéquate, d'un filtrage des données et d'un manque de mécanismes de sécurité lors des intégrations d'API tierces, constitue un autre vecteur de menace important. Ce problème est préoccupant, car les entreprises s'appuient de plus en plus sur des API tierces pour leur transformation digitale. Une étude récente a révélé que plus de 80 % des entreprises étaient confrontées à des problèmes avec des API tierces, ce qui souligne l'importance d'adopter un modèle de sécurité Zero Trust. Bien que cette vulnérabilité ne soit pas catastrophique en soi, elle peut devenir une menace de sécurité majeure lorsqu'elle est associée à d'autres failles de sécurité, telles qu'une mauvaise validation ou des dépendances non sécurisées. Par exemple, la confiance dans une API financière qui gère des transactions tierces non vérifiées risque d'entraîner des violations de sécurité.

Les alertes de sécurité liées à la norme PCI DSS et au RGPD ont augmenté respectivement de 16 % et 21 %, tandis que les alertes liées à la norme ISO 27001 ont subi une hausse de 22 %.

Garantir la conformité des API

Les meilleures pratiques pour assurer la conformité des API incluent le balisage de chaque alerte avec les normes de conformité et réglementaires spécifiques qu'elle enfreint, ce qui permet aux entreprises d'obtenir des informations immédiates sur les problèmes de conformité critiques et de fournir des conseils exploitables pour les résoudre. Cette approche proactive aide les entreprises à se maintenir en conformité avec la réglementation, ce qui réduit le risque d'amendes réglementaires, de répercussions juridiques et d'atteintes à la réputation pouvant entraîner des pertes financières considérables. Par exemple, une compagnie aérienne s'est vu infliger une amende de 20 millions de livres sterling suite à une vulnérabilité API qui a exposé les données de 400 000 clients. Cet exemple illustre les conséquences graves d'une sécurité API inadéquate par rapport au RGPD.

Les normes de conformité servent de garde-fous indispensables pour les entreprises afin de sécuriser les données sensibles, de protéger les clients et de respecter les obligations légales et réglementaires. Les normes telles que la norme PCI DSS, le RGPD et la loi HIPAA (Health Insurance Portability and Accountability Act) imposent un traitement sécurisé des informations sensibles, telles que les données de paiement et les informations à caractère personnel. Selon notre analyse des données, les alertes de sécurité liées à la norme PCI DSS et au RGPD ont augmenté respectivement de 16 % et 21 %, tandis que les alertes liées à la norme ISO 27001 ont enregistré une hausse de 22 %.

Le RGPD (Règlement général sur la protection des données)

Le RGPD s'attache à assurer la protection des données et la confidentialité des clients tout au long du cycle de vie des API. Cela implique une conception sécurisée, une authentification et une autorisation rigoureuses, une limitation du débit, des tests de vulnérabilité réguliers, le chiffrement et des évaluations continues des risques, même lors des premières étapes du développement. Ces mesures garantissent la confidentialité, l'intégrité et la disponibilité des données.

La norme PCI DSS

De même, la norme PCI DSS veille à la sécurisation des API qui gèrent les données de cartes de paiement, en intégrant la sécurité dans les phases de conception, de codage et de test. Elle impose une protection contre les vulnérabilités Web et des tests réguliers pour identifier et corriger les failles de sécurité.

En particulier, les exigences 10 et 11 exigent une journalisation et une surveillance complètes des activités de l'API, y compris les demandes, les réponses, les tentatives d'authentification et les modifications du système. Les journaux doivent être conservés pendant au moins 12 mois, et les trois derniers mois doivent être facilement accessibles à des fins d'analyse. En outre, cette norme recommande aux entreprises d'effectuer des analyses de vulnérabilité externes après des modifications importantes. Pour garantir la conformité à la norme PCI, les entreprises doivent mettre en œuvre des contrôles stricts, notamment la limitation du débit, la journalisation, le contrôle d'accès basé sur les rôles (RBAC) et la gestion des sessions, afin de s'assurer que les API sont résilientes contre les menaces et les risques.

La norme ISO 27001

La norme ISO 27001 fournit un cadre robuste pour gérer efficacement les risques liés à la sécurité des informations, améliorer la stratégie de sécurité d'une entreprise et renforcer la confiance entre ses pairs et ses clients. Les pratiques recommandées sont les suivantes :

- Mise en œuvre d'un contrôle d'accès (par exemple, clés API) pour vérifier l'identité des utilisateurs
- Utilisation du chiffrement des données de bout en bout
- Surveillance des API pour détecter tout comportement anormal
- Évaluations approfondies des risques pour identifier les vulnérabilités potentielles des API

Ces exigences de conformité mettent en évidence la relation indissociable entre la sécurité des API et les cadres réglementaires. Une mise en œuvre adéquate protège non seulement les données sensibles, mais répond également à plusieurs exigences de conformité. Pour plus d'informations sur les normes internationales existantes et émergentes, consultez la section Conformité de ce rapport.

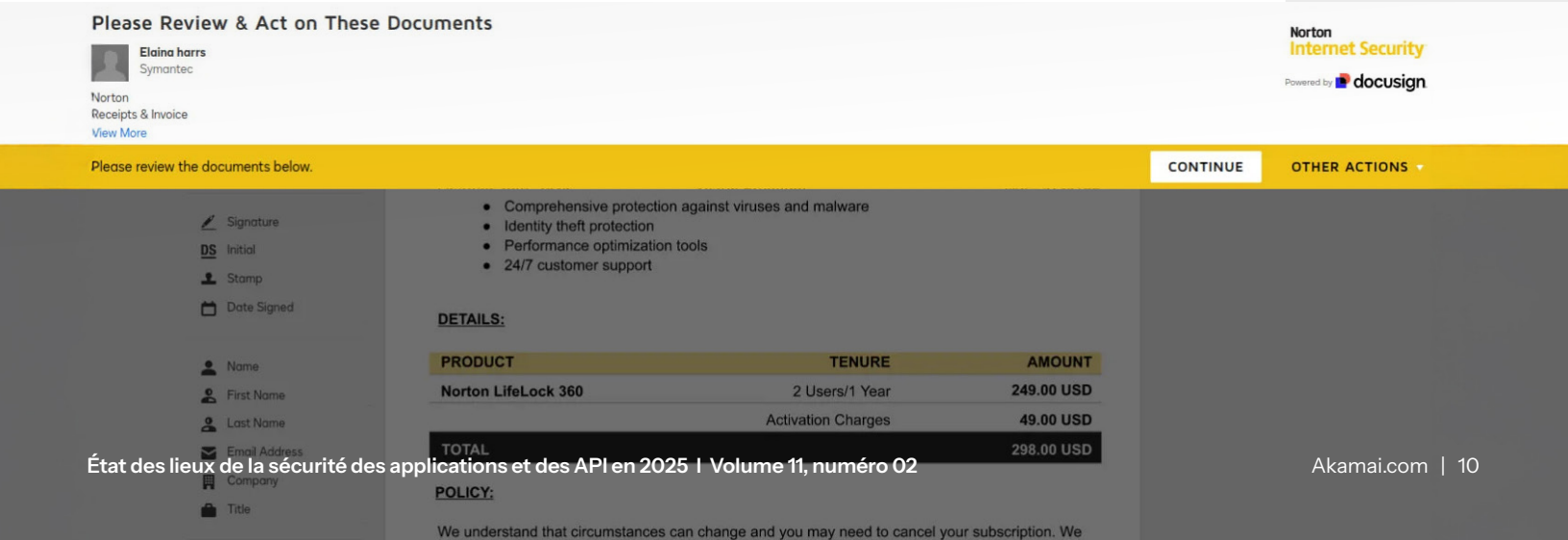
Les lacunes de visibilité des API : les accès cachés aux données

Exploitations d'API

En novembre 2024, Bleeping Computer a signalé une attaque importante contre un fournisseur de solutions de signature électronique. Les cybercriminels ont exploité un composant central de l'API de gestion et de suivi des documents du fournisseur, leur permettant d'envoyer des factures frauduleuses à de nombreuses victimes potentielles. En signant à leur insu ces documents, les destinataires ont permis aux pirates de solliciter des paiements auprès de diverses organisations.

Cet incident souligne l'impact pernicieux des exploitations d'API : les acteurs malveillants peuvent exploiter les API au-delà de leur utilisation prévue et les transformer en vecteurs d'attaque inattendus. L'émergence de l'IA générative a exacerbé ces risques en automatisant la détection des vulnérabilités et en contournant les limitations de débit, permettant ainsi des attaques plus rapides et sophistiquées.

Source : bleepingcomputer/Wallarm



Difficultés pour détecter les exploitations d'API

Les équipes de sécurité rencontrent des obstacles importants pour détecter les exploitations d'API, principalement en raison de la nécessité d'établir une base de référence permettant de distinguer les comportements normaux des comportements suspects. Ces difficultés illustrent le besoin crucial de suivre les comportements en temps réel pour identifier les anomalies et les menaces de manière préventive.

Notre étude 2024 des impacts sur la sécurité des API révèle une tendance préoccupante : seulement 13 % des entreprises interrogées testent leurs API quotidiennement, ce qui représente une nette baisse par rapport au chiffre de 37 % en 2023. Cette baisse est particulièrement alarmante compte tenu de l'écosystème actuel des menaces. La forte réduction des tests d'API quotidiens expose les entreprises à des risques de sécurité accrus, car elle réduit considérablement leur capacité à détecter et à réagir face à des menaces en constante évolution, ce qui peut empêcher les vulnérabilités critiques d'être traitées pendant de longues périodes.

En mettant en place des tests automatisés fréquents pendant les cycles de développement, les entreprises sont en mesure d'identifier et de résoudre les problèmes en amont, ce qui leur évite d'avoir à appliquer des mesures correctives coûteuses dans leurs environnements de production. À une époque où l'exploitation des API utilise de plus en plus des méthodes automatisées et secrètes, les tests proactifs jouent un rôle essentiel dans l'atténuation des risques.

API non gérées : API zombies et fantômes

La visibilité du parc d'API reste un défi essentiel pour les entreprises, qui englobe à la fois le suivi officiel des API et l'identification des données sensibles. L'étude 2024 des impacts sur la sécurité des API révèle un fossé important : 47 % des équipes AppSec disposent d'un inventaire complet de leurs API, mais ne parviennent pas à identifier les API qui gèrent les données sensibles. Les professionnels de la sécurité font état de limitations similaires, 42 % d'entre eux étant confrontés à ce problème de surveillance. Malheureusement, le nombre d'entreprises disposant d'un inventaire complet de leurs API et de données précises sur l'exposition de leurs données sensibles est passé de 40 % en 2023 à 27 % en 2024. L'étude des impacts sur la sécurité révèle également que les API zombies et fantômes sont l'une des principales causes des incidents de sécurité ciblant les API.

Plus particulièrement, les inventaires incomplets passent à côté des API zombies et fantômes. Les API zombies (c'est-à-dire les interfaces obsolètes qui restent actives en raison d'une mise hors service incomplète, d'une rotation du personnel ou pour d'autres raisons) créent des vecteurs d'attaque vulnérables. Les API fantômes (développées en tant que solutions rapides en dehors des processus d'approbation standard) représentent des menaces comparables. Des recherches indiquent qu'un tiers des transactions d'API malveillantes ciblent les API fantômes.

Les mesures de sécurité traditionnelles, telles que les pare-feux d'applications Web (WAF), s'avèrent inadéquates contre ces menaces. Les entreprises ont besoin de solutions de détection et de surveillance des API suffisamment sophistiquées pour identifier efficacement les points de terminaison vulnérables.

Un inventaire complet des API constitue la pierre angulaire d'une stratégie de sécurité efficace. Il permet aux entreprises de surveiller les modèles d'utilisation, de suivre l'historique des versions, d'identifier les vulnérabilités et de répondre aux exigences de conformité et réglementaires. Cette approche stratégique offre une visibilité claire sur l'infrastructure digitale d'une entreprise, ce qui peut renforcer la gestion des risques et améliorer la stratégie de sécurité globale.

Analyse de sécurité

Au cours du premier trimestre 2025, nous avons identifié une attaque contre une entreprise de commerce électronique via une exploitation d'API. L'API d'envoi de SMS de l'entreprise ne disposait pas de contrôles d'authentification appropriés, ce qui a permis aux pirates de l'exploiter en utilisant plus de 200 adresses IP différentes, un seul jeton d'authentification et de nombreux numéros de téléphone mobile aléatoires (à la fois réels et factices).

La stratégie d'attaque était simple mais efficace : surcharger l'entreprise en enregistrant plusieurs numéros de téléphone portable et en envoyant des SMS à des numéros frauduleux pour causer directement des dommages financiers. Lorsque les cybercriminels enregistrent un numéro de téléphone portable, l'entreprise concernée, qui paie pour un service de passerelle SMS afin de faciliter la messagerie texte entre ses applications et ses appareils mobiles, subit des frais financiers inattendus pouvant nuire à sa marque ou à sa réputation. Une stratégie de défense en profondeur, avec plusieurs couches de mesures de sécurité, peut contrer ce type d'attaque et atténuer considérablement les risques associés.

Nos alertes ont révélé que les acteurs malveillants ont lancé 11 057 requêtes POST au cours de cette attaque et que 5 659 réponses ont abouti (Figure 2).

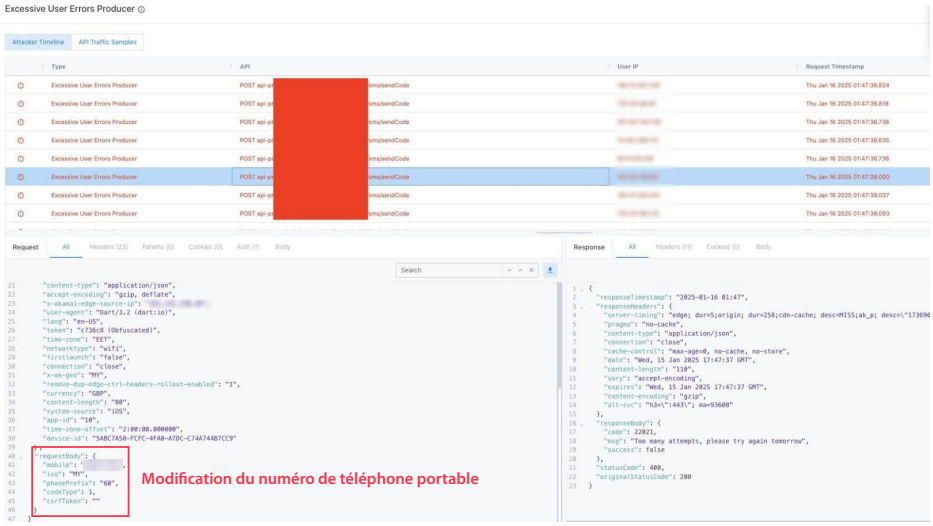


Fig. 2 : Les cybercriminels inondent l'API non sécurisée de requêtes

Ces demandes automatisées étaient identiques, à l'exception d'un paramètre critique :

Body param **mobile**: the following pattern is detected - **<number>**

De telles demandes peuvent surcharger le serveur et entraîner un déni de service, ou elles peuvent indiquer un accès non autorisé réussi à l'API. Les pare-feux d'applications Web (WAF) traditionnels ne sont pas en mesure de détecter ces attaques sophistiquées. Cependant, les solutions sophistiquées de sécurité des API, qui créent une base de référence pour le comportement normal des API, peuvent identifier de telles attaques grâce à l'analyse du comportement, atténuer les risques de manière proactive et empêcher les attaquants d'aggraver les dommages.

Attaques Web : comparaison et tendances d'une année sur l'autre

Les recherches d'Akamai ont révélé une augmentation considérable des attaques Web visant les applications Web et les API au cours de la période de janvier 2023 à décembre 2024 (Figure 3). Le nombre d'attaques mensuelles est passé de près de 14 milliards début 2023 à plus de 29 milliards en octobre 2024. Cela représente une croissance de 65 % des attaques Web entre le premier trimestre 2023 et le quatrième trimestre 2024.

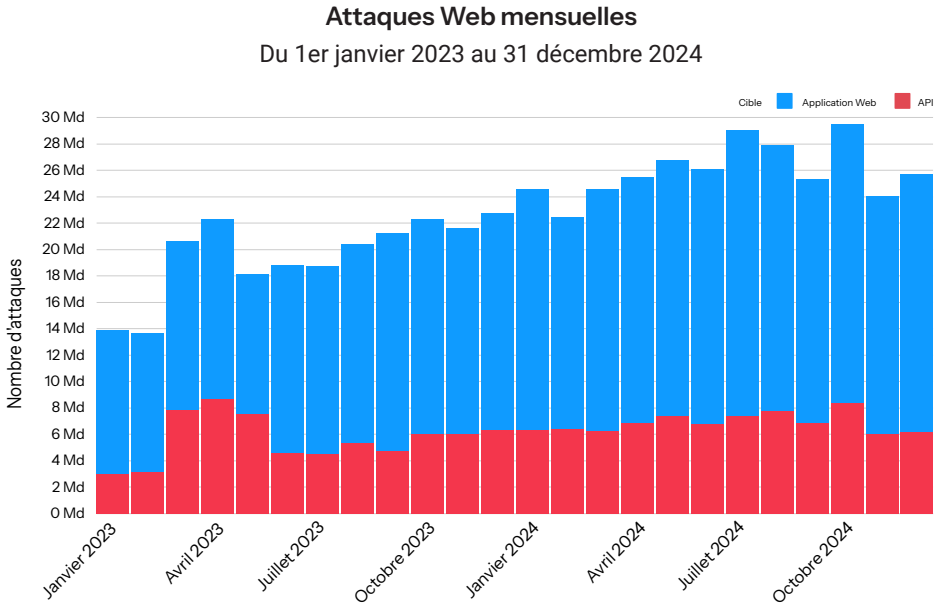


Fig. 3 : Les attaques traditionnelles ciblant les applications Web et les API continuent d'être en hausse, comme le montre une augmentation de 65 % entre le premier trimestre 2023 et le quatrième trimestre 2024.

Principaux vecteurs d'attaque : les risques traditionnels et les risques actuels basés sur le comportement se combinent

Les professionnels de la cybersécurité font face à des complexités croissantes pour protéger l'infrastructure digitale des entreprises contre un large éventail de menaces, allant des attaques Web traditionnelles aux exploits actuels ciblant les vulnérabilités inhérentes et les configurations incorrectes.

Violations des contraintes de demande d'API : une menace grandissante

Une analyse complète des points de terminaison d'API sur une période de deux ans révèle que les violations des contraintes de demande d'API représentent un domaine de préoccupation pour les entreprises (Figure 4). Ces violations se manifestent lorsque les demandes ou les réponses ne respectent pas les paramètres prédéfinis ou les exigences établies, par exemple lorsque les limites de débit sont dépassées ou lorsque des données non valides sont soumises.

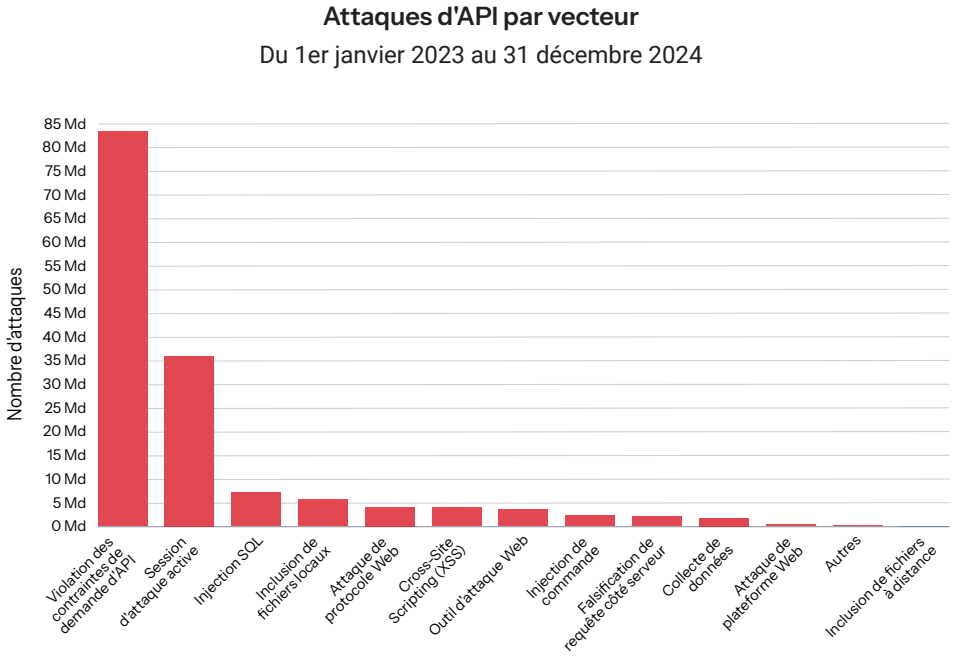


Fig. 4 : Plus de 83 milliards de violations des contraintes de demande ont été enregistrées en deux ans

Les violations des contraintes de demande d'API représentent une menace croissante, avec plus de 83 milliards d'attaques enregistrées sur une période de deux ans. Ce vecteur d'attaque a connu une forte hausse de 24 % entre 2023 et 2024, mettant en lumière les dangers de l'exploitation d'API. La généralisation de ces violations est un bon indicateur d'une exploitation potentielle d'API, et elle peut précipiter de nombreux effets indésirables, notamment la dégradation des performances du système, les interruptions de service et la vulnérabilité accrue aux attaques ciblées.

Sessions d'attaque actives : des attaques uniques qui exigent une solution créative

Les solutions d'Akamai utilisent des outils de sécurité innovants pour relever les défis uniques posés par les attaques ciblant les API. Au cœur de ces solutions se trouve un mécanisme exclusif permettant de détecter les sessions d'attaque actives et servant d'outil de défense stratégique. Ce système utilise les renseignements d'Akamai sur les menaces pour identifier et suivre les comportements suspects, ce qui permet aux entreprises de déjouer les menaces de manière proactive avant qu'elles ne se transforment en attaques massives à grande échelle.

Le système signale les acteurs malveillants et met en œuvre une approche de type « mise sur la touche ». Concernant les attaques actuelles, les cybercriminels utilisent principalement l'automatisation pour exécuter leur reconnaissance et leurs attaques. Akamai identifie rapidement ces sessions d'analyse de vulnérabilité, réagit en bloquant temporairement le client et répertorie ces menaces en tant que sessions d'attaque actives. Cette stratégie empêche efficacement les pirates potentiels d'effectuer des reconnaissances et d'exploiter les vulnérabilités du réseau.

En limitant la fenêtre d'opportunités des cybercriminels, les entreprises peuvent renforcer considérablement leur stratégie de sécurité des API. Cette approche offre une protection robuste contre un large éventail d'attaques potentielles et améliore considérablement la résilience globale en matière de cybersécurité.

L'importance de cette stratégie apparaît de manière évidente dans nos données. Les sessions d'attaque actives pour les applications Web et les API occupent la première place dans notre classement général (Figure 5). En 2023, plus de 69 milliards d'attaques étaient recensées. Ce chiffre a atteint plus de 113 milliards d'attaques en 2024, ce qui représente une augmentation considérable de 63 % d'une année sur l'autre.

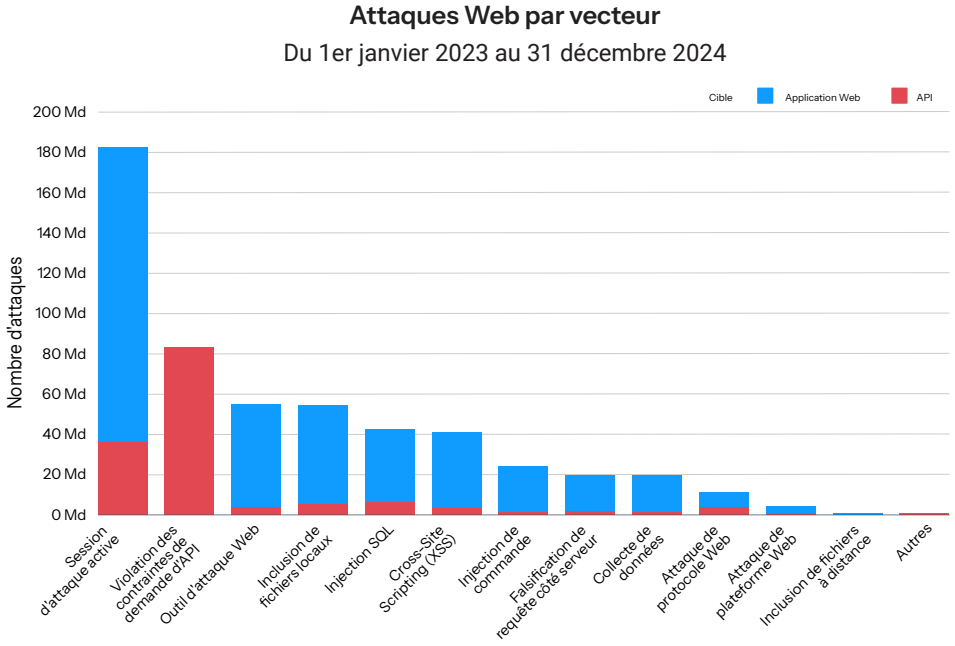


Fig. 5 : Les sessions d'attaque actives dépassent tous les autres vecteurs d'attaque pour les applications Web et les API, ce qui illustre la quête incessante des pirates pour détecter les vulnérabilités dans les réseaux ciblés.

Pourquoi nous ne pouvons pas ignorer les vulnérabilités Web traditionnelles dans les infrastructures actuelles

Les attaques par injection continuent de démontrer toute leur efficacité malgré l'émergence de méthodologies d'attaque sophistiquées, basées sur le comportement, et la sensibilisation accrue aux vulnérabilités Web traditionnelles. Nos données de janvier 2023 à décembre 2024 indiquent une augmentation significative du volume d'attaques, avec des injections SQL (Structured Query Language) et des injections de commandes enregistrant respectivement une croissance de 60 % et 34 % d'une année sur l'autre. Ces vulnérabilités permettent aux cybercriminels d'exécuter des commandes non autorisées, de compromettre l'intégrité du système et d'accéder aux données sensibles sans authentification appropriée, ce qui met en évidence leur pertinence dans le domaine de la cybersécurité.

La prévalence durable des bases de données SQL, réputées pour leur fiabilité et leur évolutivité en matière de stockage de données, contribue au ciblage persistant de ces systèmes. En particulier, les quatre bases de données les plus utilisées s'appuient sur des architectures basées sur SQL, ce qui souligne davantage la nature critique de ce vecteur d'attaque.

Bien que la liste des 10 principaux risques pour la sécurité des API selon l'OWASP ait fait l'objet de révisions (par exemple, les problèmes de configuration de la sécurité se sont substitués aux attaques par injection dans la mise à jour de 2023), le risque associé aux attaques par injection reste de taille. Parallèlement, d'autres vecteurs bien connus, tels que l'inclusion de fichiers locaux (LFI) et le cross-site scripting (XSS), sont toujours très répandus. Notre Guide 2025 à l'usage des gardiens de la sécurité Internet décrit la sophistication des techniques d'exploitation XSS, notamment l'injection de ressources à distance, le vol de cookies, le détournement de sites Web et la falsification de sessions, en se basant sur des attaques réelles observées en 2024.

Ces résultats montrent combien il est impératif de mettre en œuvre des stratégies de défense multicouche. Les professionnels de la cybersécurité doivent combiner plusieurs techniques, telles qu'un codage de sortie approprié, des stratégies de sécurité de contenu robustes et des WAF performants, pour contrer efficacement ces attaques de plus en plus sophistiquées.

Attaques DDoS de couche 7 : comparaison et tendances d'une année sur l'autre

De janvier 2023 à décembre 2024, les recherches d'Akamai ont révélé une augmentation spectaculaire des attaques DDoS de couche 7 (couche applicative) contre les applications Web et les API (Figure 6). Le volume d'attaques mensuel est passé d'un peu plus de 500 milliards début 2023 à plus de 1 100 milliards en décembre 2024. Cela représente une croissance de 94 % du nombre d'attaques DDoS de couche 7 entre le premier trimestre 2023 et le quatrième trimestre 2024.

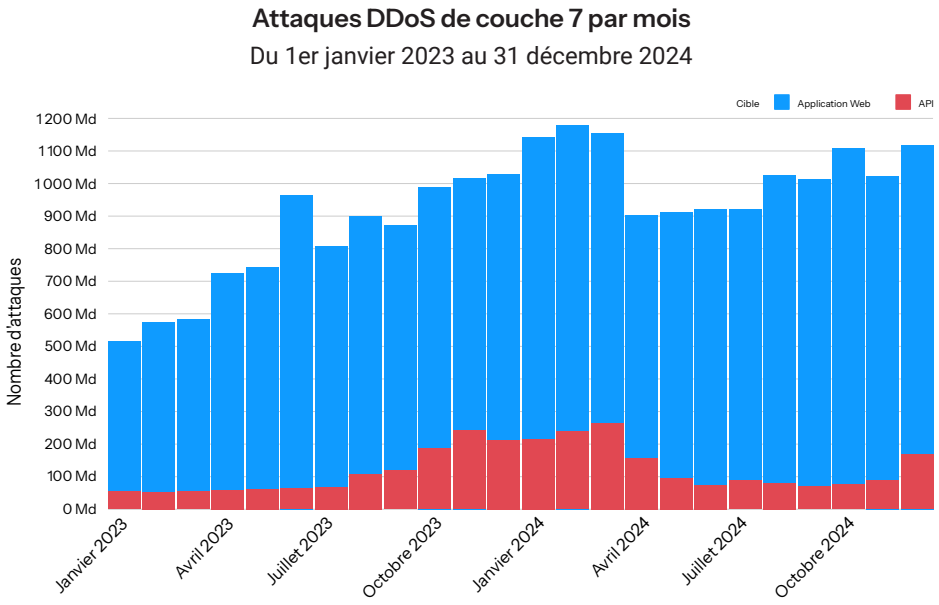


Fig. 6 : Le nombre d'attaques DDoS de couche 7 ciblant les applications Web et les API continue d'augmenter, comme le montre la hausse de 94 % entre le premier trimestre 2023 et le quatrième trimestre 2024.

Attaques DDoS de couche 7 sur les applications et les API

Les floods HTTP demeurent un vecteur de menace majeur dans l'évolution continue des attaques DDoS de couche 7 ciblant les applications Web et les points de terminaison d'API. Ces attaques submergent les ressources API en les inondant de volumes élevés de requêtes apparemment légitimes qui se concentrent sur des opérations gourmandes en ressources. Les pirates ont peaufiné leurs techniques, en créant des attaques DDoS de couche 7 pour exploiter des vulnérabilités spécifiques dans la logique applicative Web ou les API, ce qui complique les efforts de détection et d'atténuation des risques. En outre, les attaques pilotées par des bots sont de plus en plus sophistiquées, générant des modèles de trafic qui imitent l'utilisation légitime d'API.

Exploitation de l'IA par les cybercriminels : une méthode manuelle ou automatique

Les technologies d'IA générative ont révolutionné l'intégration de services interentreprises via les API, contribuant à l'adoption généralisée et à l'application pratique des API. Le marché des API basées sur l'IA devrait connaître une croissance exponentielle, passant de 44,41 milliards de dollars en 2025 à 179,14 milliards de dollars d'ici 2030 selon les prévisions, soit un taux de croissance annuel moyen de 32,2 %. Toutefois, cette adoption très forte de l'IA coïncide avec une hausse significative des attaques basées sur l'IA qui ciblent les API. La vulnérabilité plus élevée des API peut être largement attribuée aux cybercriminels qui utilisent l'IA comme un outil de reconnaissance et d'exploitation, que ce soit manuellement ou automatiquement.

Stratégies d'attaque pilotées par l'IA contre les API

Ciblage stratégique : les pirates utilisent des outils d'IA pour identifier et analyser des composants spécifiques dans les API ciblées, en créant des exploits sur mesure avec du code malveillant généré par l'IA pour des vulnérabilités précises. Cette approche permet de lancer des attaques précises et efficaces, en exploitant les failles des API.

Attaques automatisées : en automatisant le processus d'attaque, les cybercriminels réduisent considérablement leur temps et leurs efforts, car ils identifient et exploitent rapidement les failles de sécurité des API. Cette automatisation s'appuie souvent sur des bots pilotés par l'IA qui représentent une menace critique pour les entreprises et les individus.

Attaques volumétriques : les pirates tirent parti de l'IA pour submerger les API de trafic, inondant ainsi les systèmes de sécurité avec un volume important de données, dans un laps de temps très court. Les attaques DDoS automatisées illustrent cette stratégie : les bots pilotés par l'IA lancent des attaques continues tout en s'adaptant dynamiquement aux mesures défensives.

Attaques basées sur le comportement : l'IA analyse les modèles de trafic pour créer des attaques faibles et lentes qui évitent la détection en fonctionnant en dessous des seuils d'alerte habituels. Ces attaques ciblent souvent les vulnérabilités courantes des API, telles que BOLA (défaillance de l'autorisation au niveau de l'objet) et la violation d'authentification.

L'ironie des API basées sur l'IA

Paradoxalement, les API basées sur l'IA se sont avérées peu sûres. La majorité des API basées sur l'IA sont accessibles en externe. Une grande partie s'appuie sur des mécanismes d'authentification inadéquats, ce qui les rend plus vulnérables aux attaques. Notre étude 2024 des impacts sur la sécurité des API a révélé que les API présentes dans les outils d'IA générative étaient la principale cause des incidents liés aux API signalés par les équipes de sécurité du secteur du commerce de détail/de l'e-commerce.

Un écosystème de menaces liées à l'IA en constante évolution

Les progrès technologiques de l'IA ont joué un rôle considérable dans l'évolution de l'écosystème des menaces liées aux API. Une augmentation sans précédent des vulnérabilités des API basées sur l'IA a été enregistrée au cours de l'année passée, certaines sources indiquant que, pour la première fois, la majorité des vulnérabilités exploitées enregistrées par l'agence américaine de cybersécurité et de sécurité des infrastructures étaient liées aux API.

Attaques d'applications Web basées sur l'IA et stratégies de défense

En introduisant de nouveaux vecteurs d'attaque et de nouvelles capacités défensives, l'IA a également exercé une très forte influence sur la sécurité des applications Web. Les logiciels malveillants optimisés par l'IA, l'analyse des vulnérabilités assistée par l'IA, les attaques contre les systèmes utilisant l'IA, l'extraction Web sophistiquée et les systèmes WAF pilotés par l'IA font partie des principaux domaines dans lesquels l'IA a considérablement modifié le paysage de la cybersécurité concernant les attaques d'applications Web.

Logiciels malveillants optimisés par l'IA

Des experts en cybersécurité ont observé des logiciels malveillants sophistiqués exploitant l'IA pour attaquer les applications Web. Dans une campagne d'e-mails de 2024 visant les utilisateurs français, les pirates ont déployé du code malveillant, probablement conçu avec l'aide de l'IA générative, pour exécuter le logiciel malveillant AsyncRAT. Cet exemple illustre la tendance actuelle consistant à créer et à déployer des logiciels malveillants assistés par l'IA, ce qui pose de nouveaux défis pour les professionnels de la sécurité des applications Web.

Analyse des vulnérabilités assistée par l'IA

L'IA a révolutionné l'analyse des vulnérabilités pour les applications Web, en offrant des capacités défensives et offensives, qu'elles soient utiles ou malveillantes. Ces outils basés sur l'IA automatisent désormais les recherches de vulnérabilités courantes, telles que SQLi, XSS, Cross-site Request Forgery et Server-side Request Forgery (SSRF). En outre, ils effectuent des analyses basées sur l'IA pour repérer les impacts potentiels et génèrent des recommandations optimisées par l'IA pour les mesures correctives.

Attaques contre les systèmes utilisant l'IA

L'intégration de l'IA, en particulier des grands modèles de langage (LLM), dans les applications Web a introduit de nouvelles failles de sécurité. *Les attaques par injection de prompt* ciblent les systèmes d'IA pour remplacer les mesures de protection des modèles. Un exemple notable est une vulnérabilité Slack AI, désormais corrigée, qui permettait la collecte de données à partir de canaux privés via une injection de prompt indirecte. *Les attaques par empoisonnement de données* corrompent le comportement du modèle d'IA en manipulant un faible pourcentage des ensembles de données, ce qui peut compromettre l'intégrité du système. Les *techniques de Jailbreaking* contournent les mesures de sécurité LLM, permettant aux pirates de supprimer les restrictions, d'extraire des données sensibles et de produire des résultats nuisibles. Ces vecteurs d'attaque émergents nécessitent une vigilance accrue et de nouvelles stratégies de défense.

Extraction Web sophistiquée

L'IA améliore les capacités d'extraction Web, ce qui crée de nouveaux défis pour la sécurité des applications Web. Ces outils d'extraction basés sur l'IA offrent désormais des méthodes d'extraction de données plus efficaces et permettent de mieux esquiver les mesures anti-extraction. Depuis le début des années 2020, l'extraction Web sophistiquée tire parti de l'IA pour traiter les données, mais la fréquence de l'extraction LLM a récemment augmenté de manière notable. Cela est dû en grande partie à l'augmentation des requêtes basées sur les agents, ce qui accroît la demande de sources de données en temps réel (non statiques).

Malheureusement, cela a conduit à un coût moyen de la requête d'application Web (en fonction de facteurs tels que la complexité de la requête, l'infrastructure d'hébergement, etc.) compris entre 0,01 et 0,50 dollar américain par requête. Alors que le commerce était à l'origine le secteur le plus touché par l'augmentation de l'extraction LLM, la tendance a changé : d'autres secteurs (services financiers, jeux d'argent, médias digitaux et médias vidéo, par exemple) subissent aujourd'hui les conséquences de cette mutation.

Systèmes WAF pilotés par l'IA

Point positif, les systèmes WAF avancés sont optimisés par l'IA pour identifier et atténuer plus efficacement un large éventail de cybermenaces, notamment les bots, les attaques DDoS, les extracteurs et les scanners. Les systèmes WAF pilotés par l'IA aident à lutter contre les cyberattaques sophistiquées, car les WAF traditionnels dotés de règles statiques ont du mal à contenir les menaces « Zero Day » et nécessitent des mises à jour manuelles.

La stratégie d'apprentissage automatique multicouche permet la reconnaissance de modèles, l'apprentissage adaptatif, la détection d'anomalies et un temps de réponse amélioré. Grâce à un entraînement sur des milliards d'événements quotidiens et à la mise en œuvre d'une approche multicouche avec surveillance continue, les systèmes WAF pilotés par l'IA visent à prévenir de manière proactive l'évolution des menaces et à protéger les clients.

Tendances par secteur

Parmi les secteurs d'activité, le commerce arrive en tête avec près de trois fois plus d'attaques Web que les hautes technologies (deuxième secteur le plus touché) entre le 1er trimestre 2023 et le 4e trimestre 2024 (Figure 7). En outre, le nombre d'attaques d'API subies par le secteur du commerce au cours de la même période a largement dépassé le nombre total d'attaques d'API des 10 autres secteurs principaux.

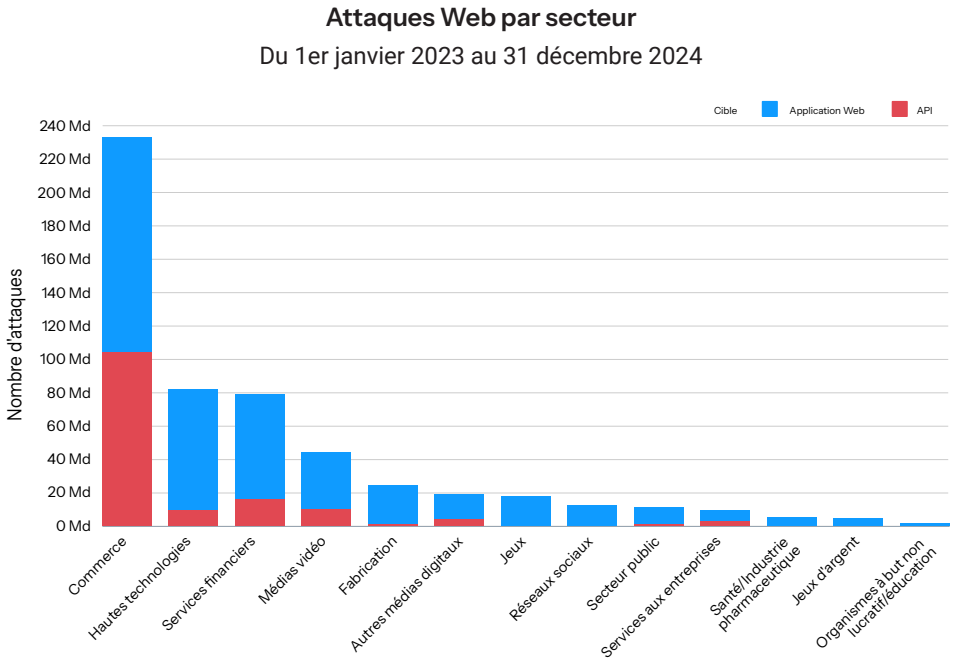


Fig. 7 : Le commerce, les hautes technologies et les services financiers ont été les trois secteurs les plus ciblés par les attaques Web.

En ce qui concerne les attaques DDoS globales de couche 7 (couche applicative), le secteur des hautes technologies a été plus touché que les autres, avec plus de 7 000 milliards d'attaques entre le 1er trimestre 2023 et le 4e trimestre 2024. Le secteur des hautes technologies est suivi par les réseaux sociaux et le commerce (Figure 8). Cependant, au cours de la même période, le nombre d'attaques DDoS de couche 7 ciblant les API dans le secteur du commerce a encore une fois largement dépassé celui de tous les autres secteurs combinés.

Attaques DDoS de couche 7 par secteur

Du 1er janvier 2023 au 31 décembre 2024

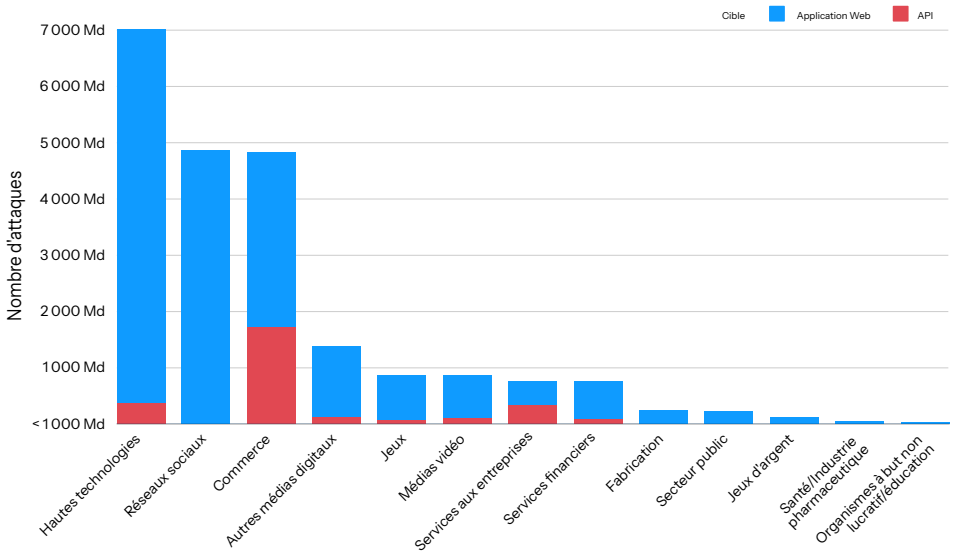


Fig. 8 : Attaques DDoS de couche 7 par secteur

Commerce

En plus des 230 milliards d'attaques Web (soit plus de 40 % des attaques Web globales) de 2023 à 2024, le secteur du commerce a été confronté à une ampleur sans précédent d'attaques DDoS de couche 7. Les données d'Akamai révèlent que plus de 4 800 milliards d'attaques se sont produites en 2023 et 2024.

Ce volume combiné représente un modèle de ciblage stratégique dans lequel les applications Web absorbent environ 64,25 % des attaques, tandis que les API représentent les 35,75 % restants. Cette répartition reflète les deux vecteurs utilisés par les pirates pour compromettre les plateformes commerciales, et elle met en évidence les multiples facettes de l'écosystème actuel des menaces.

Les entités commerciales représentent des cibles particulièrement lucratives en raison de leur concentration de données clients sensibles, d'informations de paiement et de transactions financières. L'accès direct à la monétisation via les identifiants de paiement dérobés, les comptes clients compromis et les informations personnelles sensibles crée des incitations financières immédiates pour les cybercriminels. Contrairement à certains secteurs qui imposent aux hackers des étapes supplémentaires pour pouvoir exploiter les données compromises à des fins lucratives, les plateformes commerciales fournissent souvent aux pirates des ressources directement exploitables.

Le commerce de détail dans le viseur

Le secteur du commerce de détail est le segment le plus touché au sens large. Il est confronté à des volumes d'attaques disproportionnés en raison de plusieurs caractéristiques distinctes.

Les opérations du commerce de détail impliquent généralement des écosystèmes digitaux complexes, intégrant divers systèmes et plateformes. Les initiatives ambitieuses de transformation digitale privilégient souvent la vitesse de mise sur le marché à une sécurité complète, créant ainsi des failles de sécurité. L'adoption de stratégies omnicanal augmente involontairement la complexité de la surface d'attaque. En outre, la dépendance importante envers les fournisseurs tiers crée une chaîne d'approvisionnement complexe, avec de nombreux points de violation potentiels.

Selon l'Internet Crime Complaint Center du FBI, les tendances saisonnières du trafic créent des périodes prévisibles de fort trafic qui peuvent être ciblées spécifiquement par les acteurs malveillants, les incidents de cybercriminalité augmentant de 25 à 30 % pendant les fêtes de fin d'année. Les plateformes de commerce électronique sont également confrontées à des menaces croissantes, avec une hausse de 31 % des cyberattaques en décembre par rapport à la moyenne annuelle.

L'évolution des attaques d'applications Web

Les attaques d'applications Web subissent une transformation importante, stimulée par les avancées technologiques et les nouvelles méthodologies employées par les pirates. Les cybercriminels utilisent des techniques de plus en plus sophistiquées pour exploiter les vulnérabilités des applications Web, en adaptant leurs stratégies aux nouvelles mesures de sécurité. L'essor des outils d'attaque automatisés, associé à l'intégration d'algorithmes d'apprentissage automatique, a permis aux pirates de lancer des campagnes plus précises et ciblées contre les applications Web des détaillants.

En outre, le passage aux architectures de microservices et au développement basé sur les API a étendu la surface d'attaque, ce qui nécessite une réévaluation des paradigmes de sécurité traditionnels. Cette évolution exige une approche proactive de la part des professionnels de la cybersécurité, en mettant l'accent sur la surveillance continue, les mécanismes de défense adaptatifs et une compréhension approfondie des vecteurs d'attaque émergents dans le paysage des applications Web.

L'écosystème des menaces de bots

En raison des progrès technologiques, l'écosystème des menaces de bots évolue rapidement, en particulier lorsque les pirates intègrent des capacités d'IA générative. Cette évolution a amélioré les stratégies d'attaque via des exploits « Zero Day » plus rapides et des techniques d'évasion avancées qui contournent les défenses traditionnelles. Les recherches montrent que les attaques par bots basées sur l'IA à l'encontre des détaillants ont augmenté de manière constante entre août 2022 et avril 2024, avec un pic spectaculaire de 137 % en janvier 2024. Les difficultés à détecter ces attaques aggravent encore ces menaces, et les entreprises mettent en moyenne quatre mois à identifier les attaques de bots tout en subissant des dommages financiers et une atteinte à leur réputation.

Les bots fonctionnent désormais comme des vecteurs centraux dans l'écosystème digital du commerce de détail, facilitant le piratage des comptes, la fraude à la carte de crédit et l'utilisation abusive de cartes cadeaux. Ils servent de catalyseurs pour des campagnes d'attaque plus vastes, en utilisant des données volées sur un site compromis pour lancer des attaques par « credential stuffing » contre d'autres sites, ce qui crée un effet multiplicateur dans les écosystèmes de commerce de détail. Cette activité contribue à « l'industrialisation » de la fraude en ligne, les groupes criminels mondiaux utilisant des outils automatisés pour faire évoluer les opérations bien au-delà des méthodes manuelles.

Pour obtenir une liste de recommandations sur la façon de mieux protéger les applications Web et les API de votre activité de commerce de détail contre les attaques pilotées par l'IA et les bots, consultez la section Atténuation des menaces.

Services financiers

Le secteur des services financiers est devenu une cible privilégiée pour les attaques Web et il continue de subir des attaques DDoS de couche 7. Plus de 79 milliards d'attaques Web ont été enregistrées entre janvier 2023 et décembre 2024, tandis que plus de 761 milliards d'attaques DDoS de couche 7 contre les applications Web et les API ont été dénombrées pour la même période.

Ce volume sans précédent souligne la vulnérabilité et l'attrait de ce secteur d'activité pour les cybercriminels. Plusieurs facteurs expliquent cette montée en puissance, notamment le rôle essentiel du secteur financier dans les infrastructures économiques mondiales, la valeur importante des données financières et le potentiel de perturbations importantes.

La digitalisation des services financiers

La digitalisation des services financiers a étendu la surface d'attaque pour les cybercriminels. L'adoption de la personnalisation basée sur l'IA, de la banque en tant que service et des solutions de financement intégrées a introduit de nouvelles vulnérabilités. Les conflits géopolitiques, en particulier la guerre entre la Russie et l'Ukraine, ont alimenté les activités d'hacktivistes ciblant les institutions financières. Les facteurs économiques, notamment le développement des cryptomonnaies et la potentielle mise en place d'une réserve crypto, ont accru l'intérêt des cybercriminels pour le secteur financier.

Les attaques d'applications Web se transforment rapidement, s'adaptant aux nouvelles technologies et exploitant les vulnérabilités émergentes. Les pirates exploitent désormais des algorithmes sophistiqués d'IA et d'apprentissage automatique pour contourner les mesures de sécurité traditionnelles et lancer des attaques plus ciblées et persistantes. L'essor des architectures sans serveur et des microservices a créé de nouveaux vecteurs d'attaque, tandis que l'utilisation croissante des API a étendu les points d'entrée potentiels pour les acteurs malveillants. En outre, le passage aux applications mobiles et basées sur le cloud a nécessité une réévaluation des stratégies de sécurité, car ces plateformes présentent des défis uniques en termes de protection des données et de contrôle d'accès.

L'importance du segment bancaire en tant que cible d'attaque

Dans le secteur des services financiers, les banques se démarquent comme le segment le plus ciblé pour les attaques Web (Figure 9). Comme dans le secteur du commerce, les attaques par « credential stuffing » sont désormais un vecteur de menace majeur dans le secteur bancaire.

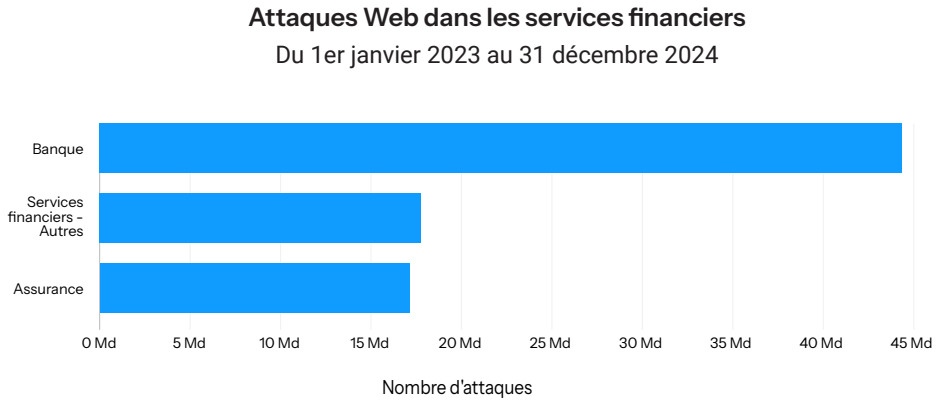


Fig. 9 : Le secteur bancaire est le segment le plus ciblé parmi les attaques Web de services financiers.

La prédominance des services bancaires en ligne, associée à la nature critique de l'accès aux comptes, attire les cybercriminels. Une attaque menée à bien promet des avantages financiers substantiels. Même un petit nombre de comptes compromis peuvent générer des gains importants. La réticence du segment bancaire à mettre en œuvre des mesures de sécurité strictes susceptibles de perturber les utilisateurs, telles que l'authentification multifactorielle, a malencontreusement contribué à sa vulnérabilité.

L'importance du segment bancaire en tant que cible d'attaque est accentuée par plusieurs facteurs. La sensibilité aux temps d'arrêt présente une opportunité d'extorsion, car les acteurs malveillants exploitent les préoccupations liées aux interruptions de service. En outre, la sophistication croissante des techniques d'attaque, notamment l'utilisation de l'IA et de l'apprentissage automatique pour échapper à la détection, pose des difficultés majeures aux mécanismes de défense traditionnels. Le paysage réglementaire, avec des exigences strictes en matière de conformité et des amendes potentielles en cas de violation de la sécurité, ajoute une complexité supplémentaire aux défis du segment bancaire en matière de cybersécurité.

Hautes technologies

Les hautes technologies restent l'un des principaux secteurs ciblés par les attaques Web et les attaques DDoS de couche 7. Dans le cadre de notre étude, le secteur des hautes technologies inclut les segments du secteur des télécommunications, des logiciels et du matériel professionnels, ainsi que des logiciels et du matériel grand public. Nos données ont montré que ce secteur était le deuxième du marché en matière de nombre total d'attaques Web, avec plus de 81,7 milliards d'attaques répertoriées au cours de la période 2023-2024. En outre, le secteur des hautes technologies a été la cible du plus grand nombre d'attaques DDoS de couche 7, avec plus de 7 000 milliards d'attaques répertoriées sur cette période de deux ans.

Les applications Web haute technologie utilisent souvent des requêtes de base de données complexes et du contenu dynamique, ce qui crée des vulnérabilités que les pirates exploitent pour submerger facilement les serveurs. Ces vulnérabilités contribuent au nombre important d'attaques DDoS de couche 7 subies par le secteur. Les réseaux blockchain ont notamment connu une augmentation significative d'attaques DDoS, les pirates utilisant des méthodes telles que l'inondation HTTP Flood et les transactions de spam pour empêcher les transactions légitimes, malgré l'architecture décentralisée de la blockchain. L'impact financier majeur des interruptions de service dans le secteur des hautes technologies incite les pirates à déployer des attaques DDoS capables de neutraliser les services essentiels. Aujourd'hui, la dépendance des développeurs de logiciels à l'égard des architectures basées sur les API introduit des risques supplémentaires, car les pirates exploitent fréquemment des points de terminaison codés de manière non sécurisée dans le cadre d'attaques HTTP Flood.

Le segment des télécommunications est confronté à des défis similaires

Le segment des télécommunications, affecté par un nombre important d'attaques API, est confronté à des défis similaires en matière de cybersécurité. Dans ce segment à fort contenu technologique, les violations de données, les attaques DDoS et les vulnérabilités de la chaîne logistique comptent parmi les principales menaces d'attaques ciblant les applications Web et les API. Ces vulnérabilités ont entraîné plusieurs violations de données de grande envergure.

Par exemple, en janvier 2025, des chercheurs ont découvert des vulnérabilités d'API critiques dans un grand réseau de télécommunications, exposant 3 000 entreprises à des risques de sécurité. L'enquête a révélé des failles de sécurité importantes, notamment des lacunes dans le processus de vérification « Know Your Customer » et une vulnérabilité Path Traversal de l'API back-end qui accorde l'accès aux systèmes internes.

L'Internet des objets (IoT) introduit de nouveaux vecteurs d'attaque

À une époque de progrès technologiques rapides, le secteur des hautes technologies continue de faire face à de nouvelles vulnérabilités affectant les applications Web et les API. Cette évolution englobe l'adoption généralisée de terminaux IoT (Internet des objets), ce qui introduit de nouveaux vecteurs d'attaque, car de nombreux terminaux ne disposent pas de mesures de sécurité robustes. L'adoption accélérée des infrastructures multi-cloud entraîne souvent des environnements mal configurés, créant ainsi des points d'entrée potentiels pouvant être exploités par les pirates.

Les vulnérabilités des terminaux IoT et des systèmes cloud mal conçus font de plus en plus l'objet d'attaques sophistiquées pilotées par l'IA. Les plateformes SaaS font face à des risques élevés d'attaques d'API en raison de leur vaste surface d'attaque. La prolifération des solutions d'IA et la dépendance accrue vis-à-vis des plateformes SaaS tierces ont considérablement élargi la surface d'attaque des API dans le secteur des hautes technologies. À mesure que les entreprises continuent d'adopter ces technologies, le potentiel d'exploitation augmente, ce qui nécessite des mesures de sécurité robustes et une surveillance attentive.

Tendances régionales

REMARQUE : nous avons modifié le format de nos rapports régionaux afin de rendre les données plus accessibles aux lecteurs et de mettre facilement en évidence les tendances des attaques dans toutes les régions, y compris l'Amérique du Nord, l'Asie-Pacifique et le Japon (APJ), l'Europe, le Moyen-Orient et l'Afrique (EMEA) et l'Amérique latine (LATAM). Nous avons également inclus un tableau récapitulatif des données que nous abordons dans cette section (Figure 10).

Données sur les attaques Web Données sur les attaques DDoS de couche 7

Région	Nombre d'attaques Web	Nombres d'attaques DDoS de couche 7	Principaux vecteurs d'attaques Web	Régions les plus ciblées	Secteurs les plus ciblés
APJ	80 Md, 14 % API	7 400 Md, 6 % API	Session d'attaque active, LFI, XSS	Australie (20,3 Md), Inde (17,3 Md), Singapour (15,9 Md)	Services financiers, commerce, réseaux sociaux
				Singapour (4 700 Md), Inde (607 Md), Corée du Sud (283 Md)	Réseaux sociaux, autres médias digitaux, commerce
EMEA	116 Md, 37 % API	2 600 Md, 20 % API	Session d'attaque active, violation des contraintes de demande d'API, LFI	Royaume-Uni (30,3 Md), Pays-Bas (19,5 Md), Espagne (14,2 Md), Allemagne (12,8 Md)	Commerce, médias vidéo, services financiers
				Allemagne (569 Md), Royaume-Uni (506 Md)	Commerce, autres médias digitaux, médias vidéo
LATAM	3 Md, 12 % API	258 Md, 18 % API	Session d'attaque active, WAT, SSRF	Brésil (19,3 Md), Mexique (2 Md)	Commerce, services financiers
				Brésil (175 Md), Mexique (39 Md)	Commerce, services financiers
Amérique du Nord	327 Md, 29 % API	11 900 Md, 16 % API			

Fig. 10 : Régions en bref, de janvier 2023 à décembre 2024 (LFI fait référence à l'inclusion de fichiers locaux ; XSS signifie « cross-site scripting » ; WAT est un outil d'attaque Web ; SSRF signifie « falsification de requêtes côté serveur »)

Deux tendances en matière d'attaques d'applications et d'API

Notre analyse des comparaisons régionales entre les attaques d'applications Web et d'API et les attaques DDoS de couche 7 au cours de la période de 24 mois s'étendant de janvier 2023 à décembre 2024 révèle deux tendances globales (Figure 11).

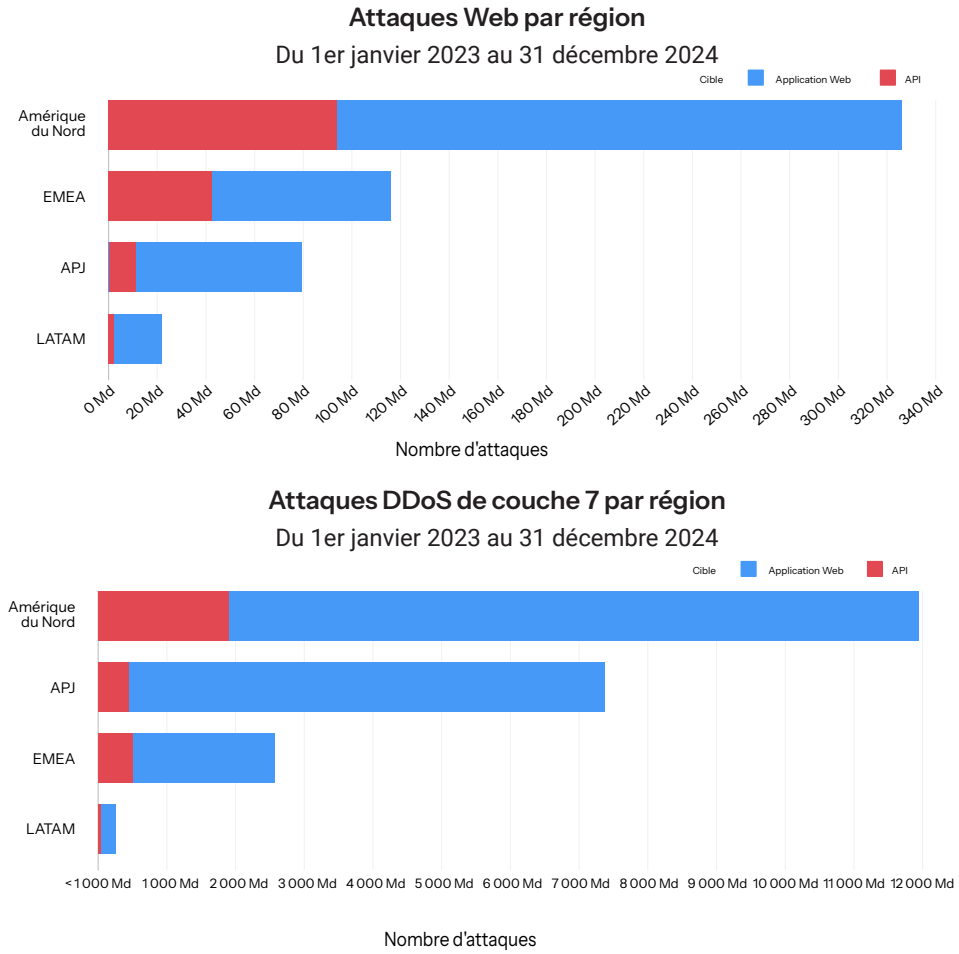


Figure 11 : Au cours de la période considérée, à l'échelle mondiale, la zone EMEA a connu le pourcentage le plus élevé d'attaques d'API, tandis que la zone APJ a enregistré le deuxième plus grand nombre d'attaques DDoS de couche 7 au total.

1re tendance des attaques : les attaques d'API étaient répandues dans la région EMEA, ce qui pourrait découler de taux d'adoption d'API plus élevés que dans d'autres régions, mais aussi de services bancaires ouverts et de la norme PCI DSS v 4.0 qui favorisent l'utilisation des API et peuvent introduire des risques de sécurité. (Reportez-vous à la section Améliorer nos renseignements sur les menaces ciblant les API pour une discussion approfondie des risques spécifiques aux API.)

Dans la continuité de la tendance observée en 2023, la zone EMEA a connu la plus forte concentration d'attaques Web sur les API au cours de la période de 24 mois : Sur les 116 milliards d'attaques Web dans la région, 37 % ont ciblé des API. En comparaison, l'Amérique du Nord a enregistré 327 milliards d'attaques Web, dont 29 % contre des API. Dans la région APJ, 14 % des 80 milliards d'attaques Web ont ciblé des API. La région LATAM suit de près, avec 12 % des 3 milliards d'attaques.

La zone EMEA a également connu la plus forte concentration d'attaques DDoS de couche 7 ciblant les API (20 %), suivie de la zone LATAM (18 %), de l'Amérique du Nord (16 %) et de la région APJ (6 %). En général, les tentatives d'attaques DDoS de couche 7 contre les API représentaient un pourcentage relativement faible par rapport au nombre total d'attaques Web dans chaque région. Nous prévoyons que ces pourcentages augmenteront au fil du temps pour diverses raisons, notamment la mise au point d'attaques plus sophistiquées, pilotées par des bots, et une augmentation des attaques basées sur l'IA ciblant les vulnérabilités des API.

2e tendance des attaques : la région APJ arrive en deuxième position dans le monde en termes d'attaques DDoS de couche 7, avec 7 400 milliards d'attaques (contre 11 900 milliards en Amérique du Nord). Suivent ensuite la région EMEA, avec un total de 2 600 milliards d'attaques, puis la région LATAM qui a enregistré 258 milliards d'attaques. Cette tendance a été initialement observée dans notre rapport État des lieux d'Internet, intitulé Les pirates à l'assaut des infrastructures informatiques, et nous continuons à l'attribuer à une forte concentration des tentatives d'attaques contre les réseaux sociaux dans la région APJ.

Examen plus approfondi des régions APJ, EMEA et LATAM

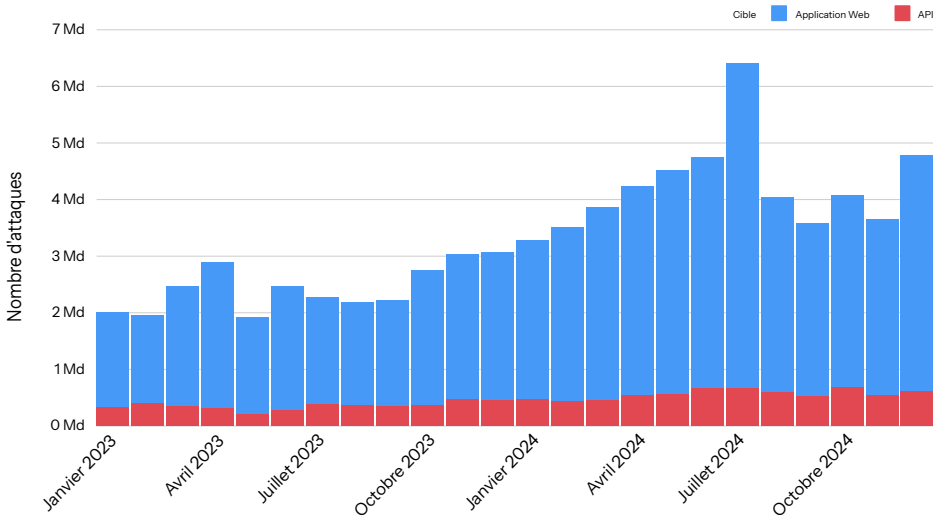
Dans cette section, nous mettons en évidence certaines tendances clés au sein des régions APJ, EMEA et LATAM. Nous incluons également des données spécifiques à certaines zones de ces régions, où nous disposons de suffisamment d'informations sur les attaques pour fournir des renseignements statistiquement significatifs.

Attaques ciblant les applications Web et les API : analyse du trafic

La comparaison des tendances mensuelles des attaques Web entre les régions présente de forts contrastes (Figure 12).

APJ : attaques Web mensuelles

Du 1er janvier 2023 au 31 décembre 2024



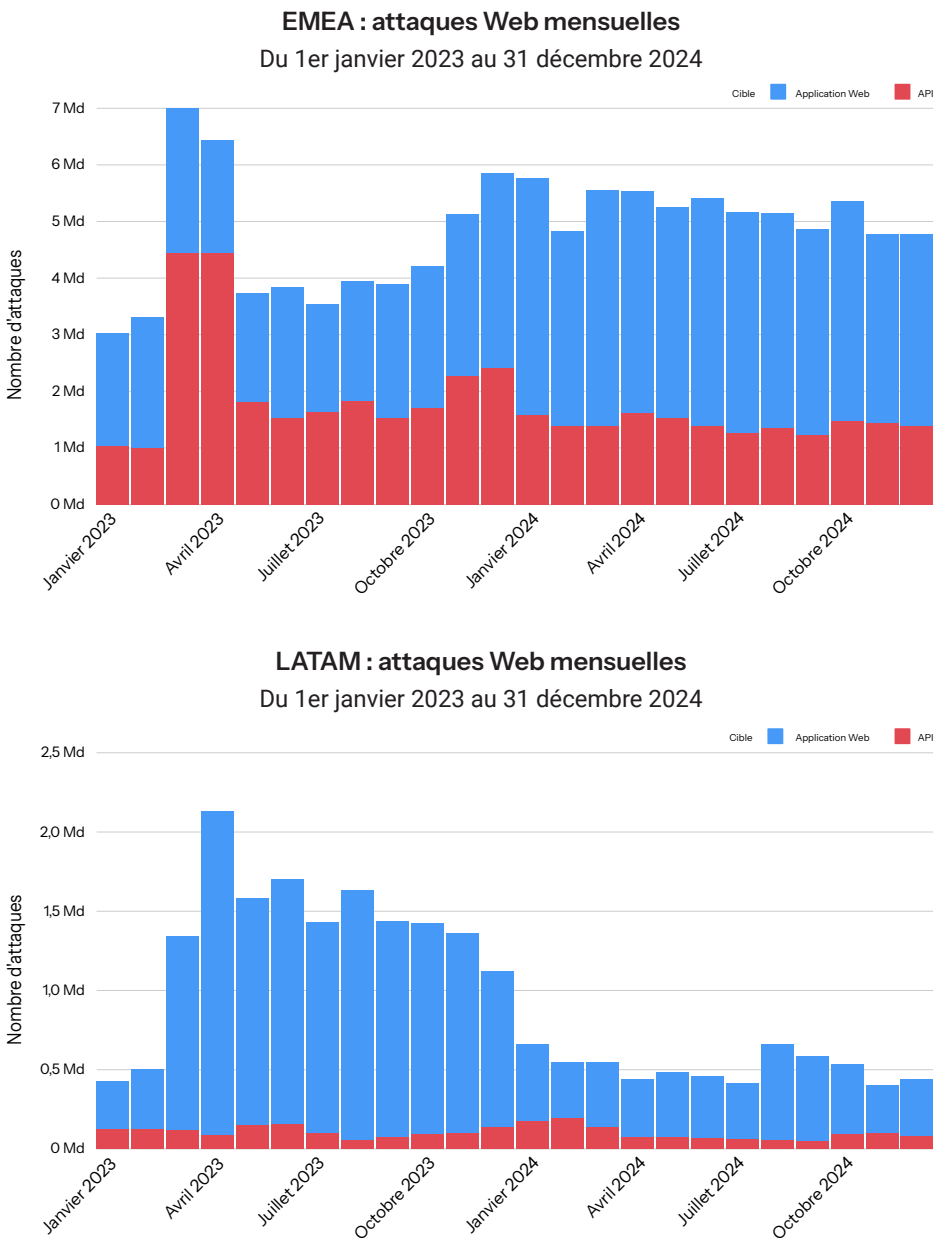


Fig. 12 : L'activité liée aux applications Web a entraîné une augmentation du nombre total d'attaques Web dans les régions APJ et EMEA, tandis que les attaques dans la région LATAM ont fortement diminué.

La région APJ a connu une augmentation importante des attaques Web totales d'une année sur l'autre, passant de 29 milliards en 2023 à 51 milliards en 2024, soit une hausse de 73 %. Dans la zone EMEA, l'augmentation d'une année sur l'autre s'est limitée à 16 % (de 54 à 62 milliards), mais cette moindre hausse a été impactée par une valeur aberrante enregistrée dans les données. Sans cette mesure statistique aberrante, l'augmentation serait proche de 33 %. Dans la région LATAM, les attaques Web ont considérablement diminué, passant d'un total de 16 milliards en 2023 à 6 millions en 2024, soit une diminution de 61 % d'une année sur l'autre.

La hausse des attaques d'applications Web semble avoir provoqué une augmentation du nombre total d'attaques Web, car les attaques d'API sont restées à des niveaux faibles, en particulier dans les régions APJ et LATAM.

Dans la région EMEA, suite à la hausse du premier semestre 2023 (liée à des attaques à grande échelle ciblant le secteur du commerce en Espagne), les niveaux d'attaques d'API ont diminué et sont restés à des niveaux faibles tout au long de l'année 2024, même s'ils restaient relativement élevés par rapport aux autres régions.

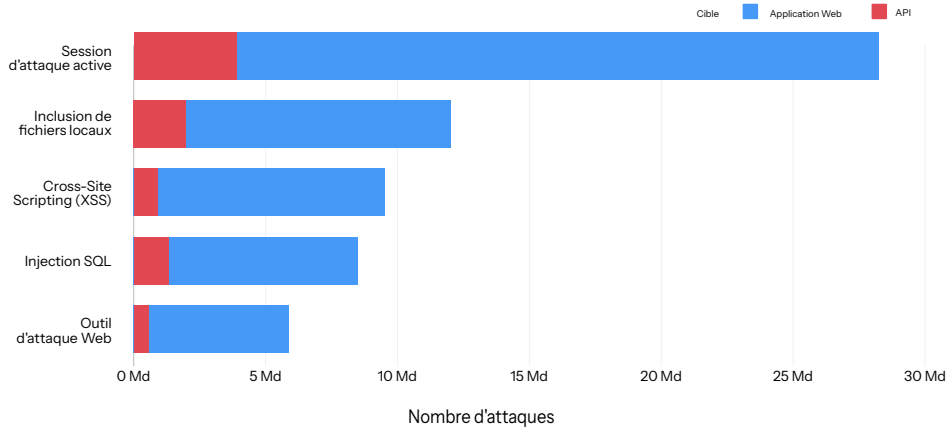
Dans la zone LATAM, les attaques Web ont diminué, car les cybercriminels ont délaissé le secteur du commerce pour axer leurs actions sur d'autres secteurs, notamment l'industrie pharmaceutique et les services aux entreprises, et vers d'autres types d'attaques, tels que les ransomwares.

Attaques ciblant les applications Web et les API : tendances observées en termes de tactiques

Au cours des deux dernières années, les pirates ont continué à s'appuyer sur des méthodes traditionnelles éprouvées, mais le recours à de nouveaux vecteurs d'attaque Web, basés sur le comportement, était également élevé (Figure 13).

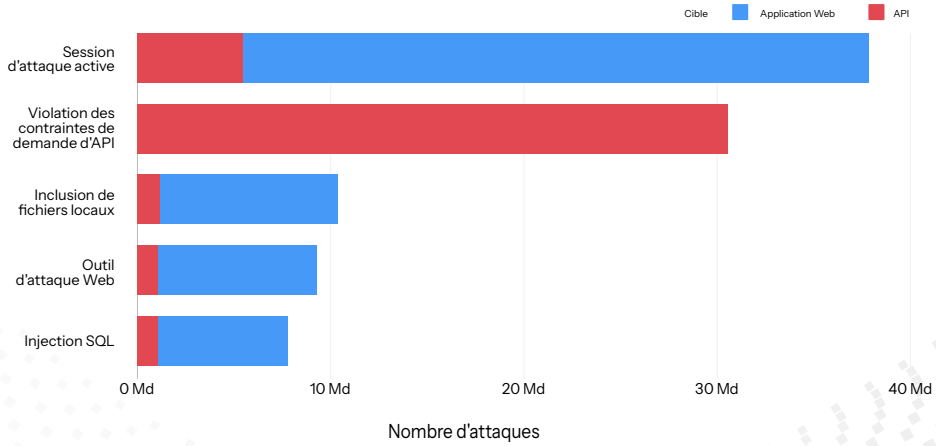
APJ : attaques Web par vecteur

Du 1er janvier 2023 au 31 décembre 2024



EMEA : attaques Web par vecteur

Du 1er janvier 2023 au 31 décembre 2024



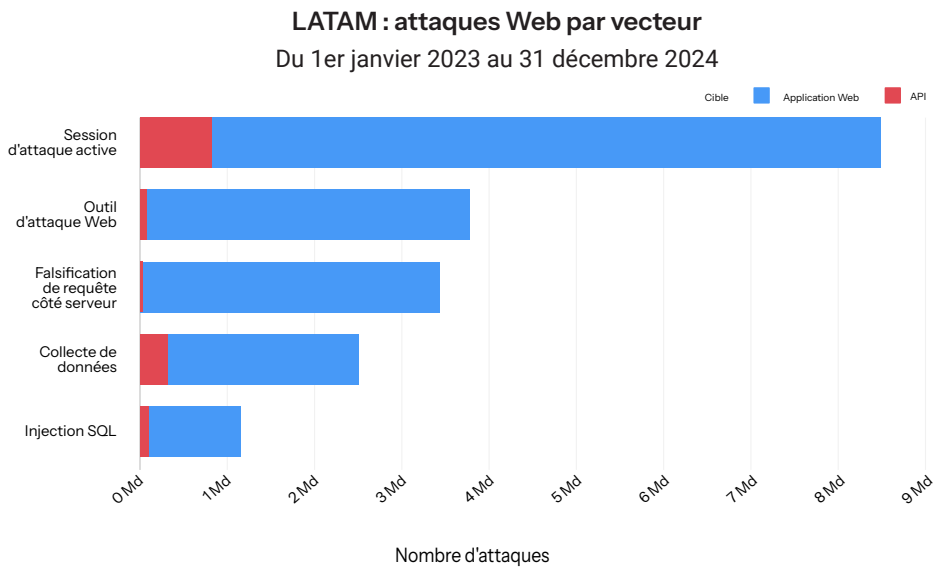


Fig. 13 : Dans toutes les régions, les principaux vecteurs d'attaque incluaient des méthodes traditionnelles et des méthodes comportementales plus récentes, ciblant spécifiquement les API.

Conformément aux tendances mondiales, dans toutes les régions, les vecteurs d'attaque traditionnels persistent, notamment les attaques de type LFI, SQLi et XSS, ainsi que les attaques SSRF dans la zone LATAM. Dans notre Guide 2025 à l'usage des gardiens de la sécurité Internet, nous avons souligné la persistance des attaques XSS et la nécessité de toujours se protéger contre les vulnérabilités Web traditionnelles.

Au moment où les cybercriminels ciblent de plus en plus les API, ce qui diffère pendant cette période, c'est l'augmentation des problèmes liés aux vecteurs d'attaque actuels, basés sur le comportement. Les pirates utilisent ces vecteurs d'attaque pour découvrir les vulnérabilités à exploiter. En suivant ces vecteurs au niveau régional, les chercheurs d'Akamai ont émis les observations suivantes :

- Dans chaque région, le principal vecteur d'attaque était une session d'attaque active, pour laquelle nos contrôles intelligents sont utilisés pour bloquer de manière proactive les requêtes des cybercriminels connus pendant une certaine période.
- La violation des contraintes de demande d'API était le deuxième vecteur d'attaque dans la région EMEA, où la concentration d'attaques ciblant les API est la plus élevée. Les pirates informatiques tentent d'exploiter les API en contournant les exigences telles que les limites de débit et les soumissions de données.
- Dans chaque région, l'outil d'attaque Web figurait dans le top 5 des vecteurs d'attaque. Les cybercriminels utilisent ce vecteur pour sonder la cible afin de solliciter des informations sur sa sécurité, ses configurations ou ses vulnérabilités potentielles, dans le but d'exploiter ces informations à des fins malveillantes.

Pour plus d'informations sur ces principaux vecteurs d'attaque, reportez-vous à la section Attaques Web.

Attaques ciblant les applications Web et les API : cibles principales

En examinant précisément les pays où les cybercriminels se sont concentrés dans chaque région, nous constatons que dans la zone APJ (Asie-Pacifique et Japon), l'Australie (20,3 milliards), l'Inde (17,3 milliards) et Singapour (15,9 milliards) ont subi la plus grosse partie des attaques contre les applications Web et les API, suivis par le Japon (6,3 milliards), la Chine (6,2 milliards), la Corée du Sud (4,9 milliards), la Nouvelle-Zélande (2,9 milliards) et la RAS de Hong Kong (2,2 milliards).

Dans la région EMEA (Europe et Moyen-Orient), les pays les plus touchés par les attaques visant les applications Web et les API ont été le Royaume-Uni (30,3 milliards), les Pays-Bas (19,5 milliards), l'Espagne (14,2 milliards) et l'Allemagne (12,8 milliards). Suivent ensuite l'Autriche (8,2 milliards), la France (7,5 milliards), l'Italie (4,1 milliards), la Suisse (3,7 milliards), la Belgique (3,5 milliards) et Israël (3,3 milliards).

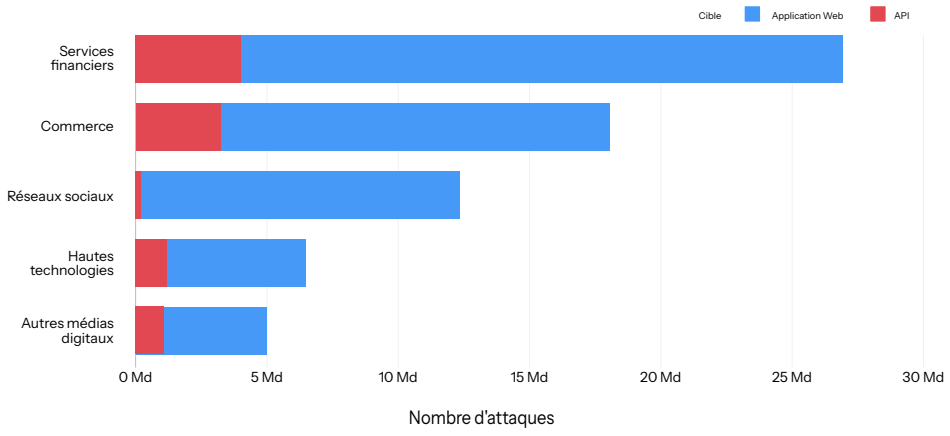
Dans la région LATAM (Amérique latine), le volume des attaques contre les applications Web et les API s'est concentré principalement au Brésil (19,3 milliards), les pays suivants tels que le Mexique (2 milliards) et le Chili (0,4 milliard) ne subissant qu'une petite partie des attaques dans cette zone.

Secteurs d'activités ciblés

L'analyse par secteur d'activité révèle que dans les régions APJ, EMEA et LATAM, le commerce et les services financiers figuraient toujours parmi les trois principaux secteurs ciblés par les attaques Web (Figure 14).

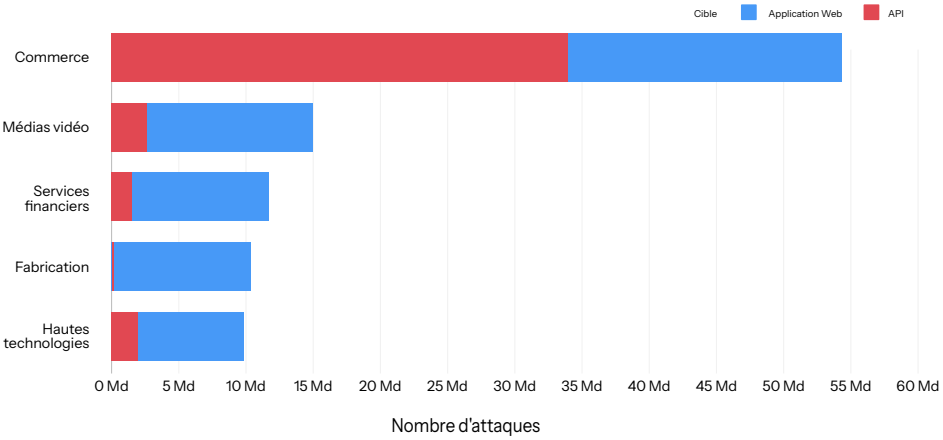
APJ : attaques Web par secteur

Du 1er janvier 2023 au 31 décembre 2024



EMEA : attaques Web par secteur

Du 1er janvier 2023 au 31 décembre 2024



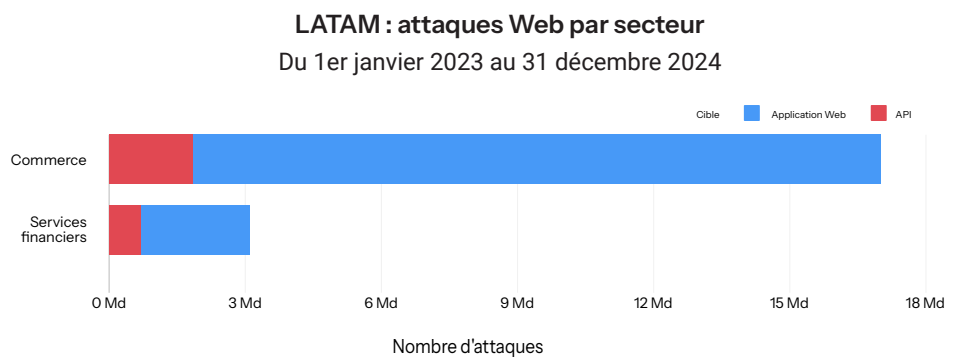


Fig. 14 : Le commerce et les services financiers figuraient parmi les trois principaux secteurs ciblés dans les régions APJ, EMEA et LATAM.

Dans la région APJ, le secteur des services financiers a connu le plus grand nombre d'attaques Web, avec un total de 27 milliards. Le commerce arrive en seconde position avec 18 milliards d'attaques. Cela représente une croissance annuelle de 52 % et 161 %, respectivement. Le secteur Autres médias digitaux a été le plus ciblé par les attaques d'API (22 %), suivi du commerce (18 %) et des services financiers (15 %).

Dans la région EMEA, le commerce a été le secteur le plus touché par les attaques Web, avec 54 milliards d'attaques, soit au moins trois fois plus que le secteur qui arrive en deuxième position. Malgré leur forte concentration, le nombre total d'attaques Web visant les entités commerciales a diminué de 10 % d'une année sur l'autre en raison d'un pic en 2023 qui a faussé les données dans cette région. Cependant, la zone EMEA a enregistré une augmentation de 16 % du nombre total d'attaques Web d'une année sur l'autre, en raison d'une hausse des attaques ciblant d'autres secteurs, notamment les services financiers (152 %) et la fabrication (96 %). En examinant de plus près les attaques dirigées contre les API dans la région, nous constatons que 63 % des attaques Web totales enregistrées dans le secteur du commerce ont ciblé les API.

Nous observons une tendance similaire dans la région LATAM, où le nombre total d'attaques Web visant le secteur du commerce a atteint 17 milliards, dépassant tous les autres secteurs, mais les attaques d'une année sur l'autre ont néanmoins diminué de 76 % dans ce secteur d'activité. Dans le même temps, l'industrie pharmaceutique et les services aux entreprises ont connu une hausse de 107 % et 129 % respectivement, d'une année sur l'autre. En outre, 11 % des attaques ciblant le commerce se sont concentrées sur les API, et les services financiers ont enregistré une concentration encore plus forte d'attaques contre les API (23 %).

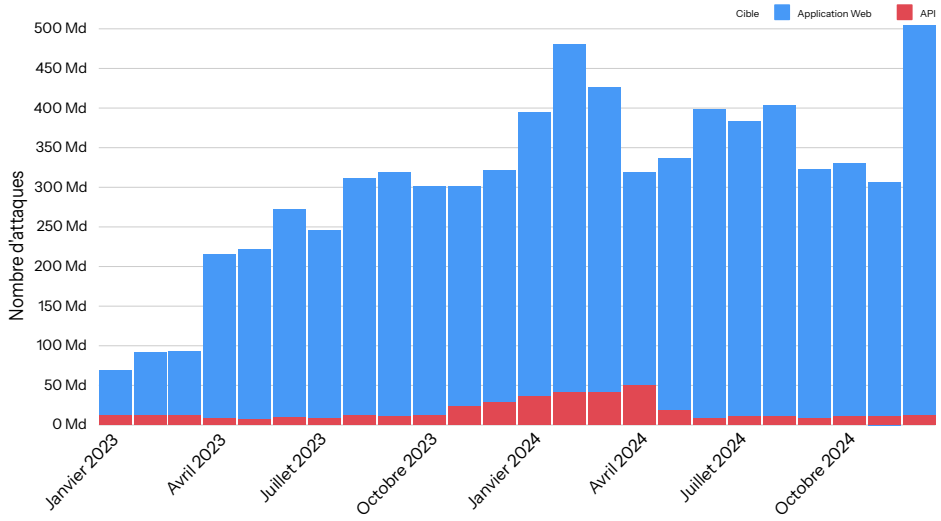
Les secteurs des services financiers et du commerce partagent des caractéristiques qui en font des cibles privilégiées des attaques visant les applications Web et les API : tous deux fonctionnent dans des écosystèmes complexes, dépendent fortement des API et possèdent des données précieuses. Les cybercriminels combinent des techniques d'attaque traditionnelles et émergentes pour atteindre leurs objectifs.

Attaques DDoS de couche 7 : analyse du trafic

Une comparaison des tendances mensuelles en matière d'attaques DDoS de couche 7 entre les régions révèle que la région APJ a été un point névralgique, tandis que les régions EMEA et LATAM ont connu des fluctuations (Figure 15).

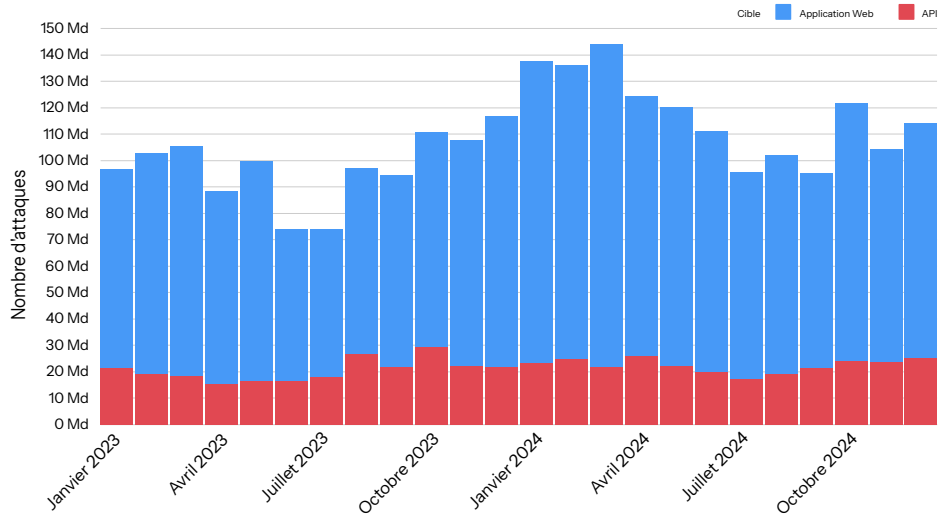
APJ : attaques DDoS de couche 7 par mois

Du 1er janvier 2023 au 31 décembre 2024



EMEA : attaques DDoS de couche 7 par mois

Du 1er janvier 2023 au 31 décembre 2024



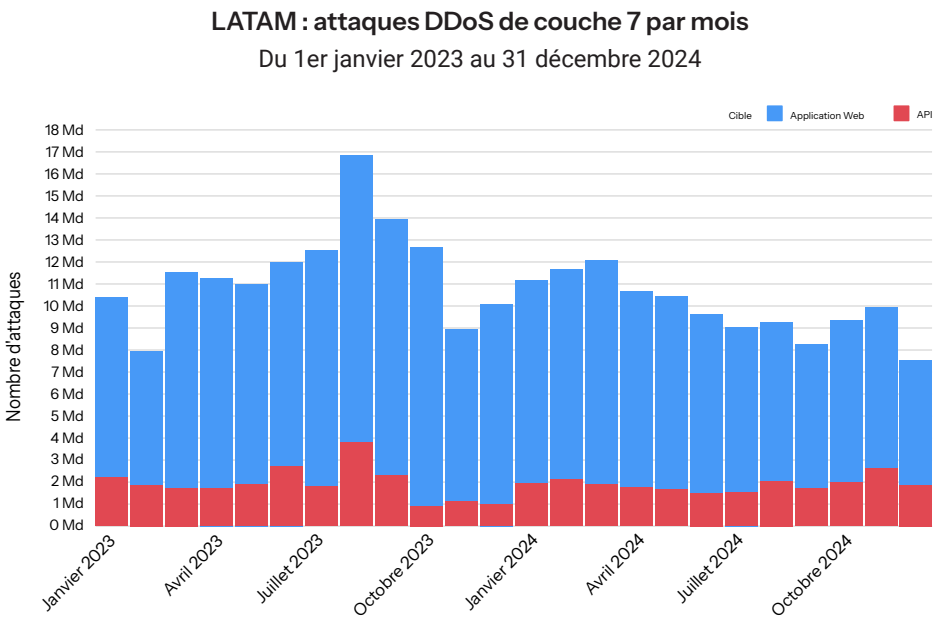


Fig. 15 : Les attaques DDoS de couche 7 ont augmenté dans les régions APJ et EMEA, tandis que ces attaques ont diminué en 2024 dans la zone LATAM.

La région APJ a connu une croissance de 66 % des attaques DDoS de couche 7 d'une année sur l'autre, et a atteint son plus haut niveau en 24 mois, avec un pic s'élevant à 504 milliards en décembre 2024. Cette hausse est principalement imputable à des attaques ciblant le secteur des réseaux sociaux.

Dans la région EMEA, les attaques DDoS de couche 7 ont atteint en mars 2024 un pic de près de 145 milliards et, après une baisse, ont enregistré une nouvelle hausse pour atteindre une croissance de 20 % d'une année sur l'autre. Cette augmentation peut être due à la conjugaison de facteurs géopolitiques et technologiques. Les tensions actuelles dans cette région ont alimenté les activités des hacktivistes. Cette tendance est accentuée par l'essor des outils optimisés par l'IA et des plateformes DDoS en tant que service, qui ont réduit les barrières techniques à l'entrée pour les cybercriminels.

La région LATAM (Amérique latine) a connu une hausse notable des tentatives d'attaques DDoS de couche 7 au début de la période étudiée, ce qui a coïncidé avec une augmentation du nombre d'attaques HTTP Flood visant à submerger les ressources API (un vecteur d'attaque abordé plus en détail dans la section Attaques DDoS de couche 7 : comparaison et tendances d'une année sur l'autre. L'activité a atteint un pic en août 2023, avec 16,8 milliards d'attaques, puis a diminué pendant le reste de la période pour atteindre 7,5 milliards, ce qui représente une baisse de 15 % des attaques d'une année sur l'autre.

Attaques DDoS de couche 7 : cibles principales

Dans chaque région, nous avons observé peu ou pas de changements dans les domaines et les secteurs ciblés par les cybercriminels par rapport à notre précédente analyse des attaques DDoS de couche 7.

Dans la région APJ, Singapour a connu la plus forte concentration d'attaques (4 700 milliards), suivi de l'Inde (1 100 milliards), de la Corée du Sud (607 milliards), de l'Indonésie (283 milliards), de la Chine (246 milliards), du Japon (111 milliards), de l'Australie (108 milliards) et de Taïwan (81 milliards).

Au sein de la région EMEA, les pays ayant subi le plus grand nombre d'attaques DDoS de couche 7 sont l'Allemagne (569 milliards) et le Royaume-Uni (506 milliards), devant Israël (205 milliards), la Suède (193 milliards) et Malte (160 milliards). L'Italie (158 milliards), la Suisse (147 milliards), la France (129 milliards), les Pays-Bas (111 milliards) et l'Espagne (96 milliards) complètent ce Top 10.

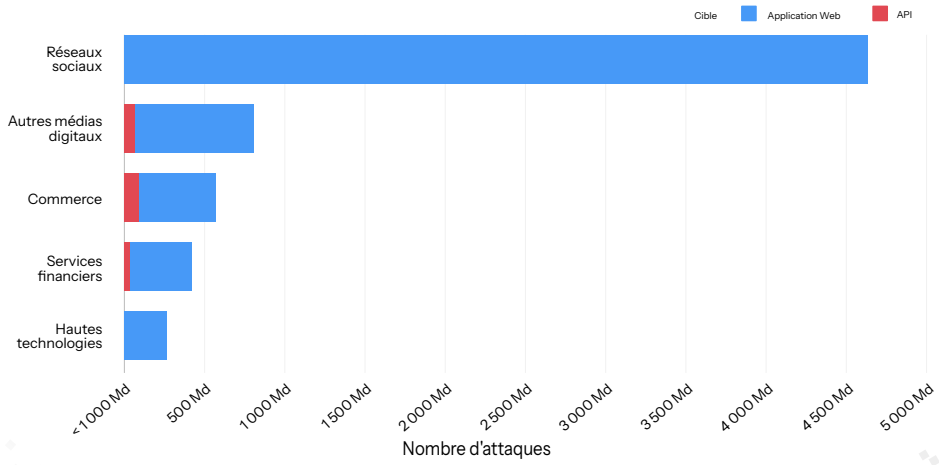
Dans la région LATAM, le Brésil a connu la plus forte concentration d'attaques DDoS de couche 7, à savoir 175 milliards, devant le Mexique (39 milliards) et le Costa Rica (19 milliards).

Secteurs d'activités ciblés

Les principaux secteurs touchés par les attaques DDoS de couche 7 dans les régions APJ et EMEA (Figure 16) n'ont pas changé depuis notre précédent rapport État des lieux d'Internet sur la sécurité des applications. Comme nous l'avons expliqué plus en détail dans ce rapport, dans la région APJ, les attaques DDoS de couche 7 sur les plateformes de réseaux sociaux ont augmenté entre janvier 2023 et juin 2024, en corrélation avec des conflits militaires étendus et des événements électoraux très médiatisés dans le monde entier. Ce n'est pas surprenant, étant donné que les plateformes de réseaux sociaux reçoivent de gros volumes de trafic en période de bouleversement géopolitique. Comme prévu, cette tendance s'est accentuée au cours du reste de l'année 2024 en raison des élections dans la région APJ et aux États-Unis. Ces facteurs ont contribué à une croissance annuelle de 130 % des attaques dans ce secteur.

APJ : attaques DDoS de couche 7 par secteur

Du 1er janvier 2023 au 31 décembre 2024



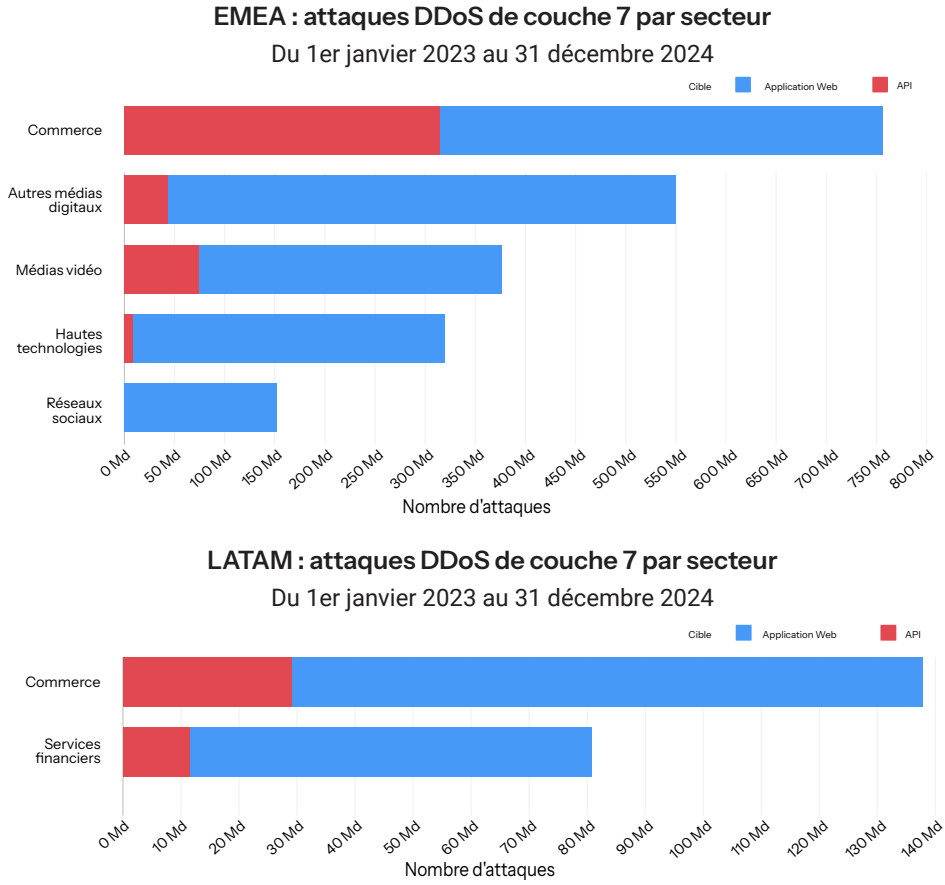


Fig. 16 : Les secteurs les plus touchés par région demeurent les mêmes depuis notre dernière analyse ; le commerce est toujours le secteur d'activité le plus impacté par les attaques DDoS de couche 7 sur les API.

Dans la région EMEA, le commerce est resté le secteur le plus touché par les attaques de DDoS de couche 7, suivi par les autres médias digitaux et les médias vidéo. Pour ce type d'attaque, les secteurs qui ont enregistré la plus forte croissance d'une année sur l'autre incluent les hautes technologies (70 %), les réseaux sociaux (23 %), et le commerce (14 %). Ces évolutions montrent que les pirates peuvent changer rapidement de cible au niveau des secteurs d'activité et des régions. Il est donc utile de suivre les tendances générales.

Le commerce était également le secteur le plus ciblé dans la région LATAM en ce qui concerne les attaques DDoS de couche 7, les services financiers arrivant en deuxième position. Au cours de la période considérée, les niveaux des attaques DDoS de couche 7 sont restés relativement constants dans tous les secteurs.

Reflétant la tendance mondiale, parmi les secteurs les plus ciblés par les attaques DDoS de couche 7, celui du commerce a connu la plus forte concentration d'attaques sur les API dans chaque région. Dans la région EMEA, 43 % des attaques enregistrées dans le secteur du commerce ciblaient les API : 21 % dans la région LATAM et 16 % dans la région APJ.

Pour des raisons qui englobent les bouleversements géopolitiques et l'impact économique potentiel des perturbations sur les services à forte visibilité, le commerce, les médias et les services financiers ont été les cibles privilégiées des attaques DDoS de couche 7 dans les régions EMEA et LATAM au cours des deux dernières années. Reportez-vous à la section Tendances par secteur pour en savoir plus sur les facteurs et les méthodes qui contribuent au niveau élevé de ces attaques dans les secteurs du commerce et des services financiers.

Conformité

Au niveau mondial et de l'Amérique du Nord

En 2025, le paysage mondial de la cybersécurité se caractérise par une complexité et une volatilité sans précédent. Les tensions géopolitiques, notamment les conflits en cours en Ukraine et au Moyen-Orient, ont intensifié les cybermenaces et les attaques commanditées par des États. L'essor de l'hacktivisme, en particulier des groupes pro-russes ciblant les nations occidentales, a rendu cet écosystème des menaces encore plus complexe. D'un point de vue économique, la transformation digitale rapide de tous les secteurs d'activité a étendu la surface d'attaque, les cybercriminels ciblant de plus en plus les infrastructures critiques à l'aide de technologies sophistiquées telles que l'IA pour optimiser leurs capacités d'action.

Ces facteurs, conjugués aux pressions économiques mondiales et aux bouleversements politiques dans des pays clés, ont créé un cocktail explosif pour les professionnels de la cybersécurité dans le monde entier. La protection des applications Web et des API est un enjeu crucial pour les entreprises. Les efforts déployés par les hackers éthiques, les professionnels de la cybersécurité et les entreprises comme Akamai pour sécuriser absolument ces points d'entrée viennent s'ajouter aux considérations croissantes en matière de conformité.

Pour répondre aux impératifs de cybersécurité, les organismes de réglementation du monde entier imposent des exigences de conformité plus strictes pour les applications. En Amérique du Nord, la priorité est désormais de mettre en œuvre des stratégies complètes de gestion des risques et d'obliger les organisations à signaler tous les incidents. Aux États-Unis, la loi Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), qui devrait entrer en vigueur en 2026, exige que les organisations dotées d'infrastructures critiques répertorient leurs systèmes d'information, classent les cyber-risques et évaluent leur stratégie de cybersécurité au moins une fois par an. Cette loi met l'accent sur la nécessité de prendre des mesures de sécurité robustes dans les applications, en particulier celles utilisées dans les secteurs critiques tels que l'énergie, la fabrication de produits chimiques et les technologies de l'information.

De même, le Canada et le Mexique alignent leurs réglementations sur les normes internationales, en se concentrant sur la protection des données et la sécurité des infrastructures critiques. Bien que les réglementations varient d'un pays à l'autre, la tendance mondiale est d'adopter des exigences de sécurité plus strictes pour les applications, notamment une validation améliorée des entrées, des pratiques de développement sécurisé et des audits de sécurité réguliers.

L'écosystème de la sécurité des API fait face à plusieurs défis parallèles, car les API deviennent des cibles privilégiées pour les cybercriminels en raison de leur rôle essentiel dans l'intégration des services et l'échange de données. Face à ces menaces, les organismes de réglementation du monde entier imposent des réglementations plus strictes qui obligent les entreprises à mettre en œuvre des mesures de sécurité robustes pour leurs API.

Il s'agit notamment de la découverte continue des API, de la surveillance et de la protection contre les nouvelles menaces. En Amérique du Nord, l'accent est mis sur l'évaluation approfondie des risques impactant les écosystèmes d'API, en mettant en œuvre des pratiques de développement sécurisé, des mécanismes d'authentification robustes et des capacités de détection des menaces en temps réel. L'adoption rapide d'outils SaaS basés sur l'IA, souvent intégrés via des API, a considérablement élargi la surface d'attaque, incitant les organismes de réglementation à exiger des approches de sécurité plus sophistiquées.

À mesure que la complexité des environnements d'API augmente, en particulier avec l'essor des applications d'IA et d'apprentissage automatique, les exigences de conformité évoluent pour atténuer les risques associés aux violations de données, aux accès non autorisés et aux interruptions de service. Alors que les régions APJ, LATAM et EMEA développent leurs propres réglementations, la tendance mondiale consiste à harmoniser les normes de sécurité des API afin de répondre à la nature interconnectée de l'architecture digitale moderne.

Au niveau de la région APJ (Asie-Pacifique et Japon)

La région APJ connaît un changement important de son paysage réglementaire, avec de nouvelles obligations de conformité imposées aux entreprises de divers secteurs. À Singapour, les récentes modifications apportées à la loi sur la cybersécurité ont élargi le champ d'application pour inclure des infrastructures d'informations critiques à la fois physiques et virtuelles, y compris celles hébergées sur des plateformes cloud et situées à l'étranger. Le Japon a mis à jour ses lois National Center of Incident Readiness and Strategy for Cybersecurity (NISC), tandis que l'Inde a remanié sa loi sur les technologies de l'information (IT Act) en adoptant le Digital Personal Data Protection Bill. L'Australie a introduit sa stratégie de cybersécurité 2023–2030, en mettant davantage l'accent sur le renforcement des mesures de cybersécurité. Dans le cadre de cette stratégie, des modifications ont été apportées fin 2024 à la loi australienne sur la sécurité des infrastructures critiques (SOCI pour Security of Critical Infrastructure) et une nouvelle loi Cyber Security Act 2024 a été introduite. Désormais, les actifs secondaires tels que les terminaux IoT, les applications et les API qui traitent des données sensibles entrent dans le champ d'application de la loi. Ces changements réglementaires imposent aux entreprises de réévaluer et d'améliorer leurs pratiques en matière de sécurité des applications Web, en mettant l'accent sur la protection de l'infrastructure critique et des données sensibles.

La norme PCI DSS v4.0.1 va avoir un impact important sur les entreprises qui gèrent les données des cartes de paiement. Le délai de mise en conformité était fixé au 31 mars 2025. Cette nouvelle version impose des exigences plus strictes pour les applications Web, notamment la mise en œuvre de contrôles pour tous les scripts de page de paiement exécutés dans les navigateurs, et l'utilisation de solutions techniques automatisées pour détecter et prévenir en permanence les attaques Web. Les entreprises de la région APJ doivent désormais effectuer des analyses approfondies des lacunes détectées, mettre à jour leurs stratégies de sécurité et mettre en œuvre les modifications techniques nécessaires pour répondre à ces normes de sécurité renforcées pour leurs applications Web.

Par ailleurs, la région APJ accorde de plus en plus d'importance à la sécurité des API, notamment suite à l'adoption croissante d'initiatives bancaires ouvertes (Open Banking). Bien que la région APJ n'ait pas encore pleinement adopté les réglementations relatives à l'Open Banking au même niveau que dans la zone EMEA, il existe une opportunité pour les pays de cette région de résoudre de manière proactive les problèmes de sécurité liés aux API. Une enquête menée en août 2024 sur la sécurité des API dans cette région révèle que les API internes sont les plus souvent utilisées, mais l'accès des utilisateurs externes reste la principale préoccupation pour le contrôle d'accès aux API. Cela indique la nécessité pour les entreprises de mettre en œuvre des mesures de sécurité robustes pour les API, notamment de solides protocoles d'authentification et d'autorisation, le chiffrement des données, ainsi que la découverte et la surveillance continues des API. À mesure que la région adopte des directives Open Banking, les entreprises doivent privilégier la sécurité des API pour garantir la conformité aux réglementations en constante évolution et se protéger contre les menaces émergentes.

Au niveau de la région EMEA (Europe et Moyen-Orient)

Le paysage de la cybersécurité dans la zone EMEA est en pleine transformation, sous l'effet d'une interaction complexe entre les tensions géopolitiques, les avancées technologiques et les changements réglementaires. La région est confrontée à des défis uniques, les conflits en cours en Ukraine et au Moyen-Orient intensifiant les cybermenaces et les attaques commanditées par des États. En outre, l'essor de l'hacktivisme, en particulier des groupes pro-russes qui ciblent les pays européens, a fait de la région un véritable centre d'intérêt pour les cyberopérations à motivation politique.

Le paysage des API au sein de la zone EMEA est confronté à des défis parallèles. Les API sont devenues des cibles privilégiées pour les cybercriminels en raison de leur rôle essentiel dans l'intégration de services et l'échange de données. Et l'adoption rapide d'outils SaaS basés sur l'IA, souvent intégrés via des API, a considérablement élargi la surface d'attaque.

En réponse à ces menaces croissantes, l'Union européenne a mis en œuvre un programme complet de réglementations en matière de cybersécurité. La mise à jour de la directive sur la sécurité des réseaux et systèmes d'information (SRI 2), en vigueur à partir de janvier 2025, élargit considérablement son champ d'application pour inclure 18 secteurs critiques, imposant des mesures strictes de cybersécurité pour les moyennes et grandes entités.

Pour le secteur financier, la loi sur la résilience opérationnelle numérique (DORA), en vigueur depuis le 17 janvier 2025, remplace la directive SRI 2. Elle impose des cadres réglementaires stricts face aux risques liés aux Technologies de l'Information et de la Communication (TIC), des mécanismes de signalement des incidents et des programmes de test de résilience opérationnelle digitale pour les applications utilisées dans les services financiers. En outre, la norme PCI DSS v4.0.1, qui est devenue obligatoire le 31 mars 2025, introduit de nouvelles exigences de conformité axées sur l'évolution des besoins en matière de sécurité, les processus de sécurité continus, les méthodologies flexibles et les procédures de validation améliorées. La prochaine révision de la directive sur les services de paiement (DSP3) de l'UE vise à combler les lacunes de la directive DSP2 en renforçant les mécanismes de partage des données et les exigences de sécurité, et en optimisant les contrôles dans le secteur des services financiers.

La loi sur la cyberrésilience (CRA), entrée en vigueur le 10 décembre 2024, impose des normes de cybersécurité pour les produits contenant un composant numérique et vendus dans l'Union européenne. Elle oblige les fabricants à mettre en œuvre des mesures de sécurité tout au long du cycle de vie de leurs produits. Pour les développeurs et utilisateurs d'applications, la CRA englobe les smartphones et les tablettes comme vecteurs de risque importants. L'inclusion de ces appareils oblige les entreprises à considérer les terminaux mobiles comme des composants fondamentaux de leur stratégie globale de cybersécurité, en mettant en œuvre des mesures de sécurité rigoureuses tout au long du cycle de vie des applications.

Au Royaume-Uni, la prochaine loi sur la cybersécurité et la résilience (Cyber Security and Resilience Bill) renforcera les cyberdéfenses et protégera les services publics essentiels. Les mises à jour cruciales apportées par cette loi au cadre réglementaire existant vont élargir son champ d'application pour protéger davantage de services digitaux et de chaînes d'approvisionnement, renforcer l'application des règles et accroître les exigences de signalement des incidents.

Au niveau de la région LATAM (Amérique latine)

En Amérique latine, le paysage de la cybersécurité évolue rapidement, façonné à la fois par les tendances technologiques mondiales et par les défis économiques et politiques propres à la région. Dans ce contexte, la transformation digitale rapide de ces pays, conjuguée aux vulnérabilités de systèmes de plus en plus interconnectés, a fait de la région une cible attrayante pour les cybercriminels et les attaques commanditées par des États. Les secteurs du commerce et des services financiers sont devenus des cibles privilégiées pour les cyberattaques. Les détaillants en ligne, les processeurs de paiement, les banques, les compagnies d'assurance, les start-ups fintech et les échanges de cryptomonnaies sont particulièrement vulnérables aux menaces qui ciblent leur infrastructure digitale, en particulier leurs applications Web et leurs API.

Les pays de la zone LATAM reconnaissent ces défis et font des progrès considérables dans le développement et la mise en œuvre de réglementations en matière de cybersécurité, en portant une attention croissante à la sécurité des applications Web et des API. Le Brésil a joué un rôle de premier plan dans la mise en œuvre de la loi Lei Geral de Proteção de Dados Pessoais (LGPD), qui est entrée en vigueur en imposant des exigences strictes en matière de protection et de sécurité des données. Bien qu'elle ne concerne pas spécifiquement les applications Web ou les API, la loi LGPD a incité les entreprises à améliorer leur stratégie globale de cybersécurité, y compris la sécurité de leurs interfaces digitales.

De même, le Chili a promulgué sa loi-cadre sur la cybersécurité, entrée en vigueur le 1er janvier 2025. Cette loi crée la National Cybersecurity Agency et prévoit des mesures complètes pour prévenir, signaler et résoudre les incidents de cybersécurité dans divers secteurs, y compris ceux qui dépendent fortement des applications Web et des API. En janvier 2025, l'Argentine a également publié son Plan fédéral de prévention de la cybercriminalité et de gestion stratégique de la cybersécurité (2025–2027).

Il existe des perspectives intéressantes dans le domaine des réglementations spécifiques aux API. Le Mexique, par exemple, a mis en œuvre une législation axée sur le secteur financier, y compris la fintech, avec des exigences détaillées pour les agences de crédit et les chambres de compensation, afin de développer des API sécurisées. Cette approche reflète une reconnaissance croissante du rôle essentiel joué par les API dans les écosystèmes digitaux actuels, et la nécessité de prendre des mesures de sécurité ciblées. En outre, au Mexique, la loi fédérale sur la protection des données personnelles détenues par des parties privées réglemente le traitement des données personnelles et établit des obligations pour les entreprises et les organisations.

La Colombie a également fait progresser son cadre réglementaire et a élargi son champ d'application juridique en publiant une politique sur la cybersécurité dans les institutions publiques et en créant un système de gestion des risques digitaux, avec différents niveaux de signalement et de réponse aux incidents. Bien qu'elles ne se concentrent pas exclusivement sur les API, ces mesures auront inévitablement un impact sur les pratiques de sécurité liées aux API dans les entreprises.

Dans toute la région, la tendance croissante est d'adopter des initiatives propres à un secteur, telles que des cadres Open Finance qui définissent les normes de sécurité des API pour protéger les données des utilisateurs. Ces cadres sont particulièrement pertinents dans le secteur financier, où la sécurité des API est cruciale pour maintenir l'intégrité des transactions financières et protéger les informations sensibles des clients. Alors que les pays de la zone LATAM continuent de privilégier les avancées en matière de sécurité et d'aligner leurs réglementations de cybersécurité sur les normes internationales, nous pouvons nous attendre à ce que des directives plus complètes et spécifiques soient adoptées pour la sécurité des applications Web et des API.

Atténuation des menaces

Dans un écosystème des menaces en constante évolution, où les techniques d'attaque sont de plus en plus sophistiquées, la protection des applications Web et des API est un enjeu crucial pour les entreprises. Voici quelques-unes des techniques de protection et d'atténuation que nous recommandons :

- **Établissez un plan complet de sécurisation des API :** adoptez une approche « shift-left » et DevSecOps, en intégrant la sécurité pendant tout le cycle de vie des API, de la conception à la post-production. Veillez à mettre en place une découverte et une visibilité continues pour mieux identifier l'ensemble de la surface d'attaque, y compris les API masquées (API fantômes, héritées et zombies). Renforcez la sécurité avec des protocoles stricts d'authentification et d'autorisation (OAuth 2.0, mTLS, contrôle d'accès basé sur les rôles et les attributs), une limitation du débit et une atténuation des bots afin d'éviter l'exploitation des API. Mettez en œuvre la détection des menaces en temps réel, la surveillance des anomalies et la protection des applications d'exécution pour identifier et contrer les attaques à mesure qu'elles surviennent. Assurez la conformité aux réglementations (DORA, RGPD, HIPAA, SRI2 et PCI DSS, notamment), tout en appliquant les politiques de gouvernance des API pour maintenir la sécurité à grande échelle.
- **Mettez en œuvre des mesures de cybersécurité robustes :** utilisez un moteur de sécurité adaptatif qui surveille en permanence l'activité, réagit en temps réel aux menaces, fournit des informations sur les menaces et assure la protection des applications d'exécution. Adoptez également des outils de test des API, tels que le test dynamique de sécurité des applications (DAST), pour vous assurer que les exigences de sécurité sont respectées, notamment l'accès sécurisé, le chiffrement et l'authentification.
- **Adoptez une défense proactive contre les menaces :** utilisez des outils de protection DDoS spécialisés, configurez la limitation du débit et la mise en cache du réseau de diffusion de contenu (CDN), et mettez en œuvre des mesures telles que la gestion des correctifs, les stratégies de contrôle d'accès et la segmentation du réseau. Protégez également l'infrastructure DNS grâce à la surveillance continue du trafic et aux plateformes hybrides.
- **Atténuez les vulnérabilités des API :** suivez les directives de sécurité établies, notamment celles fournies par l'OWASP, afin de renforcer la sécurité des API et de gérer les risques de mauvaises pratiques de codage et d'erreurs de configuration de l'architecture API. Ces risques peuvent en effet créer des vulnérabilités exploitables par les cybercriminels pour obtenir un accès non autorisé ou manipuler des données.

- **Protégez-vous contre les ransomwares :** utilisez une approche multicouche pour lutter contre les ransomwares. Mettez en place des solutions Zero Trust pour bloquer le trafic malveillant, utilisez la microsegmentation pour obtenir une visibilité détaillée et un contrôle d'accès précis, et tirez parti de l'infrastructure ATT&CK de MITRE pour comprendre les modèles d'attaque et optimiser vos stratégies pour les contrer.
- **Préparez-vous à l'IA :** adoptez une stratégie de défense complète qui englobe des solutions de défense contre les bots, des outils de sécurité optimisés par l'IA, des pare-feux spécialisés et des mesures proactives, telles que les évaluations continues et les modèles Zero Trust, pour répondre aux nouveaux risques de sécurité induits par l'utilisation croissante de l'IA. Sécurisez les systèmes d'IA avec une approche multidimensionnelle : traitez les menaces spécifiques, telles que l'injection de prompt et l'empoisonnement de données, grâce à une connaissance approfondie des modèles et des ensembles de données, effectuez des tests de vulnérabilité proactifs et utilisez des défenses robustes comme la surveillance comportementale, la validation de contenu et les réponses automatisées aux attaques, qui sont intégrées à la fois dans les environnements de développement et d'exécution.

Méthodologie

Attaques des applications Web et attaques DDoS de couche 7

Ces données décrivent les alertes de la couche applicative sur le trafic vu à travers notre Web Application Firewall (WAF). 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 DDoS de couche 7 sont déclenchées lorsque nous détectons des anomalies volumétriques dans le nombre de requêtes adressées à un site Web, une application ou une API protégés. Ces alertes peuvent être déclenchées à la fois par des requêtes malveillantes et bénignes. Généralement, les requêtes elles-mêmes sont bénignes, mais leur volume élevé indique une intention malveillante. En revanche, ces alertes 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 Cloud, un réseau d'environ 340 000 serveurs répartis sur plus de 4 000 sites et environ 1 300 réseaux 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.

Ces données couvraient une période de 24 mois, du 1er janvier 2023 au 31 décembre 2024.

Données relatives aux attaques ciblant les API

Grâce à l'intégration de Noname Security, Akamai a amélioré nos capacités de recherche et de création de rapports sur les menaces ciblant les API. Cet ensemble de données est toujours en phase initiale d'intégration et d'analyse. Pour ce rapport, nous avons utilisé un échantillon de données sur 30 jours, issu du premier trimestre 2025, pour analyser la répartition des alertes de sécurité des API en fonction de leurs cadres de sécurité et de leurs normes de conformité. Cet ensemble de données continuera d'évoluer et il fournira à l'avenir une vue plus complète des problèmes de sécurité touchant les API.

Crédits

Directeur de recherche

Mitch Mayne

Édition et rédaction

Charlotte Pelliccia
Lance Rhodes
Badette Tribbey
Maria Vlasak

Révision et expertise

Tom Emmons
Reuben Koh
Richard Meeus
Stas Neyman
Steve Winterfeld

Analyse des données

Chelsea Tuttle

Documents promotionnels

Barney Beal
Ashley Linares

Marketing et publication

Georgina Morales Hampe
Emily Spinks

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 sur akamai.com/soti

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/security-research

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

Recherche sur la sécurité d'Akamai

Lisez le blog lié à la recherche sur la sécurité d'Akamai pour obtenir une réponse rapide aux éléments de recherche les plus importants d'aujourd'hui.
akamai.com/blog/security-research