SOTI

VOLUME 10 NUMÉRO 04

10 YEARS OF SECURITY INSIGHT

Menaces à la sécurisation des architectures applicatives

Vue d'ensemble de la zone EMEA

Akamai

État des lieux d'Internet/Sécurité

Table des matières

Principales conclusions du rapport

La vue d'ensemble de la zone EMEA vient compléter notre rapport État des lieux d'Internet plus général sur la sécurité des applications, intitulé Les pirates à l'assaut des infrastructures informatiques : menaces à la sécurisation des architectures applicatives (disponible en anglais uniquement). Veuillez consulter ce rapport pour savoir comment nos adversaires exploitent la surface d'attaque en expansion. Vous y trouverez des recommandations pour mieux protéger votre organisation, ainsi que des explications concernant nos méthodologies de recherche.

Présentation

Au cours des deux dernières décennies, les applications Web ont connu une croissance exponentielle en termes de nombre et de capacités, rationalisant les opérations commerciales, améliorant l'expérience des clients et stimulant la croissance grâce à des fonctionnalités telles que la communication en temps réel, l'analyse des données et l'automatisation des processus. Les API, qui constituent la base de la communication entre les applications, ont également proliféré et sont maintenant prêtes à faire leur propre saut exponentiel.

Les applications interviennent à presque tous les niveaux de l'entreprise, facilitant des milliers de milliards de connexions tout en les rendant plus vulnérables aux attaques. Dans cette vue d'ensemble de la région EMEA, qui couvre la période de janvier 2023 à juin 2024, nous avons une vue globale des menaces qui affectent les applications, notamment les attaques Web, les attaques par déni de service distribué (DDoS) et les menaces pesant sur les charges de travail critiques, en nous concentrant sur ce que cela signifie pour vous.

Le nombre d'attaques DDoS sur les couches 3 et 4 a augmenté régulièrement dans la région Europe, Moyen-Orient et Afrique (EMEA), dépassant le nombre d'attaques en Amérique du Nord au cours de cinq des sept derniers mois. Le secteur des services financiers a été le plus touché par ces attaques.

L'activité mensuelle des attaques contre les applications Web et les API dans la région EMEA s'est accrue au cours de cette période, avec une croissance de 21 % entre le 1er trimestre 2023 et le 1er trimestre 2024 ; les attaques ciblant les API représentent en moyenne 40 % des attaques Web mensuelles.

Le commerce a été le secteur le plus touché par les attaques Web dans la région EMEA, en raison d'un pourcentage élevé d'attaques d'API, et a également été le secteur le plus touché par les attaques DDoS de couche 7.

Les ransomwares et autres attaques sur les applications et les charges de travail internes entre elles constituent une préoccupation croissante. Les entreprises se tournent vers la microsegmentation logicielle pour obtenir la visibilité et les contrôles granulaires nécessaires à la protection de cette surface d'attaque en expansion.

Les applications Web et les API : des sources riches de risques de sécurité

Les attaques contre les applications Web et les API prolifèrent à mesure que les entreprises s'empressent de déployer des applications pour améliorer l'expérience de leurs clients et stimuler leur activité. Les acteurs de la menace tirent parti des vulnérabilités de cette surface d'attaque (par exemple, des applications Web présentant des défauts de codage et de conception et des vulnérabilités vieilles de plusieurs années). En outre, l'expansion rapide de l'économie des API a offert aux cybercriminels de nouvelles possibilités d'exploitation des vulnérabilités et de la logique métier :

Les tendances des attaques en chiffres

Dans notre premier rapport État des lieux d'Internet de 2024, nous avons examiné les tendances des attaques d'API en 2023 dans le contexte de l'ensemble des attaques d'applications Web. En étudiant les 18 derniers mois, de janvier 2023 à juin 2024, les chercheurs d'Akamai ont constaté que l'activité mensuelle des attaques d'applications Web et d'API dans la région EMEA a augmenté de 21 % entre le 1er trimestre 2023 et le 1er trimestre 2024, et est restée élevée au 2e trimestre 2024. Les attaques contre les API, qui représentent en moyenne 40 % des attaques Web mensuelles au cours de cette période (EMEA, Figure 1), ont contribué à ce niveau d'activité soutenu.

Région EMEA : Attaques mensuelles ciblant les applications Web et les API

Du 1er janvier 2023 au 30 juin 2024

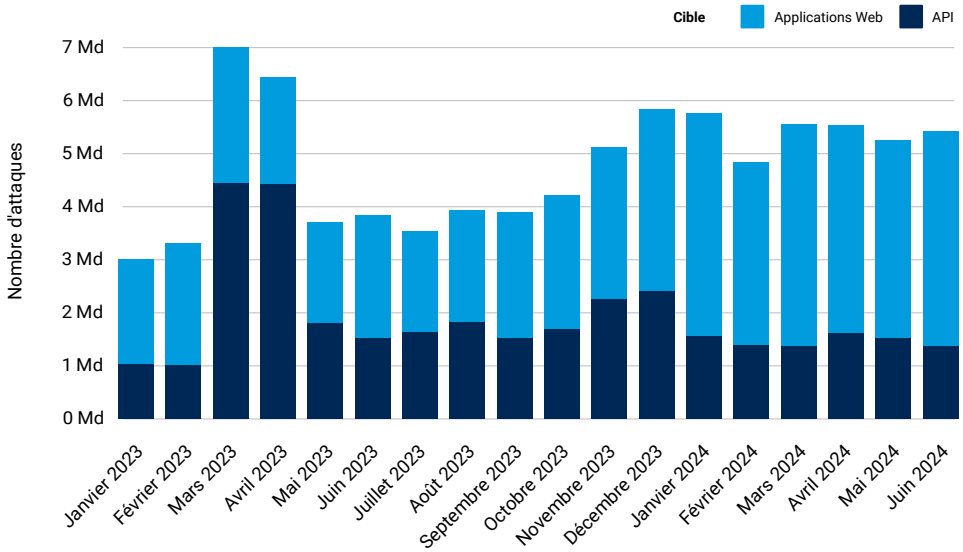

Fig. 1 zone EMEA : Les attaques mensuelles sur les applications Web et les API restent élevées en 2024 (REMARQUE : le pic d'attaques d'API est lié au secteur du commerce en Espagne, un pays où la concentration des attaques d'API est déjà très importante).

Au sein de la région EMEA, le Royaume-Uni (20,5 milliards), les Pays-Bas (15,6 milliards) et l'Espagne (12,7 milliards) ont subi le plus grand nombre d'attaques d'applications Web et d'API. L'Allemagne (8,7 milliards), l'Autriche (7,4 milliards), la France (4,8 milliards), Israël (3 milliards), l'Italie (2,7 milliards), la Suisse (2,5 milliards) et la Belgique (2,3 milliards) complètent le top 10.

Akamai suit également plusieurs vecteurs d'attaques sur le Web. Dans ce rapport, nous nous concentrons sur les cinq principales méthodes d'attaque traditionnelles basées sur des vecteurs.

Conformément aux rapports précédents, l'inclusion de fichiers locaux (LFI) est restée un vecteur d'attaque privilégié, mais d'autres vecteurs, tels que l'injection SQL (Structured Query Language) et le cross-site scripting (XSS), sont également des sujets de préoccupation (EMEA, Figure 2).

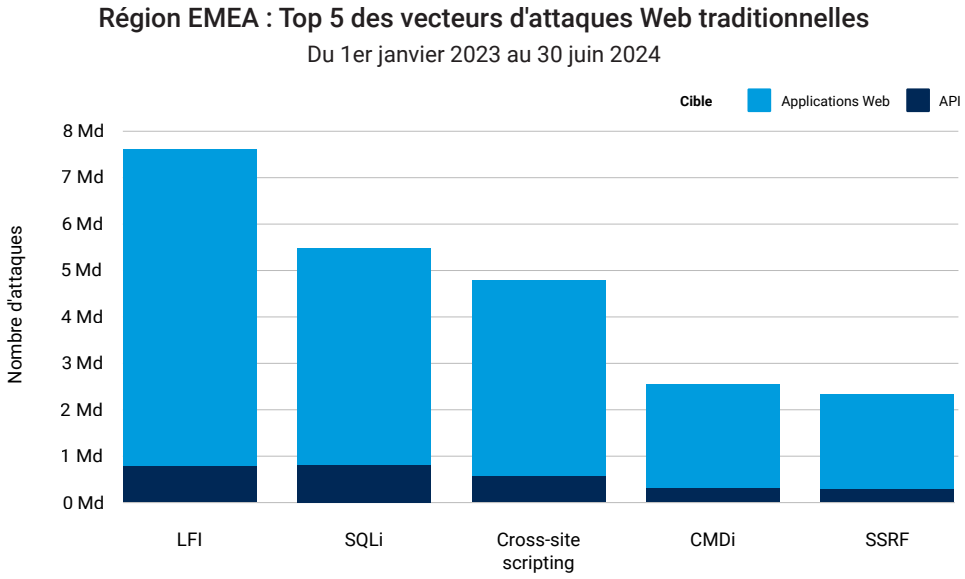

Fig. 2 zone EMEA : Les attaques LFI, SQLi et XSS stimulent la croissance des attaques d'applications Web et d'API

Il n'est pas rare que les attaquants utilisent des tactiques traditionnelles telles que les attaques de type LFI et SQLi afin d'accéder aux données de leurs cibles. En outre, l'attaque de type LFI permet aux attaquants de s'implanter dans les systèmes de leurs cibles et d'exécuter du code à distance, compromettant ainsi leur sécurité.

Conformément à la tendance observée dans les rapports précédents, le commerce et les médias vidéo sont les secteurs les plus touchés par les attaques d'applications Web et d'API dans la région EMEA. En outre, comme nous l'avons indiqué dans notre rapport État des lieux d'Internet sur la sécurité des API, le commerce a continué à subir le pourcentage le plus élevé d'attaques d'API par rapport aux autres secteurs de la région (EMEA, Figure 3).

Région EMEA : Attaques d'applications Web et d'API par segment de marché

Du 1er janvier 2023 au 30 juin 2024

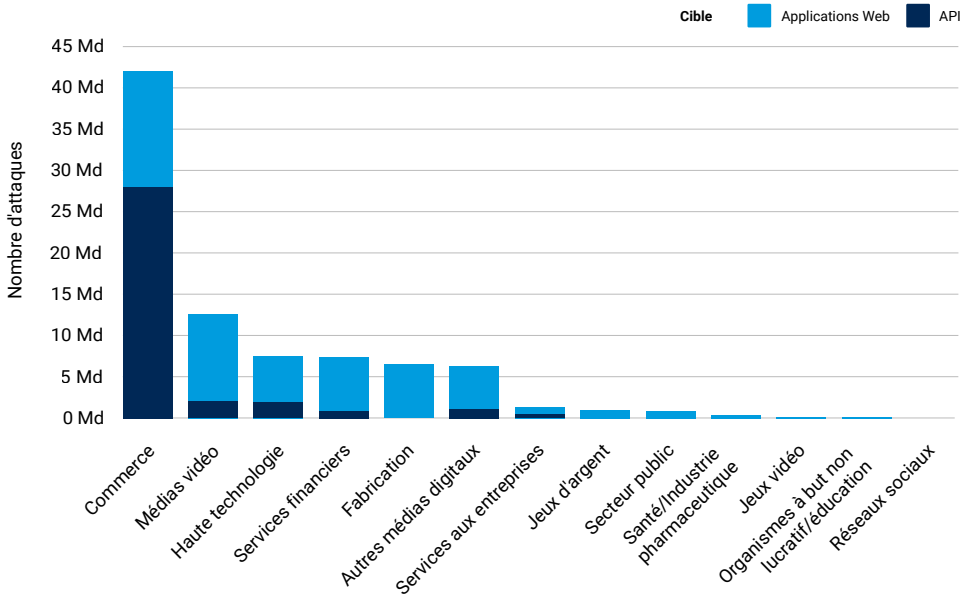

Fig. 3 zone EMEA : En raison d'un pourcentage élevé d'attaques d'API, le commerce est le secteur le plus touché par les attaques Web, suivi par les médias vidéo, la haute technologie et les services financiers.

Les attaques DDoS menacent la disponibilité des applications

La surface d'attaque continue de s'étendre, tout comme les types d'attaques DDoS qui affectent les applications. Comme expliqué plus en détail dans le rapport État des lieux d'Internet global, les attaques DDoS traditionnelles contre l'infrastructure (couches 3 et 4) sont les plus anciennes et visent à submerger la capacité du réseau ou du serveur d'application. Les attaques DDoS au niveau de la couche applicative (couche 7) exploitent les vulnérabilités, ainsi que les failles et/ou les imperfections de la logique métier dans la couche applicative. Elles sont capables de causer des dommages importants, même avec une quantité relativement faible de trafic malveillant. Quel que soit le vecteur d'attaque, une attaque DDoS réussie entraîne l'indisponibilité de l'application.

La gamme des types d'attaques DDoS et les tendances dans la région ont été explorées en profondeur dans notre récent rapport État des lieux d'Internet EMEA 2024. Nous incluons ici des données actualisées qui démontrent l'augmentation continue des menaces d'attaques DDoS des couches 3 et 4 et de la couche 7 pour l'infrastructure qui alimente les applications, ainsi que pour les applications elles-mêmes.

Attaques DDoS d'infrastructure

Au cours de la période de référence de 18 mois allant de janvier 2023 à juin 2024, les chercheurs d'Akamai ont constaté que le nombre d'attaques DDoS des couches 3 et 4 a augmenté régulièrement dans la région EMEA, dépassant le nombre d'attaques DDoS mensuelles en Amérique du Nord pendant cinq des sept derniers mois (EMEA, Figure 4).

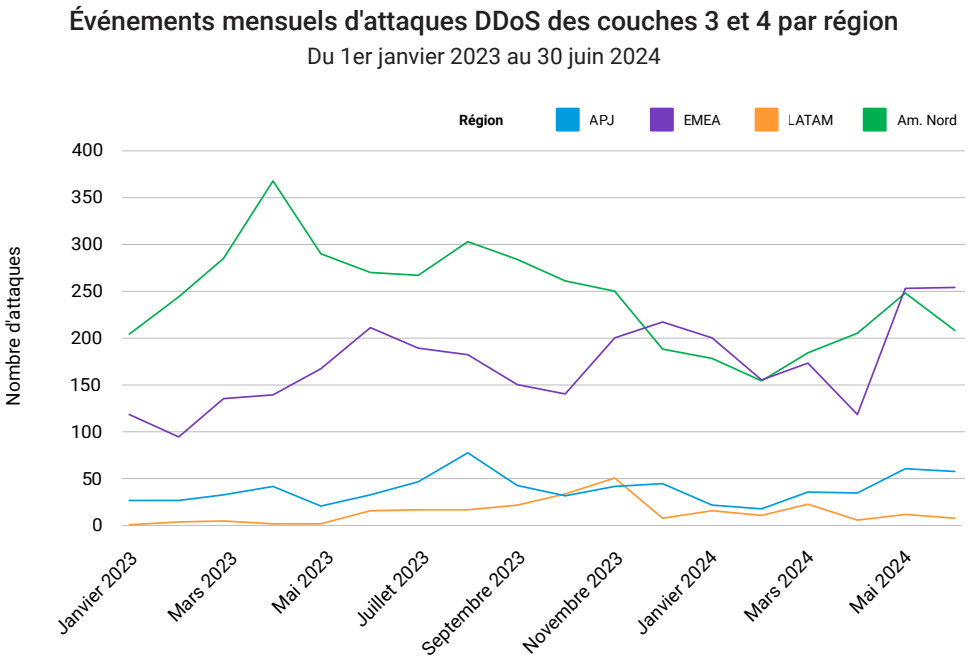

Fig. 4 zone EMEA : Le nombre mensuel d'attaques DDoS sur les couches 3 et 4 dans la région EMEA a dépassé celui de l'Amérique du Nord pendant cinq des sept derniers mois.

Dans la région EMEA, les pays les plus touchés par les attaques DDoS des couches 3 et 4 sont l'Arabie saoudite (957) et le Royaume-Uni (576), suivis de la Suisse (240), de la Turquie (205), de l'Italie (203), de l'Allemagne (189) et de la Pologne (115).

Comme indiqué dans notre rapport État des lieux d'Internet EMEA, l'attaque DDoS est un outil populaire pour les hacktivistes à motivation politique et les attaquants parrainés par des États-nations. Les guerres Russie-Ukraine et Israël-Hamas ont conduit à une multiplication des attaques.

D'un point de vue sectoriel, les services financiers (1 523) et l'industrie manufacturière (890) ont connu le plus grand nombre d'attaques DDoS des couches 3 et 4, suivis par les jeux vidéo (189), le commerce (151), les jeux d'argent (105) et la haute technologie (95).

Les attaques DDoS au niveau de la couche applicative

Outre les attaques DDoS des couches 3 et 4, la région a également été touchée par des attaques DDoS de la couche applicative (couche 7). Au cours de la période de référence de 18 mois allant de janvier 2023 à juin 2024, nos chercheurs ont constaté que la zone EMEA était la troisième région la plus touchée par les attaques DDoS de couche 7, enregistrant 1 900 milliards contre 8 700 milliards en Amérique du Nord et 5 100 milliards dans la région APJ.

Bien qu'il soit inférieur à ceux d'autres régions, il est important de noter que le nombre d'attaques DDoS de la couche 7 dans la zone EMEA est en hausse. Après une baisse en mai 2023 à 74 milliards, les attaques DDoS mensuelles de couche 7 ont eu tendance à augmenter de manière significative, doublant presque en mars 2024 ; le deuxième trimestre 2024 s'est terminé avec une moyenne mensuelle de 119 milliards d'attaques ciblant les applications Web et les API (EMEA, Figure 5).

Région EMEA : Attaques DDoS de couche 7 par mois

Du 1er janvier 2023 au 30 juin 2024

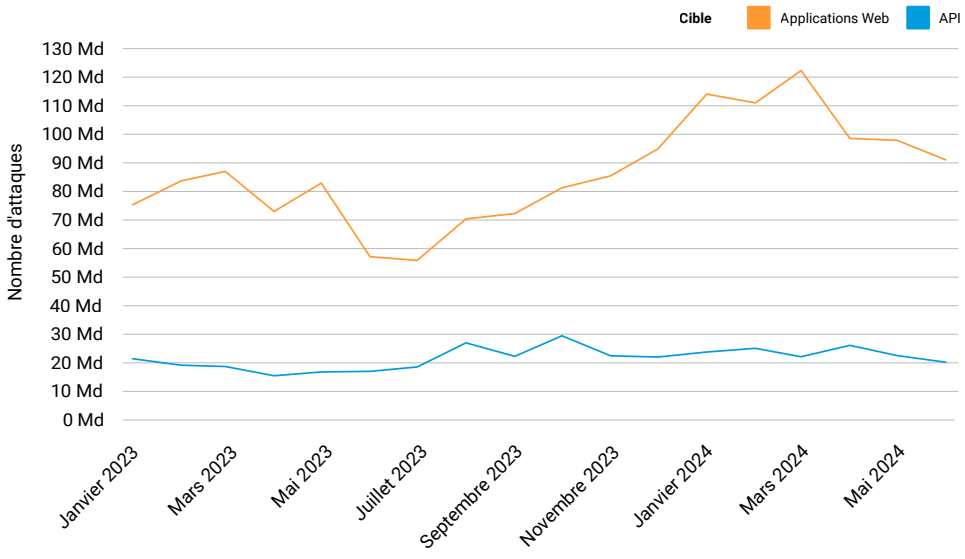

Fig. 5 zone EMEA : Les attaques DDoS de couche 7 ont augmenté de manière significative depuis juin 2023, terminant le deuxième trimestre 2024 avec une moyenne mensuelle de 119 milliards d'attaques.

Au cours de cette période, les attaques DDoS ciblant les API sont restées relativement stables, représentant 25 % du total de ces attaques. Ainsi, outre la défense contre les vecteurs d'attaque évoqués précédemment concernant les attaques contre les applications Web et les API (voir EMEA, Figure 2), la défense des API contre les attaques DDoS est un impératif évident, d'autant plus que les directives et les réglementations continuent d'encourager l'utilisation des API.

Au sein de la région EMEA, les régions ayant subi le plus grand nombre d'attaques DDoS de couche 7 sont l'Allemagne (461 milliards) et le Royaume-Uni (366 milliards), devant la Suède (167 milliards), Israël (151 milliards), l'Italie (125 milliards), Malte (113 milliards), la Suisse (112 milliards), la France (90 milliards), les Pays-Bas (79 milliards) et l'Espagne (77 milliards).

L'analyse sectorielle révèle que le secteur le plus touché par les attaques DDoS de couche 7 au début comme à la fin de cette période est le secteur du commerce, suivi par les autres médias digitaux, les médias vidéo et la haute technologie (EMEA, Figure 6).

Région EMEA : Attaques DDoS mensuelles de couche 7 par segment de marché

Du 1er janvier 2023 au 30 juin 2024

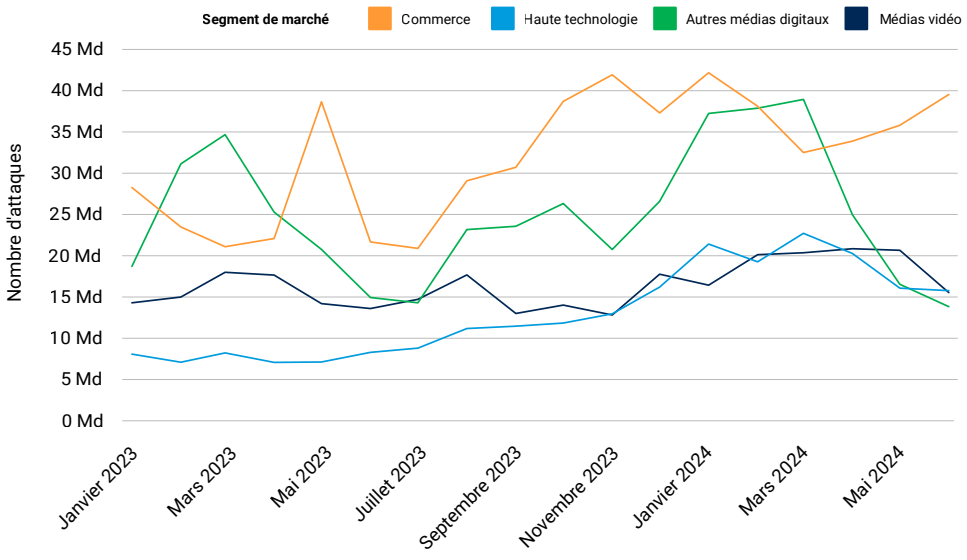

Fig. 6 zone EMEA : Le secteur du commerce a été le plus touché par les attaques DDoS de couche 7

Les attaquants se concentrent sur les charges de travail applicatives

L'approche Zero Trust est généralement envisagée dans le contexte de la sécurité des réseaux. Cependant, les applications Web et les charges de travail internes qui les relient peuvent également être exposées à des menaces telles que les ransomwares, qui cherchent n'importe quel point d'entrée et n'importe quel chemin pour atteindre leurs cibles.

Comme l'explique en détail le rapport global, pour que les applications fonctionnent (que ce soit dans le cloud, sur site ou dans un environnement hybride), chaque charge de travail individuelle doit fonctionner de manière fluide. Les charges de travail traversent plusieurs juridictions de sécurité lorsqu'elles se déplacent sur le réseau, et chaque nouvelle juridiction ajoute un point d'entrée potentiel pour un intrus. La protection de cette surface d'attaque étendue est essentielle pour renforcer la posture de sécurité globale, mais complique encore davantage le travail déjà difficile des équipes de sécurité.

La mise en œuvre d'une structure Zero Trust à partir d'une approche matérielle traditionnelle est un effort coûteux en ressources et en temps, qui nécessite des temps d'arrêt. En outre, une véritable implémentation Zero Trust exige une microsegmentation susceptible de protéger contre les ransomwares ou les attaques sur les charges de travail elles-mêmes.

La microsegmentation logicielle est rapide et facile à mettre en œuvre et à utiliser, de sorte qu'elle peut même servir de mesure viable de réponse aux incidents et de contrôle pour isoler les systèmes critiques dans le cadre de la conformité réglementaire. Elle permet une visualisation approfondie du réseau et des contrôles de gouvernance extrêmement granulaires. En raison de ces avantages, les entreprises se tournent de plus en plus vers cette approche pour détecter et atténuer une charge de travail ou un conteneur menacé dans leurs environnements dynamiques de centre de données, cloud et cloud hybride.

Enseignements tirés d'exemples concrets de protection des charges de travail applicatives

Dans cette section, nous présentons deux études de cas de la région EMEA qui illustrent la manière dont les entreprises sécurisent les charges de travail critiques et font progresser le modèle Zero Trust.

Étude de cas EMEA n° 1 : afin de protéger les systèmes critiques et les données sensibles liées aux transactions et aux paiements, le responsable des technologies de sécurité de l'information (CISO) d'une grande banque d'investissement examine régulièrement la sécurité de son infrastructure technologique afin de renforcer la posture de sécurité de tous ses domaines. Ses priorités : l'arrêt des attaques de ransomware, l'évolutivité et la couverture des différents systèmes d'exploitation et environnements cloud. Le CISO souhaitait également trouver un moyen de réduire la surface d'attaque sans encourir les coûts et les retards associés à la mise à niveau des anciens pare-feux. Les charges de travail applicatives ont été séparées les unes des autres par la mise en œuvre d'une approche de microsegmentation logicielle qui crée des zones sécurisées dans les environnements des centres de données. Si une charge de travail est attaquée, elle peut être isolée, ce qui empêche les logiciels malveillants de se propager sur l'ensemble du réseau.

Étude de cas EMEA n° 2 : un fournisseur de médias et de logiciels avait besoin d'un moyen plus facile pour faire progresser sa structure Zero Trust afin de mieux protéger les charges de travail critiques et les données des clients. Pour réaliser cette amélioration, il était impératif de ségréger les composants de grande valeur, tels que les systèmes de gestion des identités et de planification des ressources de l'entreprise, à l'aide de politiques de segmentation précises. L'objectif était de minimiser le trafic entrant et sortant et de renforcer les politiques d'accès sur des centaines de serveurs d'entreprise. Dans le même temps, l'entreprise souhaitait éviter d'apporter des changements majeurs à l'écosystème, susceptibles de provoquer des perturbations et d'accroître les risques en matière de sécurité. Une approche de microsegmentation logicielle avec une visibilité granulaire des modèles d'interaction, ainsi que des alertes, a permis à l'équipe de prévenir les mouvements latéraux malveillants dans l'ensemble du réseau.

Conclusion

Dans cette vue d'ensemble de la région EMEA, nous avons tenté de fournir une vue holistique des différentes façons dont les acteurs de la menace peuvent cibler vos applications et vos API. Du point de vue de la sécurité et de la gestion des risques, il est vital pour les organisations de comprendre les menaces qui pèsent sur les applications et les API, l'infrastructure et les charges de travail critiques et de défendre ces dernières. En outre, la législation actuelle et à venir rend impérative la sécurisation des applications.

Au sein de l'EMEA, dans l'Union européenne, la législation clé à cet égard comprend la directive sur la sécurité des réseaux et des systèmes d'information (NIS2), la réglementation sur la résilience opérationnelle digitale (DORA), la loi sur la cyberrésilience, le programme européen pour la protection des infrastructures critiques, la nouvelle norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS) v4.0 et la directive sur les services de paiement (PSD3) révisée qui sera bientôt publiée.

Les applications sont plus importantes que jamais pour les entreprises, mais aussi plus vulnérables aux attaques. Grâce à des fonctionnalités et meilleures pratiques permettant de relever les défis liés à une surface d'attaque en constante expansion, les entreprises peuvent protéger les applications qu'elles créent partout, à tout moment, sans compromettre les performances ou l'expérience des clients.

Pour en savoir plus, nous vous invitons à consulter notre rapport État des lieux d'Internet sur la sécurité des applications intitulé « Les pirates à l'assaut des infrastructures informatiques : menaces à la sécurisation des architectures applicatives ».

Méthodologie

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 Connected 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 18 mois, du 1er janvier 2023 au 30 juin 2024.

Mise à jour des données 2024

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

DDoS (couches 3 et 4)

Akamai Prolexic Routed défend les entreprises contre les attaques DDoS en bloquant les attaques et tout autre trafic indésirable ou malveillant avant que les menaces n'atteignent les applications, les centres de données et les infrastructures Internet cloud et hybrides (publiques ou privées), y compris tous les ports et les protocoles. Les experts du SOCC Akamai (Security Operations Command Center) conçoivent des contrôles d'atténuation proactifs pour détecter et arrêter les attaques instantanément, et analysent directement le trafic restant afin de déterminer des mesures d'atténuation supplémentaires, le cas échéant. Ces attaques atténuées sont organisées et regroupées en événements d'attaque, et toutes les données associées sont enregistrées par le SOCC à des fins d'analyse.

Ces données couvraient une période de 18 mois, du 1er janvier 2023 au 30 juin 2024.

Crédits

Directeur de recherche

Mitch Mayne

Édition et rédaction

Tricia Howard
Charlotte Pelliccia
Lance Rhodes
Badette Tribbey
Maria Vlasak

Révision et expertise

Sven Dummer
Reuben Koh
Tony Lauro
Richard Meeus
Menacham Perlman
Sandeep Rath
Steve Winterfeld

Analyse des données

Chelsea Tuttle

Documents promotionnels

Barney Beal

Marketing et publication

Georgina Morales
Emily Spinks

Autres rapports État des lieux d'Internet/Sécurité

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

D'autres recherches sur les menaces d'Akamai

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

Accéder aux données de ce rapport

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

En savoir plus sur les solutions Akamai

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

Akamai protège votre expérience client, votre personnel, vos systèmes et vos données en vous aidant à intégrer la sécurité dans tout ce que vous créez, dans toutes vos conceptions et diffusions. La visibilité de notre plateforme sur les menaces mondiales nous aide à adapter et à faire évoluer votre stratégie de sécurité (activer le Zero Trust, bloquer les ransomwares, sécuriser les applications et les API, ou lutter contre les attaques DDoS), vous donnant ainsi la confiance nécessaire pour innover, prospérer et ouvrir le champ des possibles. Pour en savoir plus sur les solutions de Cloud Computing, de sécurité et de diffusion de contenu, rendez-vous sur akamai.com et akamai.com/blog, ou abonnez-vous à Akamai Technologies sur X (anciennement Twitter) et LinkedIn. Publication : 08/24.