Akamai

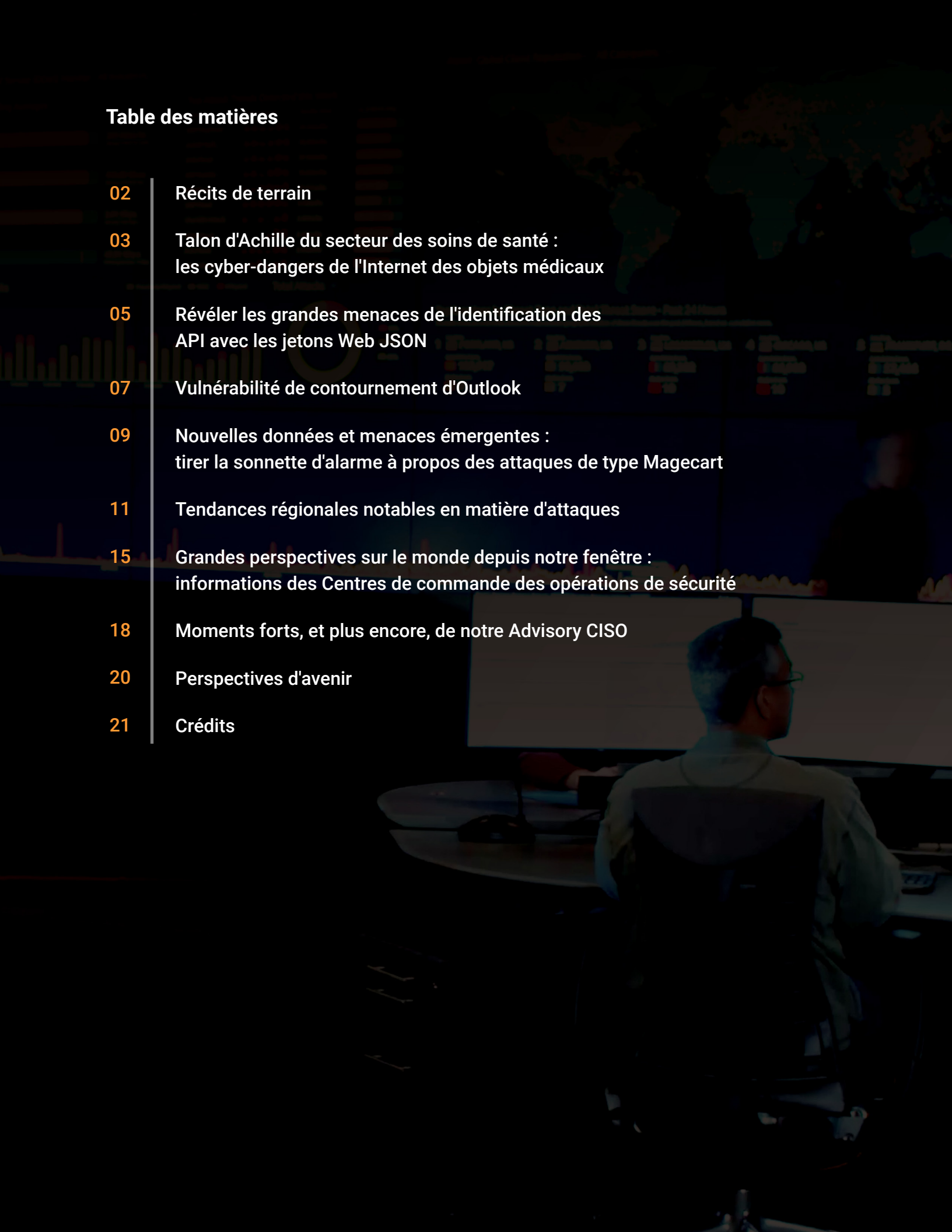
État des lieux d'Internet

Volume 9 | Numéro 6

Une année passée au crible

Étude des cybertendances en 2023 et à venir

Table des matières



Récits de terrain

Pour ce rapport État des lieux d'Internet, nous nous éloignons de l'analyse habituelle de fin d'année, dans laquelle nous revenons sur chaque rapport que nous avons publié cette année, pour plutôt nous concentrer sur le thème central suivant : quelle est votre histoire préférée de l'année en matière de sécurité ? Nous avons demandé aux rédacteurs et à un spécialiste des données du groupe Security Intelligence (SIG) d'Akamai de réaliser une évaluation de fin d'année d'une histoire parmi toutes celles que nous avons couvertes au cours des 10 derniers mois. Il a dû être difficile pour eux de choisir seulement une des nombreuses histoires marquantes et nouvelles découvertes que nous avons publiées sur notre blog de recherche sur la sécurité et dans les rapports État des lieux d'Internet en 2023. Nous avons également demandé à notre Advisory CISO et à un vice-président de nos Centres de commande des opérations de sécurité (SOCC) d'évaluer les tendances de cette année en matière d'attaques et les principales leçons à retenir pour 2024.

Beaucoup de choses se sont produites cette année dans le monde de la sécurité et en ce qui concerne la recherche sur la sécurité d'Akamai. Les contributions à la recherche de nos experts en sécurité sont sans aucun doute inestimables pour la communauté. Grâce à notre hub dédié, les professionnels de la sécurité peuvent facilement accéder à des ressources fiables contenant des informations, des stratégies d'atténuation et des tendances en matière d'attaque qui peuvent les aider à défendre leurs organisations. Ils peuvent également accéder à des outils gratuits, comme notre boîte à outils RPC, ainsi qu'à notre plateforme d'émulation pro-active des menaces open source gratuite, Infection Monkey. Agissant comme le ferait un logiciel malveillant, Infection Monkey propage et « chiffre » les fichiers auxquels il peut accéder en basculant les bits, et donne ainsi aux spécialistes une vision réaliste de la façon dont un attaquant pourrait (ou ne pourrait pas) se mouvoir dans cet environnement. La vitesse à laquelle les menaces évoluent rend nécessaire la réalisation de tests en continu. Les spécialistes ont besoin de savoir où en est leur réseau aujourd'hui, et pas seulement où il en était lors du dernier test de pénétration.

Si l'on pouvait décrire en un mot l'écosystème en 2023, ce mot serait *pivot*. Les attaquants ont modifié leurs tactiques pour contourner les mesures de sécurité, recherchant de nouvelles surfaces d'attaque et des cibles inexploitées pour semer le chaos dans les organisations de toutes tailles et de tous secteurs. Il en va de même pour les spécialistes de la sécurité qui continuent de s'adapter et d'apprendre de nouvelles façons d'atténuer les attaques et de mieux protéger les organisations. Nous pivotons à travers les solutions, la recherche et les outils avec l'objectif suivant : fournir des informations exploitables et des stratégies d'atténuation aux professionnels de la sécurité qui combattent les mêmes menaces que nous.

Bonne lecture !

Meilleures success stories de sécurité

Tendances des attaques en 2023

Perspectives d'avenir pour 2024

Talon d'Achille du secteur des soins de santé : les cyber-dangers de l'Internet des objets médicaux

Je suis Badette Tribbey, l'une des narratrices des rapports État des lieux d'Internet, et je collabore avec des experts en sécurité et des spécialistes des données pour transformer les découvertes et les données techniques en informations significatives. Je déteste les maths, mais j'aime la façon dont les chiffres peuvent révéler des tendances convaincantes en matière d'attaque.

L'un des sujets les plus importants que nous avons traités cette année nous touche de près : il concerne les risques accrus de l'Internet des objets médicaux (IoMT). Dans Se faufiler à travers les failles de sécurité et Les ransomwares évoluent, nous avons examiné le paysage des risques dans le secteur des soins de santé et des sciences de la vie, et ce qui rend ce secteur vulnérable aux attaques. L'une des choses qui m'a le plus frappée est la façon dont les ressources de l'IoMT, tels que les appareils IRM, les pompes à insuline et les accessoires connectés, bien que très bénéfiques pour les patients, ont considérablement augmenté les risques pour les professionnels de santé. Ces organisations avaient déjà des problèmes pour sécuriser leur périmètre en raison de la complexité de l'écosystème de la santé, de la vulnérabilité des technologies existantes et des problèmes de dotation en personnel informatique et de cybersécurité. En outre, l'application de correctifs en temps opportun dans cet environnement peut être une tâche herculéenne, avec des mises à jour provenant de divers fournisseurs pour des systèmes ou applications multiples, ce qui rend le suivi difficile.

Les terminaux IoMT non protégés par des correctifs comptent parmi les ressources les plus vulnérables dans tous les secteurs et ils peuvent introduire des menaces plus néfastes comme les ransomwares. Au fur et à mesure que l'IoMT croît de manière exponentielle (et avec lui, l'utilisation des API), ses vulnérabilités augmentent également, et elles peuvent potentiellement devenir des voies d'accès pour les attaquants qui peuvent ainsi s'implanter dans les systèmes de leurs cibles, ou être utilisées abusivement et entraîner des fuites de données (Figure 1). Un rapport conjoint de Cynerio et du Ponemon Institute sur une étude menée dans plusieurs hôpitaux et systèmes de santé aux États-Unis indique que plus de la moitié d'entre eux ont subi des cyberattaques en raison de failles de sécurité dans les terminaux IoMT.

> L'application rapide de correctifs dans cet environnement [de la santé] peut être une tâche herculéenne, avec des mises à jour provenant de divers fournisseurs pour des systèmes ou applications multiples, ce qui complique le suivi.
>
> **– Badette Tribbey, Senior Technical Writer, Akamai**

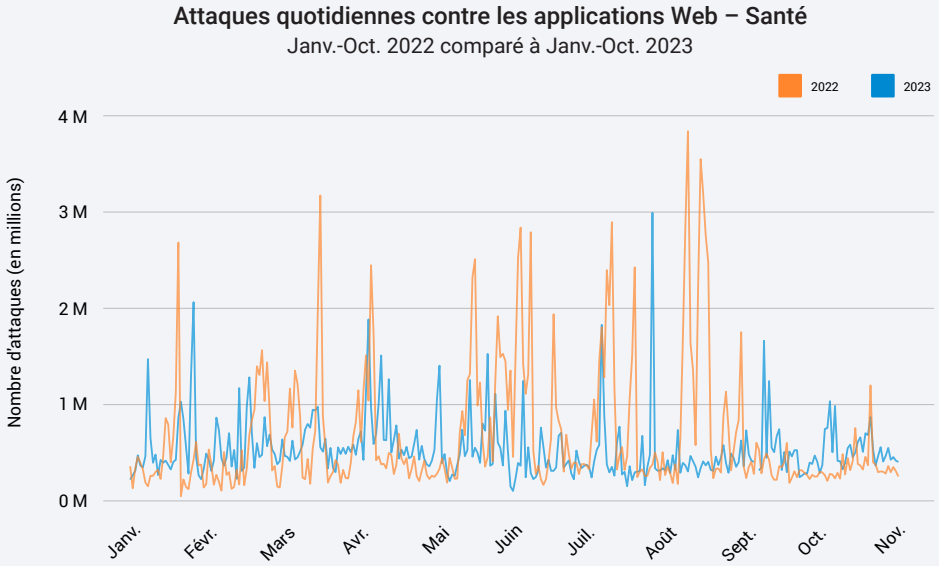


Figure 1 : Les attaques ciblant les applications Web et les API dans le secteur des soins de santé et produits pharmaceutiques sont constantes, avec des pics sporadiques entre 2022 et 2023. Bien que le nombre d'attaques ait diminué de 21 % d'une année sur l'autre, le nombre moyen d'attaques par jour en 2023 est plus élevé qu'en 2022.

Quelle est la prochaine étape pour le secteur des soins de santé ?

À mesure que le secteur des soins de santé développe son IoMT, les API vont continuer de jouer un rôle essentiel dans l'accessibilité des services médicaux (p. ex., télésanté et suivi à distance des patients), ce qui mènera à de meilleurs résultats cliniques et financiers. Et, en raison de la grande valeur des dossiers médicaux et des données des patients sur le dark web, les attaques contre le secteur des soins de santé ne ralentiront probablement pas.

À mesure que notre vision évolue entre ce qui se passe et ce à quoi nous pouvons nous attendre, il apparaît clairement que les attaquants vont continuer à innover et à accroître la portée et la complexité de leurs attaques. Il est probable que nous assisterons à une poussée continue d'attaques plus techniques tirant parti des vulnérabilités Zero Day. En outre, le contexte réglementaire (y compris, mais sans s'y limiter, la loi Protecting and Transforming Cyber Health Care [PATCH] Act de 2022) est en train de changer. Nous devons donc veiller à ce que nos solutions puissent nous aider à nous conformer à un grand nombre de lois imminentes sur la confidentialité, la création de rapports, les paiements, la souveraineté des données et la résilience. Enfin, nous nous attendons à d'autres perturbations dans les attaques pour les CISO qui modifient leurs budgets afin de diminuer le nombre de fournisseurs et utiliser des solutions qui réduisent les temps d'arrêt pour les pirates informatiques qui sont entrés dans les systèmes.

Révéler les grandes menaces de l'identification des API avec les jetons Web JSON

Je m'appelle Lance Rhodes et j'ai le plaisir d'être Cybersecurity Writer au sein de l'équipe SIG d'Akamai depuis mars 2023. Une grande partie de mon travail sert de « tissu conjonctif » entre nos rapports et nos blogs, car je travaille à la fois sur les aspects de publication et de rédaction des articles de blog et des études transversales et sur la rédaction de contenu et de supports marketing pour les rapports État des lieux d'Internet. Tout cela est lié à ma collaboration avec l'équipe pour la rédaction de nos bulletins d'information mensuels internes et externes, ainsi que pour les présentations aux conférences sur la sécurité.

Je dois dire que l'un des articles de blog les plus passionnants sur lesquels j'ai travaillé cette année était l'article sur les jetons Web JSON (JWT). Il était en lien direct avec le rapport État des lieux d'Internet sur les applications et les API (Se faufiler à travers les failles de sécurité) dans la mesure où il abordait la violation d'authentification dans les JWT, l'une des méthodes d'identification standard pour les API. Il était donc intéressant d'acquérir une compréhension plus approfondie des JWT.

Après avoir travaillé sur le rapport État des lieux d'Internet sur les applications et les API en début d'année, j'ai commencé à travailler avec Nitzan Namer sur l'article JWT, qui était axé sur les JWT comme vecteurs d'attaques d'authentification brisée des utilisateurs, un des 10 principaux risques pour la sécurité des API selon l'OWASP (Open Web Application Security Project). Le rapport État des lieux d'Internet comportait une section spécifique consacrée à ce sujet, mais l'article de blog abordait plus en détail la structure des JWT et les meilleures pratiques pour se protéger contre les menaces les plus importantes, notamment l'élévation des privilèges, la fuite de données et le piratage de comptes.

Je me souviens d'avoir parlé avec Nitzan de la façon dont nous espérions que l'article serait utilisé comme une ressource permanente pour les chercheurs en sécurité, les techniciens, et les utilisateurs et administrateurs de JWT. L'article répond à cet espoir grâce à son style structurel : les bases des JWT sont énumérées en premier, suivies de six études de cas, qui comprennent des illustrations de certaines menaces courantes et indiquent les meilleures pratiques dans chaque cas. Les principes de base fournissent des informations sur la façon dont les JWT sécurisent les API en émettant des jetons contenant des informations à partager en tant qu'objets JSON. Chaque jeton est encodé, mais non chiffré, et se compose d'un en-tête, d'une charge utile et d'une signature de vérification (autorisant le fait que les données n'ont pas été modifiées depuis que le serveur a falsifié le jeton).

> “L'article de blog abordait plus en détail la structure des JWT et les meilleures pratiques pour se protéger contre les menaces les plus importantes, notamment l'élévation des privilèges, la fuite de données et le piratage de comptes.
>
> **– Lance Rhodes, Cybersecurity Writer, Akamai**

Les six scénarios sont les suivants :

1. Autoriser le serveur à utiliser un jeton sans validation
2. Utiliser la même clé privée pour différentes applications
3. Utiliser un algorithme de signature faible
4. Choisir une clé privée courte et/ou à faible entropie
5. Conserver des données sensibles dans la charge utile d'un JWT
6. Confondre les clés

Les JWT sont l'un des formats de vérification les plus courants ; il est essentiel de mettre en œuvre des mesures de sécurité appropriées, car le format offre une grande surface d'attaque qui laisse beaucoup de place aux erreurs. Bien que ces scénarios mettent en évidence certaines des menaces les plus courantes qui pèsent sur les JWT, il en existe encore beaucoup d'autres et les techniques d'attaque sont en constante évolution.

Les JWT ne sont ni chiffrés ni mis en œuvre dans un souci de sécurité

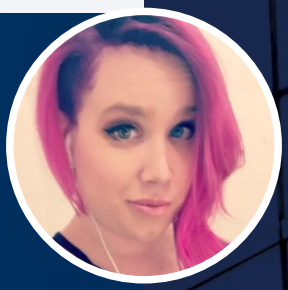
L'un des principaux enseignements que j'ai tirés de cet article de blog est que les JWT ne sont ni chiffrés ni mis en œuvre dans un souci de sécurité. Il est difficile de croire qu'un jeton d'authentification aussi populaire puisse être aussi vulnérable. Une partie de l'attrait des JWT est qu'ils permettent l'utilisation de nombreuses applications Web et API sans qu'il soit nécessaire de se connecter fréquemment. Le rapport État des lieux d'Internet et l'article de blog sur les JWT analysaient les algorithmes JWT dans le trafic Akamai et concluaient que les algorithmes symétriques sont les plus courants, même s'ils sont théoriquement moins sécurisés et moins protecteurs que les algorithmes asymétriques. Par exemple, les deux publications montrent que 54,8 % des clients d'Akamai utilisent l'algorithme HS256, qui est symétrique.

Il est probable que les algorithmes symétriques soient choisis plus souvent parce que l'utilisateur n'a besoin que d'une seule clé. En outre, les algorithmes asymétriques nécessitent une quantité plus élevée de ressources de calcul. JSON Web Encryption, la version chiffrée de JWT, n'est pas non plus très utilisé. La plupart des entreprises utilisent JWT et choisissent d'économiser de la puissance de calcul.

Résultats : la commodité, le coût et la rapidité sont souvent prioritaires sur la sécurité. Il s'agit d'un rappel précieux de l'importance de notre travail en tant que chercheurs et rédacteurs en sécurité. De bonnes études et pratiques en matière de sécurité sont nécessaires pour parvenir à un équilibre satisfaisant entre efficacité et sécurité.

> Il est difficile de croire qu'un jeton d'authentification aussi populaire puisse être aussi vulnérable.
>
> – Lance Rhodes, Cybersecurity Writer, Akamai

Vulnérabilité de contournement d'Outlook



Bonjour à tous ! J'espère que vous avez souri aujourd'hui ! Je m'appelle Tricia Howard et je travaille sur le blog du SIG. Je vis dans l'univers exigeant des rédactions techniques et je travaille avec nos chercheurs, notre équipe de communication d'entreprise et notre service juridique (entre autres) pour que les documents soient diffusés en temps voulu et de manière efficace. Ce que j'apprécie le plus dans mon travail c'est que je peux me vanter au nom de nos chercheurs parce qu'ils font des choses vraiment géniales !

Parmi tout ce qui m'a été demandé d'écrire cette année, c'est peut-être la partie la plus difficile : comment choisir ma préférée parmi toutes les choses extrêmement intéressantes que notre équipe a faites au cours des 12 derniers mois ? Mais comme il n'en faut qu'une, je choisis le travail de Ben Barnea sur la fameuse et notoire vulnérabilité de contournement d'Outlook. Ben est l'un des chercheurs les plus brillants que je connaisse et il a réussi à trouver un moyen de rompre un correctif entier… avec une seule barre oblique. Je sais que cela semble absurde, voire impossible, mais c'était possible, et il l'a fait.

La vulnérabilité d'origine permettait à un attaquant non autorisé d'envoyer une invitation Outlook avec un son de notification personnalisé. Ce son servait également de chemin d'attaque permettant à l'auteur de l'attaque de se connecter à son serveur en fournissant des informations d'identification NTLM. Il s'agit d'un gros problème : à partir de là, l'attaquant peut recourir à une attaque en force pour obtenir les informations d'identification ou lancer une attaque par relais. Toutes ces choses peuvent, bien sûr, mener à une élévation des privilèges, et nous savons tous ce qui peut se produire à partir de là. Le pire, c'est qu'il s'agit d'une vulnérabilité Zero Click, ce qui signifie qu'aucune action n'est requise de la part de l'utilisateur pour exécuter cette attaque. C'est donc une arme puissante qui devient franchement dangereuse, surtout lorsqu'on apprend qu'elle provient de Russie et qu'elle a été utilisée sur le terrain pour infiltrer diverses agences gouvernementales européennes.

Le correctif a été publié en mars. Il a annulé la possibilité d'utiliser *PidLidReminderFileParameter*, qui permettait à l'attaquant de spécifier le chemin personnalisé (c'est-à-dire de se connecter au serveur de la personne malveillante). À la place, le correctif utilise la fonctionnalité *MapURLtoZone*, qui permet de vérifier si le chemin tente de se connecter à Internet. S'il y a une tentative de connexion, le son de notification classique est émis, ce qui élimine l'option du chemin d'accès au fichier pour la notification personnalisée. En théorie, un attaquant distant n'aurait donc plus la possibilité de tirer parti de cette vulnérabilité ; il lui faudrait éventuellement passer par Internet pour établir une connexion avec la victime.

> “Les responsables des systèmes de défense ont déjà beaucoup à faire chaque jour sans avoir à se préoccuper des nouvelles vulnérabilités d'élévation des privilèges Zero Click.
>
> **– Tricia Howard, Senior Technical Writer, Akamai**

Contrecarrer le correctif

C'est là que cela devient intéressant et, si je puis dire, en fait assez drôle. Comme tout grand chercheur, Ben voulait vérifier que la vulnérabilité n'était vraiment plus exploitable. C'est une façon très simpliste de présenter les choses, mais il existe essentiellement deux options pour *MapURLtoZone* : autoriser ou refuser. Fait-il appel à Internet ou pas ? Dans l'ensemble, le correctif a agi comme prévu. Même lorsque le chemin semblait local, *MapURLtoZone* a reconnu qu'il avait pour but d'atteindre Internet et l'a empêché de le faire.

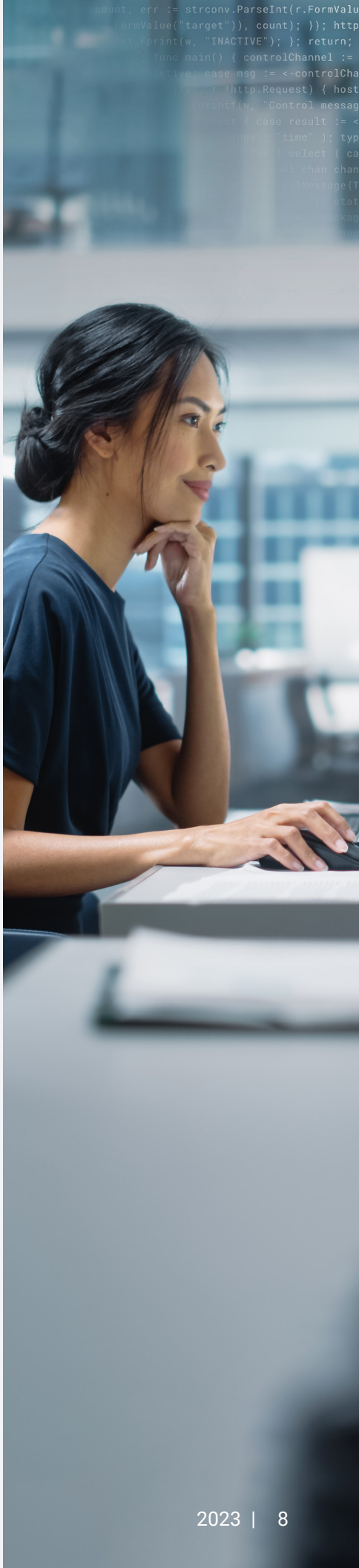
Ben a décidé de jouer avec le nom du chemin en ajoutant « / » à la fin de celui-ci. Lorsque vous fournissez un élément que *MapURLtoZone* n'attendait pas, il doit encore décider s'il l'autorise ou s'il le refuse. La barre oblique supplémentaire n'a pas été reconnue, ce qui a renvoyé un 0, que la fonction a lu comme étant local et de confiance. Ensuite, le reste de la vulnérabilité a pu s'exécuter exactement comme prévu en utilisant *CreateFile* pour le chemin personnalisé.

Et voilà ! Il a suffi d'ajouter une minuscule barre oblique pour rendre inefficace un correctif complet émis pour résoudre une vulnérabilité **critique**. Il a probablement fallu des jours, voire des semaines ou des mois, aux cyberprofessionnels pour créer ce correctif afin d'éliminer cette menace… et tout cela a été contrecarré par une seule petite barre oblique.

La sophistication même de l'attaque d'origine est assez stupéfiante lorsqu'on la décompose. L'attaquant mène un jeu de longue haleine, du niveau de Magnus Carlsen. Étant donné qu'il n'a fallu qu'une barre oblique pour rendre inutile le correctif, il va de soi que les attaquants auraient fini par trouver un contournement par eux-mêmes. C'est vraiment formidable que ce soit Ben qui l'ait découvert en sortant des sentiers battus.

C'est pour cette raison que les chercheurs qui découvrent ces bugs sont vraiment l'élément vital de la communauté de la sécurité. Les responsables des systèmes de défense ont déjà beaucoup à faire chaque jour sans avoir à se préoccuper des nouvelles vulnérabilités d'élévation des privilèges Zero Click. Les chercheurs en sécurité contribuent vraiment à rendre le monde meilleur, d'autant plus que nous devenons de plus en plus dépendants de la technologie et d'Internet dans notre vie quotidienne.

Je suis très fière de faire partie de cette formidable équipe et de travailler avec certains des esprits les plus brillants de cette planète. À tous ceux qui lisent nos blogs, nos tweets, nos rapports État des lieux d'Internet : Merci. Et aux chercheurs au sein et en dehors du SIG d'Akamai : merci pour tout ce que vous faites, interrompez et découvrez. Voyons ce que l'année prochaine nous réserve, d'accord ?



Nouvelles données et menaces émergentes : tirer la sonnette d'alarme à propos des attaques de type Magecart

Je m'appelle Chelsea Tuttle et je travaille chez Akamai depuis près de huit ans. En tant que scientifique responsable des données représentées dans les rapports État des lieux d'Internet ces quatre dernières années, je passe la majorité de mon temps à nettoyer, explorer, analyser et visualiser nos données. Lorsque je ne suis pas en train de regarder les données, je travaille en étroite collaboration avec les rédacteurs du rapport État des lieux d'Internet pour aider à communiquer les histoires que nos données nous racontent. En raison de la complexité des données volumineuses et des avantages des rapports sur les données historiques, nous ajoutons rarement un nouvel ensemble de données, mais cette année, nous l'avons fait ! Lorsque je regarde ce qui s'est passé en 2023, je pense que mes histoires préférées sont celles que nous avons publiées autour de ce nouvel ensemble de données parce que j'ai adoré les opportunités d'apprentissage qui ont accompagné cet effort.

> “Akamai s'efforce de combler l'écart entre commodité et sécurité créé par l'utilisation croissante de scripts tiers dans tous les secteurs.
>
> **– Chelsea Tuttle, Senior Data Scientist, Akamai**

Trop souvent, dans notre monde, nous nous concentrons sur le nombre de tentatives d'attaque que nous observons sur notre réseau et nous ratons des occasions importantes de signaler des données pertinentes pour sécuriser les vulnérabilités potentielles et prévenir les attaques. Un ensemble de données que nous avons ajouté à nos rapports État des lieux d'Internet cette année se démarque : il est unique car, au lieu de se concentrer sur le volume des attaques, il met en évidence une zone potentielle de vulnérabilité. Cet ensemble de données est issu des observations fournies par la solution Client-Side Protection & Compliance d'Akamai, grâce à sa vue perçante à travers des milliards de scripts de pages Web au quotidien. Le nombre de scripts internes et tiers utilisés sur les sites Web est l'un des domaines de vulnérabilité potentielle sur lesquels nous gardons un œil. Bien que l'utilisation d'un script interne ne garantisse pas la sécurité et que l'utilisation d'un script tiers n'indique pas nécessairement une vulnérabilité, plus on fait confiance à quelqu'un d'autre, par exemple en confiant à un tiers l'hébergement d'un script de page Web, plus on ajoute de risques à un profil de sécurité. Akamai s'efforce de combler l'écart entre commodité et sécurité créé par l'utilisation croissante de scripts tiers dans tous les secteurs.

Comme nous l'avons vu dans notre rapport État des lieux d'Internet Analyse des tendances des menaces : attaques dans le secteur du commerce en juin 2023, l'un des domaines d'étude d'Akamai cette année concerne les récentes attaques de web skimming de type Magecart, en particulier, l'observation de la façon dont les attaques de type Magecart continuent d'envahir le secteur du commerce digital. Ce type d'attaque vise à voler les informations d'identification sensibles des utilisateurs, telles que les informations de carte de crédit ou du panier d'achats sur un site de commerce digital en injectant un code JavaScript malveillant. Plutôt facile pour les adversaires, ce type d'attaque présente de gros risques pour les utilisateurs tout en

devenant de plus en plus difficile à détecter. Ces attaques de type Magecart, ou de web skimming, se produisent souvent sans que l'utilisateur ou le propriétaire du site Web ne s'en rende compte, et les attaquants choisissent généralement des sites Web de commerce digital qui utilisent des logiciels vulnérables ou obsolètes.

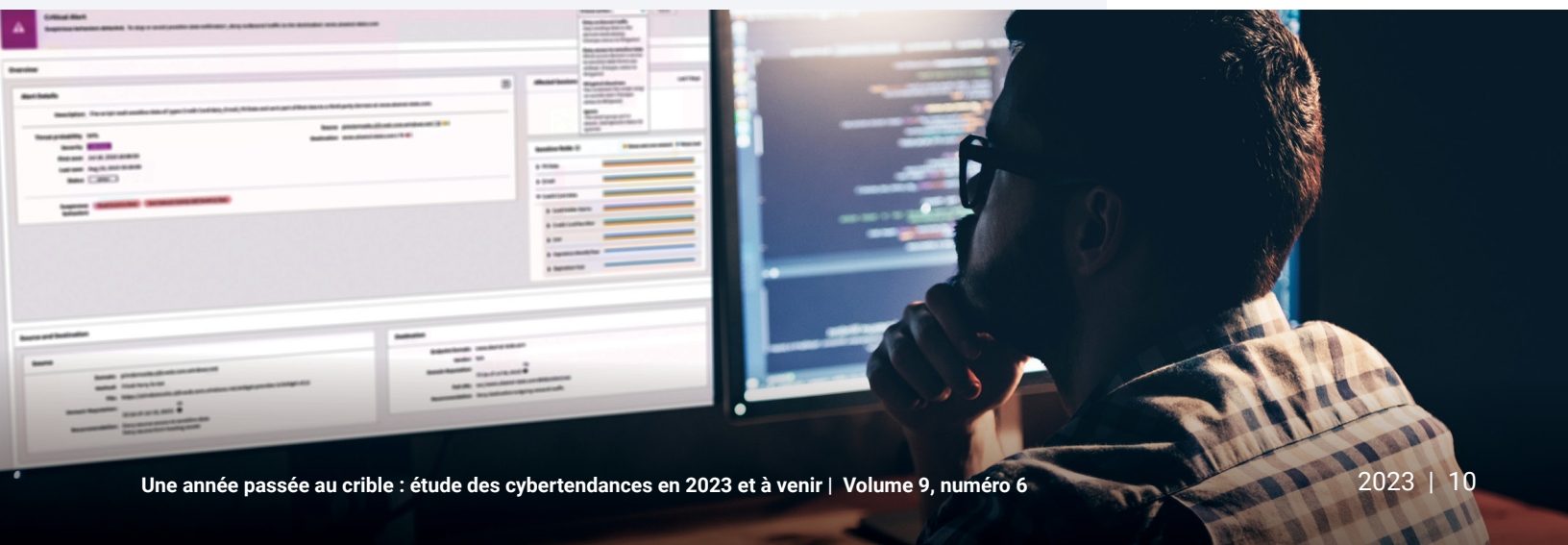
Variantes récentes de Magecart

Un certain nombre de variantes de Magecart sont visibles dans les campagnes Magecart les plus récentes que les chercheurs d'Akamai ont examinées. Notre rapport État des lieux d'Internet de juin 2023 s'est concentré sur les attaques de type Magecart côté client et a noté des vulnérabilités exploitées trouvées dans des scripts tiers provenant de bibliothèques open source pouvant conduire à des attaques de la chaîne d'approvisionnement. Peu de temps après la rédaction de ce rapport État des lieux d'Internet, nous avons publié un article de blog sur la découverte par des chercheurs d'Akamai d'une nouvelle campagne de type Magecart qui utilisait des sites Web légitimes de façon abusive pour en attaquer d'autres. Dans cette campagne, il existait essentiellement deux ensembles de sites Web victimes : les sites légitimes piratés pour l'hébergement, qui agissent comme des serveurs contrôlés par les attaquants, et les sites de commerce vulnérables subissant des attaques de web skimming côté client. Un deuxième article de blog a été publié en août. Il décrivait comment les chercheurs d'Akamai ont découvert une nouvelle campagne Magento avec une injection cachée de modèle côté serveur exploitant les sites de commerce digital pour glaner les statistiques de paiement des victimes.

Le dernier article de blog sur Magecart du SIG d'Akamai révèle une nouvelle technique de dissimulation qui permet aux attaquants de manipuler la page d'erreur 404 par défaut du site Web pour masquer le code malveillant. Les chercheurs d'Akamai ont découvert que cette nouvelle campagne se compose de deux techniques de dissimulation avancées supplémentaires, et ils présentent les tactiques de développement utilisées par les attaquants pour allonger la chaîne d'attaque et éviter la détection.

Alors que nous clôturons 2023 et que je repense à toutes les possibilités de recherche et de rapport que nous avons eues grâce aux nouvelles données et aux menaces émergentes, je ne peux m'empêcher d'attendre avec impatience les nouvelles données et les possibilités d'apprentissage qui nous attendent pour 2024.

Les chercheurs d'Akamai ont découvert une nouvelle campagne de style Magecart qui utilisait des sites Web légitimes pour en attaquer d'autres.



Tendances régionales notables en matière d'attaques

Je m'appelle Charlotte Pelliccia et j'ai rejoint l'équipe État des lieux d'Internet en 2023 pour mettre en lumière les histoires des régions Asie-Pacifique et Japon (APJ) et Europe, Moyen-Orient et Afrique (EMEA). Nos vues d'ensemble des zones APJ et EMEA viennent compléter nos rapports État des lieux d'Internet mondiaux. Je reviendrai ici sur certaines des tendances d'attaque les plus significatives que nous avons abordées en 2023, en actualisant les données des vues d'ensemble publiées en début d'année.

Attaques ciblant les applications Web et les API : l'histoire de deux segments de marché

Comme indiqué dans nos rapports État des lieux d'Internet sur les services financiers et le commerce les plus récents, les services financiers sont restés le premier segment de marché le plus touché par les attaques d'applications Web et d'API dans la région APJ, suivis du secteur du commerce. Depuis notre rapport de juin 2023, les attaques contre le secteur des services financiers sont passées de 3,7 à plus de 4,5 milliards, soit une augmentation de 22 %. Et depuis notre rapport de mars 2023, les attaques dans le secteur du commerce sont passées de 1,2 à 1,9 milliard, soit une augmentation de 58 %. La répartition entre sous-segments de marché demeure relativement cohérente (figure 2).

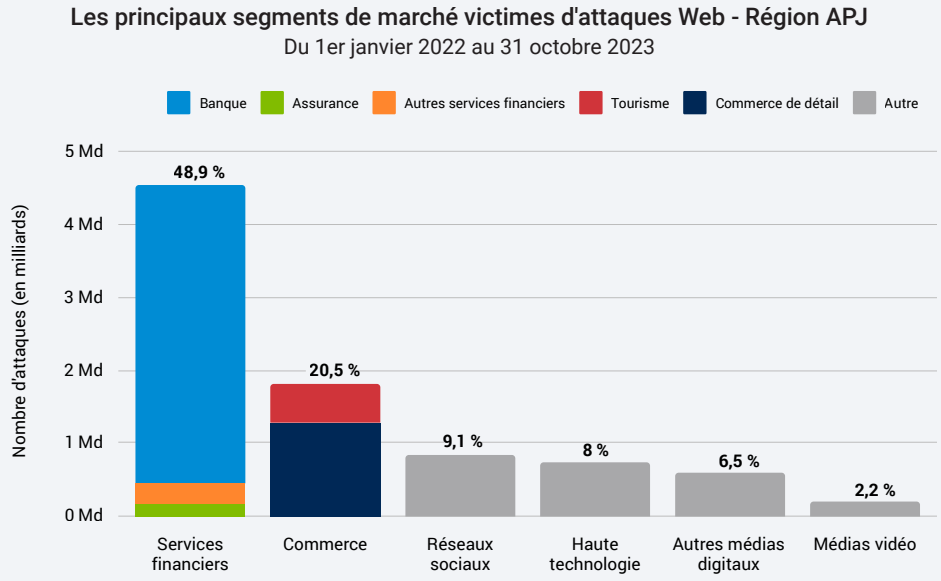


Figure 2 : Segments de marché victimes d'attaques Web dans la zone APJ jusqu'en octobre 2023

> Avoir une visibilité sur les tendances régionales en matière d'attaques est essentiel pour aider les organisations à mieux comprendre les risques auxquels elles font face et à affiner leurs outils et leurs meilleures pratiques.
>
> **– Charlotte Pelliccia, Cybersecurity Writer, Akamai**

Parallèlement, dans la zone EMEA, le commerce reste le premier segment de marché touché par les attaques d'applications Web et d'API, avec désormais plus de 6,5 milliards d'attaques (contre 4,6 milliards auparavant), soit une augmentation de 41 % depuis notre rapport de mars 2023. Bien que l'industrie manufacturière soit passée de la quatrième à la troisième position, prenant ainsi la place du secteur des services financiers, les attaques contre les services financiers ont augmenté de 70 % depuis juin 2023 pour atteindre 1,7 milliard, contre 1 milliard auparavant. Ici aussi, la répartition entre sous-segments de marché demeure relativement cohérente (Figure 3).

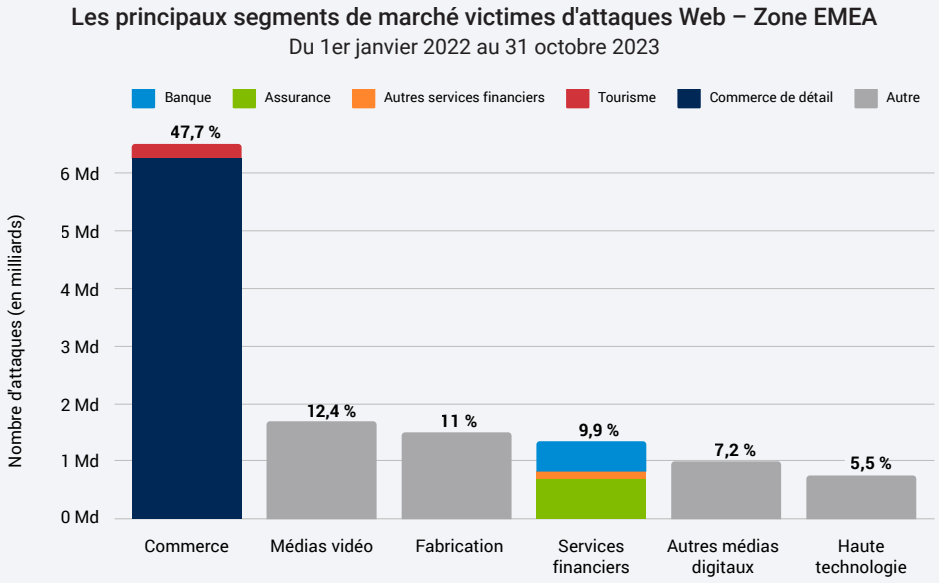
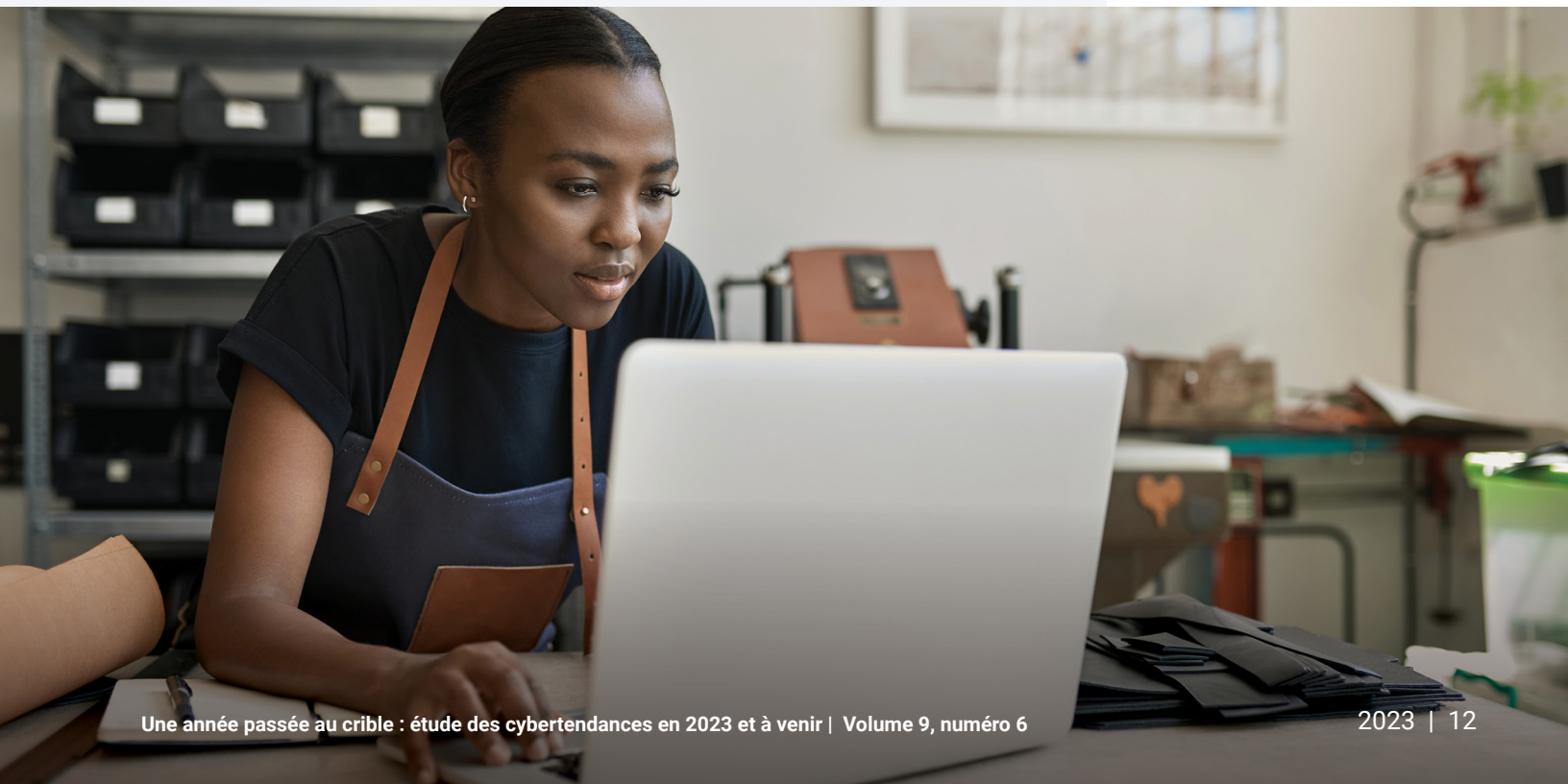


Figure 3 : Segments de marché victimes d'attaques Web dans la zone EMEA jusqu'en octobre 2023



Les bots malveillants sont une arme de choix

Dans la continuité de ce qu'indiquent les rapports précédents, la région APJ est la deuxième après l'Amérique du Nord pour ce qui est de l'activité des bots malveillants. Les trois principaux segments de marché victimes d'attaques de janvier 2022 à octobre 2023 dans la région APJ sont le commerce (27,4 %), les médias vidéo (15 %) et les services financiers (14,3 %). Dans la zone EMEA, la moitié (50,1 %) des activités des bots malveillants ciblaient le commerce, suivi par les autres médias digitaux (15,3 %) et les médias vidéo (12,2 %) (Figure 4).

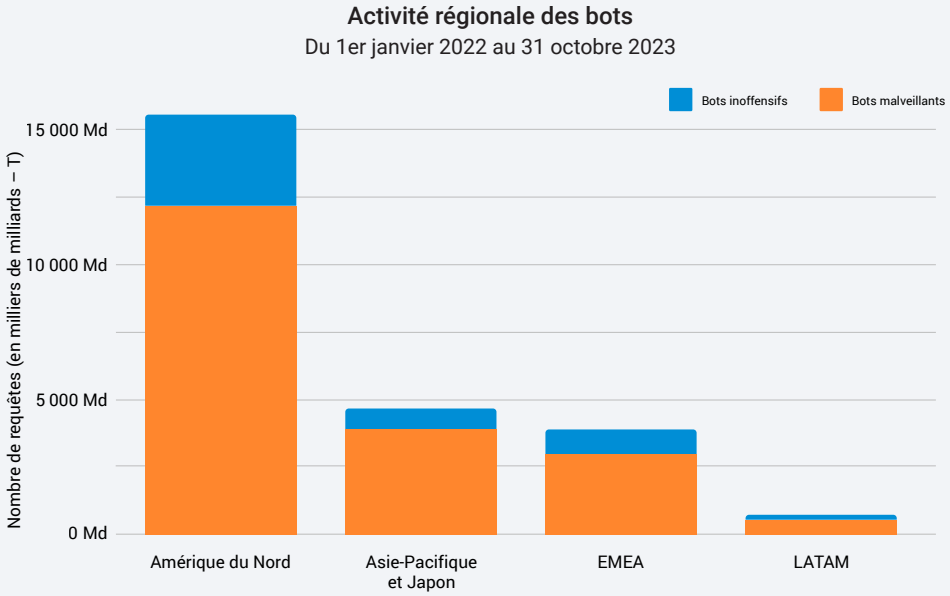


Figure 4 : L'utilisation de bots malveillants est répandue dans toutes les régions, et dépasse de loin l'utilisation de bots inoffensifs

> Consultez l'étude suivante pour obtenir des informations de notre SOCC sur l'évolution des attaques de bots et DDoS.

La zone EMEA dans la ligne de mire du changement régional impliquant les attaques DDoS

Notre rapport de 2023 a clairement montré que les acteurs malveillants ont jeté leur dévolu sur la zone EMEA, ce qui peut être attribué en partie au climat géopolitique actuel. Un exemple parfait : le nombre d'attaques par déni de service distribué (DDoS) contre les secteurs des services financiers, des jeux d'argent et l'industrie manufacturière dans la région EMEA dépasse les chiffres enregistrés dans toutes les autres régions réunies (figure 5).

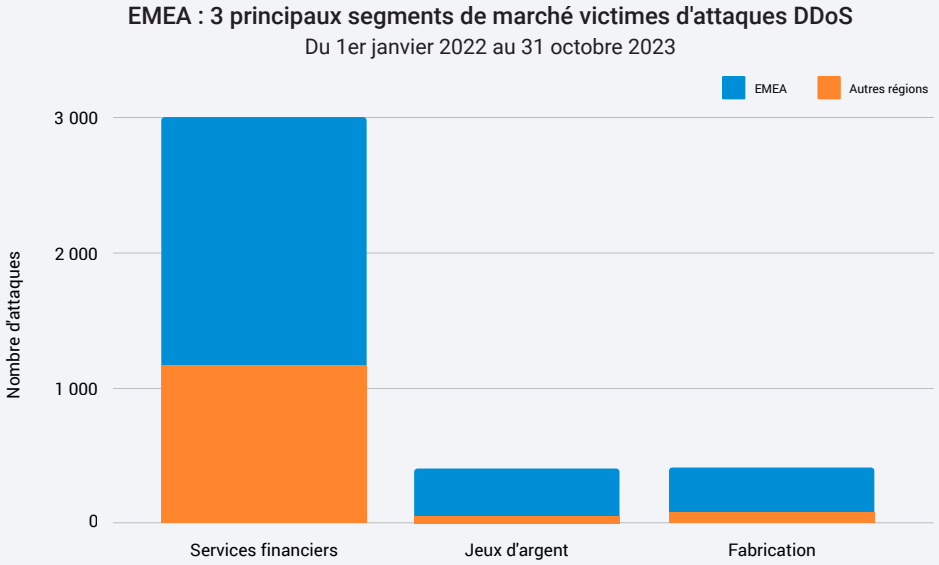


Figure 5 : La zone EMEA a connu plus d'attaques DDoS dans ces segments de marché que toutes les autres régions réunies

Regard vers l'avenir

Tant que les acteurs malveillants parviennent à leurs fins avec les attaques Web, de bots et DDoS, il est raisonnable de s'attendre à ce que celles-ci restent leurs armes de choix. En fait, ces trois vecteurs évoluent déjà pour se maintenir ou se renforcer. Les exploitations Zero Day des applications Web sont étroitement liées aux techniques de ransomwares (par des groupes de ransomwares tels que CL0P) et incluent des attaques DDoS pour créer une tactique de triple extorsion. La revente sur le Web via des bots est désormais un classique pour presque tous les événements importants et les ventes de billets de compagnies aériennes. Et les attaques API dirigées contre la logique métier de l'API font leur apparition.

En réponse à cela, le contrôle réglementaire et les exigences en matière de création de rapports continuent de croître dans le monde entier et dans tous les secteurs, car aucune région ni secteur n'est à l'abri des attaques. L'objectif est d'adapter la législation sur la cybersécurité à l'évolution de l'écosystème des menaces. Les entreprises doivent rester vigilantes quant au respect des exigences en matière de création de rapports et être prêtes à atténuer les risques grâce à une défense multicouche.

Grandes perspectives sur le monde depuis notre fenêtre : informations des Centres de commande des opérations de sécurité

Je suis Roger Barranco, Vice President of Global Security Operations. Je travaille chez Akamai depuis près d'une douzaine d'années et je suis responsable des opérations de sécurité entièrement gérées de l'entreprise, qui sont prises en charge par six SOCC positionnés dans le monde entier et gérés par une équipe fantastique. J'ai commencé ma carrière dans la cybersécurité et j'ai été attiré par ce domaine parce qu'il s'agit d'un marché intéressant et en constante évolution : 2023 en est un excellent exemple.

Le SOCC d'Akamai n'a jamais été autant sollicité : d'ici la fin de 2023, nous aurons traité environ 30 % de tickets de plus que l'année dernière liés à la sécurité. Voici les informations essentielles que nous avons recueillies en travaillant avec nos clients des services de sécurité gérés et que les organisations devraient retenir pour 2024.

Les attaques DDoS évoluent

Bien que le nombre de clients subissant des attaques augmente toujours d'année en année, la « façon de procéder » est aujourd'hui différente. Premièrement, le type et le volume des propriétés des clients attaquées ont changé. Par exemple, au lieu de 10 attaques contre des terminaux identiques ou similaires, nous en observons maintenant 100 qui visent toutes des adresses IP différentes dans l'espace réseau du client. Et ces attaques ne ciblent pas uniquement la couche 3, mais également la couche 7. En outre, le nombre d'attaques contre les DNS a augmenté de façon spectaculaire et il s'agit la plupart du temps d'attaques de requêtes valides qui peuvent facilement lasser l'infrastructure DNS du client. Quelques mégabits de trafic DNS indésirable peuvent à eux seuls causer des contraintes importantes sur une entreprise. Nous commençons également à voir un regain inquiétant de l'activité sur le front Mirai, qui s'est fait connaître en exploitant la puissance de l'Internet des objets pour provoquer des perturbations à grande échelle.

Dans l'écosystème actuel des menaces, il ne suffit pas de mettre des équipements robustes en bordure de l'Internet pour faire face aux attaques. Les entreprises ont besoin de services de sécurité robustes au niveau du cloud pour assumer cette charge de travail, en conservant l'état des points de terminaison tout en mettant en œuvre des protections uniques pour chacun d'entre eux. C'est là que réside la force d'Akamai, tant du point de vue de la plateforme que des services. Nous pouvons appliquer plusieurs couches de sécurité pour nous défendre contre l'ensemble du spectre des cyberattaques. Et nos experts de terrain examinent les nuances et les tendances pour chaque client afin de les surveiller et d'atténuer les attaques d'une manière très spécifique qui les bloque, tout en permettant au trafic attendu et propre de passer.

> “Le SOCC d'Akamai n'a jamais été autant sollicité : d'ici la fin de 2023, nous aurons traité environ 30 % de tickets de plus que l'année dernière liés à la sécurité.
>
> – **Roger Barranco, Vice President of Global Security Operations, Akamai**

Le combat contre les bots peut être difficile

Le vol d'identifiants est difficile à limiter, car il n'est pas facile de distinguer le trafic indésirable du trafic utile, et les clients ont des back-ends assez uniques qui peuvent nécessiter des protections distinctes. De plus, les attaquants qui tentent de voler des identifiants sont parmi les plus compétents et les plus vigilants, car un vol d'identifiant qui aboutit est le moyen le plus facile de faire du profit. La nature dangereuse et coûteuse de ces attaques de bots fait qu'il est important de disposer d'une solution de prévention contre le vol d'identifiants, en particulier dans les secteurs des services financiers et du commerce où l'utilisation de bots malveillants continue d'augmenter.

La région EMEA reste dans la ligne de mire des attaquants

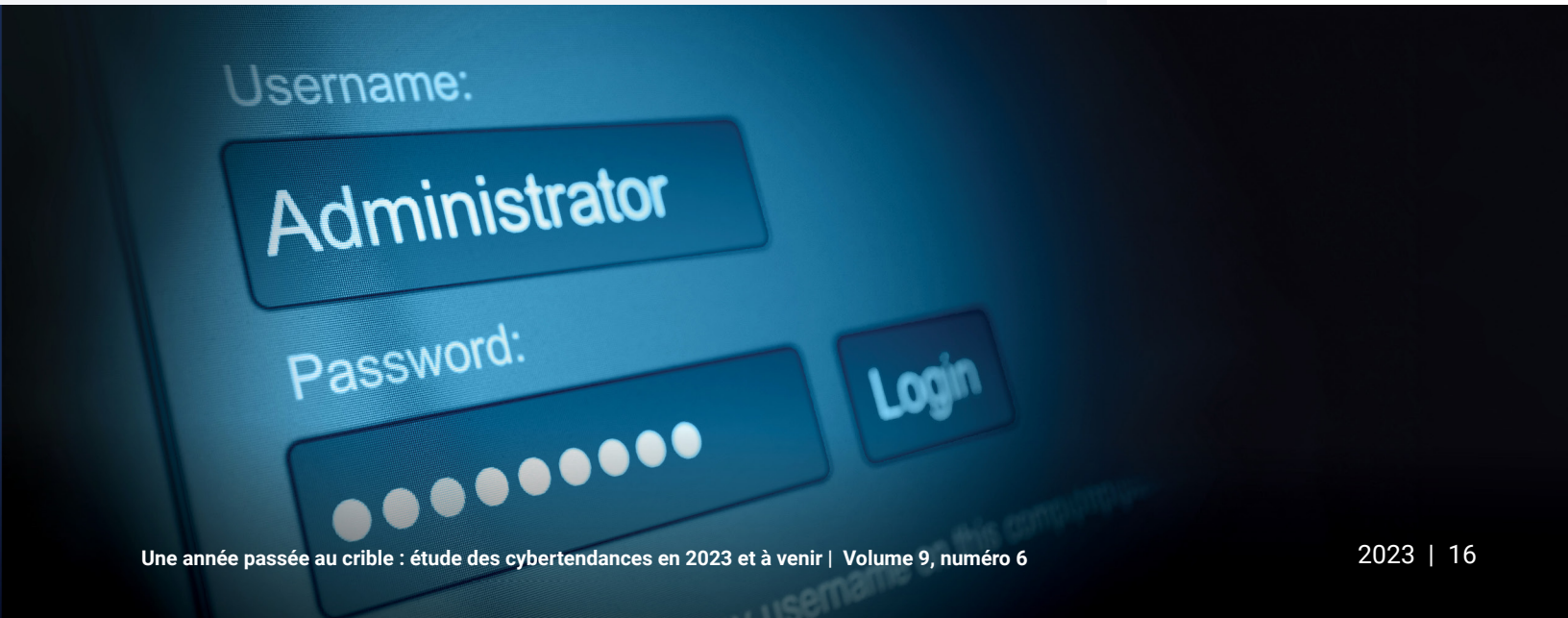
Depuis l'incursion en Ukraine, la région EMEA (l'Europe, en particulier) a supplanté les États-Unis en tant que première région touchée par les cyberattaques dans un certain nombre segments de marché et de catégories d'attaques, notamment les attaques DDoS. Cette évolution met en évidence le fait que de nombreux agresseurs sont des États-nations ou des sympathisants d'États-nations et que l'attention qu'ils portent sur l'Europe ne diminue pas.

La sophistication des attaquants s'accroît

L'époque où les « script kiddies » (pirates amateurs) représentaient la principale menace est révolue. Ils se servaient des outils génériques pour lancer une attaque en espérant avoir de la chance, ou louaient un botnet DDoS pour 10 dollars de l'heure afin d'éliminer un concurrent de jeux vidéo. Aujourd'hui, les attaquants sont plus sophistiqués et semblent se concentrer en détail sur des cibles spécifiques, planifiant leur stratégie, effectuant des reconnaissances parfois un an à l'avance et élaborant des attaques pour tirer parti des faiblesses éventuelles perçues. Conséquence du travail préparatoire réalisé par les agresseurs, les attaques d'aujourd'hui sont plus longues que les années passées, où elles ne duraient souvent que quelques minutes.

Conséquence du travail préparatoire réalisé par les agresseurs, les attaques d'aujourd'hui sont plus longues que les années passées, où elles ne duraient souvent que quelques minutes.

– Roger Barranco,
Vice President of
Global Security Operations,
Akamai



Meilleures pratiques pour l'alignement cybernétique et opérationnel

Malgré ces défis, les clients peuvent accroître l'efficacité de leurs efforts de protection en mettant en œuvre deux meilleures pratiques d'alignement cybernétique et opérationnel qui permettent à Akamai de travailler dans le prolongement de leur équipe informatique. Tout d'abord, ils peuvent collaborer avec le SOCC en temps de paix pour développer de manière proactive leur posture défensive au lieu d'essayer de le faire pendant une attaque. De cette façon, il est possible d'atténuer les attaques en amont sans conséquences sur la production et les clients reçoivent un rapport de suivi détaillant l'attaque évitée.

Deuxièmement, ils peuvent travailler de manière proactive sur la préparation opérationnelle et les plans de sauvegarde. Par exemple, lors de tests, ils peuvent s'assurer qu'ils savent comment accéder à différentes plateformes et en sortir. Une attaque de cinq minutes peut avoir des conséquences sur un client pendant une heure en raison de problèmes opérationnels. Il est donc tout aussi important d'être préparé sur le plan opérationnel que d'être prêt à répondre à un problème purement cybernétique.

Cette année a mis en évidence l'évolution constante de la cybersécurité, et nous nous attendons à ce que cette évolution se poursuive. La bonne nouvelle est qu'en mettant en pratique ces idées, les clients peuvent prendre une longueur d'avance et se protéger en 2024.

Moments forts, et plus encore, de notre Advisory CISO

Je m'appelle Steve Winterfeld et je suis l'Advisory CISO d'Akamai. Auparavant, j'ai été responsable de la sécurité des systèmes d'information pour la banque Nordstrom et directeur de la réponse aux incidents et du renseignement sur les menaces chez Charles Schwab. Mon rôle est de m'assurer que nos partenaires parviennent à défendre leurs clients et de déterminer où nous devons concentrer nos moyens.

Cette année, nous avons observé quelques tendances qui m'ont surpris et d'autres qui ont été confirmées par des données pouvant être utilisées pour mettre à jour notre stratégie. Mes neuf histoires les plus marquantes de cette année incluent des moments forts, quelques nouvelles attendues et des choses qui semblent ne jamais changer.

Moments forts

- Au total, 10 % à 16 % des entreprises ont accédé aux domaines de commandement et de contrôle (C2) au moins une fois par trimestre. En outre, 26 % des terminaux infectés ont atteint des domaines liés à des courtiers d'accès initial.
- L'écosystème des menaces liées aux ransomwares a connu une évolution préoccupante des techniques d'attaque, avec une multitude d'abus concernant les vulnérabilités Zero Day et One Day au cours des six derniers mois.
- Une étude d'Akamai a révélé que les victimes de plusieurs groupes de ransomwares sont presque six fois plus susceptibles de subir une nouvelle attaque dans les trois mois suivant l'attaque initiale.

Nouvelles attendues

- Les attaques API dirigées contre la logique métier de l'API sont compliquées à détecter et à prévenir. Par conséquent, elles sont difficiles à déterminer au niveau de chaque requête.
- Les entreprises doivent veiller à respecter les nouvelles exigences de la norme de sécurité de l'industrie des cartes de paiement (PCI DSS) v4.0 et le règlement sur la résilience opérationnelle digitale du secteur financier (DORA).

> Ces informations sont d'excellents guides pour vous aider à établir votre programme de sécurité et à identifier les outils redondants ou les lacunes.
>
> **– Steve Winterfeld, Advisory CISO, Akamai**

Des choses qui ne semblent jamais changer

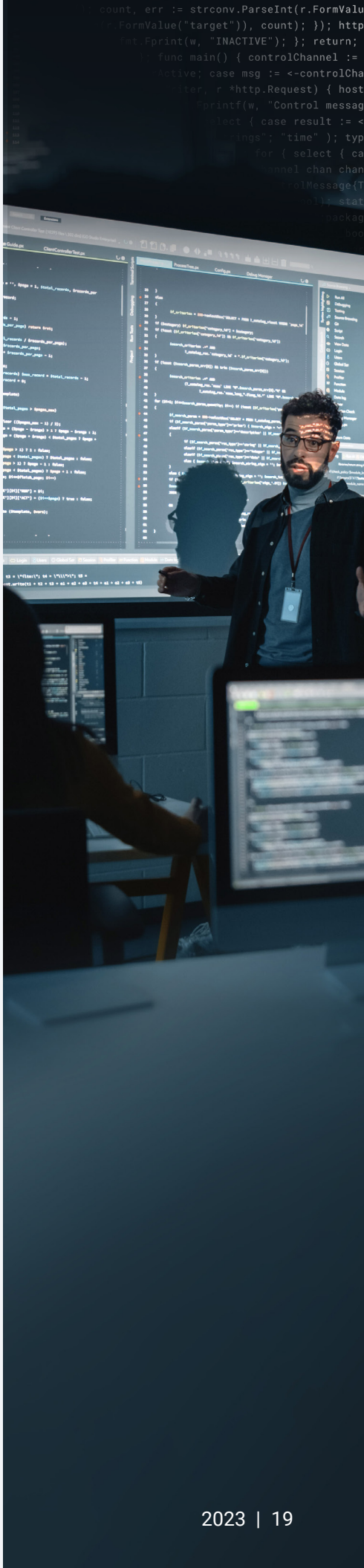
- Le nombre d'attaques de bots et d'API continue d'augmenter, et celui d'attaques DDoS atteint de nouveaux records.
- Les secteurs les plus attaqués sont généralement les services financiers, la haute technologie et le commerce.
- L'inclusion de fichiers locaux (LFI) est la technique d'attaque la plus efficace.
- L'Amérique du Nord cède la place à l'Europe en tant que région la plus touchée par les attaques DDoS.

Une découverte essentielle qui m'a fait réfléchir est celle des indicateurs validés de compromission depuis la communication C2. Ce qui est particulièrement troublant, c'est la fréquence élevée des premières détections qui se produisent après que les logiciels malveillants ont déjà réussi à pénétrer dans les systèmes et à établir la communication. Cela met en évidence l'équilibre critique nécessaire entre les mesures préventives et la détection rapide pour atténuer l'impact.

Ce qui m'a le plus surpris, c'est l'évolution entre les attaques par ingénierie sociale et les attaques Zero Day. Ces dernières années, j'ai eu l'impression que nos défenses techniques se renforçaient et j'ai eu besoin de renforcer le personnel grâce aux formations et au suivi. Mais avec le passage aux attaques Zero Day cette année, je dois examiner de près où je déploierai mes ressources l'année prochaine.

Les attaques qui semblent les plus injustes sont celles qui vous frappent alors que votre entreprise est déjà confrontée à une attaque de ransomware ou se remet d'une telle attaque. Il est facile d'être ultra concentré sur la crise et de tirer des ressources de la surveillance défensive continue. Cette étude nous a rappelé avec force que nous ne pouvons PAS nous permettre de baisser la garde !

Ces informations sont d'excellents guides pour vous aider à établir votre programme de sécurité et à identifier les outils redondants ou les lacunes. Elles permettent de mettre en place des exercices visant à mettre à jour les manuels/processus, à orienter la formation, à améliorer les plans de tests de pénétration ou à prendre en charge l'examen du portefeuille de risques. La cybersécurité est un sport d'équipe. Ces informations sont donc également utiles pour stimuler les discussions avec les partenaires internes (tels que vos équipes juridiques ou informatiques) et les fournisseurs. Comme toujours, des références/outils comme le National Institute of Standards and Technology (NIST), la base de connaissances ATT&CK de MITRE et les 10 menaces les plus dangereuses selon l'OWASP sont d'excellentes ressources.



Perspectives d'avenir

Il est impossible de prédire l'avenir, mais on peut s'attendre à ce que les attaques DDoS et API dominent 2024. Les efforts continus pour développer de plus grandes armées de botnets et de nouvelles techniques, combinés à l'influence des États-nations, vont entraîner l'augmentation des attaques DDoS. Ce facteur, associé à l'évolution des ransomwares, sera à l'origine de la législation et de la résilience.

La transformation continue d'être le moteur de la mise en œuvre des API dans la plupart des secteurs. Ce développement rapide entraînera malencontreusement une augmentation des surfaces d'attaque et davantage de vulnérabilités, des API fantômes, des API zombies et des abus d'API. Nous prévoyons une croissance significative des attaques contre les applications Web et les API. Il s'agira à la fois d'attaques standard comme les attaques LFI, et de techniques émergentes comme la falsification de requête côté serveur (SSRF) et l'injection de modèle côté serveur (SSTI), qui nécessiteront des outils capables de détecter les mouvements latéraux et d'en atténuer les impacts.

Enfin, à l'exception de certaines tendances propres aux secteurs et aux régions, nous prévoyons une pénurie globale de professionnels qualifiés en cybersécurité. L'apprentissage automatique et l'intelligence artificielle à base de grands modèles linguistiques apporteront un certain soulagement, mais dans l'ensemble, il sera extrêmement difficile de trouver et de retenir les talents dont nous avons besoin. Cela mènera à des partenariats avec des fournisseurs pour la dotation en personnel à la demande ou des services gérés pour des fonctions non essentielles.

En ce qui concerne le SIG d'Akamai, nous continuerons à tirer la sonnette d'alarme en cas de menaces courantes et de risques de sécurité émergents. Nous nous engagerons auprès de la communauté de la sécurité par le biais de nos plateformes et de nos canaux afin de renforcer les efforts en matière de renseignement sur les menaces. Et en 2024, nous célébrerons le 10e anniversaire de nos rapports État des lieux d'Internet ! Nous sommes ravis de continuer à améliorer nos rapports en introduisant de nouveaux ensembles de données, des aides visuelles et des informations clés qui peuvent aider les professionnels de la sécurité dans leur quête de protection de leurs organisations.

Nous sommes impatients de partager d'autres résultats d'études l'année prochaine. En attendant, restez protégés !

Crédits

Édition et rédaction

Roger Barranco
Tricia Howard
Charlotte Pelliccia
Lance Rhodes
Badette Tribbey
Chelsea Tuttle
Steve Winterfeld

Révision et expertise

Kimberly Gomez
Reuben Koh
Emily Lyons
Richard Meeus
Carley Thornell

Analyse des données

Chelsea Tuttle

Marketing et publication

Georgina Morales Hampe
Emily Spinks

Autres rapports État des lieux d'Internet/Sécurité

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

D'autres recherches sur les menaces d'Akamai

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

Accéder aux données de ce rapport

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

En savoir plus sur les solutions Akamai

Pour en savoir plus sur les solutions Akamai de lutte contre les menaces, consultez notre page **Solutions de sécurité**.