SOTI

10 YEARS
OF SECURITY INSIGHT

VOLUME 10
NUMÉRO 05

Faire face à l'afflux de menaces

Tendances des attaques ciblant les services financiers

Akamai

État des lieux d'Internet/Sécurité

Table des matières

Introduction

Pierre angulaire de l'économie mondiale, le secteur des services financiers est un acteur essentiel de la croissance et du développement économiques. En constante évolution, il englobe un large éventail de secteurs d'activité, dont les banques commerciales, les prestataires de services de paiements, les sociétés de gestion d'actifs, les banques d'investissement et les organismes d'assurance.

Les avancées technologiques continuent de remodeler le paysage des services financiers, donnant lieu à des innovations en matière de technologie financière (fintech) telles que les banques numériques, les robots conseillers et les actifs cryptographiques. Le nombre d'entreprises de fintech a bondi dans le monde entier, avec les États-Unis et la Chine en tête. En janvier 2024, 8 des 10 plus grandes entreprises de fintech étaient basées dans ces deux pays. Cette évolution technologique se reflète également dans la hausse du nombre de transactions hors espèces, qui devrait augmenter considérablement, en particulier dans les endroits où l'accès financier est limité. Mais l'innovation s'accompagne d'une certaine vulnérabilité.

Les cybercriminels ciblent sans relâche les institutions financières et l'impact de leurs attaques va bien au-delà des pertes financières. Des perturbations opérationnelles, des atteintes à la réputation et des sanctions réglementaires paralysantes peuvent éroder le socle de confiance sur lequel repose le secteur des services financiers. Comment les institutions financières peuvent-elles mettre en place des défenses efficaces à une époque où la vitesse de la transformation digitale n'a d'égale que la sophistication des cybermenaces ?

Ce rapport sur l'état des lieux d'Internet est spécialement conçu pour aider les professionnels des services financiers du monde entier, clients d'Akamai, chercheurs en cybersécurité et leaders du secteur, à naviguer dans le paysage de plus en plus complexe des menaces. Cible privilégiée des cybercriminels, le secteur des services financiers nécessite un effort de collaboration pour sauvegarder son infrastructure critique, protéger les entreprises et les clients, assurer la stabilité des marchés financiers et prévenir les perturbations économiques. L'étude présentée ici est une lecture indispensable pour ceux qui veulent garder une longueur d'avance sur les pirates, fortifier les actifs critiques du secteur et assurer la confiance et la fiabilité continues qui sous-tendent les relations financières mondiales.

Renforcer les services financiers grâce à la conformité, la résilience opérationnelle et la cybersécurité

L'un des principaux défis auxquels le secteur financier mondial est confronté aujourd'hui est l'impératif d'améliorer la conformité et la résilience opérationnelle. Alors que l'environnement réglementaire évolue, les institutions financières doivent s'adapter de manière proactive pour répondre aux nouvelles exigences. L'introduction du Règlement européen sur la résilience opérationnelle numérique (DORA), par exemple, souligne la nécessité d'un cadre solide capable de résister aux perturbations liées aux technologies de l'information et de la communication (TIC). Le règlement DORA, qui doit entrer en vigueur en janvier 2025, impose des stratégies de résilience complètes aux entités financières et à leurs fournisseurs de TIC, ce qui oblige les entreprises à renforcer leurs capacités de sécurité et de réponse aux incidents.

La mise à jour des directives de l'U.S. Securities and Exchange Commission renforce encore la nécessité d'une approche globale de la cybersécurité. Les institutions financières sont désormais tenues d'intégrer la résilience opérationnelle et la reprise après sinistre dans leurs stratégies, en mettant l'accent sur l'importance des cyberrisques. Cela implique une compréhension approfondie de la manière dont les menaces et les incidents importants peuvent impacter la stabilité financière et les opérations. L'obligation de divulguer rapidement les incidents importants liés à la cybersécurité et d'exposer en détail les stratégies de gestion des risques dans les rapports annuels marque un changement de paradigme dans les attentes réglementaires. Pour progresser dans ces différents environnements réglementaires, les institutions financières doivent s'associer à des entités qui offrent des solutions de sécurité de pointe et une grande visibilité. Comme le montre la présente étude, l'expertise d'Akamai peut aider les entreprises de services financiers non seulement à répondre aux normes de conformité, mais aussi à maintenir leur intégrité opérationnelle dans un cadre d'exigences réglementaires strictes.

Compte tenu de ces évolutions, les institutions financières doivent adopter une approche globale pour gérer la conformité et la résilience opérationnelle dans toute leur complexité. Cela implique d'identifier et de hiérarchiser les risques importants, susceptibles d'avoir un impact significatif sur le processus de décision d'un investisseur. Les institutions financières doivent intégrer ces risques importants dans leur cadre de gestion des risques et veiller à ce que des plans de réponse aux incidents solides soient en place. Le chemin vers une résilience opérationnelle efficace passe par l'adoption d'une stratégie de défense en profondeur multicouche. Il s'agit notamment de réduire la surface d'attaque par la segmentation et la microsegmentation du réseau, de mettre en œuvre le chiffrement des données au repos, de renforcer les serveurs et d'utiliser des pare-feu d'application Web couplés à des systèmes de détection des menaces avancés. Une surveillance continue et des évaluations régulières de la sécurité sont essentielles pour identifier et atténuer rapidement les risques.

Les institutions financières doivent impérativement mener des exercices de planification de la réponse aux incidents, basés sur les informations et recherches actuelles sur les menaces, telles que les rapports SOTI (État des lieux d'Internet) d'Akamai. Ces exercices leur permettent d'élaborer des scénarios plausibles et de s'assurer d'être en mesure de s'adapter aux nouveaux outils, techniques et procédures au fur et à mesure de leur apparition. Cette attitude proactive est indispensable pour assurer la résilience opérationnelle et maintenir la confiance des clients dans un écosystème des menaces de plus en plus volatile. À mesure que le secteur des services financiers évolue, l'intersection entre la conformité, la résilience opérationnelle et la cybersécurité continuera à façonner son avenir. En adoptant des mesures de sécurité avancées et en améliorant la visibilité, les institutions financières peuvent maîtriser les complexités réglementaires et protéger leurs opérations afin de préserver la confiance, qui est vitale pour leurs activités.

Teresa Walsh
Responsable mondiale du renseignement, FS-ISAC

Informations stratégiques

34 %

Pourcentage d'attaques DDoS des couches 3 et 4 subies par les institutions de services financiers

Les services financiers restent le secteur le plus touché par les attaques par déni de service distribué (DDoS) sur les couches 3 et 4. Viennent ensuite le secteur des jeux vidéo avec 18 % et celui de la haute technologie avec 15 %. Cette menace croissante est probablement due aux tensions géopolitiques actuelles, en particulier les guerres entre Israël et le Hamas et entre la Russie et l'Ukraine, qui ont entraîné une forte hausse de l'activité des hacktivistes dans le monde entier.

La croissance des API entraîne une augmentation des attaques DDoS de la couche 7

Bien que les applications Web soient traditionnellement les cibles privilégiées des cyberattaques, les attaques DDoS de couche 7 contre les API ont atteint des sommets notables au cours de la période considérée. Cela s'explique en grande partie par l'adoption grandissante des API dans les services financiers pour répondre à l'évolution des exigences réglementaires et de conformité. Alors que les organisations s'appuient de plus en plus sur les API, leurs adversaires adaptent leurs tactiques, et la sécurité des API devient une priorité absolue pour les entreprises d'aujourd'hui.

Les pics de trafic soulignent la nécessité d'évaluer les attaques DDoS en fonction de leur fréquence et de leur volume

Les attaques DDoS dans les services financiers révèlent un aspect critique : la fréquence des événements n'est pas toujours corrélée avec l'intensité de l'attaque. En effet, bien que le nombre d'attaques est plus faible au cours de certains mois, leurs données en Gbit/s indiquent des pics de trafic importants, ce qui souligne la nécessité de prendre en compte à la fois la fréquence et le volume des attaques lors de l'évaluation des impacts des attaques DDoS.

36 %

Pourcentage de domaines suspects ciblant les institutions financières

Les attaques par hameçonnage ciblent de plus en plus les clients des services financiers, augmentant les risques d'usurpation d'identité et de piratage de comptes. Cette tendance expose les institutions financières à une surveillance accrue de la part des régulateurs, et les violations érodent la confiance des clients.

30 %

Pourcentage de visites de pages dirigées vers des sites d'hameçonnage et d'usurpation d'identité de marque

Les pirates réussissent à diriger du trafic vers des sites frauduleux en imitant des sites Web et des applications de services financiers légitimes. Ils continuent de perpétrer des attaques par hameçonnage contre les institutions financières afin de s'emparer des précieuses informations sensibles qu'elles détiennent.

Les services financiers cible principale des attaques DDoS sur les couches 3 et 4

Les attaques DDoS des couches 3 et 4 ciblent les couches réseau et de transport, submergeant l'infrastructure réseau et épuisant ainsi les ressources serveur et la bande passante. Ces attaques envoient un énorme volume de trafic dans le but de saturer le réseau et de dégrader les performances pour les utilisateurs légitimes. Parmi tous les secteurs d'activité, celui des services financiers est la principale cible des attaques DDoS de couches 3 et 4 (figure 1). Cette tendance s'explique par plusieurs facteurs interconnectés ayant engendré une vulnérabilité accrue et de nouvelles opportunités pour les pirates.

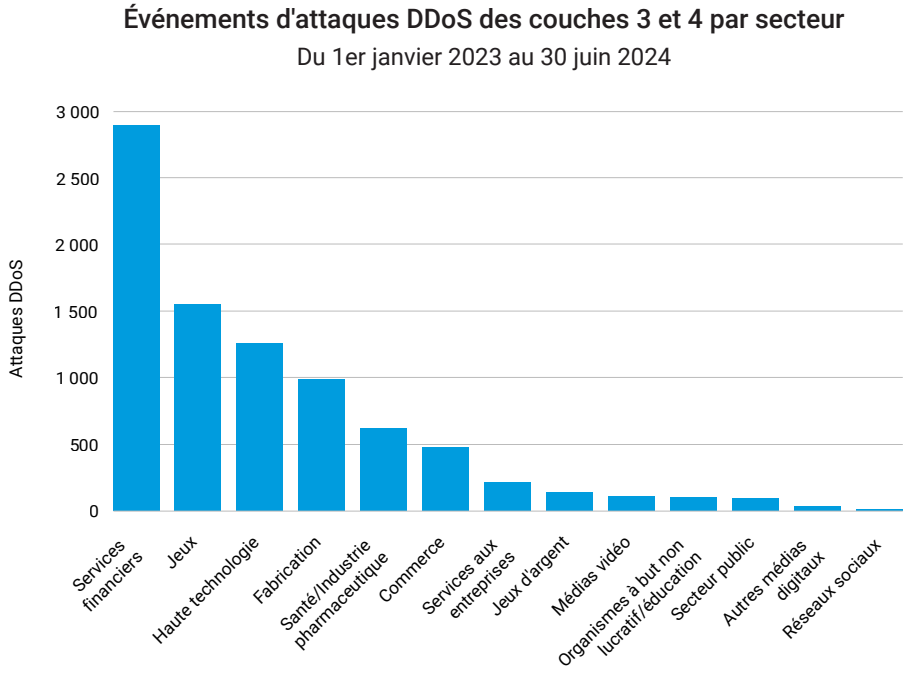


Figure 1 : le nombre d'attaques DDoS des couches 3 et 4 est nettement plus élevé dans les services financiers que dans les autres secteurs

Les tensions géopolitiques ont joué un rôle important dans l'augmentation des attaques DDoS contre les institutions financières. La guerre actuelle entre la Russie et l'Ukraine et la guerre entre Israël et le Hamas coïncident avec une augmentation notable de l'hacktivisme prorusse et propalestinien. Ces conflits ont entraîné une flambée des attaques DDoS, en particulier contre les banques européennes ayant des liens avec l'Ukraine. La nature politique de ces attaques ajoute une couche supplémentaire de complexité à l'écosystème des menaces.

Les institutions financières sont des cibles particulièrement attrayantes pour les auteurs d'attaques DDoS en raison des enjeux élevés qu'elles représentent. Une perturbation réussie des opérations peut avoir de graves conséquences financières, nuire considérablement à la réputation et entraîner une perte de confiance dans le système financier mondial. Le potentiel de conséquences à grande échelle fait des services financiers une cible de choix pour ceux qui cherchent à causer un maximum de perturbations ou à diffuser un message politique.

Les avancées technologiques ont considérablement augmenté le pouvoir et les capacités des auteurs d'attaques DDoS, qui peuvent désormais déployer des botnets de machines virtuelles (VM) pour renforcer l'efficacité de leurs attaques en utilisant les ressources informatiques d'un grand nombre de machines virtuelles et de terminaux de l'Internet des objets (IoT). Cette approche exploite la nature distribuée des services cloud pour rendre les attaques plus difficiles à atténuer et à tracer. Les attaquants peuvent tirer parti de la disponibilité d'une large bande passante et de vastes ressources informatiques, ce qui leur permet de lancer des attaques DDoS adaptables, puissantes et rentables à travers diverses stratégies.

L'élargissement de la surface d'attaque dans le secteur des services financiers a également contribué à la hausse des attaques DDoS. L'utilisation croissante de services digitaux et d'API a ouvert davantage de points d'entrée aux pirates. Cette évolution a rendu les systèmes financiers plus complexes et a introduit de nombreuses vulnérabilités potentielles que les pirates peuvent exploiter. Les API fantômes non documentées sont particulièrement préoccupantes, car les équipes chargées de la sécurité de l'information ignorent leur existence et elles sont donc rarement protégées. Les attaquants peuvent exploiter ces API pour exfiltrer des données, contourner les contrôles d'authentification ou créer des perturbations.

Les pressions réglementaires ont involontairement accru la vulnérabilité des institutions financières aux attaques DDoS. De nouvelles règles, notamment la directive révisée sur les services de paiement (DSP2) introduite par l'Union européenne, exigent que les banques ouvrent leurs systèmes à leurs fournisseurs tiers (par ex., sociétés de fintech) par le biais d'API. Si cela permet aux banques de répondre aux attentes croissantes des clients grâce à l'intégration avec la fintech, les applications pour mobile et d'autres plateformes, cela augmente également les risques de sécurité et élargit la surface d'attaque. L'utilisation supplémentaire d'API par ces diverses entités crée davantage de points de défaillance potentiels que les pirates peuvent cibler.

L'ensemble de ces facteurs a contribué à faire du secteur des services financiers la cible privilégiée des attaques DDoS des couches 3 et 4. La combinaison de motivations géopolitiques, de cibles de grande valeur, de progrès technologiques, d'une empreinte digitale croissante et de pressions réglementaires a créé un environnement dans lequel les attaques DDoS contre les institutions financières sont non seulement plus fréquentes, mais aussi potentiellement plus dommageables que jamais. Afin de s'adapter à l'évolution constante du secteur et de lutter efficacement contre des menaces persistantes de plus en plus sophistiquées, les moyens de défense doivent aussi évoluer.

Les attaquants peuvent tirer parti de la disponibilité d'une large bande passante et de vastes ressources informatiques, ce qui leur permet de lancer des attaques DDoS adaptables, puissantes et rentables à travers diverses stratégies.

Événements d'attaque DDoS des couches 3 et 4 : des montagnes russes

Bien que le secteur des services financiers soit le plus touché par les attaques DDoS des couches 3 et 4, la fréquence de ces attaques fluctue au cours de l'année (figure 2).

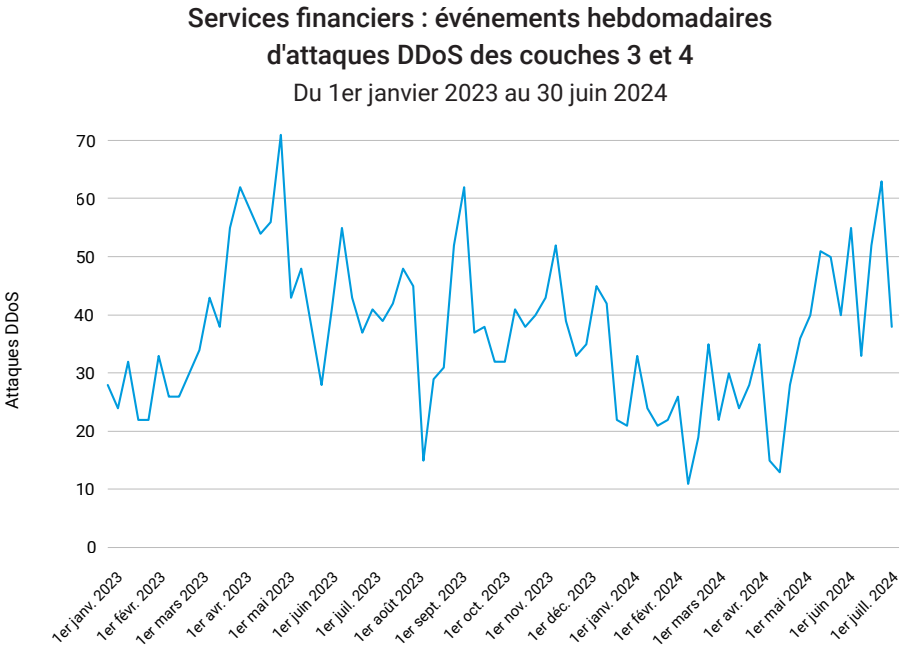


Figure 2 : les attaques DDoS des couches 3 et 4 dans le secteur des services financiers évoluent en dents de scie

Les attaques DDoS des couches 3 et 4 contre le secteur des services financiers en mars/avril 2023, août/septembre 2023 et avril/mai 2024 peuvent être attribuées à plusieurs facteurs spécifiques.

Le printemps, de mars à avril, marque la saison active de l'impôt sur le revenu aux États-Unis, ce qui constitue une opportunité intéressante pour les auteurs d'attaques DDoS. Les violations de comptes de banques nationales et régionales ont connu une augmentation notable à partir du 16 avril, date à laquelle de nombreuses banques publient leurs résultats du premier trimestre. Au cours de cette période, les fournisseurs de solutions de gestion des identités et des accès (IAM) et fournisseurs de réseaux, comme Okta et Cisco, ont également fait état d'une hausse substantielle des attaques par « credential stuffing » ciblant les services en ligne.

Plus précisément, la découverte en avril 2023 d'une vulnérabilité de gravité élevée du Service Location Protocol (SLP) (CVE-2023-29552) a probablement contribué à l'intensification des attaques. Cette vulnérabilité, qui peut amplifier les attaques DDoS dans les couches réseau et applicatives, aurait affecté plus de 2 000 organisations dans le monde et plus de 54 000 instances SLP sur Internet. Son exploitation permet aux pirates d'utiliser les instances compromises pour lancer des attaques DDoS à grande échelle. Avec un facteur d'amplification pouvant aller jusqu'à 2 200 fois, cette vulnérabilité a donné lieu à l'une des attaques par amplification les plus importantes jamais documentées.

Nous avons identifié un événement clé en examinant la période d'août/septembre 2023. Le 5 septembre 2023, Akamai a observé et déjoué la plus grande attaque DDoS jamais enregistrée contre une institution financière américaine. Cette agression combinait des techniques ACK, PUSH, RESET et SYN flood, atteignant des pics d'intensité de 633,7 gigabits par seconde (Gbit/s) et 55,1 millions de paquets par seconde (Mpps). Malgré sa forte intensité, l'attaque a été brève, puisqu'elle a duré moins de deux minutes.

Analyse de sécurité

Intensité des attaques DDoS des couches 3 et 4 : événements vs Gbit/s

Pour bien saisir la menace que représentent les attaques DDoS pour le secteur des services financiers, il est essentiel de comprendre à quel point elles sont complexes et de grande ampleur. Il ne s'agit pas de simples incidents isolés ; chaque attaque implique souvent de multiples tentatives à haut volume qui inondent les réseaux de gigabits de données et de millions de paquets par seconde. La sophistication, l'intensité, la durée des attaques augmentent et les pirates utilisent des techniques plus variées, ce qui accroît le risque pour les institutions financières (figure 3).

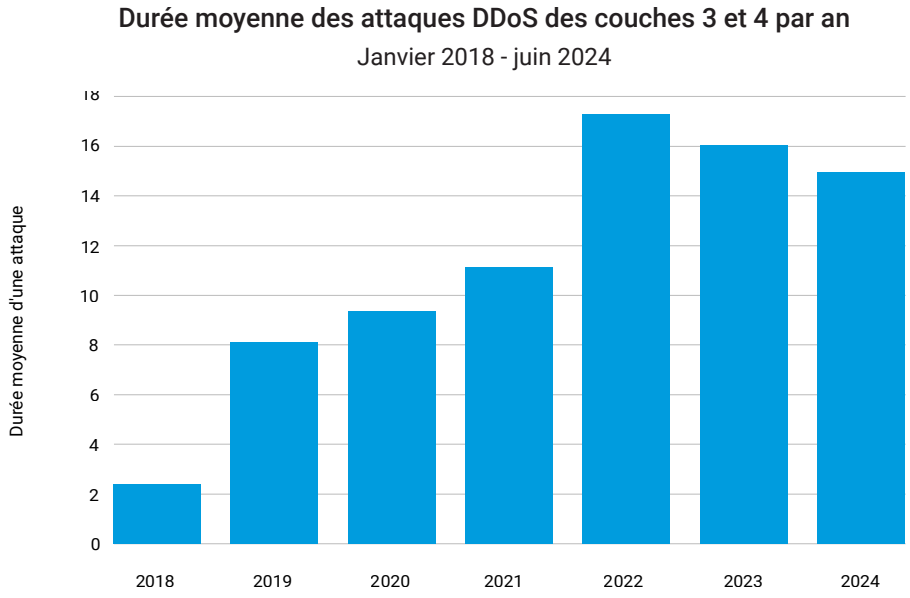


Figure 3 : la tendance mondiale est à la hausse de la durée des attaques DDoS des couches 3 et 4

En outre, si vous comparez le graphique du nombre d'attaques DDoS des couches 3 et 4 dans le secteur des services financiers avec les données correspondantes sur les attaques DDoS en Gbit/s, vous constaterez un écart important (figure 4). Le graphique des Gbit/s montre de fortes augmentations qui ne se reflètent pas dans le graphique des attaques. Cette disparité met en évidence un point important : même si le nombre d'attaques au cours d'un mois est relativement faible, le volume de trafic DDoS en Gbit/s peut être extrêmement élevé.

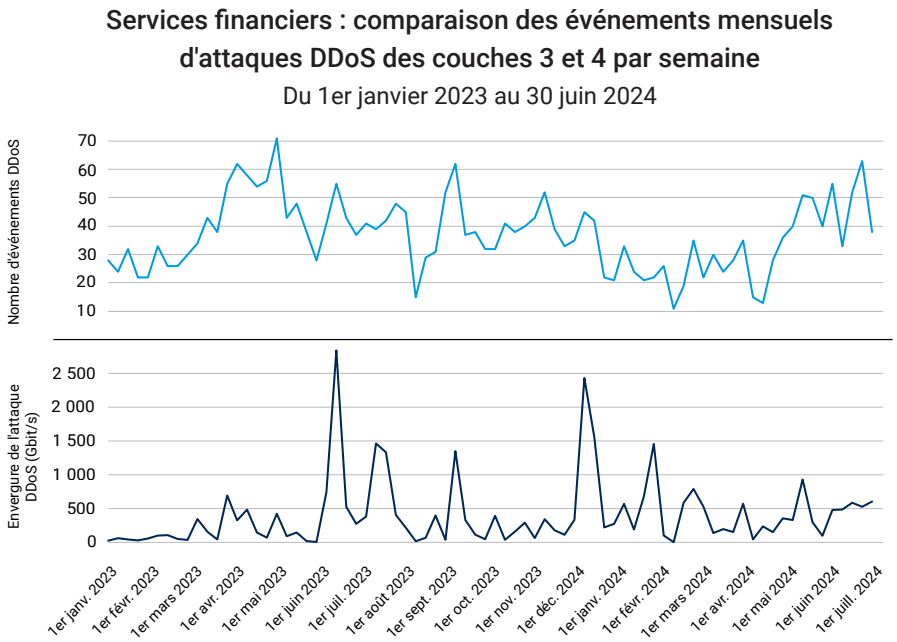


Figure 4 : événements d'attaques DDoS des couches 3 et 4 du secteur des services financiers comparées à leurs mesures en Gbit/s

Cette observation met en évidence un point essentiel : en se fiant uniquement à la fréquence des attaques, l'on sous-estime gravement la menace réelle. Il est impératif de prendre en compte à la fois le volume et l'intensité du trafic pour chaque attaque. Un petit nombre d'attaques DDoS très intenses peut causer beaucoup plus de dégâts qu'un grand nombre d'événements de moindre ampleur, d'où la nécessité d'évaluer l'étendue réelle de chaque menace.

Une tendance à faire cavalier seul : les attaques DDoS à vecteur unique des couches 3 et 4 dans les services financiers

Les attaques multivectorielles contre les applications ou les réseaux constituent une stratégie courante pour les cybercriminels qui tentent de corrompre un système ou d'y obtenir un accès non autorisé. Toutefois, les pirates qui se concentrent sur le secteur des services financiers semblent tenter plus fréquemment des attaques à vecteur unique lorsque l'attaque DDoS vise les couches 3 et 4 (figure 5).

Nombre de vecteurs d'attaque DDoS des couches 3 et 4 par événement d'attaque

Du 1er janvier 2023 au 30 juin 2024

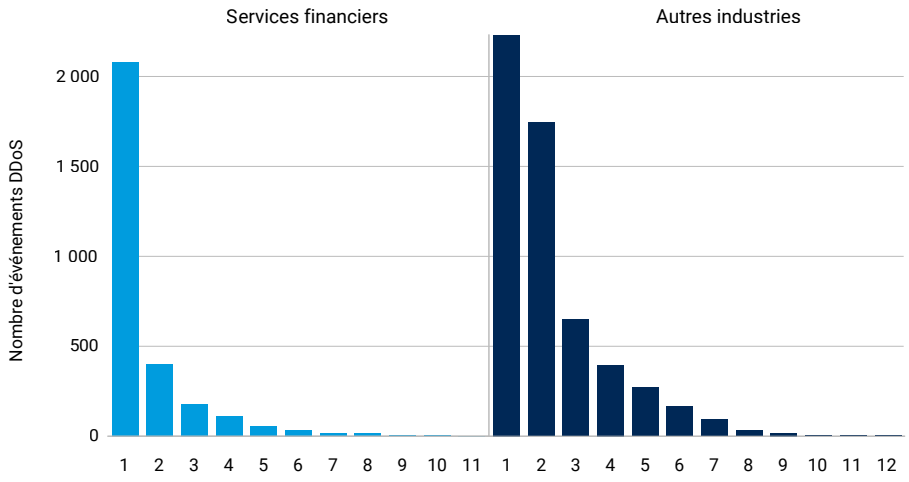


Figure 5 : les attaques à vecteur unique sont plus largement utilisées pour les attaques DDoS des couches 3 et 4 dans le secteur des services financiers

Les attaques DDoS à vecteur unique ciblant les couches 3 et 4 nécessitent moins de ressources et peuvent être très efficaces en soi, notamment lorsqu'elles visent les institutions financières qui disposent souvent de défenses solides contre les attaques plus complexes. Elles sont généralement plus faciles à exécuter et demandent moins de coordination que les attaques multivectorielles. Il se peut également que certaines vulnérabilités connues des couches 3 et 4 propres aux institutions financières puissent être exploitées efficacement avec des attaques à vecteur unique, sans courir le risque d'utiliser d'autres vecteurs d'attaque susceptibles d'être détectés par les services de sécurité.

Cette préférence pour les attaques à vecteur unique dans le secteur des services financiers représente un défi particulier pour les équipes de cybersécurité. Si la vigilance face aux attaques multivectorielles complexes reste de mise, vous devez absolument vous assurer que les défenses peuvent résister à des attaques ciblées à vecteur unique sur les couches 3 et 4.

Augmentation des attaques DDoS de la couche 7 sur les API

Les attaques DDoS au niveau de la couche applicative (couche 7), également connues sous le nom d'attaques HTTP ou de couches de trafic Web, sont de plus en plus répandues et constituent désormais une méthode privilégiée pour les acteurs de la menace qui ciblent le secteur des services financiers. Ces attaques se concentrent spécifiquement sur les composantes les plus gourmandes en ressources des applications, interdisant ainsi l'accès aux utilisateurs légitimes. Contrairement aux attaques DDoS des couches 3 et 4, qui sont souvent atténuées par les pare-feu et la protection du réseau, les attaques de la couche 7 contournent ces défenses en se faisant passer pour des requêtes légitimes lorsqu'elles ciblent des pages d'application ou des fonctions de recherche spécifiques, dans le but de submerger le serveur d'application.

Bien que les applications Web du secteur des services financiers soient généralement plus souvent visées que les API, nous avons observé une forte augmentation du nombre d'attaques DDoS de couche 7 ciblant spécifiquement des API (figure 6). Ces pics d'attaques contre les API sont nettement plus importants et variés dans ce secteur que dans les autres secteurs.

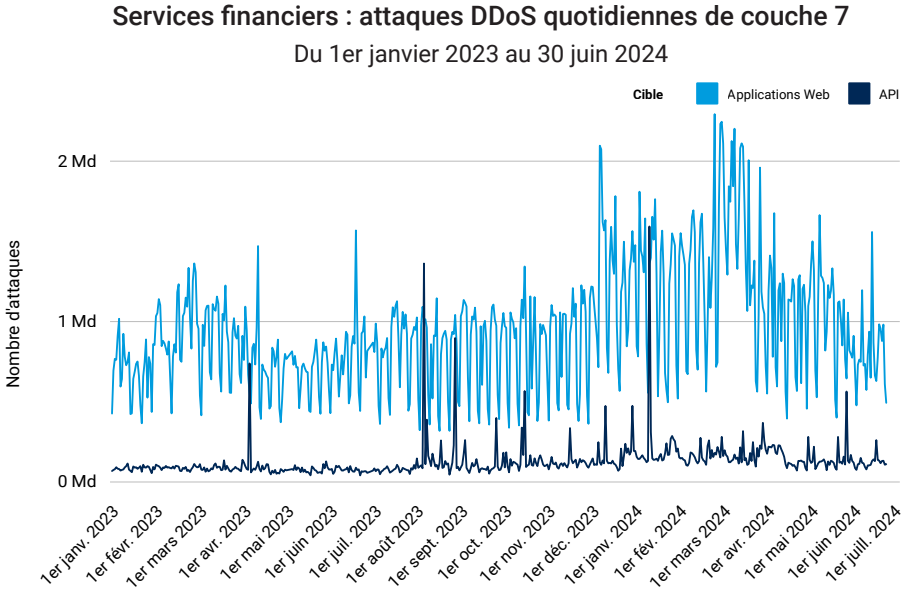
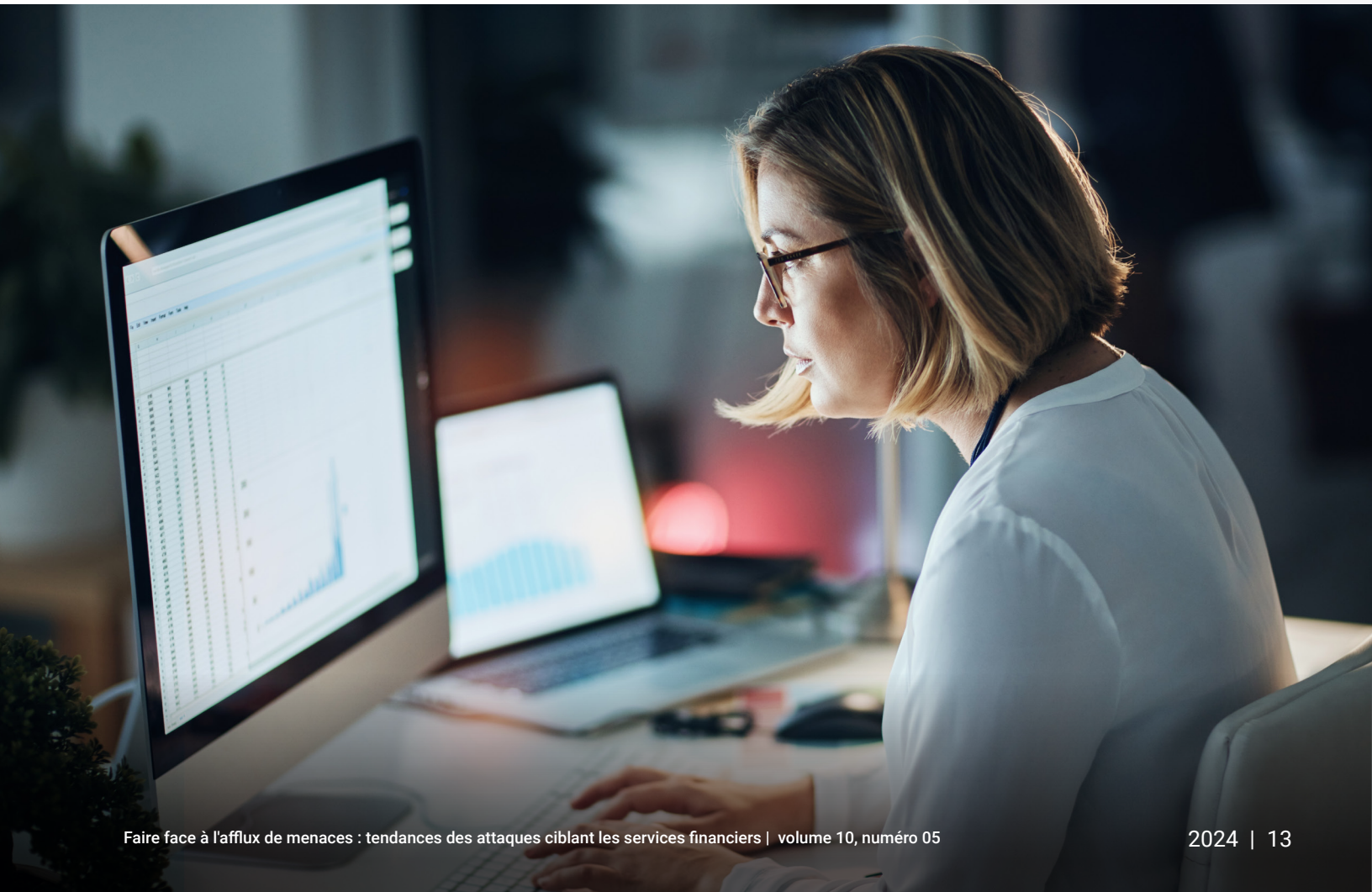


Figure 6 : les schémas d'attaque varient considérablement entre les applications Web et les API ciblées dans les attaques DDoS de couche 7 contre le secteur des services financiers

De fortes augmentations ont été observées spécifiquement en avril 2023, en août 2023 et en janvier 2024. Nous attribuons ces pics à des facteurs similaires à ceux qui affectent les attaques des couches 3 et 4, ainsi qu'à d'autres éléments spécifiques à la couche 7.

Les attaquants recherchent continuellement de nouvelles vulnérabilités à exploiter, et la découverte de nouvelles faiblesses peut entraîner une augmentation soudaine de la fréquence des attaques. Par exemple, la vulnérabilité HTTP/2 Rapid Reset (CVE-2023-44487), identifiée pour la première fois en août 2023, a permis des attaques DDoS de la couche 7 très efficaces. Cette vulnérabilité a offert aux pirates la possibilité d'exploiter une logique apparemment bénigne et de regrouper plusieurs demandes en un flux, submergeant les serveurs et les applications. Elle a donné lieu à la plus grande attaque DDoS de couche 7 jamais enregistrée à ce jour.

En outre, les attaques DDoS saisonnières restent une tactique populaire pour les cybercriminels qui ciblent les institutions financières, avec des pics notables pendant la saison des impôts et les périodes de fêtes. L'augmentation significative observée en janvier 2024, après le temps des achats de fin d'année, suggère que les pirates se préparaient à frapper pendant les périodes d'activité accrue de transactions en ligne.



Ransomware et hacktivisme dans les services financiers

Le secteur des services financiers est souvent la cible d'acteurs malveillants très sophistiqués tels que les groupes de ransomware. Ces groupes utilisent un large éventail de techniques pour infiltrer les institutions financières, voler des informations sensibles et exiger d'importantes rançons. Bien que ces opérations soient principalement motivées par des raisons financières, elles peuvent également s'inscrire dans un contexte géopolitique en ciblant des institutions financières susceptibles d'avoir certains liens politiques. Nous en avons un exemple avec le groupe de ransomware basé en Russie connu sous le nom de REvil (alias Sodinokibi). BlackCat (ALPHV) a également été impliqué dans ce type d'activité, notamment avec l'attaque d'une grande banque.

LockBit reste l'un des groupes de ransomware les plus actifs, connu pour ses attaques contre de grandes organisations, y compris des institutions financières. Et ce, malgré les récentes mesures prises par les autorités à l'encontre de ce groupe. L'opération Cronos, orchestrée par Europol et Eurojust et mobilisant une coalition unique de forces de police internationales, a été dépassée par la nouvelle infrastructure mise en place par LockBit. Le groupe de ransomware a réapparu avec une nouvelle infrastructure et un site de fuite sur le dark Web quelques jours seulement après la saisie de ses serveurs par les forces de l'ordre en février 2024. LockBit a déclaré qu'il riposterait en multipliant les attaques contre les réseaux gouvernementaux en réponse à l'opération Cronos.

Le groupe de ransomware CL0P reste également actif, et est particulièrement connu pour exploiter les vulnérabilités de logiciels de transfert de fichiers largement utilisés dans les organisations, y compris les institutions financières. Un exemple notable est celui de la vulnérabilité zero-day CVE-2023-34362 du logiciel MOVEit Transfer, qui a d'abord été exploitée par le biais d'une injection SQL pour infiltrer cette application Web. Au moins 15 banques et coopératives de crédit ont confirmé des violations de données dues à la vulnérabilité de MOVEit. CL0P a également obtenu un accès initial par d'autres techniques, notamment l'hameçonnage, et continue de fonctionner selon un modèle RaaS (ransomware as a service). Récemment, le groupe a fait évoluer ses tactiques pour employer une quadruple extorsion sur des cibles telles que les institutions financières. En plus des techniques impliquées dans la triple extorsion, la quadruple extorsion comprend l'envoi de messages destinés à harceler les partenaires commerciaux, les employés, les clients, les cadres supérieurs et les médias, les informant que l'organisation a été piratée. Cette tactique a entraîné une augmentation du montant moyen des paiements effectués au titre des ransomwares.

Anonymous Sudan, KillNet et NoName057(16) sont d'autres acteurs malveillants hacktivistes qui ciblent les institutions financières, mais ne sont pas considérés comme des groupes de ransomware. Ils sont tous connus pour leurs activités liées à la guerre entre la Russie et l'Ukraine. Anonymous Sudan a en outre affirmé avoir participé à des cyberattaques en réaction à la guerre entre Israël et le Hamas. L'année dernière, ces groupes, ainsi que de nombreux autres groupes d'acteurs malveillants, ont profité du chaos provoqué par la guerre entre la Russie et l'Ukraine pour s'attaquer à des infrastructures bancaires critiques.

Il existe de nombreux autres acteurs malveillants prolifiques qui ne sont pas classés comme des groupes de ransomware, mais sont connus pour cibler le secteur des services financiers, tels que Lazarus Group, MoneyTaker, Carbanak/FIN7, Cobalt et APT41.

Compte tenu des menaces permanentes posées par ces acteurs, il est essentiel pour les institutions financières de connaître le paysage actuel des menaces et de mieux comprendre les motivations et les techniques des pirates afin de développer des stratégies de défense plus efficaces. Pour connaître les mesures de protection recommandées, reportez-vous à la section consacrée aux mesures d'atténuation plus loin dans ce rapport.

La récente flambée de l'hacktivisme DDoSt contre les institutions financières au Moyen-Orient

Le secteur des services financiers au Moyen-Orient a récemment connu une flambée des attaques DDoS sophistiquées et soutenues motivées par des tensions géopolitiques. Cette tendance est particulièrement forte dans la région Europe, Moyen-Orient et Afrique (EMEA) et illustre la menace croissante des attaques DDoS à motivation politique contre les institutions financières.

Un exemple notable s'est produit au début de l'année, lorsque BlackMeta (également connu sous le nom de DarkMeta), un groupe d'hacktivistes propalestiniens, a lancé une attaque DDoS de couche 7 d'une durée de six jours contre une institution financière des Émirats arabes unis (EAU). L'attaque a été facilitée par InfraShutdown, un service de DDoS à louer, ce qui met en évidence l'accessibilité croissante de ces outils d'attaque. BlackMeta, qui est actif depuis novembre 2023, a déjà ciblé des organisations en Israël, aux Émirats arabes unis et aux États-Unis.

L'attaque contre l'institution financière des Émirats arabes unis a été importante tant par sa durée que par son intensité. Elle s'est étalée sur environ 100 heures, avec des vagues de requêtes Web d'une durée de 4 à 20 heures, et une moyenne de 4,5 millions de requêtes par seconde. La banque a été attaquée 70 % du temps, ce qui a eu un impact considérable sur ses services. La campagne de BlackMeta contre la banque s'inscrivait dans le cadre d'un effort plus large visant à protester contre les injustices perçues à l'encontre des Palestiniens et des musulmans, et a fait appel à des tactiques similaires à celles employées par Anonymous Sudan.

Heureusement, les efforts d'atténuation de l'institution financière ont permis d'éviter des perturbations plus importantes, mais cet incident souligne la tendance à la hausse des cyberattaques à motivation politique. Il met également en évidence la disponibilité croissante de services de DDoS à louer, qui réduisent les obstacles au lancement d'attaques à grande échelle par les groupes d'hacktivistes. Cette évolution souligne la nécessité de mettre en place des mesures de cybersécurité solides pour se protéger contre les menaces persistantes et de grande ampleur.

Une autre attaque DDoS récente, soupçonnée d'être motivée par des considérations politiques, s'est produite le 15 juillet 2024 et a visé une importante entreprise de services financiers en Israël. Cette attaque massive, qui provenait d'un botnet distribué à l'échelle mondiale, a duré près de 24 heures et a atteint un pic de 798 Gbit/s. Akamai a réussi à atténuer cette attaque DDoS sur les couches 3 et 4 qui incluait divers vecteurs, tels que la réflexion DNS et l'inondation UDP.

Lors de cette attaque, Akamai a bloqué environ 389 téraoctets de trafic malveillant au cours d'une phase intensive de trois heures, le trafic total bloqué atteignant environ 419 téraoctets sur toute la durée de l'attaque. Les services d'autres institutions financières israéliennes ont été interrompus le même jour, ce qui suggère un assaut coordonné, soulignant encore la menace croissante que représentent les attaques DDoS avancées.

Il convient de noter que cet agresseur aux ressources considérables avait déjà ciblé le même client du secteur des services financiers à 27 reprises au cours des 90 jours précédents. Le client est la cible d'attaques DDoS répétées depuis le quatrième trimestre 2023, coïncidant avec la guerre entre Israël et le Hamas. Le groupe interne de veille sur les menaces DDoS d'Akamai signale que les institutions et les entreprises en Israël ont subi un nombre sans précédent d'attaques DDoS en 2024. Cette campagne soutenue et agressive met en évidence l'ampleur et l'intensité croissantes de ces menaces, et montre clairement que les pirates sont de plus en plus persistants et ingénieux.

Miser sur la familiarité : l'usurpation de l'identité de marque dans les services financiers

Alors que les services financiers adoptent des approches axées sur le digital pour améliorer l'expérience client, l'efficacité opérationnelle, l'innovation, les revenus globaux et la visibilité, les cyberattaquants exploitent la confiance inhérente entre les organisations et leurs clients en usurpant l'identité d'une marque. La figure 7 présente des exemples de sites frauduleux qui imitent des institutions financières connues. Si l'hameçonnage et l'usurpation d'identité de marque sont des méthodes courantes, le nombre alarmant de sites Web frauduleux et la rapidité avec laquelle les pirates peuvent créer de nouveaux domaines après la mise hors ligne de leurs sites d'origine sont particulièrement préoccupants. Cette prolifération rapide constitue une menace croissante et implacable pour le secteur des services financiers.

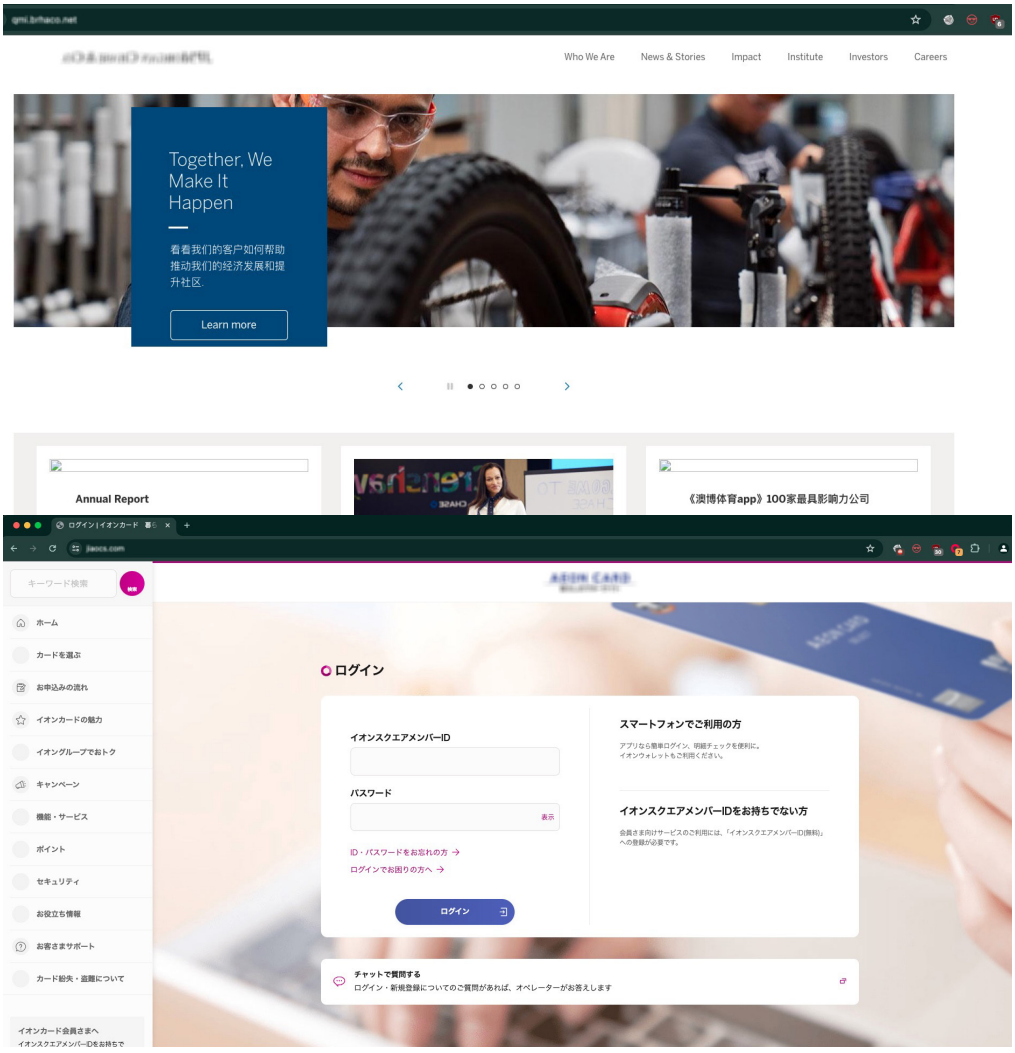


Figure 7 : exemples de sites d'hameçonnage frauduleux imitant des institutions financières connues

Le paysage de l'abus de marque a été considérablement modifié par l'émergence de boîtes à outils et de plateformes d'hameçonnage en tant que service. Ces ressources facilitent la tâche initiale des cybercriminels, ce qui a eu un impact conséquent sur l'échelle et l'ampleur des attaques d'hameçonnage contre les services financiers et leurs clients. Pour mettre les choses en perspective, l'Anti-Phishing Working Group a enregistré près de cinq millions d'attaques d'hameçonnage en 2023, marquant cette année comme « la pire année jamais enregistrée pour l'hameçonnage ».

L'utilisation abusive d'une marque peut être à l'origine d'une escalade de risques tels que l'usurpation d'identité et la violation de comptes. Très souvent, les pirates vendent des informations sur les clients sur le dark Web ou les utilisent pour pirater un compte. Du point de vue de la sécurité, il est crucial d'intervenir rapidement en cas d'attaque contre une marque. En déjouant une attaque dès le début de son cycle de vie, vous pouvez empêcher les pirates de collecter des informations d'identification à des fins malveillantes.

Les ramifications de l'utilisation abusive d'une marque vont au-delà des problèmes de sécurité immédiats. Une organisation peut subir des pertes financières considérables en raison d'atteintes à sa réputation, de problèmes de conformité et de problèmes juridiques, voire de ventes perdues à cause de produits contrefaits. Dans le paysage digital actuel, la détection précoce des attaques d'usurpation d'identité de marque est primordiale pour maintenir la confiance des clients et la continuité des activités.

Tromperies : zoom sur les attaques d'usurpation d'identité

Les équipes de sécurité sont confrontées à un défi de taille : défendre contre les potentielles usurpations d'identité de marque sur diverses plateformes en ligne, qui compliquent la protection des actifs digitaux, car les utilisateurs légitimes comme les pirates peuvent y accéder. Les pirates récupèrent souvent le contenu d'actifs publics tels que les portails bancaires en ligne pour créer leur propre site frauduleux et enregistrer un domaine mal orthographié pour tromper les utilisateurs qui ne se doutent de rien. En outre, les cyberattaquants lancent des campagnes d'hameçonnage par e-mail, sur les réseaux sociaux et par d'autres canaux digitaux afin d'attirer des victimes potentielles vers leurs sites malveillants ou leurs fausses applications.

Pour ce rapport, nous avons analysé les activités d'usurpation d'identité de marque et d'hameçonnage observées sur des domaines actifs au cours des 12 derniers mois, afin de fournir des informations sur la prévalence de l'usurpation d'identité de marque dans tous les secteurs, et plus particulièrement dans les services financiers. Grâce à la visibilité complète et à la solution propriétaire d'Akamai, nous pouvons :

- suivre le trafic sur les sites d'hameçonnage et d'usurpation d'identité de marque, y compris les marketplaces ;
- identifier le nombre de domaines malveillants actifs ;
- évaluer les scores de gravité des domaines malveillants.

Les services financiers ont été le secteur le plus usurpé (36,25 %) parmi tous les sites suspects surveillés par Akamai (figure 8). Ce résultat met particulièrement en évidence la vulnérabilité du secteur des services financiers à l'usurpation d'identité et à l'abus de marque. Les organisations des secteurs du commerce (26,41 %) et des services aux entreprises (18,90 %) arrivent respectivement en deuxième et troisième position.

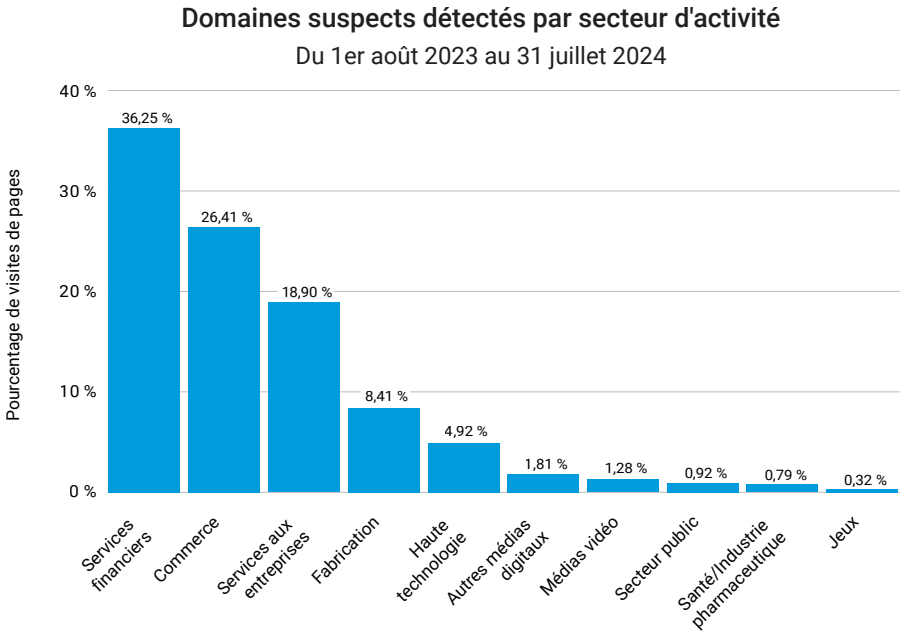


Figure 8 : les services financiers représentent 36,3 % des domaines d'hameçonnage et/ou d'usurpation d'identité de marque

Le secteur des services financiers est une cible de choix pour les attaques d'usurpation d'identité de marque en raison des grandes quantités de données sensibles et de grande valeur qu'il détient, telles que les identifiants bancaires et les informations personnelles identifiables (PII). Les informations obtenues sur des sites bancaires contrefaits permettent aux cybercriminels d'accéder facilement à des comptes et de les vider. Il est également possible d'obtenir d'autres informations financières de grande valeur, comme les identifiants de portefeuilles électroniques et de comptes de cryptomonnaies (les prix varient entre 120 et 400 dollars sur le dark Web). Les pirates peuvent alors transférer le contenu d'un compte ou vendre les informations sur des marketplaces obscurs. L'importance des gains liés à de tels stratagèmes fait des services financiers des cibles de choix pour les abus de marque et les attaques par hameçonnage.

De même, les organisations commerciales sont devenues des cibles lucratives de l'usurpation de marque depuis l'essor du commerce électronique et des achats en ligne, qui offre des possibilités de siphonner des informations d'identification et d'autres informations personnelles. Les entreprises de fabrication et les vendeurs tiers qui fournissent des services sont également vulnérables à l'usurpation de marque. Bien que la digitalisation favorise la croissance globale des entreprises, elle est devenue un point faible vulnérable pour de nombreuses organisations, entraînant la prolifération des attaques par usurpation d'identité de marque et la multiplication des tentatives d'hameçonnage.

En raison des profits importants que les stratagèmes d'usurpation d'identité de marque peuvent engendrer, les services financiers sont une cible privilégiée des attaques par usurpation d'identité et hameçonnage.

Les organisations doivent rester vigilantes et mettre en œuvre des mesures de sécurité pour protéger à la fois leurs marques et leurs clients dans ce paysage digital en constante évolution. Ces mesures comprennent une surveillance continue de l'utilisation abusive de la marque, des procédures de retrait rapide des sites frauduleux et l'éducation des clients pour qu'ils sachent reconnaître les tentatives d'usurpation d'identité potentielles. En donnant la priorité à ces efforts, les organisations peuvent mieux protéger leur réputation et la confiance de leurs clients dans un environnement de menaces de plus en plus complexe.

Les services financiers dans la ligne de mire de l'abus de marque

Pour avoir une vision globale de l'impact de l'usurpation d'identité de marque et de l'hameçonnage, nous avons également analysé le nombre de pages visitées sur les sites Web suspects. Nos résultats révèlent que les sites se faisant passer pour des institutions financières ont reçu 30 % des visites, tandis que ceux imitant des sociétés commerciales suivent avec 20 % des visites (figure 9). Ces résultats placent systématiquement les services financiers et le commerce en tête des attaques, que ce soit au niveau des requêtes ou des domaines. Cette constance met en évidence leur statut de cibles privilégiées pour les abus de marque et l'usurpation d'identité, et ce pour de bonnes raisons.

Les services financiers englobent un large éventail de cibles, depuis les banques bien établies jusqu'aux institutions plus petites disposant de moins de ressources en matière de sécurité, toutes exposées à un risque élevé. Le commerce, un autre secteur qui fait l'objet d'un examen similaire en tant que services par les forums de conformité (par exemple, le conseil des normes de sécurité de l'industrie des cartes de paiement), est également confronté à des risques importants en raison de la richesse des informations qu'il possède sur ses clients.

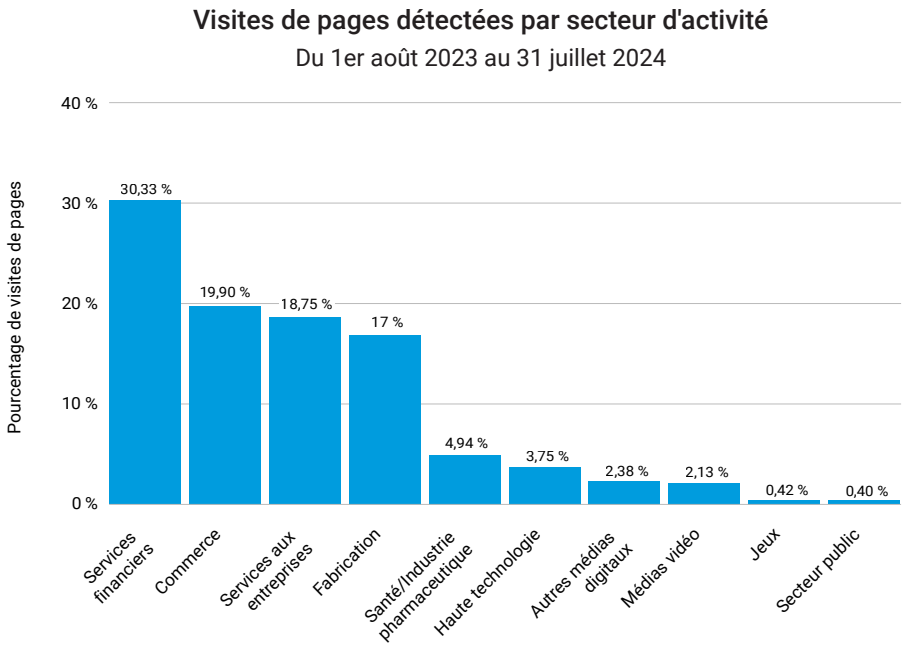


Figure 9 : plus de 30 % des pages visitées au cours de la période de référence (août 2023-juillet 2024) l'ont été sur des sites suspects qui se faisaient passer pour des sites de services financiers légitimes

Il est intéressant de noter que nous avons observé certaines disparités entre le classement des domaines usurpés et le nombre réel de visites dans les différents secteurs d'activité. Par exemple, le secteur de la haute technologie se classe parmi les cinq premiers pour les domaines usurpés, mais tombe à la sixième place en termes de visites réelles. De même, s'il y a moins de domaines se faisant passer pour des domaines pharmaceutiques ou de santé, le nombre de visites est plus élevé pour ces derniers.

Hameçonnage pour obtenir des informations d'identification

L'usurpation de marque prend de nombreuses formes, notamment des sites sosies qui reproduisent le logo et le design exacts de l'entreprise légitime, des applications frauduleuses et de faux profils de réseaux sociaux imitant les comptes officiels de l'entreprise. Pour comprendre l'ampleur de ce problème, nous avons analysé des pages contrefaites et les avons classées par type : usurpation d'identité de marque, hameçonnage, applications indésirables, fausses boutiques, contournement de paywall et faux profils sociaux. Il est important de noter que le domaine d'une même organisation peut être classé dans plusieurs catégories en fonction des pages que nous surveillons.

Notre analyse a révélé que l'hameçonnage est dominant dans les domaines contrefaits qui ciblent les institutions de services financiers, représentant un pourcentage stupéfiant de 68 % de tous les cas enregistrés (figure 10). L'usurpation d'identité de marque suit en deuxième place, avec 24 % de tous les domaines enregistrés. Parmi les sites fréquentés par les utilisateurs, l'hameçonnage et l'usurpation d'identité de marque se classent à nouveau en première et deuxième position, respectivement. D'autres formes d'abus de marque, comme les faux profils de réseaux sociaux et les fausses boutiques, sont moins importantes dans les institutions financières que dans d'autres secteurs. Malgré la diminution du nombre d'attaques ciblant des applications indésirables, il est important de noter que les pirates adoptent des méthodes de plus en plus créatives pour élargir leur champ d'action.

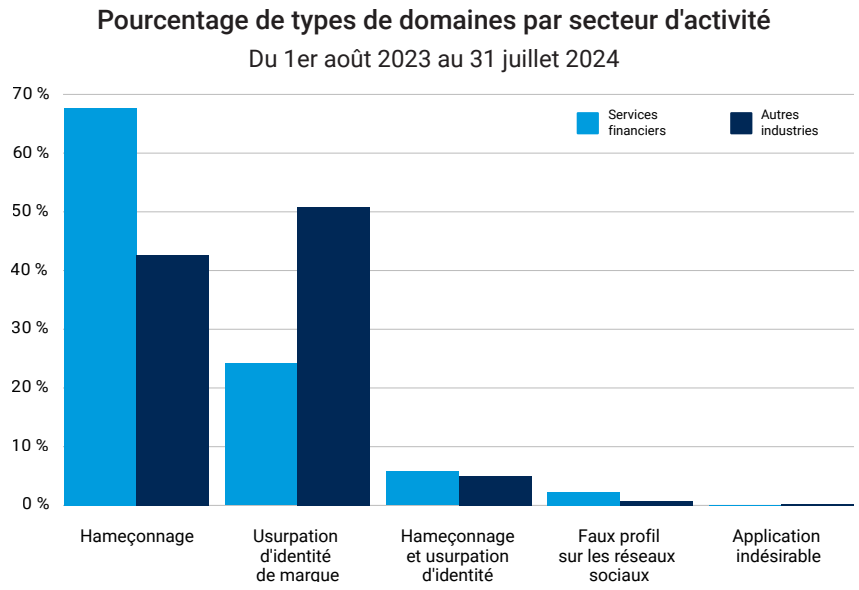


Figure 10 : la majorité des domaines que nous avons enregistrés pour les services financiers sont des sites d'hameçonnage, dépassant même le total de tous les autres secteurs combinés

Les institutions financières sont considérées comme des entités hautement fiables, ce qui en fait des cibles de choix pour les fraudeurs qui exploitent cette confiance.

Malgré une sensibilisation accrue aux risques posés par l'hameçonnage, l'élément humain reste une lacune importante en matière de sécurité. Cette lacune est exacerbée par les techniques sophistiquées utilisées par les pirates (lisez la section Anatomie de l'abus de marque pour plus de détails), ce qui fait qu'il est difficile pour un œil non averti de repérer une fausse page. Les institutions financières sont considérées comme des entités de confiance et sont donc des cibles de choix pour les fraudeurs qui exploitent cette confiance. En usurpant l'identité de ces institutions, les pirates trompent les utilisateurs pour qu'ils donnent volontairement leurs informations d'identification, tirant parti de la réputation de l'institution pour rendre leurs escroqueries plus convaincantes et plus efficaces.

Pour protéger à la fois une organisation et ses clients, il est vital d'utiliser des technologies de sécurité dotées de capacités de surveillance de la marque, capables de détecter de manière proactive toute utilisation non autorisée d'une marque, qu'il s'agisse d'un nom de domaine, d'une application pour mobile ou d'une communication par e-mail. Une fois ces éléments identifiés, l'étape suivante consiste à procéder à des démantèlements pour contrecarrer le trafic, qui pourrait potentiellement exposer les clients aux dangers (tels que le vol de données) posés par l'abus de marque et l'hameçonnage.

Étude de cas : la sophistication croissante des attaques par credential stuffing contre les institutions financières

En 2023 et 2024, une entreprise américaine de fintech a subi des attaques incessantes par « credential stuffing » visant l'une de ses applications en contact avec la clientèle. L'ampleur de ces attaques est stupéfiante : au cours d'une période de 24 heures, Akamai a détecté plus de 3 000 alertes provenant de différentes adresses IP qui tentaient d'infiltrer des comptes à l'aide d'informations d'identification volées. Nous avons observé qu'une seule adresse IP pouvait essayer au moins 115 combinaisons de noms d'utilisateur et de mots de passe. Au total, nous avons enregistré plus de 100 000 alertes en juillet 2024.

Les sites de services financiers frauduleux à un niveau de risque critique

Les renseignements exclusifs de notre réseau mondial, combinés à des données supplémentaires provenant de services de renseignements sur les menaces de tiers, nous donnent un avantage certain dans la détection des usurpations d'identité de marque. Nous utilisons ce système complet pour examiner et classer méticuleusement chaque domaine en fonction de son score de menace.

Nous calculons le score de menace à l'aide de trois facteurs clés :

1. **Le score de confiance** : notre certitude qu'un événement est une tentative d'hameçonnage.
2. **Le niveau de sévérité** : le degré de risque (critique, élevé, moyen ou faible) associé à un événement.
3. **Le facteur de fréquence** : le nombre d'événements/sessions associés au site dans un laps de temps donné.

Notre système de notation prend en compte ces trois facteurs clés : confiance, sévérité et fréquence. Nous combinons ces scores pour générer un score de menace global pour chaque domaine suspect, plafonné à 99, afin de garantir une évaluation globale des menaces.

Notre dernière analyse révèle que le secteur des services financiers détient un score médian alarmant de 85, ce qui met en évidence les risques importants auxquels le secteur reste confronté (figure 11). Ce score place les institutions financières dans la ligne de mire des cybercriminels, qui s'attaquent sans relâche à leurs vastes réserves de données sensibles.

Scores de menace par secteur d'activité

Secteur	Score de menace médian	Secteur	Score de menace médian
Secteur public	**95**	Jeux vidéo	**65**
Services financiers	**85**	Fabrication	**64**
Services aux entreprises	**85**	Autres médias digitaux	**62**
Santé/Industrie pharmaceutique	**85**	Commerce	**61**
Médias vidéo	**71**	Haute technologie	**60**

Figure 11 : notre calcul des scores de menace médians montre que les services financiers affichent un score alarmant

Si le secteur public a enregistré le score médian de menace le plus élevé, probablement en raison de sa richesse en informations sensibles et de ses ressources limitées en matière de sécurité, les services financiers restent une cible tout aussi attrayante, les pirates étant attirés par le potentiel de gains financiers considérables qu'ils recèlent. Des secteurs comme les services aux entreprises et l'industrie pharmaceutique/la santé obtiennent également des scores similaires, ce qui indique que les cybercriminels diversifient leurs cibles. Les institutions financières restent néanmoins une cible privilégiée en raison de la nature critique des données qu'elles détiennent.

Ce niveau de menace élevé exige une action immédiate pour renforcer les défenses et atténuer l'évolution des menaces avant qu'elles n'entraînent d'importants dommages financiers et de réputation.

Anatomie de l'abus de marque

L'ampleur des campagnes d'hameçonnage et d'usurpation d'identité est aggravée par l'existence de boîtes à outils d'hameçonnage.

Le succès de la fraude et de l'abus de marque repose en grande partie sur le pouvoir de la marque en tant que leurre d'ingénierie sociale. Les pirates capitalisent sur le sentiment de familiarité et la confiance inhérente que les internautes ont envers les marques connues, en concevant de faux sites Web qui imitent étroitement les sites légitimes. Dans certains cas, les fraudeurs copient même le code exact, de sorte que ces sites illégitimes semblent presque identiques aux vrais. Avec l'essor des outils d'IA générative, qui aident les fraudeurs à éliminer les fautes d'orthographe et de grammaire révélatrices, il est devenu encore plus difficile pour les internautes de faire la distinction entre les sites authentiques et les faux.

L'ampleur des campagnes d'hameçonnage et d'usurpation d'identité est aggravée par l'existence de boîtes à outils d'hameçonnage. Pour la modique somme de 50 dollars, les pirates peuvent acheter des boîtes à outils leur permettant de créer des sites d'hameçonnage convaincants. L'activité cybercriminelle qui consiste à développer, construire et vendre des boîtes à outils d'hameçonnage facilite considérablement le travail initial des campagnes d'hameçonnage et d'usurpation d'identité. Kr3pto et 16 Shop sont deux exemples de boîtes à outils d'hameçonnage répandues. Kr3pto a ciblé les banques britanniques en contournant l'authentification à deux facteurs, tandis que 16Shop s'est concentré sur de grandes marques comme PayPal et Amazon, entre autres. En août 2023, une opération de police internationale a abouti à l'arrestation des créateurs de 16Shop. Ces affaires mettent en évidence la sophistication croissante des attaques par hameçonnage et les efforts coordonnés pour lutter contre la cybercriminalité.

Sous-estimé, mais efficace : le combosquatting

Un autre aspect important de l'abus de marque est l'utilisation de noms de domaine qui ressemblent beaucoup à des sites Web légitimes. En général, les pirates enregistrent leurs domaines après avoir acheté ou créé leur propre site d'hameçonnage. C'est là que des techniques éprouvées comme le cybersquatting et ses nombreuses variantes jouent un rôle essentiel. Une tactique courante est le typosquatting, dans lequel les pirates enregistrent un domaine avec une légère erreur d'orthographe du nom d'une entreprise (par exemple, acamai[.]com), en espérant que l'utilisateur fera une faute de frappe. Une autre méthode, le combosquatting, consiste à ajouter des mots-clés supplémentaires, tels que « support », « login » ou « help », au nom de domaine. Cette tactique tire parti des microsites que l'on trouve souvent sur les sites Web d'entreprises légitimes.

Selon les recherches d'Akamai, bien qu'il s'agisse d'une tactique peu signalée, le combosquatting (l'ajout d'un mot-clé) dépasse le typosquatting (l'ajout, la suppression ou le remplacement d'un caractère) en termes de nombre de domaines actifs. Il est intéressant de noter que le mot « com » figure parmi les principaux mots-clés ajoutés dans les sites frauduleux.

Mécanisme de distribution

Les sites Web de contrefaçon et d'hameçonnage sont distribués par le biais de divers mécanismes, dont le principal est l'e-mail. Ces e-mails paraissent convaincants grâce à l'utilisation d'un logo légitime et contiennent des messages urgents, tels que des demandes de mise à jour des informations de compte. Cependant, l'abus de marque ne se limite pas aux sites Web et aux e-mails ; les pirates diffusent également des menaces par le biais des réseaux sociaux, élargissant ainsi leur portée et leurs tactiques de tromperie.

Des liens cachés à la vue de tous

D'autres tactiques observées font qu'il est plus difficile pour les internautes d'identifier un site d'usurpation d'identité, ce qui peut augmenter le taux de réussite de ces attaques. Par exemple, l'utilisation d'URL raccourcis, de codes QR, d'images hyperliées et de liens textuels dans les SMS permet de dissimuler les liens malveillants. Contrairement à l'e-mail dont les filtres antispam offrent une protection contre ce type d'abus, les escroqueries par SMS ne sont la plupart du temps pas bloquées et ont plus de chances d'être lues ou ouvertes.

D'autres tactiques observées font qu'il est plus difficile pour les internautes d'identifier un site d'usurpation d'identité, ce qui peut augmenter le taux de réussite de ces attaques.

Attaques régionales par hameçonnage et usurpation d'identité de marque dans les services financiers

Les abus de marque affectent les organisations et les consommateurs du monde entier, mais certaines régions sont plus vulnérables à la fraude et aux abus en raison de la concentration du trafic vers les sites d'usurpation d'identité de marque et d'hameçonnage. Notre analyse révèle que la région EMEA a connu le plus grand volume de trafic vers les sites d'hameçonnage et d'usurpation d'identité détectés au cours des 12 derniers mois, dépassant même ceux de l'Amérique du Nord (figure 12). Ce classement couvre à la fois les services financiers et d'autres secteurs d'activité.

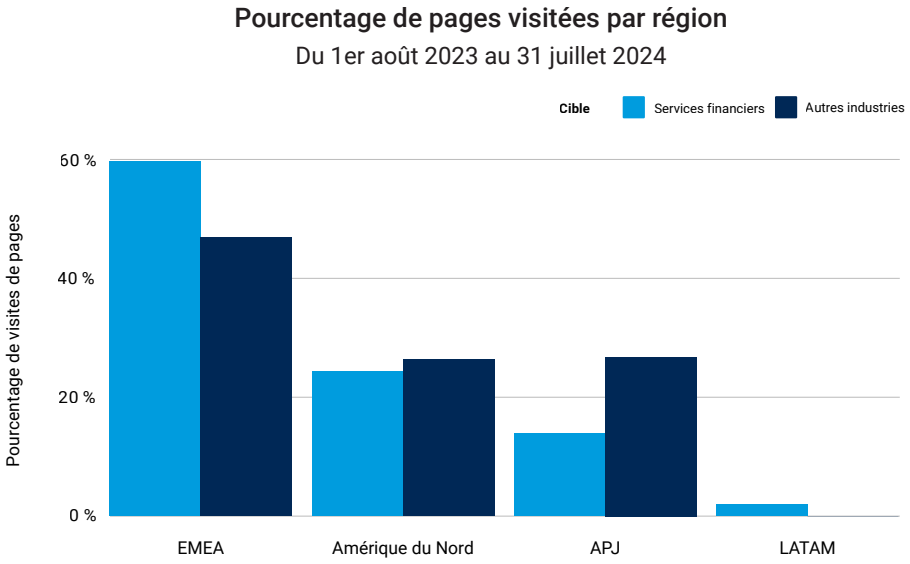
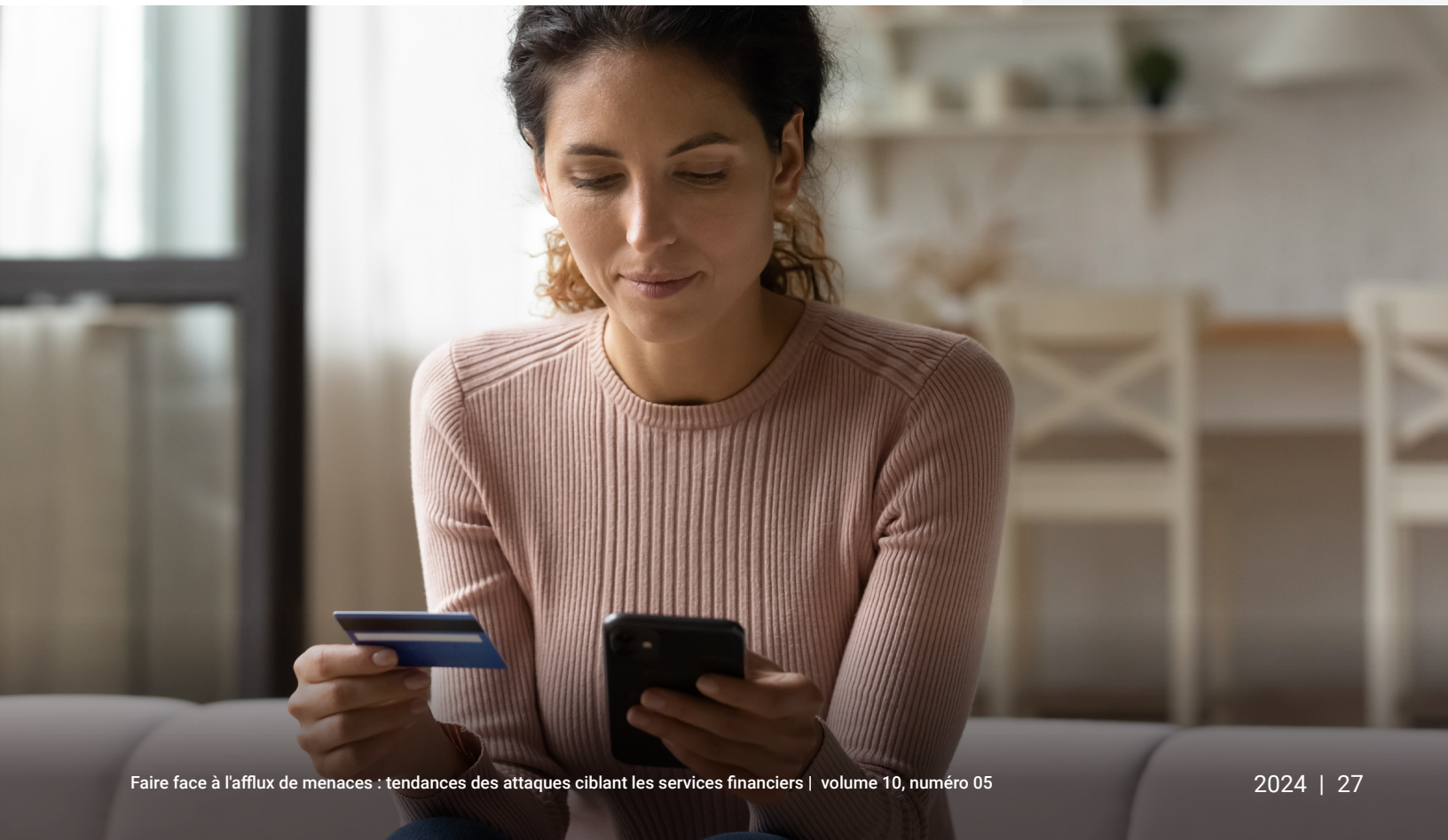


Figure 12 : l'EMEA a dépassé l'Amérique du Nord en tant que région la plus touchée par l'hameçonnage et l'abus de marque dans les services financiers

Bien que l'Amérique latine et les régions Asie-Pacifique et Japon (APJ) enregistrent un nombre relativement plus faible de visites de pages, cela ne signifie pas qu'elles sont moins ciblées. Ces résultats sont probablement plutôt le reflet de la concentration de marques mondiales ayant une clientèle importante en Amérique du Nord et dans la région EMEA, qui offre aux adversaires un plus grand nombre de victimes potentielles. Nous pouvons également attribuer ces résultats à l'émergence de boîtes à outils d'hameçonnage, telles que V3B qui cible spécifiquement les banques de l'UE depuis 2023.

Bien que la région EMEA devance la plupart des régions en nombre de domaines suspects et de pages visitées, la région APJ affiche le score médian de menace le plus élevé : 97. L'Amérique latine, bien qu'elle enregistre le plus petit nombre de visites de sites, affiche un score de menace médian surprenant de 94. Cela indique que les internautes d'Amérique latine et de la zone APJ courent un risque plus élevé de se faire voler leurs informations bancaires et autres données sensibles lorsqu'ils visitent des sites Web.

Plusieurs facteurs contribuent à l'augmentation des dangers d'abus de marque à l'encontre des services financiers dans la région APJ. Tout d'abord, la plupart des institutions de services financiers de l'APJ sont fortement digitalisées, presque tous les services pouvant être utilisés en ligne sans jamais se rendre dans une succursale physique. Le taux de pénétration d'Internet et d'adoption du digital dans la région APJ est l'un des plus élevés au monde, ce qui en fait une cible attrayante pour les cybercriminels. Deuxièmement, cette région abrite certains des pays les plus actifs au monde en matière de réseaux sociaux. Les institutions de services financiers ont intensifié leur engagement auprès des clients par le biais de ces plateformes afin de se disputer des parts de marché et de mieux fidéliser leur clientèle. L'utilisation généralisée des réseaux sociaux et des applications de messagerie dans la région APJ offre aux cybercriminels des vecteurs supplémentaires pour mener des attaques par hameçonnage et usurpation d'identité, souvent en abusant de la confiance que les utilisateurs accordent à ces plateformes.



Évolution de la conformité : comment les réglementations mondiales en matière de cybersécurité façonnent les institutions financières

Lorsqu'on lui a demandé pourquoi il dévalisait les banques, Willie Sutton, célèbre braqueur de banques, a répondu : « Parce que c'est là que se trouve l'argent ». Cette déclaration peut facilement s'appliquer aux cyberattaques contre les institutions financières d'aujourd'hui. La motivation du gain financier ne représente toutefois qu'une partie de l'histoire. Les institutions financières se retrouvent de plus en plus souvent sous le feu de pirates motivés par des préoccupations politiques, ainsi que par des motifs stratégiques géopolitiques. Ces motivations, ajoutées à l'appel du gain, créent une situation désastreuse pour les institutions financières, qui sont devenues le secteur d'activité le plus attaqué.

Cela ne devrait pas nous surprendre, car le secteur financier a toujours joué un rôle essentiel et central dans la société. Par ailleurs, il s'agit d'un secteur fortement réglementé. Dans le passé, la réglementation des institutions financières se focalisait principalement sur la protection des consommateurs dans leurs relations avec les institutions financières, mais les régulateurs cherchent aujourd'hui à appliquer aux institutions financières et aux sociétés de services une réglementation en matière de sécurité et de résilience équivalente à celle concernant les infrastructures critiques. Cette nouvelle tendance inclut des exigences non seulement pour les institutions financières elles-mêmes, mais aussi pour leurs fournisseurs de technologies de l'information et de la communication (TIC).

Il existe de nombreux exemples de réglementations en matière de cybersécurité et de résilience opérationnelle. Dans l'Union européenne, le règlement sur la résilience opérationnelle numérique du secteur financier (DORA) exige que les entités financières et leurs fournisseurs disposent de cadres solides de gestion des risques liés aux TIC, et qu'ils effectuent régulièrement des tests et des rapports sur les incidents. Aux États-Unis, la Securities and Exchange Commission (SEC) a introduit une réglementation sur l'importance des cyberincidents qui oblige les entreprises publiques, y compris les institutions financières, à divulguer les cyberincidents susceptibles d'avoir un impact important sur leurs activités. En Australie, l'Australian Prudential Regulation Authority (APRA) a établi des normes exigeant que les entités maintiennent des capacités de sécurité de l'information proportionnelles à la taille et à l'étendue des menaces pesant sur leurs actifs informationnels (règlement CPS 234). Ces exemples illustrent la tendance mondiale à renforcer la cybersécurité et la résilience opérationnelle des secteurs financiers afin de se protéger contre l'évolution des risques et de garantir la stabilité financière.

Compte tenu de ces réglementations, il incombe aux institutions financières de faire preuve de diligence raisonnable lorsqu'elles achètent des TIC et des services de sécurité, afin de s'assurer que leurs fournisseurs répondent à ces normes de plus en plus strictes. Elles doivent choisir des fournisseurs qui non seulement offrent un service résilient, mais qui comprennent également la réglementation en vigueur, offrent la visibilité nécessaire pour identifier et atténuer des menaces en constante évolution, et aident à appliquer les renseignements obtenus aux opérations en cours.

La visibilité est fondamentale, car vous ne pouvez pas protéger des éléments ou connexions si vous n'êtes pas conscients de leur existence, ni vous prémunir contre une menace que vous ignorez. Des services tels que la plateforme Akamai Guardicore offrent non seulement des protections contre les attaques, mais aident également les clients à comprendre les flux de données, à identifier les anomalies et à segmenter correctement les actifs du réseau afin d'atténuer les menaces. De même, ses services API Security sont conçus pour identifier le trafic API afin de faciliter la détection des API fantômes, ainsi que pour reconnaître les attaques potentielles via des API.

Les banques devraient peut-être ajouter la visibilité au trio habituel de la sécurité (confidentialité, intégrité, disponibilité), afin de refléter cette nouvelle tendance.

James Casey
Vice President, Chief Privacy Officer,
Akamai

Renforcement des défenses avec Zero Trust

La confiance est le fondement sur lequel les institutions financières bâtissent leur réputation. Cependant, lorsqu'il s'agit de protéger des environnements complexes et des données confidentielles, la confiance peut facilement devenir une responsabilité importante. Les cybercriminels tirent souvent parti d'une confiance implicite de multiples façons, notamment par les moyens suivants :

- Attaques par hameçonnage pour se faire passer pour des personnes au sein de l'organisation
- Attaques exploitant les failles de sécurité de fournisseurs tiers pour accéder à des cibles de grande valeur
- Menaces internes liées à des abus de l'accès à des fins malveillantes

En raison de la sophistication croissante des attaques, la sécurité traditionnelle basée sur le périmètre n'est plus adaptée, car elle suppose que tout trafic venant de l'intérieur est digne de confiance. Compte tenu des enjeux élevés pour les services financiers, il est indispensable de maintenir une posture de sécurité résiliente, avec une structure Zero Trust. Cette approche de la sécurité repose sur le principe que toute demande de connexion, tout utilisateur ou tout terminal constitue un danger potentiel. Elle met en œuvre une vérification continue et supprime la confiance implicite, en refusant par défaut l'accès aux ressources à moins que le demandeur ne soit authentifié et autorisé.

Zero Trust améliore la conformité aux exigences réglementaires en constante évolution pour les institutions financières en sécurisant les systèmes qui traitent des données réglementées, permettant ainsi à une organisation d'éviter les pénalités liées à l'échec d'un audit. Elle fournit des contrôles supplémentaires pour les systèmes existants, offrant une visibilité granulaire pour détecter les utilisateurs non autorisés qui tentent d'accéder aux applications critiques.

Le modèle Zero Trust restreint le trafic est-ouest en limitant l'accès du réseau aux systèmes critiques et en empêchant les mouvements latéraux de menaces telles que les ransomwares. Cette stratégie de confinement protège les données et les actifs essentiels en isolant les systèmes infectés. Le nombre d'attaques par ransomware contre les services financiers ayant considérablement augmenté, on ne saurait trop insister sur l'importance du Zero Trust pour la protection des informations sensibles. Grâce à sa visibilité granulaire, Zero Trust vous aide à détecter et à neutraliser les menaces dans des environnements complexes, ce qui est primordial pour empêcher la propagation des ransomwares et protéger les actifs critiques.

Un autre avantage important de Zero Trust est sa capacité à sécuriser les flux de données entre les applications afin de permettre le déploiement en toute sécurité d'applications basées sur le cloud. Cela facilite non seulement la modernisation, mais garantit également la protection des informations confidentielles dans un écosystème des menaces instable et donne aux institutions financières la possibilité d'innover sans compromettre la sécurité. La mise en œuvre d'une structure Zero Trust améliore la posture de sécurité et protège l'institution contre les menaces en constante évolution.

La segmentation, c'est bien. La microsegmentation, c'est encore mieux.

La segmentation est une approche architecturale qui divise un réseau en segments plus petits dans le but d'améliorer les performances et la sécurité. La microsegmentation est une technique de sécurité qui permet de diviser logiquement un réseau en segments de sécurité distincts, jusqu'au niveau de la charge de travail individuelle. Les contrôles de sécurité et la prestation de services peuvent alors être définis pour chaque segment unique.

La microsegmentation est un autre pilier du Zero Trust. Dans un récent rapport d'Akamai, les responsables de la cybersécurité des services financiers ont cité le renforcement du Zero Trust comme la raison la plus fréquente de la mise en œuvre d'un projet de segmentation. Presque tous les responsables qui ont procédé à une segmentation déploient ou ont déjà déployé un cadre de sécurité Zero Trust (99 %), mais moins de la moitié d'entre eux (47 %) déclarent que leur cadre Zero Trust est totalement complet et défini, et donc mature.

La microsegmentation fonctionne avec les systèmes existants et se déploie plus rapidement que les méthodes traditionnelles telles que les pare-feu. Cette approche accélère la réponse aux ransomwares de 13 heures maximum et simplifie la gestion dans tous les environnements informatiques. Elle permet également de satisfaire les besoins de conformité grâce à un contrôle précis des données.

Voici un exemple réel qui montre l'impact de la microsegmentation actuelle : il s'agit d'un projet ayant permis de réduire le temps de déploiement de 2 ans à 6 semaines et les coûts de 85 %, en utilisant un seul ingénieur. Ce cas illustre comment la microsegmentation peut faire gagner du temps et de l'argent aux entreprises. Nous encourageons les directeurs informatiques à comparer ces résultats avec les coûts de sécurité et les délais de mise en œuvre actuels.

Pour renforcer leur position en matière de cybersécurité, les institutions financières doivent donner la priorité à la mise en œuvre de stratégies de segmentation avancées. Les RSSI doivent être le fer de lance des efforts visant à aligner les mesures de sécurité sur des normes évolutives, en intégrant la microsegmentation en tant que pierre angulaire d'une architecture Zero Trust robuste. Les directeurs informatiques doivent établir une cadence d'audits de sécurité et de mises à jour des stratégies réguliers pour s'assurer que leurs défenses restent résistantes face à des cybermenaces sophistiquées.

Cette approche proactive permet non seulement d'atténuer les vulnérabilités actuelles, mais aussi de positionner les organisations de manière à pouvoir relever efficacement les nouveaux défis en matière de cybersécurité. En adoptant ces mesures, les institutions financières créent un cadre de sécurité complet qui répond à la fois aux préoccupations immédiates et à la gestion des risques à long terme.

La [microsegmentation] permet non seulement d'atténuer les vulnérabilités actuelles, mais aussi de positionner les entreprises de manière à pouvoir relever efficacement les nouveaux défis en matière de cybersécurité.

Atténuation

Lorsqu'il s'agit de protéger votre institution financière contre diverses cybermenaces, vous devez mettre en œuvre une approche à multiples facettes. Examinons les principales stratégies d'atténuation de l'hameçonnage, de l'usurpation d'identité de marque, des attaques DDoS et des ransomwares.

Protection contre l'hameçonnage et l'usurpation d'identité de marque

Afin de protéger votre institution contre l'hameçonnage et l'usurpation d'identité de marque, envisagez d'utiliser des services tiers de protection de la marque pour détecter et supprimer rapidement les contenus frauduleux. Il est également important d'informer vos employés et vos clients. Organisez régulièrement des formations de sensibilisation à la sécurité pour votre personnel sur la manière de reconnaître les tentatives d'hameçonnage et d'usurpation d'identité. Fournissez des conseils clairs indiquant comment identifier les communications légitimes de votre institution. Établissez un plan de réaction rapide aux tentatives d'usurpation d'identité, y compris un processus de notification des escroqueries à l'identité aux partenaires et aux clients.

Il est également recommandé de mettre en œuvre les techniques d'atténuation suivantes :

- Enregistrez des noms de domaine similaires pour éviter le typosquatting, et utilisez des services de surveillance de domaine pour détecter les domaines semblables.
- Renforcez les protocoles d'authentification en utilisant des mots de passe forts et uniques et des gestionnaires de mots de passe, et implémentez une authentification multifactorielle (MFA) solide pour tous les comptes et systèmes.
- Déployez des protocoles d'authentification du courrier électronique tels que Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) et Domain-based Message Authentication, Reporting and Conformance (DMARC) pour empêcher l'usurpation d'e-mails. Utilisez des solutions anti-hameçonnage et un filtrage avancé des e-mails pour détecter et bloquer les e-mails malveillants.
- Sécurisez votre site Web et vos canaux digitaux en obtenant des certificats SSL, en mettant en œuvre le protocole HTTPS et en utilisant des outils antifraude pour détecter les activités suspectes sur votre site Web et vos applications pour mobile.
- Protégez les canaux de communication en fournissant des portails sécurisés et en mettant en place une messagerie cryptée pour la correspondance sensible.

Protection contre les attaques DDoS

La protection de votre institution financière contre les attaques DDoS requiert une stratégie de défense à plusieurs couches. Déployez des stratégies proactives, telles que l'utilisation de produits spécialisés de détection, d'atténuation et de protection contre les attaques DDoS, la configuration d'une limitation du débit et la mise en cache du contenu sur un réseau de diffusion de contenu (CDN). En outre, restez informé des mesures de sécurité telles que la gestion des correctifs, les plans de réponse aux incidents, les contrôles d'atténuation pour les adresses IP exposées aux attaques DDoS et les sous-réseaux critiques, les politiques de contrôle d'accès, la segmentation du réseau et les pare-feux. Déployez des stratégies proactives telles que la configuration de la limitation du débit, la mise en cache du contenu sur un CDN et l'utilisation de produits spécialisés de détection, d'atténuation et de protection contre les DDoS.

Pour protéger l'infrastructure DNS, surveillez et analysez en permanence le trafic DNS entrant et optez pour une plateforme hybride plutôt que pour un pare-feu DNS traditionnel. Comprendre les tactiques, les techniques et les procédures utilisées par les pirates vous aidera à mieux vous protéger contre les attaques DDoS.

Protection contre les ransomwares

Comme nous l'avons déjà mentionné dans ce rapport, il est primordial de mettre en place la segmentation du réseau, en particulier la microsegmentation, dans le cadre d'une approche Zero Trust, afin de limiter la propagation des ransomwares au sein de votre institution financière. La mise en œuvre de ce type de mesures de cybersécurité robustes vous aidera à lutter contre les techniques avancées employées par les auteurs d'attaques par ransomware. Faites également preuve de vigilance et utilisez la structure MITRE ATT&CK pour mieux comprendre les tactiques et techniques courantes utilisées par les pirates, et renforcez vos plans d'action en conséquence afin de briser la chaîne d'attaque des ransomwares.

Mettez continuellement à jour vos défenses et formez votre personnel à reconnaître les menaces et à y répondre efficacement. Intégrez des défenses solides du périmètre, une protection des points de terminaison, un filtrage des e-mails et une gestion régulière des correctifs. Mettez en place une surveillance continue du trafic réseau, des journaux système et du comportement des utilisateurs, et appliquez des pratiques de détection des menaces afin d'identifier de manière proactive les menaces liées aux ransomwares.

Mettez en œuvre des sauvegardes de données régulières et sécurisées, y compris des sauvegardes isolées, afin de garantir que les informations critiques puissent être restaurées rapidement en cas d'attaque par ransomware. Mettez en œuvre l'authentification multifactorielle pour tous les comptes d'utilisateurs afin d'ajouter une couche supplémentaire de sécurité.

Grâce à ces stratégies d'atténuation complètes, vous pouvez considérablement améliorer la capacité de votre institution financière à se défendre contre diverses cybermenaces, à assurer la continuité opérationnelle, à protéger votre réputation et à préserver la confiance que vous accordent vos clients.

Conclusion

Tandis que votre institution financière adopte la transformation digitale pour améliorer l'expérience client, l'efficacité opérationnelle et la position concurrentielle, les défis en matière de sécurité s'intensifient, de même que la pression liée à l'environnement réglementaire changeant. Dans cette édition de notre rapport sur l'état des lieux d'Internet, nous avons exploré les menaces persistantes et émergentes qui pèsent sur le secteur des services financiers, soulignant la nécessité d'une évaluation et d'une amélioration continues des solutions de sécurité. Les menaces étant de plus en plus sophistiquées, il est essentiel de garder une longueur d'avance en renforçant les défenses et en affinant les stratégies de sécurité.

Les attaques DDoS contre les institutions financières dépassent désormais celles contre le secteur des jeux, longtemps considéré comme la cible principale, et cette tendance alarmante met en évidence les risques croissants. Des facteurs tels que l'hacktivisme et le climat géopolitique ont rendu les services financiers plus vulnérables que jamais. Parallèlement, il faut noter l'ampleur et la gravité du trafic généré par les sites d'usurpation d'identité de marque et d'hameçonnage qui ciblent les institutions financières, ainsi que la rapidité avec laquelle les pirates peuvent créer de nouveaux domaines après la fermeture des sites initiaux. Le suivi de telles activités oblige les organisations à mobiliser énormément de ressources, et les équipes de sécurité ont besoin de solutions qui incluent des services de démantèlement, des renseignements sur les menaces et la détection de l'usurpation d'identité de marque et de l'hameçonnage sur plusieurs canaux digitaux.

En cas d'attaques par hameçonnage ou autres escroqueries, les internautes et les régulateurs tiennent souvent les institutions financières pour responsables, même lorsqu'elles ne sont pas directement en cause. Plus important encore, l'hameçonnage et l'usurpation d'identité de marque servent souvent de précurseurs à des attaques plus graves, d'où l'importance d'interrompre le cycle d'attaque à un stade précoce. Prendre des mesures décisives vous permettra de préserver la réputation de votre institution et la confiance de vos clients, plutôt que de risquer de vous retrouver à la une des journaux à cause d'une violation.

Compte tenu de la nature incessante des attaques contre les institutions financières, la protection des informations confidentielles pour prévenir les fraudes et les abus reste un énorme défi. L'adoption d'une structure de sécurité telle que Zero Trust est indispensable pour se défendre efficacement contre les attaques par hameçonnage qui ciblent les employés et empêcher les ransomwares de se propager au sein des réseaux pour atteindre les actifs critiques, tout en garantissant la conformité avec les réglementations mondiales existantes et émergentes.

Vous trouverez dans ce rapport des informations exploitables sur les dernières tendances en matière d'attaques dans le secteur des services financiers, qui vous permettront de renforcer vos défenses. En restant vigilant et en appliquant les stratégies présentées, vous pourrez mieux protéger votre organisation et vos clients dans un écosystème de menaces grandissantes.

Tenez-vous au courant de nos dernières recherches en consultant notre centre de recherche sur la sécurité.

Méthodologie

DDoS (couche 7)

Ces données décrivent les alertes de la couche applicative sur le trafic vu à travers notre pare-feu d'application Web (WAF). Les alertes DDoS L7 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, les 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 couvrent une période de 18 mois, du 1er janvier 2023 au 30 juin 2024.

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 centre de commande des opérations de sécurité d'Akamai (SOCC) 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.

Les données de ce rapport couvrent la période de 18 mois allant du 1er janvier 2023 au 30 juin 2024, sauf indication contraire.

Attaques par usurpation d'identité de marque

Akamai Brand Protector est une solution anti-abus conçue pour protéger les entreprises et leurs clients contre les attaques d'usurpation d'identité de marque, telles que l'hameçonnage, les sites Web contrefaits, les faux comptes sur les réseaux sociaux et les applications indésirables. Elle utilise le réseau mondial d'Akamai en bordure de l'Internet, qui analyse plus de 900 To de données par jour, pour détecter les menaces avant qu'elles n'aient un impact sur les clients. Ces informations sont enrichies par des flux tiers provenant de partenaires afin d'offrir une vue d'ensemble des menaces sur diverses plateformes en ligne.

Les différentes caractéristiques de chaque domaine suspect détecté sont analysées et les niveaux de risque déterminés contribuent au calcul du score de menace du domaine. Ces domaines suspects sont surveillés, les données associées sont tracées et les clients concernés sont alertés de ces campagnes malveillantes qui tentent d'exploiter l'identité de la marque.

Les données de ce rapport couvrent les domaines suspects détectés au cours de la période de 12 mois allant du 1er août 2023 au 31 juillet 2024.

Crédits

Directeur de recherche

Mitch Mayne

Édition et rédaction

James Casey
Lance Rhodes
Badette Tribbey

Révision et expertise

Cheryl Chiodi
Ziv Eli
Reuben Koh
Gal Meiri
Richard Meeus
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 concernant les menaces ciblant les services financiers, rendez-vous sur notre **page sur les services financiers**.

Akamai Security protège les applications qui stimulent votre activité à chaque point d'interaction, sans compromettre les performances ou l'expérience client. En tirant parti de l'envergure de notre plateforme mondiale et de la visibilité qu'elle offre sur les menaces, nous travaillons avec vous pour prévenir, détecter et atténuer les menaces, afin de vous permettre de renforcer la confiance en votre marque et de concrétiser votre vision. 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 : 09/24.