Le Chef de la cybersécurité :

des recettes infaillibles pour résister aux attaques DDoS de couche 7

Table des matières

Introduction

Concocter la bonne défense contre les attaques par déni de service distribué (DDoS) d'aujourd'hui représente un défi même pour les professionnels de la sécurité les plus accomplis. Cela est particulièrement vrai pour les attaques DDoS de couche 7, qui comportent des complications supplémentaires. Pour vous aider, vous pouvez vous munir d'un ensemble d'instructions étape par étape avec différentes approches des différentes menaces, ou en d'autres termes, d'un livre de recettes pour lutter contre les attaques DDoS de couche 7.

Les différents adversaires préparent les attaques DDoS différemment. Les attaques de couches 3 et 4 sont surtout une question de force. Qui a la meilleure capacité de réseau, l'attaquant ou la défense ? Les attaques de couche 7, quant à elles, ciblent la couche applicative du modèle OSI (Open Systems Interconnection), qui est responsable de l'interaction directe avec les applications logicielles. Elles visent à submerger un serveur Web, une base de données ou une application en exploitant la capacité, les allocations de mémoire ou les faiblesses dans la façon dont ces systèmes traitent les requêtes.

Les attaques DDoS de couche 7 présentent donc des défis spécifiques en matière d'atténuation, d'autant que les requêtes apparaissent souvent comme du trafic légitime. Il est donc difficile de filtrer les requêtes malveillantes sans conséquences sur les utilisateurs légitimes. De plus, la disponibilité des ressources d'automatisation et de cloud permet aux attaquants de lancer ce type d'attaques rapidement et à grande échelle.

Dans ce document, nous abordons les défis liés à l'atténuation des attaques DDoS de couche 7 avec des recettes détaillées, qui présentent les outils et techniques utilisés par les attaquants, les tactiques de détection et d'atténuation pour les contrer, ainsi que l'analyse post-événement et des suggestions de récupération.

Grâce à l'expérience d'Akamai en matière de diffusion de contenu et de cybersécurité, ainsi qu'à notre plateforme cloud distribuée comptant plus de 4 200 points de présence dans le monde, nous avons une perspective unique sur les attaques DDoS actuelles. Alors que les attaques DDoS au niveau de la couche applicative sont toujours plus complexes et multiformes, il est important d'avoir une vue d'ensemble et d'adopter une stratégie approfondie de défense. C'est ce que nous proposons ici.

Que vous soyez un professionnel de la sécurité de première ligne à la recherche d'aide concernant une menace ou une vulnérabilité spécifique, ou un RSSI cherchant à améliorer votre posture de sécurité, vous trouverez dans ce livre la recette du succès.

Cibles courantes et exemples d'attaques DDoS de couche 7

Les attaques DDoS de couche 7 ciblent la couche supérieure du modèle OSI, soit la couche applicative. Leur objectif est de submerger les ressources d'une cible en exploitant la façon dont les applications Web traitent les requêtes. Les cibles courantes des attaques DDoS de couche 7 sont les suivantes :

Serveurs Web : les attaquants ciblent les serveurs Web pour perturber la diffusion de contenu aux utilisateurs légitimes. Cela peut ralentir le chargement des sites Web ou les rendre complètement inaccessibles.

Applications Web : les applications qui reposent sur des bases de données ou des services back-end sont vulnérables aux attaques DDoS de couche 7, car elles sont capables d'exploiter les faiblesses dans la façon dont ces applications analysent et traitent les requêtes, ou encore gèrent les sessions.

Interfaces de programmation d'applications (API) : les API sont une composante essentielle des services Web actuels et des applications pour mobile. Les attaquants ciblent les API pour perturber l'interaction entre les différents services logiciels, affectant ainsi la fonctionnalité des applications qui s'appuient sur ces API.

Services DNS : bien que des attaques DNS se produisent parfois au niveau d'autres couches, les attaques de couche 7 peuvent impliquer le bombardement du service DNS avec des requêtes malveillantes en vue de perturber la résolution des noms de domaine, ce qui entraîne des problèmes d'accessibilité généralisés. L'adoption croissante de DNS sur HTTP/TLS pourrait se traduire par une augmentation de ce type d'attaques.

Serveurs de messagerie : cibler les serveurs de messagerie peut perturber les communications, affectant à la fois les e-mails entrants et sortants.

Passerelles de paiement et services financiers : ce sont des cibles lucratives pour les attaquants qui cherchent à perturber les transactions et à semer le chaos dans les opérations financières.

Les rapports SOTI (État des lieux d'Internet) et les analyses de sécurité d'Akamai examinent régulièrement l'évolution du paysage des attaques DDoS de couche 7, mettant en évidence la diversité des vecteurs d'attaque et les secteurs les plus exposés.

Vecteurs d'attaque

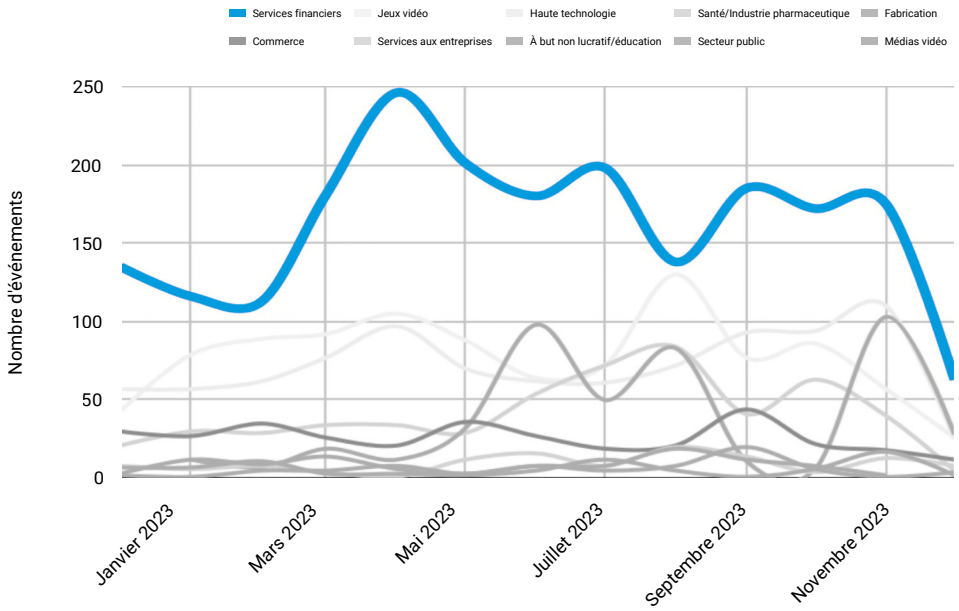
- Attaques ciblant les applications Web et les API : les attaquants visent le plus souvent les points d'entrée des sites Web, y compris les points de terminaison API, qui ne sont généralement pas mis en cache en raison de leur contenu ou de leur configuration. Certains des chemins couramment ciblés incluent « / », « /home », « /en-US », « /pricing/ », etc.

- Parmi les vecteurs d'attaque les plus fréquents :
  • HTTP GET / POST flood sur les pages d'accueil
  • HTTPS GET flood sur des chemins aléatoires et des chaînes de requête
  • Attaques Slow read
  • Floods de téléchargement de fichiers volumineux

De plus, si l'on observe depuis longtemps une augmentation du nombre d'entreprises confrontées à des attaques DDoS, le mode opératoire a changé. Tout d'abord, le type et le volume des propriétés attaquées ont évolué. Par exemple, au lieu de 10 attaques contre un terminal ou des points de terminaison similaires, 100 attaques peuvent aujourd'hui viser des adresses IP différentes dans l'espace réseau. Et ces attaques ne ciblent pas uniquement la couche 3, mais également la couche 7.

Secteurs d'activités ciblés

Le nombre d'attaques par déni de service distribué (DDoS) contre les secteurs des services financiers, des jeux d'argent et de l'industrie manufacturière, en particulier dans la région EMEA, a dépassé en 2023 les chiffres enregistrés dans toutes les autres régions réunies.

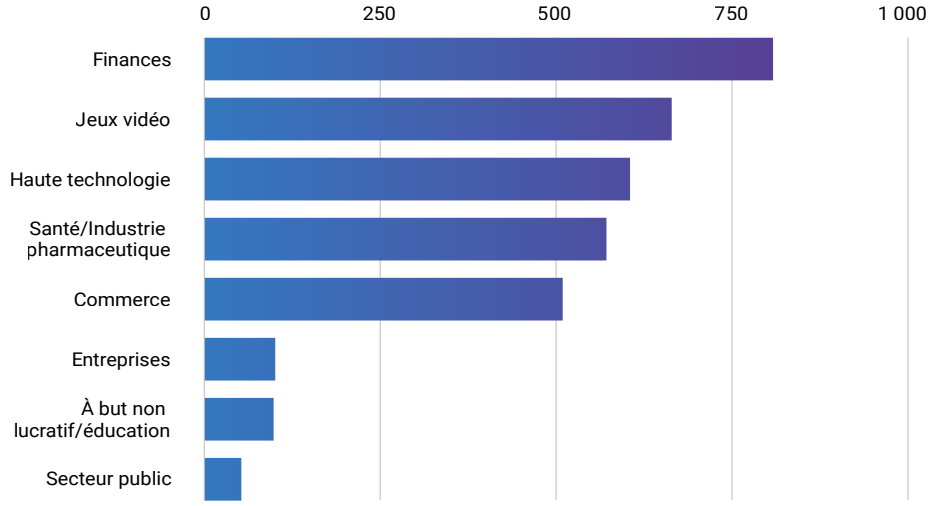


DDoS : Here to Stay, mars 2024

Les services financiers en particulier sont devenus une cible de prédilection pour les attaques DDoS de couche 7. Depuis 2021, Akamai a constaté une augmentation notable du nombre d'attaques DDoS contre des sociétés de services financiers. Plus d'un tiers (35 %) des attaques contre l'ensemble des secteurs visaient des institutions de services financiers en 2023, ce secteur devenant une cible encore plus attrayante que le jeu. L'analyse d'Akamai montre que le secteur bancaire a été la cible de 63 % des attaques DDoS dans le monde. Près des trois quarts (72 %) des attaques dans la région EMEA et 91 % dans la région APAC concernaient des banques. En Amérique, cependant, les attaques DDoS étaient réparties de manière plus uniforme entre les banques, les assurances et les autres institutions de services financiers.

Amérique : les services financiers représentent 28 % des attaques DDoS

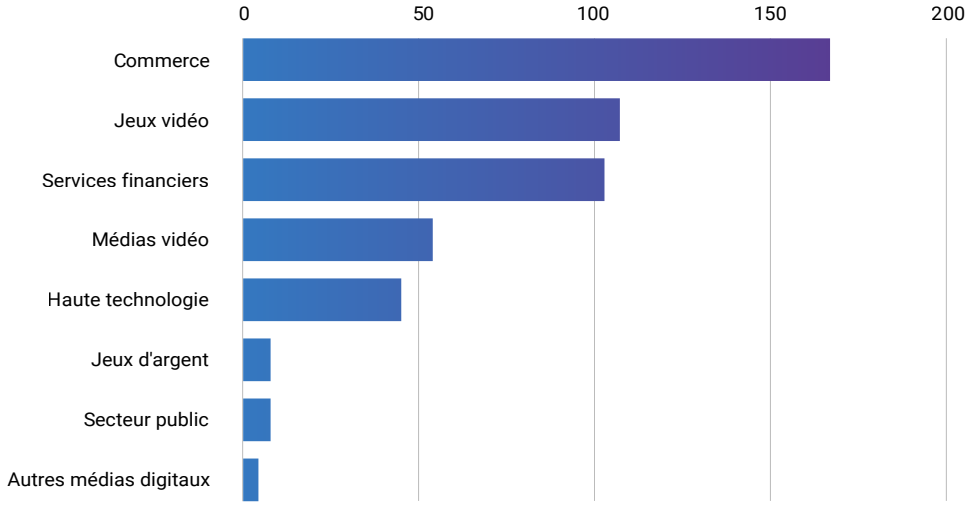
Juin 2023 à décembre 2023



DDoS : Here to Stay, mars 2024

APAC : les services financiers représentent 11 % des attaques DDoS

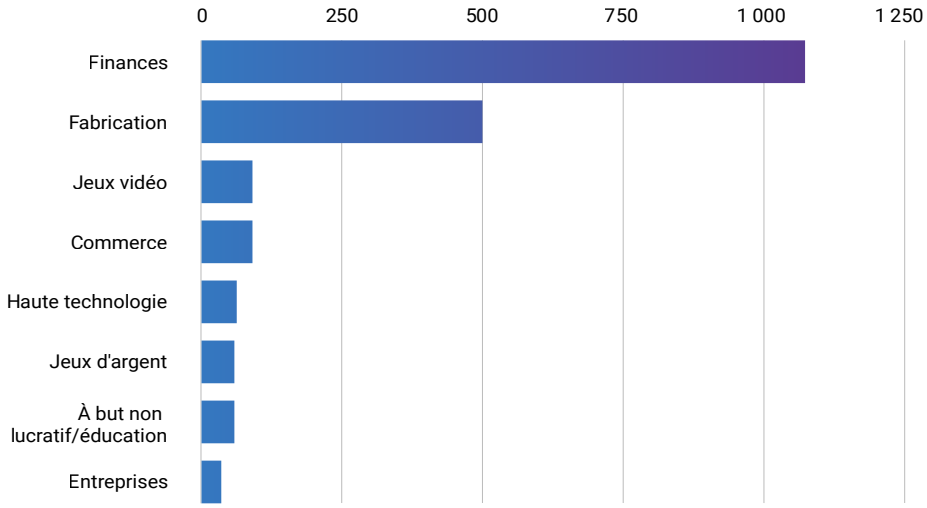
Juin 2023 à décembre 2023



DDoS : Here to Stay, mars 2024

Région EMEA : les services financiers représentent 66 % des attaques DDoS

Juin 2023 à décembre 2023



DDoS : Here to Stay, mars 2024

Dans l'exemple récent d'une attaque DDoS sophistiquée de couche 7 sur l'un des clients d'Akamai du secteur des services financiers, les cyberattaquants ont utilisé l'automatisation et créé une attaque hautement distribuée. Cette attaque a exploité HTTP GET flood, ciblant principalement les URL ne pouvant pas être mises en cache (comme la page d'accueil et les points de terminaison de connexion). Grâce à divers contrôles proactifs, cette attaque a été atténuée avec succès, sans impact sur l'origine du client. Cette carte des sources d'attaque souligne l'utilisation croissante de fournisseurs de services cloud, de nœuds de sortie Tor et de nœuds de proxy anonymes ou ouverts.

Attaques DDoS par système autonome

Visualisation d'une attaque de la couche applicative visant un établissement financier au premier trimestre 2024 dans plus de 100 pays, attaque qu'Akamai a contribué à atténuer

Les auteurs d'attaques DDoS ont la capacité de construire et de coordonner une infrastructure d'attaque largement dispersée, exploitant les adresses IP dynamiques sur des réseaux étendus et couvrant de nombreux pays et régions du monde entier.

Outils et techniques utilisés par les attaquants

Malheureusement, les pirates lançant des attaques DDoS ne restent pas figés, et leurs méthodes non plus. Ne manquant jamais d'idées pour monétiser leurs actes, les attaquants adaptent leurs techniques, tirent parti des nouveaux outils et inventent de nouvelles méthodes. Différents facteurs témoignent de cette évolution.

Automatisation : les attaquants utilisent des scripts et des bots automatisés pour imiter le comportement des utilisateurs légitimes, ce qui rend la détection beaucoup plus difficile. En outre, les attaquants se tournent désormais vers des algorithmes d'apprentissage automatique qui s'adaptent et échappent à la détection traditionnelle.

Attaques multivectorielles : les attaquants emploient de plus en plus de stratégies multivectorielles, associant différents types d'attaques (comme GET et POST flood) et des cibles DNS (comme les attaques par amplification et fragmentation) avec d'autres combinaisons pour submerger à la fois les ressources réseau et applicatives.

Ciblage des API : les attaquants profitent du fait que les entreprises s'appuient de plus en plus sur les API pour alimenter leurs applications afin d'abuser des vulnérabilités de ces API dans leurs attaques DDoS. Les attaques visent à épuiser les ressources du serveur en demandant des milliers de connexions simultanément, ou à exploiter des failles logiques, provoquant des interruptions de service.

Exploitation des terminaux IoT : la prolifération de terminaux IoT mal sécurisés fournit une vaste armée pour les botnets. Ces terminaux sont souvent détournés et utilisés pour lancer des attaques DDoS massives tirant parti de leur connectivité réseau et de leur puissance de calcul.

Hausse du niveau de sophistication

Avec ces nouveaux outils et techniques, les attaques DDoS sont devenues plus fréquentes et plus complexes, les attaquants employant des méthodes sophistiquées pour contourner les défenses traditionnelles. Voici quelques-unes des tendances notables :

Chiffrement : une bascule notable vers les attaques DDoS basées sur HTTPS a rendu l'atténuation plus difficile. Ces attaques, qui sont chiffrées, se font passer pour du trafic légitime et sont donc plus difficiles à détecter et à filtrer, car les mesures de protection DDoS traditionnelles ont des capacités limitées de déchiffrement du trafic SSL/TLS de la couche applicative.

Botnets et proxys : compte tenu de la croissance significative des botnets DDoS et de la prévalence des proxys anonymes par les attaquants, les requêtes sont désormais envoyées depuis une multitude d'adresses IP (généralement plus de 10 000 adresses IP par attaque). Les attaquants utilisent cette stratégie pour contourner les mesures d'atténuation qui dénombrent les requêtes provenant d'une seule adresse IP. La prévalence des plateformes d'hébergement dans le cloud et l'adoption de services basés sur le cloud facilitent encore davantage la conception de ces attaques de haute intensité et hautement distribuées.

Attaques DDoS par système autonome

Visualisation d'une attaque DDoS récente au niveau de la couche applicative contre un client financier d'Akamai : 650 000 transactions par seconde (TPS), 20 Gbit/s, plus de 9 milliards de requêtes au total

Les auteurs d'attaques DDoS sont capables de créer et de coordonner une infrastructure d'attaque extrêmement distribuée, principalement à partir de fournisseurs de cloud.

Une approche de plus en plus prisée par les défenseurs consiste à suivre les requêtes par empreinte TLS, celle-ci étant composée de plusieurs signaux de couche TLS, comme le type et l'ordre de chiffrement. Bien que sensible aux faux positifs, si elle est utilisée correctement, cette approche peut fournir une atténuation plus efficace lorsque l'attaquant opère à partir de différentes machines et adresses IP, car le même logiciel est installé sur les terminaux compromis. Ces terminaux présentent des caractéristiques environnementales similaires, dont la bibliothèque TLS partagée.

Approvisionnement en ingrédients

Alors que les outils disponibles sur le marché changent fréquemment, l'évolution des techniques d'attaque implique l'adoption de méthodes plus sophistiquées et moins détectables. En voici quelques exemples :

- **Terminaux IoT compromis :** les attaquants continuent d'utiliser des terminaux IoT compromis dans des botnets comme méthode pour lancer des attaques DDoS à grande échelle, soulignant la vulnérabilité permanente de ces terminaux.

- **Services DDoS-for-hire :** la disponibilité des services DDoS-for-hire a abaissé la barrière d'entrée des attaques, permettant à des individus ne possédant pas de connaissances techniques approfondies de mener des attaques à grande échelle.

- **Techniques d'évasion :** les techniques d'évasion avancées, telles que les paramètres d'en-tête aléatoires et les arguments de requête dynamiques, sont devenues plus courantes. Ces techniques remettent en question les approches traditionnelles de détection et d'atténuation en rendant le trafic malveillant plus difficile à distinguer des requêtes légitimes.

Vulnérabilités généralement exploitées dans de telles attaques

Les vulnérabilités que les attaquants exploitent dans les attaques DDoS de couche 7 sont souvent liées à la façon dont les applications Web traitent les entrées des utilisateurs et gèrent les données. Pour atténuer ces vulnérabilités, il est crucial d'employer une combinaison de mesures de sécurité.

Ces dernières années, l'une des vulnérabilités les plus importantes exploitées par les attaquants lors d'attaques DDoS au niveau de la couche applicative était la faille HTTP/2 Rapid Reset, largement publiée fin 2023. De telles attaques ont tiré parti d'une faille du protocole HTTP/2, qui est indispensable au bon fonctionnement d'Internet et de tous les sites Web. L'exploitation de cette vulnérabilité a entraîné une augmentation globale de 65 % du trafic d'attaques DDoS HTTP en un trimestre par rapport au précédent, mettant en évidence la gravité et l'impact des attaques utilisant cette vulnérabilité.

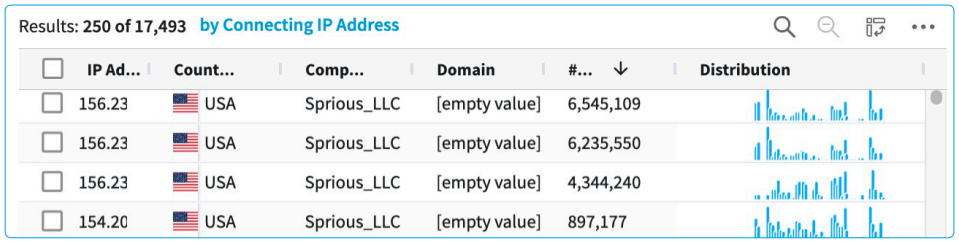
Cette vulnérabilité particulière a permis aux attaquants de générer un impact plus important en exploitant les plateformes de cloud computing et HTTP/2 pour perpétrer des attaques DDoS hyper-volumétriques avec des botnets relativement petits. Les secteurs les plus ciblés par ces attaques comprenaient les jeux vidéo, l'informatique, la cryptomonnaie, les logiciels informatiques et les télécommunications, les États-Unis, la Chine, le Brésil, l'Allemagne et l'Indonésie étant les principales sources de ces attaques.

En réponse, un effort coordonné à l'échelle de tous les secteurs a révélé la vulnérabilité HTTP/2 Rapid Reset (CVE-2023-44487) pour mettre en lumière les attaques DDoS utilisant cette faille. Divers fournisseurs ont été ciblés, y compris les principaux fournisseurs de services cloud et de CDN, entre autres.

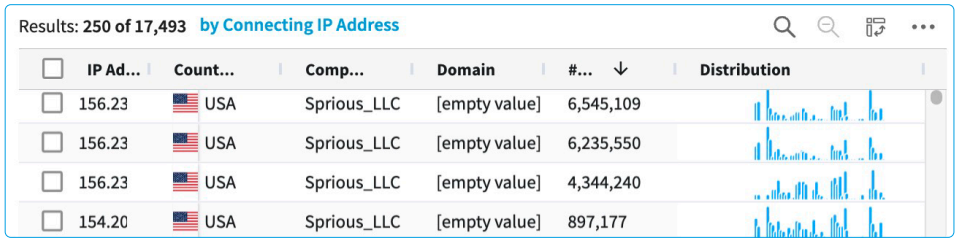
Exemples concrets : utilisation de l'automatisation dans une attaque DDoS

Les attaquants utilisent souvent plusieurs outils DDoS pour exécuter les mêmes attaques DDoS, chacun tirant parti de plusieurs techniques pour contourner les produits de sécurité ou au moins réduire leur efficacité. Un exemple d'attaque de ce type est décrit ci-dessous à l'aide d'Akamai Web Security Analytics.

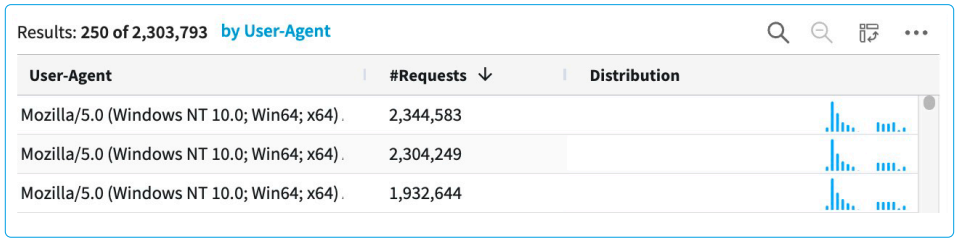
- Attaque vue depuis plus de 17 000 adresses IP



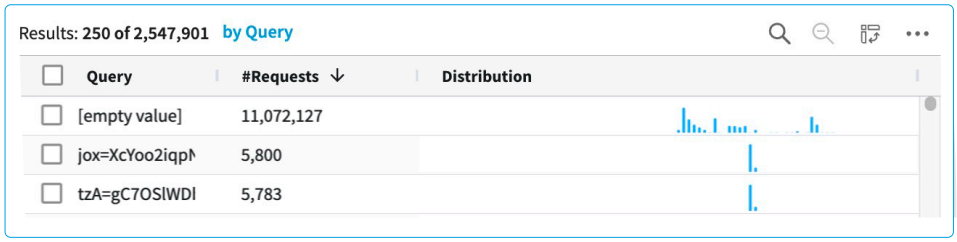
- Sources d'attaque depuis plus de 400 réseaux



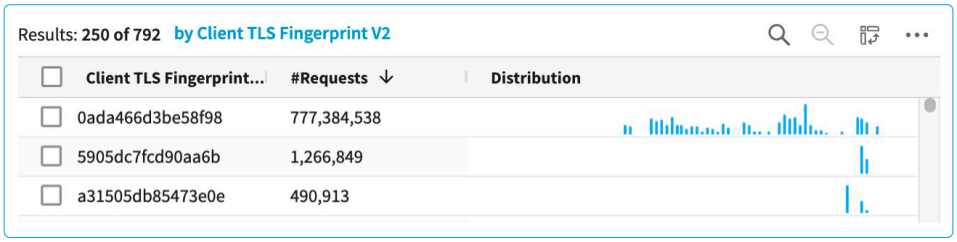
- 2 303 793 agents utilisateurs uniques



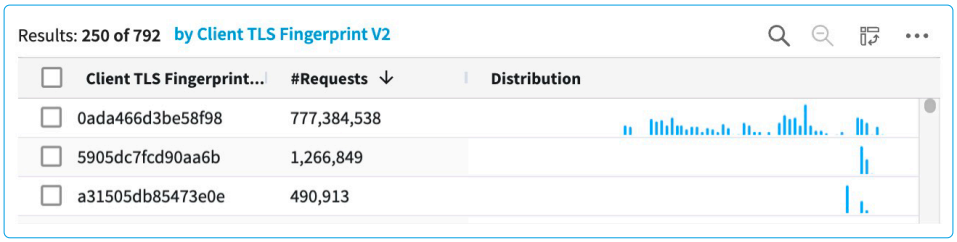
- 2 547 901 chaînes de requête uniques et aléatoires



- Rotation de l'en-tête HTTP (par exemple, Accept-Language, Referer)



- Rotation du réglage TLS



L'atténuation d'attaques aussi sophistiquées nécessite une stratégie de protection à plusieurs niveaux. Il peut être utile de mettre en place des contrôles proactifs et réactifs, tels qu'une combinaison avancée de correspondances de demandes et de caractéristiques de trafic source dans la limitation de débit ou des contrôles de la réputation de la source.

Des adversaires mieux armés : usurpation d'identité de signal TLS

Des observations récentes ont montré que les acteurs malveillants utilisent plus fréquemment les signaux TLS dans leurs outils DDoS afin d'échapper à la détection en faisant en sorte que ces connexions semblent provenir de navigateurs Chrome légitimes. Au lieu d'utiliser une version sans interface de Chrome gourmande en ressources et susceptible de ralentir l'attaque, il est possible que les attaquants aient utilisé une version modifiée de la bibliothèque TLS et ainsi réussi à définir et usurper l'identité des signaux TLS de n'importe quel navigateur authentique. Bien qu'il existe des outils conçus pour répliquer les empreintes TLS, on les trouve rarement dans les outils d'attaque DDoS. Le recours à ce type d'attaque suggère un renforcement des capacités techniques des attaquants et une connaissance approfondie des défenses. C'est pourquoi les stratégies de défense contre les attaques DDoS de couche 7 doivent inclure des recherches régulières sur les dernières tendances en matière d'attaques. Cela semble également suggérer que les outils DDoS qui incluent l'usurpation TLS sont de plus en plus courants.

Regarder autour de vous : évaluation des risques et identification des vulnérabilités

Vous pouvez améliorer de manière significative votre stratégie d'atténuation des attaques DDoS de couche 7 en identifiant vos ressources critiques et en déterminant où elles pourraient être vulnérables à ce type d'attaque. Cette évaluation des risques permet d'établir des priorités en termes de ressources à protéger, en fonction de leur importance et de leur vulnérabilité. En comprenant les vecteurs d'attaque potentiels et leur impact, les entreprises peuvent mettre en œuvre des contre-mesures spécifiques, telles que la limitation du débit, les pare-feux d'application Web et l'analyse du comportement, afin de limiter efficacement les risques. En outre, une évaluation continue des risques permet d'élaborer une stratégie de défense qui évolue en réponse aux nouvelles menaces et aux exigences changeantes de l'entreprise.

Différents secteurs d'activités et entreprises peuvent adopter des approches différentes pour l'évaluation des risques DDoS au niveau de la couche applicative. Par exemple :

E-commerce : avant un événement de vente majeur, une évaluation des risques peut identifier le processus de paiement comme une vulnérabilité critique. Les mesures d'atténuation peuvent inclure la mise en œuvre d'un pare-feu d'application Web (WAF) et la limitation du débit pour protéger le service.

Services financiers : pour une application bancaire, l'évaluation des risques peut déterminer que la page de connexion est une cible privilégiée pour les attaques DDoS. La banque pourrait alors utiliser une combinaison de limitation de débit et de détection comportementale adaptée aux points de terminaison pour faire la distinction entre les utilisateurs légitimes et le trafic d'attaque.

La compréhension des vulnérabilités spécifiques permet de cibler les défenses et d'augmenter les services critiques lors d'une attaque.

Éviter la multiplication des intervenants : rôles et responsabilités

La définition de rôles et de responsabilités clairs est une étape incontournable pour une stratégie DDoS de couche 7 performante, car elle maximise les possibilités de réponse coordonnée et efficace en cas d'attaque. Sans rôles clairs, les efforts de réponse peuvent devenir chaotiques, avec des tâches qui se chevauchent et des lacunes dans la défense. Bien définir les responsabilités aide à identifier les tâches spécifiques de chaque membre de l'équipe, depuis la surveillance du trafic et l'identification des anomalies jusqu'à la mise en œuvre de stratégies d'atténuation et la communication avec les parties prenantes. Cette coordination permet de minimiser l'impact des attaques, de maintenir la disponibilité du service et de protéger les ressources critiques.

En effet, le fait d'avoir trop de décideurs sans rôles clairs peut entraîner des retards dans les réponses lors d'une attaque DDoS. Par exemple, si les équipes d'exploitation du réseau et de cybersécurité décident indépendamment d'approches d'atténuation différentes sans coordination, elles risquent de neutraliser par inadvertance les efforts de l'une vis-à-vis de l'autre et inversement, ou de négliger des vulnérabilités critiques. La bonne stratégie implique de prédéfinir des rôles, par exemple un responsable désigné de la réponse aux incidents, un coordinateur de la communication et une équipe de réponse technique, garantissant des actions rapides et unifiées contre les attaques, minimisant les temps d'arrêt et rationalisant l'analyse post-incident.

Choisir les bons outils pour votre cuisine

La détection et l'atténuation d'une attaque de la couche applicative peuvent s'avérer difficiles, car il est extrêmement difficile de distinguer le trafic légitime du trafic malveillant. En réponse à ces menaces évolutives, nous recommandons une approche multiforme de la défense :

- **Préférer les solutions toujours actives plutôt qu'à la demande :** assurez-vous que les contrôles de sécurité DDoS sont toujours actifs et mettez à jour les plans de réponse aux incidents pour répondre rapidement aux menaces émergentes.

- **Établir une architecture résiliente et fiable :** anticipez un point de défaillance unique, car les attaquants cibleront probablement plusieurs services, y compris le DNS, les applications Web, les API, l'infrastructure réseau et le centre de données. L'utilisation d'une architecture adaptée s'avère cruciale pour la protection contre les attaques DDoS de couche 7. Ces considérations d'architecture peuvent inclure le choix d'une protection DDoS en bordure de l'Internet ou basée sur un CDN et activée en permanence. Ne surestimez pas votre fiabilité. L'ampleur des attaques DDoS actuelles peut facilement submerger la plupart des infrastructures.

- **Évaluer les SLA de votre fournisseur** et les aligner sur votre stratégie.

- **Examiner le niveau de préparation de votre fournisseur :** choisissez un fournisseur qui effectue des examens réguliers de ses composants réseau critiques et évalue différents mécanismes de protection contre les attaques DDoS afin de mieux comprendre leur efficacité contre les méthodes d'attaque actuelles.

- **Revoir votre manuel de réponse aux attaques DDoS :** travaillez en collaboration avec votre personnel informatique, des opérations, de sécurité et de communication client afin d'être mieux préparés en cas d'attaque.

- **Protection DDoS d'urgence :** préparez un plan pour intégrer un fournisseur de solutions de protection contre les attaques DDoS en cas de crise. Si vous disposez d'un partenaire spécialisé dans la protection DDoS, appelez sa ligne d'assistance DDoS.

Recettes pour la détection et l'atténuation

Une protection DDoS efficace au niveau de la couche 7 nécessite plusieurs stratégies de détection et d'atténuation. Il existe différentes méthodologies que vous pouvez appliquer, chacune ayant ses points forts et ses limitations.

Détection comportementale et basée sur les anomalies

Points forts : cette approche repose sur l'utilisation de l'apprentissage automatique et de l'analyse statistique pour comprendre vos schémas de trafic normaux, puis identifier les écarts qui pourraient indiquer la présence d'une attaque DDoS. Elle est très efficace contre des attaques complexes encore jamais vues.

Limitations : une détection efficace nécessite une période d'apprentissage qui peut prendre jusqu'à plusieurs semaines afin d'établir une base de référence pour le trafic « normal ». Au cours de cette période, la détection peut être moins performante. Un modèle qui n'est pas correctement entraîné risque de renvoyer des faux positifs.

Détection basée sur le débit

Points forts : simple à mettre en œuvre, cette méthode surveille le débit et le volume des requêtes, déclenchant des alertes ou des processus d'atténuation lorsque le trafic dépasse des seuils prédéfinis. Elle est efficace pour identifier rapidement les attaques volumétriques à grande échelle.

Limitations : les pics de trafic légitimes, tels que ceux se produisant lors d'événements promotionnels, peuvent être confondus avec des attaques DDoS. Elle peut ne pas détecter les attaques à faible volume et à faible fréquence qui restent sous le radar.

Détection basée sur la signature

Points forts : en comparant le trafic à une base de données de schémas d'attaque connus, cette méthode permet d'identifier et de bloquer rapidement les menaces reconnues. Elle s'avère très efficace contre les vecteurs d'attaque communs et précédemment identifiés.

Limitations : elle ne détecte pas les attaques nouvelles ou modifiées qui ne correspondent pas aux signatures existantes. Des mises à jour régulières sont nécessaires pour maintenir son efficacité.

Tests défi-réponse

Points forts : cette approche pose des défis au trafic entrant pour déterminer s'il est généré par des humains ou des bots. Les CAPTCHA ou calculs JavaScript peuvent atténuer efficacement les bots et les outils d'attaque automatisés.

Limitations : les défis peuvent perturber l'expérience utilisateur s'ils sont mis en œuvre de manière agressive. Certains bots plus sophistiqués sont capables de passer certains tests défi-réponse. Par conséquent, une mise à jour régulière des mécanismes de défi est indispensable.

Approches hybrides

La combinaison de plusieurs stratégies de détection et d'atténuation peut offrir une protection plus complète. Par exemple, l'utilisation de la détection basée sur les anomalies pour signaler les attaques potentielles, complétée par des méthodes basées sur le débit et la signature pour une couverture plus large, procure des mécanismes de défense plus robustes. Des tests défi-réponse ajoutent un filtrage supplémentaire pour distinguer les bots sophistiqués des utilisateurs légitimes.

Méthodes conventionnelles

Filtrage IP et géographique : bloquer ou limiter le trafic de certaines plages IP/CIDR et régions géographiques non pertinentes pour votre entreprise permet de réduire votre exposition aux attaques provenant de ces régions. Bien que cette méthode puisse être utile lorsque l'origine des utilisateurs professionnels est connue et limitée, elle pose parfois des défis quant à la maintenance continue et la mise à jour de la liste des sources acceptées. En outre, les pirates expérimentés peuvent utiliser des proxys pour contourner le géoblocage. Néanmoins, cela reste un choix populaire et une stratégie de défense initiale contre les attaques DDoS de couche 7.

Analyse du protocole de couche applicative : cette méthode permet d'atténuer les attaques DDoS de couche 7 en examinant les données dans les protocoles de la couche applicative afin de détecter les anomalies ou les schémas malveillants, permettant de mettre en place des mécanismes de défense proactifs. Elle contribue à empêcher les attaques DDoS sophistiquées qui contournent les mesures de sécurité conventionnelles. Toutefois, elle peut consommer beaucoup de ressources pour une inspection approfondie des paquets et présente un risque plus élevé de faux positifs, ce qui pourrait bloquer par inadvertance le trafic légitime.

Trouver la recette juste et équilibrée pour une stratégie de défense contre les attaques DDoS à plusieurs couches

L'élaboration d'une stratégie de défense contre les attaques DDoS à plusieurs couches implique une approche nuancée, adaptée au profil de risque spécifique d'une entreprise et à l'évolution du paysage des cybermenaces. Cette stratégie nécessite essentiellement une évaluation initiale pour identifier les ressources critiques et les vecteurs d'attaque probables, suivie de la mise en œuvre de protections de base telles que la limitation du débit et les pare-feux. Les étapes avancées requièrent la combinaison d'une détection basée sur les anomalies pour les nouvelles menaces, d'une détection basée sur les signatures pour les attaques connues et de mécanismes de défi-réponse pour filtrer les bots.

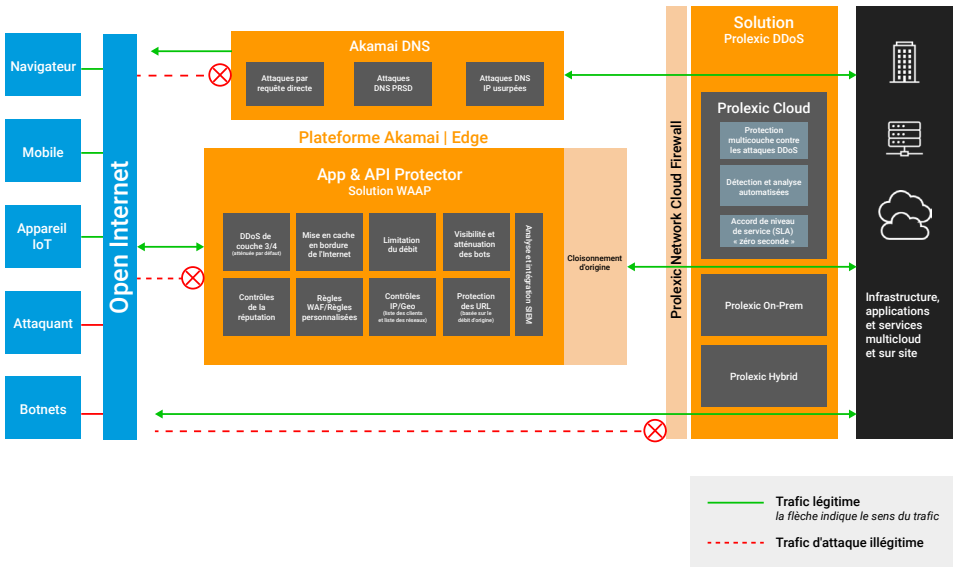
En intégrant des renseignements adaptatifs sur les menaces, tels que des algorithmes qui déterminent les modèles d'empreintes TLS des sources d'attaques DDoS connues et émergentes, le système de sécurité peut automatiquement adapter son atténuation pour bloquer ou contester le trafic présentant cette empreinte, atténuant ainsi efficacement l'attaque. Un plan complet de réponse aux incidents et de récupération est essentiel pour minimiser les dommages et maintenir la confiance pendant et après une attaque. Un apprentissage et des ajustements continus basés sur les attaques passées et les tendances émergentes maintiennent l'efficacité et la résilience de la stratégie de défense.

Les institutions financières offrent un parfait exemple de l'importance d'avoir une stratégie de défense équilibrée et multicouche pour faire face aux attaques DDoS sophistiquées. L'impact potentiel des temps d'arrêt sur leurs opérations et la confiance de leurs clients font de ces institutions des cibles privilégiées.

En intégrant une combinaison de méthodes de détection et d'atténuation telles que la détection des anomalies de trafic, en utilisant des méthodes conventionnelles telles que la limitation de débit, le filtrage IP/géographique, la réputation IP et la veille stratégique en temps réel sur les menaces, ainsi qu'un plan de réponse aux incidents robuste, elles peuvent protéger leurs ressources critiques contre les interruptions tout en assurant la continuité du service à leurs clients. Cette approche globale illustre la façon dont les entreprises peuvent se défendre contre la nature multiforme des attaques DDoS dans le paysage numérique actuel.

Préparation : stratégie de défense en profondeur avec l'architecture d'Akamai en bordure de l'Internet

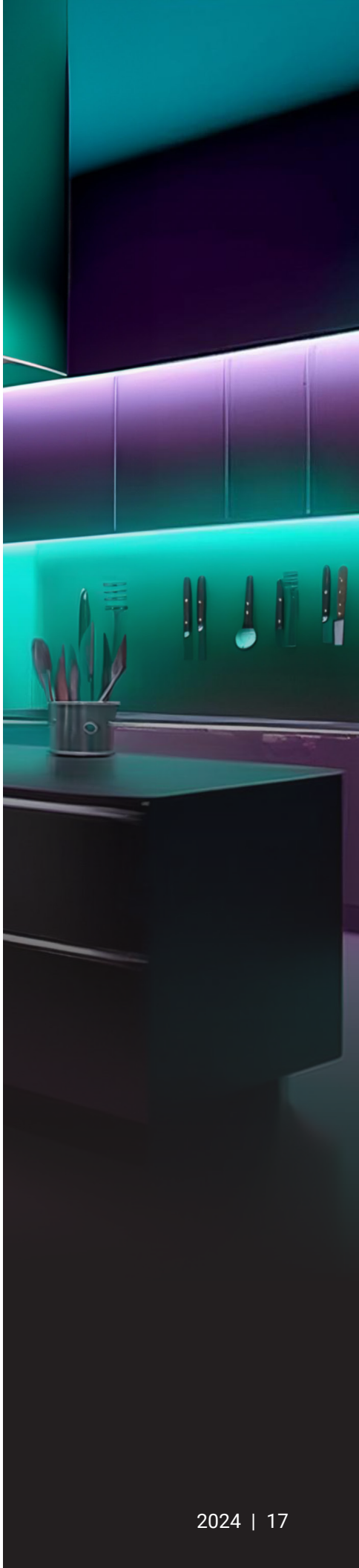
L'approche d'Akamai en matière de protection contre les attaques DDoS au niveau de la couche applicative est multicouche, complète et adaptative. Elle est conçue pour protéger les sites Web, les applications et les API contre les attaques les plus sophistiquées. Notre solution App & API Protector exploite plusieurs fonctionnalités clés qui fournissent une protection complète, combinant un pare-feu d'application Web, une visibilité et une atténuation des bots, la sécurité des API et des protections contre les attaques DDoS de couche 7 dans un seul produit pour offrir une protection étendue.



Architecture de référence pour une protection globale contre les attaques DDoS à l'aide des solutions Edge DNS, App & API Protector et Prolexic

La stratégie de protection contre les attaques DDoS d'Akamai repose sur une architecture de défense en bordure de l'Internet acheminant le trafic via la plateforme massivement distribuée d'Akamai, où chaque requête est inspectée en temps réel. Cette configuration protège contre les attaques DDoS, les attaques d'API et d'applications Web et les bots malveillants en bordure de l'Internet, les empêchant d'atteindre les applications ou l'infrastructure. Cela améliore la continuité de l'activité en maintenant une architecture rapide, hautement sécurisée, toujours disponible et qui évolue avec les attaques.

La suite robuste d'outils et d'ingrédients d'Akamai fournit des contrôles proactifs et réactifs, chacun ayant un objectif distinct dans la stratégie de défense globale.



Contrôles proactifs

Les contrôles proactifs aident à prévenir les attaques avant qu'elles ne se produisent, en se concentrant sur le renforcement de la posture de sécurité pour minimiser les vulnérabilités. Parmi eux :

- **Contrôles IP (bloquent les plages IP/CIDR et les ASN) :** faisant office de couche de défense fondamentale, ces contrôles bloquent les adresses IP malveillantes connues ou les plages identifiées par le biais des renseignements sur les menaces.

- **Contrôles géographiques (pour bloquer certaines zones géographiques) :** en autorisant ou en limitant le trafic provenant de régions spécifiques, les entreprises peuvent restreindre de manière préventive l'exposition aux attaques provenant de zones à haut risque.

- **Règles de pare-feu d'application Web (WAF) :** la mise en œuvre de règles contre les vulnérabilités et les vecteurs d'attaque connus, tels que les outils DDoS comme FiberFox, offre une première ligne de défense solide.

- **Contrôles de la réputation IP :** l'utilisation des renseignements par le biais d'heuristiques des ressources malveillantes connues des attaques DDoS, de l'extraction Web et d'autres activités malveillantes permet de bloquer ou d'examiner de manière préventive le trafic suspect.

- **Intelligence DDoS de la plateforme :** les informations stratégiques sur les attaques DDoS provenant de la plateforme Akamai en bordure de l'Internet distribuée dans le monde entier peuvent contribuer à la création d'une stratégie d'atténuation proactive pour lutter contre les attaques DDoS visant la couche applicative.

- **Mise en cache :** l'optimisation de la mise en cache du contenu permet de réduire considérablement la charge sur les serveurs d'origine, atténuant indirectement l'impact des attaques DDoS en traitant les requêtes provenant du cache en bordure de l'Internet.

- **Site Shield :** le masquage de l'origine en autorisant uniquement les requêtes à l'origine via le réseau d'Akamai en bordure de l'Internet permet de réduire davantage la charge des serveurs.

Contrôles réactifs

Les contrôles réactifs sont des réponses à une attaque détectée, visant à atténuer son impact et à maintenir la disponibilité du service.

- **Limitation du débit (règles de taux) :** ces contrôles sont cruciaux pour atténuer les pics de trafic soudains qui peuvent indiquer la présence d'une attaque DDoS. La configuration peut être effectuée et personnalisée en fonction des profils de trafic spécifiques au client. La limitation du débit constitue souvent la première ligne de défense pour protéger l'origine du client contre les attaques DDoS volumétriques et distribuées.

- **Protection Slow POST :** ciblant spécifiquement les attaques HTTP POST lentes, ce contrôle réagit aux schémas de trafic anormaux qui visent à épuiser les ressources du serveur.
- **Règles personnalisées dans le WAF :** vous devez pouvoir adapter rapidement les règles en réponse aux menaces émergentes, en offrant des mécanismes de défense flexibles et dynamiques.
- **Visibilité et atténuation des bots :** grâce à l'apprentissage automatique pour détecter l'usurpation d'identité du navigateur, vous pouvez identifier et bloquer des attaques DDoS sophistiquées qui proviennent de l'automatisation.
- **Protection des URL avec délestage de charge intelligent :** les contrôles qui limitent le nombre excessif de requêtes à l'origine et donnent la priorité aux utilisateurs légitimes par rapport au trafic malveillant peuvent vous aider à maintenir la disponibilité du service lors d'une attaque DDoS.
- **Intelligence DDoS de la plateforme :** le délestage de charge est une catégorie de protection des URL qui utilise les informations sur les attaques DDoS de la plateforme Akamai distribuée dans le monde entier et permet à nos clients de créer une stratégie d'atténuation proactive pour lutter contre les attaques DDoS visant la couche applicative.

Mélanger les ingrédients et atteindre l'équilibre avec votre recette

- **Exemple :** une grande entreprise de services financiers élabore une stratégie de défense approfondie avec la solution WAAP d'Akamai

Certaines entreprises peuvent être plus fréquemment la cible d'attaques DDoS. Par exemple, selon une étude d'Akamai, plus d'un tiers des attaques DDoS menées en 2023 ciblaient des institutions de services financiers. Victime d'une attaque ciblée sur sa page de connexion, une grande entreprise de services financiers, cliente d'Akamai, a pu suivre une recette éprouvée pour la défense. Vous pouvez faire de même.


Profil de l'attaquant : hacktiviste


Cible : point de terminaison de connexion


Méthode : HTTP POST flood


Sources d'attaque : environ 66 000 adresses IP et 140 pays

Recette

Atténuation d'une attaque HTTP POST flood

Ingrédients :

Contrôles proactifs :

- **Contrôles IP** : utilisez les renseignements sur les menaces pour bloquer des adresses IP ou des plages CIDR associées à des entités malveillantes connues.
- **Contrôles Geo** : utilisez des listes pour bloquer le trafic en provenance de zones géographiques connues pour abriter des groupes d'hacktivistes, telles que les régions associées à « Anonymous Sudan ».
- **Règles de pare-feu d'application Web (WAF)** : implémentez des règles spécifiquement conçues pour contrecarrer les outils et tactiques DDoS connus, y compris les modèles typiques de floods HTTP GET.
- **Contrôles de la réputation IP** : surveillez attentivement ou bloquez activement (en temps réel) le trafic provenant de sources dont les scores de réputation sont médiocres.
- **Intelligence DDoS de la plateforme** : appliquez les informations stratégiques issues des données d'attaque DDoS mondiales d'Akamai pour anticiper et contrer les vecteurs de menaces émergents.
- **Site Shield** : activez des listes de contrôle d'accès (ACL) de pare-feu pour autoriser uniquement le trafic provenant du réseau d'Akamai en bordure de l'Internet et bloquer le reste.

Contrôles réactifs :

- **Limitation du débit** : établissez des stratégies de taux pour atténuer les pics soudains de trafic, en définissant des seuils appropriés pour les requêtes par seconde vers la page d'accueil. Optimisez votre limitation de débit en (1) réduisant les fenêtres temporelles pour mesurer la vitesse des requêtes à une requête par seconde, et (2) en appliquant une limitation de débit basée sur la géographie et le score de réputation des sources IP connectées tout en autorisant la liste des sources telles que les adresses IP de l'entreprise et les partenaires de l'institution financière.
- **Règles personnalisées dans le WAF** : créez des règles sur mesure en réponse aux caractéristiques spécifiques d'une attaque une fois qu'elle est détectée. L'utilisation de contrôles d'échantillonnage de trafic dans vos règles personnalisées vous aidera dans l'analyse du trafic, afin d'examiner plus efficacement les principales sources d'attaque, tandis que l'utilisation de contrôles IP/géographiques dans des règles personnalisées peut contribuer à une atténuation rapide.
- **Visibilité et atténuation des bots** : utilisez la détection de l'usurpation d'identité des navigateurs pour identifier et bloquer les requêtes qui imitent le comportement légitime des utilisateurs mais font partie de la submersion.
- **Protection URL** : appliquez des contrôles pour limiter les taux de requêtes spécifiquement à l'URL de connexion, préservant ainsi la bande passante pour les utilisateurs légitimes. La configuration du délestage intelligent avec des catégories telles que les proxys, les nœuds de sortie Tor, les bots de base, les adresses IP de faible réputation, etc., aide à hiérarchiser le trafic utilisateur réel par rapport à ces sources potentiellement malveillantes.

Méthode de préparation :

Phase de révision :

- **Revoir la configuration** : effectuez un examen approfondi de votre posture de sécurité actuelle. Configurez vos contrôles proactifs en fonction de vos conclusions, en vous assurant que tous les contrôles géographiques et IP pertinents sont correctement gérés.
- **Optimiser la configuration** : ajustez la configuration pour reconnaître et atténuer les schémas de trafic inhabituels, y compris ceux caractéristiques des attaques HTTP POST flood.

Phase de détection et d'atténuation :

- **Surveillance et alerte** : l'architecture de défense en bordure de l'Internet d'Akamai permet de surveiller le trafic entrant à la recherche de modèles susceptibles d'indiquer une attaque DDoS. Vous pouvez configurer des alertes en cas de pics de trafic anormaux ou de modèles correspondant aux méthodes DDoS connues, telles que HTTP POST flood.
- **Détection et prévention** : divers contrôles proactifs tels que la réputation IP, la mise en cache et les contrôles IP/géographiques fournissent automatiquement des capacités de détection et d'atténuation s'ils sont correctement configurés. Une fois qu'une attaque est détectée, des contrôles tels que la limitation du débit, la protection des URL et la détection des usurpateurs de navigateur s'activent automatiquement sans aucune intervention de l'utilisateur.
- **Analyse et adaptation** : analysez en permanence les schémas d'attaque et adaptez vos mesures défensives en temps réel pour contrecarrer l'évolution des tactiques. Vous pouvez, par exemple, créer des règles personnalisées ou des stratégies de limitation du débit personnalisées basées sur une analyse récente du trafic d'attaque.

Récupération et analyse post-attaque :

- **Analyse des journaux** : après une attaque, effectuez une analyse détaillée des journaux de trafic pour identifier les vecteurs d'attaque et l'efficacité des contrôles déployés.
- **Ajustements** : apportez les ajustements nécessaires aux contrôles proactifs et réactifs en vous basant sur les enseignements tirés de l'analyse de l'attaque.

Suggestions de service :

- Révisez et mettez à jour régulièrement votre stratégie de défense pour vous adapter à l'évolution des tactiques DDoS. Ces examens peuvent varier considérablement d'une entreprise à l'autre, en fonction de leurs besoins spécifiques, de leur exposition aux menaces et des meilleures pratiques du secteur. Une entreprise de services financiers peut avoir besoin de revues trimestrielles, tandis qu'une plateforme de commerce électronique ciblera des évaluations semestrielles pour se préparer aux pics d'achats saisonniers.
- Mettez en place une formation continue afin que l'équipe de sécurité reconnaisse et réagisse aux nouveaux vecteurs d'attaque DDoS.
- Effectuez des simulations d'attaques pour tester l'efficacité des mesures déployées et établir l'état de préparation de l'équipe en cas d'incidents réels.

Récupération et analyse post-attaque

Dans le cadre de la lutte contre les attaques DDoS au niveau de la couche applicative (couche 7), la phase post-attaque est cruciale pour renforcer les défenses futures et comprendre votre adversaire. Cela implique deux étapes critiques : analyser le modèle d'attaque et améliorer vos défenses en fonction de votre analyse. Ces étapes sont essentielles pour élaborer une stratégie de défense résiliente et assurer la continuité et l'intégrité des services en ligne.

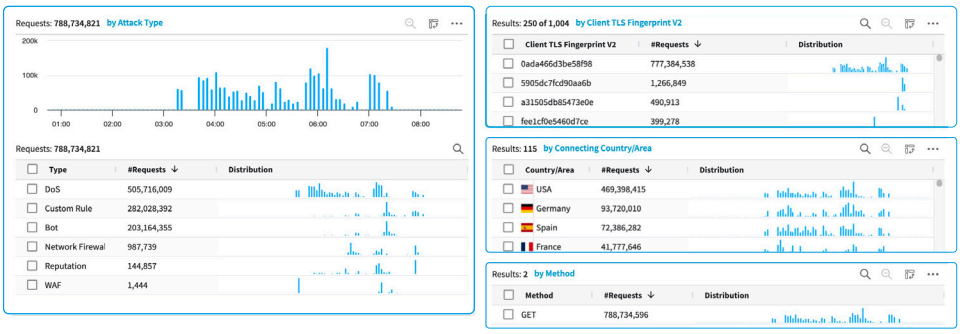
Analyse du trafic et du modèle d'attaque

Après avoir géré une attaque, l'étape suivante consiste à analyser l'incident pour comprendre quelle stratégie a fonctionné et laquelle n'a pas fonctionné comme prévu. Cette évaluation englobe des facteurs à plus long terme tels que l'impact sur la confiance des clients, l'intégrité des données et les potentielles pertes financières. Les systèmes complets d'analyse de la sécurité, tels qu'Akamai Web Security Analytics, sont des outils indispensables lors de cette phase, car ils permettent aux entreprises de comprendre le trafic lié à une attaque et son impact.

L'analyse implique notamment de disséquer les tactiques, techniques et procédures (TTP) utilisées par les attaquants. Les principales questions à aborder sont les suivantes :

- Quelle était la nature du pic de trafic ?
- Des fonctionnalités d'application spécifiques ont-elles été ciblées ?
- L'attaque a-t-elle exploité des vulnérabilités connues ?

Akamai Web Security Analytics identifie les anomalies dans les schémas de trafic, localise l'origine géographique de l'attaque et détermine le type d'attaque en fonction des comportements observés. L'exemple suivant montre certaines des caractéristiques ou dimensions du trafic peuvent être appliquées pour enquêter sur une attaque DDoS.



Les images présentées proviennent de Web Security Analytics, qui offre une visibilité sans précédent et une analyse proactive des événements de sécurité

Revoir et mettre à jour les stratégies de défense en fonction de votre analyse d'attaque

L'examen et la mise à jour des stratégies de défense basées sur l'analyse des attaques sont un élément essentiel du renforcement de la posture de cybersécurité d'une entreprise. En examinant les spécificités d'une attaque passée, les entreprises peuvent identifier les vulnérabilités de leurs défenses actuelles et procéder à des ajustements éclairés. Voici quelques exemples de la manière dont ce processus peut être appliqué à l'aide d'Akamai Web Security Analytics.

Exemple 1 : mise à jour des règles WAF en fonction des modèles d'attaque

Scénario : une entreprise subit une attaque DDoS de couche 7 ciblant son application Web avec un barrage de requêtes malveillantes vers la page d'accueil de l'application.

Évaluation : l'analyse de l'attaque révèle que les règles de pare-feu d'application Web (WAF) existantes ont détecté et bloqué de manière adéquate plus de 90 % du trafic d'attaque, mais que les 10 % restants se sont infiltrés, car il existait une liste d'autorisation géographique explicite qui a permis aux sources d'attaque de cette zone géographique de submerger l'application.

Mise à jour : sur la base de cette analyse, l'organisation a mis à jour ses configurations WAF pour utiliser une règle WAF personnalisée correspondant à des caractéristiques spécifiques du trafic d'attaque de cette zone géographique particulière. Les remplacements peuvent continuer à autoriser la zone géographique tout en bloquant les attributs spécifiques du trafic d'attaque. En outre, les paramètres de limitation du débit pour cette zone géographique particulière ont été rendus plus stricts.

Exemple 2 : renforcement de la protection de l'origine

Scénario : le processus de connexion d'un site Web de vente au détail est frappé par une attaque DDoS de couche 7 hautement distribuée et sophistiquée, exploitant des bots automatisés.

Évaluation : l'analyse post-attaque indique un trafic d'attaque hautement distribué en provenance de plus de 150 pays et des centaines d'empreintes TLS qui ressemblent à des navigateurs légitimes. Une bonne partie du trafic provenait de fournisseurs de cloud, dont certains étaient autorisés comme sources partenaires de confiance. Bien que l'attaque ait été efficacement atténuée, l'analyse a révélé la nécessité de mesures de défense supplémentaires.

Mise à jour : pour protéger les URL à forte intensité de calcul, comme un processus de paiement, cette organisation a mis en œuvre la protection des URL, une fonctionnalité spécialement conçue pour protéger les URL à forte intensité de calcul et les points de terminaison API contre les attaques DDoS hautement distribuées au niveau de la couche applicative. Un architecte de sécurité a également activé le délestage intelligent des charges pour les bots, les proxys, la réputation IP, etc. Cette sous-fonctionnalité de protection des URL permet de hiérarchiser le trafic utilisateur réel en refusant dans un premier temps les requêtes provenant de sources potentiellement malveillantes.

L'entreprise a également décidé d'activer la fonctionnalité intégrée de protection contre les bots dans le pare-feu d'application web (WAF), qui n'avait pas été prise en compte précédemment en raison de la présence d'une solution de bots sur site, cette dernière n'étant pas parvenu à monter en puissance lors de cette attaque à grande vitesse.

Exemple 3 : mise en place d'une limitation du débit pour les points de terminaison API

Scénario : un point de terminaison API d'une application de services financiers est submergé par un flot de demandes de transaction frauduleuses, indiquant la présence d'une attaque DDoS de couche 7 visant à épuiser les ressources du serveur.

Évaluation : l'analyse du modèle d'attaque montre que les attaquants ciblaient spécifiquement des points de terminaison API moins protégés et incapables de traiter un volume élevé de requêtes.

Mise à jour : en réponse, l'entreprise a mis en place une limitation stricte du débit sur tous les points de terminaison API, en particulier ceux identifiés comme vulnérables. Elle a également adopté un module complémentaire dédié à la sécurité des API qui fournit des couches avancées pour la sécurité des API, y compris l'exploitation de la logique des API, la menace des API fantômes et la surveillance de la vulnérabilité des API.

Points stratégiques

- **Surveillance et journalisation continues :** établissez des systèmes de surveillance et de journalisation robustes pour détecter rapidement les anomalies et évaluer avec précision les dommages pendant et après une attaque.
- **Gestion des failles de sécurité :** mettez régulièrement à jour et corrigez les systèmes pour atténuer les vulnérabilités connues, réduisant ainsi le risque d'exploitation.
- **Analyse des modèles d'attaque :** utilisez des outils de visibilité appropriés pour une analyse approfondie des schémas d'attaque afin de comprendre les méthodologies et les intentions des attaquants.

Analyse post-attaque

L'évaluation des dégâts et l'analyse du schéma d'attaque sont des éléments essentiels d'une stratégie de défense DDoS de couche 7 robuste. Ces étapes aident non seulement à comprendre et à atténuer les impacts immédiats d'une attaque, mais aussi à améliorer continuellement les mécanismes de défense, assurant ainsi une meilleure préparation aux menaces futures.

Maintenir et mettre à jour vos recettes

Le maintien d'une défense forte contre les attaques DDoS de couche 7 exige une surveillance constante des dernières tendances et techniques.

Les attaquants combinent systématiquement les schémas d'attaque, en exploitant de nouveaux outils et de nouvelles vulnérabilités. Pour contrer ces menaces de manière proactive, les entreprises doivent investir du temps et des efforts dans la recherche, la surveillance, l'évaluation des défenses, l'automatisation des protections et la collaboration avec la communauté de renseignements sur les menaces.

Surveiller les principaux forums de cybersécurité est un bon point de départ, mais ne suffit pas. Nous suggérons une approche plus prescriptive :

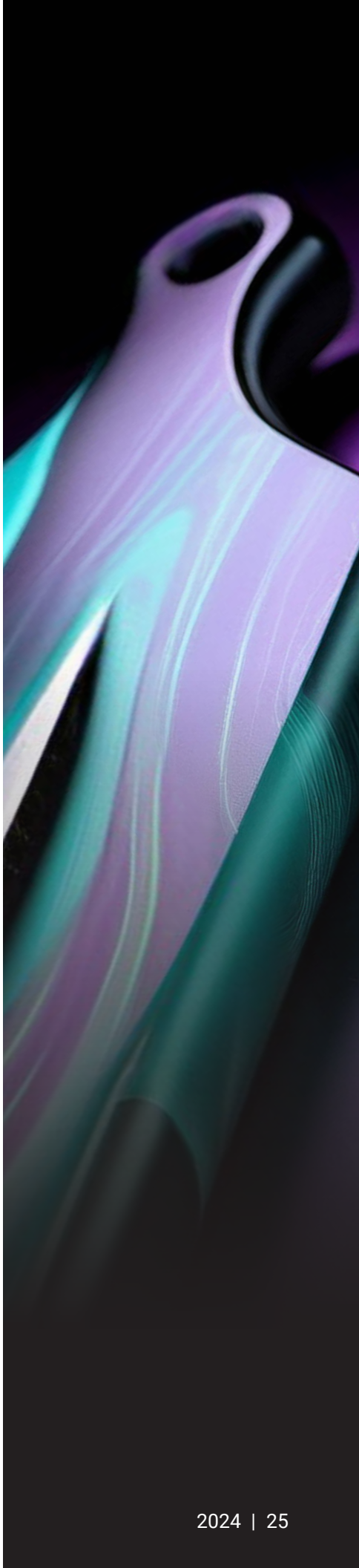
Surveiller et évaluer en permanence : surveillez régulièrement les performances de votre réseau et de vos applications pour détecter de nouveaux schémas ou de nouvelles anomalies qui indiquent des menaces émergentes. Utilisez ces données pour évaluer l'efficacité de vos mécanismes de défense existants, en identifiant les domaines à améliorer ou à ajuster.

Former une équipe anti-DDoS : désignez un interlocuteur ou une équipe au sein de l'entreprise qui effectuera des recherches et surveillera le paysage des attaques DDoS, et rendra compte à l'ensemble de l'entreprise au moins une fois par trimestre de ses conclusions et recommandations clés.

Dialoguer avec la communauté des renseignements sur les menaces : les attaquants communiquent entre eux sur les méthodes les plus récentes et les plus efficaces. Il n'y a aucune raison de ne pas communiquer avec des collègues d'autres entreprises et secteurs au sujet des meilleures défenses. Tenez-vous au courant des dernières informations sur les menaces. Abonnez-vous à des flux de sécurité, participez à des forums sur la cybersécurité et collaborez avec des pairs de votre secteur. Les informations recueillies vous aideront à anticiper les nouveaux vecteurs d'attaque et à ajuster vos défenses en conséquence.

S'appuyer sur votre fournisseur de cybersécurité : les fournisseurs de technologies ont souvent des groupes de recherche dédiés aux menaces, et ceux qui disposent d'un réseau de diffusion de contenu pourront vous communiquer des informations qui ne sont pas disponibles ailleurs. Profitez de ces opportunités d'apprentissage quand et où vous le pouvez. Il est également judicieux de faire appel périodiquement à des experts-conseils en sécurité.

Tester vos propres défenses : qui ne prépare pas sa réussite, prépare son échec, on se perfectionne par la pratique… Quelle que soit votre maxime, le message est le même : effectuer des tests et des exercices réguliers paye.



Réalisez des revues périodiques et des scénarios d'attaque simulés (exercices en équipe rouge) pour tester la résilience de vos stratégies de défense. Ces exercices peuvent révéler des faiblesses dans votre configuration actuelle et fournir des informations sur la façon dont les attaquants pourraient exploiter votre système.

Testez votre réseau au moins une fois par an. Les profils d'attaque récents peuvent également être une bonne référence pour un cas de test, en particulier les profils d'attaques ayant ciblé une entreprise de votre secteur.

Partagez vos apprentissages avec la communauté. Il est utile de répéter ce qui suit : tout comme les attaquants partagent leurs outils et leurs tactiques, les entreprises devraient partager leurs connaissances sur les stratégies de défense réussies.

En documentant à la fois les réussites et les échecs, les professionnels de la cybersécurité peuvent fournir des informations concrètes qui enrichissent la base de connaissances collective. Participer à des forums du secteur, mentorer les personnes moins expérimentées et participer à des projets collaboratifs est essentiel pour favoriser un écosystème de défense robuste. Ces efforts contribuent non seulement à l'élaboration de stratégies et d'outils plus efficaces, mais permettent également de disposer d'un ensemble diversifié d'expériences et de connaissances capables de s'adapter aux tactiques changeantes des acteurs malveillants. Cet esprit de collaboration est vital pour rester bien préparés dans le paysage de la cybersécurité, rendant chaque contribution précieuse pour construire un monde numérique plus fort et plus résilient.

Points à retenir

Le paysage des menaces DDoS est dynamique, les attaquants recherchant constamment de nouveaux moyens de contourner les défenses. Le processus de maintenance et de mise à jour de vos stratégies de protection contre les attaques DDoS de couche 7 est un processus continu qui exige vigilance, adaptabilité et approche proactive. En restant informés, en procédant régulièrement à des tests et à des examens et en favorisant une culture d'amélioration continue, vous pouvez maintenir une solide défense contre les menaces présentes et futures.

Conclusion

Il est clair que les attaques DDoS de couche 7 sont non seulement devenues plus sophistiquées, mais aussi plus faciles à lancer grâce aux avancées de l'automatisation et à la coordination accrue des attaquants. Dans le même temps, les entreprises doivent défendre un paysage plus vaste et plus complexe tandis que les coûts des défaillances augmentent.

Concocter une recette de défense n'est pas une tâche facile. Aucune méthode unique n'est parfaite pour contrer les attaques DDoS de couche 7. Comme nous l'avons démontré, une approche multidimensionnelle, combinant plusieurs stratégies de détection et d'atténuation, fournit la défense la plus robuste.

De plus, le choix des méthodes doit être guidé par les besoins spécifiques, les modèles de trafic et le profil de risque de l'application ou du service protégé. L'élaboration d'une défense efficace nécessite une bonne compréhension de l'entreprise, du trafic et de ses vulnérabilités. Des mises à jour et des ajustements réguliers des stratégies adoptées sont essentiels pour s'adapter à l'évolution du paysage des menaces DDoS.

Enfin, il est également devenu clair que votre travail n'est pas terminé lorsqu'une attaque se termine. L'analyse et les ajustements post-attaque sont indispensables à la réussite continue et peuvent favoriser le partage des connaissances. Ils peuvent également contribuer au développement d'une carrière.

Heureusement, Akamai est là pour vous aider à chaque étape du processus. Akamai offre aux entreprises la possibilité de se procurer toutes les protections contre les attaques DDoS de couche 7 dont elles ont besoin auprès d'un seul fournisseur, de la protection des applications et des API à des renseignements sur le trafic mondial d'une richesse inégalée, en passant par une analyse post-attaque experte.

Découvrez les protections contre les attaques DDoS de couche 7 d'Akamai au travail. Testez une version d'évaluation gratuite d'App & API Protector.

Akamai

Crédits

Édition et rédaction

Aseem Ahmed
Barney Beal

Révision et expertise

Abdeslam Bella
Sean Flynn
Alex Marks-Bluth
Nitesh Shrivastava
Prathmesh Verma
Dennis Birchard
Ryan Gao
Pawan Sajnani
Patrick Sullivan
Danielle Walter

Marketing et publication

Georgina Morales Hampe
Shivangi Sahu

Akamai

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 d'Akamai, rendez-vous sur akamai.com et akamai.com/blog, ou abonnez-vous à Akamai Technologies sur X (anciennement Twitter) et LinkedIn. Publication : 10/24.