SOTI

10 YEARS
OF SECURITY INSIGHT

V 10 NUMÉRO 02

Comment lutter

contre la hausse des menaces DDoS dans la région EMEA

Akamai

État des lieux d'Internet/Sécurité

Table des matières

Les attaques DDoS sont de plus en plus fréquentes dans la région EMEA

Les attaques par déni de service distribué (DDoS) augmentent en volume dans le monde entier et se perfectionnent. Cette augmentation est particulièrement visible en Europe, au Moyen-Orient et en Afrique (EMEA), où les chercheurs d'Akamai ont observé une hausse spectaculaire du taux de croissance des attaques DDoS. En effet, le taux d'attaques DDoS augmente encore plus rapidement dans cette région que dans le reste du monde. Les attaques DDoS affectent les cibles en envoyant un trafic malveillant indésirable et entravent le fonctionnement des réseaux et des sites web dans la région EMEA.

Nous pensons que ce changement dans la région est dû en grande partie aux tensions géopolitiques, notamment aux activités des États-nations et à l'hacktivisme dans le cadre des conflits en cours, notamment entre la Russie et l'Ukraine et entre Israël et le Hamas. En outre, les événements à haute visibilité et les élections en Europe sont susceptibles d'accroître encore le risque d'attaques DDoS. Si l'ampleur des attaques DDoS dans la région EMEA est considérable et ne cesse de croître, nous avons également constaté une augmentation du nombre de vecteurs d'attaques DDoS utilisés par les cybercriminels et de la durée de ces attaques.

Dans ce rapport État des lieux d'Internet (SOTI), nous étudions la nature et la fréquence des attaques DDoS dans la région EMEA et examinons certains des principaux segments de marché touchés par ces attaques, notamment les services financiers, le commerce et la santé. Nous nous intéressons également de plus près à la nouvelle législation de la région EMEA visant à renforcer la protection contre les menaces de cybersécurité en hausse dans la région, et proposons des techniques d'atténuation et de sauvegarde pour lutter contre celles-ci.

Principales conclusions du rapport

Les chercheurs d'Akamai ont observé que le nombre d'attaques DDoS dans la région EMEA n'a cessé d'augmenter, avec des pics plus élevés, depuis le début de l'année 2019.

Plus d'un tiers des attaques DDoS dans le monde se produisent dans cette région.

La complexité et la gravité des attaques DDoS s'y sont accrues pour des motifs géopolitiques, tels que l'hacktivisme, avec des conséquences potentiellement mortelles.

Parmi tous les types d'attaques DDoS, les attaques DDoS DNS sont les plus répandues, selon une étude d'Akamai. Plus précisément, nous avons observé que le vecteur NXDOMAIN (domaine inexistant), également appelé vecteur Pseudo-Random Subdomain, inondait les serveurs de noms DNS de requêtes pour des domaines inexistants.

Plus d'un tiers des événements DDoS ont utilisé plusieurs vecteurs d'attaque (jusqu'à 12) pour accroître leur efficacité.

Dans la région EMEA, les services financiers sont le segment de marché qui connaît le plus grand nombre d'attaques de couche 3 et 4, tandis que le commerce est le secteur qui subit le plus grand nombre d'attaques de couche 7.

Les gouvernements et les nations de la région EMEA ont repensé le pouvoir de l'infosécurité en adoptant de nouvelles mesures législatives, telles que les directives NIS2 et DORA, afin d'influencer positivement les stratégies informatiques et de cybersécurité, notamment en améliorant la résilience et la protection contre les attaques DDoS.

Les attaques DDoS, hier et aujourd'hui

Les attaques DDoS, qu'elles soient le fait d'individus ou de réseaux de botnets, inondent les serveurs de requêtes et les submergent de trafic, ce qui rend les services et les sites hébergés indisponibles pour les utilisateurs et les visiteurs.

Les attaques DDoS ont bien évolué depuis l'époque où les acteurs malveillants utilisaient des outils open source. Leurs motivations étaient souvent simples : une insatisfaction concernant la dernière fonctionnalité d'un jeu, l'espoir d'obtenir un avantage compétitif ou parfois le simple amusement. En général, ce groupe d'acteurs malveillants ne dominait pas le paysage des attaques en ciblant les infrastructures critiques ou les hôpitaux, ni en cherchant à endommager gravement les réseaux ou à mettre des vies humaines en danger.

L'hacktivisme a radicalement changé le paysage, tant en termes d'identités des acteurs malveillants que de motivations. Si certaines attaques d'hacktivistes n'ont qu'un impact limité ou ne produisent que de simples nuisances, d'autres visent l'industrie commerciale pour obtenir un gain financier important et peuvent entraîner des interruptions de service qui durent plusieurs jours. Les attaques peuvent avoir des conséquences potentiellement mortelles, comme on le voit dans certaines attaques de centres de soins.

Ces dernières années, il est devenu bien plus simple de lancer des attaques DDoS avec l'émergence de services tels que les booters DDoS, qui permettent aux adversaires même les plus inhabiles de lancer une attaque pour une somme symbolique, parfois de l'ordre de 10 €, en cliquant simplement sur un bouton. Ces attaques simples génèrent un trafic intense, qui met hors ligne des sites Web et des réseaux entiers, nuit aux entreprises tant sur le plan financier qu'opérationnel et prive les clients et les utilisateurs de services essentiels.

Zoom sur la géopolitique

Le DDoS est un outil populaire pour les hacktivistes à motivations politiques et les attaquants financés par des États-nations. Par exemple, dans la cyberguerre en cours entre les acteurs ukrainiens et russes, les incidents DDoS ont joué un rôle important, car les hacktivistes ont constaté l'efficacité de ces attaques peu coûteuses.

Début 2022, Akamai a commencé à soutenir le gouvernement ukrainien dans sa lutte contre la cyberguerre en défendant 20 ressources Web de diverses entités gouvernementales. Parmi elles, citons notamment le site Internet president.gov.ua, le plus attaqué, qui a subi un grand nombre d'attaques DDoS, avec un pic d'un million de requêtes malveillantes par seconde.

Des hacktivistes comme Anonymous Sudan, NoName057(16) et Killnet font les gros titres depuis que la Russie a envahi l'Ukraine en février 2022. Killnet a été le premier de ces groupes à émerger, et a commencé ses activités vers octobre 2021 en offrant des services de location DDoS. Killnet a attaqué des organismes gouvernementaux, le secteur de la santé, des sociétés de médias et d'autres entités considérées comme des alliés de l'Ukraine.

NoName057(16) est considéré par de nombreux chercheurs comme un soutien de la Russie et privilégie l'utilisation d'attaques DDoS basées sur HTTP (couche 7). Au début de l'année 2023, le groupe pro-russe Anonymous Sudan a commencé à lancer des attaques DDoS contre des entités au Danemark, en Suède, aux États-Unis et dans d'autres pays. En juin 2023, de nombreux groupes d'acteurs malveillants, dont ReVIL, Killnet et Anonymous Sudan, ont tourné leur attention vers les infrastructures bancaires critiques, profitant du chaos provoqué par la guerre entre la Russie et l'Ukraine.

Plus récemment, Anonymous Sudan a revendiqué l'attaque de l'application de messagerie Telegram en France dans le cadre d'une attaque DDoS sans précédent contre le réseau interministériel de l'État, qui a perturbé plus de 17 000 adresses IP et terminaux et plus de 300 domaines. Cette attaque contre les sites Web et les services du gouvernement français répondait probablement à l'annonce du président Emmanuel Macron, le 26 février 2024, de l'envoi potentiel de troupes françaises en Ukraine.

Le conflit entre l'Ukraine et la Russie n'est pas la seule bataille qui provoque une vague d'attaques DDoS dans la région EMEA. La guerre entre Israël et le Hamas a également entraîné une augmentation des attaques. Anonymous Sudan a revendiqué des attaques DDoS contre le Mossad, l'agence nationale de renseignement israélienne, ainsi que contre le site web et les comptes Facebook du Premier ministre israélien et contre des sites pro-israéliens liés à l'escalade du conflit dans la mer Rouge. NoName057(16) a également attaqué des sites web israéliens en réponse à ce conflit.

Triple extorsion

À l'origine, les attaques par ransomware chiffraient les données de la victime, les rendant inutilisables à moins qu'une rançon ne soit payée. Puis sont apparues les attaques à double extorsion, plus préjudiciables pour les victimes, lors desquelles les criminels copient les données des victimes avant de crypter leur réseau, et menaçent de les publier ou de les vendre si elles ne payent pas la rançon. Un troisième type d'attaque, la triple extorsion, a fait son apparition peu après. Dans ces attaques, l'auteur de la menace utilise le DDoS pour entraver les activités de la victime en plus des deux autres tactiques. Ces triples extorsions sont souvent appelées Ransom DDoS, ou RDDoS.

Le DDoS est couramment utilisé dans les attaques d'extorsion, soit comme écran de fumée pour distraire les équipes d'infosécurité pendant que les pirates tentent de s'introduire dans les systèmes, soit pour augmenter la pression sur la victime. L'utilisation de plusieurs vecteurs d'attaque augmente les chances qu'une victime paie la rançon exigée. L'une des premières attaques à triple extorsion connues a eu lieu dans une clinique de psychothérapie finlandaise, Vastaamo, en octobre 2020, alors que l'Europe s'efforçait de trouver des moyens de mieux partager les données de santé dans l'ensemble de l'Union européenne.

Le secteur de la santé reste une cible privilégiée des acteurs de la menace qui recourent à des attaques à triple extorsion. C'est notamment le cas du groupe de ransomwares NoEscape, qui a émergé l'année dernière de l'ancien groupe russophone Avaddon et cible les organismes de santé. Et certaines entreprises de cybersécurité se préparent déjà à ce que davantage de groupes ciblent le secteur de la santé à l'avenir.

En outre, le groupe de ransomwares basé en Russie LockBit aurait dirigé l'opération de ransomware la plus importante et la plus destructrice au monde en février 2024, déclenchant des dégâts qui se chiffrent en milliards d'euros. Europol et Eurojust se sont associés pour coordonner un groupe de travail international appelé Opération Cronos afin de démanteler LockBit. L'Opération Cronos a donné lieu à des arrestations, des mandats, des mises en examen et à la confiscation de 34 serveurs dans la région EMEA, en Australie et aux États-Unis. LockBit était connu pour avoir testé de nouvelles méthodes pour faire pression sur les victimes et les amener à payer des rançons, telles que les RDDoS.

Bien qu'il existe d'autres groupes bien connus utilisant RDDoS tels que Darkside, Lazarus, AvosLocker et BlackCat, l'impact de l'Opération Cronos contre LockBit est significatif, car c'est la première fois que l'application de la loi informatique démontre une telle efficacité. Cette campagne d'une ampleur inédite a entraîné le démantèlement et la prise de contrôle complète de l'infrastructure d'un grand groupe de ransomwares alors qu'il était encore opérationnel.

Actions cyberoffensives : lancer des attaques DDoS pour contrer les attaques DDoS

L'idée de mener des actions de piratage contre les cybercriminels fait l'objet de débats depuis des années. Certains considèrent cette stratégie comme un moyen de défense efficace (« la meilleure défense, c'est l'attaque »), dans le sens où elle peut protéger les entreprises contre les menaces internationales. D'autres pensent qu'elle créerait un dangereux précédent en autorisant les entreprises de cybersécurité à lancer des attaques DDoS dans le monde entier, ce qui pourrait déstabiliser les relations entre les États et intensifier les tensions diplomatiques. En outre, les ambiguïtés réglementaires concernant les contre-attaques, telles que les attaques DDoS, soulèvent des questions juridiques très complexes.

Comme nous le savons, LockBit a utilisé des attaques DDoS dans le cadre de ses triples extorsions. Paradoxalement, l'utilisation de cette méthode a été en partie influencée par une attaque DDoS que le groupe a subi lui-même. La société de cybersécurité Entrust a été ajoutée à la liste des victimes de LockBit en juillet 2022. En réponse, Entrust a lancé une contre-attaque DDoS qui a efficacement paralysé les systèmes Darknet que LockBit utilisait pour publier des données volées.

Les contre-attaques sont également utilisées comme tactique de guerre par certains États-nations. L'Ukraine a recruté des volontaires pour intégrer une « armée informatique » composée de pirates informatiques du monde entier qui tentent de défendre les réseaux contre les hackeurs en les piratant à leur tour. Cette initiative est considérée comme la première du genre.

Examen des données d'attaques DDoS dans la région EMEA

Les attaques DDoS sont en hausse dans le monde entier, et particulièrement dans la région EMEA. Les chercheurs d'Akamai ont analysé les données DDoS régionales et constatent que le nombre d'attaques DDoS dans la région EMEA augmente plus régulièrement que dans l'ensemble des autres régions, y compris l'Amérique du Nord, qui occupe la première place (figures 1a et 1b).

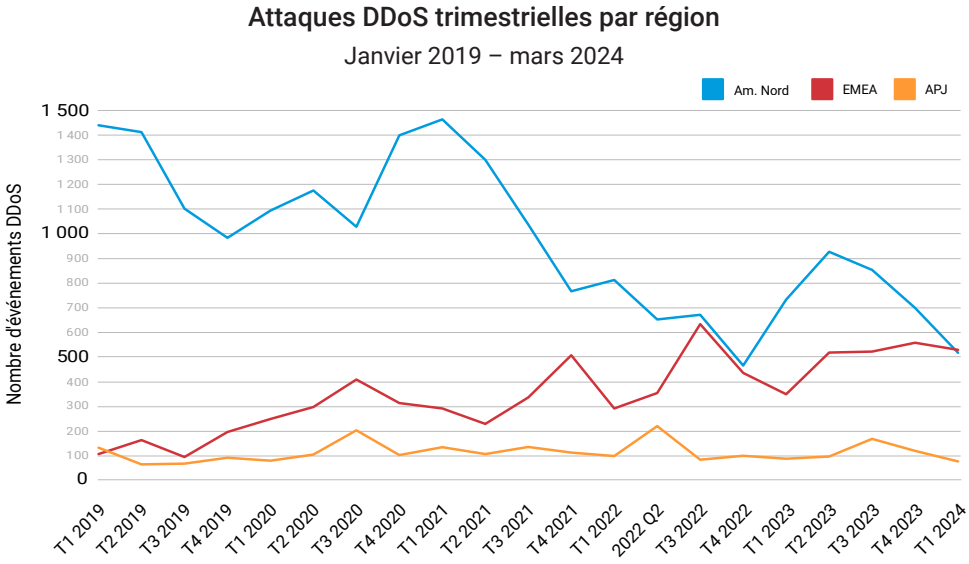

Fig. 1a : Le nombre d'attaques DDoS dans la région EMEA augmente plus régulièrement que dans toute autre région, y compris en Amérique du Nord

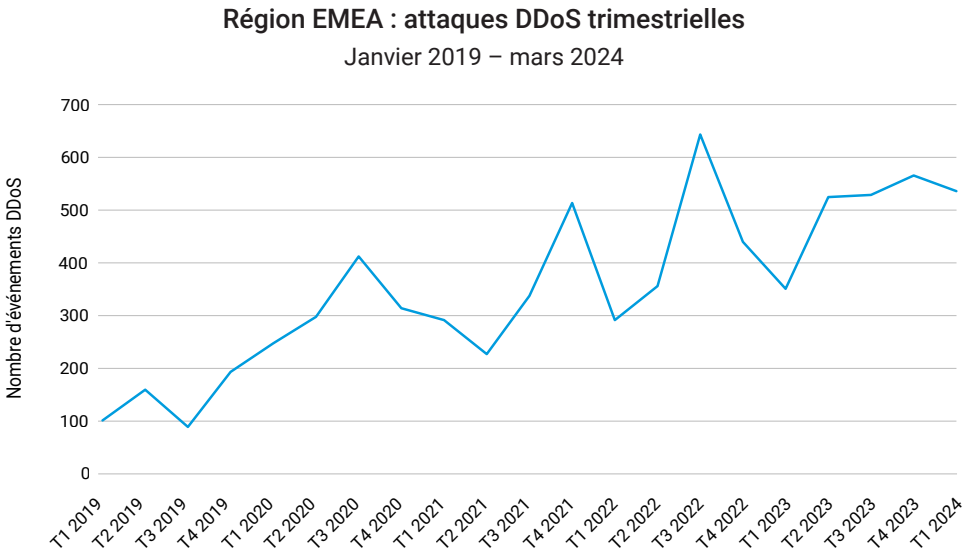

Fig. 1b : Croissance des attaques DDoS dans la région EMEA

Dans la région EMEA, le Royaume-Uni (26 %), l'Arabie saoudite (22,3 %) et l'Allemagne (9,1 %) sont en tête des pays ayant subi le plus grand nombre d'attaques. Les conclusions d'Akamai montrent également que plus d'un tiers de toutes les attaques DDoS au niveau mondial se produisent dans la région EMEA (figure 2).

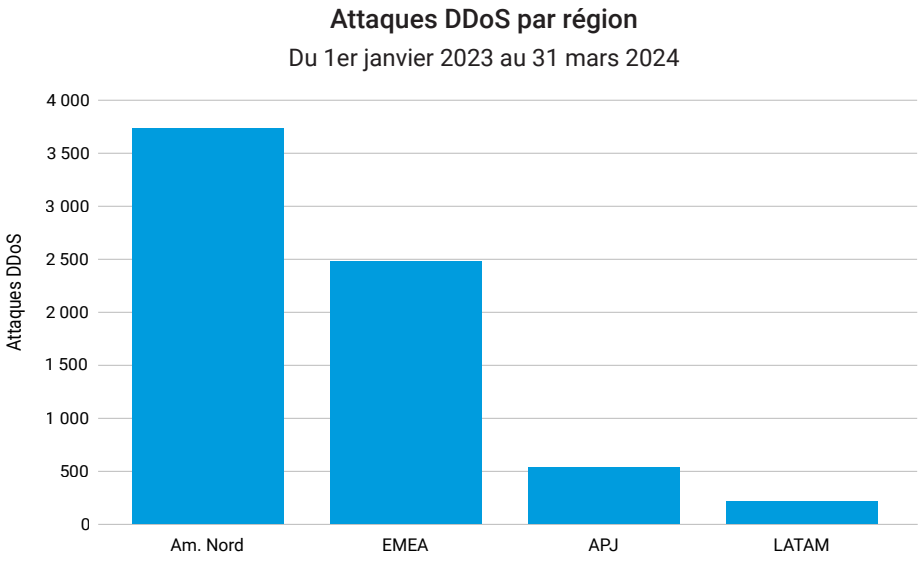

Figure 2 : Le nombre d'attaques DDoS dans la région EMEA a grimpé à près de 2 500 entre le début de l'année 2023 et le premier trimestre 2024, soit plus de trois fois plus que dans les régions Asie-Pacifique/Japon (APJ) et Amérique latine (LATAM) réunies

Dans le secteur des services financiers, la région EMEA est celle qui enregistre le plus grand nombre d'attaques DDoS de couche 3 et 4 (figure 3). Comme nous l'avons déjà mentionné, des groupes d'hacktivistes russes ont déclaré leur intention de lancer des attaques DDoS sur le système bancaire européen, et nous supposons que la principale raison de l'augmentation du nombre d'attaques DDoS dans le secteur des services financiers est lié à l'hacktivisme géopolitique.

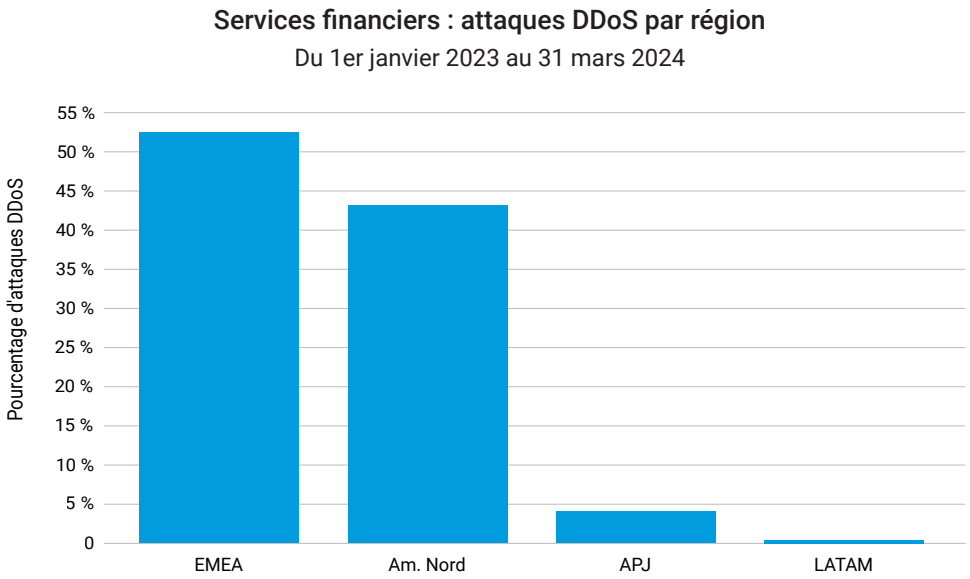

Figure 3 : La région EMEA a enregistré 52,5 % du trafic régional d'attaques DDoS de couche 3 et 4 dans le secteur des services financiers.

Outre les attaques de couche 3 et 4, les applications de services financiers sont également victimes d'attaques DDoS de couche 7. Cependant, c'est dans le secteur du commerce que l'on observe la plus forte augmentation du nombre d'attaques DDoS de couche 7 dans la région EMEA, avec près de 30 % de l'ensemble des attaques dans la région (figure 4).

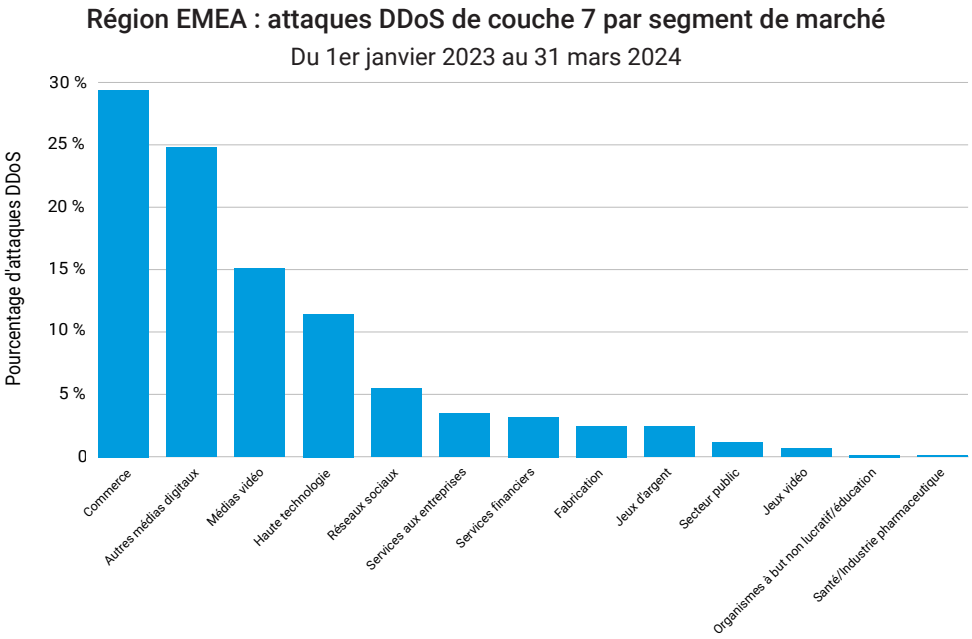

Figure 4 : Le secteur du commerce représente 29,4 % du trafic régional d'attaques DDoS de couche 7 dans la région EMEA.

Les attaques DDoS ciblant la couche applicative, telles que les inondations HTTP Flood, sont peut-être plus répandues dans le secteur du commerce, car elles représentent aux yeux des pirates une opportunité de lourdement perturber le chiffre d'affaires. Ces attaques sont particulièrement handicapantes pour les entreprises commerciales, car elles peuvent rendre une boutique en ligne inaccessible ou un système de réservation indisponible, entraînant une importante perte de chiffre d'affaires pour l'entreprise qui en est victime. En outre, elles peuvent être utilisées comme tactique de diversion pour monopoliser les ressources de réponse aux incidents, tandis que les attaquants ciblent des données clients lucratives (telles que des informations de carte de paiement) dans d'autres zones du réseau de la victime.

Alors que le nombre d'événements d'attaque DDoS est en hausse, nous avons également observé que le nombre de vecteurs utilisés pour déployer ces attaques a fortement augmenté (figure 5a). Ces types d'attaques comprennent les inondations DNS, la fragmentation UDP et la réflexion NTP (figure 5b). Les attaques durent également plus longtemps.

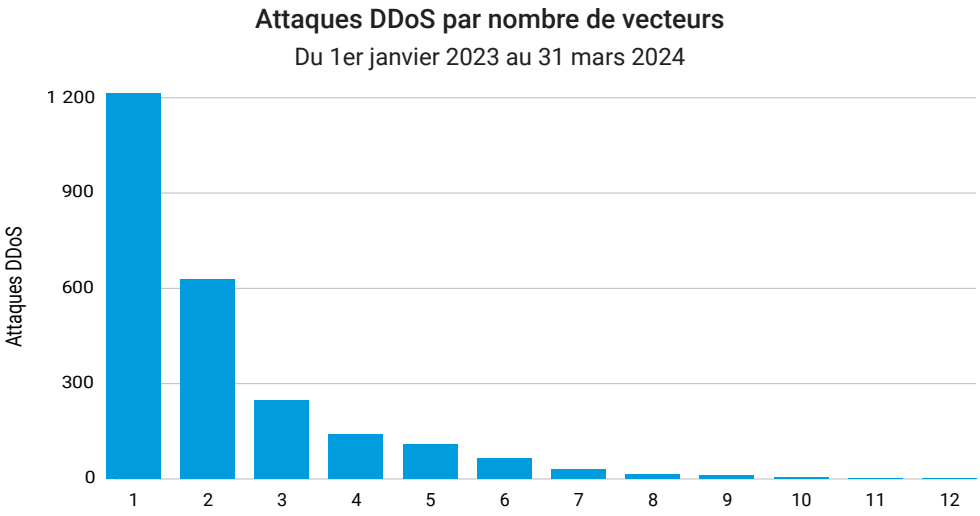

Fig. 5a : Le nombre de vecteurs utilisés pour déployer des attaques DDoS a fortement augmenté

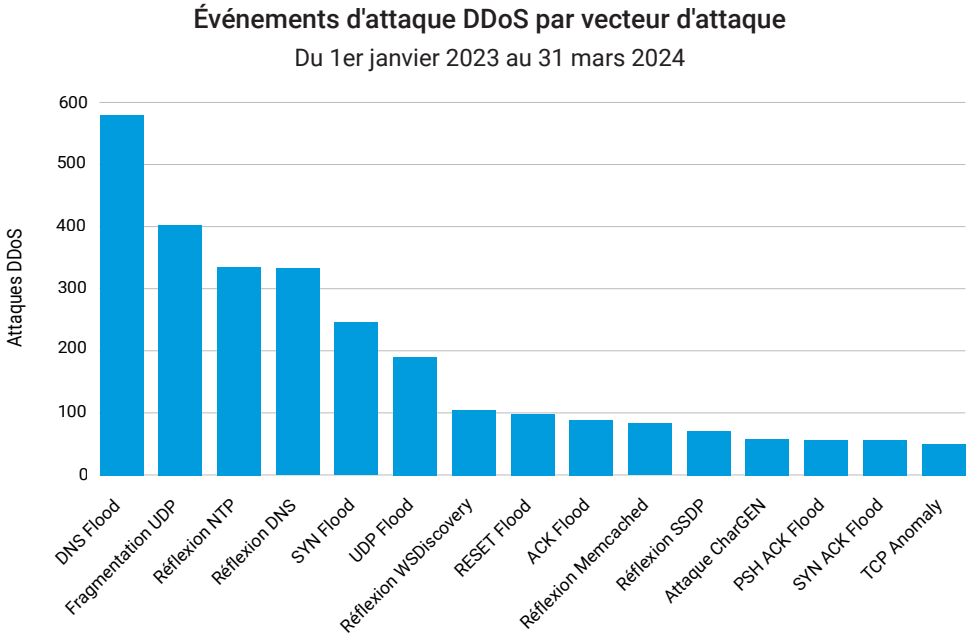

Fig. 5b : Les types d'attaques DDoS de la région EMEA incluent les inondations DNS, la fragmentation UDP et la réflexion NTP.

Les attaques prolongées entravent la productivité et la capacité des entreprises à maintenir leur activité lorsque d'autres menaces sont découvertes et que des contre-mesures sont nécessaires. Les techniques DDoS impliquant des attaques plus longues avec un nombre plus élevé de vecteurs d'attaque DDoS sont des stratégies efficaces pour les attaquants, qui leur permettent de mieux épuiser les ressources et de submerger les équipes de sécurité du réseau des entreprises.

Le DNS, la nouvelle cible des attaques DDoS

Parmi tous les types d'attaques DDoS, celles qui ciblent le DNS (Domain Name System) sont parmi les plus répandues (figure 6). Le DNS est une cible très populaire des attaques DDoS en raison de l'impact que le trafic malveillant peut avoir sur ce service essentiel et fondamental. Une attaque DNS réussie a le potentiel d'effacer littéralement la présence d'une entreprise sur Internet.

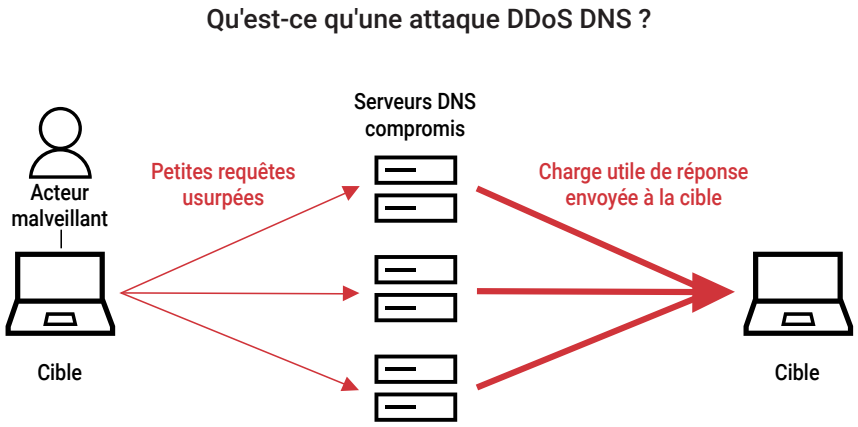

Figure 6 : Une attaque DDoS DNS compromet les serveurs DNS avec des requêtes usurpées, provoquant un envoi massif de charges utiles vers la cible en réponse

Plus précisément, les attaques NXDOMAIN (domaine inexistant), également appelées Pseudo-Random Subdomain (PRSD) ou DNS Water Torture, inondent l'infrastructure DNS de requêtes pour des domaines inexistants. Ce type d'attaque vise à atteindre les serveurs de noms d'origine et à provoquer une forte charge sur les systèmes. Le traitement d'une demande pour un domaine inexistant est une tâche complexe qui consomme de nombreux cycles de traitement, ce qui finit par épuiser la capacité de réponse des systèmes. Nous avons vu de nombreuses attaques courtes de ce type, qui sont généralement utilisées pour sonder la configuration de l'infrastructure DNS de la victime, pour revenir plus tard avec une attaque en force et bien rodée. Selon les résultats des recherches menées auprès de nos 50 principaux clients du secteur financier utilisant le service Edge DNS d'Akamai, les requêtes vers des domaines inexistants représentaient près de 60 % de leur trafic Internet en mars 2024 (figure 7).

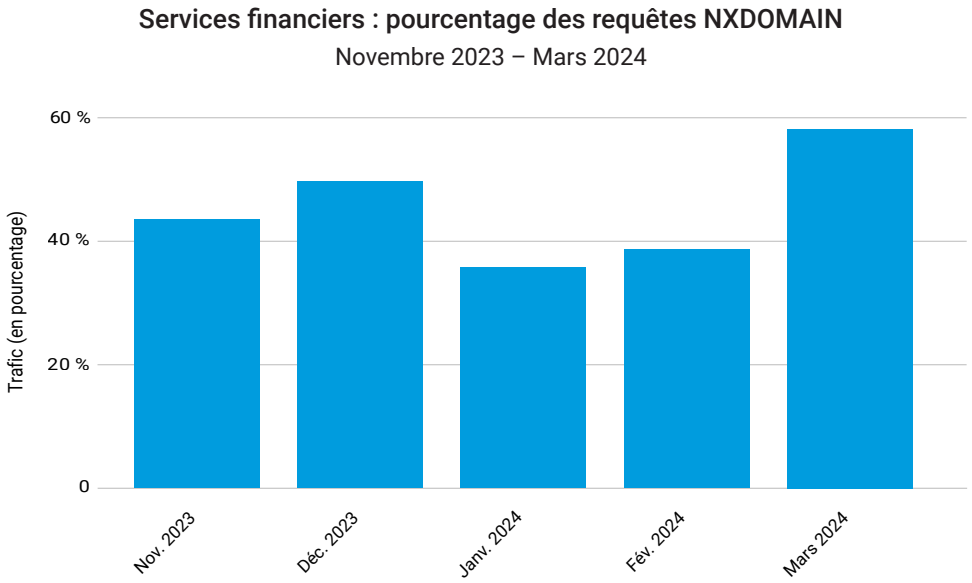

Figure 7 : Depuis la fin de l'année 2023, les requêtes NXDOMAIN ont atteint un pic en mars 2024 avec 58 % des requêtes.

Les attaques d'inondation DNS sont l'un des deux principaux groupes d'attaques DDoS DNS. L'autre est celui des attaques par amplification DNS, qui comprend les attaques par réflexion et consiste à usurper des adresses IP créées par l'attaquant pour envoyer un nombre important de requêtes DNS afin de paralyser les ressources du système ciblé. La facilité d'exécution est une autre raison qui incite l'attaquant à choisir le DDoS DNS, car la majeure partie du trafic passe par le protocole UDP (User Datagram Protocol), qui permet d'utiliser des adresses usurpées.

Déjouer les attaques grâce au pouvoir de l'infosécurité

Pour combattre et prévenir l'augmentation des menaces de cybersécurité (y compris les attaques DDoS) dans la région, les gouvernements et les nations de la région EMEA ont repensé le pouvoir de l'infosécurité. L'environnement réglementaire poursuit son évolution avec la nouvelle directive sur les réseaux et les systèmes d'information (NIS2) et le règlement sur la résilience opérationnelle numérique (DORA), entre autres nouvelles mesures législatives (p. ex. le règlement général sur la protection des données [RGPD], la loi sur la cyberrésilience [CRA], le programme européen pour la protection des infrastructures critiques, etc.)

Il est essentiel que les entreprises mettent en place des mesures de sécurité robustes et évaluent régulièrement leurs applications et leurs réseaux afin d'éviter et de bloquer les cyberattaques. Il s'agit d'une stratégie cruciale pour se protéger contre les attaques DDoS, qui ne laissent pas beaucoup de temps de réaction. En outre, les attaques DDoS ont tendance à cibler des entités moins bien protégées, que les attaquants identifient grâce à une reconnaissance et à des tests précis. Il est donc important que les organisations mettent en place des procédures de sécurité efficaces et disposent de plans de continuité des activités et de reprise après sinistre. Combinées, les nouvelles mesures législatives et directives peuvent constituer des garde-fous pour les organisations.

La directive NIS2, qui a été adoptée en décembre 2022 et abroge et remplace la directive NIS1, vise à étendre, renforcer et harmoniser la mise en œuvre du cadre de cybersécurité existant de l'Union européenne afin de répondre à l'exposition accrue de l'Europe aux cybermenaces. Les États membres de l'UE ont jusqu'au 17 octobre 2024 pour transposer la directive.

Les procédures de gestion des fournisseurs, tels que les tiers, sont également importantes. Le règlement DORA s'appuie sur la réglementation des services financiers de l'UE et s'appliquera à compter du 17 janvier 2025. En plus de promouvoir la cyberrésilience et d'aider les entités de l'UE dans le domaine des services financiers à faire face aux incidents de cybersécurité, le règlement DORA fournit des conseils sur les procédures de gestion des fournisseurs tiers. Cela permet aux entités financières de s'assurer que les fournisseurs de technologies de l'information et de la communication (TIC) avec lesquels elles passent des contrats respectent les normes de sécurité de l'information adéquates. Il s'agit d'éléments clés du modèle des cinq piliers du DORA, qui vise à renforcer la cyberrésilience des entités du secteur des services financiers. Les cinq piliers sont la gestion des risques, la notification des incidents, les tests de résilience opérationnelle numérique, les risques liés aux TIC pour les tiers et le partage d'informations et de renseignements.

La directive NIS2 et le règlement DORA contiennent tous deux des conseils sur les stratégies de résilience utilisant l'approche Zero Trust. La confiance et la disponibilité sont cruciales, en particulier dans l'univers en ligne, et une attaque DDoS peut gravement saper la confiance du public. Il est donc important que les entreprises suivent des procédures de sauvegarde appropriées, telles que la cyberhygiène de base. Ce concept inclut l'utilisation de principes Zero Trust, qui mettent en place un mécanisme de contrôle d'accès plus granulaire et contextuel qui vérifie en permanence l'identité, la posture du terminal et le comportement de l'utilisateur avant d'accorder l'accès à des ressources sensibles. En outre, le concept de moindre privilège est un élément clé des pratiques de sécurité Zero Trust et segmente les utilisateurs dont l'accès est approuvé. Les solutions Zero Trust aident également à protéger les actifs critiques des entreprises contre les attaques RDDoS.

Outre la législation relative aux attaques DDoS, il est également important que les entreprises se familiarisent avec d'autres réglementations existantes visant à lutter contre les cybermenaces dans la région EMEA. Par exemple, la nouvelle Loi sur la cyberrésilience de l'Union européenne cible les vulnérabilités logicielles et matérielles que les attaquants exploitent de plus en plus pour infiltrer les organisations et lancer des attaques par ransomware. En outre, le RGPD a créé des obligations pour toutes les organisations qui traitent des données personnelles d'entreprises et de clients européens.

En dehors de l'Union européenne, d'autres pays créent et appliquent également leurs propres contrôles. L'Autorité nationale de cybersécurité d'Arabie saoudite a adopté des lois sur la protection des données similaires au RGPD, et le Bureau africain des opérations cybercriminelles d'Interpol a mis en place des programmes comme Africa Cyber Surge.

Étude de cas : une organisation européenne de commerce électronique subit une attaque DDoS au niveau de la couche réseau

Le maintien de la disponibilité et de la résilience d'un site Web est essentiel pour les entreprises de commerce électronique et leur permet de stimuler la croissance de leur chiffre d'affaires. C'est pourquoi la protection des actifs et des applications Web contre les attaques DDoS afin d'éviter tout événement ayant un impact sur leur activité (et leurs clients) est une priorité pour les responsables de la sécurité. Mais que se passerait-il si l'infrastructure sous-jacente ou les systèmes back-end qui gèrent le cycle de vie des commandes étaient perturbés ou complètement mis hors service ? C'est une chose qu'un client passe une commande, mais si la commande ne peut pas être traitée ou validée, les opérations risquent de s'arrêter net. C'est ce qui est arrivé à une entreprise de commerce électronique en Europe. Une attaque DDoS au niveau du réseau a réussi à cibler des services au sein du centre de données, dont les contrôles étaient insuffisants.

De nombreux acteurs malveillants ont l'habitude de lancer des campagnes d'attaque les week-ends et les jours fériés, lorsqu'il y a moins de personnel de sécurité et de ressources de réponse aux incidents pour réagir à une menace. Dans le cas de cette entreprise européenne de commerce électronique, les pirates ont utilisé une combinaison de vecteurs d'attaque SYN et UDP Flood pour cibler le centre de données de la société un vendredi après-midi et mettre hors service ses ressources vulnérables, telles que les e-mails. Cela a empêché la transmission de données importantes à d'autres parties de l'entreprise, y compris aux entrepôts logistiques.

En conséquence, l'infrastructure logistique a été incapable de fonctionner et de traiter les commandes reçues de la plateforme de commerce électronique, même si l'infrastructure logistique elle-même n'a pas été touchée. L'entreprise étant incapable de se défendre contre ce grand nombre d'attaques DDoS volumétriques, Akamai a été appelé à réaliser une intégration d'urgence pour protéger les centres de données de l'entreprise de vente au détail. En moins de 24 heures, le client était sur la plateforme Prolexic d'Akamai et sa connexion aux services critiques de l'entreprise était rétablie.

En bref, les entreprises de commerce électronique doivent adopter une approche globale des attaques DDoS, qui comprend l'atténuation des attaques de couche 7 (application) et des attaques des couches 3 (réseau) et 4 (transport), afin d'éviter les temps d'arrêt et de garantir la résilience tout au long du cycle de vie.

Sauvegarde et atténuation des risques

Maintenant que nous avons abordé les principales tendances et réglementations en matière de DDoS dans la région EMEA et analysé quelques exemples d'attaques, voyons ce que vous pouvez faire pour protéger votre organisation. Outre le respect des mesures législatives mentionnées précédemment, notamment NIS2, DORA, RGPD et CRA, et l'utilisation de solutions Zero Trust, les chercheurs d'Akamai recommandent trois stratégies concrètes pour lutter contre l'évolution du paysage DDoS.

1. **Préparez-vous de manière proactive en adoptant une posture de protection contre les attaques DDoS pour vos actifs digitaux.**
   Cela nécessite :
   - de s'assurer que des contrôles d'atténuation sont en place pour toutes les adresses IP exposées et les sous-réseaux critiques ;
   - de déployer des contrôles de sécurité DDoS correspondant à la posture de protection en ligne ;
   - de veiller à ce que les plans et les équipes d'intervention en cas d'incident soient à jour et désignés ;
   - de renforcer votre protection DDoS sur site avec une plateforme de protection hybride pour vous défendre contre les attaques qui surchargent les équipements sur site ;
   - de mettre en place des contrôles de sécurité proactifs via un pare-feu réseau dans le cloud et un pare-feu d'application Web ;
   - de configurer la limitation du débit ;
   - de mettre en cache du contenu sur un CDN ;
   - d'utiliser une équipe du centre de commandement des opérations de sécurité pour alléger la pression sur les ressources internes essentielles.

2. **Protégez votre infrastructure DNS.** Si le DNS d'une entité tombe, la présence de l'entité disparaît également. Un pare-feu DNS traditionnel peut ne pas fournir une protection adéquate si l'installation gère des zones à la fois sur site et dans le cloud. Dans ce cas, une plateforme hybride peut être la solution optimale. En règle générale, pour garantir une sécurité suffisante contre les attaques DDoS, il convient d'examiner minutieusement le trafic Internet destiné à votre réseau, et d'atténuer et de filtrer le trafic d'attaque avant qu'il n'atteigne vos applications, vos API et votre infrastructure, y compris votre DNS.

3. **Ne vous contentez pas de solutions « suffisantes ».** Il peut sembler plus simple de n'utiliser que les protections minimales adaptées à vos besoins et à votre budget. Cependant, les entreprises constatent souvent que cette « économie » initiale conduit à des sinistres ultérieurs plus graves, qui entraînent des dépenses et des dommages supplémentaires qui dépassent largement les avantages du plan initial. Il est donc important de tester vos défenses du point de vue des meilleures pratiques et des solutions techniques. Ces tests doivent inclure la documentation relative aux incidents, les processus, les runbooks, etc., afin de garantir que vos solutions offrent un niveau de cybersécurité élevé.

Conclusion

La nature et l'impact des attaques DDoS ont grandement évolué au fil du temps et sont désormais de plus en plus sévères et complexes.

La région EMEA a été particulièrement touchée par cette hausse des attaques DDoS. Les gouvernements, les services financiers, le commerce et le secteur de la santé ont tous connu une augmentation du nombre de ces types d'attaques. Cette évolution régionale peut être attribuée, en partie, aux tensions et conflits géopolitiques actuels dans la région EMEA, qui favorisent l'essor de l'hacktivisme et des activités DDoS associées.

En outre, les événements et les élections à venir en Europe, notamment les élections au Parlement européen, les élections au Royaume-Uni et les Jeux olympiques d'été en France, sont susceptibles d'accroître encore le risque d'attaques DDoS. Ces événements, qui revêtent une importance politique et économique considérable, constituent des motivations de premier ordre pour les acteurs malveillants qui cherchent à perturber et à influencer les événements en utilisant des tactiques DDoS.

Les législateurs de la région EMEA ont repensé le pouvoir de l'infosécurité et renforcé les mesures de sécurité en adoptant de nouvelles directives et réglementations. En général, les entreprises et les organisations qui respectent ces réglementations et ont mis en place des mesures de protection sont moins susceptibles d'être considérées comme des proies faciles par les cybercriminels. Les auteurs d'attaques DDoS ont tendance à viser des cibles vulnérables et mal protégées, et mènent en permanence des opérations de reconnaissance pour découvrir les cibles les plus faciles à exploiter via des attaques DDoS. En raison de la multitude de vecteurs d'attaque DDoS et des nombreux chemins existant entre les couches réseau, transport et application, il est crucial d'utiliser un ensemble de solutions pour assurer une protection complète contre les attaques DDoS. Ce type de défense est essentiel pour lutter le plus efficacement possible contre les menaces DDoS croissantes dans la région EMEA.

Méthodologie

DDoS (couches 3 et 4)

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

Les données de ce rapport couvrent la période de 15 mois allant du 1er janvier 2023 au 31 mars 2024, sauf indication contraire.

DDoS (couche 7)

Ces données décrivent les alertes de la couche applicative sur le trafic vu à travers notre Web Application Firewall (WAF). Les alertes DDoS de couche 7 sont déclenchées lorsque nous détectons des anomalies volumétriques dans le nombre de requêtes adressées à un site Web, une application ou une API protégés. Ces alertes peuvent être déclenchées à la fois par des requêtes malveillantes et bénignes. Généralement, les requêtes elles-mêmes sont bénignes, mais leur volume élevé indique une intention malveillante. En revanche, ces alertes n'indiquent pas si ces attaques sont fructueuses. Bien que ces solutions soient hautement personnalisables, nous avons recueilli les données pour ce rapport d'une manière qui ne tient pas compte des configurations personnalisées des ressources 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.

Les données de ce rapport couvrent la période de 15 mois allant du 1er janvier 2023 au 31 mars 2024.

DDoS (NXDOMAIN)

Ces données décrivent le trafic vu à travers notre réseau en bordure de l'Internet pour 50 de nos principaux clients du secteur des services financiers. Les requêtes visant les NXDOMAINs sont suivies et documentées. Ces requêtes peuvent être faites avec des intentions malveillantes ou bénignes. En général, une augmentation du nombre de requêtes NXDOMAIN dans un laps de temps et/ou une zone géographique donnés indique un comportement malveillant. Nos équipes de sécurité utilisent ces données pour étudier les attaques, signaler les comportements malveillants et fournir des renseignements supplémentaires aux solutions d'Akamai.

Ces données couvrent la période de cinq mois allant de novembre 2023 à mars 2024.

Crédits

Édition et rédaction

Lance Rhodes – Rédacteur en chef
Susan McReynolds – Rédactrice de l'étude de cas
Maria Vlasak – Rédaction

Révision et expertise

Christian Borggreen
Cheryl Chiodi
Sven Dummer
Jim Gilbert
Mitch Mayne
Richard Meeus
Craig Sparling
Carley Thornell

Analyse des données

Chelsea Tuttle

Documents promotionnels

Annie Brunholzl

Marketing et publication

Georgina Morales Hampe
Emily Spinks

Autres rapports État des lieux d'Internet/Sécurité

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

D'autres recherches sur les menaces d'Akamai

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

Accéder aux données de ce rapport

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

En savoir plus sur les solutions Akamai

Pour en savoir plus sur les solutions Akamai pour les attaques DDoS, consultez nos **solutions Prolexic** et nos pages sur la **Sécurité des API** et des applications.