LIVRE BLANC

L'évolution rapide et la menace croissante des attaques DDoS

Les attaques devenant de plus en plus ciblées, sophistiquées et fréquentes, toutes les entreprises doivent rester vigilantes.

Désormais, plus aucune entreprise n'échappe aux attaques par déni de service distribué (DDoS). Les cybercriminels, motivés par l'extorsion, l'hacktivisme ou la vengeance, peuvent facilement cibler n'importe quelle organisation avec des attaques importantes et sophistiquées. C'est pourquoi toutes les entreprises axées sur le digital ont désormais besoin d'une défense globale contre les attaques DDoS.

L'un des types d'attaque les plus anciens sur Internet

Le 22 juillet 1999, 114 ordinateurs compromis ont submergé un seul ordinateur de l'Université du Minnesota avec des paquets de données superflus,ce qui a causé sa mise hors ligne pendant deux jours.

Selon le magazine MIT Technology Review, il s'agissait de la première attaque DDoS documentée.

Au cours des semaines et des mois qui ont suivi cet événement, des acteurs majeurs comme CNN ou Amazon ont été mis hors ligne lorsque des hacktivistes et d'autres cybercriminels ont pris conscience de la facilité avec laquelle ils pouvaient lancer ce type d'attaque. Quelques lignes de code suffisaient.

Les attaques DDoS sont devenues une menace pour toute entreprise disposant d'une présence en ligne.

Les attaques évoluent et sont plus sophistiquées

Les solutions de défense contre les attaques DDoS ont beaucoup évolué depuis 1999. Mais il en va de même pour les cybercriminels. Aujourd'hui, les acteurs des menaces DDoS disposent de dizaines de vecteurs d'attaque à exploiter, de kits d'outils peu coûteux destinés aux pirates, ainsi que d'innombrables terminaux vulnérables sur Internet à cibler pour amplifier leurs campagnes. En 2016, des attaquants ont mis hors service une grande partie d'Internet à l'aide d'enregistreurs vidéo numériques de caméras de sécurité compromis.

Depuis, des centaines de millions d'autres terminaux IoT non protégés ont été connectés à Internet. La révolution de la technologie 5G promet d'en ajouter encore plusieurs centaines d'autres millions. Imaginez la force et l'importance des attaques alimentées par les améliorations exponentielles de la 5G en termes de vitesse, de capacité et de latence.

En outre, il existe de de plus en plus de serveurs non protégés et non entretenus que les criminels peuvent détourner pour des attaques par amplification et par réflexion. Un grand nombre de ces serveurs (dont les adresses IP sont connues des criminels) peuvent multiplier les demandes frauduleuses par un facteur de plus de 50 000.

Service d'urgence de protection et de lutte contre les attaques DDoS disponible 24 h/24, 7 j/7

Les clients d'Akamai existants menacés par une attaque DDoS doivent contacter le Centre de commande des opérations de sécurité d'Akamai (SOCC).

Si vous n'êtes pas client d'Akamai mais que vous avez besoin d'une protection d'urgence, complétez le formulaire sur notre **page d'assistance DDoS** ou appelez le **+1-877-425-2624** pour obtenir une assistance immédiate.

Les attaques DDoS touchent tous les secteurs

Aujourd'hui, Akamai atténue chaque année des milliers d'attaques DDoS.

Dans certains cas, les motifs de celles-ci semblent évidents. Un joueur peut utiliser des attaques DDoS pour ralentir les réseaux et obtenir un avantage concurrentiel sur ses adversaires. Par le passé, des étudiants ont utilisé des attaques DDoS ciblées pour contrarier les clients d'un FAI et les pousser à rejoindre un concurrent.

Cependant, les motifs sont parfois plus complexes à identifier. Nous avons vu des cybercriminels utiliser des attaques DDoS pour distraire les équipes de réponse aux incidents d'une partie d'une entreprise, alors qu'ils tentaient une attaque moins évidente dans une autre.

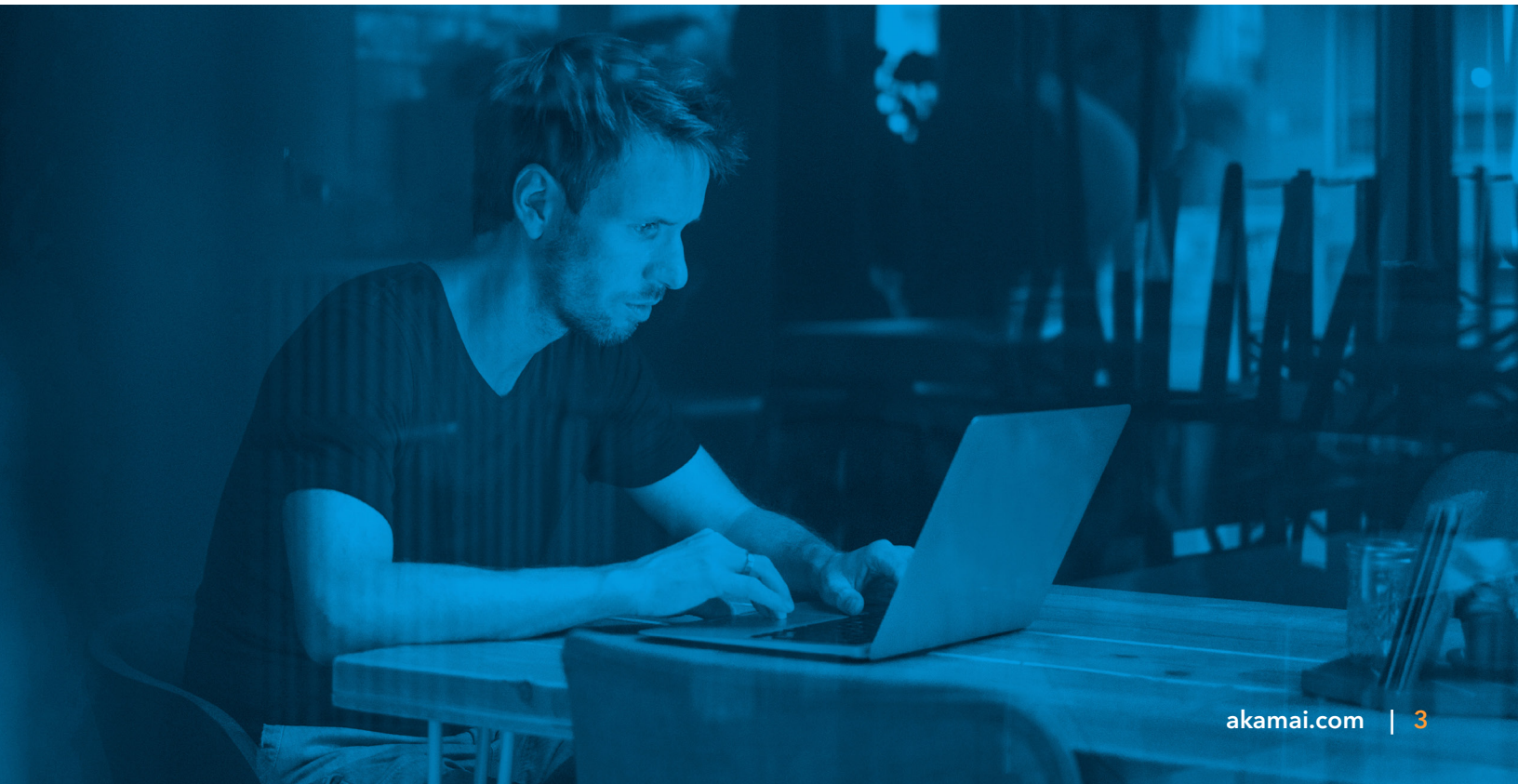
Pour les acteurs malveillants qui n'ont pas les compétences requises, il existe des offres « DDoS for Hire » (DDoS à louer) sur le Darknet. Les prix commencent à 5 $ pour une attaque de 5 minutes et peuvent grimper jusqu'à 400 $ pour 24 heures. Si une personne souhaite se venger, elle peut dépenser 200 ou 300 dollars pour faire perdre des millions à une entreprise.

2020 a entraîné des attaques plus importantes et plus sophistiquées

Au cours du premier semestre 2020, Akamai a stoppé des attaques massives de 1,44 térabit par seconde (Tbit/s) et de 809 millions de paquets par seconde (Mpps), la plus grande attaque Mpps jamais enregistrée.

Bien qu'atténuées en moins d'une seconde, ces attaques reflètent la tendance des cybercriminels à se tourner davantage vers des attaques de 100 Gbit/s ou plus. Nombre d'entre elles utilisent des combinaisons uniques et complexes de plusieurs vecteurs. Elles visent à submerger ou à contourner les défenses et à consommer les ressources de réponse aux incidents.

Les attaques qui nécessitent un minimum de mesures d'atténuation réalisées par l'homme, et pas seulement des réponses automatisées, sont également en hausse.



La plus grande campagne d'extorsion DDoS de l'histoire

En août 2020, l'équipe Security Intelligence Research d'Akamai a publié une alerte, mettant en garde sur le fait que des entreprises de divers secteurs avaient reçu des e-mails d'extorsion DDoS. Les attaquants ont menacé de paralyser les opérations, en insinuant que les entreprises seraient confrontées à des temps d'arrêt très importants et à de lourdes pertes financières si elles ne payaient pas une rançon en Bitcoin.

Quelques semaines plus tard, le FBI a déclaré que des milliers d'organisations dans le monde avaient reçu des e-mails d'extorsion similaires. Les cybercriminels auraient afflué en masse dans un secteur et menacé les entreprises, avant de passer un autre, et ainsi de suite. Très organisés, les attaquants sont souvent revenus menacer des cibles d'attaques précédentes.

Plus vos défenses sont efficaces, moins vous êtes susceptible d'être attaqué

Les cybercriminels sont des criminels comme les autres. Ils font du « repérage » pour identifier les vulnérabilités. Pour les attaques DDoS, cela signifie qu'ils recherchent d'abord dans le DNS, les applications Web et les actifs du centre de données en ligne de la victime visée.

Si cette reconnaissance révèle des ressources, des sites ou des services vulnérables, les attaquants peuvent passer à l'action. Si elle met en évidence des défenses renforcées, les cybercriminels abandonnent et passent à la cible suivante.

En fait, parmi les nouveaux clients Prolexic qui se sont tournés vers nous en urgence après avoir été attaqués avant d'adopter la plateforme, la grande majorité d'entre eux n'ont plus été touchés une fois les défenses Prolexic mises en place. Pour un cybercriminel, les cibles défendues par Prolexic ne valent peut-être pas la peine de perdre son temps, surtout lorsqu'il existe d'autres cibles plus vulnérables ailleurs.

Comment fonctionne une défense DDoS globale

Akamai fournit une défense DDoS approfondie grâce à un maillage transparent de solutions d'atténuation en bordure de l'Internet, de DNS distribué et de nettoyage sur le cloud avec une capacité réseau totale de plus de 175 Tbit/s. Ces clouds dédiés sont conçus pour renforcer les postures de sécurité DDoS tout en réduisant les surfaces d'attaque. Cette protection DDoS de bout en bout a été conçue pour améliorer la qualité de l'atténuation et réduire les faux positifs, tout en renforçant la résilience contre les attaques les plus importantes et les plus complexes.

En outre, cette solution peut être adaptée aux besoins spécifiques de vos applications Web et de vos services en ligne.

Défense en bordure de l'Internet

Akamai a conçu son Intelligent Edge Platform, distribuée dans le monde entier, comme un proxy inverse qui n'accepte le trafic que via les ports 80 et 443. Toutes les attaques DDoS au niveau de la couche réseau sont instantanément neutralisées en bordure de l'Internet grâce à un accord de niveau de service (SLA) immédiat.

Kona Site Defender absorbe les attaques DDoS au niveau des événements de la couche application, y compris ceux lancés via les API, tout en permettant l'accès aux utilisateurs légitimes.

Défense du DNS

Le service DNS de référence d'Akamai, Edge DNS, filtre également le trafic en bordure de l'Internet. Contrairement aux autres solutions DNS, Akamai a spécifiquement conçu Edge DNS dans une optique de disponibilité et de résilience face aux attaques DDoS. Edge DNS offre également des performances supérieures, avec des redondances architecturales à plusieurs niveaux, notamment les serveurs de noms, les points de présence, les réseaux et même les clouds IP Anycast segmentés.

Défense par nettoyage sur le cloud

Prolexic protège des centres de données entiers et des infrastructures hybrides contre les attaques DDoS, sur tous les ports et protocoles, grâce à 20 centres de nettoyage mondiaux et 8,2 Tbit/s de défense DDoS dédiée. Cette capacité est conçue pour maintenir la disponibilité des actifs en ligne, une pierre angulaire de tout programme de sécurité de l'information.

En tant que service entièrement géré, Prolexic permet de développer des modèles de sécurité positifs et négatifs. Ce service associe des défenses automatisées à une atténuation experte assurée par le réseau mondial de SOCC d'Akamai. Prolexic propose également un SLA d'atténuation instantanée de pointe via des contrôles défensifs proactifs.

Comment Prolexic a stoppé une attaque record

L'attaque de 809 Mpps en juin 2020 a été la plus grande attaque basée sur les paquets par seconde (PPS) jamais vue sur Internet. Contrairement aux attaques par bits par seconde les plus courantes, qui tentent de submerger le pipeline Internet entrant, les attaques PPS ont été lancées pour épuiser les équipements réseau du centre de données ou du cloud.

Cette attaque de grande envergure a impliqué un très grand nombre d'adresses IP sources. Plus de 96 % de celles-ci n'avaient jamais été observées dans une attaque auparavant. L'attaque est également passée de 418 Gbit/s à 809 Mpps en seulement deux minutes.

Heureusement, l'entreprise ciblée était un client Prolexic et elle avait un SLA d'atténuation immédiate. Le SOCC d'Akamai a collaboré avec ce client pour comprendre ses profils de référence de trafic en période normale et mettre en place des contrôles ainsi que des stratégies de sécurité pour bloquer les attaques DDoS instantanément.

Planifiez un rapport sur les menaces personnalisé dès aujourd'hui

Rendez-vous sur **akamai.com/ddos-briefing**