Dompter le monstre continuellement changeant des attaques DDoS

CLOUDFLARE®

Le premier déni de service (DoS) a été observé en 1974, lorsqu'un lycéen curieux a réalisé une expérience avec un logiciel pour refuser à une salle remplie d'utilisateurs la possibilité de s'authentifier sur un ordinateur. Depuis, cette petite expérience consacrée au déni de service s'est aujourd'hui transformée en un véritable cybermonstre – un monstre qui a connu une évolution spectaculaire. À titre d'exemple, au cours de la dernière décennie, nous avons observé la création de sites web proposant des attaques DDoS à la demande, qui offrent aux utilisateurs techniques et non techniques des capacités DDoS-as-a-Service.

Voici les 3 horribles têtes du monstre DDoS : ampleur, approche multi-vecteurs et omniprésence

1. AMPLEUR

En 2016, une **attaque DDoS lancée par le botnet Mirai** a attiré l'attention du monde entier : cette attaque DDoS volumétrique massive a ciblé et mis hors ligne OVH, un des plus grands fournisseurs d'hébergement européens. Selon les mesures de télémétrie d'OVH, l'attaque a culminé à 1 Tb/s et a été lancée depuis 145 000 appareils IoT.

Quelques années plus tard, en 2018, **GitHub** a subi l'une des plus vastes attaques DDoS volumétriques, enregistrée à 1,35 Tb/s. Cette attaque reposait sur un vecteur inconnu d'attaque par amplification : le protocole **memcached**, qui utilise le port UDP 11211.

Les attaques de grande ampleur sont percutantes. Cependant, générer de grands volumes de trafic pour épuiser les ressources de la victime ciblée est une opération coûteuse. C'est pourquoi les attaques tendent aujourd'hui à devenir des attaques « en rafale ». Ces dernières sont d'une ampleur considérable, mais d'une durée plus courte. Elles submergent le site web ciblé, mais ne peuvent pas être détectées par les systèmes automatiques, en raison de leur brévité.

2. APPROCHE MULTI-VECTEURS

Les tactiques des attaques DDoS, comme d'autres tactiques d'attaques contre la de sécurité, exploitent souvent les faiblesses des processus de communication des protocoles. Prenons l'exemple du protocole TCP : une attaque DDoS peut utiliser les tactiques SYN flood ou ACK flood pour épuiser les ressources du serveur. L'existence de ces vulnérabilités dans plusieurs protocoles tels qu'UDP et ICMP offre un arsenal de tactiques d'attaque dont les acteurs malveillants peuvent tirer profit pour lancer une attaque DDoS.

À titre d'exemple, en septembre 2019, Wikipédia a détecté une perturbation majeure de l'accès des utilisateurs du monde entier à ses sites, qui a duré environ 9 heures. Alors que la disponibilité et les performances de l'application web étaient affectées au niveau du serveur HTTP, l'attaque DDoS ciblait directement les data centers de Wikipédia, au niveau de la couche réseau. L'attaque était d'une ampleur supérieure à 250 Gb/s et reposait sur l'association des tactiques ACK flood et UDP flood.

3. OMNIPRÉSENCE

Les attaques DDoS sont une triste réalité pour les organisations et les entreprises d'aujourd'hui. Si les entreprises des grandes puissances économiques telles que les États-Unis sont des cibles lucratives pour les attaquants malveillants, les entreprises du monde entier subissent des attaques DDoS sophistiquées, quel que soit leur secteur d'activité. En 2019, les banques sud-africaines ont subi des attaques DDoS durables, qui étaient accompagnées de demandes de rançon, tandis que les opérateurs de télécommunications sud-africains tels que Liquid Telecom repoussaient des attaques DDoS massives, dont la taille excédait 100 Gb/s.

> « Les acteurs malveillants explorent continuellement de nouvelles approches et tactiques pour lancer des attaques DDoS évoluées. »

L'appétit grandissant du monstre DDoS

Le début de l'année 2020 a été marqué par un déchaînement d'attaques DDoS. EVE Online, une entreprise exploitant un jeu massivement multijoueurs en ligne (MMO), a subi une interruption de ses services de plusieurs jours suite à une attaque DDoS. Les forums en ligne du jeu ont été inondés de messages de joueurs frustrés qui demandaient à clôturer leur compte ou exigeaient une indemnisation parce que, plusieurs jours durant, ils ne pouvaient plus se connecter à leur compte. Pour les MMO, la moindre augmentation des temps de réponse (sans même parler d'une perturbation de plusieurs jours) est extrêmement frustrante pour les clients.

Les acteurs malveillants explorent continuellement de nouvelles approches et tactiques pour lancer des attaques DDoS évoluées. Par exemple, des pirates informatiques recherchent actuellement sur Internet les appareils NSC Linear eMerge E3 non protégés, afin d'exploiter la vulnérabilité CVE-2019-7256 qui leur permettrait de prendre le contrôle des appareils, de télécharger et d'installer des logiciels malveillants, puis de lancer des attaques DDoS contre d'autres cibles. Ces équipements sont généralement installés dans des locaux d'entreprises, des usines et des infrastructures similaires, et constituent le système de contrôle des accès des employés et des visiteurs.

Pourfendez le monstre DDoS dans le Cloud

Les approches patrimoniales consistant à installer des équipements matériels sur site pour déployer une protection anti-DDoS sont dépassées, car les attaques DDoS actuelles sont plus vastes, plus sophistiquées et de portée mondiale. Or, les solutions anti-DDoS sur site ne sont pas adaptées à l'ampleur, à la vélocité et à la nature distribuée des attaques.

Cependant, l'architecture distribuée des solutions de protection anti-DDoS dans le Cloud offre une approche toujours active, permettant de mitiger les attaques DDoS à l'échelle mondiale. Il est essentiel de tenir compte des aspects suivants lors du choix d'une solution de protection anti-DDoS dans le Cloud :

ARCHITECTURE DISTRIBUÉE

La nature mondiale des attaques DDoS exige que la solution de protection anti-DDoS possède une architecture distribuée au niveau mondial, afin de mitiger les attaques le plus près possible de leur source. Puisque la taille des attaques DDoS a augmenté, l'approche patrimoniale reposant sur un centre de nettoyage des données des solutions anti-DDoS dans le Cloud est rapidement devenue obsolète, à cause de la propension des centres de nettoyage de données à constituer un « goulet d'étranglement ». Traditionnellement, les fournisseurs de solutions anti-DDoS ont investi dans un petit nombre de centres de nettoyage de données, vers lesquels les attaques DDoS de grande ampleur devaient être réacheminées, car ils ne disposaient pas d'une architecture véritablement distribuée. Pour en savoir plus sur les failles que comporte l'approche reposant sur un centre de nettoyage de données, consultez cette excellente publication de blog : « **No scrubs** ».

La solution moderne de protection contre les attaques DDoS de Cloudflare s'exécute sous forme de service sur tous les serveurs dans chacun de ses data centers, présents dans 200 villes à traves le monde, ce qui en fait une solution anti-DDoS véritablement distribuée. Lorsqu'une attaque DDoS est détectée, peu importe sa région d'origine, elle est atténuée dans le data center Cloudflare le plus proche, ce qui permet de mitiger plus rapidement l'attaque et d'augmenter la disponibilité de l'infrastructure des clients.

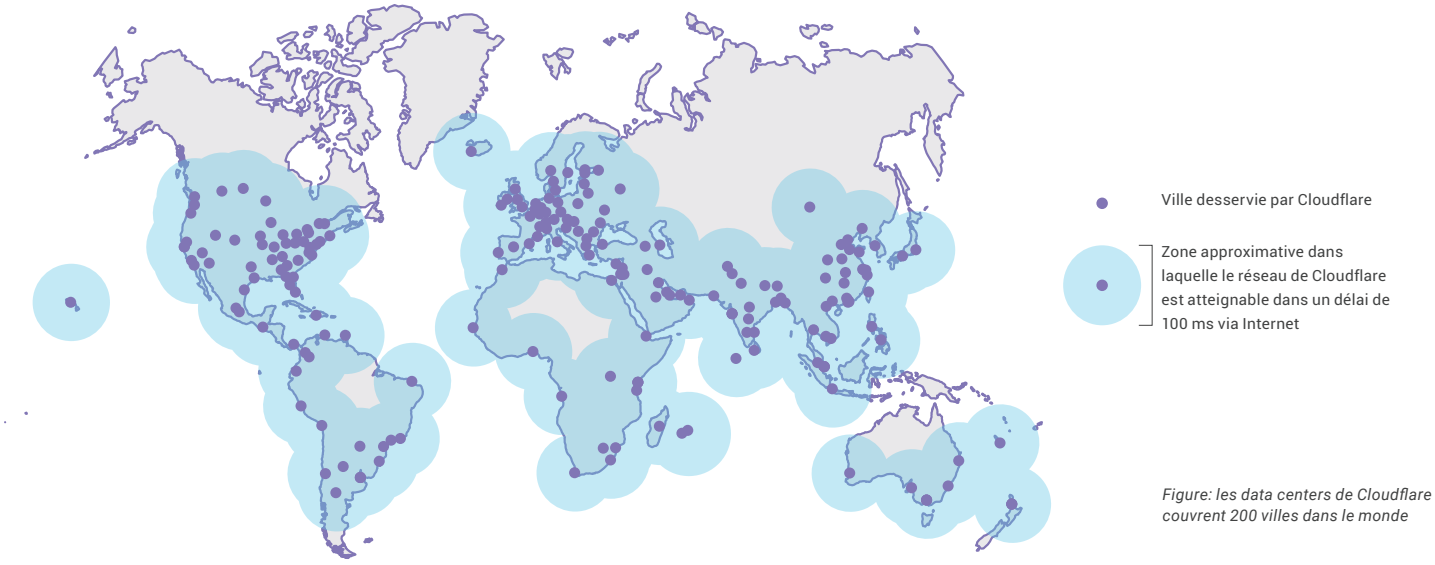


Figure: les data centers de Cloudflare couvrent 200 villes dans le monde

CAPACITÉ DU RÉSEAU

Pour réduire l'étendue et l'ampleur de l'attaque DDoS, la capacité du réseau de la solution de protection anti-DDoS joue un rôle essentiel, en particulier lors d'attaques DDoS de l'ordre du Tb/s.

Le réseau mondial Anycast de Cloudflare possède une capacité de plus de 30 Tb/s, qui lui permet d'atténuer même les attaques DDoS les plus vastes. De plus, Cloudflare est connecté à un plus grand nombre de points d'interconnexion Internet que tout autre fournisseur dans le monde. Le réseau de Cloudflare est interconnecté avec plus de 8 000 réseaux dans le monde, notamment ceux d'éminents FAI, services de Cloud et entreprises.

COUVERTURE COMPLÈTE

Il existe un véritable arsenal de tactiques d'attaque dont les acteurs malveillants peuvent tirer profit pour lancer une attaque DDoS au niveau des couches application et réseau. Les solutions anti-DDoS dans le Cloud devraient permettre de mitiger de manière exhaustive les attaques DDoS visant plusieurs couches.

La protection anti-DDoS avancée de Cloudflare offre une couverture complète contre les attaques DDoS de couche 7, tandis que les solutions Cloudflare Spectrum et Magic Transit mitigent les attaques DDoS des couches 3 et 4. La note de **blog** de ThousandEyes consacrée à l'analyse de l'attaque DDoS lancée contre Wikipédia souligne comment Cloudflare a pu mitiger rapidement et exhaustivement une attaque DDoS multi-vecteurs de grande ampleur.

INFORMATIONS EN TEMPS RÉEL

Au lieu d'adopter un mode de fonctionnement réactif, les solutions de protection anti-DDoS devraient être étayées par des informations en temps réel concernant les menaces, permettant de développer une approche proactive de la mitigation d'attaques DDoS.

La solution de protection contre les attaques DDoS de Cloudflare repose sur les informations concernant les menaces collectées sur son réseau, qui apprend continuellement, protège plus de 20 millions de propriétés Internet et inspecte plus d'un milliard d'adresses IP uniques chaque jour. Grâce à ces informations concernant les menaces, aux modèles d'apprentissage automatisé et à l'expertise en matière d'ingénierie d'une équipe expérimentée, la protection anti-DDoS de Cloudflare offre une solution performante face aux attaques DDoS les plus sophistiquées.

MITIGATION AUTOMATISÉE

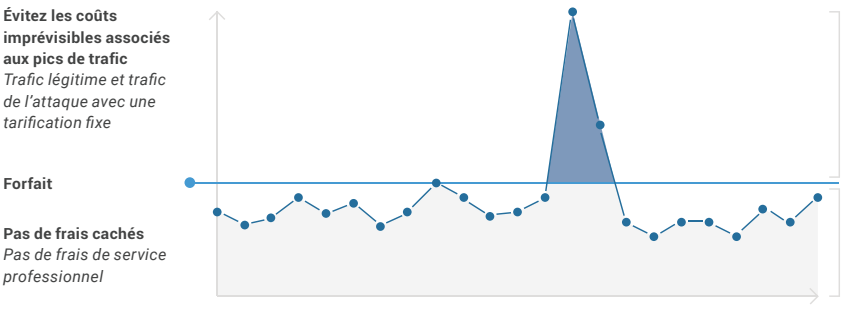
Les attaques DDoS sophistiquées nécessitent une capacité de mitigation automatisée, qui inspecte en permanence le trafic transféré vers une entreprise (qu'elle opère sur site ou dans le Cloud), exécute une analyse en temps réel et mitige rapidement les attaques DDoS.

Les systèmes automatisés de Cloudflare (**gatebot** et **dosd**) analysent continuellement les empreintes des attaques, les anomalies, les règles, les listes noires et bien davantage. Le système gatebot contribue à mitiger les attaques volumétriques globales, tandis que le système dosd s'exécute sur chaque serveur, afin d'atténuer les attaques localisées. Ensemble, ces systèmes automatisés recommandent plus de 400 000 règles dynamiques par seconde pour une mitigation rapide.

ÉCONOMIQUE

À mesure que l'étendue et l'ampleur des attaques DDoS augmentent, toutes les entreprises et organisations doivent considérer que le coût d'une protection anti-DDoS est durable. Les fournisseurs de solutions de protection anti-DDoS dans le Cloud proposent souvent une protection anti-DDoS mesurée. Bien que les solutions dans le Cloud offrent une protection supérieure à celle des solutions sur site, en évoluant avec flexibilité pour offrir une protection contre les attaques DDoS, la mitigation mesurée peut souvent entraîner une augmentation phénoménale des montants facturés. Au lieu de perdre de l'argent parce qu'elle ne parvient pas à servir ses clients, une entreprise risque d'être confrontée à de graves difficultés financières en raison des coûts de la mitigation mesurée d'une attaque DDoS.

Cloudflare propose une mitigation des attaques DDoS **illimitée et non mesurée**. Ceci élimine le concept patrimonial de « facturation des pics », qui est particulièrement douloureux pour une entreprise, déjà durement éprouvée, qui subit une attaque DDoS. Ceci vous permet d'éviter les coûts imprévisibles associés aux pics de trafic.



Soyez un héros – **pourfendez dès aujourd'hui le monstre DDoS !**