Protection contre les attaques DDOS avec Cloudflare

Évolution des attaques DDoS modernes

2016

1 Tbit/s

Attaque de la couche 7 par le botnet IoT

La plus grande attaque de la couche 7 jamais enregistrée à l'aide du botnet IoT Mirai. L'attaque était non seulement volumétrique, mais elle a également utilisé des ressources serveur.

2014

400 Gbits/s

Attaque d'amplification NTP

Un agresseur a utilisé 4 529 serveurs NTP pour amplifier une attaque à partir d'un serveur source d'à peine 87 Mbits/s

2013

120 Gbits/s

Attaque DDoS des couches 3/4

L'attaque Spamhaus était considérée comme l'une des plus importantes à l'époque et a été qualifiée « d'attaque qui a pratiquement détruit Internet ».

Les attaques par déni de service distribué (DDoS) sont en augmentation et ont évolué vers des questions de sécurité complexes et démesurées pour les entreprises. Bien que les attaques DDoS ne soient pas un phénomène récent, les méthodes et ressources disponibles pour mener et camoufler ces attaques ont considérablement progressé. Une étape importante de l'évolution des attaques DDoS est la formation du botnet Mirai. Celui-ci se composait de plus de 300 000 appareils IoT piratés pour générer l'attaque DDoS la plus importante connue à l'heure actuelle, dont le pic de trafic d'attaque a dépassé un débit d'1 Tbit/s. Les attaques de cette ampleur deviennent monnaie courante.

Les attaques DDoS ne sont généralement pas des événements exceptionnels, et les victimes sont souvent visées plusieurs fois par an. D'après l'expérience de Cloudflare, tout le monde, c'est-à-dire tant les petites que les grandes entreprises, peut être visé. Même si de nombreuses juridictions disposent de lois définissant les attaques DDOS comme illégales, des fournisseurs DDOS-as-a-Service proposent des abonnements, dont certains pour seulement 5 ou 10 $/mois.

La perte de revenus ne constitue que l'une des nombreuses menaces que ce type d'attaque peut faire peser sur votre site web ou votre entreprise. Même le site web d'Amazon (99 milliards de dollars de recettes provenant de la vente au détail en 2015) a connu plusieurs temps d'arrêt dans le passé pour des raisons inconnues. À titre d'exemple, en 2013, Amazon.com a été arrêté pendant environ 15 à 45 minutes, générant pour la société une perte de ventes de l'ordre de 1,8 à 5,3 millions de dollars, sur la base des ventes moyennes de la société de 117 882 $ par minute. En outre, des inconvénients tels que l'inaccessibilité du site génèrent des pertes moins facilement quantifiables, comme la mise à mal de la réputation de la marque et le mécontentement du client.

Solution DDoS évolutive et précise

Le réseau anycast™ global de 10 Tbits/s de Cloudflare est 10x plus grand que la plus importante des attaques DDoS jamais enregistrées, ce qui permet à toutes les ressources Internet du réseau de Cloudflare de résister à d'énormes attaques DDoS modernes. La protection DDoS de Cloudflare pour les couches 3, 4 et 7 est disponible sous forme de service au niveau du périmètre du réseau, ce qui correspond à l'ampleur des menaces modernes, et peut permettre d'atténuer les attaques DDoS de toutes formes et tailles. La limitation du débit complète la protection DDoS de Cloudflare en contribuant à l'atténuation précise des attaques les plus sophistiquées contre la couche d'application.

PROTECTION CONTRE LES ATTAQUES DDOS DES COUCHES 3 ET 4

Les attaques DDOS des couches 3 et 4 sont généralement des attaques volumétriques, telles que les attaques d'amplification DDoS, par inondation DDoS et par inondation SYN DDOS. Alors que ces attaques peuvent surcharger un réseau monodiffusion classique, le réseau Anycast de Cloudflare accroît la surface par nature en propageant le trafic de l'attaque vers chacun des plus de 102 datacenters Cloudflare et vers un ensemble divers d'interconnexions haut débit avec d'autres réseaux pour simplement absorber le trafic de l'attaque.

Fonctions de protection DDoS

- Protection DDoS des couches 3, 4 et 7
- Protection contre une attaque DNS
- Blocage de menace subtile avec la limitation du débit
- Sécurité prédictive avec base de données de réputation IP

« Lorsque l'on sait que l'on n'a pas à se soucier des attaques DDoS à l'encontre de nos API et serveurs de passerelle, on peut se concentrer en toute quiétude sur l'amélioration de notre produit. »

- Jake Heinz, Ingénieur logiciel chez Discord

Réseau de Cloudflare

- Réseau Anycast™ global de plus de 102 datacenters
- Débit de 10 Tbits/s permettant d'absorber des attaques volumétriques
- 6 millions de propriétés Internet
- Tarification de la bande passante au forfait

« Pourquoi utilisons-nous Cloudflare ? Parce que les fonctions de sécurité sont excellentes, parce que le CDN offre des performances élevées et parce que le fait que ces solutions soient fournies ensemble est vraiment pratique. Cloudflare simplifie la gestion et nous permet de nous concentrer sur nos principales activités. »

-Amanda Kleha GM, Unité des services en ligne de Zendesk

PROTECTION CONTRE LES VULNÉRABILITÉS D'APPLICATION DE LA COUCHE 7

Les types courants d'attaques de la couche 7 comprennent notamment l'injection SQL et les scripts de site à site (XSS), qui peuvent permettre aux agresseurs d'accéder aux données des clients ou à tout autre type de données d'application, et de s'en servir. Cloudflare élimine ces menaces grâce à son pare-feu d'applications web (WAF). Le WAF bloque automatiquement les menaces détectées dans l'ensemble des 10 principales règles OWASP, les ensembles de règles d'application de Cloudflare, ainsi que dans les règles personnalisées créées par la communauté/les clients. Cloudflare peut protéger ses clients contre les principales vulnérabilités zero-day, notamment la vulnérabilité Shellshock et le bogue Heartbleed.

LIMITATION DU DÉBIT

Activez la limitation du débit de Cloudflare pour bénéficier d'un contrôle du trafic subtil en plus des services de protection DDoS et du pare-feu d'applications web (WAF) de Cloudflare. La limitation du débit protège des attaques par déni de service, des tentatives d'attaque de mot de passe par force brute et d'autres types de comportement abusif visant la couche d'application. Configurez des seuils de requête, définissez des réponses personnalisées, telles que l'atténuation des actions (défis ou CAPTCHAS) ou des codes de réponse, et l'obtention d'informations analytiques à des points terminaux de votre site web, application ou API.

Sécurité prédictive

Cloudflare propose une plateforme d'apprentissage automatique, où le trafic réseau est analysé en temps réel pour identifier des requêtes anormales ou malveillantes. Une fois qu'une nouvelle attaque est identifiée, Cloudflare commence automatiquement à bloquer ce type d'attaque pour le site web en particulier et l'ensemble de la communauté. Étant donné que Cloudflare continue de développer son réseau et sa communauté, il devient de plus en plus difficile de lancer une attaque DDoS efficace contre les utilisateurs de Cloudflare.

Tarification de la bande passante au forfait

Cloudflare offre une protection DDoS illimitée à l'échelle de l'entreprise pour un forfait mensuel. Cloudflare pense que les utilisateurs ne doivent pas être pénalisés pour le pic du trafic réseau associé à une attaque DDoS. Grâce à la protection DDoS de Cloudflare, les utilisateurs ont la garantie que leur site web reste en ligne et que leur facture mensuelle est prévisible.

Inscription à Cloudflare

Inscrivez-vous auprès de Cloudflare et activez la limitation du débit pour protéger votre site web, application ou API des attaques DDoS, tout en réduisant la latence et en bénéficiant des technologies web les plus récentes. La configuration est aisée et prend généralement moins de 5 minutes. Consultez les plans, de l'offre gratuite à l'offre entreprise sur www.cloudflare.com.