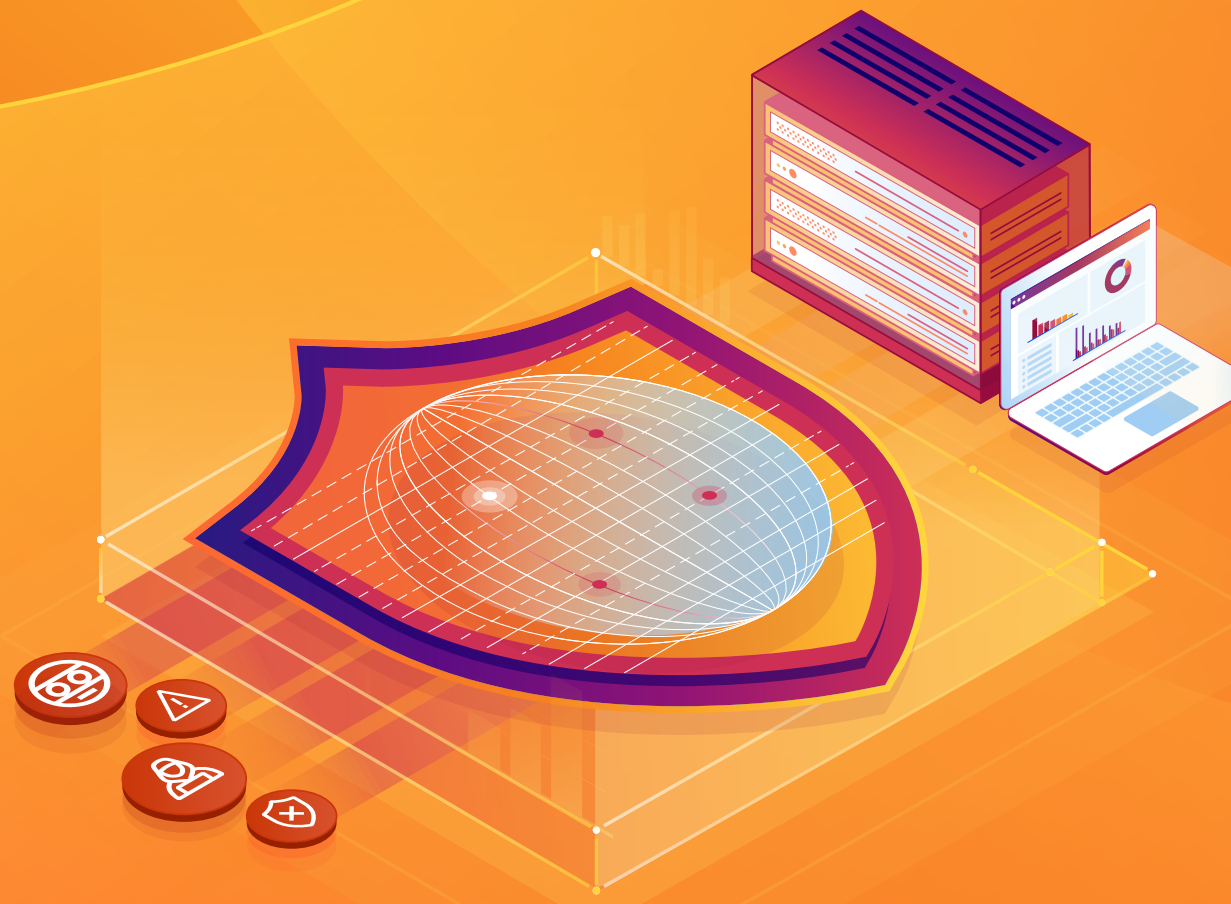
CLOUDFLARE

Rapport Cloudflare sur les tendances des attaques DDoS



Contenu

Quatrième trimestre 2023

Synthèse

Bienvenue dans la seizième édition du rapport Cloudflare consacré aux menaces DDoS. Les attaques DDoS, pour Distributed Denial-of-Service (déni de service distribué), constituent un type de cyberattaque visant à perturber les sites web (et d'autres types de propriétés Internet). Elles ont pour objectif de rendre ces derniers indisponibles aux utilisateurs légitimes en les submergeant sous un trafic excessif. Par analogie, l'opération ressemble à ce qui se passerait si quelqu'un devait causer un embouteillage sur une route indispensable, afin d'empêcher les usagers d'atteindre leur destination.

Notre réseau, l'un des plus grands du monde, couvre plus de 310 villes réparties dans plus de 120 pays. Nous manipulons une quantité énorme de trafic Internet, avec la diffusion de plus de 70 millions de requêtes web par seconde en pic et le traitement de 2,6 milliards de requêtes DNS chaque jour. En moyenne, nous déjouons quotidiennement 170 milliards de cybermenaces. Ce vaste volume de données nous assure un point de vue unique sur le panorama des menaces DDoS, qui nous permet en retour de partager des statistiques et tendances utiles avec la communauté de la cybersécurité.

Ces dernières semaines, nous avons observé une brusque hausse des attaques DDoS et des autres cyberattaques suite aux élections générales taïwanaises qui viennent de se terminer et ont entraîné des tensions avec la Chine. Parallèlement, alors que le conflit militaire entre Israël et le Hamas se poursuit, les sites web palestiniens et israéliens font face à un nombre considérablement plus élevé d'attaques DDoS.

Sur une base annuelle, les attaques DDoS sur la couche applicative ont chuté de 20 % en 2023 par rapport à 2022. Ironiquement, l'année 2023 a également vu le plus grand nombre de campagnes d'attaques DDoS sur cette couche dépasser les 100 millions de requêtes par seconde sur plusieurs instances, notamment la campagne d'attaques HTTP/2 Rapid Reset observée plus tôt cette année. Au niveau de la couche réseau, nous avons constaté une tendance radicalement différente, avec une augmentation de 85 % des attaques DDoS sur cette couche en 2023 par rapport à 2022.

Fait remarquable, les entreprises de services environnementaux ont enregistré le plus fort volume de trafic hostile lié à des attaques DDoS HTTP, cette dynamique coïncidant avec la 28e Conférence des Nations unies sur les changements climatiques (COP 28).

Une version interactive de ce rapport est également disponible sur Cloudflare Radar.

Points clés du rapport

Les tendances de l'année 2023 en matière d'attaques DDoS

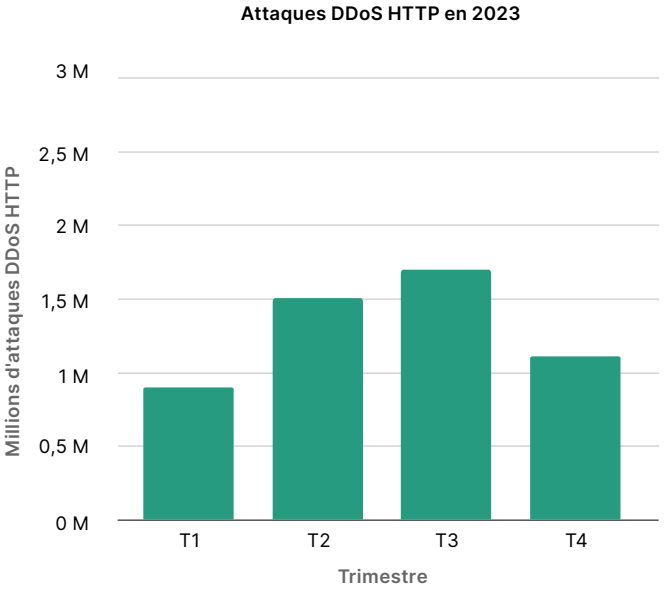
Après cette campagne d'attaques hyper-volumétriques, nous avons constaté une chute inattendue du nombre d'attaques DDoS HTTP, avec 20 % d'attaques en moins par rapport à 2022. Dans l'ensemble, sur l'année 2023, nos défenses automatisées ont atténué plus de 5,2 millions d'attaques DDoS HTTP, totalisant plus de 26 000 milliards de requêtes. Malgré la baisse du nombre d'attaques, le nombre moyen d'attaques bloquées s'avère très important, avec 594 attaques DDoS HTTP stoppées et trois milliards de requêtes atténuées par heure en 2023.

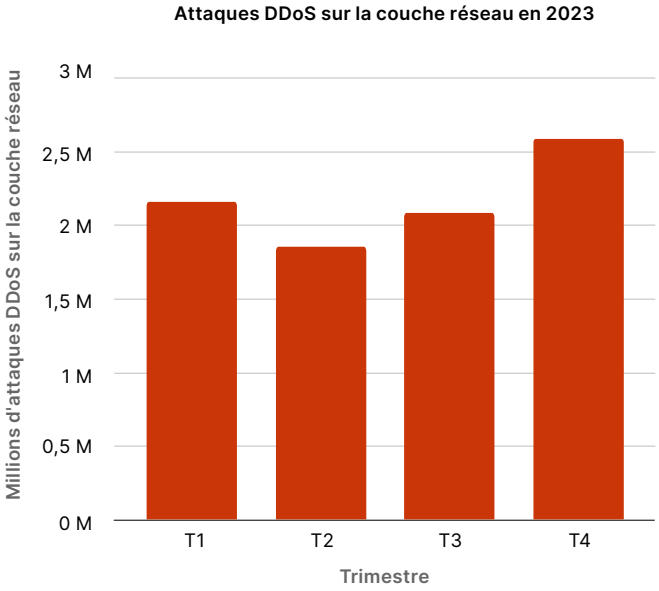
Nous avons observé une tendance complètement différente au niveau de la couche réseau. Nos défenses automatisées ont ainsi atténué 8,7 millions d'attaques DDoS sur la couche réseau en 2023. Ce chiffre représente une augmentation de 85 % par rapport à 2022. En moyenne, nos systèmes ont atténué 996 attaques DDoS sur la couche réseau et 27 téraoctets par heure.

2023 — Les attaques DDoS en chiffres

Attaques DDoS HTTP
5,2 millions d'attaques atténuées en 2023
-20 % par rapport à l'année précédente

Attaques DDoS sur la couche réseau
8,7 millions d'attaques atténuées en 2023
+85 % par rapport à l'année précédente





Zones de conflit spécifiques et attaques DDoS : les élections générales taïwanaises et le conflit entre Israël et le Hamas

La hausse des attaques visant des régions spécifiques (Taïwan, Israël et les territoires palestiniens) souligne l'utilisation des attaques DDoS en tant qu'arme dans le cadre de la cyberguerre, dont l'objectif consiste à tirer parti de ses capacités informatiques pour exercer des pressions politiques ou perturber les infrastructures numériques essentielles.

Élections générales taïwanaises

Par rapport à l'année dernière, nous avons relevé une hausse de 3 370 % du nombre d'attaques DDoS HTTP visant les sites web taïwanais. La vaste majorité d'entre elles (82 %) provenaient de Chine, un point qui coïncide tout à fait avec la rhétorique politique enflammée faisant rage entre la Chine et Taïwan à l'heure actuelle. Fait surprenant, les sites de divertissement pour adultes ont davantage été visés que les secteurs couramment ancrés dans le quotidien, comme les services financiers, les soins de santé et les transports.

La guerre entre Israël et le Hamas

Les attaques DDoS sont un instrument de guerre et de perturbation largement accepté. Nous avons constaté une hausse de l'activité DDoS lors de la guerre russo-ukrainienne et observons actuellement le même phénomène au cours de la guerre entre Israël et le Hamas. Nous avons signalé cette cyberactivité pour la première fois dans notre article de blog intitulé Les cyberattaques dans la guerre entre Israël et le Hamas et continuons de la surveiller aujourd'hui.

Les territoires palestiniens ont été la deuxième région la plus touchée par les attaques DDoS HTTP et visant la couche réseau au quatrième trimestre. Les attaques DDoS totalisaient plus de 68 % de l'ensemble du trafic de couche 3 et 4 destiné aux réseaux palestiniens et plus de 10 % de l'ensemble des requêtes HTTP adressées aux sites web palestiniens. Sur l'ensemble de ces attaques DDoS, 9 sur 10 ciblaient des sites web bancaires palestiniens.

Les sites web israéliens ont également fait l'objet d'un trafic DDoS particulièrement dense, mais n'ont connu qu'une modeste hausse de 27 % du trafic DDoS HTTP par rapport au trimestre précédent. Les secteurs de la presse et des médias, de même que celui des logiciels, ont fait les frais de près de 65 % de l'ensemble des attaques DDoS HTTP à l'encontre des sites israéliens.

Nos données suggèrent un effort concerté visant à nuire aux secteurs ancrés dans la vie quotidienne des deux camps.

Tendance croissante : les événements politiques internationaux en tant que facteur déclencheur de cyberattaques

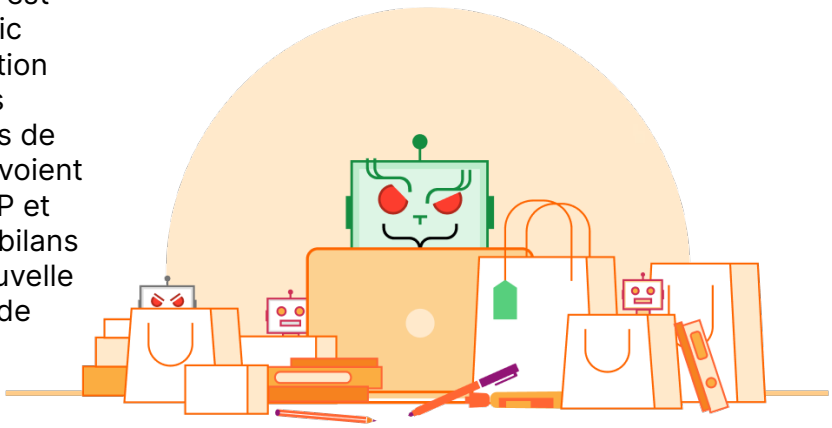
Une tendance croissante que nous avons pu observer montre que les événements internationaux peuvent devenir un facteur déclencheur pour les cyberattaques. La 28e Conférence des Nations unies sur les changements climatiques (plus connue sous le nom de COP 28) s'est terminée le 13 décembre 2023. Nous avons constaté une augmentation ahurissante (plus de 61 000 %) du nombre d'attaques DDoS HTTP à l'encontre des entreprises de services environnementaux entre octobre et décembre 2023, par rapport à la même période en 2022. Ce schéma ne s'est d'ailleurs pas cantonné à ce seul événement.

Après réexamen des données historiques, notamment autour de la COP 26 et de la COP 27, ainsi que des autres résolutions ou annonces de l'ONU liées à l'environnement, un schéma similaire émerge. Chacun de ces événements s'est accompagné d'une augmentation correspondante des cyberattaques à l'encontre des sites web de services environnementaux.

Période des fêtes du quatrième trimestre : le Grinch DDoS

Nous avons observé un accroissement de l'activité DDoS HTTP à l'encontre des sites de vente, d'expédition et de relations publiques entre Black Friday, Noël et les fêtes de fin d'année. Au niveau de la couche applicative, le secteur de la livraison de colis/fret s'est avéré le deuxième plus touché (après celui des services environnementaux) par rapport au trafic HTTP global de chaque secteur. Ce secteur sous-tend le succès de l'expérience d'achat au moment de Black Friday et de la période des fêtes. Les cadeaux et les biens achetés doivent en effet atteindre leur destination avec précision et en temps opportun. Les acteurs malveillants pourraient avoir essayé d'interférer dans ce processus. Les attaques DDoS sur la couche applicative visant les entreprises de commerce ont également augmenté de 16 % par rapport à l'année précédente, 2022.

Concernant les attaques sur la couche réseau, c'est le secteur des relations publiques (RP) et de la communication qui s'est révélé le plus touché, avec 36 % de son trafic identifié comme malveillant. Toute perturbation des opérations de ce secteur peut avoir des effets immédiats et considérables en termes de réputation. Les mois d'octobre à décembre voient souvent un accroissement de l'activité de RP et de communication en raison des fêtes, des bilans de fin d'année et des préparatifs pour la nouvelle année. En résumé, il s'agit donc d'une période essentielle sur le plan opérationnel, que les acteurs malveillants aimeraient perturber.

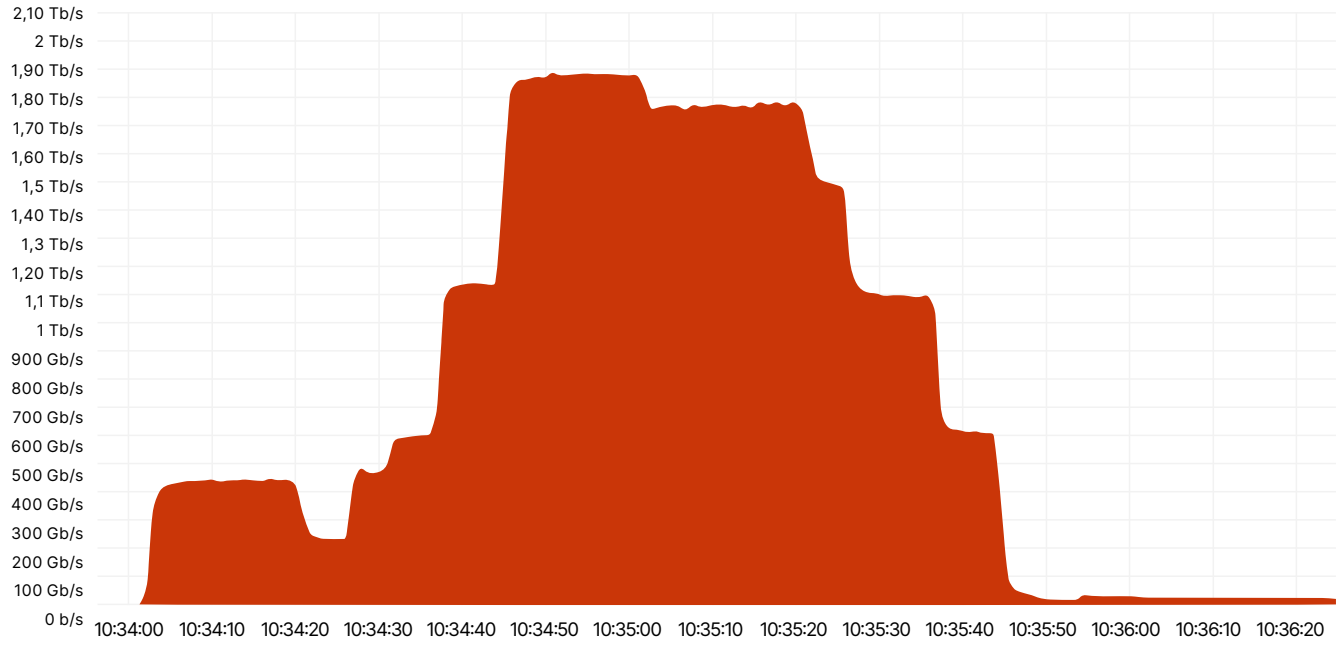


Les vecteurs d'attaque émergents sur la couche réseau

Examinons une attaque spécifique afin d'explorer le panorama changeant des attaques DDoS sur la couche réseau.

L'une des attaques les plus volumineuses survenues entre les mois d'octobre et de décembre 2023 était une attaque par botnet Mirai visant un célèbre fournisseur de cloud européen et provenant de plus de 18 000 adresses IP uniques (supposément usurpées). Elle a été automatiquement détectée et atténuée par les défenses de Cloudflare.

Une attaque par botnet Mirai d'envergure à l'encontre d'un fournisseur de cloud européen

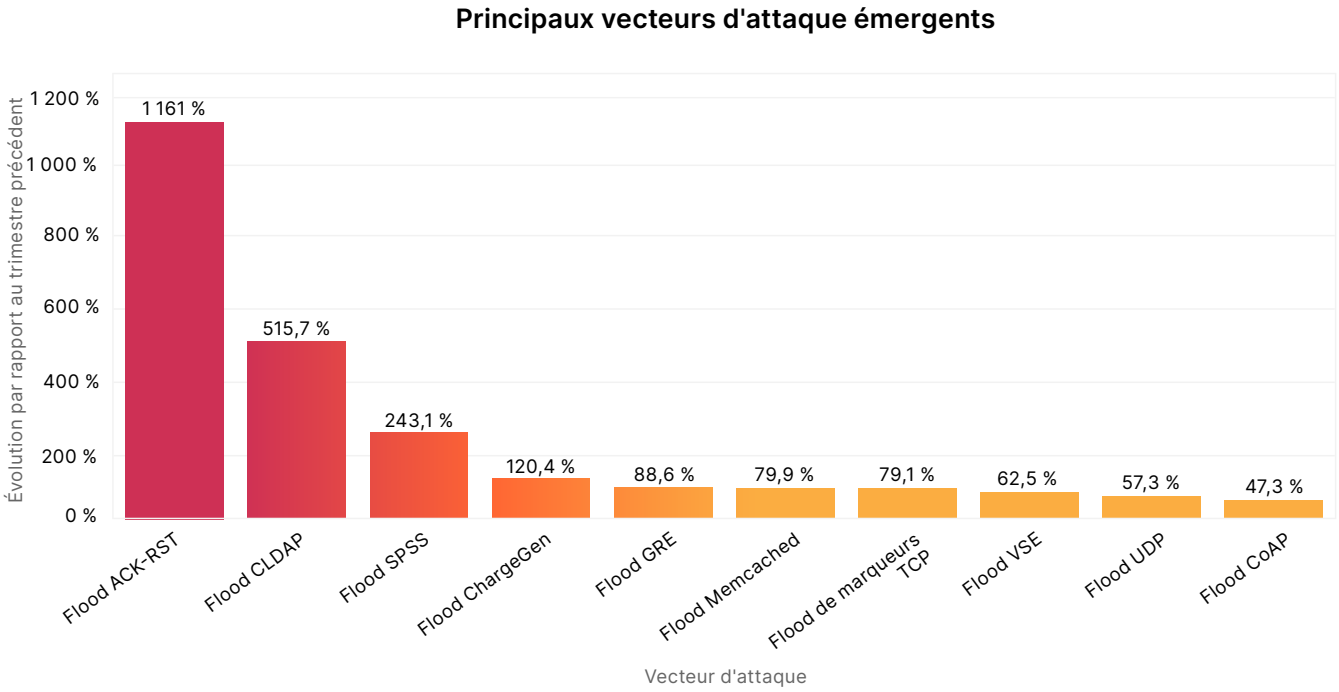


Cette attaque était unique de par son débit élevé de bits par seconde et sa nature d'attaque multivectorielle, mais elle n'a pourtant eu qu'une courte durée d'activité. Culminant à 1,9 térabits par seconde, elle associait plusieurs méthodes d'attaque, dont le flood de fragments UDP, le flood UDP/Echo, le flood SYN, le flood ACK et les marqueurs TCP mal formés. Les attaques affichant un débit aussi élevé de bits par seconde sont rares. Le fait qu'une attaque combine plusieurs méthodes s'avère d'autant plus sophistiqué.

À 160 millions de paquets par seconde, le débit de paquets n'était pas le plus imposant que nous ayons jamais observé, ce dernier ayant été enregistré à 754 millions de paquets par seconde en 2020.

Au-delà de cette attaque aux caractéristiques uniques, les entreprises ne peuvent se permettre de recourir à des centres de nettoyage manuels pour leur protection contre les attaques DDoS. Elles ont besoin de systèmes de défense automatisés et intégrés (in-line).

Parmi les menaces émergentes que nous suivons, nous avons enregistré une augmentation de 1 164 % des attaques par flood ACK-RST, une hausse de 515 % des attaques par flood CLDAP et un accroissement de 243 % des attaques par flood SPSS, le tout par rapport au trimestre précédent. Intéressons-nous plus en détail à certaines de ces attaques afin de découvrir de quelle manière elles sont conçues pour provoquer des perturbations.



Flood ACK-RST

Une attaque par ACK-RST exploite le protocole TCP (Transmission Control Protocol, protocole de contrôle des transmissions) en envoyant de nombreux paquets ACK et RST à la victime. Cette opération submerge la victime et l'empêche de traiter ces paquets et d'y répondre, afin de conduire une perturbation de service. Cette attaque est efficace, car chaque paquet ACK ou RST provoque une réponse du système de la victime et consomme ainsi ses ressources. Les floods ACK-RST se révèlent bien souvent difficiles à filtrer, car ils imitent le trafic légitime et compliquent ainsi la détection et l'atténuation.

Flood CLDAP

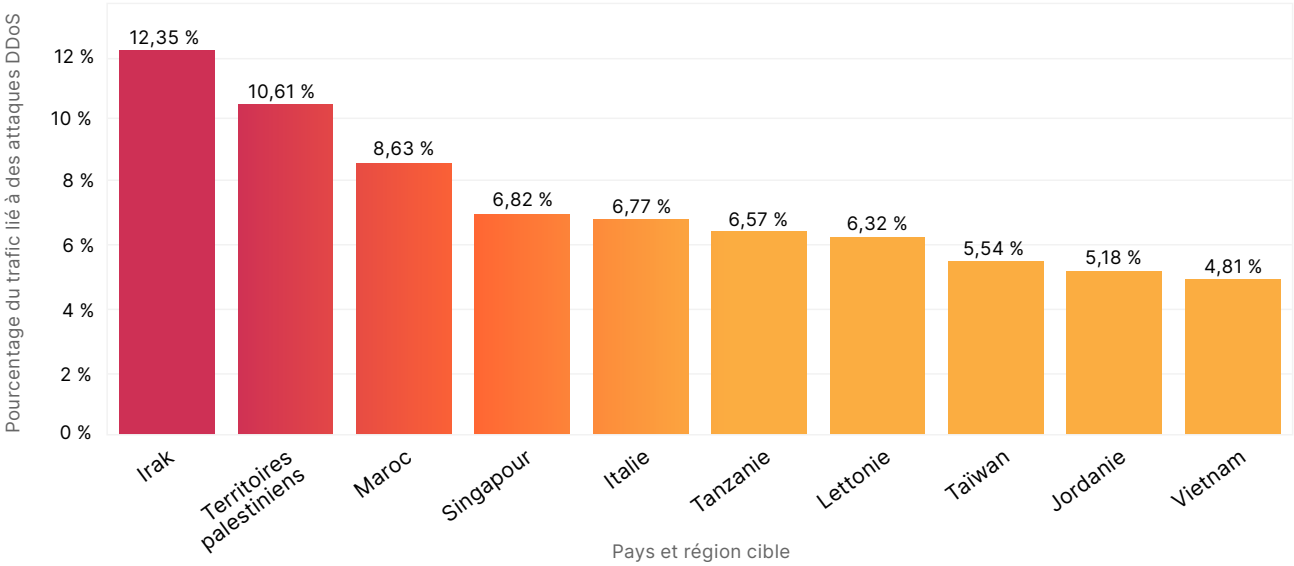
Le protocole CLDAP (Connectionless Lightweight Directory Access Protocol, protocole d'accès aux répertoires léger et sans connexion) est une variante du LDAP (Lightweight Directory Access Protocol). Il sert à interroger et à modifier les services de répertoire exécutés sur des réseaux IP. Comme le CLDAP est sans connexion et utilise le protocole UDP plutôt que le TCP, il est plus rapide, mais moins fiable. Comme il s'appuie sur l'UDP, il ne comporte aucune exigence de négociation préalable. Les acteurs malveillants peuvent donc usurper l'adresse IP et l'exploiter comme vecteur de réflexion. Ces attaques envoient des requêtes de petite taille accompagnées d'une adresse IP source usurpée (l'adresse IP de la victime) dans le but d'amener les serveurs à renvoyer des réponses de grand volume à la victime, afin de la submerger. Les stratégies d'atténuation à mettre en œuvre impliquent le filtrage et la surveillance du trafic CLDAP inhabituel.

Flood SPSS

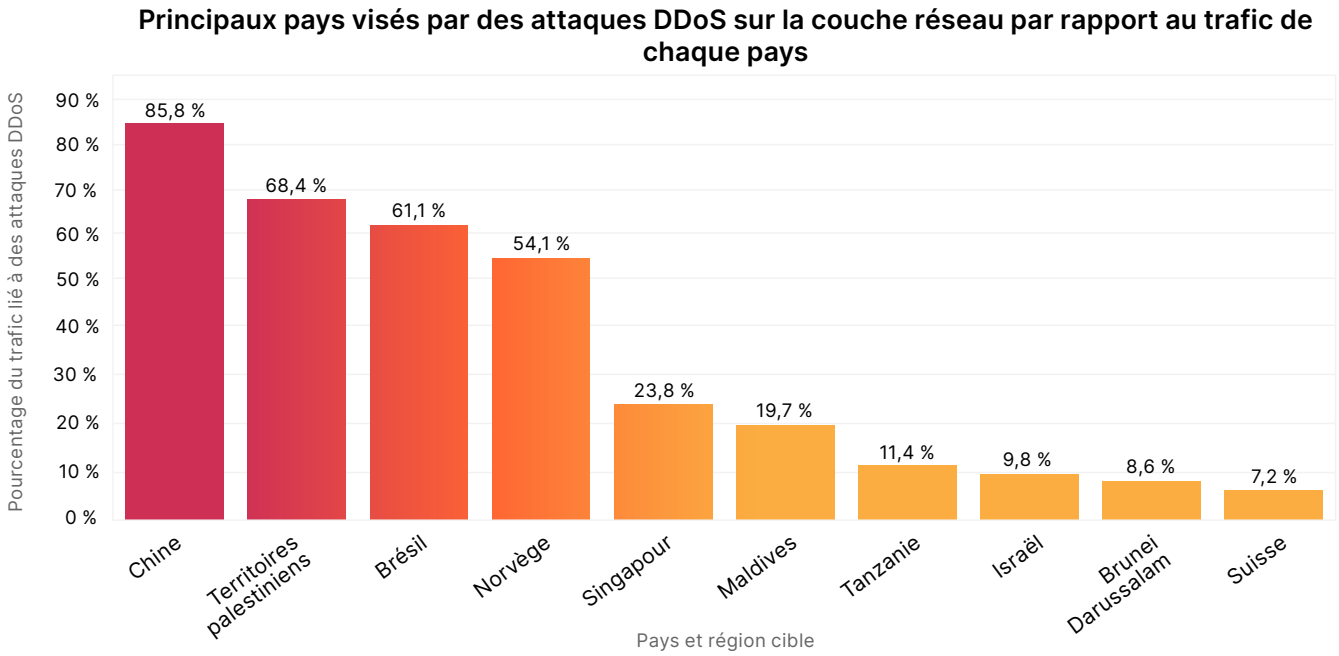
Les attaques flood abusant du protocole SPSS (Source Port Service Sweep) constituent une méthode d'attaque réseau impliquant l'envoi de paquets à partir d'un grand nombre de ports sources usurpés ou aléatoires vers divers ports de destination du système ou du réseau ciblé. L'objectif de cette attaque est double. En premier lieu, submerger les capacités de traitement de la victime, afin de provoquer des perturbations de service ou une défaillance du réseau, et en second lieu, rechercher les ports ouverts et identifier les services vulnérables. Le flood s'effectue en envoyant un volume élevé de paquets afin de saturer les ressources réseau de la victime et d'épuiser les capacités de ses pare-feu et de ses systèmes de détection des intrusions. Pour atténuer ce type d'attaque, il est essentiel de faire appel à des fonctionnalités de détection automatisées et intégrées (in-line).

Principales régions visées

Principaux pays visés par des attaques DDoS HTTP par rapport au trafic de chaque pays



L'Irak, les territoires palestiniens et le Maroc prennent la tête en tant que régions les plus attaquées par rapport à leur trafic entrant total. Le point intéressant est que Singapour arrive en quatrième position. Singapour a donc non seulement fait face à la plus grande quantité de trafic hostile en lien avec des attaques DDoS HTTP (4 % de l'ensemble du trafic DDoS mondial), mais ce trafic malveillant constituait également une part significative du trafic HTTP total destiné à la ville. À l'inverse, les États-Unis étaient le deuxième pays le plus attaqué par volume de trafic DDoS (3,8 % de l'ensemble du trafic DDoS mondial), mais arrivaient en quinzième position une fois ce volume normalisé par rapport au trafic HTTP total destiné aux États-Unis.



Les tendances en matière d'attaques sur la couche réseau par région sont encore plus frappantes que pour la couche applicative.

La Chine continue d'être le pays le plus visé par les attaques sur la couche réseau en 2023. Fait encore plus spectaculaire que les tendances en matière d'attaques DDoS HTTP contre Singapour, la Chine est à la fois le pays le plus visé par le trafic hostile DDoS sur la couche réseau, mais également par rapport à l'ensemble du trafic destiné à la Chine. Près de 86 % de ce dernier a été atténué par Cloudflare, car en lien avec des attaques DDoS sur la couche réseau. Pour les trois régions suivantes, les territoires palestiniens, le Brésil et la Norvège, plus d'un bit sur deux adressé au pays entrait dans le cadre d'une attaque DDoS.

Recommandations et points à retenir

Bonnes pratiques	Optimiser votre utilisation de Cloudflare
Mettre à jour ou définir un plan de réponse en cas de déni de service	Vous souhaitez vous assurer que votre prestataire de sécurité propose une assistance d'urgence disponible 24 h/24, 7 j/7. Le service d'assistance en cas d'attaque de Cloudflare déploiera son expertise en matière de sécurité, ses processus et sa technologie afin de traiter les attaques en temps réel. Testez les processus de réponse aux incidents et les contrats de niveau de service (SLA, Service Level Agreements) de vos prestataires de sécurité avant qu'une véritable attaque DDoS ne survienne. Identifiez et formez des collaborateurs à votre propre plan documenté de réponse aux attaques DDoS. Assurez-vous qu'ils lisent les documents consacrés aux attaques DDoS de notre parcours d'apprentissage afin d'optimiser les mesures de contrôle de Cloudflare.
Déployer un système d'information sur les menaces et des solutions d'atténuation des attaques DDoS intégrées (in-line) et automatisées Les centres de nettoyage manuels ne peuvent lutter contre les attaques modernes à volume élevé et de courte durée	Utilisez plusieurs techniques de détection pour optimiser votre stratégie de sécurité face à un panorama des menaces en évolution constante : 1. Analyse des empreintes numériques sans état 2. Classification basée sur l'apprentissage automatique 3. Détection du trafic anormal 4. Profilage du trafic et atténuation avec état 5. Informations sur l'activité et les tendances actuelles des attaques DDoS
Mettre à jour votre infrastructure réseau, DNS et applicative afin qu'elle soit plus résiliente pour votre profil de trafic	Assurez-vous que la capacité de votre solution d'atténuation des attaques DDoS est suffisante pour traiter deux fois la taille des attaques les plus volumineuses jamais enregistrées et deux fois le débit maximal de votre trafic légitime. Veillez à ce que votre prestataire de sécurité puisse atténuer les dernières vulnérabilités des protocoles régissant la couche réseau et la couche applicative. Déchargez le trafic DNS vers des plateformes cloud conformes aux normes et sécurisées, dont le trafic est routé via des réseaux de périphérie situés au plus près de l'utilisateur.
Améliorer les performances de votre réseau et de vos applications afin d'éviter les engorgements	Tirez parti d'une file d'attente numérique pour vous assurer que vos utilisateurs véritables et vos visiteurs soient aimablement informés du délai d'attente sans surcharger vos serveurs d'applications. Optimisez la mise en cache et gérez mieux les charges grâce à un réseau de diffusion de contenu (CDN) et à des solutions d'équilibrage de charge basées sur le cloud.
Utiliser un modèle de sécurité positive, en vous assurant que le trafic que vous souhaitez recevoir soit acheminé de manière fiable	Maintenez les protocoles, les adresses IP, les ASN, les ports et les agents-utilisateur essentiels à l'activité ouverts au trafic légitime. Utilisez la validation de schéma et une passerelle d'API pour gérer le trafic lié aux API.
Tirer parti de l'intelligence artificielle pour garder une longueur d'avance sur les menaces émergentes.	Vous pouvez utiliser les scores de bot dans vos règles de pare-feu et de contrôle du volume de requêtes. Identifiez automatiquement vos API en contact avec le public et protégez-les contre les attaques DDoS.

Chez Cloudflare, nous souhaitons qu'il soit encore plus simple (et gratuit) pour les entreprises de toutes tailles de se protéger, même contre les attaques DDoS les plus volumineuses et les plus complexes. Nous proposons une protection anti-DDoS gratuite et totalement illimitée à l'ensemble de nos clients depuis 2017, année du lancement de ce concept.

Apprenez-en davantage sur la manière de vous protéger contre les dernières menaces DDoS grâce à Cloudflare.

+33 7 57 90 52 73 | enterprise@cloudflare.com | www.cloudflare.com/fr-fr/

RÉV. : BDES-5497.2024FEB08