CLOUDFLARE

État des lieux en matière de menaces DDoS : troisième trimestre 2023

Contenu

Synthèse

Bienvenue dans le troisième rapport consacré aux menaces DDoS de 2023. 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 300 villes réparties dans plus de 100 pays. Nous nous occupons d'une quantité énorme de trafic Internet, avec la diffusion de plus de 64 millions de requêtes web par seconde en pic et le traitement de 2,3 milliards de requêtes DNS chaque jour. En moyenne, nous déjouons quotidiennement 140 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 coïncidant avec la reprise du conflit israélo-palestinien. Nous avons décidé de proposer nos services gratuitement pour soutenir les efforts humanitaires pendant cette période difficile. Nos pensées vont à tous ceux qui s'efforcent de ramener la paix au Moyen-Orient.

Cloudflare a atténué avec succès des milliers d'attaques DDoS HTTP à volume élevé. Parmi ces attaques, 89 ont notablement dépassé les 100 millions de requêtes par seconde (r/s), la plus volumineuse culminant même à 201 millions de r/s, soit un trafic trois fois supérieur à celui de l'attaque record précédente de 71 millions de r/s. Cette campagne a contribué à l'augmentation générale de 65 % du trafic lié aux attaques DDoS HTTP observée au cours du troisième trimestre par rapport au trimestre précédent.

De manière similaire, les attaques DDoS sur les couches 3 et 4 ont augmenté de 14 %, avec de nombreuses attaques atteignant des niveaux de l'ordre du térabit par seconde. L'attaque la plus volumineuse visait le résolveur DNS public de Cloudflare, 1.1.1.1, et a atteint un pic de 2,6 térabits par seconde (Tb/s).

Les entreprises du secteur des jeux/jeux de hasard ont subi le plus gros volume de trafic lié aux attaques DDoS HTTP, détrônant ainsi le secteur des cryptomonnaies qui occupait la première place lors du trimestre précédent.

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

Points clés du rapport

La campagne d'attaques DDoS hyper-volumétriques exploitant la vulnérabilité HTTP/2 Rapid Reset

À partir de la fin août 2023, Cloudflare et d'autres fournisseurs ont commencé à être la cible d'une campagne d'attaques DDoS sophistiquée et persistante exploitant la vulnérabilité HTTP/2 Rapid Reset (CVE-2023-44487).

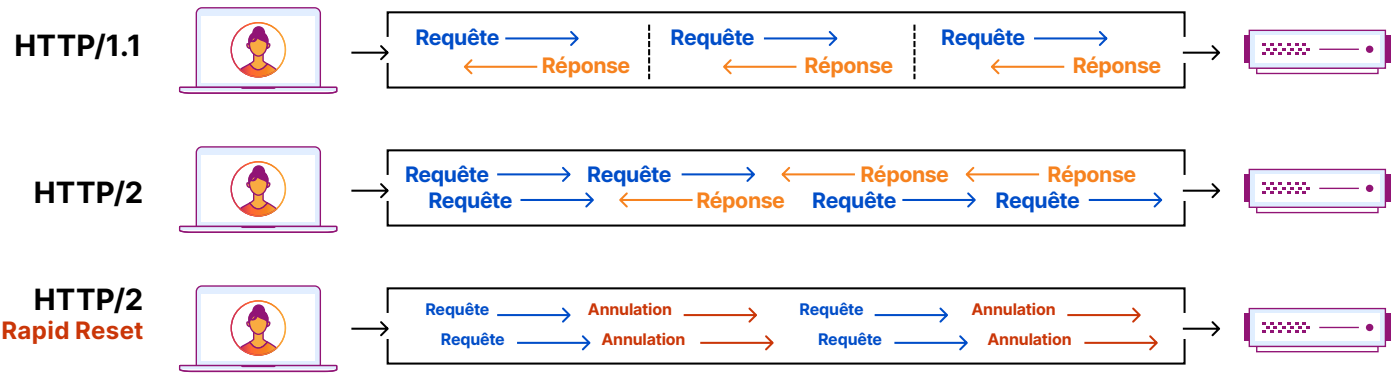
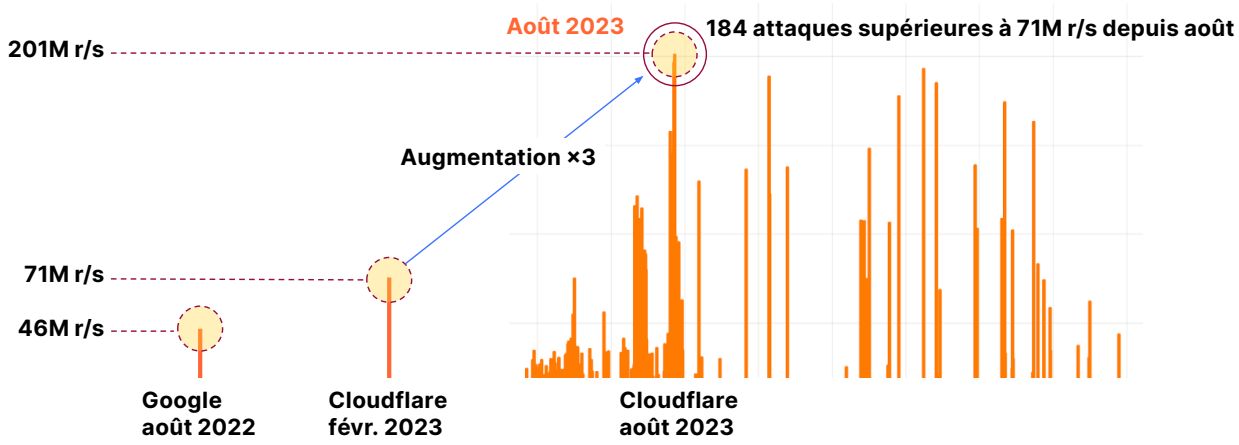


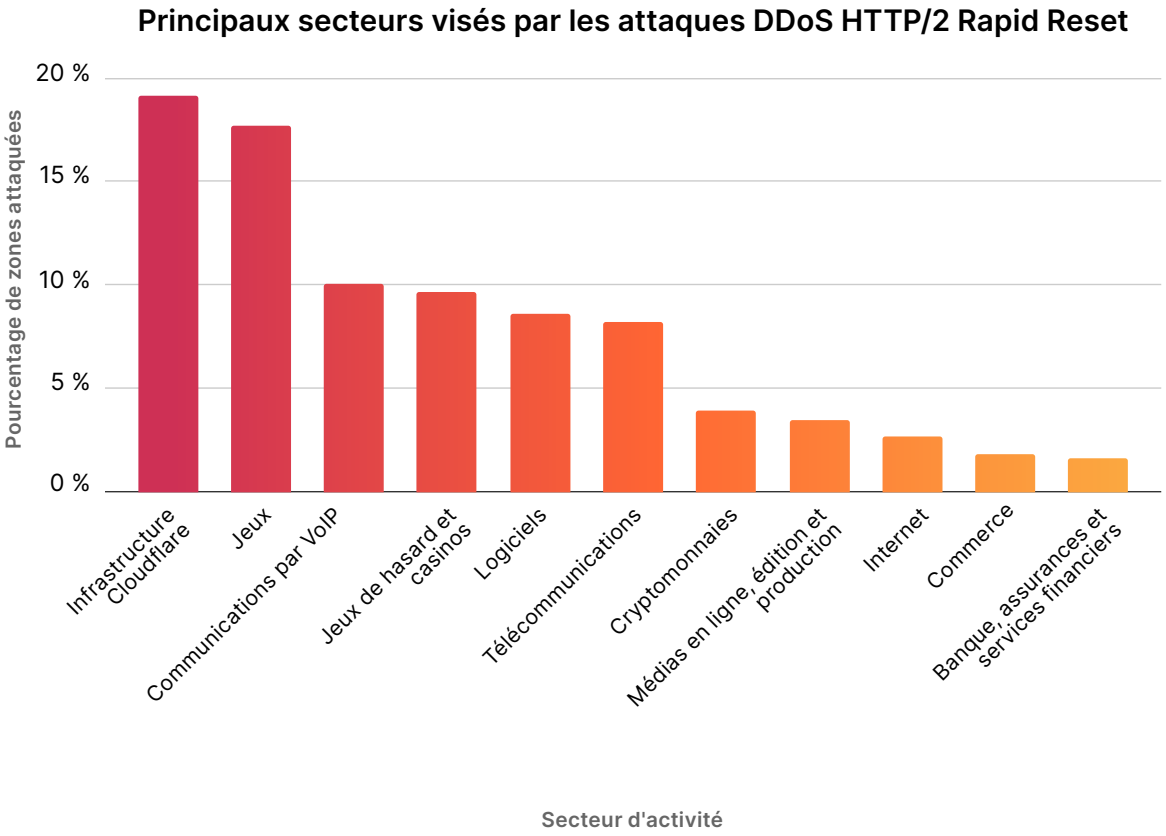
Schéma d'une attaque DDoS HTTP/2 Rapid Reset

La campagne se composait de milliers d'attaques DDoS hyper-volumétriques envoyées via HTTP/2 et culminant à plusieurs dizaines de millions de requêtes par seconde. Le volume moyen d'une attaque était de 30 millions de r/s. Parmi ces attaques, près de 89 dépassaient les 100 millions de r/s, tandis que la plus volumineuse atteignait les 201 millions de r/s.

La campagne d'attaques DDoS hyper-volumétriques HTTP/2 Rapid Reset



L'objectif principal de cette campagne DDoS longue de deux mois portait sur les fournisseurs d'infrastructure cloud, tels que Cloudflare. Plus spécifiquement, 19 % de l'ensemble des attaques ont visé les sites web et l'infrastructure de Cloudflare. 18 % ont visé les entreprises de jeux et 10 % des fournisseurs de VoIP bien connus.

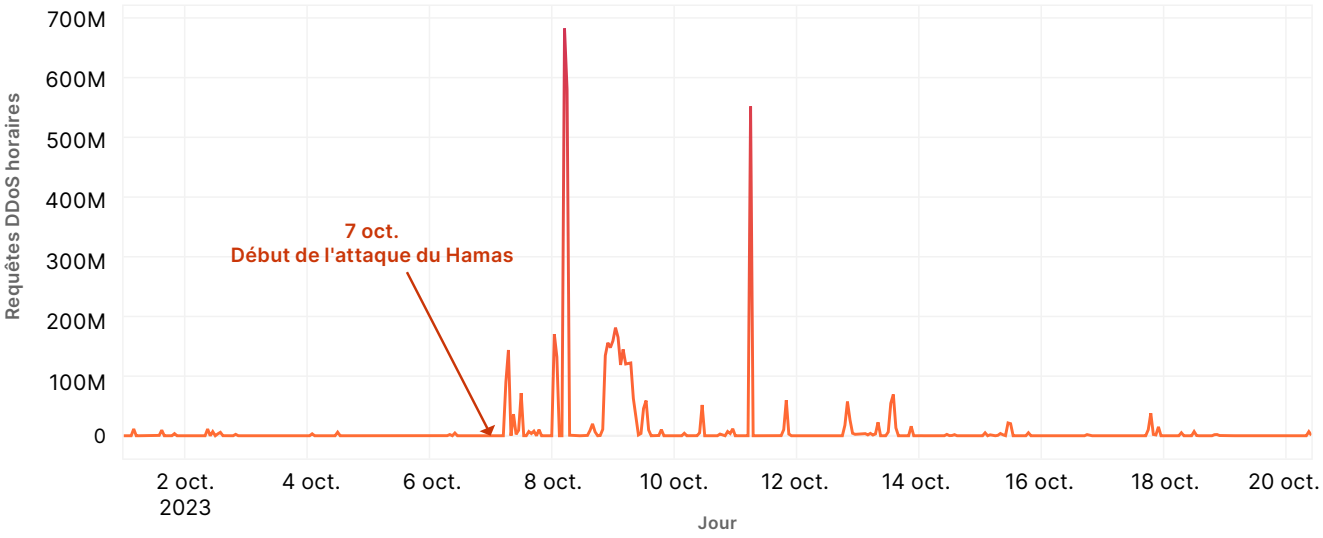


Les cyberattaques dans la guerre entre Israël et le Hamas

Divers groupes d'hacktivistes pro-palestiniens s'en sont pris aux applications mobiles et aux sites web israéliens. Le 14 octobre, nous avons révélé les conclusions d'une enquête réalisée par l'équipe de réponse aux menaces Cloudforce One. Nous avons identifié des applications mobiles Android malveillantes usurpant l'identité de l'application légitime « RedAlert - Rocket Alerts ». Les applications malveillantes ont obtenu un accès non autorisé à des informations sensibles sur les utilisateurs, notamment la liste des contacts du téléphone mobile, les messages SMS, les journaux d'appels et les applications installées, mais aussi des informations sur la carte SIM et le téléphone eux-mêmes. Vous trouverez plus d'informations techniques sur notre enquête ici.

Après l'attaque du 7 octobre lancée par le Hamas, les sites web israéliens ont subi un barrage soutenu d'attaques DDoS dans les jours qui ont suivi. Cloudflare a contribué à l'intégration et la protection de bon nombre de ces sites.

Attaques DDoS HTTP sur la couche applicative à l'encontre des sites web israéliens utilisant Cloudflare



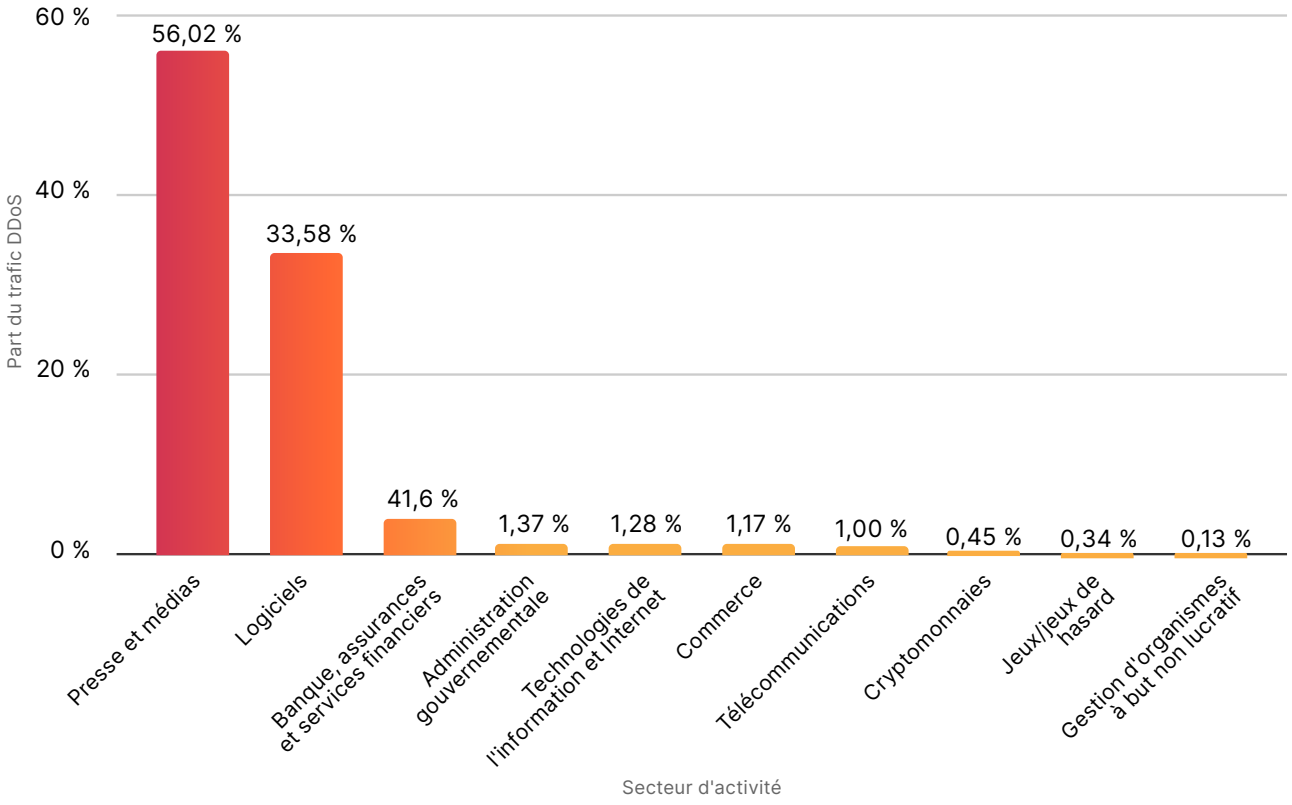
Avant le 7 octobre, nous n'observions qu'une quantité minimale de requêtes liées à une attaque DDoS HTTP contre des sites web israéliens utilisant Cloudflare. Toutefois, la situation a brusquement empiré le 7 octobre, lorsque le pourcentage de trafic lié aux attaques DDoS est grimpé en flèche. Ce jour précis, près d'une requête sur 100 adressée à des sites web israéliens utilisant Cloudflare a été identifiée comme faisant partie d'une attaque DDoS HTTP. Ce chiffre alarmant a quadruplé le 8 octobre.

Depuis l'attaque du 7 octobre, les sites web de la presse et des médias ont été la principale cible des attaques DDoS, en totalisant 56 % de l'ensemble des attaques lancées contre des sites web israéliens. Nous avons observé les mêmes tendances au cours de la guerre russo-ukrainienne, lorsque les sites web des médias et de l'audiovisuel ukrainiens ont été fortement ciblés. Ces dernières années, les conflits terrestres s'accompagnent souvent de cyberattaques contre des sites web fournissant des informations cruciales aux populations civiles.

Le deuxième secteur d'industrie le plus fortement ciblé en Israël était celui des logiciels: Près de 34 % de l'ensemble des attaques DDoS ciblaient des entreprises de développement logiciel. Le secteur de la banque, des assurances et des services financiers (Banking, Financial Services and Insurance, BFSI) se situait notablement à la troisième place. Les sites web des administrations publiques arrivaient en quatrième position.

Principaux secteurs israéliens visés par des attaques DDoS HTTP

(en pourcentage de l'ensemble des attaques DDoS ciblant des ressources web basées en Israël)



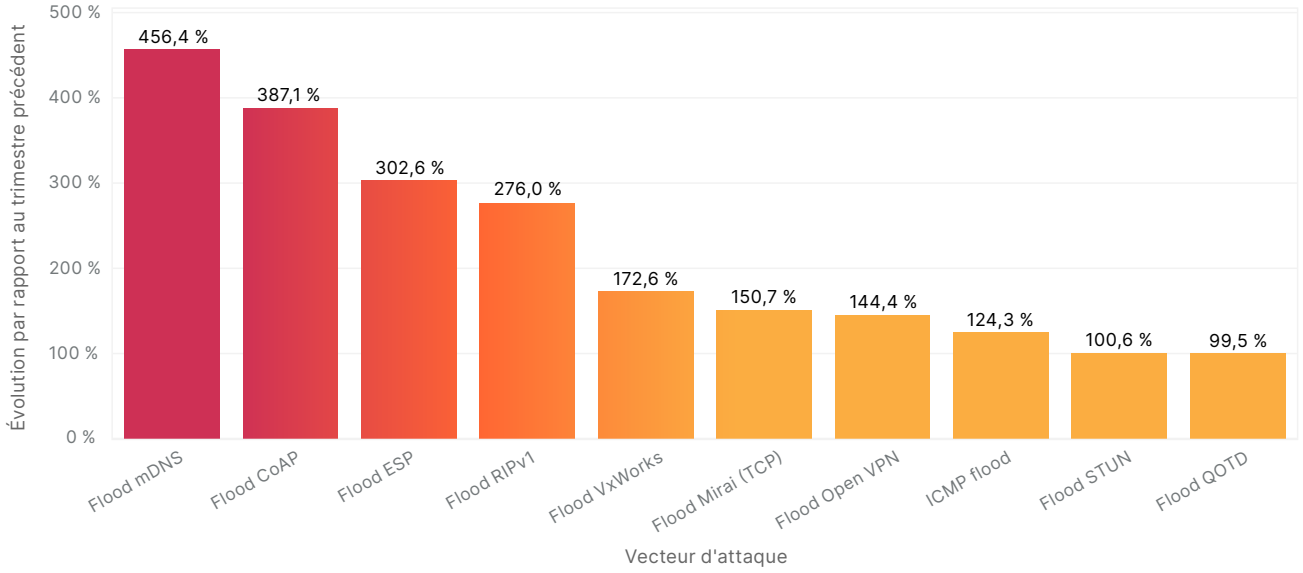
Cyberattaques contre des sites web palestiniens

Pendant la même période, à partir du 1er octobre, Cloudflare a automatiquement détecté et atténué plus de 454 millions de requêtes HTTP liées à des attaques DDoS ciblant des sites web palestiniens utilisant Cloudflare. Si ce chiffre représente à peine un dixième du nombre de requêtes liées à des attaques que nous avons observées contre des sites web israéliens utilisateurs de Cloudflare, il représente une part plus importante du trafic global acheminé vers les sites web palestiniens reposant sur Cloudflare.

Nous n'avons observé aucune attaque DDoS contre des sites web palestiniens utilisant Cloudflare avant l'attaque du Hamas. La situation a évolué le 7 octobre. Plus de 46 % de l'ensemble du trafic acheminé vers des sites web palestiniens était ainsi lié à des attaques DDoS HTTP. Le 9 octobre, ce chiffre a atteint près de 60 %. Près de 6 requêtes HTTP sur 10 adressées à des sites web palestiniens basés sur Cloudflare faisaient partie d'une attaque DDoS HTTP.

Les vecteurs d'attaque émergents sur la couche réseau

Répartition des principales menaces DDoS émergentes visant la couche réseau



Les attaques DDoS mDNS ont augmenté de 456 %

Basé sur UDP, le protocole Multicast DNS (mDNS) est utilisé dans les réseaux locaux à des fins d'identification de service/appareil. Les serveurs mDNS vulnérables répondent aux requêtes unicast provenant de l'extérieur du réseau local, l'adresse de ces requêtes étant « usurpée » (remplacée) par l'adresse source de la victime. Une attaque par amplification en résulte. Nous avons constaté une forte augmentation des attaques mDNS au troisième trimestre, avec une hausse de 456 % par rapport au trimestre précédent.

Les attaques DDoS CoAP ont augmenté de 387 %

Le protocole CoAP (Constrained Application Protocol) est conçu pour être utilisé dans les appareils électroniques simples. Il permet la communication entre appareils dans un contexte de faible alimentation et au sein d'un environnement léger. Il peut toutefois faire l'objet d'une utilisation abusive dans le cadre d'attaques DDoS via l'usurpation d'adresse IP ou l'amplification. En effet, les acteurs malveillants exploitent sa prise en charge du multicast ou tirent parti d'appareils CoAP mal configurés pour générer de grandes quantités de trafic réseau indésirable. Ce processus peut conduire à une perturbation de service ou à une surcharge des systèmes visés, qui deviennent dès lors indisponibles pour les utilisateurs légitimes.

Les attaques DDoS ESP ont augmenté de 303 %

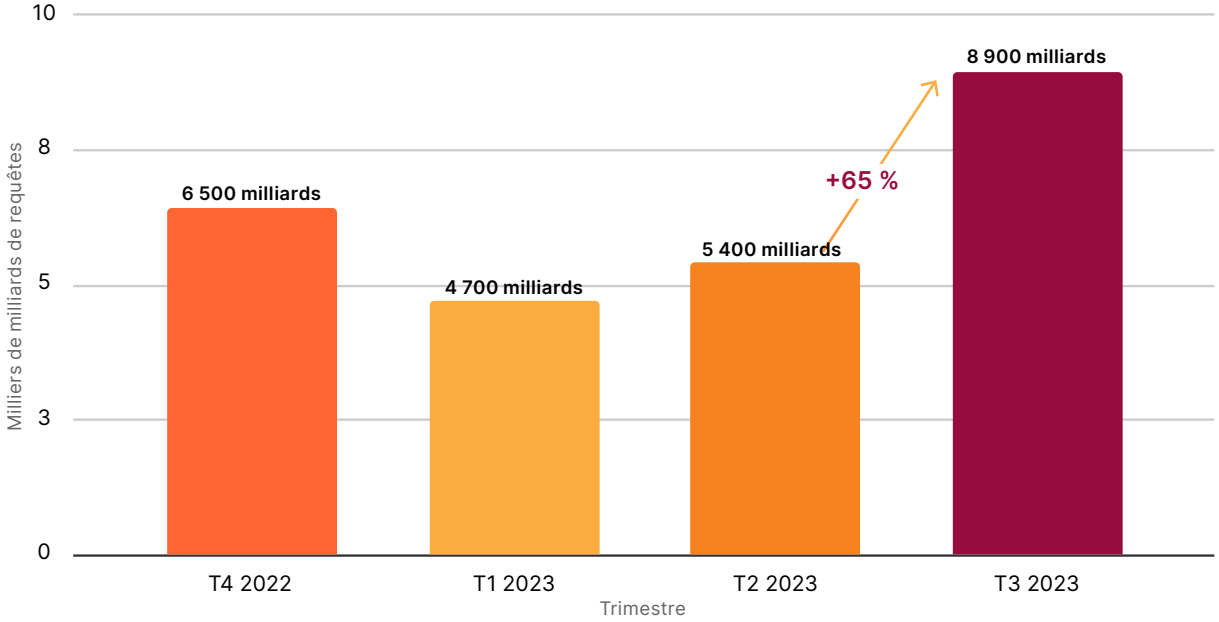
Le protocole Encapsulating Security Payload (ESP, encapsulation de contenu de sécurité) fait partie du cadre IPsec et assure confidentialité, authentification et intégrité aux communications réseau. Toutefois, il peut potentiellement faire l'objet d'une utilisation abusive lors d'attaques DDoS si les acteurs malveillants exploitent des systèmes vulnérables ou mal configurés pour réfléchir ou amplifier le trafic vers une cible, afin de provoquer une perturbation de service. Comme pour tous les autres protocoles, la sécurisation et la configuration adéquate des systèmes utilisant l'ESP s'avèrent essentielles pour atténuer le risque d'attaques DDoS.

Tendances trimestrielles des attaques DDoS — Troisième trimestre 2023

Modifications générales du volume de trafic

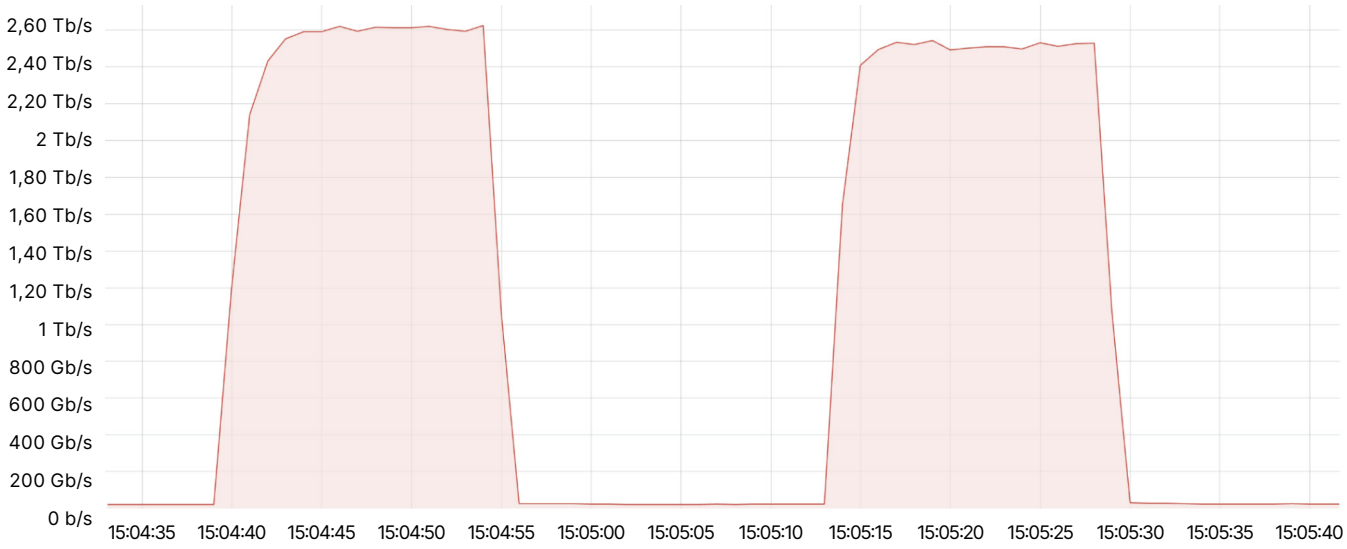
Le trimestre dernier, le volume des attaques DDoS HTTP a augmenté de 15 % par rapport au trimestre précédent. Il s'est encore accru ce trimestre. Le volume d'attaques a augmenté de 65 % par rapport au trimestre précédent, pour atteindre un chiffre impressionnant de 8 900 milliards de requêtes DDoS HTTP automatiquement détectées et atténuées par les systèmes Cloudflare.

Croissance des attaques DDoS sur la couche applicative au cours des deux trimestres précédents



Nous avons constaté une légère augmentation (14 %) des attaques DDoS sur les couches 3 et 4, soit un chiffre similaire à ceux que nous avons observés lors du premier trimestre de cette année. Lors du troisième trimestre, nos systèmes de défense anti-DDoS ont automatiquement détecté et atténué des attaques DDoS de l'ordre du térabit par seconde. L'attaque la plus volumineuse que nous ayons observée culminait à 2,6 Tb/s. Cette dernière faisait partie d'une campagne plus vaste visant le résolveur DNS public de Cloudflare, 1.1.1.1. Il s'agissait d'une attaque de type UDP flood lancée par un botnet reposant sur une variante de Mirai.

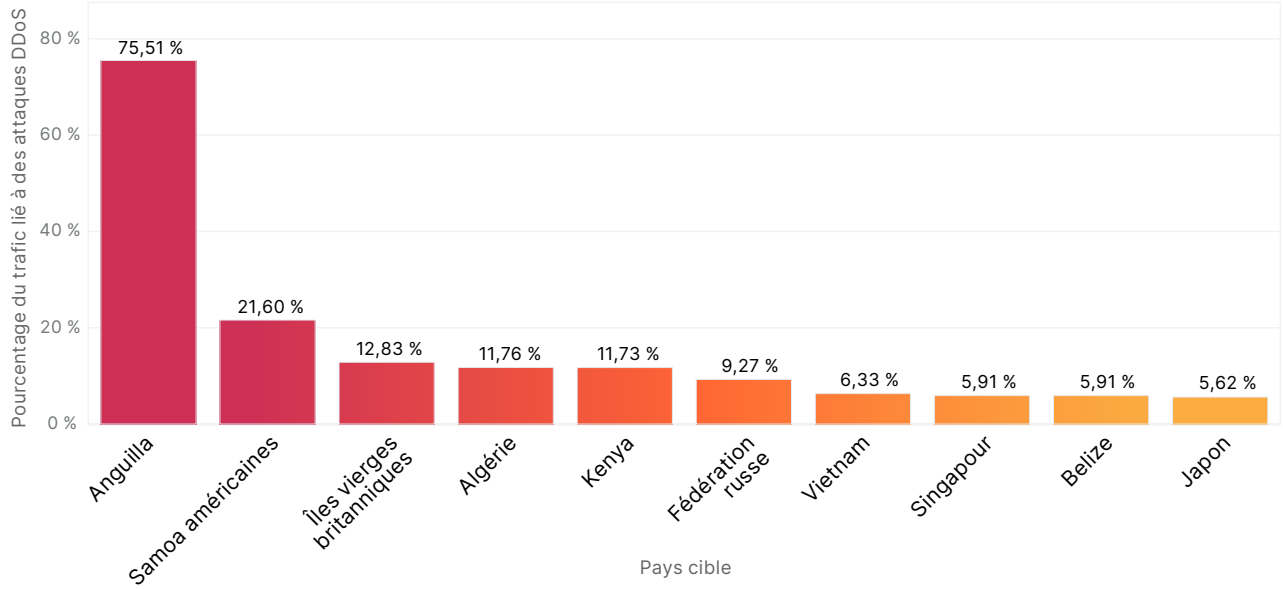
Les attaques UDP flood basées sur un botnet Mirai culminant à 2,6 Tb/s



Principaux pays visés

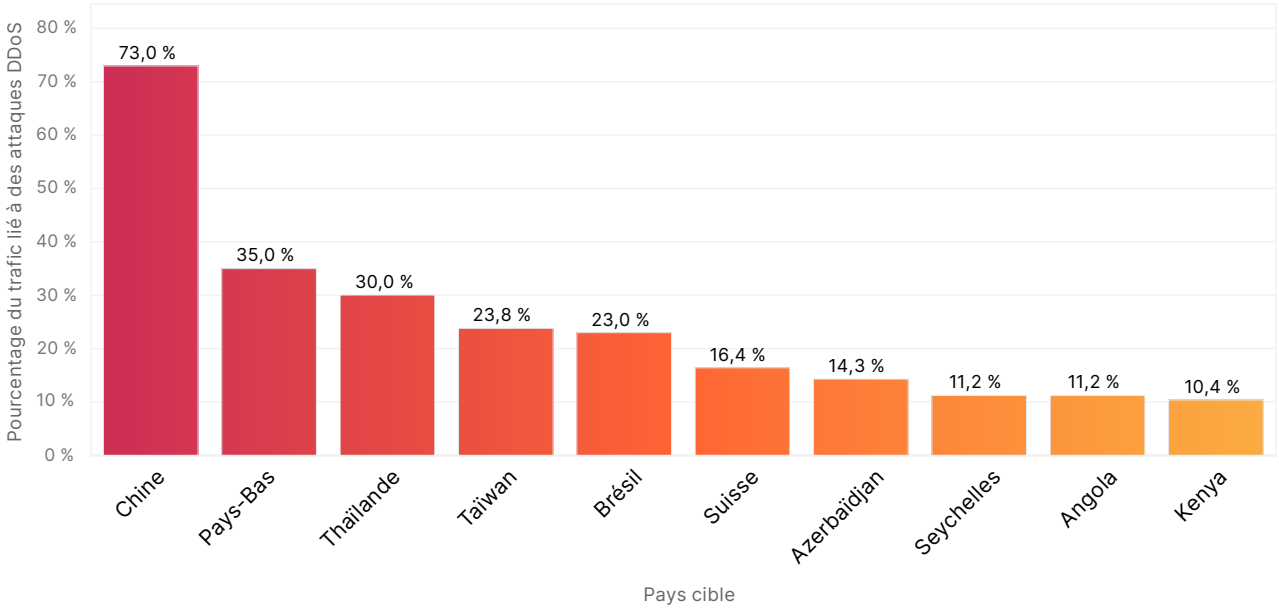
Les trois pays les plus visés, en pourcentage de leur trafic HTTP global, étaient des nations insulaires, à la population réduite. Anguilla, un petit archipel situé à l'est de Porto Rico, a bondi à la première place des pays les plus attaqués. Plus de 75 % de l'ensemble du trafic circulant vers les sites web anguillais était lié à des attaques DDoS HTTP. Les Samoa américaines, un groupe d'îles à l'est des Fidji, arrivaient à la deuxième place. Les Îles Vierges britanniques se plaçaient à la troisième position. L'Algérie se situait à la quatrième place, suivie par le Kenya, la Russie, le Vietnam, Singapour, le Bélize et le Japon.

Trafic DDoS sur la couche applicative en pourcentage du trafic HTTP des principaux pays visés



Au niveau de la couche réseau, la comparaison basée sur le pays et la région est particulièrement frappante. Tout comme lors du deuxième trimestre 2023 (avril à juin), la Chine conserve la première place ce trimestre (juillet à septembre) en tant que pays le plus attaqué, en pourcentage de son trafic réseau global. Cloudflare a constaté que 73 % du trafic adressé aux réseaux Internet chinois se composait de trafic hostile. Les Pays-Bas ont reçu la deuxième plus grosse proportion de trafic hostile (soit 35 % de l'ensemble du trafic du pays), suivis de près par la Thaïlande, Taïwan et le Brésil.

Trafic DDoS sur la couche réseau en pourcentage du trafic réseau des principaux pays visés



Variations sectorielles et régionales des attaques DDoS

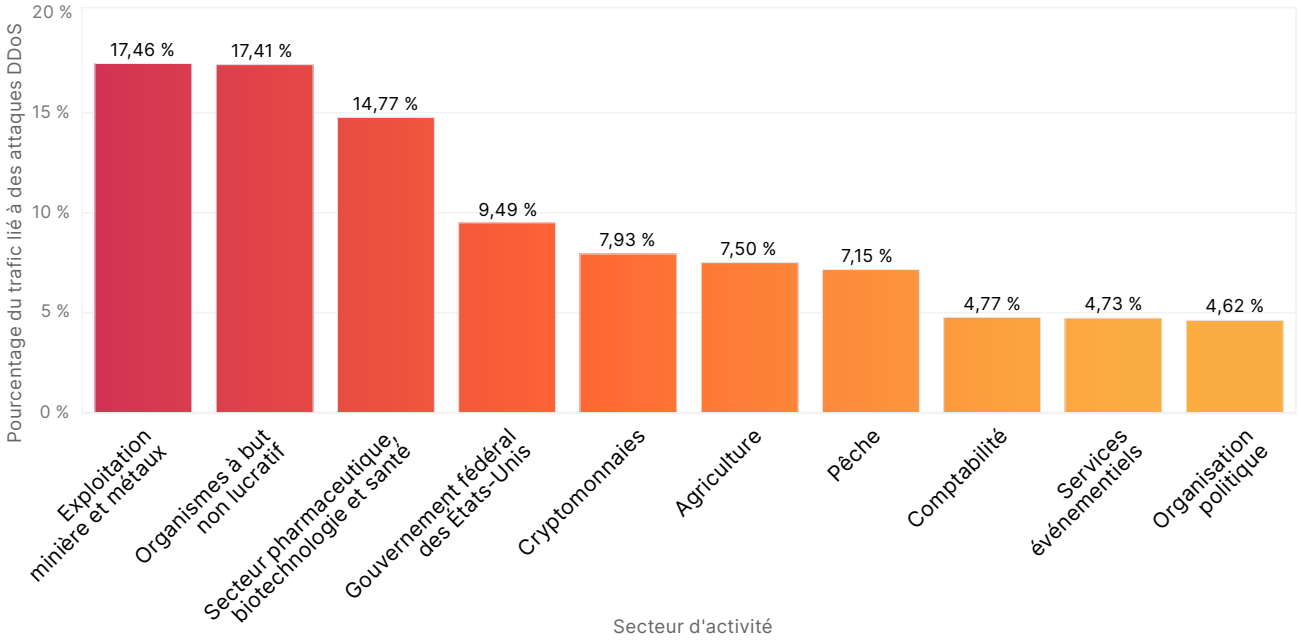
Le secteur des jeux/jeux de hasard est depuis longtemps l'un des plus visés par rapport aux autres. Toutefois, lorsque nous examinons le trafic lié aux attaques DDoS HTTP relatif à chaque secteur spécifique, nous voyons se dessiner une image différente. Le secteur des jeux/jeux de hasard voit tellement de trafic utilisateur circuler qu'il n'intègre même pas le Top 10 des secteurs les plus sujets aux attaques, bien qu'il s'agisse du secteur le plus visé en termes de volume.

À la place, c'est le secteur de l'exploitation minière et des métaux qui a été visé par le plus grand nombre d'attaques par rapport à son trafic total. 17,45 % de l'ensemble du trafic des entreprises du secteur faisait ainsi partie d'attaques DDoS.

Le secteur des organisations à but non lucratif le suivait de près à la deuxième place, avec 17,41 % de l'ensemble du trafic de ce dernier en lien avec des attaques DDoS HTTP. La plupart de ces attaques visaient plus de 2 400 organisations à but non lucratif et organismes médiatiques indépendants (dans 111 pays) protégés gratuitement par Cloudflare dans le cadre du projet Galileo, qui a fêté son neuvième anniversaire cette année. Au cours du seul trimestre précédent, Cloudflare a atténué chaque jour une moyenne de 180,5 millions de cybermenaces visant des sites web protégés par Galileo.

Les entreprises du secteur pharmaceutique, de la biotechnologie et de la santé arrivaient en troisième place, tandis que les sites web du gouvernement fédéral des États-Unis décrochaient la quatrième place. Près d'une requête HTTP sur 10 adressée à des propriétés Internet du gouvernement fédéral des États-Unis faisait partie d'une attaque. Le secteur des cryptomonnaies se plaçait en cinquième position, suivi de peu par le secteur de l'agriculture et de la pêche.

Attaques DDoS HTTP : principaux secteurs visés par rapport à leur propre trafic



Recommandations et points à retenir

Bonnes pratiques	Optimisez votre utilisation de Cloudflare
Mettre à jour ou définir un plan de réponse en cas de déni de service	Avez-vous intégré les alertes et les informations sur les menaces à vos opérations de sécurité ? Savez-vous comment joindre tous les collaborateurs nécessaires en cas d'attaque ? Sont-ils formés au plan de réponse ?
Déployer un système d'information sur les menaces et des solutions d'atténuation des attaques DDoS internes (in-line) et automatisées	Utilisez plusieurs techniques de détection pour faire face aux tendances d'attaques recensées dans ce rapport : 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 afin qu'elle soit plus résiliente pour votre profil de trafic **Améliorer les performances de votre réseau et de vos applications afin d'éviter les engorgements**	Assurez-vous que la capacité de vos outils 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. Réduisez automatiquement le plafond de multiplexage HTTP/2 lorsque vous êtes attaqué, afin d'activer le pare-feu WAF. Tirez parti d'une file d'attente numérique. 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 ports utilisés et importants pour votre activité ouverts. Utilisez la validation de schéma et une passerelle d'API pour gérer le trafic lié aux API.
Tirer parti des informations sur les menaces et de l'intelligence artificielle pour garder une longueur d'avance sur les menaces émergentes	Vous pouvez utiliser des scores de bot dans vos règles de pare-feu et de contrôle du volume de requêtes.

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.

Assistez au webinar consacré aux tendances des attaques DDoS afin d'en apprendre davantage sur les menaces DDoS émergentes et la marche à suivre pour vous défendre contre elles.

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

RÉV. : BDES-5348.2023NOV20