CLOUDFLARE

Rapport Cloudflare sur les menaces DDoS

Deuxième trimestre 2023

Contenu

Synthèse

Bienvenue dans le rapport trimestriel de Cloudflare consacré aux attaques par déni de service distribué (Distributed Denial-of-Service, DDoS) survenues entre avril et juin 2023. Ce document présente des statistiques et des tendances relatives au panorama des menaces DDoS observées sur le réseau mondial de Cloudflare lors du deuxième trimestre 2023.

Le deuxième trimestre 2023 s'est caractérisé par des vagues de campagnes d'attaques DDoS pensées en amont, taillées sur mesure, persistantes et portant sur différents fronts.

Au niveau de la couche HTTP, nous avons détecté une forte activité des groupes d'hacktivistes pro-russes REvil, Killnet et Anonymous Sudan à l'encontre des sites web occidentaux, ainsi qu'une hausse des attaques DDoS HTTP fortement randomisées et à faible volume. Au cours du dernier trimestre, les attaques DDoS basées sur le DNS sont devenues le vecteur d'attaque DDoS le plus courant, avec 32 % de l'ensemble des attaques DDoS visant le protocole DNS. Au niveau de la couche UDP, nous avons observé des attaques tirer parti d'une vulnérabilité zero-day (CVE-2022-26143, TP240PhoneHome) que nous avions révélée en mars 2022.

Au-delà des campagnes d'attaque spécifiques, nous détaillerons les tendances d'attaques sur la couche applicative et la couche réseau selon leurs variations sectorielles et régionales. Enfin, nous vous proposerons des conseils sur la marche à suivre pour renforcer votre sécurité de manière proactive afin de mieux assurer la continuité de vos services dans un contexte de menaces DDoS en évolution constante.

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

Points clés du rapport

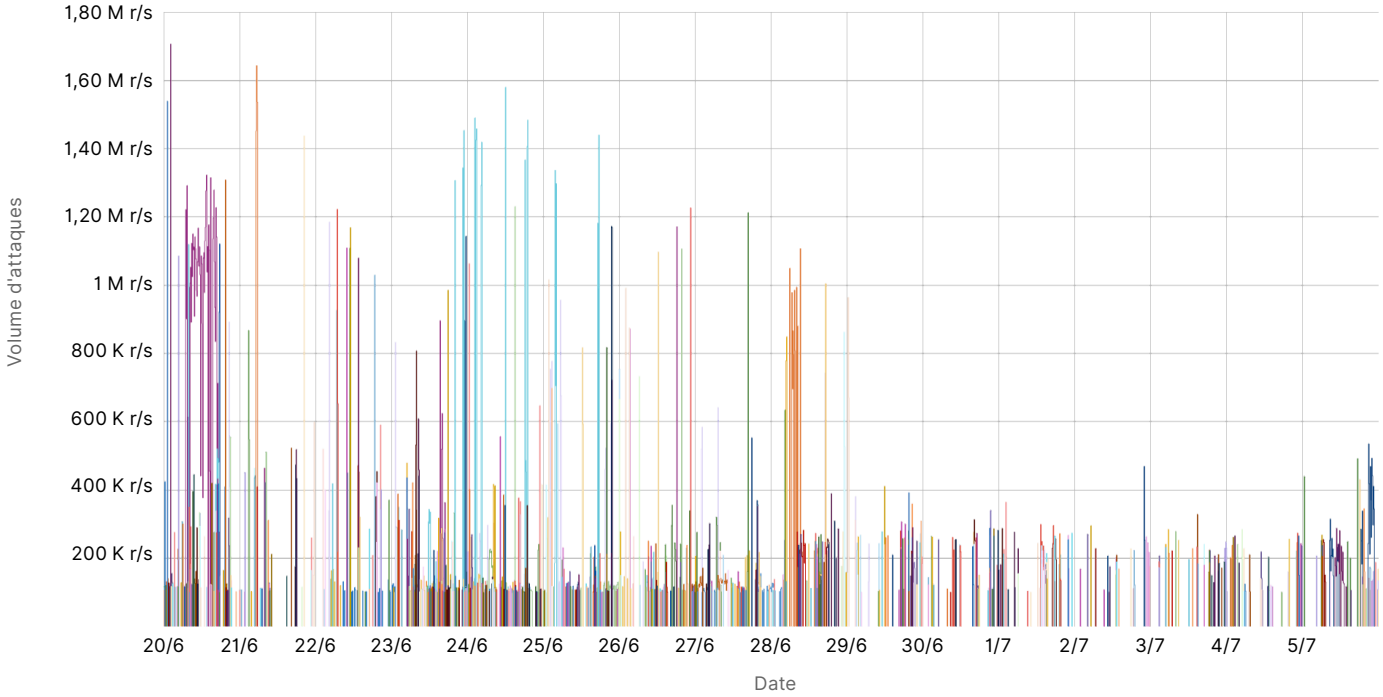
L'alliance d'hacktivistes surnommée « Darknet Parliament » en action

Le 14 juin, plusieurs groupes d'hacktivistes pro-russes, dont Killnet, une résurgence de REvil et Anonymous Sudan, ont annoncé avoir uni leurs forces sous la forme d'une alliance connue sous le nom de « Darknet Parliament » (le parlement du Darknet).

Leur objectif déclaré consiste à lancer des cyberattaques « de grande ampleur » à l'encontre du système financier occidental, notamment les banques occidentales, la Réserve fédérale américaine et le réseau SWIFT (Society for Worldwide Interbank Financial Telecommunication, la Société de télécommunications interbancaires mondiales).

Ce trimestre, le Darknet Parliament a lancé près de 10 000 attaques DDoS contre des sites web protégés par Cloudflare. Toutefois, les sites du secteur des services bancaires et financiers ne constituaient que le neuvième secteur le plus attaqué, si l'on se base sur les attaques que nous avons observées à l'encontre de nos clients dans le cadre de cette campagne. Nos systèmes ont détecté et atténué automatiquement les attaques DDoS associées à cette dernière.

10 000 attaques lancées par Killnet, REvil et Anonymous Sudan au deuxième trimestre 2023, tous secteurs confondus



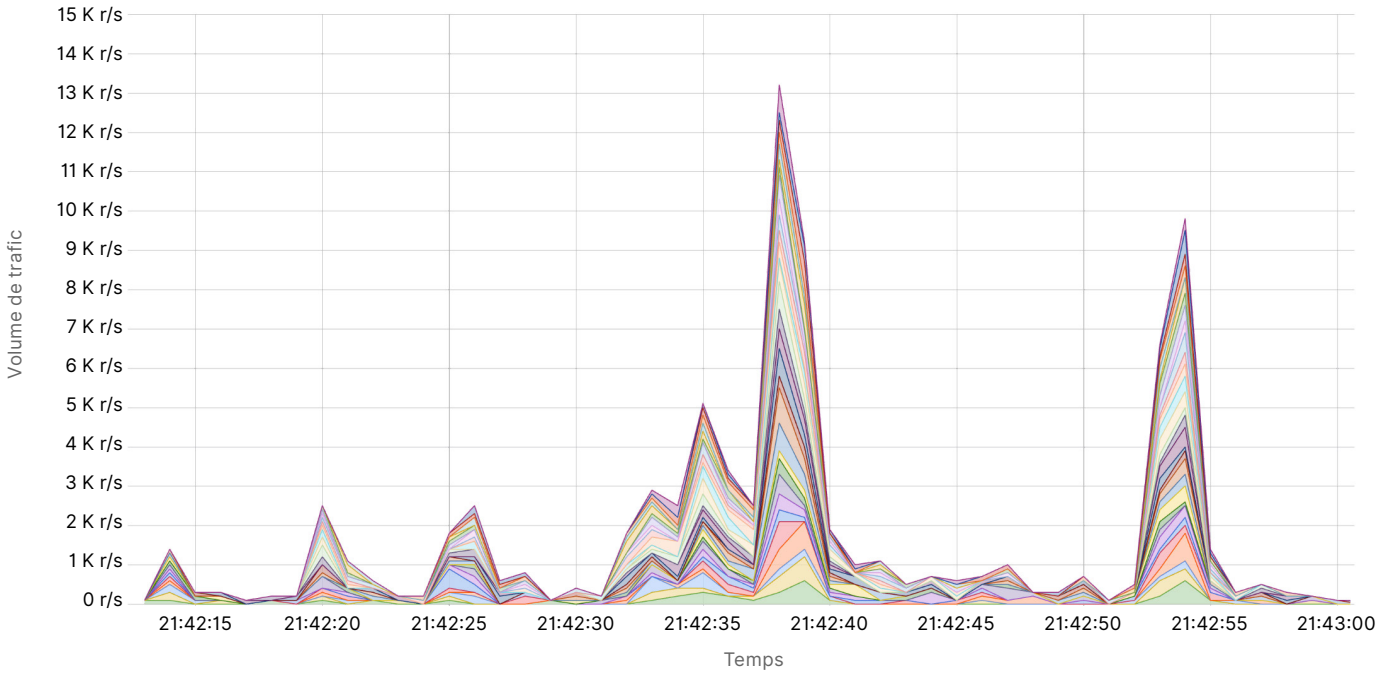
Attaques DDoS HTTP fortement randomisées et à faible volume

Une attaque DDoS HTTP est une attaque DDoS lancée via l'Hypertext Transfer Protocol (HTTP, protocole de transfert hypertexte). Elle prend pour cibles les propriétés Internet HTTP, telles que les sites web et les passerelles d'API. Nous avons observé une hausse des attaques DDoS HTTP fortement randomisées et à faible volume au cours des derniers mois. Par le passé, il s'agissait principalement d'une tactique employée par des acteurs confortablement financés et soutenus par des États-nations.

Il semble que les acteurs malveillants à l'origine de ces attaques ont délibérément modifié ces dernières afin de circonvenir les systèmes d'atténuation en imitant avec habileté et grande précision le comportement du navigateur des utilisateurs. Dans certains cas, ils introduisent un haut niveau de randomisation sur diverses propriétés, comme les agents utilisateur et les empreintes JA3.

Nous vous présentons un exemple de ce type d'attaque ci-dessous. Chaque couleur représente une fonctionnalité de randomisation différente.

Évolution du volume de trafic HTTP lors d'une attaque DDoS HTTP fortement randomisée et à faible volume



Les attaques DDoS par blanchiment de DNS

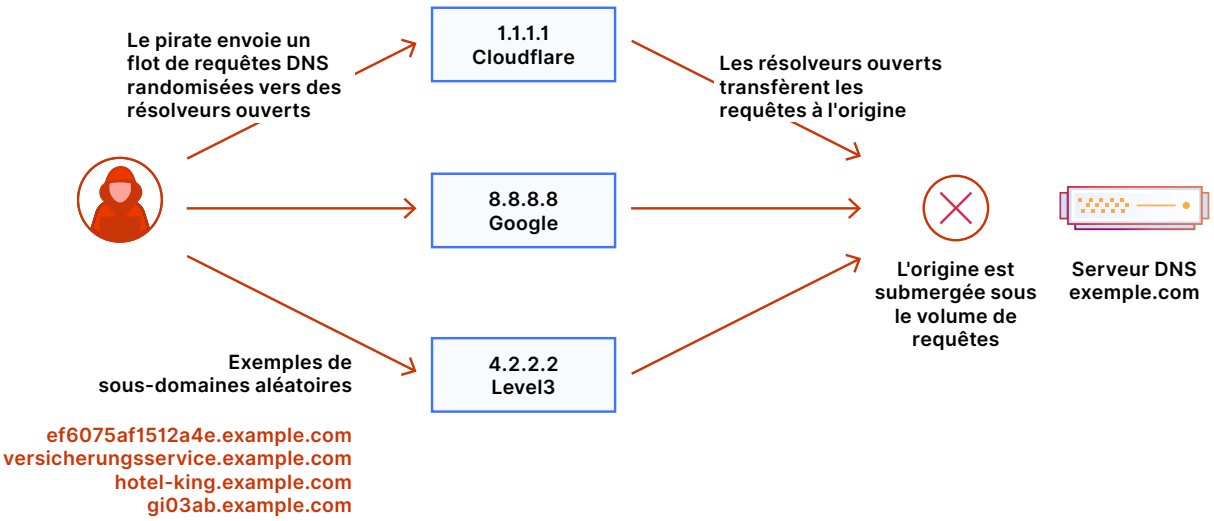
Lors du dernier trimestre, les attaques DDoS basées sur le DNS sont devenues le vecteur d'attaque DDoS le plus courant, avec 32 % de l'ensemble des attaques DDoS visant le protocole DNS. Le système de noms de domaine, ou DNS (Domain Name System), fonctionne comme un annuaire téléphonique pour Internet. Il aide à traduire les adresses web lisibles par l'humain (p. ex. www.cloudflare.com) en adresse IP lisible par la machine (p. ex. 104.16.124.96). En perturbant les serveurs DNS, les acteurs malveillants influent sur la capacité de cette dernière à se connecter à un site web et, ce faisant, rendent les sites indisponibles aux utilisateurs.

Les attaques par blanchiment de DNS constituent un type d'attaque particulièrement préoccupant et en croissance rapide. Elles peuvent mettre sérieusement en péril les entreprises qui exécutent leurs propres serveurs DNS de référence. Une attaque DDoS par blanchiment de DNS désigne le processus visant à faire apparaître le trafic malveillant comme du trafic utile et légitime par l'intermédiaire de résolveurs DNS récursifs réputés. L'opération est similaire à celle qui vise à donner l'apparence de la légalité à des gains financiers illégaux (l'« argent sale »), également connue sous le nom de blanchiment d'argent.

Lors d'une attaque par blanchiment de DNS, l'acteur malveillant adresse des requêtes aux sous-domaines d'un domaine géré par le serveur DNS de la victime. Randomisé, le préfixe qui définit le sous-domaine n'est jamais utilisé plus d'une ou deux fois lors de ces attaques. Du fait de cette randomisation, les serveurs DNS récursifs ne disposeront jamais d'une réponse en cache et devront dès lors transférer la requête au serveur DNS de référence de la victime. Ce dernier est alors bombardé d'un nombre colossal de requêtes jusqu'à ce qu'il ne puisse plus traiter les requêtes légitimes, voire qu'il s'effondre.

Une importante institution financière située en Asie et un fournisseur DNS nord-américain figurent au rang des victimes les plus récentes de ces attaques. La source de l'attaque inclut des serveurs DNS récursifs renommés pour leur fiabilité, comme le serveur 8.8.8.8 de Google et le 1.1.1.1 de Cloudflare. Le domaine attaqué est valide et doit diffuser les requêtes légitimes. Les administrateurs DNS ne peuvent donc pas bloquer la source de l'attaque ni l'ensemble des requêtes adressées au domaine attaqué. Il n'est pas toujours évident de faire la distinction entre les requêtes légitimes et les requêtes malveillantes.

Schéma d'une attaque DDoS par blanchiment de DNS

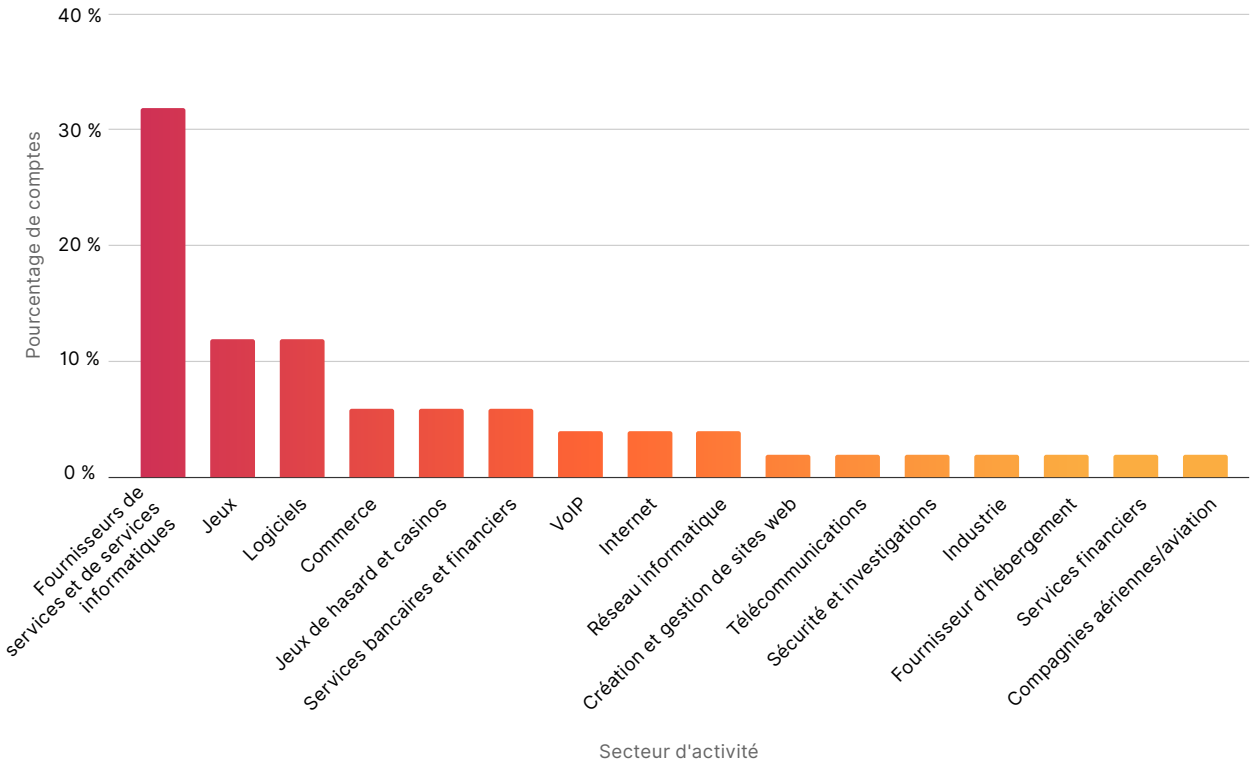


« Startblast » : exploiter les vulnérabilités de Mitel dans le cadre des attaques DDoS

Au niveau de la couche UDP, nous avons observé des attaques tirer parti d'une vulnérabilité zero-day (CVE-2022-26143, TP240PhoneHome) que nous avions révélée en mars 2022. Conjointement à d'autres membres de la communauté de la sécurité de l'information, nous avons identifié cette vulnérabilité (qui expose le système aux attaques DDoS par amplification UDP) au sein du système de téléphonie d'entreprise Mitel MiCollab.

Le nom de la campagne « Startblast » provient de la commande de débogage éponyme essentielle à l'exploitation de la vulnérabilité. Nous avons détecté que la plus grande partie des attaques visaient les fournisseurs de services et de services informatiques, plus que l'industrie du jeu. Ce type d'attaque a connu la croissance la plus rapide parmi les attaques DDoS sur la couche réseau ce dernier trimestre.

Attaques liées à la campagne Starblast, par secteur, au deuxième trimestre 2023



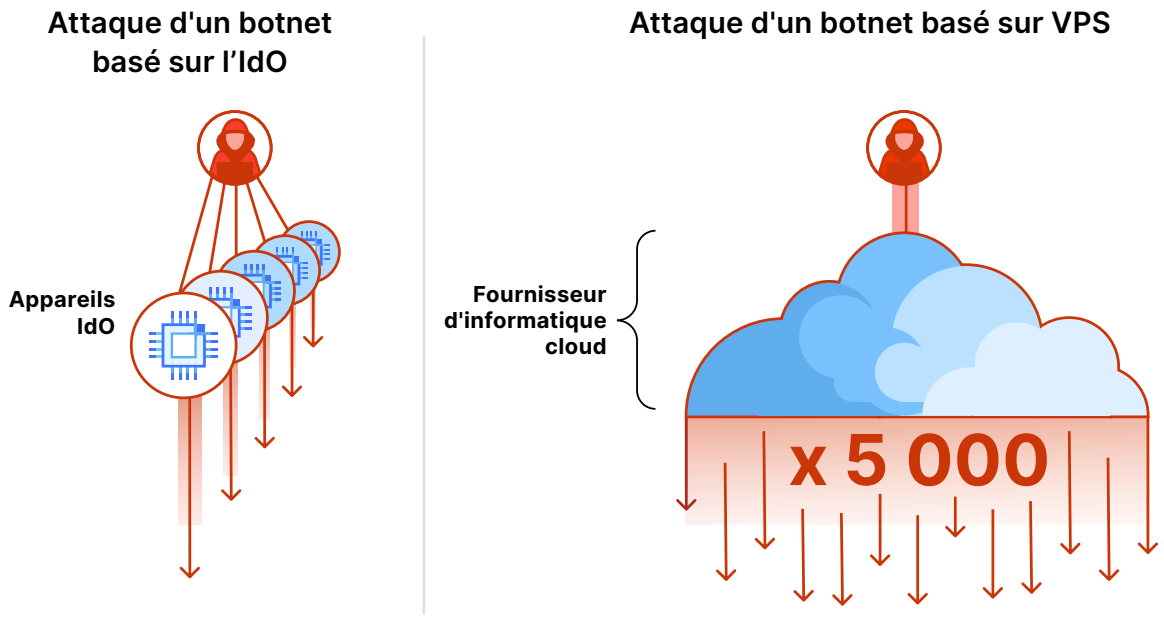
L'essor continu des botnets hautes performances

Comme nous l'avons communiqué dans le rapport Cloudflare sur les tendances des attaques DDoS au premier trimestre 2023, nous continuons d'assister à une évolution de l'ADN des botnets. L'époque des botnets DDoS basés sur machines virtuelles est arrivée et, avec elle, celle des attaques DDoS hypervolumétriques. Composés de machines virtuelles (VM, pour Virtual Machines) ou de serveurs privés virtuels (VPS pour Virtual Private Servers) plutôt que d'appareils liés à l'Internet des objets (IdO), ces botnets se révèlent ainsi jusqu'à 5 000 fois plus puissants.

Cloudflare collabore avec les principaux fournisseurs d'informatique cloud pour lutter contre ces nouveaux botnets. Nous avons observé les premiers résultats de notre stratégie commune, à savoir la neutralisation de plusieurs composants importants de ces botnets. Depuis cette intervention commune, nous n'avons observé aucune nouvelle attaque hypervolumétrique au cours du deuxième trimestre 2023 (de l'ampleur observée lors du premier trimestre 2023 et par le passé).

Notre objectif consiste à automatiser et à étendre davantage cette collaboration. Nous invitons ainsi les fournisseurs d'informatique cloud, les fournisseurs d'hébergement et les autres fournisseurs de services généraux à rejoindre le Botnet Threat Feed (le flux d'informations sur les menaces liées aux botnets) de Cloudflare.

L'accès est gratuit pour les fournisseurs et nous ne vendons en aucune façon nos données à des tiers. Ce flux assure une visibilité sur les attaques provenant de l'intérieur du réseau des fournisseurs de services et contribue ainsi à notre effort collectif visant à démanteler les botnets.



Tendances principales en matière d'attaques DDoS — Deuxième trimestre 2023

Les sections suivantes du rapport passeront en revue les principales tendances concernant les cibles des attaques (identité et nature).

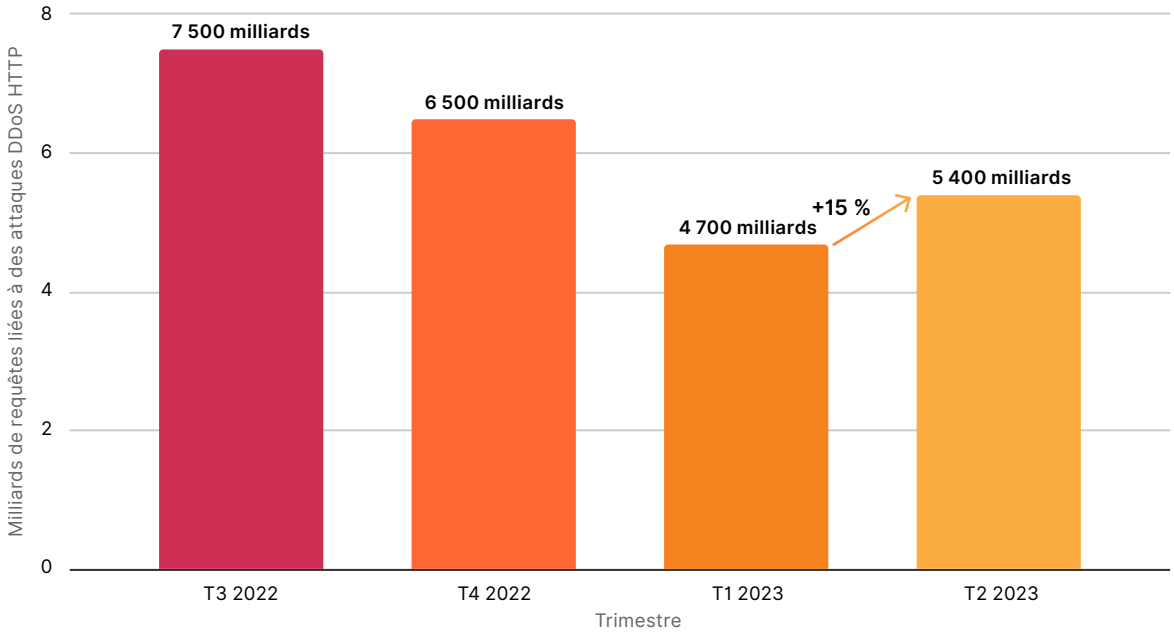
Modifications générales du volume de trafic

Les attaques DDoS sur la couche applicative et la couche réseau ont diminué respectivement de 35 % et de 14 % dans les six premiers mois de l'année 2023 par rapport à la même période l'année dernière. Chez Cloudflare, nous espérons également que cette tendance baissière par rapport à l'année précédente se poursuivra, car Cloudflare et la communauté de la sécurité de l'information rendent la tâche plus difficile et pénible pour les cybercriminels.

À titre de mise en garde, nous avons néanmoins constaté une hausse de 15 % des attaques DDoS sur la couche applicative entre le deuxième trimestre 2023 et la même période l'année dernière. Il n'est pas encore temps de baisser votre garde !

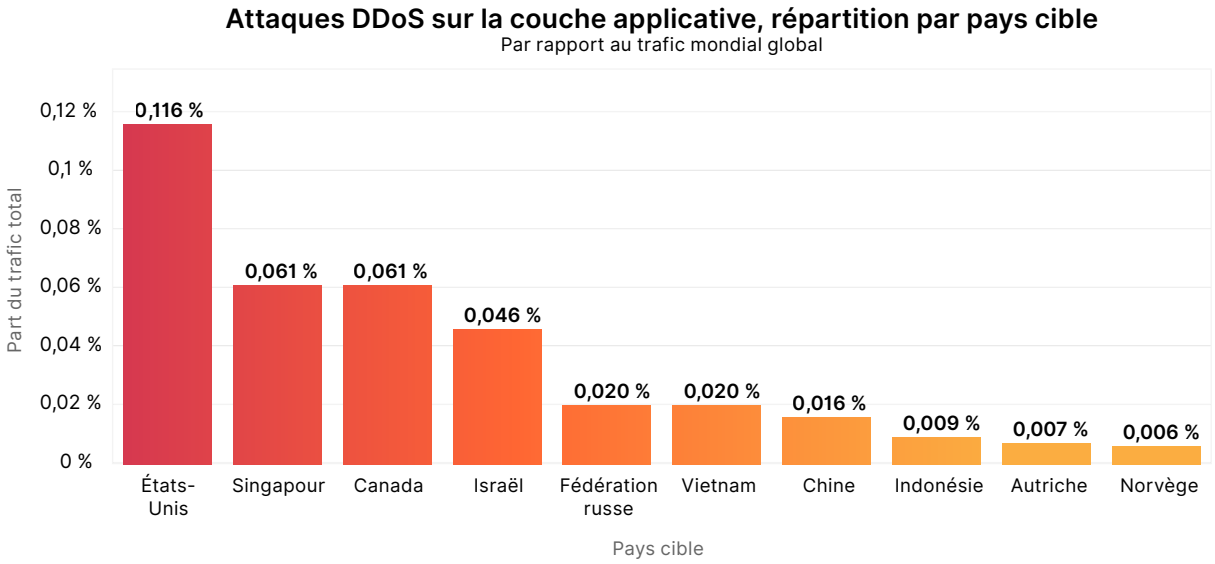
Au total, le nombre d'attaques DDoS HTTP a augmenté de 15 % par rapport au trimestre précédent, malgré une baisse de 35 % par rapport à l'année précédente. De même, les attaques DDoS sur la couche réseau ont également diminué d'environ 14 % par rapport au trimestre précédent.

Trafic lié aux attaques DDoS HTTP, répartition trimestrielle



Principaux pays visés

Le trimestre dernier, nous précisions qu'Israël était le pays le plus visé par des attaques DDoS sur la couche applicative. Ce trimestre, les sites web situés aux États-Unis reprennent la première place, avec les sites situés à Singapour et au Canada respectivement à la deuxième et à la troisième place. Les attaques ciblant des sites web israéliens ont diminué de 33 %, soit un chiffre qui place le pays en quatrième position.



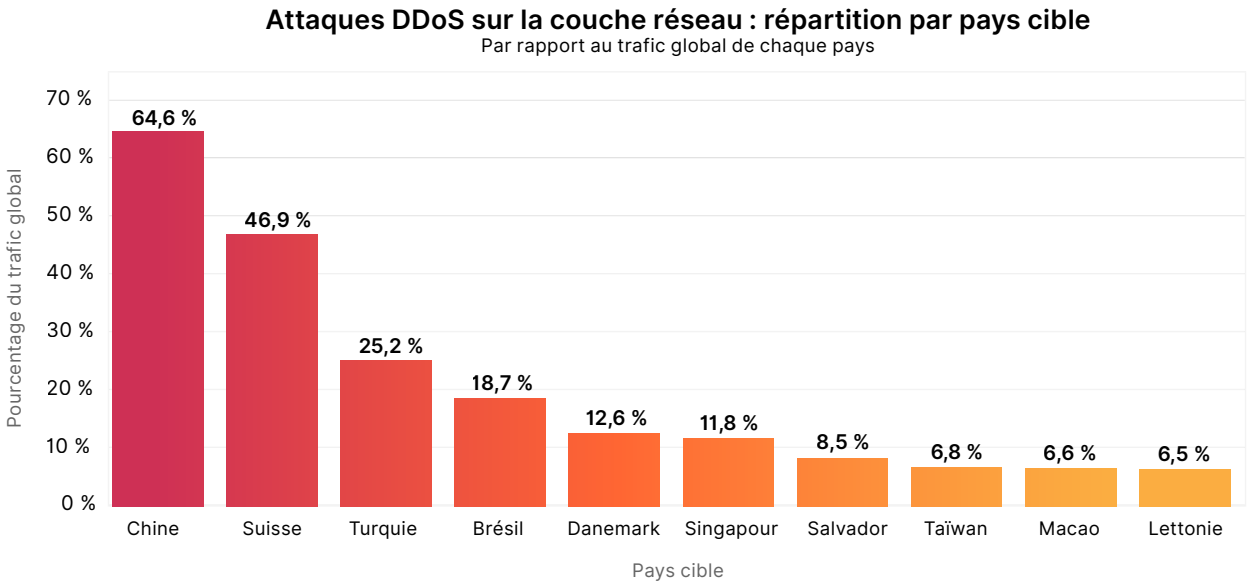
⚠ 2 fois plus d'attaques DDoS sur la couche applicative

Les États-Unis ont subi 2 fois plus d'attaques DDoS sur la couche applicative que le pays suivant dans la liste.

⚠ Plus de 10 %

Plus de 10 % du trafic global sur la couche applicative circulant en Palestine et à Saint-Christophe-et-Niévès était lié à des attaques DDoS.

Du point de vue de la couche réseau, la Chine reprend la première place en termes de nombre d'attaques DDoS observées sur la couche. Deux octets sur trois à destination des réseaux chinois étaient liés à des attaques DDoS au deuxième trimestre 2023. Nous avons d'ailleurs observé ce haut niveau de trafic malveillant à destination de la Chine à plusieurs reprises lors des trimestres précédents. La situation unique du premier trimestre 2023, qui voyait 83 % des octets à destination de réseaux finlandais se trouver liés à des attaques DDoS, s'est résorbée. La Finlande a quitté le classement des dix premiers pays (et régions) à faire face au plus grand nombre d'attaques DDoS.



Variations sectorielles et régionales des attaques DDoS

Les sites web d'achat de cryptomonnaies ont été les plus visés au deuxième trimestre 2023 et ont ainsi reçu la plus grande quantité de trafic lié à des attaques DDoS HTTP. Six requêtes HTTP sur 10 000 adressées à des sites d'achat de cryptomonnaies faisaient ainsi partie de ce type d'attaque. Ce chiffre représente une augmentation de 600 % par rapport au trimestre précédent.

Les sites web liés au secteur des jeux et des jeux de hasard se sont placés en deuxième position, avec un accroissement de 19 % de leur part du volume d'attaques par rapport au trimestre précédent. Les sites de marketing et de publicité arrivaient non loin, à la troisième place, avec une variation minime de leur part d'attaques subies.

Malheureusement, les organisations à but non lucratif font face à un grand nombre d'attaques. Au final, 12 % du trafic adressé à ces organisations faisaient partie d'attaques DDoS. Il s'agit ainsi du deuxième secteur le plus touché en termes de part de trafic. Cloudflare protège plus de 2 271 organisations à but non lucratif dans 111 pays dans le cadre de son projet Galileo, qui a célébré son neuvième anniversaire cette année. Ces derniers mois, ces organismes se sont ainsi retrouvés chaque jour sous les feux de 67,7 millions de cyberattaques (en moyenne).

Principaux secteurs pris pour cible, par région

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 d'un système d'information 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 vastes 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 webinaire 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-4839.2023AUG28