CLOUDFLARE

RAPPORT SUR LES MENACES

Rapport sur le panorama des menaces DDoS

Tendances des attaques DDoS au quatrième trimestre 2022

Contenu

Synthèse

Bienvenue dans le rapport trimestriel de Cloudflare consacré aux attaques par déni de service distribué (Distributed Denial-of-Service, DDoS) pour le quatrième et dernier trimestre de l'année 2022. Ce document présente des statistiques et des tendances relatives au panorama des menaces DDoS recensées sur le réseau mondial de Cloudflare d'octobre à décembre 2022.

Les attaques DDoS se sont poursuivies au cours du dernier trimestre, tandis que des milliards de personnes dans le monde célébraient ou s'apprêtaient à célébrer diverses fêtes de fin d'année. Nous avons ainsi observé une progression en termes d'ampleur, de fréquence et de sophistication de ces attaques. Conçues pour perturber notre mode de vie, leurs secteurs de prédilection ont été l'aéronautique et l'aérospatiale, les jeux/jeux de hasard, les services financiers et la gestion de l'éducation.

Les défenses anti-DDoS automatisées de Cloudflare ont atténué des millions d'attaques au cours du seul quatrième trimestre. Pendant la dernière semaine de novembre, nous avons automatiquement détecté et atténué une attaque DDoS évaluée à 1 térabit par seconde (Tb/s) contre un fournisseur d'hébergement basé en Corée.

Pour ce document, nous avons rassemblé, agrégé et analysé les données concernant l'ensemble de ces tentatives d'attaque, avant de préparer des conclusions qui vous permettront de mieux comprendre le panorama des menaces actuelles. Dans les sections ci-dessous, nous vous présenterons les tendances générales en matière d'attaques DDoS avant de nous intéresser plus avant aux statistiques relatives aux attaques sur la couche applicative, aux attaques sur la couche réseau et aux attaques DDoS avec demande de rançon. Nous détaillerons également à quel endroit les attaques DDoS ont été observées, communiquerons sur les schémas constatés en termes de débit et de durée des attaques, avant d'étudier les vecteurs d'attaques et les menaces émergentes de façon plus approfondie. Enfin, nous vous proposerons des conseils sur la marche à suivre pour renforcer votre sécurité de manière proactive afin de mieux vous préparer contre les menaces DDoS actuelles et émergentes.

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

Points clés du rapport

Tendances mondiales en matière d'attaques DDoS

Malgré une tendance à la baisse sur l'année, le trafic des attaques DDoS HTTP a néanmoins augmenté de 79 % au quatrième trimestre 2022 par rapport à l'année précédente. Si la plupart de ces attaques se sont révélées de faible ampleur, notre réseau a uniformément constaté des attaques DDoS de l'ordre du térabit comptant plusieurs centaines de millions de paquets par seconde. Nous avons également observé des attaques DDoS HTTP lancées à l'aide de botnets sophistiqués et au pic pouvant atteindre des dizaines de millions de requêtes par seconde.

Vous trouverez ci-dessous quelques-unes des autres tendances émergentes :

Les attaques volumétriques ont connu une forte augmentation

- Le nombre d'attaques présentant des débits supérieurs à 100 gigabits par seconde (Gb/s) a progressé de 67 % par rapport au trimestre précédent.

Les menaces DDoS avec demande de rançon se sont poursuivies

- Plus de 16 % des personnes interrogées ont déclaré avoir reçu une menace ou une demande de rançon dans le cadre d'une attaque DDoS.

La durée des attaques a augmenté

- Le nombre d'attaques d'une durée comprise entre 1 et 3 heures a augmenté de 349 % par rapport au trimestre précédent, tandis que le nombre d'attaques d'une durée supérieure à trois heures a augmenté de 87 % sur la même période.

Les secteurs les plus fréquemment pris pour cible par les attaques DDoS

- Le secteur de l'aéronautique et de l'aérospatiale a été le plus visé par les attaques DDoS sur la couche applicative, qui représentent 35 % de l'ensemble du trafic web destiné à ces propriétés Internet.
- Le secteur de la gestion de l'éducation a été le plus ciblé par les attaques DDoS sur la couche réseau, dont la part totalise 92 % de l'ensemble du trafic web.
- Les autres secteurs fortement touchés par les attaques sur la couche réseau comprennent le secteur des technologies et services de l'information (74 %), le secteur des relations et des communications publiques (73 %), ainsi que le secteur financier (31 %).

Source et cibles des attaques DDoS

- Le trafic hostile des attaques sur la couche réseau provenait du Botswana (52 % de l'ensemble du trafic enregistré), d'Azerbaïdjan (environ 40 %), du Paraguay (environ 40 %) et de Palestine (environ 40 %).
- Les attaques sur la couche réseau étaient destinées à la Chine (93 % du trafic de la couche réseau), à la Lituanie (plus de 86 %) et à la Finlande (80 %).
- Les attaques sur la couche applicative visaient la Géorgie (42 % de l'ensemble du trafic), Belize (28 %), Saint-Marin (près de 20 %) et la Libye (près de 20 %).

Remarque : *nous avons modifié nos algorithmes ce trimestre dans le but d'améliorer la précision de nos données. Certains points de données ne sont donc pas comparables à ceux des trimestres précédents. Pour en savoir plus sur ces modifications, consultez la section suivante : Modifications des méthodologies d'établissement de rapports.*

Inscrivez-vous pour assister au webinaire consacré aux tendances des attaques DDoS afin d'en apprendre plus sur les menaces émergentes et la marche à suivre pour vous défendre contre elles.

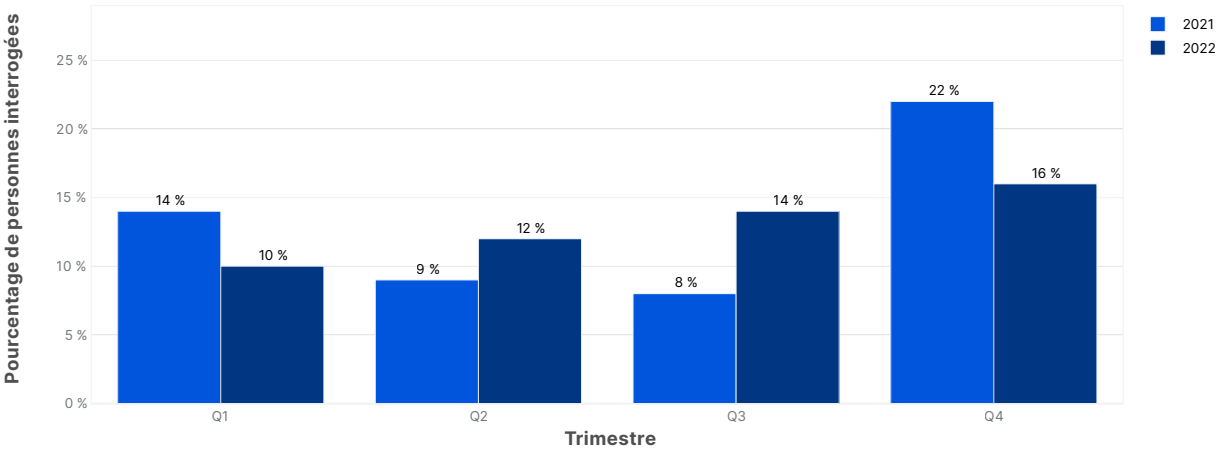
Attaques DDoS avec demande de rançon

Contrairement aux attaques par rançongiciel, dans lesquelles la victime est incitée à télécharger un fichier ou à cliquer sur un lien inclus dans un e-mail (un comportement qui entraîne dès lors le chiffrement et le verrouillage les fichiers de son ordinateur jusqu'au paiement d'une rançon), les attaques DDoS avec demande de rançon peuvent être beaucoup plus faciles à lancer pour les acteurs malveillants. Ainsi, ces dernières n'impliquent pas d'amener la victime à ouvrir un e-mail ou à cliquer sur un lien. De même, leur mise en œuvre ne nécessite pas non plus d'intrusion ou d'établissement d'une présence sur un réseau.

Lors d'une attaque DDoS avec demande de rançon, le pirate submerge les propriétés web de sa victime sous un volume de trafic malveillant suffisant pour perturber ses services Internet. Il exige ensuite le versement d'une rançon, généralement sous forme de bitcoins, pour mettre un terme à l'attaque. Dans certains cas, l'acteur malveillant envoie une demande de rançon avant de procéder à l'attaque DDoS, en s'appuyant sur la menace d'une attaque pour percevoir un paiement frauduleux des entreprises ou des particuliers pris pour cible.

Au quatrième trimestre, 16 % des clients Cloudflare interrogés ont signalé avoir fait les frais d'attaques DDoS HTTP accompagnées d'une menace ou une demande de rançon. Ce chiffre représente une augmentation de 14 % par rapport au trimestre précédent, mais une baisse de 16 % par rapport à l'année précédente.

Répartition trimestrielle des attaques DDoS avec demande de rançon : 2021 et 2022, par trimestre



Procédure de comptabilisation des signalements d'attaques DDoS avec demande de rançon

Les systèmes de Cloudflare analysent le trafic en permanence et atténuent automatiquement les attaques DDoS dès leur détection. Au cours des deux années passées, nous avons envoyé des enquêtes automatiques à chaque client ciblé afin de nous aider à mieux comprendre la nature de ces attaques et la réussite des services d'atténuation de Cloudflare. Nous avons en moyenne recueilli près de 187 réponses par trimestre. Nous demandons notamment aux clients s'ils ont reçu une menace ou une demande de rançon lors de l'attaque. Les réponses servent à calculer le pourcentage d'attaques DDoS avec demande de rançon signalées.

Panorama des attaques DDoS sur la couche applicative

Les attaques DDoS sur la couche applicative (et plus spécifiquement, les attaques DDoS HTTP) perturbent le fonctionnement des serveurs web en les bombardant de plus de requêtes qu'ils ne peuvent en gérer. Cette opération conduit souvent le serveur à abandonner les requêtes légitimes, en entraînant ainsi une dégradation des performances, voire des pannes.

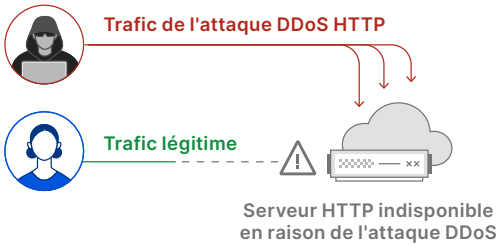
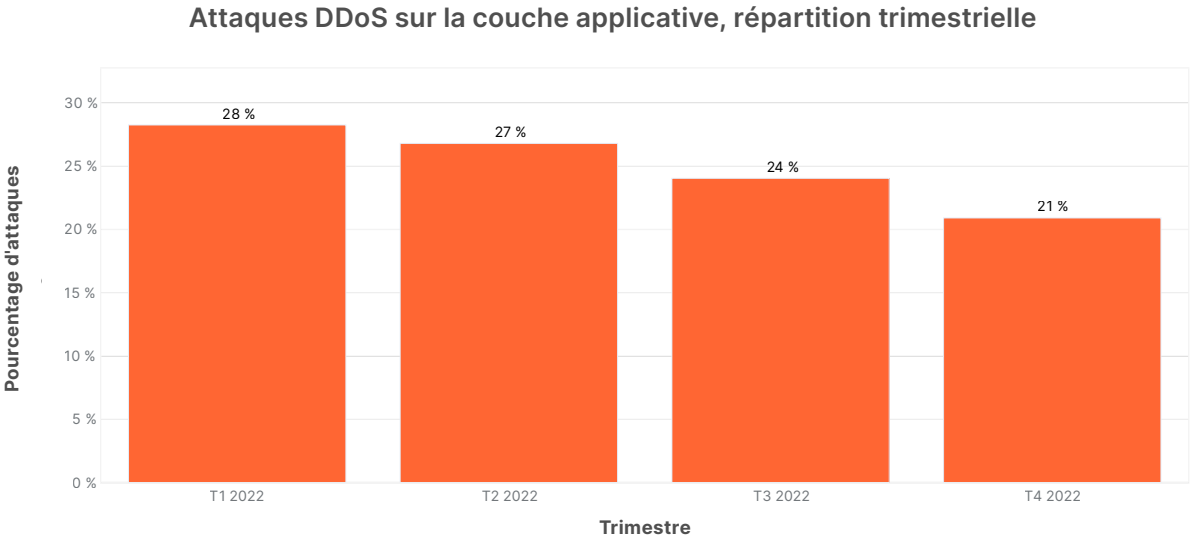


Schéma d'une attaque DDoS sur la couche applicative aboutissant à un événement de déni de service pour les utilisateurs légitimes

Tendances concernant les attaques DDoS sur la couche applicative

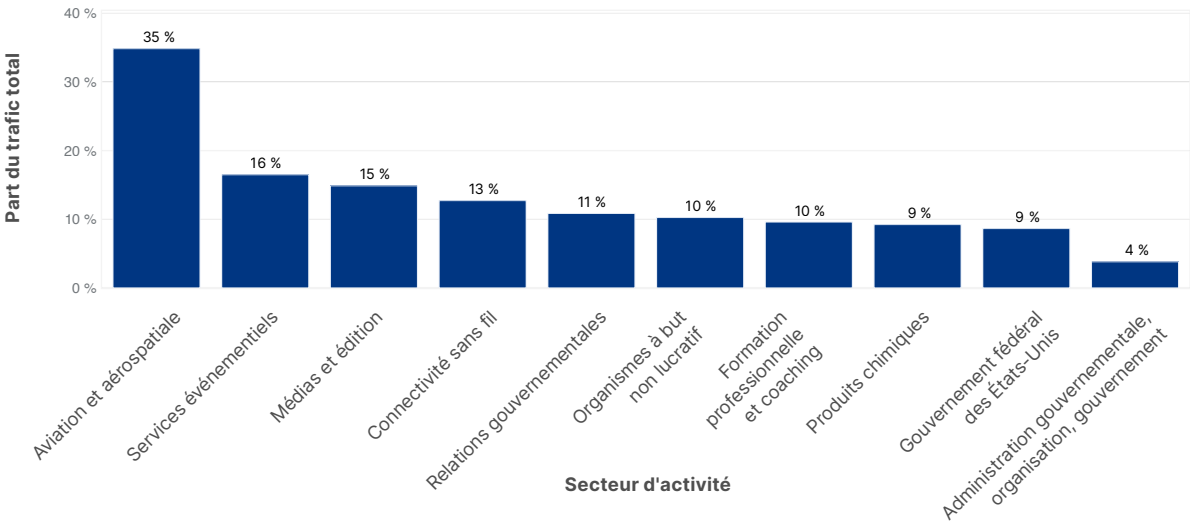
Comme nous pouvons l'observer dans le graphique ci-dessous, malgré une baisse à chaque trimestre de l'année 2022, les attaques DDoS HTTP ont néanmoins affiché une augmentation de 79 % par rapport à l'année précédente (c'est-à-dire, au quatrième trimestre 2021).



Secteurs cibles d'attaques DDoS sur la couche applicative

Au trimestre où de nombreux voyageurs partent en vacances, le secteur de l'aéronautique et de l'aérospatiale est celui qui a subi le plus d'attaques. Près de 35 % de l'ensemble du trafic acheminé vers ces propriétés Internet faisaient ainsi partie d'attaques DDoS HTTP. Le deuxième secteur le plus visé est celui des services événementiels, avec des attaques DDoS HTTP constituant plus de 16 % de son trafic. Suivaient le secteur des médias et de l'édition, le secteur de la connectivité sans fil, le secteur des relations gouvernementales et celui des organisations à but non lucratif. Pour plus d'informations sur la manière dont Cloudflare protège les organisations à but non lucratif et les organismes de défense des droits humains, consultez notre dernier Impact Report.

Attaques DDoS sur la couche applicative, répartition par secteur



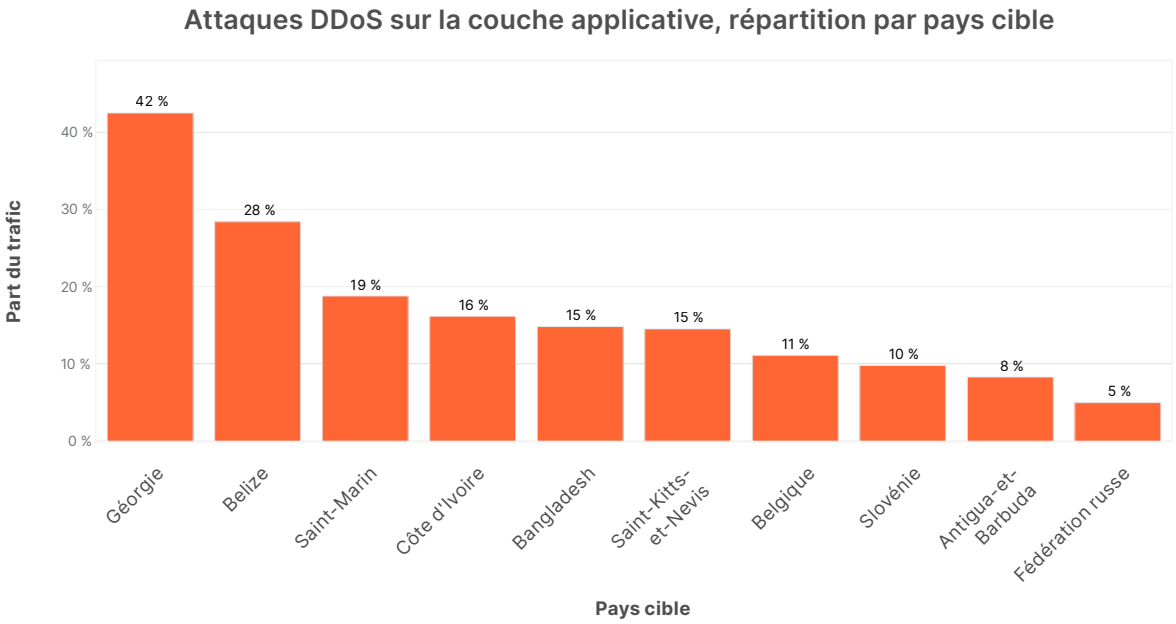
La répartition des attaques par région montre que le secteur des télécommunications a été le plus visé en Amérique du Nord et en Océanie.* En Amérique du Sud et en Afrique, c'est le secteur de l'hôtellerie qui a été le plus fréquemment pris pour cible. En Europe et en Asie, le secteur des jeux/jeux de hasard a été le plus touché. Enfin, au Moyen-Orient, c'est le secteur de l'éducation qui a subi le plus d'attaques.

Principaux secteurs pris pour cible, par région

À l'exception des secteurs génériques, comme Internet et les services logiciels

Pays cibles d'attaques DDoS sur la couche applicative

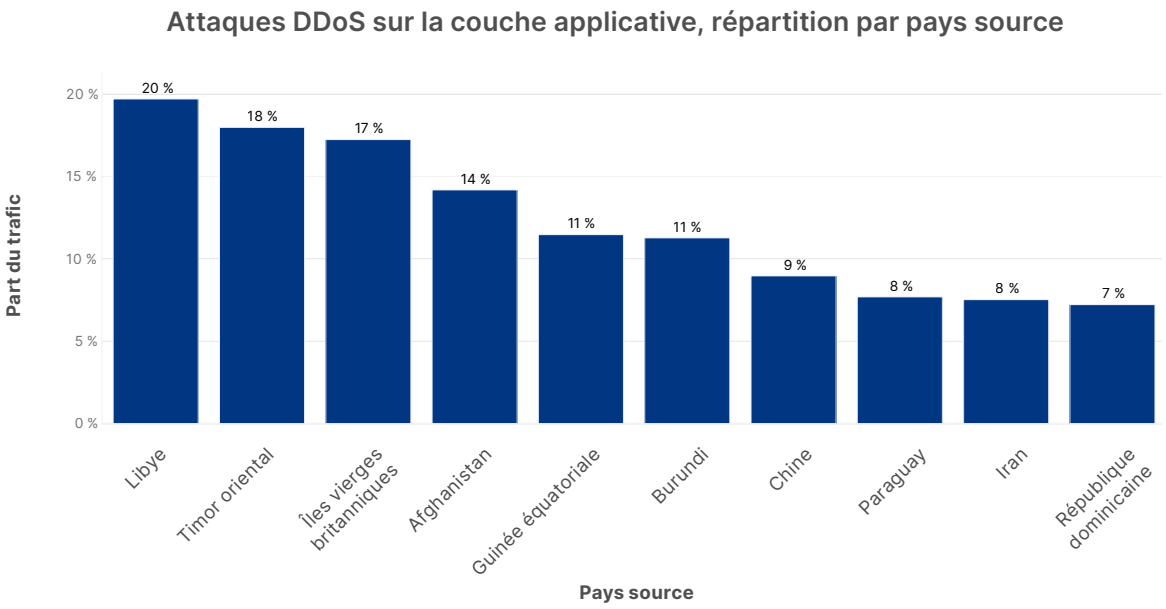
Le regroupement des attaques en fonction des adresses de facturation des clients nous permet de mieux comprendre quels pays sont les plus fréquemment attaqués. Au quatrième trimestre, les attaques DDoS représentaient plus de 42 % de l'ensemble du trafic acheminé vers les applications HTTP géorgiennes. La seconde place est attribuée à Belize, avec des attaques DDoS totalisant près d'un tiers de l'ensemble du trafic acheminé vers les clients. Saint-Marin vient ensuite, à un peu moins de 20 %.



Source d'attaques DDoS sur la couche applicative

Dans le cadre de notre analyse des tendances en matière d'attaques, nous observons les pays qui envoient et reçoivent le volume de trafic hostile le plus élevé. Il est toutefois intéressant de noter que les attaques DDoS sont souvent lancées à distance, afin de camoufler la véritable position géographique de l'acteur malveillant. Les principaux pays source indiquent le plus souvent la présence de nœuds de botnets agissant depuis ce pays. Ces derniers se présentent généralement sous la forme de serveurs ou d'appareils IdO compromis.

Au quatrième trimestre, les attaques DDoS représentaient près de 20 % de l'ensemble du trafic HTTP émis depuis la Libye. Les autres principaux pays comprennent le Timor oriental (18 %), les Îles vierges britanniques (17 %) et l'Afghanistan (14 %).



Attaques DDoS sur la couche réseau

Comme leur nom l'indique, les attaques DDoS sur la couche réseau cherchent à submerger l'infrastructure réseau. Alors que les attaques DDoS sur la couche applicative (également appelées attaques à haut débit binaire) tentent de saturer la connexion Internet afin de créer un événement de déni de service, les attaques sur la couche réseau (ou attaques à haut débit de paquets) ont pour objectif de désactiver les équipements inline, notamment les routeurs, les serveurs et la liaison Internet elle-même. Si une attaque envoie plus de paquets que les serveurs ou les autres équipements inline ne peuvent en gérer, ces derniers peuvent alors ne plus être en mesure de traiter le trafic légitime, soit un événement susceptible d'entraîner une dégradation des performances ou une panne du système.

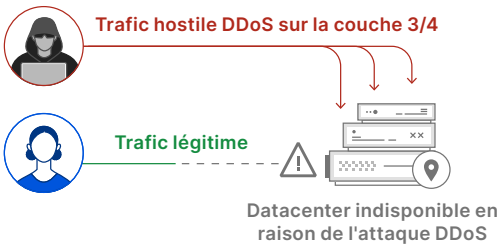
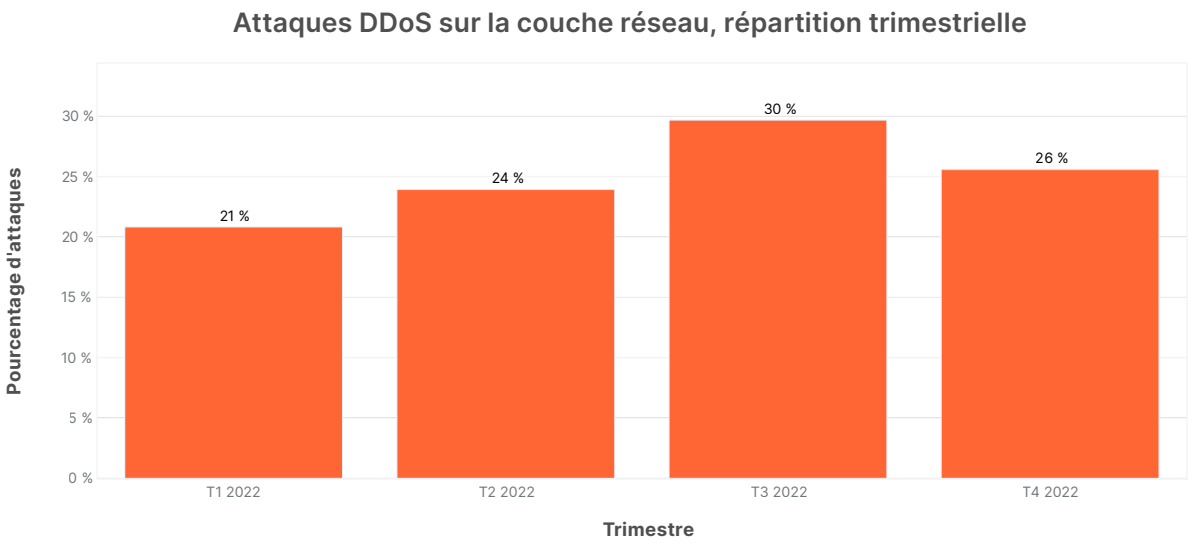


Schéma d'une attaque DDoS sur la couche réseau aboutissant à un événement de déni de service pour les utilisateurs légitimes

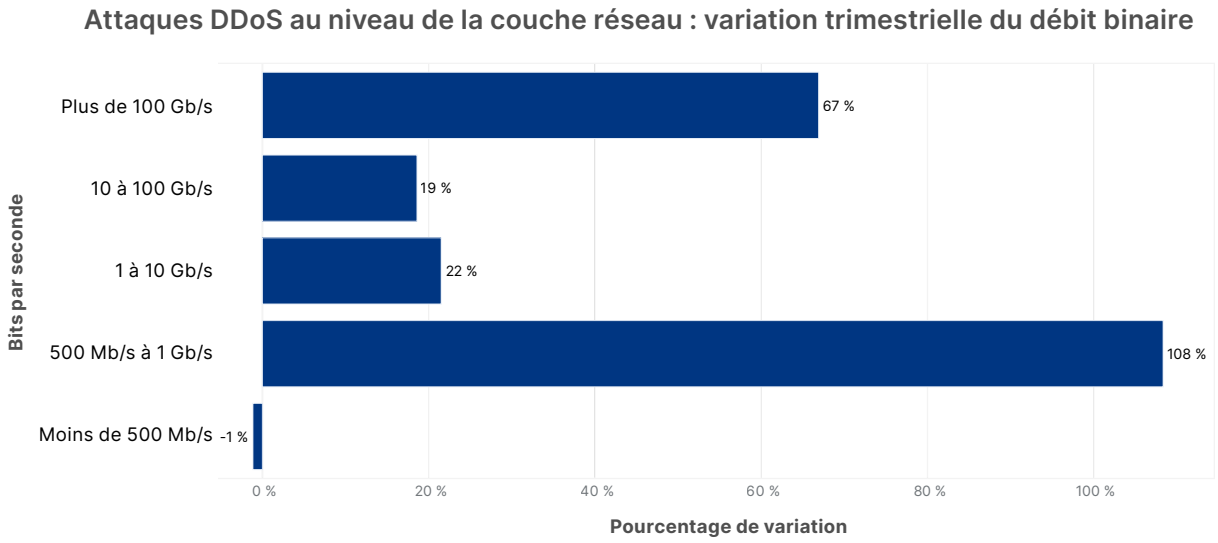
Tendances des attaques DDoS au niveau de la couche réseau

Après une année d'augmentation continue des attaques DDoS sur la couche réseau, le nombre d'attaques au quatrième et dernier trimestre de l'année a diminué de 14 % par rapport au trimestre précédent et de 13 % par rapport à l'année précédente. Si nous n'avons pas de données définitives sur les raisons de cette baisse, nous avons constaté que les médias évoquaient de plus en plus fréquemment des opérations de neutralisation de plateformes d'attaques DDoS à la demande (« DDoS-for-hire »). Cette couverture médiatique accrue peut également indiquer la mise en place proactive de systèmes d'atténuation des attaques DDoS par les entreprises afin de protéger leurs réseaux.

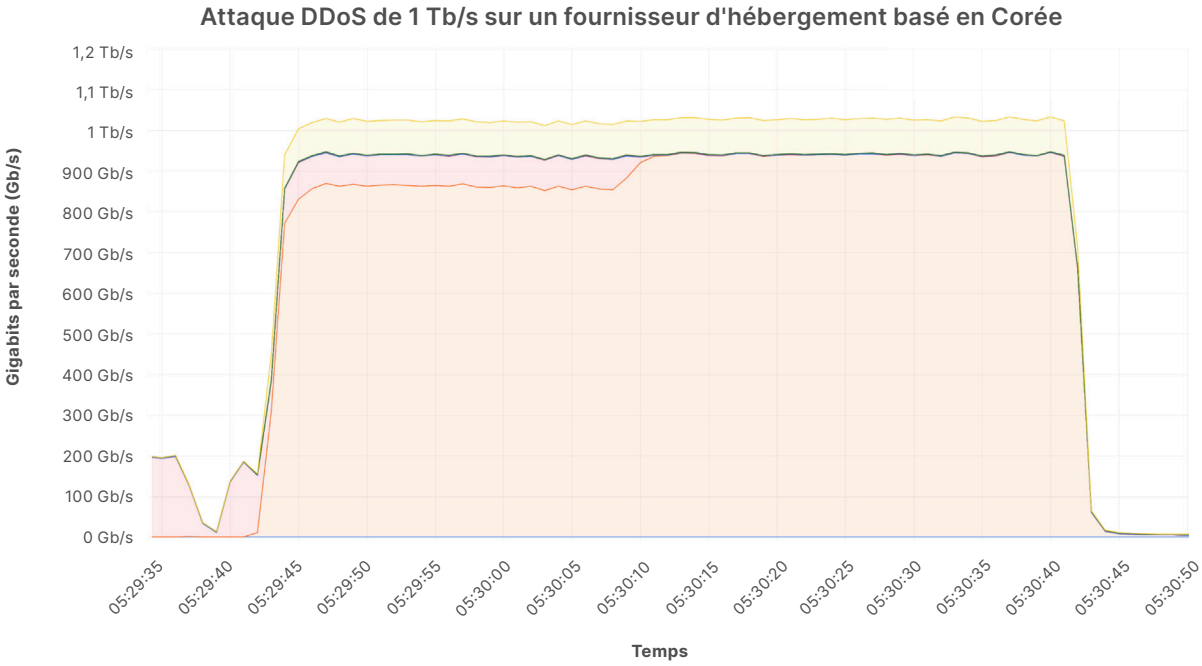


Débit des attaques DDoS sur la couche réseau

Si l'immense majorité des attaques sur la couche réseau se révèlent relativement brèves et de petite taille, nous avons constaté un pic des attaques de plus longue durée et de plus grande ampleur ce trimestre. Le nombre d'attaques DDoS volumétriques sur la couche réseau dont le débit dépassait les 100 Gb/s a augmenté de 67 % par rapport au trimestre précédent. De même, les attaques situées dans une plage de 1 à 100 Gb/s ont augmenté d'environ 20 % par rapport au trimestre précédent, tandis que les attaques comprises entre 500 Mb/s et 1 Gb/s ont augmenté de 108 % sur la même période.

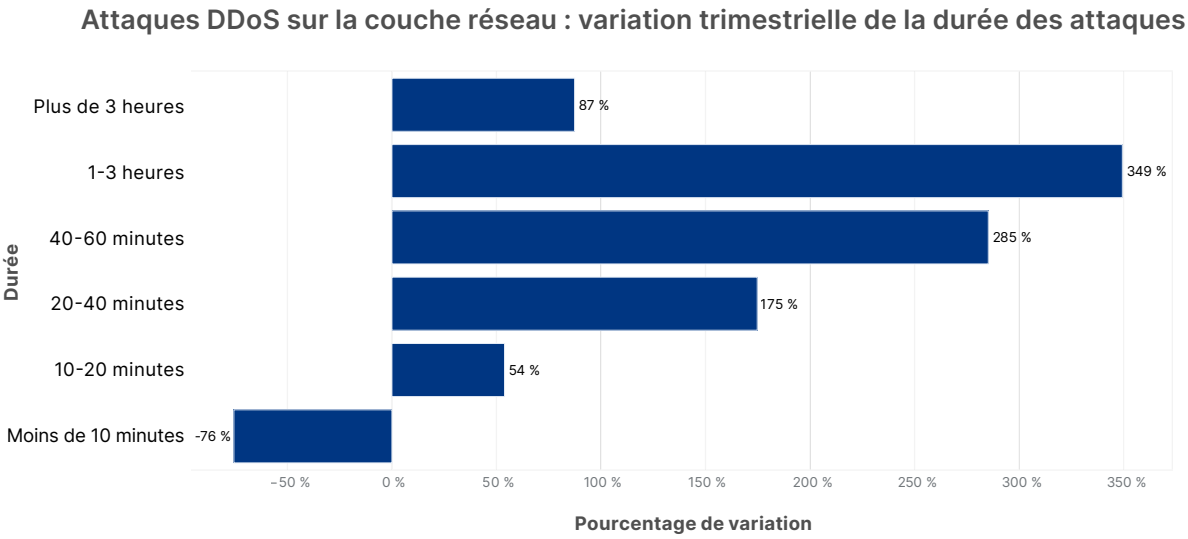


Pendant la dernière semaine de novembre, nous avons observé une attaque DDoS de 1 Tb/s ciblant un fournisseur d'hébergement basé en Corée. L'attaque (par ACK flood) a duré près d'une minute, avant d'être automatiquement détectée et atténuée à l'aide du service de protection contre les attaques DDoS sur la couche 3 de Cloudflare, Magic Transit.



Durée des attaques DDoS sur la couche réseau

Au quatrième trimestre, le nombre d'attaques d'une durée inférieure à 10 minutes a diminué de 76 % par rapport au trimestre précédent, tandis que la fréquence des attaques de plus longue durée a augmenté. Plus spécifiquement, le nombre d'attaques d'une durée comprise entre 1 et 3 heures a augmenté de 349 % par rapport au trimestre précédent, tandis que le nombre d'attaques d'une durée de trois heures ou plus a augmenté de 87 % sur la même période.



Vecteurs des attaques DDoS sur la couche réseau

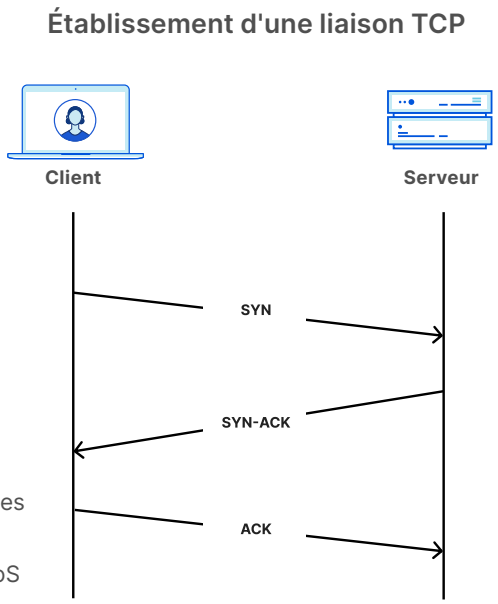
Au quatrième trimestre, le principal vecteur d'attaque observé (c'est-à-dire, la méthode de cette dernière) était le SYN flood, qui totalisait près de la moitié de l'ensemble des attaques DDoS sur la couche réseau atténuées par Cloudflare.

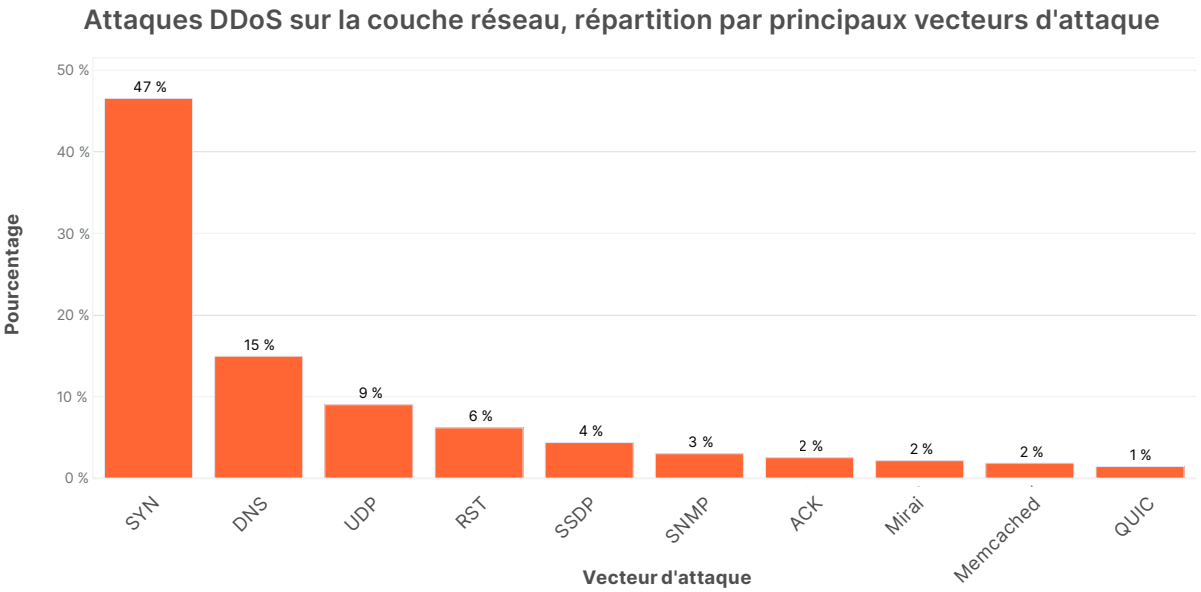
Les attaques SYN flood visent à saturer les ports des serveurs à l'aide de paquets SYN. Les attaques SYN flood exploitent le caractère dynamique de la négociation TCP en trois temps, qui constitue le moyen principal d'établissement d'une connexion entre un serveur et un client.

Lors d'une négociation TCP, une certaine quantité de mémoire est allouée à chaque connexion. Dans une attaque SYN flood, les adresses IP source peuvent être usurpées (modifiées) par un acteur malveillant. Le serveur répond alors à l'aide de paquets SYN/ACK aux adresses IP usurpées. Les adresses IP usurpées ignorent ces paquets, tandis que le serveur continue d'attendre (en vain) les paquets ACK afin de finaliser la négociation. Après un certain temps, le délai d'attente du serveur expire et les ressources correspondantes sont libérées.

Cette méthode d'attaque épuise rapidement les ressources du serveur, rendu incapable de gérer les connexions légitimes des utilisateurs, voire contraint à s'arrêter.

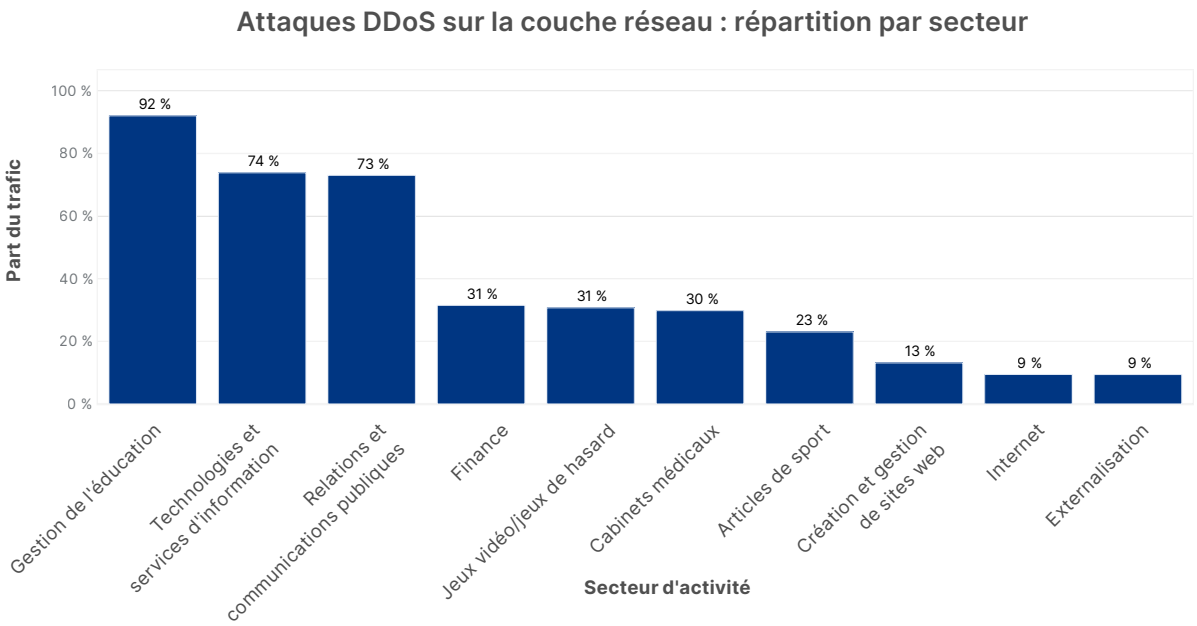
Après les attaques SYN flood, les attaques DNS flood et les attaques par amplification totalisaient environ 15 % de l'ensemble des attaques DDoS sur la couche réseau, tandis que les attaques DDoS et les floods basés sur le protocole UDP en représentaient 9 %.





Secteurs cibles d'attaques DDoS sur la couche réseau

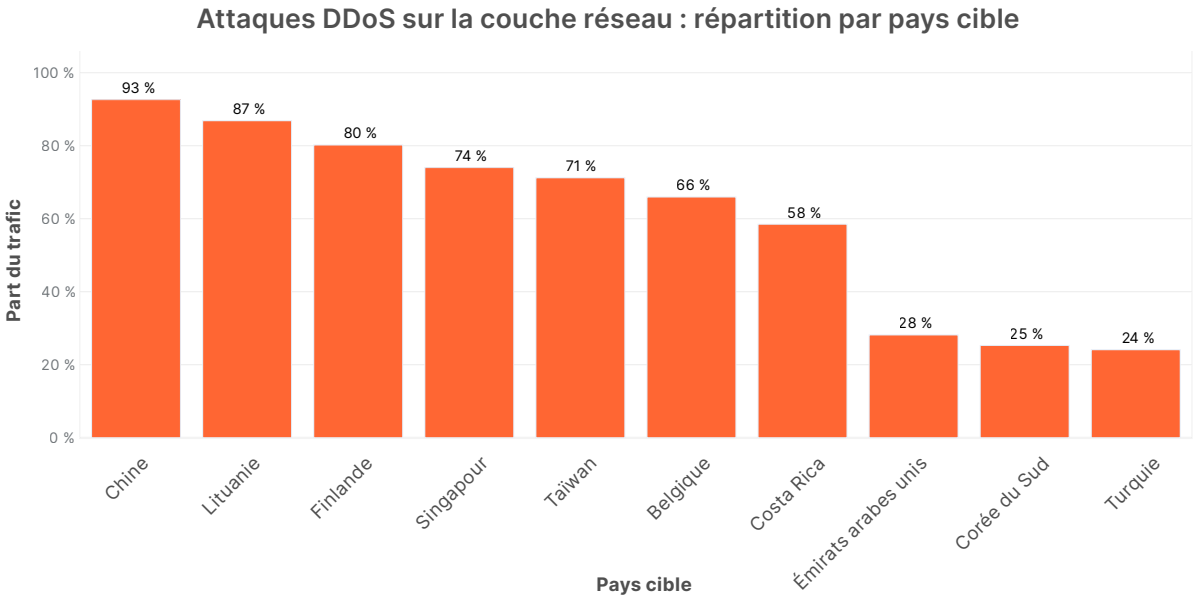
Au quatrième trimestre, le secteur de la gestion de l'éducation a observé le plus fort pourcentage de trafic lié à des attaques DDoS sur la couche réseau (92 %). Le secteur des technologies et des services de l'information a également enregistré un important trafic lié à des attaques DDoS sur la couche réseau (74 %), suivi par le secteur des relations et des communications publiques à la troisième place (73 %).



Secteurs cibles d'attaques DDoS sur la couche réseau

Le regroupement des attaques en fonction du pays de facturation de nos clients nous permet de suivre quels pays subissent le plus grand volume d'attaques. Au quatrième trimestre, le trafic des attaques DDoS sur la couche réseau représentait 93 % de l'ensemble du trafic web destiné à des propriétés web situées en Chine.

Les autres pays fortement touchés par les attaques sur la couche réseau sont la Lituanie (87 %), la Finlande (80 %), Singapour (74 %) et Taïwan (71 %).

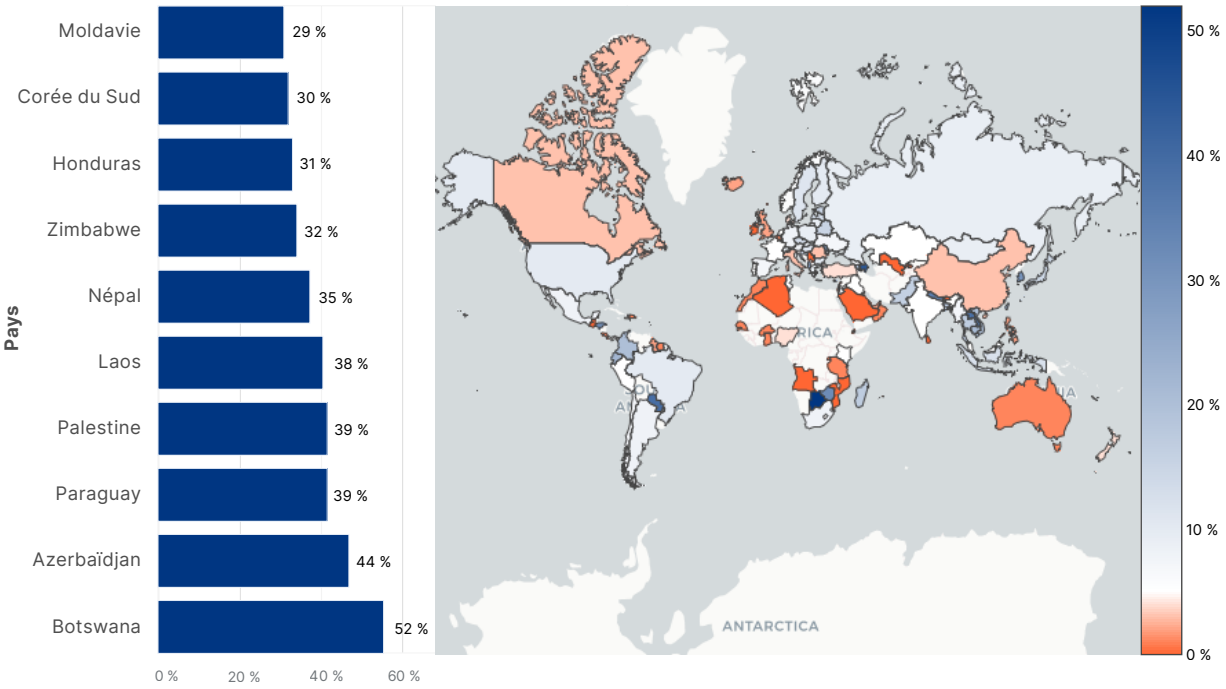


Source d'attaques DDoS sur la couche applicative

Afin de mieux comprendre d'où provenait le trafic hostile, nous avons observé les adresses IP au niveau de la couche applicative. Cette méthode est utile, car les adresses IP ne peuvent pas être usurpées au niveau de cette couche, tandis qu'elles peuvent l'être au niveau de la couche réseau. Pour identifier l'origine des attaques sur la couche réseau, nous utilisons l'emplacement géographique de nos datacenters afin d'observer à quel endroit les paquets hostiles ont été ingérés.

Au quatrième trimestre, le trafic hostile totalisait plus de 52 % de l'ensemble du trafic web ingéré dans notre datacenter implanté au Botswana. Les autres principaux pays de cette catégorie sont l'Azerbaïdjan (43 %), le Paraguay (39 %), la Palestine (39 %), le Laos (38 %) et le Népal (35 %).

Attaques DDoS sur la couche réseau : principaux pays source de trafic entrant au niveau mondial



Trafic hostile par rapport au trafic total

Remarque : *les fournisseurs d'accès Internet peuvent parfois acheminer différemment le trafic et fausser les résultats. Le trafic en provenance de Chine peut ainsi être acheminé via la Californie, pour différentes raisons opérationnelles.*

Menaces DDoS émergentes

Au quatrième trimestre, trois attaques DDoS ont connu un pic important par rapport au trimestre précédent : les attaques Memcached, les attaques SNMP et les attaques VxWorks.

Les attaques DDoS Memcached ont augmenté de 1 338 % depuis le troisième trimestre 2022. Memcached est un système de mise en cache de base de données qui accélère les sites web et les réseaux, mais dont les serveurs peuvent être utilisés de manière abusive pour lancer des attaques DDoS par amplification/réflexion.

Ces attaques fonctionnent en demandant du contenu au système de mise en cache et en usurpant l'adresse IP de la victime, qu'elles utilisent comme adresse IP source dans les paquets UDP. La victime est alors submergée de réponses Memcached susceptibles d'être amplifiées jusqu'à 51 200 fois.

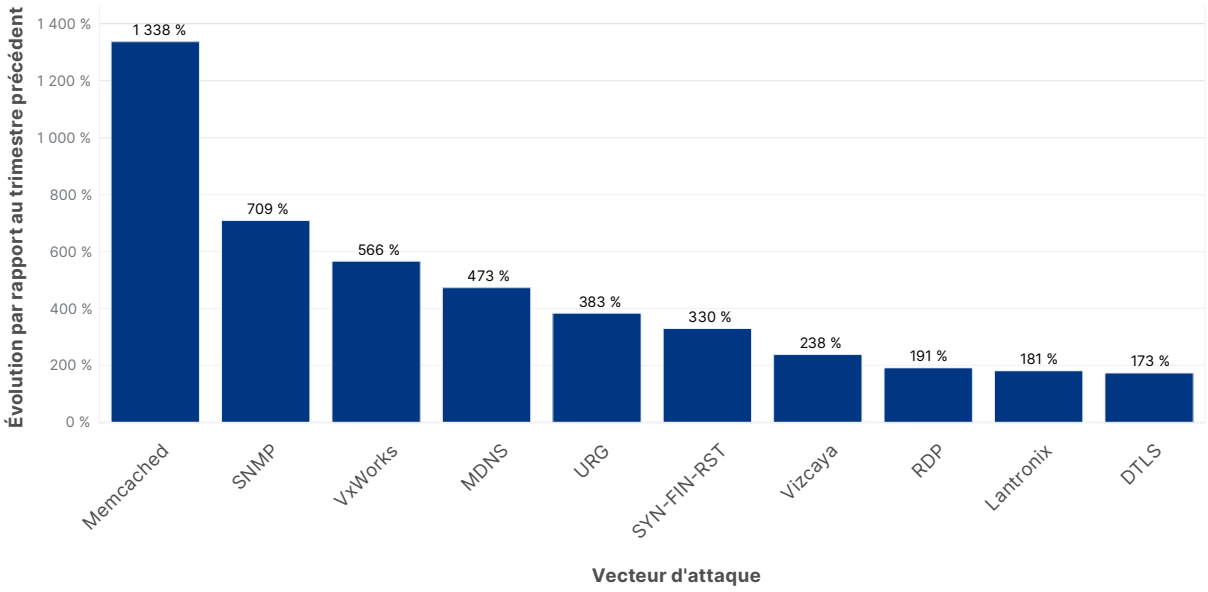
Les attaques DDoS basées sur le protocole SNMP ont également augmenté de 709 % par rapport au trimestre précédent. Basé sur UDP, le protocole SNMP (Simple Network Management Protocol) est fréquemment utilisé pour l'identification et la gestion d'appareils connectés au réseau, comme les imprimantes, les commutateurs, les routeurs et les pare-feu qui s'appuient sur le port UDP 161.

Lors d'une attaque par réflexion SNMP, l'acteur malveillant transmet un grand nombre de requêtes SNMP tout en usurpant l'adresse IP source du paquet. Cette opération lui permet de cibler des appareils connectés au réseau. Il en résulte une attaque DDoS volumétrique lorsque les appareils tentent de répondre à ces requêtes frauduleuses.

En troisième position, les attaques DDoS basées sur VxWorks ont augmenté de 566 % par rapport au trimestre précédent. VxWorks est un système d'exploitation en temps réel (RTOS, Real-Time Operating System) souvent utilisé dans les systèmes embarqués, tels que les appareils IdO. Il est également utilisé par les équipements de connectivité réseau et de sécurité, comme les commutateurs, les routeurs et les pare-feu.

Par défaut, VxWorks dispose d'un service de débogage activé automatiquement, qui peut servir à lancer des attaques DDoS par amplification. Révélée dès 2010, cette exploitation de vulnérabilité (CVE-2010-2965) constitue toujours une menace pour les appareils ciblés.

Attaques DDoS sur la couche réseau, répartition par principales menaces émergentes



Conclusion

À l'approche de la fin de l'année 2022, les attaques de plus longue durée et de plus grande ampleur ont gagné en fréquence. La durée des attaques a augmenté dans tous les secteurs, tandis que les attaques volumétriques ont fortement progressé et que les attaques DDoS avec demande de rançon ont poursuivi leur essor. Pendant les fêtes de fin d'année 2022, les secteurs de l'aéronautique/aérospatiale et celui des services événementiels ont été les plus fréquemment pris pour cible par les attaques DDoS au niveau de la couche applicative. Les attaques DDoS sur la couche réseau ont visé des entreprises du secteur des jeux/jeux de hasard, du secteur finance et du secteur de la gestion de l'éducation. Nous avons également constaté une évolution concernant les principales menaces émergentes, tandis que la fréquence et la sévérité des attaques DDoS basées sur Memcached ont continué à augmenter.

La défense contre les attaques DDoS est essentielle pour les entreprises de toutes tailles. Si les attaques sont lancées par des humains, elles sont mises en œuvre par des bots, qui se révèlent pratiquement impossibles à atténuer à grande échelle. Les processus de détection et d'atténuation des attaques doivent être aussi automatisés que possible, car le fait de s'en remettre uniquement aux humains constitue un désavantage pour les défenseurs. L'étendue du réseau mondial de Cloudflare nous permet d'observer les schémas de trafic malveillant, de suivre les menaces émergentes et d'atténuer automatiquement les attaques à la place des clients, afin de les décharger de cette tâche.

Au fil des ans, il est devenu plus facile et moins cher pour les auteurs d'attaques et les « prestataires de services d'attaque » de lancer des attaques DDoS, qui sont ainsi devenues plus accessibles. 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 importantes 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.

Cloudflare s'est donné pour mission de contribuer à bâtir un Internet meilleur, c'est-à-dire un Internet plus sécurisé, plus rapide et plus fiable pour tous.

Inscrivez-vous pour assister au webinaire consacré aux tendances des attaques DDoS afin d'en apprendre plus sur les menaces DDoS émergentes et la marche à suivre pour vous défendre contre elles.

Modifications des méthodologies d'établissement de rapports

Depuis notre premier rapport consacré aux tendances des attaques DDoS publié en 2020, nous avons toujours utilisé des pourcentages pour représenter le trafic hostile (c'est-à-dire, le pourcentage de trafic hostile par rapport à l'ensemble du trafic, trafic légitime inclus). Nous avons adopté cette démarche afin de normaliser nos données, d'éviter les biais et de bénéficier d'une plus grande flexibilité lors de l'incorporation des données de nouveaux systèmes d'atténuation à nos rapports.

Dans ce rapport, nous avons modifié la méthode de calcul de ces pourcentages pour les catégories suivantes :

- Secteurs cibles d'attaques DDoS sur la couche applicative
- Pays cibles d'attaques DDoS sur la couche applicative
- Source d'attaques DDoS sur la couche applicative
- Secteurs cibles d'attaques DDoS sur la couche réseau
- Secteurs cibles d'attaques DDoS sur la couche réseau

Nous divisions jusqu'à présent le nombre de requêtes HTTP/S liées à une attaque au sein d'une dimension donnée par le nombre total de requêtes HTTP/S dans l'ensemble des dimensions. Dans la section concernant la couche réseau, plus spécifiquement pour les catégories des secteurs cibles et des pays cibles, nous divisions la quantité de paquets IP liés à une attaque au sein d'une dimension donnée par le nombre total de paquets liés à une attaque sur l'ensemble des dimensions.

- **Pourcentage de trafic lié à des attaques DDoS sur la couche applicative :** $\frac{attack\_requests\_to\_dimensionX}{all\_requests}$
- **Pourcentage de trafic lié à des attaques DDoS sur la couche réseau :** $\frac{attack\_packets\_to\_dimensionX}{all\_attack\_packets}$

À compter de ce rapport, nous diviserons désormais uniquement le nombre de requêtes (ou de paquets) liées à une attaque au sein d'une dimension donnée par le nombre total de requêtes (ou de paquets) transmis au sein de cette dimension. Nous avons effectué ces modifications dans le but de normaliser nos méthodes de calcul dans l'ensemble du rapport et d'améliorer la précision de nos données, afin qu'elles reflètent mieux le panorama des attaques.

- **Pourcentage de trafic lié à des attaques DDoS sur la couche applicative :** $\frac{attack\_requests\_to\_dimensionX}{all\_requests\_to\_dimensionX}$
- **Pourcentage de trafic lié à des attaques DDoS sur la couche réseau :** $\frac{attack\_packets\_to\_dimensionX}{all\_packets\_to\_dimensionX}$

Ainsi, en suivant notre méthode de calcul précédente, le secteur le plus visé par les attaques DDoS sur la couche applicative était celui des jeux/jeux de hasard. Les requêtes liées à des attaques contre ce secteur représentaient 0,084 % de l'ensemble du trafic (lié ou non à des attaques) par rapport à l'ensemble des secteurs. Avec cette même méthode, le secteur de l'aéronautique et de l'aérospatiale arrivait à la 12e place (0,0065 %).

Après la modification de notre méthode de calcul, le secteur de l'aéronautique/aérospatiale est devenu le secteur le plus fréquemment visé, les attaques représentant 35 % de l'ensemble du trafic (lié ou non à des attaques) vers ce seul secteur. Avec cette même méthode de calcul, le secteur des jeux/jeux de hasard occupait la 14e place (2,4 %).

Aucune autre modification n'a été apportée aux méthodes de calcul de ce rapport. L'indicateur « Source des attaques DDoS sur la couche réseau » emploie la nouvelle version de notre méthode de calcul depuis notre premier rapport de 2020. Par ailleurs, aucune modification n'a été apportée aux sections « Attaques DDoS avec demande de rançon », « Débit des attaques DDoS », « Durée des attaques DDoS », « Vecteurs d'attaques DDoS » et « Principales menaces émergentes ». Ces indicateurs ne prennent pas en compte le trafic légitime et aucun alignement méthodologique n'a été nécessaire.

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

RÉV. : BDES-4180.2023JAN20