

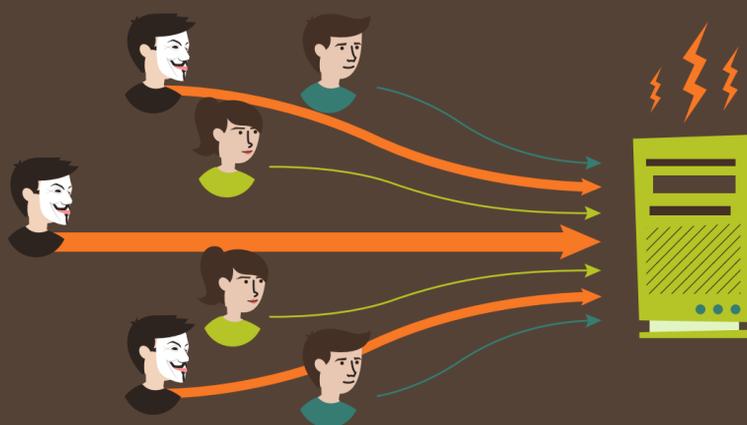


ATTAQUES DDoS MODERNES

Impact et coût des attaques DDoS

Définition des attaques DoS et DDoS

Les attaques de déni de service (DoS) et de déni de service distribuées (DDoS) sont des moyens employés par des individus ou des organisations pour priver d'autres des services ou des ressources auxquels ils ont habituellement accès.



Principaux styles d'attaques DDoS



Attaques via trafic réseau excessif (attaques par saturation indirecte)

Parasitage des communications pour submerger le trafic Internet.



Attaques dirigées d'épuisement de service (attaques par saturation directe)

Saturation d'une ressource par des requêtes indiquant qu'elle ne peut communiquer avec de nouveaux utilisateurs.



Attaques réfléchies

Utilisation de nombreux tiers pour envoyer du trafic vers le système ciblé et inonder son réseau.



Attaques par exploitation de bugs ou mauvaise utilisation (attaques par manipulation des systèmes)

Envoi d'une requête provoquant une erreur dans le logiciel ou utilisant une fonction qui surcharge une ressource.

Principales raisons des attaques DDoS



Hactivisme

L'unique but de l'agresseur est la protestation sociale et politique par des attaques contre les plus grandes sociétés mondiales.



Extorsion et autres motivations financières

Le but de l'agresseur est de réaliser un gain financier en menaçant la santé financière d'une entreprise en ligne.



Cybercriminalité et crimes haineux

Bien que rares, ces cas proviennent de concurrents, de clients mécontents, d'anciens employés, ou de groupes d'agresseurs résolus à commettre des cybercrimes.



Expérimentation

De nombreuses attaques qui ne font jamais la une sont menées par des pirates débutants qui peaufinent leurs compétences techniques sur des cibles aléatoires.

Les attaques croissantes perturbent les entreprises

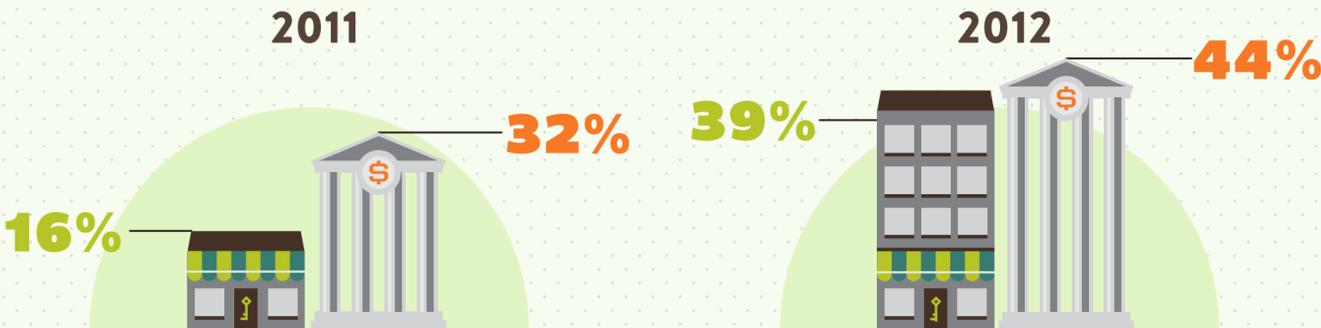
Un tiers (35%) des entreprises ont été victimes d'au moins 1 attaque DDoS en 2012, soit une hausse significative par rapport à 2011. Certains secteurs ont été plus durement touchés que d'autres. 39% des commerces et 44% des institutions financières telles que les banques ont été victimes d'attaques l'année dernière.



COMMERCES

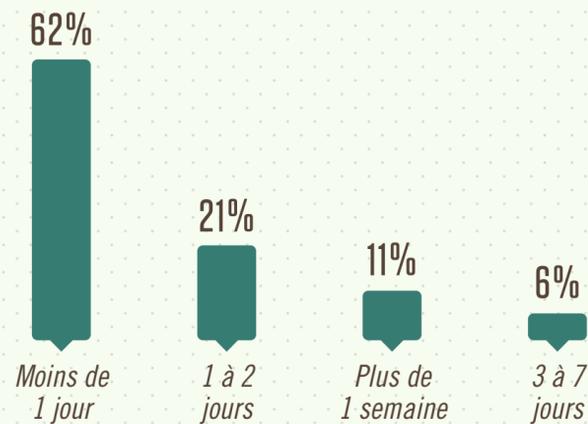


SERVICES FINANCIERS



Durée des attaques DDoS

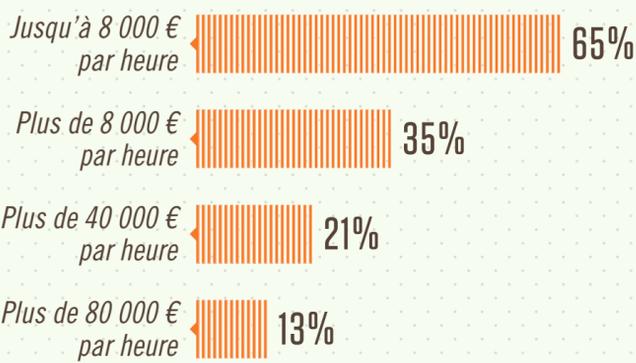
38% des attaques DDoS durent plus de 24 heures.



Selon une enquête annuelle récente menée auprès de professionnels de l'informatique d'entreprises nord-américaines, une attaque DDoS peut coûter de 8 000 € à 40 000 € par heure de chiffre d'affaires perdu.

Le coût élevé des temps d'arrêt

Plus de la moitié (65%) des entreprises déclare que les attaques DDoS leur coûteraient 200 000 € de chiffre d'affaires par jour.



Les dommages dépendent pour beaucoup du secteur : Plus de 80% des entreprises de services financiers indiquent qu'elles perdraient plus de 8 000 € par heure, et près de 70% des commerces déclarent qu'ils perdraient plus de 1,6 million d'euros par jour, ou plus de 80 000 € par heure, de chiffre d'affaires.

Éléments à considérer lors de la création d'un plan d'action



1. Comment déterminer que vous êtes victime d'une attaque DDoS ?



2. Quels sont les services essentiels ?



3. La disponibilité des services essentiels peut-elle être améliorée ?



4. Qui contacter en cas d'attaque et quelles sont les informations à fournir ?



5. Atténuation des attaques : automatique ou manuelle ?