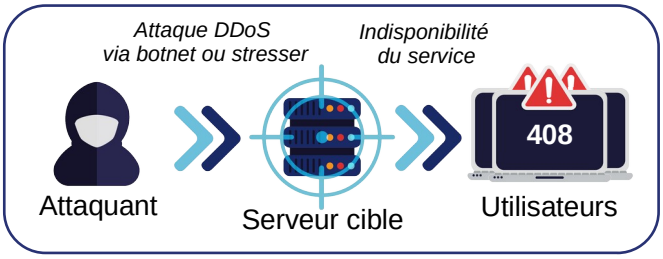
MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

COMCYBER-MI
« Nos forces, pour votre cyber-protection »

FICHE CYBER

Le déni de service distribué (*DDoS*), un phénomène cybercriminel

Confiance : **Bonne**
Statut : **En cours**
Secteurs affectés : **Tous**
Zones géographiques touchées : **Monde**
Objectifs : **Lucratif, sabotage, déstabilisation**



SYNTHÈSE

Le DDoS, ou "déni de service distribué", est une attaque informatique visant à saturer un site web ou un service avec des requêtes illégitimes. A l'image d'une foule envahissant un magasin et empêchant les clients légitimes d'entrer, le DDoS rend le service internet légitime inaccessible. Ce principe d'attaque simple et ancien, en augmentation en 2023, reste très utilisé en 2024 notamment contre des sites français.

I. Contexte : en quoi consiste ce phénomène cybercriminel ?

Les attaques par déni de service distribué (*DDoS*) constituent une forme de cybercriminalité visant à perturber les services ou le site *web* d'une entité en **saturant ses machines de trafic malveillant**.

Elles peuvent cibler tout système connecté à internet (box, serveur, objet connecté etc.). En pratique, cela se concrétise par l'utilisation simultanée d'un grand nombre de systèmes compromis, formant ainsi un ***botnet***, ou par l'utilisation d'une machine puissante couplée à une connexion internet importante, constituant un ***stresser***.

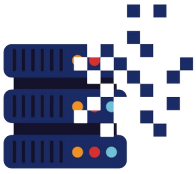
Ces dispositifs sont utilisés pour générer un trafic excessif sur les serveurs ou l'ordinateur cibles et entraîner une congestion du réseau. Mobilisés intensivement, les services légitimes seront rendus indisponibles temporairement ou de façon prolongée pour les utilisateurs. Les attaques *DDoS* ne sont pas destinées à s'introduire dans un SI et à accéder aux données de la cible, mais plutôt à compromettre sa **disponibilité**.

Les conséquences pour les systèmes ciblés sont souvent limitées : **les attaques durent fréquemment de quelques minutes à quelques heures**. Lorsque les effets de l'attaque sont plus longs, les répercussions peuvent être plus graves pour les organisations victimes (**réputation**, **perte de confiance de leurs clients**) ou bien **entraîner** des **pertes financières** plus ou moins importantes selon le temps d'indisponibilité de leurs services.

L'année 2023 et le début 2024 ont ainsi été marqués par des attaques visant des entreprises ou des institutions françaises en résonance avec des **événements sociaux, sociétaux et géopolitiques nationaux ou internationaux**.

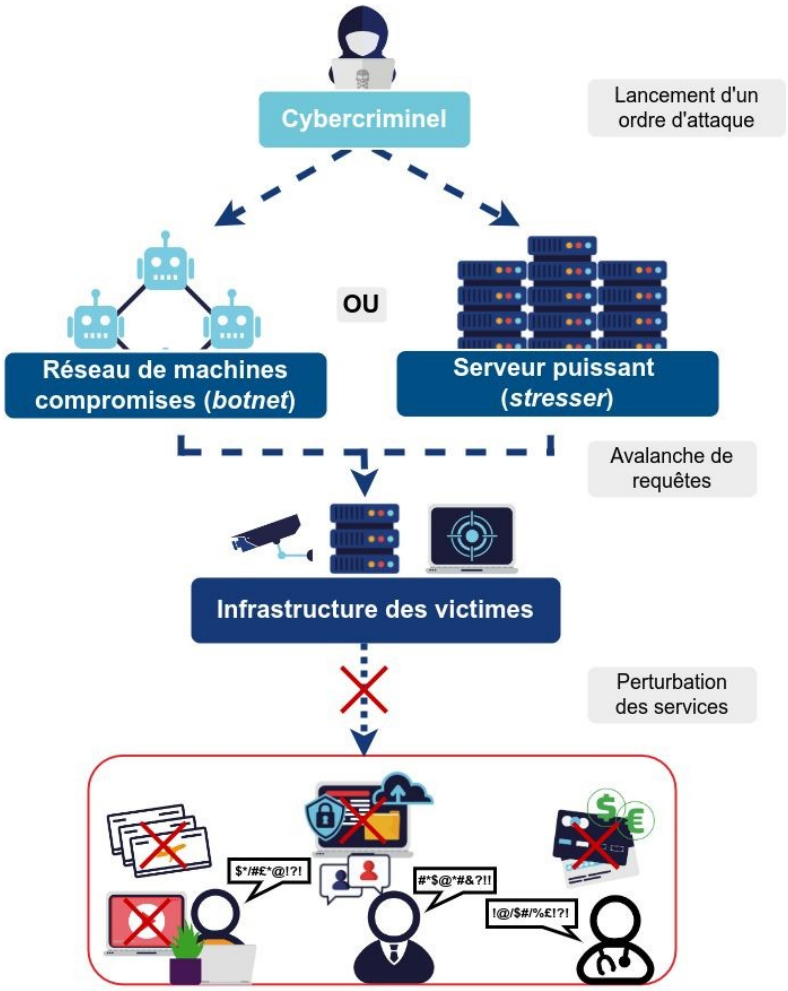
II. Profils et objectifs des cybercriminels

Les profils des cybercriminels qui orchestrent des attaques par déni de service distribué (*DDoS*) sont divers.
Certains sont des **hacktivistes**, tandis que d'autres sont des **pirates informatiques**. On retrouve aussi des ***script-kiddies***, souvent jeunes et peu expérimentés.



Les motivations des attaquants utilisant les attaques *DDoS* sont variées.
On y trouve des **revendications idéologiques**, des **intérêts politiques**, des **compétitions malveillantes**, l'**appât du gain** (actes d'extorsion, rétribution d'attaques menées) ou le **vandalisme numérique**.
Certains attaquants cherchent avant tout une **médiatisation** de leurs actions.
Les attaques *DDoS* peuvent également servir d'outil de **déstabilisation** ou de **sabotage contre des entreprises ou des États.**

III. Modes opératoires



Les attaques par déni de service distribué (*DDoS*) adoptent différents modes opératoires pour perturber les services en ligne des cibles.

Parmi les variantes notables, on retrouve :

- Le ***DDoS as a Service***, permettant aux attaquants de louer des services d'attaque *DDoS* à des prestataires ;
- Le ***Ransom DDoS***, où une rançon est exigée par les criminels pour mettre fin à l'attaque ;
- L'**amplification *DDoS***, exploitant des protocoles amplificateurs pour accroître l'impact de l'attaque.

Le *DDoS* est à la portée de nombreux pirates informatiques, même pour ceux sans compétences techniques avancées. La possibilité de louer certains services rend ce type d'attaque très abordable.

Les pirates les plus expérimentés n'ont parfois besoin que de louer l'accès à des ***botnets*** ou à des ***stressers***, dans le but de mener eux-mêmes les attaques.

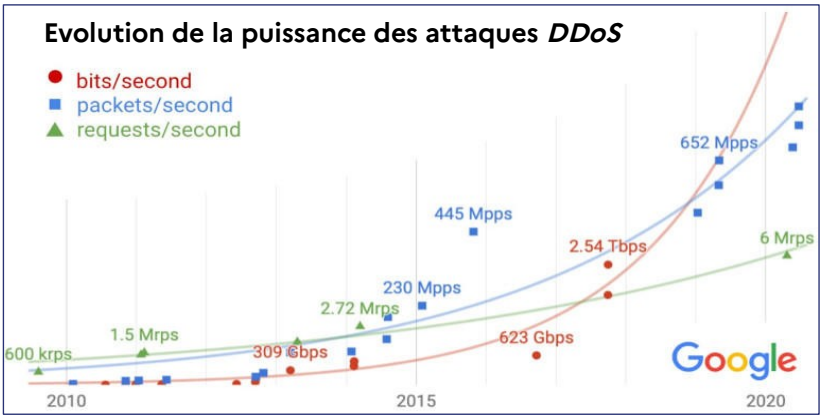
Les attaques par déni de service distribué (*DDoS*) sont en hausse tant en termes de fréquence (**+11 % en 2023)** qu'en matière d'intensité. Les cybercriminels continuent d'évoluer et adoptent des méthodes nouvelles d'amplification de leurs attaques (**0-day**, **http2**).

De plus, de nouveaux *botnets* continuent d'émerger et il est possible que l'assistance de l'intelligence artificielle, en plein essor, finisse par être intégrée dans ces attaques.

Comment s'en protéger

- renforcer la **détection précoce** ;
- **diversifier les points d'entrée réseau** ;
- utiliser des **pare-feu efficaces** ;
- **surveiller le trafic anormal** ;
- être réactif en **adaptant les règles de filtrage** à l'attaque subie ;
- élaborer des **plans de réponse aux incidents**.

Evolution de la puissance des attaques *DDoS*



SOURCES

https://cesin.fr/document.php?d=65b3d73136c80
https://www.cloudflare.com/fr-fr/learning/ddos/what-is-a-ddos-attack/
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/attaque-en-deni-de-service-ddos
https://cyber.gouv.fr/publications/denis-de-service-distribues-ddos