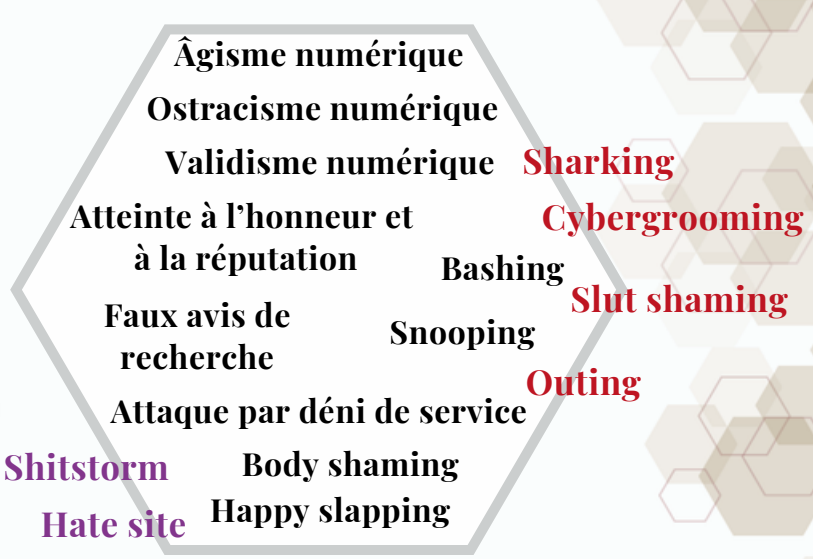
PROJET CYBERNETIC

# ATTAQUE PAR DENI DE SERVICE

*Etiologie des pratiques de cyberharcèlement*


POUVOIR

## SYNONYMES

- DoS
- DDoS
- Rapport de masse
- Faux rapport
- Massive reporting
- Bombardement de messages
- Message bombing
- Whamming
- Inondation
- Bombarderie

## Définition

### Concept-clé :

**Une attaque par déni de service (DoS) cherche à porter atteinte informatiquement à une victime en l'empêchant d'avoir accès temporairement ou indéfiniment à un lien réseau, à un service, à une application ou encore à un site web, qui lui sont indispensables, en submergeant le système de données.**

Ces cyberattaques sont particulièrement **fréquentes** au regard de la simplicité de leur mise en œuvre et de leur efficacité redoutable, tout spécialement contre une cible qui n'est pas préparée. Les **pertes financières et réputationnelles**, en raison de l'interruption de service ou encore indirectement par le préjudice porté à l'image, peuvent être considérables.

Une attaque par déni de service est le résultat d'une **attaque coordonnée** de plusieurs ordinateurs infectés furtivement (on parle de "**bot**" constitué par des PC Zombies que peuvent être un ordinateur, un smartphone, une cafetière connectée, etc.). La **simultanéité** de ces connexions **submerge** les ressources des infrastructures de la victime (site web, serveur ou réseau) qui finissent par **s'écrouler** ou **se bloquer**. Même si le site ne se paralyse pas, il ne peut plus répondre aux demandes légitimes. Un seul individu peut mener ce genre d'attaques en contrôlant furtivement plusieurs dizaines de milliers d'ordinateurs infectés à travers le monde. Il dispose ainsi d'une armée qu'il peut facilement monnayer.

# Ce qu'il faut retenir...

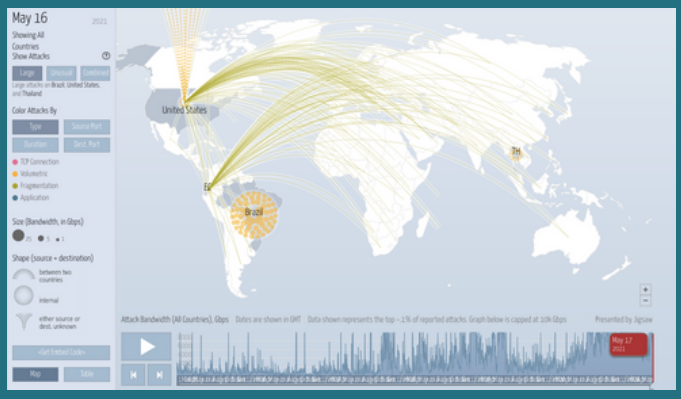
Un amalgame entre une attaque DoS (Denial of Service) et une attaque DDoS (Distributed Denial of Service) peut parfois prêter à confusion, alors que certains paramètres caractéristiques permettent pourtant de les dissocier :

- **Signification** : DoS signifie « Déni de service » / DDoS signifie « Déni de service distribué »
- **Source** : L'attaque DoS est issue d'une source simple (un ordinateur) / L'attaque DDoS inonde les systèmes de très nombreuses requêtes venant de plusieurs ordinateurs qui sont combinées ensemble pour former un gigantesque botnet
- **Vitesse** : L'attaque DoS est plus lente qu'une attaque DDoS / L'attaque DDoS est plus rapide que l'attaque DoS
- **Contrôle** : Une attaque DoS peut être bloquée plus facilement car un seul système est utilisé / L'attaque DDoS est plus compliquée à bloquer car elle provient de plusieurs emplacements
- **Traçage** : Les attaques DoS sont faciles à tracer car elles sont plus faciles à exécuter / Les attaques DDoS sont difficiles à tracer car elles affectent grandement les systèmes touchés et l'espoir de localiser la source de l'attaque est assez faible
- **Volume** : Le volume de trafic de données dans l'attaque DoS est inférieur à celui des attaques DDoS car il est exécuté à partir d'un seul système / Les attaques DDoS permettent à l'attaquant d'envoyer un plus grand trafic de données vers le réseau victime

De manière générale, les attaques DoS et DDoS peuvent être regroupées ainsi :
- **L'attaque sur le volume** : Il s'agit de submerger une cible par un afflux élevé de paquets ou de connexions (UDP, ICMP, etc.), saturant ainsi sa bande passante et qu'elle soit dans l'impossibilité de traiter le trafic et s'effondre.
- **L'attaque par le protocole** : Elle vise les ressources du réseau afin de saturer les connexions. Certaines spécificités de protocole (connexion en plusieurs temps) permettent à l'attaquant de commencer une requête, sans la finir, et ainsi submerger la cible de requête non aboutie.
- **L'attaque d'application** : Ces attaques visent les applications plutôt que le réseau.

> *Je n'ai pas pris ces menaces au sérieux. Quand l'attaque a été déclenchée, notre site Internet s'est retrouvé complètement paralysé.*

# Un exemple concret :




**Aux origines...**

Est identifiée comme la toute première **attaque DDoS**, celle qui s'est produite en juillet **1999** et qui a désactivé le réseau informatique de **l'université du Minnesota** pendant deux jours en infectant un total de **114 systèmes informatiques**, par le biais d'un **script** malveillant appelé **Trin00**.

Même si ce malware ne peut être considéré comme un grand ***botnet*** (ensemble d'appareils connectés sous le contrôle d'un attaquant), il n'en demeure pas moins qu'il s'agit là du premier incident enregistré faisant état de cyberattaquants qui se sont emparés d'ordinateurs qui ne leur appartenaient pas et qui ont **submergé le trafic web pour perturber le réseau.**

Peu de temps après ce premier incident, plusieurs sites web tels que **Yahoo**, **Amazon**, **Dell**, **CNN** ou encore **eBay**, ont été victimes à leur tour d'attaques DDoS, provoquant un **ralentissement** majeur de leur fonctionnement, voire rendant leurs portails internet **inaccessibles** pendant plusieurs heures.

Après quelques mois d'investigation, les forces de l'ordre ont réussi à identifier le cyberattaquant tant recherché qui se dissimulait sous le pseudonyme de **MafiaBoy** : (alias Michael Calce), ce jeune montréalais était seulement âgé de **15 ans** à l'époque des faits. Condamné à purger huit mois dans un centre de détection juvénile, il est devenu depuis **analyste en sécurité informatique.**

Au cours des deux décennies qui ont suivi, les attaques n'ont eu de cesse de s'amplifier et de compromettre des milliers de systèmes sur internet.

# Que dit le cadre légal...

L'incrimination principale qui peut être retenue pour les **attaques par déni de service** est celle de **l'entrave à un système de traitement automatisé de données (STAD).**

**L'article 323-1 du code pénal** précise que "*le fait d'**accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données***" *est passible de deux ans d'emprisonnement et de 60 000 euros d'amende. "Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système", les auteurs des faits sont passibles de trois ans d'emprisonnement et de 100 000 euros d'amende. "Lorsque les infractions [...] ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État, la peine est portée à cinq ans d'emprisonnement et à 150 000 euros d'amende*".

**L'article 323-2 du code pénal** peut être appliqué s'il concerne "*le fait d'**entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données***". *Il est passible d'une peine de cinq ans d'emprisonnement et de 150 000 euros d'amende. "Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État, la peine est portée à sept ans d'emprisonnement et à 300 000 euros d'amende*".

**L'article 323-3 du code pénal** dispose que "*le fait d'**introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient***" est passible de cinq ans d'emprisonnement et de 150 000 euros d'amende. "*Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État, la peine est portée à sept ans d'emprisonnement et à 300 000 euros d'amende*".

# Pour aller un peu plus loin...

## Quelques références scientifiques :


ABRUNTON Finn, Une histoire du spam. Le revers de la communauté en ligne, *Réseaux*, n° 197-198, 2016, pp. 33-67.

DE MEREUIL Albert, BONNEFOUS Annabel-Mauve, Anatomie d'une cyber-attaque contre une entreprise : comprendre et prévenir les attaques par déni de service, *Annales des Mines - Gérer et comprendre*, n° 123, 2016, pp. 5-14.

EVRON Gadi, Battling Botnets and Online Mobs: Estonia's Defense Efforts During the Internet War, Georgetown *Journal of International Affairs*, 2008, pp. 121-126.

McWILLIAMS Brian, *Spam Kings: The Real Story Behind the High-Rolling Hucksters Pushing Porn, Pills, and %*@)# Enlargements*, O'Reilly Media, 2014, 372 pages.

MARVIN Lee-Ellen, Spoof, Spam, Lurk and Lag: the Aesthetics of Text-Based Virtual Realities, *Journal of Computer-Mediated Communication*, Volume 1, n° 2, 1995, URL: https://onlinelibrary.wiley.com/doi/full/10.1111/j.1083-6101.1995.tb00324.x

PARIKKA Jussi, SAMPSON Tony D., *The Spam Book: On Viruses, Porn, and Other Anomalies from the Dark Side of Digital Culture, Hampton Press*, 2009.

SAUTER Molly, "LOIC Will Tear Us Apart: The Impact of Tool Design and Media Portrayals in the Success of Activist DDOS Attacks", *American Behavioral Scientist*, Volume 57, Issue 7, 2013, pp. 983-1007.


Certains sites comme https://www.digitalattackmap.com permettent de visualiser en temps réel combien d'attaques DDoS ont lieu dans le monde entier.