Forum: Sécurité

Topic: Cyberattaque massive

Subject: Re: Cyberattaque massive

Publié par: LoupBlanc

Contribution le : 14/03/2024 01:18:29

ahmgm a écrit:
Citation :

Oui, en effet le principe des attaques DDOS est de saturer par des millions de requêtes les serveurs d'un site mais ne s'attaque pas aux données.
Si les sites visés sont équipées d'un intranet, ils peuvent continuer à fonctionner en local, seules les trafics vers internet sont bloqués.
Il faut attendre que l'orage passe et mettre en place des mesures de blocages d'IPs non désirées,travail fastidieux mais nécessaire.

Tout à fait les attaques DDOS (Denial of service) n'ont pas pour objet de pirater des données en règle générale, le but est au contraire de les empêcher de transiter à travers le réseau.

Sans entrer dans les détails le but est de faire "tomber" le réseau plus rien ne rentre plus rien ne sort.

Par contre bémol:
L'intranet fonctionne sous DDOS: oui et non tout dépend de l'architecture réseau retenue et de l'attaque subie. Si c'est le serveur d'AD ou le serveur DHCP qui subi une attaque, ton intranet tombera comme n'importe quel fruit mur.
Et comme aujourd'hui la majorité des intranet locaux sont couplés à un Extranet la vulnérabilité à ce type d'attaques est très prégnante.

Comme le souligne **"ahmgm"** les mesures à prendre sont celles décrites.

Bref si vous voyez une erreur 502 quand vous essayez de vous connecter sur un site, c'est que en général le serveur est indisponible. Plus rarement vous aurez une erreur 511.
Une autre solution plus radicale consiste à isoler du réseau le serveur subissant l'attaque. Dans ces cas l'utilisateur aura une erreur 403 ou 404.

Bonne soirée