



Forum: Sécurité

Topic: Cyberattaque massive

Subject: Re: Cyberattaque massive

Publié par: ahmgm

Contribution le : 14/03/2024 09:57:23

Citation :

LoupBlanc a écrit:

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

Merci pour ces compléments d'informations détaillées que je confirme.

Dans ma réponse je ne savais pas si je pouvais donner toutes ces précisions.

Je travaillais dans une société avec un intranet protégé d'internet par un pare-feu matériel (sous Unix) très efficace, aussi en cas d'attaques DDOS de ce genre, nous n'étions pas bloqués dans nos tâches internes.