Les attaques par déni de service

Une attaque par déni de service a pour objectif d'empêcher l'accès à un serveur ou à un site Web. Les utilisateurs des services d'e-banking peuvent non seulement subir de telles attaques, mais aussi y participer inconsciemment. À vous de vous protéger !

Pour vous protéger contre les attaques DoS (par déni de service),

- utilisez un programme antivirus parfaitement à jour.
- surveillez les connexions avec un pare-feu.
- installez régulièrement les mises à jour de votre système d'exploitation et de tous les programmes installés.
- soyez attentif et vigilant.

Il existe différents types d'attaques DoS. La méthode la plus fréquente consiste à envoyer simultanément de très grandes quantités de données à un service hébergé sur un serveur, si bien que celui-ci se retrouve inondé de demandes et ne parvient plus à y répondre (ce qui peut se traduire p. ex. par l'impossibilité d'afficher le site Web dans le navigateur). En règle générale, ce type d'attaque ne comporte néanmoins ni le vol ni l'altération des données.

La plupart du temps, ces énormes quantités de données sont transmises à l'aide d'un réseau de bots (ou botnet). On parle alors d'une attaque par déni de service distribué (DDoS) (cf. ci-dessous).

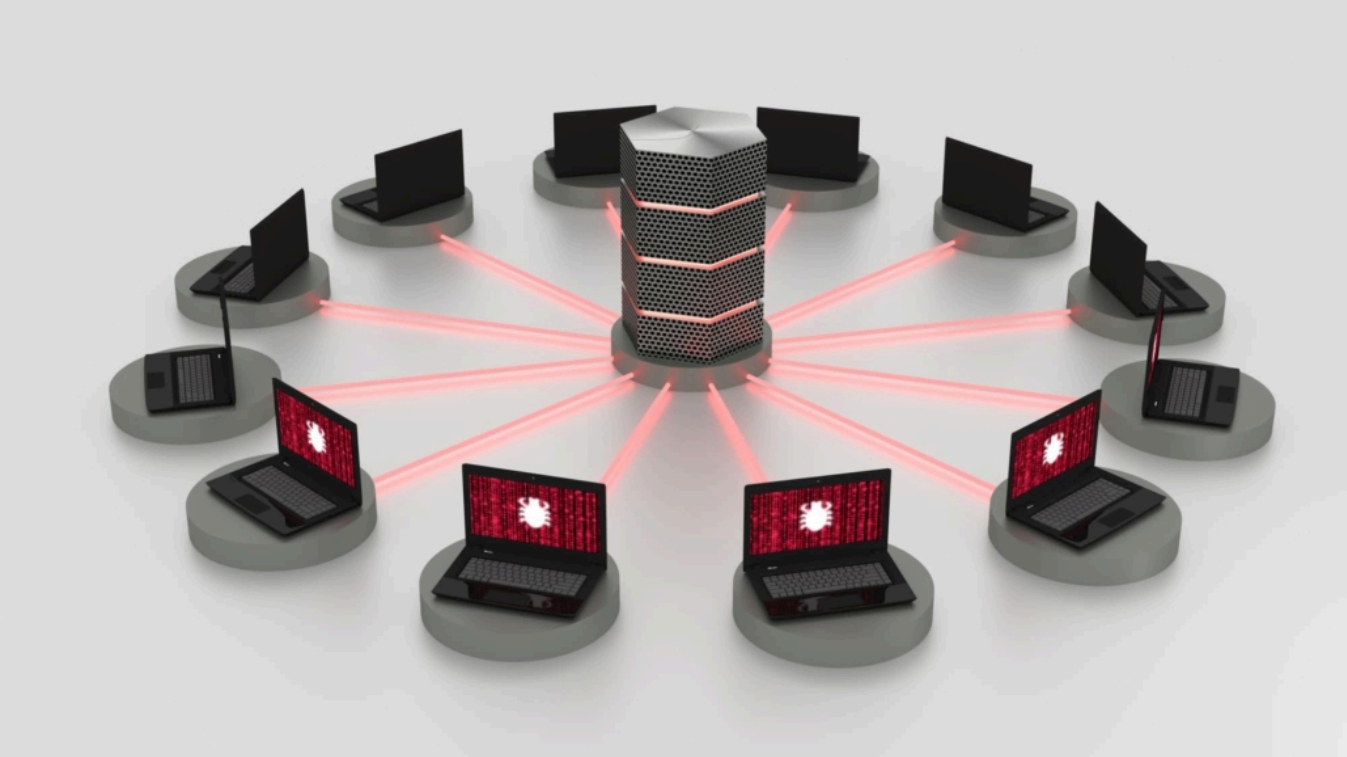
Afin d'empêcher que votre dispositif ne fasse partie d'un réseau de bots et ne devienne un « co-acteur involontaire » d'une attaque DDoS, il est donc essentiel de bien respecter les « 5 règles pour votre sécurité numérique » (https://www.ebas.ch/fr/5-regles-pour-votre-securite-numerique/) .

Attaque par déni de service distribué (DDoS – Distributed Denial of Service)

La méthode la plus fréquente des attaques DoS est ce que l'on appelle le déni de service distribué (DDoS) qui fait intervenir de manière coordonnée un très grand nombre de dispositifs.

L'attaque DDoS ou par déni de service distribué s'articule en deux temps. La première étape prévoit que l'assaillant se rende maître de plusieurs objets connectés à l'aide d'un cheval de Troie ou d'un autre maliciel pour constituer ainsi un botnet ou réseau de bots. La deuxième étape consiste à donner l'ordre à tous les dispositifs dont il a pris le contrôle d'attaquer la cible en même temps (p. x. : un site Web).

Une attaque DDoS est très efficace dans la mesure où elle part de plusieurs dispositifs simultanément, ce qui permet de générer très facilement l'importante quantité de données requise. Les cyberpirates l'utilisent principalement pour paralyser les serveurs et les sites Web. Dans le cas d'une attaque DDoS, il est généralement difficile de dénicher l'auteur de l'attaque dans la mesure où le dispositif de l'assaillant n'attaque pas lui-même directement la cible.



On parle d'une attaque par déni de service ou DoS (pour Denial of Service) lorsqu'un hacker sature ou suspend le fonctionnement d'un serveur ou d'un site Web en le bombardant de requêtes ciblées, le but étant d'en bloquer l'accès à l'ensemble des utilisateurs.

Ce type d'attaque concerne la plupart du temps des sites Web et ne comporte donc en règle générale pas de vol ni de compromission de données. Le hacker n'a pas d'autre intention que d'empêcher les utilisateurs d'accéder au site (pour l'e-banking par exemple).