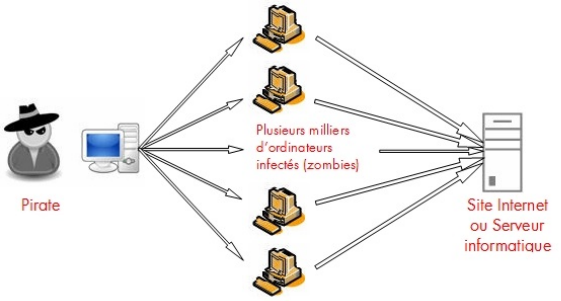
Dis papa, c’est quoi une attaque DDOS ?

	**Dis papa, c’est quoi une attaque DDOS ?**

L'objectif d'une attaque DDOS, (en déni de service) vise à rendre inaccessible ou inopérant un site Internet. Parmi les attaques les plus fréquemment lancées, ce sont les attaques en déni de service distribué (DDoS : Distributed Denial of Service) qui sont les plus fréquentes.

Ce type d'attaque s'appuie sur un principe simple, celui du nombre qui fait la force : Il suffit de faire en sorte que plusieurs milliers machines sur Internet lancent de façon synchronisée de multiples requêtes vers leur cible.

Les machines lançant ces attaques peuvent le faire soit à l'insu de leur propriétaire (cas d'un « botnet » ou réseau de machines zombies) ou alors le font sur demande explicite et consciente d'une personne (cyber hacktivisme).



Le pirate active à distance tous les zombies (plusieurs milliers) préalablement infectés et leur donne l'ordre de contacter simultanément une cible. Au bout de quelques minutes, cette cible ne peut plus répondre à de nouvelles connexions, elle devient inaccessible.

Saturation des ressources

Dans le deux cas, le résultat est le même : les capacités de traitement du site sont dépassées, celui-ci est inaccessible. La saturation peut concerner tant la bande passante de l'accès réseau, des tables de session d'un firewall, la CPU des serveurs web, …

En fonction du point de saturation, on peut constater un effet boule de neige : Si c'est la bande passante réseau qui est totalement consommée inutilement alors, non seulement le site visée par l'attaque sera bloqué mais tous les autres serveurs de la plateforme seront aussi inaccessibles.

Le trou-noir (« blackholing ») à la rescousse

Le trou-noir est l'une des contre-mesures utilisée communément pour contrer une attaque en DDoS. Le fournisseur d'accès Internet va activer, au sein de son réseau, une règle de routage spécifique afin de détruire tous les flux à destination de l'adresse IP ciblée par l'attaque.

Cela aura pour effet immédiat de bloquer les flux d'attaques en amont de l'accès réseau et donc d'annuler tout effet de saturation. Activer un blackholing ne nécessite aucun équipement spécifique car tout est réalisé via les fonctions de routage de paquets nativement présentes dans les équipements réseau.

Pour se protéger d'une attaque de ce type, plusieurs solutions existent, le blackholing en est une, la plus simple à mettre en oeuvre, mais comme à chaque fois, quand le voleur s'est fait piéger en rentrant par la porte, la prochaine fois il rentrera par la fenêtre ou ailleurs…

Vous avez été victime d'une attaque DDOS ?
Vous souhaitez mettre en oeuvre une protection ?
Profitez de notre expertise et consultez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source :
http://www.orange-business.com/fr/blogs/securite/series/les-5-minutes-du-professeur-audenard-episode-3-cleanpipe-bgp-et-gre