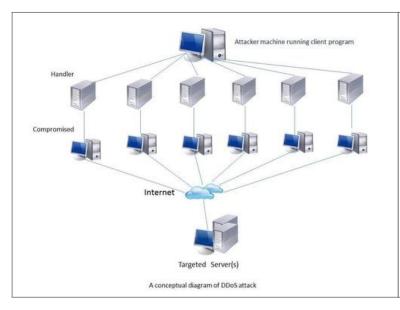
Comment se protéger des attaques DDoS ? | Denis JACOPINI



Comment se protéger des attaques DDoS ? Les entreprises doivent arrêter de compter sur leurs fournisseurs de services Internet pour les protéger des attaques DDOS et doivent prendre les choses en main.

Les attaques par Déni de Services Distribués (DDS) sont l'une des menaces Internet les plus anciennes et continuent d'être le principal risque pour les réseaux à travers le monde. En même temps que les protections ont évolué, la technologie utilisée par les hackers s'est adaptée et est devenue bauxcomp plus sophistiquée. De nouveaux typns d'attaques ciblent déscrasis les applications et services, et sont souvent occhés dans les couches 3 et 4, e qui les rend difficillement détectables. En matière d'attaques DDGs, les cettere financier es l'une des cibles privilégiées des opéreriainels, suivie de près par le secteur public. Dutre le fait de perturber les opérations internet par un assaut brutal de données, les attaques DDGs ont récement été utilisées pour recueillir des informations financières et relatives au comerce en ligne. Ces attaques ont souvent pour objectif de perturber les opérations, principalement en détruisant l'accès à l'information.

Il y a généralement trois catégories de motivations derirâre les attaques DDGs, poitique, de représsilles et financière. Les réfinancière, les rois entraines poitiques, sociales ou religieuses. Lorsqu'un botnet ou un important réseau cybercrissinel, est démanté, cela peut déclencher des attaques de représsilles contre cœux qui ont aidé ou assist la sutorités. Les attaques motivées par l'argent suivent un schéma « pay-te-play » dans lequel les hackers sont compensés par une tierce partie qui leur desande de mener l'attaque pour elle. Quelle que soit la motivation, le résultes et le même « voir réseau et services en liuges doits entrain indisponibles, et pevent restre impondant un lang moment.

ffizer-vous des attaques DDOS avancées visant la couche applicative

Lesiste de mondreux types of sittaque DDOS avancées visant la couche applications. L'inondation de requêtes SYN et NITP GET sont les plus communes et utilisée pour recharger les communes et utilisée applications visant la couche 7 et ciblant les applications. L'inondation de requêtes SYN et NITP GET sont les plus communes et utilisée pour recharger les communes intéres au les serveurs derrières les pare-feu et système de prévention d'intrusion (IPS).

Toutefois, le plus inquiétant est que les attaques visant la couche applicative utilisent des mécanismes beaucoup plus sophistiqués pour attaquer les services et réseau des organisations. Plutôt que d'inonder simplement un réseau avec du trafic ou des sessions, ces types d'attaques ciblent des services et applications spécifiques pour épuiser lentement les ressources au niveau de l'application (couche 7).
Les attaques visant la couche applicative peuvent être très efficaces en utilisant peu de volumes de trafic, et peuvent être considérer comme tout à fait normales par la plupart des méthodes de détection DOOS traditionnelles. Cela rend les attaques visant la couche applicative peuvent être visant la couche applicative peuvent des méthodes de détection DOOS traditionnelles.

Le options en satière de protection DDOS

La plupart des FAI offrent une protection DDOS des couches 3 et 4 pour empêcher les liens des organisations d'être inondés lors d'attaques volumétriques de masse. Cependant, ils n'ont pas la capacité de détecter les plus petites attaques visant la couche 7. Ainsi, les centres de données ne devraient
pas uniquement compete sur leur FAI pour bénéficier d'une solution complète DDOS, dont la protection de la couche applicative. Au lieu de cela, ils devraient envisager de mettre en place une des mesures suivantes:

1. Les fournisseurs de services DDOS: Il estre beaucoup de solutions hébergées DDOS basées sur les Cloud qui fournisseurs des services de protection des couches 3, d et 7. Elles wont des projets peu couteux pour les petits sites Méb jusqu'à ceux pour les grandes entreprises qui requièrent la converture de plusieurs sites Meb jusqu'à ceux pour les grandes entreprises qui requièrent la converture de plusieurs sites Meb jusqu'à ceux pour les grandes entreprises qui requièrent la converture de plusieurs sites Meb jusqu'à ceux pour les services de détection avancée de la conche 7 à disposition des masses. Per ailleurs, la perforament des conches de devieres, les periodes de la conche 2 de deviere de sonderes, de sorties de deviere de la conche 7 à disposition des masses. Per ailleurs, la perforament de la principal de la particultérement problèmatique pour les strapes de la conche 7 à disposition des masses. Per ailleurs, la perforament problèmatique pour les strapes de la conche 7 à disposition des masses. Per ailleurs, la perforament problèmatique pour les strapes de contre de deviere de la conche 7 à disposition des masses. Per ailleurs, la perforament problèmatique pour les strapes de la conche 7 à disposition des masses. Per ailleurs, la perforament problèmatique pour les strapes de la conche 7 à disposition des masses. Per ailleurs, la perforament produ

asses. Par alleurs, la performance n'est parfois pas à la hauteur car les fournissurus de services redirigent le trafic Dods were les centres de protection au Lius de les stopper en temps redi, ce qui est particulièrement problèmatique pour les attaques de courte durée, qui a ont celles généralement contrais.

In parformance de protection (DNG) entre plus facile à géner, mais il pout être submerge par des attaques volumétriques BOds, et entre pas wort its enécasises sophistiques de détection pour la couche 7 que d'autres solutions ont. Il autre comprais à prendre en complete att que l'activation de la voncetion BOds autre par des attaques volumétriques BOds, et entre pas wort its enécasises sophistiques de détection pour la couche 7 que d'autres solutions ont. Il autre comprais à prendre en complete att que l'activation de la voncetion BOds autre par de par des attaques volumétriques en masse et surveiller te performance plobaled de seul dispositif, entrainant des debits rédistir se des la latence pour le utilisateurs finance.

1. Appliances dédiées à la protection d'attaques BOds: Ce sont des dispositifs matériels qui sont déployés dens un centre de données et utilisés pour détecter et stopper les attaques BOds basiques (couche 2 et 4) et avancées (couche 7). Déployées su point d'entrée principal pour tout le trafic tende es appliances pouvent à la foisi bloquer les attaques volumétriques en masse et surveiller tout le trafic entrait et sortent de contrait es supprise de sout en la couche 3 et 4) et avancées (couche 2 et 4) et avancées (couche

sentrepties devical considered to splinners of transport of transport

ource : http://www.journaldunet.com/solutions/expert/59977/comment-se-proteger-des-attaques-ddos.shtml