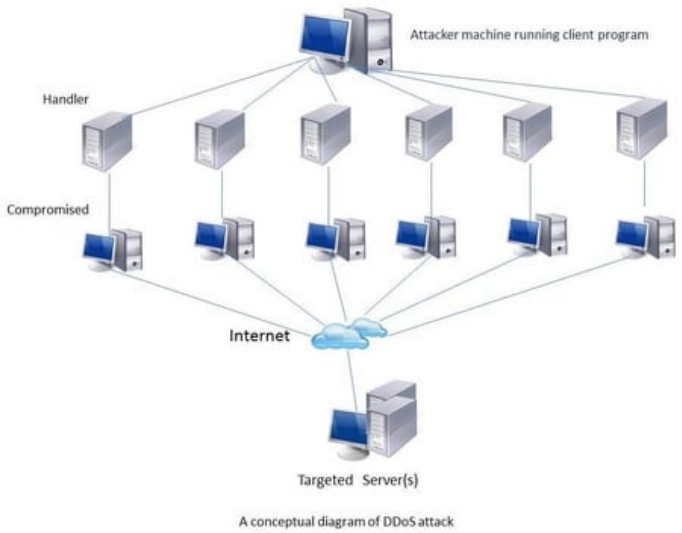
Comment se protéger des attaques DDoS ? | Denis JACOPINI



A conceptual diagram of DDoS attack

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 (DDoS) 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 beaucoup plus sophistiquée. De nouveaux types d'attaques ciblent désormais les applications et services, et sont souvent cachés dans les couches 3 et 4, ce qui les rend difficilement détectables.
En matière d'attaques DDoS, le secteur financier est l'une des cibles privilégiées des cybercriminels, suivie de près par le secteur public. Outre le fait de perturber les opérations Internet par un assaut brutal de données, les attaques DDoS ont récemment été utilisées pour recueillir des informations financières et relatives au commerce 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 derrière les attaques DDoS: politique, de représailles et financière. Les attaquants politiques ciblent ceux qui ne sont pas d'accords avec leurs convictions politiques, sociales ou religieuses. Lorsqu'un botnet ou un important réseau cybercriminel est démantelé, cela peut déclencher des attaques de représailles contre ceux qui ont aidé ou assisté les autorités. Les attaques motivées par l'argent suivent un schéma « pay-to-play » dans lequel les hackers sont compensés par une tierce partie qui leur demande de mener l'attaque pour elle. Quelle que soit la motivation, le résultat est le même – votre réseau et services en ligne deviennent indisponibles, et peuvent rester ainsi pendant un long moment.

Méfiez-vous des attaques DDoS avancées visant la couche applicative
Il existe de nombreux types d'attaque DDoS largement utilisés aujourd'hui, allant des anciennes méthodes des débuts de l'Internet aux dernières attaques avancées visant la couche 7 et ciblant les applications. L'inondation de requêtes SYN et HTTP GET sont les plus communes et utilisée pour surcharger les connexions réseau ou les serveurs derrière 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 DDoS traditionnelles. Cela rend les attaques visant la couche applicative beaucoup plus difficiles à détecter que les autres types d'attaque DDoS basiques.

Les options en matière 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 compter 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 existe beaucoup de solutions hébergées DDoS basées sur le cloud qui fournissent des services de protection des couches 3, 4 et 7. Elles vont des projets peu couteux pour les petits sites Web jusqu'à ceux pour les grandes entreprises qui requièrent la couverture de plusieurs sites Web. Elles sont en général très faciles à mettre en place et fortement poussées auprès des petites et moyennes entreprises. La plupart offre des options de tarification personnalisée et beaucoup ont des services de détection avancée de la couche 7 à disposition des grandes organisations qui nécessitent que des capteurs soient installés dans le centre de données. Beaucoup d'entreprises choisissent cette option, mais certaines d'entre elles doivent faire face à des frais excédentaires importants et imprévus lorsqu'elles sont frappées par des attaques DDoS en masse. Par ailleurs, la performance n'est parfois pas à la hauteur car les fournisseurs de services redirigent le trafic DDoS vers les centres de protection au lieu de les stopper en temps réel, ce qui est particulièrement problématique pour les attaques de courte durée, qui sont celles généralement rencontrées.
2. Pare-feu ou IPS: Presque tous les pare-feux et systèmes de prévention d'intrusion (IPS) modernes revendiquent un certain niveau de défense DDoS. Les pare-feu nouvelles générations avancés (NGFW) offrent des services DDoS et IPS et peuvent protéger de nombreuses attaques DDoS. Avoir un dispositif pour le pare-feu, IPS et DDoS est plus facile à gérer, mais il peut être submergé par des attaques volumétriques DDoS, et peut ne pas avoir les mécanismes sophistiqués de détection pour la couche 7 que d'autres solutions ont. Un autre compromis à prendre en compte est que l'activation de la protection DDoS sur le pare-feu ou l'IPS peut impacter la performance globale du seul dispositif, entrainant des débits réduits et une augmentation de la latence pour les utilisateurs finaux.
3. Appliances dédiées à la protection d'attaques DDoS: Ce sont des dispositifs matériels qui sont déployés dans un centre de données et utilisés pour détecter et stopper les attaques DDoS basiques (couche 3 et 4) et avancées (couche 7). Déployées au point d'entrée principal pour tout le trafic Web, ces appliances peuvent à la fois bloquer les attaques volumétriques en masse et surveiller tout le trafic entrant et sortant du réseau afin de détecter les comportements suspects des menaces visant la couche 7. En utilisant un dispositif dédié, les dépenses sont prévisibles car le coût est fixé quelle que soit la fréquence des attaques, que l'entreprise soit attaquée une fois en six mois ou tous les jours. Les aspects négatifs de cette option sont que ces dispositifs sont des pièces matérielles supplémentaires à gérer, que les unités à faible bande passante peuvent être submergées lors d'attaques volumétriques en masse, et que de nombreux fabricants nécessitent des mises à jour fréquentes en matière de signatures.
Les solutions matérielles dédiées de protection des attaques DDoS existent en deux versions principales – celle pour les opérateurs télécoms et celles pour les entreprises. Les premières sont des solutions complètes conçues pour les réseaux mondiaux des FAI et sont très coûteuses. La plupart des organisations qui veulent protéger leurs centres de données privés optent habituellement pour les modèles entreprises qui offrent une détection et protection DDoS rentable. Les modèles d'aujourd'hui peuvent gérer des attaques volumétriques en masse et assurer une protection à 100% des couches 3, 4 et 7 ou peuvent être utilisés pour compléter une protection fournie par le FAI contre les attaques DDoS en masse et assurer une détection et protection avancées de la couche 7. Bien que ces dispositifs nécessitent un investissement initial, ce qui n'est pas le cas des solutions hébergées, ils sont généralement beaucoup moins chers à long terme si l'on prend en compte les frais excédentaires dans le budget total.

Les entreprises devraient considérer des appliances de protection d'attaques DDoS qui utilisent des méthodes d'adaptation basées sur le comportement pour identifier les menaces. Ces appliances apprennent les bases de référence de l'activité normale des applications et ensuite surveillent leurs trafics par rapport à ces bases. Cette approche d'adaptation/apprentissage a l'avantage de protéger les utilisateurs des attaques zero-days inconnues puisque que le dispositif n'a pas besoin d'attendre que les fichiers signatures soient mis à jour.
Les attaques DDoS sont en hausse pour presque toutes les organisations, grandes ou petites. Les menaces potentielles et volumes augmentent à mesure que de plus en plus d'appareils, y compris les téléphones mobiles, accèdent à Internet. Si votre organisation a une propriété Web, la probabilité de subir une attaque n'a jamais été aussi élevée.
La nature évolutive des attaques DDoS signifie que les entreprises ne peuvent plus compter uniquement sur leur FAI pour se protéger. Les organisations doivent commencer à effectuer des changements dès à présent pour une plus grande prévoyance et bénéficier de défenses plus proactives pour les services au niveau des applications et du réseau.

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

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