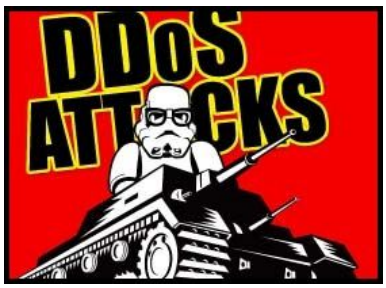
DDoS : les hébergeurs doivent prendre d’urgence des mesures pour défendre leurs clients

	DDoS : les hébergeurs doivent prendre d’urgence des mesures pour défendre leurs clients

Faisant chaque jour la une des journaux, les attaques par DDoS se multiplient. De ce fait, de nombreuses entreprises s'interrogent : leur stratégie de mitigation des DDoS les protège-t-elle suffisamment ? Aujourd'hui, elles se tournent vers leurs fournisseurs de cloud et leurs hébergeurs pour avoir la bonne réponse.

Malheureusement, l'hébergement procure aux hackers une surface d'attaque incroyablement attrayante. En effet, la taille et l'ampleur des infrastructures réseaux des data centers des opérateurs et l'importante base de clients que cela représente, présentent de multiples points d'entrée et se traduisent une énorme bande passante globale qui offre un véritable boulevard aux attaques DDoS perturbatrices et destructrices. En s'appuyant de plus en plus sur l'hébergement pour leurs services et leurs infrastructures critiques, les entreprises s'exposent elles-mêmes au risque de subir des cyber-menaces dévastatrices – même en tant que cibles indirectes.
L'aspect multi-tenant des centres de données du cloud peut expliquer la confiance relative des locataires. Une attaque DDoS volumétrique contre un des 'tenants' peut engendrer des répercussions désastreuses envers les autres : un effet « domino » de latence, de dégradation du service et d'interruption des activités de longue durée, avec de lourds dommages potentiels. Un trafic malveillant excessif qui bombarde un seul locataire au cours d'une attaque DDoS volumétrique, peut avoir des effets négatifs sur d'autres locataires et sur l'ensemble des opérations du centre de données. Il est en fait, de plus en plus fréquent qu'une attaque visant à l'origine un seul locataire ou un seul service, étouffe complètement les ressources partagées, en infrastructure et en bande passante. Ceci provoque de sévères ralentissements allant parfois jusqu'à la mise hors service du centre de données tout entier. En quelque sorte les effets secondaires du DDoS.

La technique du trou noir est un moyen de défense brut, utilisé couramment lors des attaques pour atténuer les effets secondaires des DDoS. Par cette technique, les fournisseurs de cloud et d'hébergement bloquent tous les paquets destinés à un domaine, le trafic étant re-routé vers un itinéraire nulL pour l'adresse (ou les adresses) IP sous attaque. Ce mode de défense contre les attaques DDoS pose un certain nombre de problèmes. En particulier, quand plusieurs locataires partagent une gamme d'adresses IP publiques. Dans ce cas, ils verront leur accès supprimé à l'ensemble des services, qu'ils soient ou non la cible spécifique de l'attaque. En pratiquant cette technique, l'opérateur du data center achève en fait lui-même le travail de l'attaquant en dosant complètement ses propres clients ! De plus, l'injection de routes nulL est un processus manuel qui nécessite des analystes humains, des processus workflow et des autorisations. On augmente alors les temps de réponse à l'attaque et on laisse tous les locataires du data center partagé en subir les conséquences sur des périodes pouvant atteindre plusieurs heures.
La dépendance croissante à Internet rend les effets – financiers ou autres – des attaques DDoS réussies de plus en plus douloureux pour les fournisseurs de services, les entreprises et les administrations. Et l'arrivée de nouveaux outils DDoS toujours plus puissants promettent le déclenchement d'attaques encore plus destructrices dans les mois et les années à venir.

Il est temps que les entreprises qui s'appuient sur des infrastructures ou des services hébergés commencent à se poser les bonnes questions, comme se demander si leurs fournisseurs d'hébergement ou de centres de données les protègent correctement quand une attaque DDoS frappe. Comme cela s'est vu à maintes reprises, les clients hébergés comptent en fait tout simplement sur leur fournisseur pour « s'occuper » des attaques quand elles surviennent, sans appréhender pleinement le danger et les conséquences de fermer les yeux face à ce type de comportement malveillant.

Voici trois étapes-clés pour que les fournisseurs protègent mieux leur propre infrastructure et celle de leurs clients.

1. Éliminer les délais entre le moment où les dispositifs de surveillance traditionnels détectent une menace et génèrent une alerte et le moment où un opérateur est en mesure d'y répondre. Initialement de quelques heures, l'effet de l'attaque sera réduit à quelques secondes. Ceci est possible par le déploiement d'appliances qui surveillent et atténuent automatiquement les menaces DDoS. La solution de mitigation doit pouvoir mettre à disposition des rapports d'alertes et d'événements en temps réel, avec une infrastructure de maintenance opérationnelle en arrière-plan pour des temps de réaction rapides, et fournir toute la visibilité indispensable pour comprendre l'état de la menace et améliorer pro-activement la défense anti-DDoS.

2. Déployer la mitigation DDoS inline. Si des périphériques out of band sont en place pour nettoyer le trafic, il convient de déployer rapidement des équipements de détection des menaces inline qui pourront inspecter, analyser et contrer les DDoS en temps réel.

3. Investir dans une solution de mitigation DDoS architecturée pour ne jamais abandonner le bon trafic. Les prestataires de services hébergés doivent impérativement empêcher que l'équipement de sécurité ne devienne un goulot d'étranglement pour les services rendus et toujours permettre au trafic légitime de passer, sans aucune interruption ; voilà une approche de défense anti-DDoS réussie et sans dommage collatéral.

Les entreprises font confiance à leurs fournisseurs pour assurer la disponibilité de leurs services et, finalement, leur protection contre les cyber-menaces et les attaques par DDoS. Le déploiement d'une première ligne de défense complète contre les attaques DDoS permet de protéger pleinement les clients contre les menaces volumétriques dommageables, qu'elles soient dirigées vers les réseaux, qu'elles en proviennent ou qu'elles y transitent.

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

Source : http://www.programmez.com/avis-experts/ddos-les-hebergeurs-doivent-prendre-durgence-des-mesures-pour-defendre-leurs-clients-21827
par Adrian Bisaz