Les attaques DDoS atteignent des sommets en 2015

Un peu comme le rapport de la Cour des comptes, le rapport sur la sécurité d'Arbor Networks est souvent le moment de faire un état des lieux des attaques par déni de service. Eric Michonnet responsable des activités Europe du Sud, Centrale et Afrique du Nord chez Arbor Networks, constate d'emblée « *qu'il y a une amplification des attaques avec des intensités de 300 à 500 Gbps et même une pointe à 500 Gbps pour l'année 2015* ». Une accélération continue depuis quelques années notamment en raison de techniques plus affûtées comme celle de l'amplification par rebond DNS. Résultat : en 11 années de rapport, l'intensité des attaques a été multipliée par 60.

Et cela n'est pas prêt de s'arrêter confie Eric Michonnet. *« En 2016, il devrait y avoir des attaques encore plus forte sans qu'il soit possible de déterminer si on sera sur des niveaux de 600 à 700 Gbps. »* Ce type de méga-offensive devrait être néanmoins limité à « *une, deux ou trois* », considère le responsable. Pour lui, ce genre d'attaques massives bénéficient à la fois des travaux réalisés par des cybercriminels sur les techniques d'amplifications, mais aussi des bandes passantes importantes pour le trafic sortant.

Des petites attaques plus complexes et plus gênantes

Pour les motivations des attaques DDoS, Eric Michonnet souligne qu'en France, « *il existe deux motivations : l'extorsion d'argent comme le groupe DD4BC (DDoS pour des bitcoins) et les considérations géopolitiques comme le montre les attaques des Anonymous hier sur le site de l'Assemblée Nationale ou du Sénat* ». Des cibles faciles, mais qui ne doivent pas masquer une autre réalité propre à la complexité des petites attaques par saturation, souligne le dirigeant. « *Elles sont plus nombreuses et leur taille modeste fait qu'elles génèrent beaucoup de bruit dans le réseau. Elles sont même parfois plus longues pouvant durer jusqu'à 2 ou 3 jours.* » Ce genre de menaces cible principalement les fournisseurs de services et les administrations. Dans le cadre des ISP, les cybercriminels visent les hébergeurs. « *La cloudification des applications apporte une simplification pour les attaques en déni de service* », constate Eric Michonnet. En effet, en visant le datacenter de l'hébergeur, il est plus facile de faire tomber plusieurs services en saturant la bande passante.

Sur la protection, le responsable avoue sa satisfaction. « *Il y a une prise de conscience et une évolution dans les entreprises sur cette problématique.* » Et de pointer du doigt que « *la France est dans cette démarche avec plusieurs appels d'offres et la mise en place de POC* ». Il s'agit néanmoins d'une première étape. Pour lui, « *la préparation aux attaques nécessitent d'avoir une équipe et celle-ci doit être formée* ». Or la formation est un gros problème et les entreprises se tournent vers des solutions alternatives comme l'outsourcing.

A lire aussi :

12% des attaques DDoS menées par des concurrents

Plus de 1500 attaques DDoS au 3e trimestre 2015

crédit photo © Duc Dao – shutterstock