Start-up : Efficient IP ou la réponse aux attaques DDoS 'made in France'

Et si la réponse la plus efficace à ce jour aux attaques par déni de service (DDoS) venait… de Courbevoie, commune des Hauts-de-Seine limitrophe de Paris ? Créée en 1997 par **deux anciens de l'Epita**, la société Efficient IP revendique en effet une appliance capable d'absorber **jusqu'à 17 millions de requêtes DNS par seconde**. Une solution basée sur l'utilisation d'un cache permettant de décharger le serveur DNS proprement dit. Pas une innovation à proprement parler, d'autres sociétés comme Infoblox ou Blue Coat vendant des appliances similaires. « *Mais ces serveurs ne permettent que de monter à environ 1 million de requêtes par seconde* », assure Hervé Dhélin, le directeur marketing de la société, un ancien de Mercury, BMC ou encore SPSS. Selon ce dernier, le gain en performances provient d'optimisations logicielles dans la gestion du cache, améliorations imaginées par les équipes R&D d'Efficient IP (une trentaine de personnes).

Les composants embarqués dans l'appliance maison, baptisée SOLIDserver DNS Blast, sont eux tout à fait standards. Vendue **à partir de 150 000 euros** (pour une unique appliance, des architectures en cluster étant également envisageables pour faire face à davantage de trafic), le serveur spécialisé peut **traiter plus de 99 % du trafic** une fois implanté depuis quelques temps dans l'infrastructure (le temps que le maximum d'informations soit placé en cache). Il cible avant tout les grands fournisseurs de service et opérateurs télécoms. Rappelons que récemment des fournisseurs majeurs de services Cloud comme Evernote, application de prise de notes, Feedly, agrégateur de flux RSS, ou le service musical français Deezer ont connu des interruptions de service en raison d'attaques DDoS.

Un PC infecté = 200 000 requêtes/s

« *Mais, au-delà des opérateurs et autres fournisseurs de services Internet, ce sont désormais toutes les entreprises sont concernées* », assure Hervé Dhélin, pointant les conclusions d'un récent rapport d'Akamai. **27 % des entreprises françaises** interrogées par IDC, pour le compte d'Efficient IP, reconnaissent d'ailleurs avoir une subi une attaque par DDoS sur leur DNS au cours des 12 derniers mois. « *Contrairement à ce que l'on pense, la majorité des attaques vient aujourd'hui de l'intérieur. Un simple PC de bureau infecté est capable de générer jusqu'à 200 000 requêtes par seconde en tâche de fond*, explique le directeur marketing. *Il suffit d'une poignée de PC infectés par exemple via une campagne de phishing pour faire tomber les DNS, donc tout le réseau interne. Car les échanges entre les applications, les bases de données, les serveurs d'applications jusqu'aux connexions à des éléments comme les réfrigérateurs de supermarché ou les caméras de surveillance exploitent tous l'IP.* »

Certes, la technique du cache n'est pas la seule possible pour tenter de contrer les attaques par déni de service. Quand elles ne se réfugient pas derrière l'illusoire protection d'un firewall, les entreprises placent ainsi souvent des **serveurs DNS en cluster** pour tenter d'encaisser les pics de charge (avec du load balancing). Une technique qui reste à la fois assez lourde à mettre en œuvre et relativement limitée. Un serveur DNS n'encaissant que 300 000 requêtes par seconde. « *Or, les dernières vagues d'attaques sont marquées par une augmentation des volumes. On a frôlé récemment les*

400 Gbit/s. Il faudrait des datacenters entiers de serveurs DNS pour y faire face », assure Hervé Dhélin.

Sécurité du DNS : pas de réponse globale

Autre technique souvent exploitée : **le filtrage du trafic entrant**. Une voie efficace. Mais qui peut générer des effets de bord, selon le directeur marketing. « *Les assaillants utilisent de fausses adresses IP afin de mener leurs attaques DDoS. L'objectif n'est alors plus de bloquer la société ciblée par la montagne de requêtes mais d'obtenir que l'entreprise d'où semblent émaner les requêtes soit blacklistée* ».

Efficient IP, qui emploie environ 80 personnes et a réalisé un chiffre d'affaires de 4,3 millions d'euros en 2012 (en progression de 33%) pour une perte de 220 000 euros, n'en est **pas à son coup d'essai quant à la sécurisation du DNS**. « *C'est la 6ème tactique que nous déployons pour répondre au problème, car il n'existe pas une réponse globale à l'ensemble des problématiques qui se posent* », assure Hervé Dhélin. Après un système de masquage du master, un firewall spécifique, la société a récemment sorti une solution (Hybrid DNS) embarquant les trois principaux serveurs DNS du marché (Bind, NSD et Unbound) et permettant d'activer l'un ou l'autre alternativement, en fonction des failles détectées dans telle ou telle solution.

Crédit photo : © Duc Dao – shutterstock

En complément :

Avis d'expert : l'importance d'une défense contre les attaques DDoS dans les plans de continuité d'activité