Identifier un attaquant qui a triché sur son adresse IP source

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 2 novembre 2011

https://www.bortzmeyer.org/identifier-spoofer.html

À la réunion OARC <https://www.dns-oarc.net/> de Vienne, le 29 octobre 2011, Duane Wessels a présenté un très intéressant (et très technique) exposé « "*Tracing a DNS reflection attack*" » (voir ses transparents <https://www.dns-oarc.net/files/workshop-201110/tracing-dns-reflection.pdf>). L'exposé présente l'analyse d'une attaque déni de service utilisant les serveurs DNS de la racine. Son originalité est la découverte d'une méthode pour identifier l'origine de l'attaquant, alors même que ce dernier met des adresses IP mensongères dans ses paquets.

Cette méthode utilise le fait que la plupart des serveurs de la racine du DNS sont "*anycastés*". Revenons d'abord sur l'attaque : il s'agissait d'une attaque par réflexion. Le méchant envoie une requête DNS à un serveur. Celui-ci répond à l'adresse IP (mensongère) que le méchant a mis dans la question... et frappe ainsi la victime (p. 3 des transparents).

Comment savoir qui est l'attaquant ? Dans les romans policiers, lorsque le méchant envoie une lettre, il laisse plein de traces dessus : empreintes digitales, ADN, type de papier utilisé, caractéristiques de l'imprimante... Rien de tel dans un paquet réseau. Les bits ne conservent pas l'ADN... Il faut donc suivre en sens inverse le flux de paquets, demandant à chaque opérateur d'analyser d'où vient l'attaque. C'est lent et cela dépend de la bonne volonté de **tous** les opérateurs sur le trajet.

Duane Wessels, en analysant l'attaque, a fait une observation. Les requêtes du pirate passent parfois subitement d'une instance d'un serveur racine à une autre. Par exemple, p. 17, on voit les requêtes vers le serveur K passer de l'instance du NAP à celle du LINX vers 0233, puis repasser au NAP vers 0240 (et re-changer encore par la suite). C'est le comportement normal de l'"*anycast*" : BGP a changé les routes (contrairement à ce qu'indique le transparent p. 19, ce n'est pas forcément suite à une panne) et l'attaque a suivi. L'idée de Duane a donc été : quel est le trafic qui a changé **exactement au même moment** ? Car ce trafic vient forcément du même point que l'attaque et a été routé pareil. Naturellement, au début, on trouve plein de suspects mais, sur des serveurs fortement "*anycastés*" comme ceux de la racine, la liste se réduit vite et on arrive à un seul AS (p. 22). Le trafic d'attaque vient donc de là (un hébergeur situé sur la côte Est des États-Unis).

À noter que les "*glitches*" BGP qui ont permis de repérer l'origine étaient accidentels. On pourrait imaginer d'appliquer cette technique volontairement, en modifiant les annonces BGP pour voir où le trafic se déplace, détectant ainsi l'attaquant qui se croyait bien caché.