La journée du 31 mars sur les serveurs racine du DNS

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 31 mars 2012

https://www.bortzmeyer.org/racine-dns-opblackout.html

Le 12 février dernier, des individus anonymes annonçaient une attaque <http://pastebin.com/XZ3EGsbc> sur la racine du DNS pour le 31 mars. Que s'est-il effectivement passé ?

Les serveurs de la racine qui ont des statistiques publiques (ce n'est pas le cas de tous) montrent tous un petit accroissement de trafic en début de journée. Cet accroissement est de faible ampleur, il n'est pas prouvé que ce soit une attaque (l'Internet connait un trafic permanent de choses curieuses et tout ce qui est bizarre n'est pas forcément malveillant), et, surtout, il n'a pas eu de conséquence sur la capacité de la racine à assurer son service.

Ainsi, on voit que les serveurs K et L ont vu cet accroissement entre 0200 et 0400 UTC. Sur K, cela donne : . L'augmentation semble géographiquement limitée (seul le nœud de Tokyo l'a vue). Sur L, cela donne : . Ici, le petit pic d'augmentation est localisé en Amérique du Nord.

Pour H, c'est entre 0500 et 0700 : .

Mais le point important est qu'une augmentation de trafic ne signifie pas un problème pour les utilisateurs : les serveurs racine sont largement suffisants pour faire face à un trafic bien plus important que leur moyenne. Pour connaître les conséquences pratiques d'une attaque ou d'une panne, il faut regarder si les serveurs répondaient bien pendant le problème. dnsmon <http://dnsmon.ripe.net> nous montre que oui : la racine reste presque entièrement en vert. On voit seulement le maillon faible habituel, le serveur B, qui a subi des pertes importantes entre 0600 and 0900 :

Il n'y a guère eu de changement dans le reste de la journée. Bref, rien de bien important à signaler.

Merci à Alain Thivillon pour sa vigilance et ses bonnes remarques.

Rappelez-vous bien qu'on ne sait pas qui est derrière l'annonce de l'attaque <http://owni.fr/2012/02/25/operation-com-anonymous/index.html>. Quelques analyses techniques de l'attaque, telle que décrite dans l'annonce originale : par Robert David Graham <http://erratasec.blogspot.com/2012/02/no-anonymous-cant-ddos-root-dns-servers.html>, par Cricket Liu <http://www.cricketondns.com/post.cfm/could-a-ddos-attack-against-the-roots-succeed>, et par Pierre Col <http://www.zdnet.fr/blogs/infra-net/vers-un-blackout-de-l-internet-le-31-mar
htm>. Un autre bon article explique les précautions qu'il faudrait prendre pour rendre ces attaques encore plus difficiles (par Duane Wessels <https://www.dns-oarc.net/wiki/mitigating-dns-denial-of-servi
Si on préfère rire, l'article d'Alan Woodward <http://www.bbc.com/news/technology-17472447>
est sans doute celui qui contient le plus d'erreurs techniques.