Allez, encore une attaque par déni de service contre la racine du DNS ?

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 9 avril 2011

https://www.bortzmeyer.org/racine-6avril.html

Un mystérieux problème a gêné un bon nombre de serveurs racine du DNS le mercredi 6 avril entre 08 :00 et 14 :00 UTC. Il s'est traduit par une absence de réponse de la part de plusieurs serveurs, déclenchant des alertes à certains endroits. Un exemple de ces problèmes est donné par le service de débogage DNSSEC DNSviz <http://dnsviz.net/> qui affichait des erreurs qui n'étaient dues, ni à un problème de la zone testée, ni à une bogue dans DNSviz lui-même. Voici par exemple une « erreur » vue par DNSviz qui était en fait due à ce problème à la racine (192.228.79.201 est B-root, un des serveurs de la racine) :

Le fait que le problème ne soit pas spécifique à DNSviz se voyait avec d'autres outils. Par exemple, l'excellent DNSmon <http://dnsmon.ripe.net/> montrait de grandes plages jaunes <http://dnsmon.ripe.net/dns-servmon/domain/plot?domain=root&af=ipv4&day=6&month=4&year=2011&hour=6&period=12h&plot=SHOW> pour certains des serveurs de la racine, notamment B, D et E, ce jaune indiquant que le taux de réponses était nettement en dessous des 100 %. Au cas où le lien donné plus haut ne fonctionne plus (si DNSmon a fait de la place dans son historique), voici l'image originelle : . Les trois bandes jaunes indiquent les trois serveurs le plus touchés. Si on se focalise sur l'un d'eux, mettons D-root, cela donne : . Chaque trait horizontal est pour une sonde particulière de DNSmon. On voit que le problème n'était pas constant : chaque sonde voyait parfois zéro réponse de la part du serveur D, parfois une partie des réponses. Un autre serveur, I, a mieux résisté : . On voit que deux sondes ont noté le même problème que pour D mais toutes les autres ne voyaient rien. (Les grands traits rouges étaient probablement des sondes en panne : on note qu'elles ne marchaient pas du tout pendant la période considérée et même au delà.)

Si on regarde d'autres services de statistiques que DNSmon, on voit la même chose. Le serveur H a un service de statistiques public <http://h.root-servers.org/>, qui ne maintient pas l'historique mais on voit bien sur cette copie la montée du trafic le 6 : . Montée du trafic ne signifie pas panne : contrairement à B, D et E, H a ainsi toujours continué à marcher. Autre serveur qui a vu une augmentation du trafic, L, qui a également des statistiques publiques <http://dns.icann.org/cgi-bin/dsc-grapher.pl?window=604800&plot=bynode&server=L-root>. Le graphe pris à

ce moment montrait bien une légère, mais détectable, augmentation du trafic : , sans conséquences pratiques. (Il existe aussi d'autres services de statistiques non publics par exemple à l'OARC <https://www.dns-oarc.net/> mais je ne peux pas en parler, désolé, ce ne sont pas mes données.)

Que s'est-il passé ? La simultanéité de la hausse du trafic sur plusieurs serveurs, le fait que le service ne se soit pas totalement interrompu mais que le taux de pertes ait simplement augmenté considérablement, semble indiquer une attaque par déni de service concertée. Si c'est bien le cas, cette attaque a été nettement moins réussie que celle de 2007 <https://www.bortzmeyer.org/attaque-serveurs-racine.html>. Seuls trois des treize serveurs <https://www.bortzmeyer.org/combien-serveurs-racines.html> ont été très perturbés. On notera que ces trois là sont parmi les derniers à être encore "*unicast*", la plupart des serveurs de la racine étant désormais "*anycast*" comme I, cité plus haut, qui n'a vu de problème que sur une petite partie de ses instances. Cela laisse entendre que l'attaque n'était pas très distribuée et ne partait que d'un petit nombre d'endroits. L'examen des données de DNSmon ne permet pas de déterminer cet endroit avec précision (on trouve parmi les points possibles les États-Unis, l'Allemagne, le Japon...).

Voilà, je ne peux pas en dire plus, les autres données ne sont connues que des opérateurs de serveurs racine. Peut-être y aura-t-il une publication ou peut-être pas : ce genre d'attaques n'est pas un évenement exceptionnel et il n'a guère eu de conséquences visibles.

Merci à Philippe Renaut pour sa vigilance qui a permis de détecter le problème.