Attaque contre les serveurs DNS de la racine - juin 2011

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 29 juin 2011. Dernière mise à jour le 8 juillet 2011

https://www.bortzmeyer.org/racine-dns-28-juin-2011.html

Les attaques dDoS contre les serveurs DNS de la racine ne sont pas quotidiennes mais ne sont pas non plus des évenements exceptionnels. Le mardi 28 juin, une nouvelle attaque a eu lieu, pendant presque deux jours.

La précédente attaque d'ampleur datait du 6 avril <https://www.bortzmeyer.org/racine-6avril.html>. L'attaque du 28 juin et celle du 6 avril étaient loin d'atteindre l'ampleur de celle de 2007 <https://www.bortzmeyer.org/attaque-serveurs-racine.html>. Le "*botnet*" utilisé cette fois semble de petite taille et très concentré géographiquement : pour les serveurs "*anycastés*", seul un tout petit nombre d'instances est touché.

Commençons par les informations disponibles. L'excellent service public DNSmon <http://dnsmon.ripe.net/> nous montre que certains serveurs comme B (l'habituel maillon faible) ont été très touchés : D'autres ont été attaqués mais n'ont pas cédé comme K : .

Un serveur comme K, dont toutes les instances reçoivent en temps normal entre 10 000 et 20 000 requêtes par seconde a vu son trafic passer à 60 000 requêtes par seconde. S'agit-il bien d'une attaque ? Certainement, oui, par son côté coordonné (tous les serveurs ont vu le début au même moment) et par des caractéristiques inhabituelles, notamment le fait que la requête DNS avait le bit RD ("*Recursion Desired*") à 1, ce qui n'est normalement jamais le cas dans les requêtes d'un vrai résolveur à un serveur faisant autorité : .

J'ai dit que le "*botnet*" était probablement très concentré géographiquement. En effet, les serveurs "*anycastés*" n'ont vu l'attaque que sur certaines instances, en général européennes. Par exemple, L : Quelle était la taille du "*botnet*" ? Difficile à dire, évidemment, mais sans doute pas très gros. Un flot continu de 50 000 requêtes par seconde peut être envoyé, sans aucun effort de programmation, par trois ou quatre PC ordinaires. Même multiplié par les treize serveurs racine, ce n'est pas impressionnant.

L'attaque n'avait donc aucune chance de réussir, avec si peu de moyens déployés. Alors, quel était le but de l'attaquant ? Était-il incompétent ou voulait-il simplement faire une démonstration commerciale à l'usage de ses futurs "*prospects*" ? Car rappelons-nous que les propriétaires de "*botnet*" gagnent leur vie en les louant. Imaginons un dialogue en IRC sur un serveur discret...

```
(11:27:50) Prospect: J'ai besoin d'un botnet pour dDoSer quelqu'un
(11:28:37) Herder: J'en ai un superpuissant, pas cher
(11:29:21) Prospect: Vraiment puissant ?
(11:31:33) Herder: Ouais, man, trop fort
(11:31:34) Prospect: OK, démontre-le, attaque la racine du DNS à 1700 UTC, je verrai sur dnsmon si ça a marc
(11:31:43) Herder: C'est parti
```

D'autres hypothèses sont évidemment possibles : gouvernements voulant faire passer une loi répressive en montrant que nous sommes en danger, agences voulant obtenir un meilleur budget cyber-sécurité, lycéens désœuvrés depuis la fin des cours, etc.

Un rappel utile : la meilleure source d'information, et de pointeurs vers les statistiques des serveurs de la racine du DNS est <http://www.root-servers.org/>. Au moment où je publie, l'attaque est finie (depuis apparemment le 30 au matin) et ne peut donc plus être observée. Voici son étendue dans le temps, mesurée sur B : .

Un des opérateurs de serveur racine, celui de K, a communiqué sur ce sujet <http://labs.ripe.net/Members/wnagele/increased-query-load-on-root-name-servers> puis produit une excellente analyse technique, très détaillée <http://labs.ripe.net/Members/wnagele/analysis-of-incre de l'attaque (même s'ils ne sont pas sûrs que ce terme soit mérité.).