Attaque contre les serveurs DNS de la racine le 6 février 2007

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 11 février 2007

http://www.bortzmeyer.org/attaque-serveurs-racine.html

Ce mardi 6 février matin, vers 10h00 UTC, une attaque massive a visé plusieurs cibles DNS sur Internet. Comme d'habitude, plusieurs erreurs importantes sont apparues dans les articles publiés à ce sujet. Une nouveauté a été la guerre des communiqués des opérateurs, chacun expliquant que l'Internet avait tenu grâce à lui.

Parmi les principaux serveurs visés :

— les serveurs DNS de la racine,
— les serveurs DNS de l'opérateur UltraDNS (filiale de Neustar et qui héberge `.org`, `.info` et plusieurs ccTLD),
— les serveurs de l'ICANN, comme whois.iana.org (c'était peut-être un effet de bord de l'attaque contre l.root-servers.net, hébergé à l'ICANN).

Au plus fort de l'attaque, l.root-servers.net (ICANN) et g.root-servers.net (Pentagone) étaient pratiquement inutilisables. La moitié des serveurs d'UltraDNS étaient plus ou moins dans le même cas, ainsi que tous les services non-DNS de l'ICANN (de 95 % à 99 % de perte de paquets sur leurs serveurs Web ou whois).

Voici par exemple l'état de `.org` vers 10h50 UTC :

```
% check_soa org
tld1.ultradns.net has serial number 2007036253
There was no response from tld6.ultradns.co.uk
There was no response from tld5.ultradns.info
tld4.ultradns.org has serial number 2007036252
There was no response from tld3.ultradns.org
There was no response from tld2.ultradns.net
```

L'attaque a sérieusement baissé d'ampleur à partir de 12h00 UTC pour disparaître dans les heures qui ont suivi.

Les serveurs des ccTLD comme `.fr` ou `.uk` n'ont pas été visés directement. Seuls leurs éventuels serveurs hébergés par UltraDNS ont été touchés.

Vous pouvez voir les effets de l'attaque sur des moniteurs publics comme <http://www.cymru.com/monitoring/dnssumm/> ou bien <http://dnsmon.ripe.net/>.

Les statistiques publiées <http://www.nanog.org/mtg-0702/presentations/knight.pdf> par l'ISC montrent que l'attaque était menée essentiellement depuis l'Asie (Chine populaire, Hong Kong, Corée, notamment). Les nœuds "*anycast*" locaux d'Australie ou du Brésil n'ont rien vu. Les nœuds globaux et surtout les nœuds locaux asiatiques ont souffert. Le noeud pékinois de f.root-servers.net a vu 50 000 paquets / seconde pendant deux heures. Mais une partie de l'attaque provenait aussi d'autres pays comme la France.

Que tirer comme leçon de cette attaque ? D'abord qu'elle a échoué. Malgré la mobilisation de ce qui était sans doute un immense "*botnet*", seuls deux serveurs ont été mis hors d'usage contre cinq lors de la plus grosse attaque précédente <http://www.isc.org/f-root-denial-of-service-21-oct-2002>, en octobre 2002. La technologie "*anycast*" a sans doute sauvé des serveurs comme F <http://archives.neohapsis.com/archives/bind/2007/0006.html>.

Mais il faut aussi se rappeler que cette victoire n'est pas définitive : la lutte contre les DDoS est très difficile et on ne connait pas de solution magique pour la plupart des cas.

Ensuite, il faut noter que tous les serveurs ne sont pas égaux. Si certains opérateurs de serveurs racine, comme l'ISC ont mis beaucoup d'efforts et de moyens dans la sécurité de leur système, certains ont nettement moins travaillé.

Enfin que la sécurité ne s'accomode guère des discours marketing. Si le RIPE-NCC peut se vanter <http://www.ripe.net/news/global-root-server.html> de la bonne tenue de son serveur K (mais on peut se demander s'il n'y avait rien de plus important à faire cette semaine que de publier un communiqué de victoire), le marketing très virulent <http://www.merit.edu/mail.archives/nanog/2006-11/msg00247.html> d'UltraDNS, à base de coups de téléphone de FUD, n'a pas protégé leurs serveurs...

À noter que l'ICANN a publié un très bon résumé de l'attaque <https://www.icann.org/announcements/announcement-08mar07.htm>. Certes, ils n'ont pu résister à la tentation d'y glisser un peu de pub mais le document reste une bonne synthèse.