

Début du processus de diffusion des signatures de la racine DNS

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 28 Janvier 2010

<http://www.bortzmeyer.org/la-racine-commence-signature.html>

Pendant que les moutons fidèles de Steve Jobs se pressaient pour le voir présenter un nouvel engin ultra-fermé et contrôlé par Apple, un autre événement suscitait de nombreux articles (moins nombreux, quand même), le début de diffusion des signatures par les serveurs racines du DNS. Ce processus avait été annoncé en octobre dernier <<http://www.bortzmeyer.org/signature-racine.html>> et, jusqu'à présent, suit à peu près son cours.

Hier soir (heure française), un serveur racine a commencé à diffuser des informations signées avec DNSSEC. C'est `L.root-servers.net`, géré par l'ICANN qui s'y est collé pour être le premier. Le déploiement progressif (jusqu'en juillet), permet aux administrateurs réseaux de vérifier leur configuration, **même si eux-mêmes ne font pas de DNSSEC**. Ils doivent en effet s'assurer que leur réseau laisse passer les réponses DNS de grande taille <<http://www.bortzmeyer.org/dns-size.html>>.

Les autres serveurs racines suivront petit-à-petit, selon le plan publié sur le site officiel <<http://www.root-dnssec.org>> (le serveur A a suivi le 10 février.) En mai, certains des réseaux qui ont une configuration boguée (bloquant les réponses supérieures à 512 octets ou bien ne gérant pas la fragmentation) n'auront plus d'accès au DNS.

Quelques observations amusantes ou intéressantes. La réponse envoyée par `L.root-servers.net` atteint désormais dans les 600 octets pour une question typique (celle qui mène à une référence vers un TLD, par exemple `dig AAAA www.bortzmeyer.fr`), mais 1900 octets si on demande toutes les informations (`dig ANY .`). À cause de la taille des enregistrements NSEC, les demandes pour les TLD inexistantes sont un peu plus grosses que les références (dans les 650 octets). Et la requête initiale des résolveurs ("*priming*"), `dig NS .`, atteint maintenant 800 octets.

Comme annoncé, la clé publiée n'est pas celle de signature et on ne peut donc pas encore valider la racine :

```
% dig +dnssec +multi @L.root-servers.net DNSKEY .

; <<>> DiG 9.5.1-P3 <<>> +dnssec +multi @L.root-servers.net DNSKEY .
; (2 servers found)
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47275
;; flags: qr aa rd; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
; . IN DNSKEY

;; ANSWER SECTION:
. 86400 IN DNSKEY 256 3 8 (
AwEAAalLh+++++THIS/IS/AN/INVALID/
KEY/AND/SHOULD/NOT/BE/USED/CONTACT/ROOTSIGN/
AT/ICANN/DOT/ORG/FOR/MORE/INFORMATION+++++
+++++8
) ; key id = 23763
. 86400 IN DNSKEY 257 3 8 (
AwEAAawBe+++++THIS/IS/AN/INVALID/
KEY/AND/SHOULD/NOT/BE/USED/CONTACT/ROOTSIGN/
AT/ICANN/DOT/ORG/FOR/MORE/INFORMATION+++++
+++++
+++++
+++++8=
) ; key id = 19324
. 86400 IN RRSIG DNSKEY 8 0 86400 20100204235959 (
20100121000000 19324 .
NO9bHgWYB3wQlVZXQKwDGUjTgIyFz1i8aWH8nBlT5isn
Ybr6PTfR4fWlSx8+avFfR0fVekauaQelKOyiUav4H9Y1
AZ20Bguu7RjjozQu1qErKboWd1Ng1IIOGar00l4Ur9+4b
o2LSxjp/X4ESypW0lX04z5uB6DZzeilzafzRGUnLIMdV
9xdKEOJrm9UCKvYK5g8bjRq8KA8vT+pidexZMrBQ3ie8
R9daf/s6VK7zUJK0jF1vqhPbZFSQmBpJULxh4VnOv7nn
hcq4MoJ49wqmNxKRqfvSwHAJBG6dEgShnlu/rfVsdxfF
UCjIGX8YnSC7lYqODwguGh+i/arAAK+bzg== )

;; Query time: 135 msec
;; SERVER: 2001:500:3::42#53 (2001:500:3::42)
;; WHEN: Thu Jan 28 09:31:22 2010
;; MSG SIZE rcvd: 736
```

Plusieurs organisations ou personnes ont déjà publiées d'intéressantes statistiques. Par exemple, l'OARC <<http://www.dns-oarc.net>> a publié « *"L-Root now serving "DURZ" signed responses"* <<https://www.dns-oarc.net/node/240>> » avec des jolis graphiques qui montrent notamment :

- L'augmentation de taille des réponses au *"priming"*, de 630 (en moyenne) à 760 (en moyenne, c'est moins que ce que je mesure car certains résolveurs demandent sans EDNS, cf. RFC 2671¹),
- Un bond considérable des requêtes en TCP, venant des résolveurs qui, bêtement, n'utilisent pas EDNS et récupèrent donc des réponses tronquées. Mais le pourcentage reste négligeable <http://stats.l.root-servers.org/cgi-bin/dsc-grapher.pl?window=604800&plot=transport_vs_qtype&server=L-root>).

L'ICANN rend aussi publiques les statistiques de son serveur racine et on peut voir en <<http://stats.l.root-servers.org/>> (attention, il y a trois sites physiques <<http://www.bortzmeyer.org/combien-serveurs-racines.html>>, prg, mia et lax3) que rien n'a cassé.

1. Pour voir le RFC de numéro NNN, <http://www.ietf.org/rfc/rfcNNN.txt>, par exemple <http://www.ietf.org/rfc/rfc2671.txt>