Problème DNSSEC au Libéria

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 13 juin 2024. Dernière mise à jour le 16 juin 2024

https://www.bortzmeyer.org/dnssec-liberia.html

Le 12 juin, une panne (partielle ?) a touché le TLD .lr. Il s'agit d'un problème DNSSEC (qui a fait l'objet d'un retex détaillé par le gestionnaire technique.

L'alerte a été donné sur la liste de l'OARC <https://lists.dns-oarc.net/pipermail/dns-operations/2024-June/022595.html>. Au matin du 13 juin, on constate :

— Que Zonemaster <https://zonemaster.fr/> voit un problème <https://zonemaster.fr/en/result/77c33ec33e528a59>. Et que DNSviz <https://dnsviz.net/> est d'accord que ça ne va pas <https://dnsviz.net/d/lr/ZmqhSQ/dnssec/>.
— Que la plupart des résolveurs DNS <https://www.bortzmeyer.org/resolveur-dns.html>, même ceux qui valident avec DNSSEC, n'ont pas de problème avec .lr. Principale exception : celui de Cloudflare, 1.1.1.1.

Les sondes RIPE Atlas <https://atlas.ripe.net/> sont d'accord pour dire que ça marche mais pas parfaitement :

```
% blaeu-resolve --requested 200 --type SOA --displayvalidation lr
[ (Authentic Data flag)  rip.psg.com. hostmaster.psg.com. 1718251170 345600 3600 2592000 14400] : 88 occurrences
[rip.psg.com. hostmaster.psg.com. 1718251170 345600 3600 2592000 14400] : 85 occurrences
[ERROR: SERVFAIL] : 13 occurrences
[ERROR: NXDOMAIN] : 11 occurrences
[ (Authentic Data flag)  rip.psg.com. hostmaster.psg.com. 1718225894 345600 3600 2592000 14400] : 1 occurrences
[] : 1 occurrences
Test #73322645 done at 2024-06-13T07:39:43Z
```

L'explication technique est probablement la suivante : en interrogeant tous les serveurs faisant autorité <https://www.bortzmeyer.org/serveur-dns-faisant-autorite.html> pour .lr, avec la requête lr/DNSKEY, on voit que certains envoient deux signatures (ayant le même identificateur de clé, 29984) :

```
lr. 86400 IN DNSKEY 257 3 8 (
AwEAAbdBaOsz0xNn+L+8+GopcC0w9NneWhK19GJyCR5d ...
) ; KSK; alg = RSASHA256 ; key id = 29984
lr. 86400 IN DNSKEY 256 3 8 (
AwEAAci9weuAQKBbKsqkOYnm1H0C5a7ZX/8xoQDmNp8Y ...
) ; ZSK; alg = RSASHA256 ; key id = 42940
lr. 86400 IN RRSIG DNSKEY 8 1 86400 (
20240626012025 20240611235025 29984 lr.
YeZQ3KiSsDQD3jizNHXnTUYxRtzJwXl0aoctrgqDqajW ...
lr. 86400 IN RRSIG DNSKEY 8 1 86400 (
20240626205813 20240612192813 29984 lr.
lDt9P1RZtcs+/SDilJZ6tNRsZr+F5EdisfmsNw7E62+1 ...
```

Cela ne se voit pas à l'œil nu mais une des deux signatures est invalide (cf. les rapports de DNSviz et Zonemaster). Les résolveurs qui réussissent sont ceux qui sont tombés sur le serveur faisant autorité qui ne servait que la bonne signature, ou bien testaient les deux signatures (d'où l'importance de tester plus qu'une signature, malgré KeyTrap <https://www.bortzmeyer.org/keytrap.html>). Notez que, malgré cette différence des réponses, tous les serveurs faisant autorité ont le même numéro de série :

```
% check-soa lr
fork.sth.dnsnode.net.
77.72.229.254: OK: 1718251170
2a01:3f0:0:306::53: OK: 1718251170
ns-lr.afrinic.net.
196.216.168.61: OK: 1718251170
2001:43f8:120::61: OK: 1718251170
rip.psg.com.
2001:418:1::39: OK: 1718251170
147.28.0.39: OK: 1718251170
```

La commande pour interroger tous les serveurs est :

```
% for server in 77.72.229.254 2a01:3f0:0:306::53 2001:43f8:120::61 196.216.168.61 2001:418:1::39 147.28.0.39
  echo $server
  dig +dnssec @$server lr DNSKEY
done  > lr.txt
```

Comme elle est faite depuis un seul point de mesure (mon bureau), elle a ses limites, notamment, elle ne détectera pas les différences entre instances d'un même nuage "*anycast*".

Y avait-il collision des identificateurs de clé comme en Russie en début d'année <https://www.bortzmeyer.org/ru-dnssec.html> ? Comme vu plus loin, le problème était autre. Un indice : le Liban, qui a le même gestionnaire technique, avait le même problème <https://dnsviz.net/d/lb/ZmvOgA/dnssec/>.

Bref, les explications techniques complètes figurent dans cet article <https://archive.psg.com/240614.dns-post-mortem> très détaillé ; une attaque par déni de service a déclenché une bogue assez bizarre dans le signeur, Knot <https://www.knot-dns.cz/>.