Problème DNSSEC subtil dans fbi.gov

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 19 juillet 2013

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

Le système de sécurité DNSSEC vise à protéger la résolution DNS contre les attaques par empoisonnement (comme l'attaque Kaminsky <https://www.bortzmeyer.org/comment-fonctionne-la-faille-kamins
html>). Mais, comme toutes les techniques de sécurité, il introduit d'autres risques, notamment celui de casser des choses si on ne fait pas très attention. C'est ce qui arrive en ce moment à `fbi.gov`, domaine du FBI.

La question a été discutée depuis le 17 juillet sur la liste des utilisateurs de BIND <https://lists.isc.org/mailman/listinfo/bind-users> (et n'est pas encore résolue). À première vue, tout se passe bien :

```
% dig A fbi.gov
...
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 7, ADDITIONAL: 1
...
;; ANSWER SECTION:
fbi.gov. 600 IN A 72.21.81.85
fbi.gov. 600 IN RRSIG A 7 2 600 ...
...
```

On récupère la donnée qu'on voulait, l'adresse IPv4 (type `A`) et une signature (type `RRSIG`). La signature est valide, c'est pour cela que le résolveur DNS a mis le "*flag*" AD ("*Authentic Data*"). Donc, pourquoi certains parlent d'un problème ? Parce que si on demande quelque chose qui n'existe pas, mettons l'adresse IPv6, le résolveur proteste :

```
% dig AAAA fbi.gov
...
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 14748
...
```

On a cette fois SERVFAIL ("*Server Failure*"). Était-ce bien un problème DNSSEC ? Demandons au résolveur de ne **pas** valider, avec CD ("*Checking Disabled*") :

```
% dig +cd AAAA fbi.gov
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23962
;; flags: qr rd ra cd; QUERY: 1, ANSWER: 0, AUTHORITY: 3, ADDITIONAL: 1
...
;; QUESTION SECTION:
;fbi.gov. IN AAAA

;; AUTHORITY SECTION:
...
```

Cette fois, pas de problème (NOERROR) et pas de réponse (ANSWER: 0, ce qui est normal en l'absence d'une adresse IPv6). Donc, le problème est lié à DNSSEC puisque couper la validation le fait disparaître.

Mais comment se fait-il qu'un excellent service en ligne de vérification des zones DNSSEC, <http://dnsviz.net/>, ne voie aucun problème et affiche fbi.gov comme normal ? C'est parce que le problème ne se produit que sur les types de données qui n'existent pas dans cette zone. Si on déroule les options de DNSviz et qu'on coche "*Denial of existence*", cette fois, il affiche une erreur "*RRset is not covered by any RRSIG*".

Et cela nous donne une indication sur la cause du problème. Relisons la sortie de la commande dig +cd AAAA fbi.gov tapée plus haut. J'avais omis la section "*Authority*". Voyons-la :

```
;; AUTHORITY SECTION:
fbi.gov. 525 IN SOA ns1.fbi.gov. dns-admin.fbi.gov. 2013071601 7200 3600 2592000 43200
fbi.gov. 525 IN RRSIG SOA 7 2 600 20131014154120 20130716154120 32497 fbi.gov. mjg99/NUrrtRn51Ju90FeYyIlF0I
97S2G907NEFOJ79P721E4FEQ9LR3IT1S.fbi.gov. 525 IN NSEC3 1 0 10 BBAB A867R4P7R3SHMBUEO5I35R55QH3IEFAI A NS SO
```

L'erreur est dans la dernière ligne. Il y a bien un enregistrement NSEC3 (normalisé dans le RFC 5155[1]), qui sert à prouver que ce type AAAA n'existe pas. Mais ce NSEC3 n'est pas signé... Sur une zone correcte, ici afnic.fr, on trouverait cette signature (je prends le type LOC car afnic.fr a un AAAA) :

```
% dig LOC afnic.fr
...
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 1
...
;; AUTHORITY SECTION:
afnic.fr. 5400 IN SOA dnsmaster.nic.fr. hostmaster.nic.fr. 2013071908 7200 1800 2419200 5400
afnic.fr. 5400 IN RRSIG SOA 8 2 172800 20130726131527 20130719181913 43854 afnic.fr. IOjRTsqU++CxhlwMW3VAH8
4vti9ma10fgk5bpja8qq4phrc4ikk83g.afnic.fr. 5400 IN RRSIG NSEC3 8 3 5400 20130724210757 20130718041857 43854
4vti9ma10fgk5bpja8qq4phrc4ikk83g.afnic.fr. 5400 IN NSEC3 1 1 1 546A5140353A2BE3 68O926N7PINN2OC9URC70JUE5742
```

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc5155.txt

Le NSEC3 est bien signé, comme il doit l'être, permettant ainsi au résolveur de valider la réponse.

Maintenant, pourquoi cette curieuse absence de signature ? Aucun serveur de noms normal ne fait cela. La faute en revient probablement à un pare-feu placé devant le serveur et qui, trop zélé et pratiquant la DPI, élimine uniquement les signatures des NSEC3. C'est difficile à croire, je le sais, mais je ne vois pas d'autre explication.

Je n'ai rien trouvé par moi-même dans ce cas, cet article est entièrement tiré des excellentes analyses de Michael Sinatra, Bill Owens et Casey Deccio. Notez une autre erreur dans la zone : l'enregistrement SOA indique une adresse de contact dns-admin@fbi.gov mais celle-ci génére un avis de non-remise...