Free, noblogs.org et un curieux problème DNS / DNSSEC

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 9 octobre 2015

https://www.bortzmeyer.org/free-noblogs-dnssec.html

Quelques mois après le problème juralib.noblogs.org, les rézosocios ont bruissé de clameurs sur le domaine ladiscordia.noblogs.org, invisible depuis Free. Censure ou bavure ?

Beaucoup de gens ont crié à la censure, ce qui est raisonnable dans le contexte politique actuel <https://www.bortzmeyer.org/censure-francaise.html>, vu que le site Web derrière ce domaine sert en général des contenus politiquement radicaux <http://ladiscordia.noblogs.org/a-propos-dun-dispositif-de-surveillance-trouve-documente-et-detruit-a-paris/>. (Voir par exemple une discussion très foutraque sur Reddit <https://www.reddit.com/r/france/comments/3o02eo/cet_%C3%A9t%C3%A9_la_police_installe_un_syst%C3%A8me_de/>.) Mais, si la censure existe, les bogues existent aussi, et il existe davantage de maladroits que de méchants. Étudions donc la question.

D'abord, plaçons nous sur une machine connectée par Free **et** utilisant les résolveurs DNS de Free (ce n'est pas obligatoire <https://www.bortzmeyer.org/son-propre-resolveur-dns.html>). On constate qu'on ne peut pas visiter la page Web citée plus haut. Des tests techniques montrent que le problème est dans la résolution DNS. Pas moyen de trouver l'adresse IP associée au nom. Testons avec dig :

```
%  dig ladiscordia.noblogs.org
...
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 937
                                       ^^^^^^^^
                                       Server Failure
```

Ah, Houston, nous avons un problème. Le domaine noblogs.org étant signé avec DNSSEC (une excellente idée), regardons avec l'option +cd ("*Checking Disabled*") qui coupe la validation DNSSEC :

```
%  dig +dnssec +cd ladiscordia.noblogs.org

; <<>> DiG 9.10.2-P2 <<>> +cd ladiscordia.noblogs.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16475
;; flags: qr rd ra cd; QUERY: 1, ANSWER: 15, AUTHORITY: 5, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;ladiscordia.noblogs.org. IN A

;; ANSWER SECTION:
ladiscordia.noblogs.org. 2284 IN CNAME www.l.autistici.org.
ladiscordia.noblogs.org. 2284 IN RRSIG CNAME 7 2 9600 (
                                20151101063004 20151002063004 64367 noblogs.org.
                                LuRSXa97Yjr+wYVGjq8yFxIOTXeufRMNaL6L31jqq3im
                                MphTYlJRGvwTzZTPwbbbkZjSuCtt5P7l3/iMx50ZEZ/B
                                x3q0PDD3Yo4ckrfcIzMQ9V+HeosW+W78UBTC0LyQIxSq
                                eRdlhsNZKSELmR8k9sVpJ5mrQPTQ3HzGzUr4z1w= )
ladiscordia.noblogs.org. 2284 IN CNAME www.l.autistici.org.
ladiscordia.noblogs.org. 2284 IN RRSIG CNAME 7 2 9600 (
                                20151101063004 20151002063004 64367 noblogs.org.
                                LuRSXa97Yjr+wYVGjq8yFxIOTXeufRMNaL6L31jqq3im
                                MphTYlJRGvwTzZTPwbbbkZjSuCtt5P7l3/iMx50ZEZ/B
                                x3q0PDD3Yo4ckrfcIzMQ9V+HeosW+W78UBTC0LyQIxSq
                                eRdlhsNZKSELmR8k9sVpJ5mrQPTQ3HzGzUr4z1w= )
ladiscordia.noblogs.org. 2284 IN CNAME www.l.autistici.org.
ladiscordia.noblogs.org. 2284 IN RRSIG CNAME 7 2 9600 (
                                20151101063004 20151002063004 64367 noblogs.org.
                                LuRSXa97Yjr+wYVGjq8yFxIOTXeufRMNaL6L31jqq3im
                                MphTYlJRGvwTzZTPwbbbkZjSuCtt5P7l3/iMx50ZEZ/B
                                x3q0PDD3Yo4ckrfcIzMQ9V+HeosW+W78UBTC0LyQIxSq
                                eRdlhsNZKSELmR8k9sVpJ5mrQPTQ3HzGzUr4z1w= )

ladiscordia.noblogs.org. 2284 IN CNAME www.l.autistici.org.
ladiscordia.noblogs.org. 2284 IN RRSIG CNAME 7 2 9600 (
                                20151101063004 20151002063004 64367 noblogs.org.
                                LuRSXa97Yjr+wYVGjq8yFxIOTXeufRMNaL6L31jqq3im
                                MphTYlJRGvwTzZTPwbbbkZjSuCtt5P7l3/iMx50ZEZ/B
                                x3q0PDD3Yo4ckrfcIzMQ9V+HeosW+W78UBTC0LyQIxSq
                                eRdlhsNZKSELmR8k9sVpJ5mrQPTQ3HzGzUr4z1w= )
ladiscordia.noblogs.org. 2284 IN CNAME www.l.autistici.org.
ladiscordia.noblogs.org. 2284 IN RRSIG CNAME 7 2 9600 (
                                20151101063004 20151002063004 64367 noblogs.org.
                                LuRSXa97Yjr+wYVGjq8yFxIOTXeufRMNaL6L31jqq3im
                                MphTYlJRGvwTzZTPwbbbkZjSuCtt5P7l3/iMx50ZEZ/B
                                x3q0PDD3Yo4ckrfcIzMQ9V+HeosW+W78UBTC0LyQIxSq
                                eRdlhsNZKSELmR8k9sVpJ5mrQPTQ3HzGzUr4z1w= )
ladiscordia.noblogs.org. 2284 IN CNAME www.l.autistici.org.
ladiscordia.noblogs.org. 2284 IN RRSIG CNAME 7 2 9600 (
                                20151101063004 20151002063004 64367 noblogs.org.
                                LuRSXa97Yjr+wYVGjq8yFxIOTXeufRMNaL6L31jqq3im
                                MphTYlJRGvwTzZTPwbbbkZjSuCtt5P7l3/iMx50ZEZ/B
                                x3q0PDD3Yo4ckrfcIzMQ9V+HeosW+W78UBTC0LyQIxSq
                                eRdlhsNZKSELmR8k9sVpJ5mrQPTQ3HzGzUr4z1w= )
www.l.autistici.org.    1800 IN A 94.23.50.208
www.l.autistici.org.    1800 IN A 82.94.249.234
www.l.autistici.org.    1800 IN RRSIG A 7 4 30 (
                                20151105063002 20151006063002 2207 l.autistici.org.
                                HDkkzb8afOIlk5P0HRmiVal7KmAu4bevmkAPpHuAMruS
                                9Pj2OkWjeWwJiLm7zX5MjqIcfUBvJ6gbODvRGr7dDJHn
                                7qqLNA3IXMvxm5trBWz2/YZsTs/2XEgIBDVgxRel+OBp
                                HD+riKX0ZylmTGXG7/fyRfcYLquwphS4gNTMWbk= )

;; AUTHORITY SECTION:
l.autistici.org.        1800 IN NS ns1.investici.org.
```

---

https://www.bortzmeyer.org/free-noblogs-dnssec.html

```
l.autistici.org.        1800 IN NS ns2.investici.org.
l.autistici.org.        1800 IN NS ns2-v6.investici.org.
l.autistici.org.        1800 IN NS ns1-v6.investici.org.
l.autistici.org.        1800 IN RRSIG NS 7 3 30 (
                                20151105063002 20151006063002 2207 l.autistici.org.
                                bA28B6AP9NQzyavLXFZoxDCsV1kDpZwid+QyPcR2qhrj
                                c3wfuB6P2PM7WBHzlbZevt1C3+z/FMqvXRr/TrhbseDy
                                ScKCai/LPD68z0bqUucz0uuFbDpTxvJNDf+0zJrMQTsw
                                +zse/UsiopBVrqCjOXRWte2DvDxyCPtN3WnEYJc= )

;; Query time: 26 msec
;; SERVER: 192.168.2.254#53(192.168.2.254)
;; WHEN: Fri Oct 09 11:09:32 CEST 2015
;; MSG SIZE  rcvd: 1648
```

Ouh là, là, c'est long. Bien trop long, la répétition de l'enregistrement `CNAME` et de sa signature est tout à fait anormale. Est-ce de la faute du résolveur DNS Free ou bien du domaine `noblogs.org` ? Allons sur une autre machine qui utilise son propre résolveur, un Unbound :

```
% dig +dnssec ladiscordia.noblogs.org

; <<>> DiG 9.9.5-9+deb8u3-Debian <<>> +dnssec ladiscordia.noblogs.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62823
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 5, AUTHORITY: 7, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;ladiscordia.noblogs.org. IN A

;; ANSWER SECTION:
ladiscordia.noblogs.org. 6082 IN CNAME www.l.autistici.org.
ladiscordia.noblogs.org. 6082 IN RRSIG CNAME 7 2 9600 (
                                20151101063004 20151002063004 64367 noblogs.org.
                                LuRSXa97Yjr+wYVGjq8yFxIOTXeufRMNaL6L31jqq3im
                                MphTYlJRGvwTzZTPwbbbkZjSuCtt5P7l3/iMx50ZEZ/B
                                x3q0PDD3Yo4ckrfcIzMQ9V+HeosW+W78UBTC0LyQIxSq
                                eRdlhsNZKSELmR8k9sVpJ5mrQPTQ3HzGzUr4z1w= )
www.l.autistici.org.    30 IN A 94.23.50.208
www.l.autistici.org.    30 IN A 82.94.249.234
www.l.autistici.org.    30 IN RRSIG A 7 4 30 (
                                20151105063002 20151006063002 2207 l.autistici.org.
                                HDkkzb8afOIlk5P0HRmiVal7KmAu4bevmkAPpHuAMruS
                                9Pj2OkWjeWwJiLm7zX5MjqIcfUBvJ6gbODvRGr7dDJHn
                                7qqLNA3IXMvxm5trBWz2/YZsTs/2XEgIBDVgxRel+OBp
                                HD+riKX0ZylmTGXG7/fyRfcYLquwphS4gNTMWbk= )

;; AUTHORITY SECTION:
EDG28OM0KF8LV6JVVTUAE9R7GLNTNKMD.noblogs.org. 82 IN NSEC3 1 0 10 5CA1AB1E (
                                K1C26GO8L9TJ398E8MKH7QLSP4LB88UO
                                CNAME RRSIG )
EDG28OM0KF8LV6JVVTUAE9R7GLNTNKMD.noblogs.org. 82 IN RRSIG NSEC3 7 3 3600 (
                                20151101063004 20151002063004 64367 noblogs.org.
                                juTchEjZZFdj5WkhyKh/2qZxffIjahcjtWrC7aiM78QT
                                nuBLP6AqRatIwpbIauM9ZbBwXD1ZXwRhpZrLTDKqS8bK
                                qU5dsUCKsB3vIYba84I12t1bAg0YKv0HP8bkEMp9ftO+
                                bZNLtY+TXyaZ5FULNI26gMen2YYsqPovY0YnH0M= )

l.autistici.org.        30 IN NS ns2-v6.investici.org.
l.autistici.org.        30 IN NS ns2.investici.org.
l.autistici.org.        30 IN NS ns1.investici.org.
l.autistici.org.        30 IN NS ns1-v6.investici.org.
```

```
l.autistici.org.        30 IN RRSIG NS 7 3 30 (
                                20151105063002 20151006063002 2207 l.autistici.org.
                                bA28B6AP9NQzyavLXFZoxDCsV1kDpZwid+QyPcR2qhrj
                                c3wfuB6P2PM7WBHzlbZevt1C3+z/FMqvXRr/TrhbseDy
                                ScKCai/LPD68z0bqUucz0uuFbDpTxvJNDf+0zJrMQTsw
                                +zse/UsiopBVrqCjOXRWte2DvDxyCPtN3WnEYJc= )

;; Query time: 239 msec
;; SERVER: ::1#53(::1)
;; WHEN: Fri Oct 09 11:12:01 CEST 2015
;; MSG SIZE  rcvd: 977
```

On n'a pas cette fois la répétition des `CNAME`, c'est plus normal (et valide : le bit AD "*Authentic Data*" dans la réponse nous l'indique). Autre façon de vérifier qu'il y a bien un problème spécifique à Free, demander aux sondes RIPE Atlas <https://atlas.ripe.net/> françaises (avec ce programme <https://github.com/RIPE-Atlas-Community/ripe-atlas-community-contrib/blob/master/resolve-name.py>) ce qu'elles voient :

```
% python resolve-name.py -r 500 -c FR -t A ladiscordia.noblogs.org
Measurement #2490878 for ladiscordia.noblogs.org/A uses 500 probes
[ERROR: REFUSED] : 3 occurrences
[ERROR: SERVFAIL] : 116 occurrences
[82.94.249.234 94.23.50.208] : 338 occurrences
Test done at 2015-10-08T08:58:30Z
```

La plupart voient la bonne réponse (deux adresses IP), 116 d'entre elles reçoivent le `SERVFAIL`. Ce sont celles situées sur ce réseau de Free. Limitons la requête à l'AS de Free :

```
% python resolve-name.py -r 500 --as 12322 -t A ladiscordia.noblogs.org
Measurement #2495118 for ladiscordia.noblogs.org/A uses 233 probes
[ERROR: REFUSED] : 1 occurrences
[ERROR: SERVFAIL] : 161 occurrences
[82.94.249.234 94.23.50.208] : 62 occurrences
Test done at 2015-10-09T09:18:07Z
```

La majorité des sondes Atlas chez Free ont le problème (certains clients de Free ont leur propre résolveur et ne voient donc pas le problème).

Donc, c'est chez Free ? Il n'y a pas de problème dans la zone `noblogs.org` ? Je dois confesser que j'avais stupidement mis en cause cette zone sur Twitter, en confondant avec un autre cas. Comme les gens qui criaient à la censure, j'avais réagi trop vite en sens inverse. Toutes mes excuses au mainteneur de `noblogs.org`, cette zone ne semble pas avoir de problème DNSSEC grave, comme le montrent très bien DNSviz <http://dnsviz.net/d/ladiscordia.noblogs.org/VhbpAg/dnssec/> ou ZoneMaster <https://www.zonemaster.fr/test/38179> (il y a des erreurs mais pas graves et sans lien avec DNSSEC).

Mais, alors, qu'est-ce qui se passe ? Y aurait-il bien censure délibérée par Free ? Sans doute pas. En effet, en comparant le résultat des commandes dig avec le résolveur DNS de Free et un autre résolveur, on voit le problème : **l'enregistrement NSEC3 est manquant**. Ça veut dire quoi ? NSEC3, normalisé dans le RFC 5155 [1], sert à prouver qu'un nom n'existe pas. Ici, comme la zone `noblogs.org` utilise des jokers (tout nom, même `gfcgf565FsdZE523SEDvgGFSS.noblogs.org` va marcher, cf. RFC 1034, section 4.3.3), le NSEC3 doit être envoyé pour prouver que le nom demandé, `ladiscordia.noblogs.org`, n'existait pas réellement mais été synthétisé via le joker. Dans la réponse du résolveur correct, on a le NSEC3 :

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

```
EDG28OM0KF8LV6JVVTUAE9R7GLNTNKMD.noblogs.org. 82 IN NSEC3 1 0 10 5CA1AB1E (
                                K1C26GO8L9TJ398E8MKH7QLSP4LB88UO
                                CNAME RRSIG )
```

Mais on ne l'a pas dans la réponse du résolveur de Free. Si on teste avec DNSviz <https://dnsviz.net/> en local, en passant à travers le résolveur de Free, le rapport (en JSON) nous dit la même chose :

```
"errors": [
    {
        "description": "No NSEC RR(s) were returned to validate the wildcard response.",
        "code": "MISSING_NSEC_FOR_WILDCARD",
        "servers": [
            "192.168.2.254"
        ],
        "tags": [
            "UDP_272_EDNS0_32768_4096"
        ]
    }
...
```

(Au passage, notez que Free force un TTL minimum <https://www.bortzmeyer.org/forcer-ttl.html>, ce qui fait également couiner DNSviz, car DNSSEC ne permet pas ce genre de manips :

```
"errors": [
      {
          "description": "The TTL of the RRset (1665) exceeds the value of the Original TTL field of the RRSIG
          "code": "ORIGINAL_TTL_EXCEEDED"
      }
...
```

)

Comment un résolveur ayant ces données voit qu'il y a un problème DNSSEC (et va donc renvoyer SERVFAIL)? Grâce au champ "*Number of labels*" de la signature (RFC 4034, section 3.1.3). Lorsque le nom existe, ce champ indique le nombre de composants dans le nom demandé :

```
www.noblogs.org.        9600 IN RRSIG CNAME 7 3 9600 (
                                20151101063004 20151002063004 64367 noblogs.org.
                                k7l/nfVCejZ+pO7BPIPEPaQs7w09CE/4SJL7rjItAEqf
                                ...
```

Le champ est le troisième après le type RRSIG. Ici, il vaut trois, ce qui est bien le nombre de composants du nom de domaine demandé. Mais lorsque le nom a été synthétisé grâce au joker :

```
ladiscordia.noblogs.org. 5073 IN RRSIG CNAME 7 2 9600 (
                                20151101063004 20151002063004 64367 noblogs.org.
                                LuRSXa97Yjr+wYVGjq8yFxIOTXeufRMNaL6L31jqq3im
...
```

Alors, le champ ne vaut que deux, indiquant qu'il y a un joker dans le deuxième composant (la zone `noblogs.org` ; après tout, le joker pourrait être dans une zone parente ou grand-parente). Le résolveur DNSSEC voit donc que la signature couvre en fait le joker :

```
*.noblogs.org.          9600 IN RRSIG CNAME 7 2 9600 (
                                20151101063004 20151002063004 64367 noblogs.org.
                                LuRSXa97Yjr+wYVGjq8yFxIOTXeufRMNaL6L31jqq3im
                                ...
```

(Regardez la signature, c'est la même que pour `ladiscordia` mais pas la même que pour `www`.) Le résolveur validant va donc chercher un NSEC3 prouvant que le nom n'existe pas (un nom existant masque le joker), ne le trouve pas, et paf, `SERVFAIL`.

Pourquoi le résolveur de Free a-t-il omis le NSEC3, qui est bien envoyé par les serveurs faisant autorité pour `noblogs.org` ? L'investigation doit s'arrêter là, je n'ai pas accès à l'intérieur de ces résolveurs. Je soupçonne que la duplication anormale des `CNAME` a mené à une réponse trop grosse et que l'enregistrement NSEC3 a été abandonné.

Donc, ma conclusion est que les résolveurs de Free sont en tort, mais qu'il s'agit très probablement d'une bogue et pas d'une attaque délibérée. Quant à la zone `noblogs.org`, elle n'avait d'autres torts que de combiner des techniques compliquées (jokers et NSEC3).

Notez que, six mois plus tard, la bogue n'était pas réparée <`https://www.bortzmeyer.org/free-dnssec-reloaded.html`>, et se déclenche même sans NSEC3.