Censure DNS du domaine d'Uptobox par Orange

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 15 mai 2023

https://www.bortzmeyer.org/uptobox-orange.html

Depuis ce matin, Orange censure le service Uptobox <https://uptobox.com/> via un résolveur DNS <https://www.bortzmeyer.org/resolveur-dns.html> menteur. Avec quelques particularités techniques...

Voyons d'abord les faits. Depuis une machine connectée via Orange, testons avec dig (et j'expliquerai plus tard le rôle de l'option +nodnssec, sachez seulement que le client DNS typique d'un résolveur envoie exactement cette même requête) :

```
% dig  +nodnssec A uptobox.com
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38435
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
...
;; ANSWER SECTION:
uptobox.com. 5 IN A 127.0.0.1

;; Query time: 60 msec
;; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)
;; WHEN: Mon May 15 16:52:31 CEST 2023
;; MSG SIZE  rcvd: 56
```

Bon, cas classique de censure par résolveur DNS <https://www.bortzmeyer.org/resolveur-dns.html> menteur. Au lieu de renvoyer la vraie adresse IP, il renvoie ce 127.0.0.1 qui indique la machine locale (rien ne fonctionnera, donc). Est-ce juste chez moi ? Non. En testant avec les sondes RIPE Atlas <https://atlas.ripe.net/>, on voit que cela affecte beaucoup d'utilisateurs d'Orange (AS 3215) :

```
% blaeu-resolve --requested  100 --as 3215 --type A Uptobox.com
[104.22.30.128 104.22.31.128 172.67.29.218] : 17 occurrences
[127.0.0.1] : 82 occurrences
[] : 1 occurrences
Test #53746153 done at 2023-05-15T11:02:58Z
```

Les sondes qui obtiennent les vraies adresses sont probablement celles situées sur un réseau qui utilise un autre résolveur, par exemple un résolveur local non-menteur <https://www.bortzmeyer.org/son-propre-resolveur-dns.html>.

Parfois, en cas de mensonge, des résolveurs envoient des détails, par exemple sous forme d'un enregistrement SOA, dont les données indiquent la source de la censure, mais rien de tel ici.

Ah, et, sinon, le blocage concerne également `uptostream.com`, `uptobox.fr`, `uptostream.fr`, `beta-uptobox.com` et `uptostream.net` mais je ne les ai pas testés.

Pourquoi ce blocage ? Aucun autre FAI en France ne semble le faire. Testons chez Free ou chez Bouygues :

```
% blaeu-resolve --requested  100 --as 12322 --type A Uptobox.com
[104.22.30.128 104.22.31.128 172.67.29.218] : 99 occurrences
Test #53746411 done at 2023-05-15T11:07:43Z

% blaeu-resolve --requested  100 --as  5410 --type A Uptobox.com
[104.22.30.128 104.22.31.128 172.67.29.218] : 33 occurrences
Test #53746432 done at 2023-05-15T11:08:30Z
```

Bon, donc, pour l'instant, seul Orange bloque (même plusieurs heures après, la situation n'avait pas changé). On aurait pu penser qu'il ne s'agissait donc probablement pas de censure étatique (puisque celle-ci s'appliquerait aux autres gros FAI) mais en fait si, comme publié par la suite <https://www.linforme.com/tech-telecom/article/piratage-la-justice-ordonne-le-blocage-de-l-heberge
650.html>.

La censure est cohérente pour IPv6 :

```
% blaeu-resolve --requested  100 --as 3215 --type AAAA Uptobox.com
[] : 19 occurrences
[::1] : 76 occurrences
[::] : 1 occurrences
Test #53746202 done at 2023-05-15T11:04:00Z
```

On obtient le `::1`, équivalent IPv6 du `127.0.0.1`.

Mais revenons à ce `+nodnssec` que j'avais promis d'expliquer. Eh bien, le comportement des résolveurs DNS d'Orange va changer selon que son client envoie ou non le bit DO ("*DNSSEC OK*"). Par défaut, dig ne l'envoie pas (donc, en toute rigueur, l'option `+nodnssec` n'était pas nécessaire) et le résolveur ment. Mais si on demande DNSSEC, on a une réponse sincère :

```
% dig  +dnssec A uptobox.com
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50574
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1
...
;; ANSWER SECTION:
uptobox.com. 300 IN A 104.22.30.128
uptobox.com. 300 IN A 172.67.29.218
```

```
uptobox.com. 300 IN A 104.22.31.128
uptobox.com. 300 IN RRSIG A 13 2 300 (
20230516155749 20230514135749 34505 uptobox.com.
qMunXCqcFHp34LAnTgMcJkQaUvlMaZBLIneA5eqTHW+0
pjuD6vTVvn1xsnAAI59SOcQdgRIo5hlMLxKHZzg3Ew== )

;; Query time: 36 msec
;; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)
;; WHEN: Mon May 15 16:57:45 CEST 2023
;; MSG SIZE  rcvd: 195
```

Notez que le résolveur DNS par défaut de la connexion utilisée était un petit routeur 4G, qui relaie aux « vrais » résolveurs derrière. Si je parle directement à ceux-ci, j'observe le même phénomène :

```
~ % dig @81.253.149.5 +nodnssec A uptobox.com
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24064
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
...
;; ANSWER SECTION:
uptobox.com. 5 IN A 127.0.0.1

;; Query time: 52 msec
;; SERVER: 81.253.149.5#53(81.253.149.5) (UDP)
;; WHEN: Mon May 15 16:59:14 CEST 2023
;; MSG SIZE  rcvd: 84

% dig @81.253.149.5 +dnssec A uptobox.com
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15640
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1
...
;; ANSWER SECTION:
uptobox.com. 300 IN A 104.22.31.128
uptobox.com. 300 IN A 172.67.29.218
uptobox.com. 300 IN A 104.22.30.128
uptobox.com. 300 IN RRSIG A 13 2 300 (
20230516155921 20230514135921 34505 uptobox.com.
ebLAOe7dQSbyfE9Jvbq3+lvLvH5ZVB8esGxEW0mhuaR9
HLvMNfTwkYZBEy8HEJwbfmci0sVavIhQ6ZaPJbw6SA== )

;; Query time: 64 msec
;; SERVER: 81.253.149.5#53(81.253.149.5) (UDP)
;; WHEN: Mon May 15 16:59:17 CEST 2023
;; MSG SIZE  rcvd: 223
```

Mais quel est le rôle de ce bit DO ("*DNSSEC OK*") et pourquoi cette différence de comportement, que je n'avais jamais observée sur le terrain ? Ce bit, normalisé dans le RFC 3225 [1], indique à un serveur DNS que son client comprend DNSSEC, et qu'il veut obtenir les informations DNSSEC, notamment les signatures. Outre le déboguage (dig avec l'option `+dnssec`), il est utilisé lorsqu'un résolveur validant parle à un serveur DNS, afin d'obtenir les informations cryptographiques à valider. Le « bête » client DNS, qui se trouve dans la machine de M. Toutlemonde, ne valide pas et fait donc une confiance aveugle au résolveur. Il n'envoie pas de bit DO (et c'est pour cela que la majorité des utilisateurs voient le nom être censuré). Mais si vous avez un résolveur qui valide, par exemple sur votre machine ou dans

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc3225.txt`

votre réseau local <https://www.bortzmeyer.org/son-propre-resolveur-dns.html>, il va envoyer le bit DO. Pourquoi est-ce que les résolveurs d'Orange se comportent différemment dans ces deux cas ? Il y a une certaine logique technique : les résolveurs DNS menteurs cassent DNSSEC (puisque DNSSEC a justement été conçu pour détecter les modifications faites par un tiers), et il est donc raisonnable, bien que ce soit la première fois que je vois cela, de ne pas mentir si on a un client validant.

Petit détail technique au passage : le domaine `uptobox.com` est signé mais il n'y a pas d'enregistrement DS dans la zone parente (`.com`) donc il n'aurait pas été validé de toute façon.

Quelques références :

— Tweet d'Uptobox <https://twitter.com/Uptobox_com/status/1658074496757104641> (avec des conseils contestables <https://www.bortzmeyer.org/dns-resolveurs-publics.html>).