

Qu'est-ce qu'un « DNS menteur » ?

Stéphane Bortzmeyer

<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 28 octobre 2026

<https://www.bortzmeyer.org/resolveur-dns-menteur.html>

Cet article explique le concept de « DNS menteur », terme souvent entendu, par exemple dans le contexte de la censure de l'Internet.

Si vous lisez souvent ce blog, vous n'apprendrez rien de nouveau ici. Le but de cet article est juste d'avoir une référence stable pour expliquer ce terme de « DNS menteur », sinon pour un large public, du moins pour une population plus large que les seuls experts DNS.

Donc, pour commencer, tout petit rappel sur le DNS ("*Domain Name System*") : le DNS permet de distribuer de l'information aux machines connectées à l'Internet. (Les humain-es normaux ne regardent en général pas cette information, qui est purement technique.) La clé d'accès à cette information est un nom de domaine comme `www.bortzmeyer.org` ou `phy.cam.ac.uk`. Le point important est que quasiment toute interaction sur l'Internet commence par une utilisation du DNS, que votre machine fait pour vous. Si le DNS est en panne, c'est quasiment comme si vous n'avez plus d'Internet. Et, ce qui nous intéresse ici, si le DNS vous ment sur les informations techniques récupérées, vous n'avez guère d'autre choix que de le croire. (Avis aux expert-es : oui, je simplifie. J'ai indiqué quelques ressources plus complètes à la fin de cet article.)

Votre machine (ordinateur, ordiphone, brosse à dents connectée) fait des requêtes DNS pour vous et elle les fait à un serveur nommé résolveur DNS <<https://www.bortzmeyer.org/resolveur-dns.html>>. C'est une machine en général gérée par l'organisation qui vous fournit l'accès à l'Internet. Normalement, en l'absence de « DNS menteur », votre résolveur ne fabrique pas d'information, il se contente de vous transmettre ce qu'il a appris d'une autre famille de serveurs DNS, les serveurs faisant autorité <<https://www.bortzmeyer.org/serveur-dns-faisant-autorite.html>>. Ceux-ci sont gérés par diverses organisations, par exemple les serveurs faisant autorité pour `cnrs.fr` sont gérés par le CNRS, alors que ceux faisant autorité pour `sephora.fr` sont gérés par l'hébergeur Akamai.

Donc, normalement, lorsque vous voulez envoyer du courrier à `QuelqUn@cnrs.fr`, une machine va demander à un résolveur DNS quel est le serveur de messagerie du CNRS et cette réponse viendra des serveurs faisant autorité pour `cnrs.fr`. Mais ça, c'est le comportement normal. Or, puisque presque toute interaction sur l'Internet commence par un appel au DNS, un certain nombre de gens se sont dit

qu'ils pouvaient utiliser ce qui était conçu comme un service technique en **outil de contrôle**. Après tout, qui contrôle le résolveur, contrôle la quasi-entièreté du vécu de l'utilisateurice.

Un « DNS menteur » ou, plus rigoureusement, un « **résolveur DNS** <https://www.bortzmeyer.org/resolveur-dns.html> » est donc un résolveur qui, au lieu de relayer sincèrement les réponses des serveurs faisant autorité, invente des réponses, en général, dans le but de bloquer l'accès à un service Internet.

Notez bien que les résolveurs DNS menteurs ne sont pas tous pareils. Ils diffèrent par :

- La raison du mensonge : cela peut être la censure étatique, la censure au profit des ayant-droits, le blocage des publicités, le blocage de l'accès à des services malveillants, etc,
- la nature de l'entité qui décide : le résolveur menteur a pu être configuré pour mentir par l'utilisateurice, par quelqu'un agissant sur demande de l'utilisateurice ou par un tiers (par exemple dans le cas de la censure).

Vous noterez donc que « résolveur DNS menteur » est une simple description factuelle, les motivations et les acteurs étant variés. Des exemples d'utilisation pour la censure sont communs en Europe. Au moment de l'écriture de cet article, le gouvernement français a annoncé son intention <https://www.blast-info.fr/articles/2026/information-exclusive-blast-le-premier-ministre-a-prepare> de pouvoir bloquer les réseaux sociaux sur simple demande de sa part, et, si cela se fait, ce sera sans doute via des résolveurs DNS menteurs. (D'autres pays dans le monde utilisent d'autres techniques de censure de l'Internet.) Si vous voulez par contre un exemple dans le domaine du blocage de ces insupportables (et dangereuses <https://citizenlab.ca/research/how-discover-tech-turned-targeted-a>) publicités, le système Pi-hole est un résolveur configuré pour mentir sur les noms de domaine utilisés par les services de publicité.

On fait souvent remarquer que, comme technique de censure, le résolveur DNS menteur n'est pas efficace car il est toujours possible de changer de résolveur. C'est techniquement exact mais il y a deux limites :

- L'opération est souvent plus complexe qu'il ne paraît, par exemple certains FAI, comme Orange, ne permettent pas cette opération sur leur "box". OK, on peut toujours y arriver mais tout le monde n'a pas forcément envie de se lancer dans ce genre de manipulations. (Si vous n'êtes pas technicien-ne et qu'un technicien prétentieux vous affirme que c'est trivial à faire, ne le croyez pas <https://www.bortzmeyer.org/changer-dns.html>.)
- Et, surtout, il n'est pas normal que l'accès à l'information soit limité aux citoyen-nés qui ont la connaissance de la technique.

(Oui, je sais, on peut aussi utiliser un VPN.)

Le reste de cet article est consacré à un certain nombre de détails, en général de nature technique. D'abord, que se passe-t-il précisément quand un résolveur vous ment. Essayons avec le domaine `tarjetarojatvlive`. Ironiquement, le site Web ne marche plus (il semble rediriger vers des choses assez louches, ne l'essayez pas) mais, à une époque, une décision de justice au profit des ayant-droits exigeait sa censure. Avec les résolveurs de Free :

```
% dig @212.27.40.240 tarjetarojatvlive.net
...
;; Got answer:
;; -->HEADER<- opcode: QUERY, status: NOERROR, id: 35658
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;tarjetarojatvlive.net. IN A
```

```
;; ANSWER SECTION:
tarjetarojatvlive.net. 600 IN A 127.0.0.1

;; Query time: 5 msec
;; SERVER: 212.27.40.240#53(212.27.40.240) (UDP)
;; WHEN: Wed Oct 28 16:26:09 CET 2026
;; MSG SIZE rcvd: 66
```

La réponse est clairement mensongère, l'adresse 127.0.0.1 étant l'adresse locale de la machine. (Les vraies adresses sont 172.104.149.86 et quelques autres.)

Ensuite, comment savoir si le résolveur que vous utilisez ment ? Une solution possible est évidemment de lire sa documentation mais, par exemple, en France, je ne connais aucun FAI qui documente les censures pratiquées. Il existe une solution technique pour que le résolveur indique qu'il a menti, les EDE ("*Extended DNS Error*"), normalisées dans le RFC 8914¹ mais, là encore, je ne connais pas de FAI français qui les utilise (comme vous le voyez dans la réponse de Free ci-dessus). Par contre, Google Public DNS le fait. Regardons avec dig :

```
% dig @8.8.8.8 tarjetarojatvlive.net
...
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 65388
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
; EDE: 16 (Censored): (The requested domain is subject to a judicial injunction or other governmental blocking o
;; QUESTION SECTION:
;tarjetarojatvlive.net. IN A

;; Query time: 6 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Wed Oct 28 16:22:46 CET 2026
;; MSG SIZE rcvd: 276
```

Il ne s'agit pas réellement d'un résolveur DNS menteur car Google a été franc : le domaine est censuré (code EDE 16) et Google renvoie même à la page Lumen décrivant ce cas <<https://lumendatabase.org/notices/41939614>>. Mais le résultat va être le même pour l'utilisateur, simplement plus clair. D'ailleurs, je ne sais pas pourquoi Free, dans l'exemple plus haut, renvoie une adresse bidon (le 127.0.0.1) au lieu d'un code REFUSED (comme Google) ou à la rigueur NXDOMAIN (indiquant que le domaine n'existe pas). Certains résolveurs DNS menteurs renvoient une adresse IP qui est celle d'un serveur Web contenant des explications mais c'est la pire solution de toutes, par exemple pour la vie privée <<https://www.bortzmeyer.org/google-detourne-par-orange.html>>.

La censure dépend évidemment du pays et, pour étudier la censure dans d'autres pays que le vôtre, vous pouvez utiliser, par exemple, les sondes RIPE Atlas <<https://labs.ripe.net/author/>>

1. Pour voir le RFC de numéro NNN, <https://www.ietf.org/rfc/rfcNNN.txt>, par exemple <https://www.ietf.org/rfc/rfc8914.txt>

stephane_bortzmeyer/dns-censorship-dns-lies-as-seen-by-ripe-atlas/> (attention toutefois aux questions éthiques <<https://labs.ripe.net/author/kistel/ethics-of-ripe-atlas-measurements>>).

J'ai dit qu'on pouvait toujours (plus ou moins facilement) changer de résolveur. Je ne vais pas donner de liste de résolveurs, car, dès qu'ils sont largement utilisés, ils deviennent des cibles pour la censure. Il faut au contraire, dans ce cas comme dans beaucoup, plein de résolveurs un peu partout. (Et les résolveurs publics des GAFAs sont évidemment à éviter <<https://www.bortzmeyer.org/dns-resolveurs-publics.html>>.)

Et quelques lectures supplémentaires :

- Sur ce blog, le premier article que j'avais fait sur le sujet <<https://www.bortzmeyer.org/dns-menteur.html>> en 2009, un article plus détaillé sur le cas de la censure administrative française <<https://www.bortzmeyer.org/censure-francaise.html>> (ce n'est hélas pas un sujet nouveau), un autre exemple français, cette fois sur demande des ayant-droits <<https://www.bortzmeyer.org/uptobox-orange.html>>, un article sur le fait qu'un résolveur qui refuse de mentir n'a parfois d'autre choix que d'arrêter de servir un pays <<https://www.bortzmeyer.org/opendns-quitte-france.html>> et un article sur la possibilité d'avoir son propre résolveur <<https://www.bortzmeyer.org/son-propre-resolveur-dns.html>>, qu'on contrôle.
- L'IETF a produit le RFC 7754 pour discuter du problème du blocage et du filtrage sur l'Internet (voir aussi le RFC 9707). Puisqu'on parle de l'IETF, notons que cette organisation a renoncé à normaliser le système RPZ <<https://www.bortzmeyer.org/echec-rpz.html>> qui sert à configurer certains résolveurs DNS menteurs <<https://www.bortzmeyer.org/rpz-faire-mentir-resolveur-dns.html>>.
- La question des résolveurs DNS menteurs est ancienne et le Conseil Scientifique de l'Afnic avait fait une excellente étude <<https://www.afnic.fr/observatoire-ressources/actualites/le-conseil-scientifique-de-lafnic-partage-sur-le-filtrage-internet-par-dns/>> sur la question, en 2013.
- L'article de Wikipédia sur le sujet est médiocre et ancien. Si vous avez le courage de l'améliorer, vous pouvez copier-coller du contenu de cet article, les licences sont compatibles.