Utiliser un résolveur DNS public ?

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 15 janvier 2017

https://www.bortzmeyer.org/dns-resolveurs-publics.html

Après la censure administrative en France via des DNS menteurs <https://www.bortzmeyer.org/censure-francaise.html>, puis une panne spectaculaire des résolveurs DNS d'Orange <https://www.bortzmeyer.org/resolveur-dns-en-panne.html>, au moins trois pannes analogues de ceux de Free <https://www.nextinpact.com/news/102862-free-problemes-dns-a-repetition-rendent-htm>, et enfin un détournement accidentel de Google et Wikipédia vers le Ministère de l'Intérieur <https://www.bortzmeyer.org/google-detourne-par-orange.html>, pas mal d'utilisat[Caractère Unicode non montré [1]]eur[Caractère Unicode non montré]rice[Caractère Unicode non montré]s de l'Internet se demandent si on peut vraiment faire confiance au résolveur <https://www.bortzmeyer.org/resolveur-dns.html> DNS de son FAI. Et beaucoup se mettent alors à utiliser un résolveur DNS public, le plus célèbre étant Google Public DNS <https://www.bortzmeyer.org/google-dns.html>. Mais est-ce une bonne idée ?

D'abord, recadrons un peu la terminologie. Le protocole DNS a deux sortes de serveurs, qui n'ont pas grand'chose à voir, les **serveurs faisant autorité <https://www.bortzmeyer.org/serveur-dns-faisant-autorit html>** et les **résolveurs <https://www.bortzmeyer.org/resolveur-dns.html>**. Confondre les deux (par exemple en parlant du vague « serveur DNS ») ne va pas aider l'utilisat[Caractère Unicode non montré]eur[Caractère Unicode non montré]rice à comprendre, et donc à faire des choix corrects. Les serveurs faisant autorité sont ceux qui connaissent les informations sur le contenu des domaines. Par exemple, ceux de l'AFNIC connaissent le contenu de `.fr` et ceux de CloudFlare, hébergeur utilisé par Next INpact, connaissent le contenu de `nextinpact.com`, par exemple l'adresse du site Web <https://www.nextinpact.com/> (`104.25.248.21` et `104.25.249.21` aujourd'hui). Les résolveurs (on dit aussi serveurs récursifs, ou bien serveurs caches), eux, ne connaissent rien, à part l'adresse des serveurs de la racine, où ils commencent leurs interrogations. Les serveurs faisant autorité sont gérés par des hébergeurs DNS spécialisés (comme Dyn <https://www.nextinpact.com/news/101871-dyn-on-fait-point-sur-attaque-ddos-qui-a-impactee-nombreux-sites.htm>), ou bien directement par le titulaire du nom de domaine. Les résolveurs sont typiquement gérés par le service informatique du réseau où vous vous connectez, ou bien par le FAI, pour les accès grand

1. Car trop difficile à faire afficher par LaTeX

public. Ces résolveurs sont une partie cruciale du service d'accès à l'Internet : sans DNS, il n'y a quasiment rien qui marche. S'ils sont en panne, plus d'Internet. S'ils mentent <https://www.bortzmeyer.org/dns-menteur.html>, on est détourné vers un mauvais site.

On voit depuis des années apparaître des résolveurs DNS **publics**, qui ne dépendent ni du FAI, ni du réseau local d'accès. Ce sont Google Public DNS <https://www.bortzmeyer.org/google-dns.html>, Cisco OpenDNS <https://www.bortzmeyer.org/opendns-non-merci.html>, FDN <https://www.fdn.fr/actions/dns/>, OpenNIC <https://www.opennicproject.org/>, Verisign <https://www.verisign.com/fr_FR/security-services/public-dns/index.xhtml>, Yandex <https://dns.yandex.com/>, etc. Attention à ne pas confondre ces résolveurs **publics** avec ce qu'on nomme les résolveurs **ouverts**. Tous ont en commun qu'ils acceptent de répondre à des requêtes DNS, quelle que soit leur source. Mais les résolveurs ouverts le sont par accident, par erreur de configuration, et ne sont pas gérés. Les résolveurs publics, eux, le sont déliberement, ils sont (normalement...) gérés par des gens sérieux. La différence est importante car un résolveur ouvert est un outil utile dans de nombreuses attaques comme les attaques par amplification <https://www.bortzmeyer.org/jres-dos-2013.html> ou comme certains empoisonnements <https://www.bortzmeyer.org/dns-attaques-shulman.html>. C'est pour cette raison que le RFC 5358 [2] demande que les résolveurs DNS ne soient pas ouverts.

Après ce long préambule, retour aux pannes de résolveurs DNS. Aujourd'hui, dès qu'un problème Internet survient, et quelle que soit la cause réelle du problème, la réponse fuse sur tous les rézosocios : « utilise Google DNS » (ou bien, version libriste, « utilise FDN »). Un exemple, pris au hasard lors de la dernière panne Free est ce tweet <https://twitter.com/Ybalrid/status/819547603633373184>. (Et voici une documentation plus élaborée <https://www.degroupnews.com/internet/tutoriel-panne-de

Ce genre de conseils ne tient pas compte de plusieurs inconvénients sérieux des résolveurs publics. Je vais commencer par les inconvénients communs à **tous** les résolveurs publics. Le principal est que le lien entre vous et le résolveur public est long et non sécurisé. Même si vous avez une confiance aveugle dans le résolveur public et ceux qui le gèrent, sur le trajet, des tas de choses peuvent aller mal. D'abord, le trafic peut être écouté trivialement (les seuls résolveurs publics qui proposent une solution à ce problème sont Cisco OpenDNS et OpenNIC, avec DNSCrypt). Comme le rappelle le RFC 7626, le trafic DNS est très bavard (trop), circule en clair, passe par des réseaux supplémentaires (en plus du trafic « normal »), et peut donc poser des problèmes de vie privée. Avec un résolveur DNS habituel, le problème est limité car le résolveur est proche de vous, limitant le nombre de gens qui peuvent écouter. Avec un résolveur public, le nombre d'écoutants potentiels augmente.

Mais il y a pire : la plupart des résolveurs publics n'offre aucune authentification (là encore, la seule exception est Cisco OpenDNS et OpenNIC, mais où cette authentification est facultative, et je ne sais pas combien d'utilisateurs s'en servent réellement). Même les mesures les plus triviales comme le NSID du RFC 5001 ne sont pas mises en œuvre (NSID ne fait pas une réelle authentification, mais il permet de détecter certains problèmes). Si vous utilisez des résolveurs publics pour contourner la censure, c'est un sérieux problème. Des censeurs ont déjà effectué des détournements de résolveurs DNS public (comme en Turquie <https://www.bortzmeyer.org/dns-routing-hijack-turkey.html>, mais aussi dans d'autres pays <http://arstechnica.com/information-technology/2014/03/google-dns-briefl>). Donc, même si le résolveur public est géré par des gens biens, et que vous connaissez, **cela ne suffit pas**, car vous n'avez aucun moyen de savoir si vous parlez bien à ce résolveur, et pas à un usurpateur (le DNS utilise UDP, qui n'offre aucune protection contre l'usurpation d'adresse <https://www.bortzmeyer.org/usurpation-adresse-ip.html>).

2. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc5358.txt

Il est amusant (et révélateur du manque de connaissances sur le fonctionnement de l'Internet) que les débats sur les résolveurs ouverts se focalisent souvent sur la confiance que l'on peut accorder (ou pas) au serveur, et jamais sur celle qu'on peut accorder (ou pas) au réseau qui y mène !

Il y a aussi des inconvénients qui sont spécifiques à certains des résolveurs publics souvent recommandés :

— Je soupçonne que certains ne sont pas si bien gérés que cela (normalement, ils doivent faire de la limitation de trafic, être supervisés 24 heures sur 24, etc) et peuvent être utilisés pour des attaques par réflexion, avec amplification <https://www.bortzmeyer.org/attaques-reflexion.html>,
— Google, Cisco et Verisign sont situés aux États-Unis, pays qui n'a **aucune** protection des données personnelles, même théorique (argument bien développé chez Shaft <https://www.shaftinc.fr/arretez-google-dns.html>),
— Yandex est en Russie, si vous voulez donner vos informations au FSB plutôt qu'à la NSA,
— OpenNIC est une racine alternative <https://www.bortzmeyer.org/racines-alternatives.html>, ce qui veut dire qu'ils ajoutent des TLD « bidons <http://wiki.opennicproject.org/OpenNICNamespaces> », qui ne marcheront que chez eux,
— Certains services sont peu fiables, souvent en panne, très lents, ou disparaissant sans laisser de nouvelles.

Alors, si utiliser les résolveurs publics est une mauvaise idée, quelle est la bonne ? Le mieux serait évidemment de pouvoir utiliser les résolveurs DNS de son FAI. Un résolveur DNS correct fait partie (ou devrait faire partie) de l'offre Internet de base. Les utilisateurs devraient réclamer un tel service, fiable et rapide. Les pannes récentes, ou bien les horreurs des résolveurs DNS des points d'accès Wi-Fi des hôtels et des aéroports, et enfin le problème de la censure étatique (qu'un service de qualité chez le FAI ne résoudra pas) font qu'il n'y a plus guère le choix, il faut utiliser d'autres résolveurs que ceux du FAI. La solution la plus propre est d'avoir son propre résolveur DNS <https://www.bortzmeyer.org/son-propre-resolveur-dns.html>, pas forcément sur chaque machine de son réseau local, mais plutôt dans une machine unique, typiquement le routeur d'accès. Avant qu'on ne me dise « mais ce n'est pas Michu-compatible, M. Michu ne vas quand même pas installer OpenBSD sur un Raspberry Pi pour avoir un résolveur sur son réseau », je dis tout de suite qu'évidemment, cela ne doit pas être fait directement par M. Michu mais une fois pour toutes dans un paquet logiciel et/ou matériel qu'il n'y a plus qu'à brancher. (Un truc du genre de la Brique Internet <https://labriqueinter.net/>.)

Parfois, il est difficile ou peu pratique d'avoir son propre résolveur. En outre, un résolveur à soi sur le réseau local protège bien contre la censure, ou contre les pannes, mais peu contre la surveillance, puisqu'il va lui-même émettre des requêtes en clair aux serveurs faisant autorité. Il est donc utile d'avoir des résolveurs publics accessibles en DNS-sur-TLS (RFC 7858), ce qui protège la confidentialité et permet l'authentification du résolveur. Ces résolveurs publics (comme par exemple celui de LDN <https://ldn-fai.net/serveur-dns-recursif-ouvert/> ou bien celui de Yeti <https://www.afnic.fr/fr/ressources/blog/resolveur-public-de-dns-sur-tls-yeti.html>) peuvent être utilisés directement, ou bien servir de relais pour le résolveur local. Attention, la plupart sont encore très expérimentaux. Vous trouverez une liste sur le portail DNS Privacy <https://portal.sinodun.com/wiki/display/TDNS/DNS-over-TLS+test+servers>. (Pour la solution non normalisée DNScrypt, on trouve, outre le site Web officiel, la doc de malekalmorte <http://www.malekal.com/simple-dnscrypt-dns-securises/> ou bien celle-ci <https://computersecuritypgp.blogspot.fr/2016/03/what-is-dnscrypt.html>.)

Pour se prémunir contre la censure (mais pas contre les pannes, ni contre la surveillance), une autre technologie utile est DNSSEC. Le résolveur local doit donc valider avec DNSSEC. Notez que, malheureusement, peu de domaines sont signés.

La meilleure solution est donc un résolveur DNS validant avec DNSSEC et tournant sur une machine du réseau local (la « *"box"* » est l'endroit idéal). Cela assure un résolveur non-menteur et sécurisé. Si on

veut en plus de la vie privée, il faut lui faire suivre les requêtes non-résolues à un résolveur public de confiance (donc pas Google ou Verisign) et accessible par un canal chiffré (DNS sur TLS).

Si votre "*box*" est fermée et ne permet pas ce genre de manips, remplacez-la par un engin ouvert, libre et tout ça, comme le Turris Omnia <https://www.bortzmeyer.org/turris.html> qui a par défaut un résolveur DNSSEC.

---

https://www.bortzmeyer.org/dns-resolveurs-publics.html