

OpenDNS, surtout pas

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 17 Septembre 2009. Dernière mise à jour le 4
Décembre 2009

<http://www.bortzmeyer.org/opensdns-non-merci.html>

Quand survient un problème avec les résolveurs DNS d'un FAI, la réponse courante dans les forums bas de gamme est « il faut utiliser les résolveurs d'OpenDNS ».

Un exemple courant de problème est lorsque le FAI déploie des DNS menteurs (<http://www.bortzmeyer.org/dns-menteur.html>) pour diriger ses utilisateurs vers des sites Web de publicité. Par exemple, lorsque SFR a rétabli ses DNS menteurs en août 2009, des tas de blogueurs ont conseillé sur leur site d'utiliser OpenDNS. Même chose lorsqu'une faille de sécurité touchant au DNS est publiée (par exemple lors de l'attaque contre Eircom (<http://news.softpedia.com/news/Possible-DNS-Hack-at-Ireland-shtml>)).

Dans le premier cas, l'idée est particulièrement tordue : les résolveurs d'OpenDNS sont également des menteurs ! On peut le voir facilement soi-même, ici avec dig :

```
% dig @208.67.222.222 A nexistepas.bortzmeyer.org
...
;; ANSWER SECTION:
nexistepas.bortzmeyer.org. 0      IN      A       67.215.65.132
...
```

Bien que `bortzmeyer.org` existe et ne leur appartienne pas, OpenDNS n'hésite pas à mentir en dirigeant `nexistepas.bortzmeyer.org` vers une de leurs adresses IP.

Donc, utiliser OpenDNS pour échapper aux résolveurs menteurs de son FAI, c'est comme plonger dans le lac lorsqu'il pleut, pour éviter d'être mouillé. Le seul avantage, c'est qu'on est mouillé volontairement... (Je plaisante mais j'ai vu l'argument « Oui, mais OpenDNS, on n'est pas obligé de l'utiliser ». Justement, puisqu'on n'est pas obligé, ne l'utilisons pas.)

À noter que ces mécanismes de mensonge sur les réponses DNS sont débrayables si on se crée un compte (gratuit) chez OpenDNS avant d'indiquer ses adresses IP et de décocher la case « Je veux des mensonges » (qui est cochée par défaut).

La publicité d'OpenDNS repose sur plusieurs arguments, la plupart fallacieux. Un des plus courants est la vitesse. Cet argument est très souvent répété sur les forums, par des gens qui n'ont jamais mesuré eux-même (<http://www.bortzmeyer.org/mesurer-temps-execution.html>), et n'est pas très différent de tous les arguments marketing « X est plus rapide que Y », argument qui ne s'impose que par la répétition. Si tout le monde le dit, c'est que ça doit être vrai, non ? Eh bien non, si on mesure soi-même (<http://www.bortzmeyer.org/performances-serveur-dns.html>) au lieu de répéter ce que disent les moutons, on s'aperçoit qu'OpenDNS est toujours plus lent que les serveurs DNS de votre réseau local ou de votre FAI. Comme le note seizurebattlerobot lors d'une discussion (<http://yro.slashdot.org/article.pl?sid=09/07/09/1811249>) sur Slashdot, c'est logique, « *"Despite their claims to the contrary, OpenDNS's servers are likely farther away from you than your local ISP's."* ».

D'autre part, OpenDNS affirme protéger l'utilisateur de la pornographie et du "malware" malware en mentant sur les réponses DNS, même lorsque le nom de domaine existe.

Enfin, il y a ce qu'OpenDNS ne dit pas : puisque l'usage de leurs résolveurs est gratuit, quel est leur modèle d'affaires ? Simplement vendre l'information qu'ils ont récolté sur vous. Comme le note encore seizurebattlerobot sur Slashdot, en juillet 2009 : « *"They also keep permanent logs of all queries, which could be subpoenaed by a government entity. Their joke of a privacy policy allows them to sell your logs to "Affiliated Businesses", which pretty much means anybody. Not that it really matters - they could amend their privacy policy tomorrow morning and be selling your info by the afternoon."* subpoenaed ». Un résolveur DNS reçoit énormément d'informations sur ce que font ses clients (et je sais de quoi je parle, grâce à des systèmes comme DNSmezzo (<http://www.dnsmezzo.net/>)).

Donc, pour l'utilisateur typique, il n'existe aucune raison valable d'utiliser OpenDNS. Y a t-il des cas où on n'a pas le choix ? Sur certains réseaux (par exemple chez beaucoup de FAI africains, sur un "hotspot" hotspot mal géré, dans beaucoup d'hôtels), les serveurs DNS sont souvent en panne ou très lents. Si on est coincé sur un tel réseau, on a bien besoin de résolveurs DNS quand même. Autrefois, tous les résolveurs DNS étaient ouverts à tous et il suffisait d'en prendre un au hasard. Aujourd'hui, pour diverses raisons (voir par exemple le RFC 5358¹), de tels serveurs récursifs ouverts sont de plus en plus rares et ceux qui restent ne sont pas forcément dignes de confiance. Une des solutions est de les utiliser quand même, et d'être prêt à changer lorsqu'ils tombent en panne ou bien se sécurisent.

Une autre solution est d'avoir un résolveur DNS local sur sa machine ou son réseau. Cela peut sembler une solution très "geek" geek mais c'est plus simple que ça n'en a l'air. Sur Debian ou Ubuntu, un simple `aptitude install unbound` et le résolveur Unbound est prêt à l'emploi (il faut modifier `/etc/resolv.conf` pour indiquer comme serveur de noms `127.0.0.1`, la machine locale, ou bien changer les réglages DHCP si c'est possible). Unbound est probablement plus sûr que BIND car moins chargé en fonctions. Mais, bien sûr, on peut utiliser BIND aussi. Pour les amateurs de MS-Windows, Gils Gayraud me recommande TreeWalk (<http://www.ntcanuck.com/>).

Certaines personnes peuvent s'inquiéter à cette idée d'un résolveur sur chaque machine (ou en tout cas sur chaque petit réseau), en raison de la charge supplémentaire que cela imposera aux serveurs de la racine ainsi qu'à ceux des domaines de tête. Sans le partage des informations dans les grands caches des résolveurs DNS des FAI, les serveurs de la racine tiendront-ils le coup ? C'est en raison de cette

1. Pour voir le RFC de numéro NNN, <http://www.ietf.org/rfc/rfcNNN.txt>, par exemple <http://www.ietf.org/rfc/rfc5358.txt>

question que je ne conseille pas d'installer son résolveur à soi sans une bonne raison. Dans le futur, il est possible qu'on n'ait plus le choix, si on veut un service DNS correct. Et, à ce moment, on verra bien. Lors de réunions d'experts comme à l'OARC (<http://www.dns-oarc.net/>), les opérateurs des serveurs racine ont toujours déclaré qu'ils n'étaient pas inquiets sur ce point.

Reste le cas des documentations dont l'auteur ne sait pas sur quel réseau tournera la machine et où il préfère indiquer les serveurs d'OpenDNS pour permettre un copier-coller des instructions (voir par exemple http://wiki.openmoko.org/wiki/Android_usage). Une meilleure solution serait de recommander d'utiliser DHCP, pour récupérer les serveurs du réseau local.

La dernière solution est d'utiliser un concurrent d'OpenDNS. La plupart utilisent les mêmes méthodes et ont des résolveurs tout aussi menteurs. C'est le cas de Comodo (<http://www.comodo.com/secure-dns/>), de Scrubit (<http://www.scrubit.com/>) ou de Neustar/Advantage (<http://www.dnsadvantage.com/>). À défaut de tout, les utiliser permet d'éviter la constitution d'un monopole d'OpenDNS. Mais il existe aujourd'hui un service de résolveur ouvert honnête, c'est Google DNS (<http://www.bortzmeyer.org/google-dns.html>) et c'est donc une possibilité intéressante. Pour une liste plus complète (trop complète, on y trouve de tout mais, heureusement, avec tous les détails pratiques), voir l'excellent `resolv.conf` de Chris Hills.

Je laisse la conclusion à, à nouveau, seizurebattlerobot : *« "I think many people read the "Open" part of the OpenDNS name and turn their brains off." »*