Changer de serveur résolveur DNS facilement

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 8 janvier 2012. Dernière mise à jour le 9 janvier 2012

https://www.bortzmeyer.org/changer-dns.html

La sortie, le 30 décembre 2011, du décret n° 2011-2122 relatif aux modalités d'arrêt de l'accès à une activité d'offre de paris ou de jeux d'argent et de hasard en ligne non autorisée <http://legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000025062583&fastPos=1&fastReqId=1801775252&categorieLien=id>, décret qui permet à l'ARJEL <https://www.bortzmeyer.org/arjel.html> de demander le blocage d'un site de paris ou de jeux en ligne, a ramené sur le devant de la scène la question du blocage via le DNS. En effet, le décret dit explicitement « Lorsque l'arrêt de l'accès à une offre de paris ou de jeux d'argent et de hasard en ligne non autorisée a été ordonné, [...] les [FAI] procèdent à cet arrêt en utilisant le protocole de blocage [sic] par nom de domaine (DNS) ». Il existe plusieurs façons de comprendre cette phrase. Si le FAI décide de mettre en œuvre cet arrêt en configurant ses résolveurs DNS <https://www.bortzmeyer.org/resolveur-dns.html> pour mentir, un moyen simple de contourner cette censure sera alors pour les utilisateurs de changer de résolveur DNS. Est-ce simple ? Est-ce réaliste ? Des logiciels peuvent-ils aider ?

D'abord, un petit rappel de vocabulaire, car j'ai déjà lu pas mal d'articles sur le sujet, où l'auteur est plein de bonne volonté et veut vraiment aider les autres à contourner la censure, mais où il ne connait pas vraiment le DNS et où il utilise un vocabulaire approximatif, voire complètement faux. Il y a **deux** sortes de serveurs DNS : la première, ce sont les **serveurs faisant autorité <https://www.bortzmeyer.org/serveur-dns-faisant-autorite.html>**, qui sont ceux qui contiennent les données (par exemple, les serveurs de DENIC ont la liste de tous les noms de domaine en `.de`, des serveurs de la société NS14 font autorité pour le domaine `shr-project.org`, etc). L'ARJEL ou un autre censeur ne peut pas toujours agir sur eux car ils peuvent être situés en dehors de la juridiction française.

Et il y a les **résolveurs DNS <https://www.bortzmeyer.org/resolveur-dns.html>**. Ils ne connaissent au démarrage aucune donnée et servent uniquement de **relais** et de **caches** (stockage temporaire de données). Ils sont typiquement gérés par votre FAI ou bien par le service informatique de votre boîte. Ce sont eux qui sont indiqués à la machine cliente (en général par le protocole DHCP), qui les utilisera à chaque fois qu'elle aura une question (c'est-à-dire pas moins d'une centaine de fois pour la seule page d'accueil de CNN).

Si on veut censurer en France l'accès à un site de jeu en ligne, par le protocole DNS, c'est un bon endroit pour attaquer. Il en existe d'autres, mais que je garde pour d'autres articles. Modifier le comportement du résolveur est facile (les logiciels ont déjà ce qu'il faut pour cela <https://www.bortzmeyer.org/rpz-faire-mentir-resolveur-dns.html>) et certains FAI le faisaient déjà pour des raisons financières <https://www.bortzmeyer.org/dns-menteur.html>.

Mais c'est aussi une technique de censure relativement facile à contourner : l'utilisateur de la machine cliente peut changer la configuration de son système pour utiliser d'autres résolveurs que ceux de son FAI, par exemple ceux de Telecomix <http://dns.telecomix.org/>, qui promettent de ne pas censurer. C'est cette technique qui est discutée dans cet article.

Si vous lisez les forums un peu au hasard, vous trouverez souvent des allusions à cette méthode, de la part de "*geeks*" vantards qui affirment bien haut « rien à foutre de leur censure à la con, je change mon DNS car je suis un top-eXpeRz et je surfe sans filtrage ». La réalité est plus complexe. Prenons l'exemple d'une machine Ubuntu (il y a peu près les mêmes problèmes sur Windows ou Mac OS X). La liste des résolveurs DNS utilisés figure dans le fichier `/etc/resolv.conf`. Suffit-il d'éditer ce fichier, comme on le lit souvent (et bien à tort) ?

— Déjà, il faut rappeler au frimeur de forum que la grande majorité des utilisateurs de l'Internet n'ont même pas idée qu'ils peuvent choisir (et je ne parle pas seulement du résolveur DNS, mais aussi du navigateur, du système d'exploitation, etc). Si on veut que la solution soit accessible à tout le monde, pas seulement à quelques "*geeks*" auto-proclamés, elle doit être **simple**.
— Même sur Ubuntu, tout le monde ne sait pas éditer un fichier système (surtout qu'il faut être root).
— Le frimeur à grande gueule qui écrit sur `forum.blaireaux.com/index.php` découvrira vite, s'il essayait ce qu'il prêche, qu'éditer `resolv.conf` n'est **pas** la bonne méthode, car le client DHCP effacera ses modifications à la prochaine connexion. Il faut modifier la configuration dudit client DHCP (cela varie énormément selon le système et le logiciel installé ; sur ma Debian, en ce moment, c'est `/etc/resolvconf/resolv.conf.d/head`).
— Sur certains systèmes d'exploitation, changer un réglage aussi banal est très difficile. Par exemple, sur Android (merci à Aissen pour les informations), les serveurs DNS utilisés sur le réseau mobile ne sont pas modifiables et, sur le Wi-Fi, on ne peut les changer que si on coupe DHCP. Comme la publicité fait tout son possible pour migrer les utilisateurs vers les accès Internet sur téléphone mobile, bien plus contrôlés et moins libres, l'avenir est inquiétant.
— Une fois qu'on sait quel fichier éditer et comment, reste la question, que mettre dans ce fichier ? Il existe plusieurs résolveurs publics situés en dehors du pouvoir de l'ARJEL, et le plus souvent cité est OpenDNS. Intéressant paradoxe : pour échapper à la censure et garder sa liberté de citoyen, on utilise un résolveur menteur <https://www.bortzmeyer.org/dns-menteur.html>, qui pratique lui-même la censure (et parfois se trompe <http://www.thewhir.com/web-hosting-news/010612_Thousands_of_Sites_Mislabeled_Phishers_After_OpenDNS_Blocks_Google_Hosted_Scripts>). Utiliser OpenDNS, c'est se jeter dans le lac pour éviter d'être mouillé par la pluie. Sans compter leurs autres pratiques, comme l'exploitation des données personnelles <https://www.bortzmeyer.org/opendns-non-merci.html> (le résolveur DNS utilisé sait tout de vous... chaque page Web visitée lui envoie au moins une requête...). À noter qu'on peut avoir aussi un résolveur local à sa machine, ce point est traité un peu plus loin.

À noter que tous les cas ne peuvent pas être couverts dans un article. Par exemple, on peut aussi envisager de changer les réglages DNS sur la "*box*" si elle sert de relais DNS pour le réseau local vers les « vrais » résolveurs.

Pour résoudre tous ces problèmes, on peut écrire des documentations (exemples à la fin de cet article). Mais la plupart des utilisateurs auront du mal à les suivre et je pense donc que la bonne solution est la disponibiité d'un logiciel qui automatise tout cela. Quel serait le cahier des charges d'un tel logiciel ?

- Tourne sur les systèmes utilisés par M. Toutlemonde (Windows, Android, Ubuntu, etc).
- Indépendant de l'application (le DNS ne sert pas que pour le Web) et marche donc avec tous les services (c'est pourquoi je n'ai pas discuté dans cet article des extensions Firefox comme MAFIAAFire <https://addons.mozilla.org/en-US/firefox/addon/mafiaafire-piratebay-dancing/> ou DeSOPA <https://addons.mozilla.org/en-US/firefox/addon/desopa/> - ce dernier ayant en outre un mode de fonctionnement très bizarre).
- Simple à utiliser.
- Vient avec une liste pré-définie de bons résolveurs. Je préférerais que cette liste n'inclue pas les résolveurs menteurs comme ceux d'OpenDNS. En tout cas, il est impératif qu'on puisse ajouter les résolveurs de son choix.
- M. Toutlemonde va certainement avoir des problèmes pour décider s'il doit se servir de « Telecomix » ou « Comodo » ou « Level-3 » pour ne citer que quelque uns des résolveurs publics les plus fameux. Il faudrait donc que le logiciel teste ces résolveurs automatiquement, pour leurs performances, bien sûr (la plupart des articles trouvés sur le Web sur le thème « comment choisir son résolveur DNS ? » ne prennent en compte que leur vitesse, pas leur sincérité, contrairement à cet article) mais aussi pour leur obéissance à la censure. Le logiciel devrait venir avec une liste de domaines peut-être censurés (`wikileaks.org`, etc) et tester les réponses des résolveurs candidats. Ce n'est pas facile à faire car il faut aussi connaître les bonnes réponses, et elles peuvent changer. Peut-être le logiciel devrait-il interroger des résolveurs de confiance pour avoir cette information ? Le fait de tester pourrait même permettre de choisir automatiquement un résolveur, ce qui serait certainement meilleur pour M. Toutlemonde.
- Autre cas vicieux (merci à Mathieu Goessens), celui des résolveurs DNS qui, en violation des bonnes pratiques, contiennent des données spécifiques qu'on ne trouve pas dans le DNS public. C'est le cas de pas mal de portails captifs de "*hotspots*", par exemple. dnssec-trigger <https://www.bortzmeyer.org/dnssec-trigger.html> gère ce problème en ayant un mode spécial, manuellement activé, « "*Hotspot sign-on*" ». Mais il y a pire : certains FAI (notamment Orange) utilisent des données non publiques pour certains services réservés aux clients (VoIP, serveur SMTP de soumission, etc) donc une solution qui gère la connexion initiale ne suffit pas. La seule solution dans ce cas est d'avoir un mécanisme d'aiguillage qui envoie les requêtes pour certains domaines à certains résolveurs.

Un tel logiciel est vulnérable à un blocage du port 53 <https://www.bortzmeyer.org/port53-filtre.html>. Si cette mesure se répand, il faudra aussi que le logiciel teste s'il peut atteindre des résolveurs publics et des serveurs faisant autorité, ou bien s'il faut passer à d'autres méthodes comme de tunneler le DNS sur TLS, port 443, comme le permet déjà Unbound, dans sa version de développement. D'autres attaques suivront alors (par exemple des FAI qui annonceront les adresses `8.8.8.8` et `8.8.4.4` sur leur propre réseau, pour se faire passer pour Google Public DNS <https://www.bortzmeyer.org/google-dns.html>, profitant du fait que ce service n'est pas authentifié).

Compte-tenu de ce cahier des charges, quels sont les logiciels qui conviennent aujourd'hui ? Il n'en existe aparemment qu'un seul, DNS Jumper <http://www.sordum.com/?p=4573> (je ne suis pas sûr d'avoir mis un lien vers le site officiel, ce logiciel n'a pas de références bien précises et, son source n'étant pas distribué, on peut être inquiet de ce qu'il fait). DNS Jumper tourne sur Windows, assure les quatre premières fonctions de mon cahier des charges mais pas l'avant-dernière : il ne vérifie pas que le résolveur est digne de confiance. Il est décrit, par exemple, dans « "*Easily Switch Between 16 DNS Servers with DNS Jumper*" <http://mytechquest.com/internet/easily-switch-between-16-dns-servers-with-d> » (l'article est un peu ancien, le logiciel s'est perfectionné depuis), ou, en français, dans « DNS Jumper - Changez rapidement de serveurs DNS <http://korben.info/outil-changer-dns.html> ».

Les autres logiciels restent à écrire (un truc comme DNS Helper ne compte pas, puisqu'il ne permet de changer... que pour les DNS de Google). Mais que les censeurs ne se réjouissent pas, les logiciels vont vite sortir, écrire un tel programme n'est pas un exploit technique, et la demande est forte, avec le décret ARJEL déja cité pour la France, SOPA pour les États-Unis, etc.

Sur le problème général de changer manuellement ses résolveurs DNS, un bon article est « "*How to Change DNS Server*" <http://www.techsupportalert.com/content/how-change-dns-server.

htm> » de Remah (Windows seulement). Pour Mac OS, un bon article est « "*Disabling DNS servers from DHCP*" <http://qmail.jms1.net/djbdns/osx.shtml#dhcp-nameserver> ».

Quelques petits détails techniques pour finir : on peut parfaitement installer un serveur DNS résolveur sur sa propre machine (enfin, sur un ordinateur portable, pas sur un "*smartphone*"). La résolution DNS sera alors entièrement sous le contrôle d'un logiciel qu'on gère, fournissant ainsi le maximum de sécurité. Le processus n'est pas très compliqué sur Unix, ni même sur Windows <http://petitteckel.wordpress.com/2006/12/09/installation-de-bind-sous-windows-xp/> (merci à Gils Gayraud et Mathieu Bouchonnet pour leur aide sur Windows). On peut le rendre encore plus simple avec des logiciels astucieux comme dnssec-trigger <https://www.bortzmeyer.org/dnssec-trigger.html>, qui ne teste pas la censure (son but est tout autre) mais pourrait servir de point de départ à un paquetage simple d'installation, vraiment utilisable par M. Toutlemonde (ce n'est pas encore le cas). Par contre, un tel résolveur local a des conséquences négatives sur l'infrastructure du DNS : comme il n'y a plus de cache partagé (avec le résolveur/cache du FAI, une requête pour www.bortzmeyer.org reste en mémoire et bénéficie à **tous** les clients du FAI), les serveurs faisant autorité verront leur charge s'accroître.

Pour éviter cet inconvénient, une des solutions serait pour le résolveur local de faire suivre les requêtes aux résolveurs du FAI (de tels résolveurs sont nommés "*forwarders*"). Mais cela implique de détecter lorsque le résolveur du FAI ment, pour le court-circuiter dans ce cas. DNSSEC fournit une piste intéressante pour cela mais, début 2012, les résolveurs ayant cette fonction "*forwarder*" (BIND et Unbound) n'ont pas de tel service de détection et de contournement.

Pire encore, on peut combiner le résolveur local (ou le remplacer) avec des fichiers statiques locaux (/etc/hosts sur Unix, C:\WINDOWS\system32\drivers\etc\hosts sur Windows) mais la maintenance de tels fichiers serait un cauchemar.

Cela ne veut pas dire que cela n'arrivera pas : dans ce maelstrom d'attaques et de contre-attaques, les solutions les plus mauvaises seront certainement déployées par certains acteurs et le futur est sombre pour le système de résolution de noms <https://www.bortzmeyer.org/resolution-de-demain.html>.