Filtrage du port 53, la prochaine attaque contre la neutralité du réseau

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 29 juin 2010. Dernière mise à jour le 17 septembre 2010

http://www.bortzmeyer.org/port53-filtre.html

Il n'y a plus guère aujourd'hui de vrai FAI pour le particulier ou la petite entreprise, c'est-à-dire de fournisseur qui donnerait accès à l'Internet, pas seulement à un sous-ensemble de celui-ci (par exemple le Web). Ainsi, le filtrage du port 25 en sortie (le port utilisé par le protocole SMTP d'envoi du courrier) est souvent bloqué par défaut, en raison de l'importante quantité de spam envoyé par des zombies. Et le port **53**, celui du DNS ?

Il y a bien d'autres violations de la neutralité du réseau par les FAI (cf. RFC 4924 [1]). Parfois, d'autres services que le courrier sont interdits (la palme du ridicule à OVH pour son offre d'hébergement <http://www.ovh.com/fr/cloud/> où IRC est interdit - apparemment XMPP ou les protocoles de messagerie instantanée fermés ont été oubliés par le juriste d'OVH). Parfois, le client peut ouvrir les ports fermés, le filtrage n'étant que mis par défaut, mais débrayable (c'est le cas, à l'heure actuelle, chez Free avec le port 25, automatiquement et gratuitement).

Jusqu'à présent, l'accès DNS, qui se fait sur le port 53, a toujours été ouvert. Cela risque de changer bientôt. Il y a eu plusieurs alertes (donc certaines se sont révélées être de fausses alertes) comme chez Comcast <http://comcastisfuckingwithyourport53traffic.wordpress.com/> (voir aussi la discussion sur Slashdot <http://tech.slashdot.org/story/09/06/09/1731238/Comcast-Intercepts-and
et il est probable qu'un FAI tentera bientôt de généraliser ce filtrage.

En effet, un document du MAAWG publié en juin 2010, « "*Overview of DNS security - Port 53 protection*" <http://www.maawg.org/sites/maawg/files/news/MAAWG_DNS%20Port%2053V1.0_2010-06.pdf> » prône ce filtrage. La caution du MAAWG, cartel de gros opérateurs réseau, sera sans doute utilisé comme prétexte. Par contre, pour le client, c'est une mauvaise nouvelle : le MAAWG s'est déjà

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc4924.txt

signalé par ses positions éradicatrices, considérant que le citoyen n'a pas à avoir un accès complet à l'Internet et qu'il faut le forcer à passer par les filtres du fournisseur d'accès. Par exemple, pour le courrier, le MAAWG a toujours prôné, comme approche anti-spam, l'acceptation du courrier uniquement entre gros opérateurs, excluant la réception du courrier envoyé par les serveurs des petits fournisseurs, petites entreprises ou particuliers.

Le titre du rapport du MAAWG est déjà un chef d'œuvre de novlangue, comme de parler de « managing traffic on port 53 » pour dire « interdiction du port 53 ».

Quels sont les arguments du MAAWG ? Que plusieurs logiciels malveillants changent les réglages DNS des machines infectées, pour pointer vers des serveurs DNS contrôlés directement ou indirectement (via un empoisonnement de cache) par un méchant. Bloquer le port 53 forcerait les machines Windows infectées à passer par les résolveurs DNS du FAI, gênant ainsi le logiciel malveillant.

De telles attaques arrivent dans la nature et sont par exemple documentées dans l'article « "*Corrupted DNS Resolution Paths : The Rise of a Malicious Resolution Authority* " <http://www.citi.umich.edu/u/provos/papers/ndss08_dns.pdf> ». L'attaquant, via un logiciel malveillant, change les réglages DNS et le PC de l'utilisateur, sans que ce dernier s'en rende compte, envoie désormais ses requêtes DNS à un résolveur géré par le méchant (ou empoisonné par celui-ci). Ce résolveur peut alors, par exemple, indiquer une fausse adresse IP pour `www.ma-banque.example`. Ainsi, l'utilisateur, sans qu'il y aie eu besoin d'envoyer du spam prétendument depuis sa banque, peut être dirigé vers un serveur de hameçonnage.

Bien conscient de la restriction de la liberté de choix qui résulte de l'interdiction proposée, le MAAWG propose des exceptions vers les serveurs DNS « bien connus » ("*legitimate DNS resolvers*", sans que cette « légitimité » soit définie). On suppose que cela inclus ceux d'OpenDNS <http://www.bortzmeyer.org/opendns-non-merci.html> (qui se vante de censurer pour « protéger la famille » <http://www.pcmag.com/article2/0,2817,2365554,00.asp>) ou de Norton DNS qui affirme mentir sur les réponses DNS pour empêcher l'utilisateur d'aller sur des sites Web dangereux. Est-ce que cela inclura aussi les serveurs de Google DNS <http://www.bortzmeyer.org/google-dns.html>, pour lesquels Google s'est engagé à ne pas interférer avec les réponses légitimes ? En tout cas, cette idée d'une « liste blanche » de serveurs officiels est bien dans l'esprit du MAAWG, qui verrait bien l'accès Internet réduit à passer par un petit nombre de fournisseurs. En revanche, le rapport du MAAWG ne mentionne pas une seule fois la possibilité d'"*opt-out*" pour le client.

En quoi est-ce un problème de ne pas avoir accès au port 53 ? D'abord, il faut préciser que c'est une restriction du choix : le FAI détermine ce qui est bon pour le client, au lieu de laisser celui-ci se déterminer tout seul. Ensuite, d'un point de vue plus pratique, bloquer le port 53 peut empêcher le client de chercher ailleurs une solution aux dysfonctionnements des résolveurs DNS du FAI, ou à leurs insuffisances (par exemple, chez Free, la moitié des résolveurs ne gère toujours pas EDNS). C'est d'autant plus grave que les défaillances peuvent être volontaires, comme dans le cas des DNS menteurs <http://www.bortzmeyer.org/dns-menteur.html> où le FAI trompe délibérement ses clients. Le rapport du MAAWG mentionne d'ailleurs cette question de manière fort elliptique en indiquant que le blocage du port 53 permet de préserver les revenus provenant de l'exploitation du DNS... (En termes clairs : la publicité sur le site Web vers lequel on redirige les clients.)

Un autre problème du blocage du port 53 concerne DNSSEC. Tant que les résolveurs des FAI ne font pas de validation DNSSEC, la seule solution pour celui qui veut utiliser cette technique de sécurité chez lui est d'installer son propre résolveur <http://www.bortzmeyer.org/ou-valider-dnsssec.html> (ce qui est très simple aujourd'hui) validant. Le blocage du port 53 empêcherait cela et gênerait donc le déploiement d'une méthode de sécurité intéressante.

À noter que le blocage du port 53 empêcherait immédiatement la technique la plus utilisée aujourd'hui pour contourner les portails captifs de tant d'aéroports et hôtels : le tunnel DNS <http://thomer.com/howtos/nstx.html>. Le rapport du MAAWG ne cite pas ce point, sans doute parce qu'il rendrait leurs intentions répressives trop voyantes mais cela a dû compter dans cette recommandation.

Comment savoir si son FAI bloque déjà le port 53 ? Lui demander ne donne jamais aucun résultat (essayez : appelez le support de votre FAI). Lire les CGV a peu de chances de vous apporter des explications claires. Il vaut donc mieux tester. Si, sur une machine Unix, vous pouvez utiliser dig :

```
% dig @a.nic.fr A www.wikipedia.fr
```

et récupérer la bonne valeur (une redirection vers les serveurs du domaine de Wikipédia) :

```
...
;; AUTHORITY SECTION:
wikipedia.fr.           172800  IN      NS      c.dns.gandi.net.
wikipedia.fr.           172800  IN      NS      a.dns.gandi.net.
wikipedia.fr.           172800  IN      NS      b.dns.gandi.net.
...
```

c'est que vous avez un accès au port 53 : vous pouvez interroger directement les serveurs faisant autorité. Vous pouvez aussi tester d'autres TLD que `.fr`, bien sûr.

Parfois, le filtrage dépend du contenu. Ainsi, en Chine, les requêtes DNS sont souvent modifiées <http://www.bortzmeyer.org/detournement-racine-pekin.html> par la censure et il faut donc tester, non seulement avec `www.wikipedia.fr` mais également avec des noms sensibles (en Chine, `facebook.com` ou `twitter.com`). Même si vous avez l'impression que vous parlez directement au serveur DNS (option `@` de dig), des équipements intermédiaires sur le réseau modifient vos réponses.

Si vous n'avez pas dig, vous pouvez aussi utiliser le service <http://netalyzr.icsi.berkeley.edu/faq.html#nolaunch> (il nécessite Java).

Si le FAI filtre le port 53, y a t-il des solutions de contournement ? On peut imaginer, par exemple (voir l'article de Spyou <http://blog.spyou.org/wordpress-mu/2010/09/17/comment-censurer-internet/>) un serveur DNS interne qui parle à un serveur externe sur un autre port que le 53. Avec un récurseur comme Unbound, une configuration comme cela fonctionnerait pour le serveur interne, l'externe écoutant sur le port 443 (qui a peu de chances d'être filtré) :

```
forward-zone:
  name: "."
  forward-addr: 192.0.2.73@443
```

Le serveur externe, toujours si c'est un Unbound, a juste besoin de :

```
server:
    interface: 192.0.2.73@443
```

pour écouter sur le port 443 en sus de ses ports habituels.
