

Le déploiement des résolveurs DNS menteurs

Stéphane Bortzmeyer

<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 16 Juillet 2009

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

L'annonce récente (<http://www.comcastvoices.com/2009/07/domain-helper-service-here-to-help-y.html>) par Comcast du début du déploiement de résolveurs DNS menteurs pour ses clients a remis sur le devant de la scène une technique que, malheureusement, beaucoup de FAI déploient. Mais, d'abord, il faut bien comprendre de quoi il s'agit.

Comme à chaque nouvelle publication, il y a de nombreux débats sur cette mesure, par exemple sur Slashdot (<http://yro.slashdot.org/story/09/07/09/1811249/Comcast-DNS-Redirection-Launched-In>) sur DSLreports (<http://www.dslreports.com/forum/r22679191-DNS-Comcast-Launches-Trial-of-Domai>) ou sur la liste NNSquad (<http://www.nnsquad.org/archives/nnsquad/msg01775.html>). Mais ces débats ne sont pas toujours bien informés et mélangent parfois plusieurs choses. D'abord, qu'est-ce qu'un résolveur DNS menteur ? L'abonné typique d'un FAI utilise les résolveurs DNS de son FAI. Il connaît leurs adresses IP via des protocoles comme DHCP. En général, à l'heure actuelle, la plupart des FAI laissent l'utilisateur libre d'utiliser d'autres résolveurs (dans le futur, cela pourrait changer, avec le blocage du port 53). Mais, évidemment, l'écrasante majorité des utilisateurs ne connaît pas le DNS et n'ose pas changer les réglages et tombe donc sur les résolveurs du FAI. Il est donc tentant pour celui-ci de violer la neutralité du réseau et d'utiliser ces résolveurs pour rabattre du trafic vers ses serveurs, par exemple pour y installer de la publicité. (Certains FAI prétendent mettre en place des DNS menteurs pour « le bien des clients » alors qu'en réalité, ils sont poussés par des intermédiaires qui leur proposent de « monétiser » l'audience du site Web ainsi pointé, comme l'a bien expliqué le directeur technique de Free (<http://www.mail-archive.com/frnog@frnog.org/msg06675.html>)). C'est le rôle du résolveur DNS menteur, qui est typiquement chargé, lorsqu'il reçoit un code NXDOMAIN ("*No Such Domain*", ce nom n'existe pas) de le remplacer par le code NOERROR et d'ajouter une adresse IP où écoute un serveur HTTP qui sert de la publicité.

Comcast n'est pas, et de loin, le seul FAI à faire cela. Aux États-Unis, RoadRunner le fait déjà (et plusieurs autres) et, en France, cela est apparemment fait par SFR. Je dis « apparemment » car, contrairement à Comcast, la plupart des FAI ne s'en vantent pas et n'annoncent jamais qu'ils procèdent à de telles manœuvres. Il est donc difficile de vérifier ces informations. Ignorant le RFC 4084¹, ils n'informent ni leurs clients, ni leurs potentiels futurs clients (essayez, avant de choisir un FAI, de connaître leur

1. Pour voir le RFC de numéro NNN, <http://www.ietf.org/rfc/rfcNNN.txt>, par exemple <http://www.ietf.org/rfc/rfc4084.txt>

politique en matière de réécriture DNS. Vous n’y arriverez pas.) Une fois que vous avez signé, vous pouvez toujours tester avec un client DNS comme dig. Si digAnexistesurementpas.bortzmeyer.org affiche autre chose que status : NXDOMAIN, c’est que votre résolveur vous ment.

Cette pratique pose de nombreux problèmes techniques et politiques. Je ne les cite pas tous ici (un bon nombre ont été déjà notés, par exemple dans le document 32 du SSAC (<http://www.icann.org/committees/security/sac032.pdf>)). Mais les principaux problèmes techniques sont :

- Cette réécriture est conçue uniquement pour un client final qui utilise un navigateur Web. Les autres protocoles, ou bien les clients HTTP non-Web (par exemple les clients REST) récupèrent des adresses qui, au mieux ne leur servent à rien, au pire les déroutent.
- Ce mensonge empêche le déploiement de toutes les techniques de sécurité du DNS de bout en bout comme DNSSEC (RFC 4033).
- Les applications qui testent si une entrée est présente dans le DNS (par exemple les listes noires DNS ou simplement les programmes de détection de liens Web morts (<http://www.bortzmeyer.org/disastrous.html>)) ne peuvent plus fonctionner.

Mais les principaux problèmes que pose cette technique sont politiques :

- Le titulaire d’un domaine en perd le contrôle puisque le résolveur menteur va prétendre que xxxxx.wikipedia.org existe, malgré le fait que le gérant de wikipedia.org ne l’ai pas créé. C’est donc un coup de force du gérant du résolveur DNS (le FAI) contre celui du domaine.
- Le fait qu’un intermédiaire technique, le FAI, se permette de modifier les données en transit par son système est une violation de la neutralité du réseau, qui en appelle d’autres. Si on abandonne le principe du « transporteur neutre », qui relaie mécaniquement les paquets de ses clients, demain, on assistera à des ingérences encore plus nettes.

Ces résolveurs DNS menteurs ont des points communs, mais aussi des grosses différences, avec les jokers que mettent certains gérants de domaines dans leur zone (comme l’avait fait Verisign dans .com en 2003). Il y a notamment une différence technique : les jokers dans un domaine respectent le protocole DNS, les résolveurs menteurs non, donc seuls les premiers sont compatibles avec DNSSEC et une différence politique, les jokers dans un domaine sont mis par le titulaire du domaine, alors que le résolveur menteur est un tiers qui se permet de modifier les domaines qui ne sont pas à lui. À tout point de vue, les jokers dans un domaine, quoique une mauvaise idée, sont donc « moins graves ». Néanmoins, il est normal de ne pas les déployer, comme s’y est engagée, par exemple, l’AFNIC (<http://www.afnic.fr/actu/nouvelles/103/1-afnic-et-les-wildcards-jokers>).

La confusion entre les deux techniques persiste trop souvent. Par exemple, le rapport 32 du SSAC (<http://www.icann.org/committees/security/sac032.pdf>), “*Preliminary Report on DNS Response Modification*” est très bien fait techniquement, comme d’habitude avec le SSAC (<http://www.icann.org/en/committees/security/>), et fait bien le tour de la question. Mais il mélange trop les jokers dans un domaine (par exemple un TLD) et le mensonge par un résolveur, un serveur de noms récursif. (Probablement pour que l’ICANN puisse exercer une pression sur les TLD en leur interdisant les jokers, comme proposé à la réunion ICANN de Sydney.)

Comcast, en annonçant son début de déploiement de résolveurs DNS menteurs, a également tenu à citer l’IETF en affirmant que sa technique avait été présentée à la dite IETF. C’est exact (document draft-livingood-dns-redirect) mais cela oublie deux choses. L’une est que n’importe qui peut présenter n’importe quoi à l’IETF, il n’y a pas de barrière à l’entrée. Si l’approbation d’un RFC, surtout sur le chemin des normes, est une affaire sérieuse, la publication d’un “*Internet-Draft*” est entièrement automatique et ne vaut donc pas approbation du document. Ensuite, le document a bien été discuté au sein du groupe de travail DNSOP (<http://tools.ietf.org/wg/dnsop>) mais il a été très largement rejeté par tous les participants (<http://www.ietf.org/mail-archive/web/dnsop/current/msg07353.html>) et a peu de chances de devenir un RFC un jour (ce qui n’empêchera pas Comcast ou les autres de continuer leurs pratiques, d’ailleurs). Au contraire, le RFC 4924 rappelle bien, dans sa section 2.5.2, que cette pratique est fortement déconseillée.

D’autres articles sur le sujet : “*Comcast Unleashes Trial DNS Redirection in Select States*” (http://www.circleid.com/posts/20090709_comcast_unleashes_trial_dns_redirection_in_select_states/) et “*Comcast Finally Launches DNS Redirection*” (<http://www.dslreports.com/shownews/Comcast-Finally-Launches-DNS-Redirection-103386>).