Comment Free bloque les pubs

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 5 janvier 2013. Dernière mise à jour le 12 février 2013

https://www.bortzmeyer.org/free-adgate.html

Beaucoup de gens se sont exprimés depuis l'annonce <http://dev.freebox.fr/blog/?p=1123> par Free de leur nouveau service de blocage des publicités (désactivé temporairement le 7 janvier, puis réactivé ensuite). La plupart se sont focalisés sur les aspects politiques ou économiques. Comme je n'ai guère trouvé de détails techniques, j'ai profité d'une connexion Free pour regarder comment cela marchait.

Attention, à l'heure actuelle (février 2013), le « service » n'est pas activé par défaut. Si on le fait, on découvre que la liste noire est actuellement vide. Donc, ces tests ne peuvent pas être reproduits dans l'immédiat. Cet article reflète donc la situation lors de la première phase, aux environs du nouvel an 2013.

D'abord, première déception, après avoir redémarré la Freebox pour mettre à jour le logiciel, je vois toujours les publicités, sur tous les sites que je regarde. Je lis alors quelques tweets (et un courrier anonyme), qui expliquent que le filtrage des publicités utilise le DNS. Ah, je comprends, j'utilise un résolveur DNS qui n'est pas celui de Free, donc je vois toujours les pubs. Testons la fonction DNS de la Freebox. Celle-ci indique aux machines du réseau local, avec le protocole DHCP (et également avec les annonces du RFC 8106 [1]), les adresses des serveurs de noms à utiliser pour résoudre un nom comme www.owni.fr en une adresse IP. On peut changer la valeur indiquée, en passant par le panneau de contrôle de la Freebox v6.

Revenons aux résolveurs officiels. Sur une machine Unix, l'examen du fichier /etc/resolv.conf nous dira ce que la Freebox v6 nous a dit :

```
% cat /etc/resolv.conf
# Generated by dhcpcd from eth0
...
nameserver 192.168.2.254
```

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc8106.txt

On a donc un résolveur, `192.168.2.254`, la Freebox elle-même. Celle-ci utilise un relais DNS, dnsmasq, qui transmet aux « vrais » résolveurs de Free (la Freebox v5 utilisait un système différent).

On va interroger ce résolveur. L'outil sérieux le plus courant pour le déboguage DNS, l'outil qui est au DNS ce que ping est au réseau, est dig. Pour changer un peu, on va se servir de son concurrent **drill**, qui fait partie de l'excellente (mais peu connue) bibliothèque ldns <`http://www.nlnetlabs.nl/projects/ldns/`>. drill n'a pas davantage particulier sur dig dans ce cas, c'est juste pour changer et pour ne pas connaître qu'un seul outil. Il fait partie du paquetage `ldns` sur Arch Linux ou `ldnsutils` sur Debian.

D'abord, demandons à ce relais/résolveur dans la Freebox l'adresse IPv4 d'une régie publicitaire bien connue, DoubleClick :

```
% drill @192.168.2.254 doubleclick.net A
...
doubleclick.net. 1411 IN A 212.27.40.246
```

Ah, on voit ici la triche. whois nous indique que `212.27.40.246` n'est **pas** une adresse de DoubleClick mais de Proxad, le réseau de Free. La Freebox abrite donc un **DNS menteur <`https://www.bortzmeyer.org/dns-menteur.html`>**. La vraie adresse de DoubleClick peut être obtenue en demandant à un résolveur honnête (ici, l'ODVR de l'OARC <`https://www.dns-oarc.net/oarc/services/odvr`>) :

```
% drill @2001:4f8:3:2bc:1::64:21 doubleclick.net A
...
doubleclick.net. 300 IN A 70.32.146.212
```

Cette fois, on obtient bien une adresse de DoubleClick (plus exactement de sa maison mère, Google).

Et que se passe-t-il lorsque le navigateur Web de M. Michu, client de Free, se connecte à cette adresse en croyant qu'il va récupérer un bandeau de pub à afficher ? Voyons avec curl :

```
% curl -v http://212.27.40.246/fcggddgdf
...
< HTTP/1.1 200 OK
< Server: nginx
< Date: Sat, 05 Jan 2013 20:17:13 GMT
< Content-Type: text/plain
< Content-Length: 0
```

Pour tous les chemins demandés (j'ai tapé `fcggddgdf` au hasard), on récupère un fichier de taille nulle, donc rien ne sera affiché. Si je teste avec un navigateur sur une machine qui utilise le résolveur indiqué par Free, je ne vois pas les pubs.

Au passage, le serveur HTTP qui sert ces fichiers vides semble être sur la Freebox elle-même :

```
% traceroute  212.27.40.246
traceroute to 212.27.40.246 (212.27.40.246), 30 hops max, 60 byte packets
 1  212.27.40.246 (212.27.40.246)  0.409 ms  0.328 ms  0.366 ms
```

Donc, résumons, la Freebox inclut un résolveur DNS menteur, qui donne, pour certains noms (ceux des grandes régies publicitaires, probablement), une réponse mensongère. Celle-ci pointe vers un serveur de fichiers vides.

Voici pour la partie technique. À part l'intérêt intellectuel de savoir, cela permet de comprendre les limites du service :

— Comme souvent avec le filtrage par DNS, il y a **surblocage**, on ne peut pas regarder la page d'accueil du service DoubleClick <http://doubleclick.net/>, par exemple.
— Il y a aussi sous-blocage : la liste des noms de domaines bloqués (et que Free ne communique pas à ses clients, ce qui est tout à fait anormal) n'est jamais complète et des publicités échapperont donc à ce filtre.
— Le panneau de contrôle de la Freebox v6 (**pas** celui du compte Free) permet de désactiver ce filtrage (qui était activé par défaut à l'origine). J'ai testé et le DNS menteur redevient sincère immédiatement. Mais, de toute façon, il suffit d'utiliser un autre résolveur que celui de Free (au moins pour les systèmes où un tel réglage est possible, par exemple Debian). C'est plus ou moins facile <https://www.bortzmeyer.org/changer-dns.html> mais cela marche, en tout cas tant que le port 53 n'est pas filtré <https://www.bortzmeyer.org/port53-filtre.html> ou détourné.

À noter qu'une façon de ne pas utiliser les résolveurs menteurs de Free est d'avoir son propre résolveur. Dans ce dernier cas, le conseil donné en général (et mis en œuvre automatiquement par des logiciels comme dnssec-trigger <https://www.bortzmeyer.org/dnssec-trigger.html>) est d'utiliser les résolveurs du FAI comme "*forwarders*", afin de profiter du cache partagé et d'épargner ainsi les serveurs faisant autorité. Ce conseil n'est plus bon si le "*forwarder*" est un menteur, puisqu'il peut alors empoisonner le résolveur local.

Une autre façon de contourner les résolveurs menteurs de Free est... d'utiliser les résolveurs de Free. Les vrais résolveurs, pas le relais/cache dnsmasq de la Freebox, disent la vérité. Regardons ceux annoncés avec les RA ("*Router Advertisment*") du RFC 8106) :

```
% drill @2a01:e00::1  A doubleclick.net
...
doubleclick.net. 1632 IN A 70.32.146.212
```

Et avec ceux qui sont utilisés par les Freebox v5 :

```
% drill @212.27.40.241  A doubleclick.net
...
doubleclick.net. 1800 IN A 70.32.146.212
```

C'est donc bien dans la Freebox que se trouve la fonction menteuse.

Quelques lectures pour approfondir le sujet. D'abord, sur les aspects techniques :

— Le rapport du Conseil Scientifique <http://www.afnic.fr/fr/l-afnic-en-bref/actualites/actualites-generales/6573/show/le-conseil-scientifique-de-l-afnic-partage-sur-le-fil.html> de l'AFNIC sur le filtrage par DNS et ses limites.
— Mon article sur le filtrage DNS <https://www.bortzmeyer.org/dns-filtering.html> et ma vision pessimiste <https://www.bortzmeyer.org/resolution-de-demain.html> des conséquences.
— Une compilation <http://downforeveryoneorjustfree.fr.nf/> des noms de domaine bloqués.
— L'analyse technique de PC Inpact <http://www.pcinpact.com/news/76477-free-adgate-methode-util.htm> (plutôt sur Windows, pour ceux qui utilisent ce système).

Sur les aspects politiques et économiques :

— L'article de PC Inpact <http://www.pcinpact.com/news/76470-la-freebox-server-se-met-a-jour-.htm> qui avait sonné l'alarme.
— Une excellente analyse de Benjamin Bayart <http://blog.fdn.fr/?post/2013/01/03/Free-porte-t-il-
— La réaction du Front de Gauche <http://numerique.frontdegauche.fr/?p=268>.