Détournement des serveurs racine en Chine ?

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 26 mars 2010. Dernière mise à jour le 16 novembre 2010

https://www.bortzmeyer.org/detournement-racine-pekin.html

Avant de lire cet intéressant article, merci de prendre connaissance d'un avertissement préalable : dès qu'il s'agit de la Chine, il faut bien admettre qu'on ne sait pas grand'chose. La plupart des gens qui pontifient sur la situation de l'Internet en Chine ne parlent pas chinois et ne connaissent du pays que les hôtels internationaux de Pékin et Shanghai. (Le prix de l'énormité pro-chinoise revient au député UMP pro-LOPPSI <https://www.bortzmeyer.org/loppsi.html> Jacques Myard pour son soutien à la dictature <http://tempsreel.nouvelobs.com/actualites/politique/20091217.OBS1017/un_depute_ump_propose_de_nationaliser_le_reseau_interne.html>.) Quand il s'agit du DNS, un des services les moins compris d'Internet, le taux de production de conneries augmente considérablement et la combinaison des deux fait donc que la plupart des phrases où il y a « DNS » et « Chine » sont fausses...

Je vais donc essayer de ne pas faire comme Myard, de ne parler que de ce que je connais, ce qui va donc rendre cet article assez court et plein de conditionnels. Contrairement aux films policiers étatsuniens, à la fin de cet article, vous ne connaitrez pas le nom du coupable, vous ne saurez même pas s'il y a eu crime...

À plusieurs reprises (par exemple lors de la réunion IETF à Paris en 2005) a été discutée la question d'un détournement du trafic des serveurs DNS de la racine en Chine, afin de mettre en œuvre les politiques, notamment de censure, de la dictature chinoise. Il est très difficile de savoir exactement ce qui se passe en Chine car les utilisateurs chinois, pour des raisons culturelles mais, surtout, par peur de la répression, ne diffusent guère d'informations. Bien sûr, des tas de gens voyagent en Chine mais ils ne sont pas forcément experts du DNS et il est difficile d'obtenir d'eux des résultats de mtr ou des dig exécutés correctement et avec les bonnes options. Les rapports existants sur la censure de l'Internet en Chine <http://cyber.law.harvard.edu/filtering/china/> sont souvent pauvres en détails techniques.

Toutefois, de temps en temps, le détournement a des conséquences visibles à l'extérieur. C'est ainsi que, le 24 mars, le responsable technique de `.cl` note que le serveur racine I, anycasté et géré par Netnod, répond bizarrement <https://lists.dns-oarc.net/pipermail/dns-operations/2010-March/005260.html> depuis le Chili :

```
$ dig @i.root-servers.net www.facebook.com A

; <<>> DiG 9.6.1-P3 <<>> @i.root-servers.net www.facebook.com A
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7448
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.facebook.com.              IN      A

;; ANSWER SECTION:
www.facebook.com.       86400   IN      A       8.7.198.45

;; Query time: 444 msec
;; SERVER: 192.36.148.17#53(192.36.148.17)
;; WHEN: Wed Mar 24 14:21:54 2010
;; MSG SIZE  rcvd: 66
```

Les serveurs racine ne font pas autorité pour `facebook.com`. Il aurait donc du renvoyer une réference aux serveurs de `.com`. Au lieu de cela, on trouve une adresse IP inconnue. Bref, quelqu'un détourne le trafic du serveur. En effet :

- Aussi bien les gérants du serveur I <https://lists.dns-oarc.net/pipermail/dns-operations/2010-March/005343.html> que ceux qui l'hébergent <https://lists.dns-oarc.net/pipermail/dns-operations/2010-March/005280.html> nient toute modification des données reçues de Verisign (qui gère le serveur maître de la racine).
- Les autres serveurs de la racine (sauf, curieusement, D) sont également affectés <https://lists.dns-oarc.net/pipermail/dns-operations/2010-March/005265.html>.
- Le seul trafic détourné est celui en UDP, TCP n'a pas de problèmes. Les traceroutes vont parfois vers des instances fiables du serveur I, par exemple au Japon, ce qui semble indiquer que la manipulation ne concerne que le port 53 celui du DNS.
- Les noms affectés sont ceux de service censurés en Chine, comme Facebook ou Twitter (pas uniquement pour des raisons politiques, mais également parce que ces services ont des concurrents chinois).

À noter que le pirate ne se cache même pas. Si on utilise la requête `CH TXT hostname.bind` (on demande au serveur son nom), au lieu du vrai nom (par exemple `s1.sth`), on obtient le nom du pirate (par exemple `c1-zaojunmiao-ns1`) ce qui montre bien que le vrai serveur racine I est innocent. Si vous voulez tester vous-même, le réseau `123.112.0.0/12`, hébergé par China Unicom, est un exemple curieux (à noter qu'il ne répond que pour les noms censurés) :

```
% dig A www.facebook.com @123.123.123.123

; <<>> DiG 9.5.1-P3 <<>> A www.facebook.com @123.123.123.123
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44684
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.facebook.com.              IN      A

;; ANSWER SECTION:
www.facebook.com.       86400   IN      A       37.61.54.158

;; Query time: 359 msec
;; SERVER: 123.123.123.123#53(123.123.123.123)
;; WHEN: Fri Mar 26 10:46:52 2010
;; MSG SIZE  rcvd: 66
```

(L'adresse `37.61.54.158` n'est pas actuellement affectée et n'est pas une adresse de Facebook.)

Une autre solution pour tester est de trouver un résolveur DNS ouvert en Chine (c'est la méthode suivie par l'article de Lowe, Winters et Marcus cité plus loin). Quelques essais/erreurs et on trouve que `ns.bnu.edu.cn` veut bien répondre (attention, il est très lent) :

```
% dig +short @ns.bnu.edu.cn www.bortzmeyer.org
208.75.84.80
```

La réponse est correcte. Et avec un nom censuré ?

```
% dig +short @ns.bnu.edu.cn www.twitter.com
37.61.54.158
```

Réponse mensongère (`37.0.0.0/8` n'est même pas alloué).

Enfin, si vous êtes situé en Chine, c'est encore plus simple (ici dans le Liaoning) :

```
% dig A www.facebook.com.
...
;; ANSWER SECTION:
www.facebook.com.       86400   IN      A       46.82.174.68
```

Cette adresse n'est pas officiellement allouée. Encore plus drôle, une adresse IPv4 "*multicast*" :

```
% dig A www.twitter.com
...
;; ANSWER SECTION:
www.twitter.com.        86400   IN      A       243.185.187.39
```

À noter que les résultats ne seront pas forcément les mêmes selon que le nom de domaine est un IDN ou pas. La censure ne trafique pas que le routage !

Il est donc très probable qu'il existe en Chine des copies pirates des serveurs racine, et que les FAI chinois ont bricolé leur IGP (OSPF ou autre) pour détourner le trafic à destination des serveurs racine (variante de l'explication : des équipements intermédiaires, par exemple des routeurs, réécrivent les paquets). Cela n'explique quand même pas tout (par exemple pourquoi les copies fiables installées en Chine voient quand même un trafic DNS non négligeable) mais, sans tests détaillés faits un peu partout en Chine, difficile d'en dire plus.

À propos de tests détaillés, si vous êtes en Chine, et que vous avez une machine Unix, j'apprécierai que vous fassiez tourner le programme (en ligne sur `https://www.bortzmeyer.org/files/dns-china.sh`) et que vous me renvoyiez le résutat. Comme il produit beaucoup de données (et prend du temps), une façon de le faire tourner est `sh dns-china.sh 2>&1 > /tmp/dns-china.log` et vous pouvez ensuite m'envoyer le fichier `/tmp/dns-china.log`. Précisez bien si vous voulez que je cite votre nom, je remercie normalement tout le monde mais, ici, pour des raisons évidentes, je ne citerai que les

---

`https://www.bortzmeyer.org/detournement-racine-pekin.html`

gens qui le demandent. Un exemple de résultat (depuis un hôtel pékinois) est disponible (en ligne sur https://www.bortzmeyer.org/files/dns-china-beijing-2010-11.log).

Merci aux premiers et anonymes (pour vous, pas pour moi) testeurs, qui ont permis de voir que la Chine, c'est grand, et qu'on n'observe pas le même résultat selon les régions et/ou les opérateurs (par exemple, un test depuis Shanghai montre d'autres résultats, où les réponses des serveurs racine ne sont pas réécrites).

Bref, une fois qu'il est établi qu'il y a réécriture de certaines réponses DNS en Chine, revenons au Chili. Pourquoi ont-ils vu le problème ? Une fuite de ce bricolage de routes (analogue à celle qui avait touché YouTube <https://www.bortzmeyer.org/pakistan-pirate-youtube.html>) explique sans doute que l'annonce du serveur pirate ait atteint l'autre bout du Pacifique...

On pourrait penser qu'il suffit aux internautes chinois de créer un VPN avec un réseau à l'étranger, avec service DNS, pour échapper à cette censure mais la dictature est efficace : elle ne compte pas sur une seule méthode technique, elle en utilise plusieurs (filtrage IP, interception HTTP, DPI, etc).

Parmi les sources d'information fiables sur les manipulations DNS en Chine, l'excellent article technique de Graham Lowe, Patrick Winters et Michael L. Marcus « "*The Great DNS Wall of China*" <http://cs.nyu.edu/~pcw216/work/nds/final.pdf> » (bonne méthodologie et étude sérieuse) ou le « "*Report about national DNS spoofing in China*" <http://www.dit-inc.us/hj-09-02.html> ». Des bizarreries dues au filtrage chinois avaient déjà été signalées <https://lists.dns-oarc.net/pipermail/dns-operations/2009-June/003944.html>. Le NIC chilien a documenté ses observations en espagnol <http://www.nic.cl/anuncios/2010-03-29.html> et en anglais <http://www.nic.cl/anuncios/2010-03-29-eng.html>. Les réécritures faites en Chine par la censure peuvent avoir des conséquences techniques complexes, et parfois défavorables au censeur (voir l'analyse touffue de David Dagon <https://lists.dns-oarc.net/pipermail/dns-operations/2010-March/005340.html>, le chercheur en sécurité bien connu). Et quelques articles en anglais sont parus sur le récent problème décrit ici : « "*China censorship leaks outside Great Firewall via root server*" <http://arstechnica.com/tech-policy/news/2010/03/china-censorship-leaks-outside-great-ars> » (plutôt technique et de bonne qualité), « "*Accidentally Importing Censorship*" <http://www.renesys.com/blog/2010/03/fouling-the-global-nest.shtml> » (bonne analyse technique avec notamment une analyse de la probabilité de voir la censure depuis l'extérieur), « "*China's Great Firewall spreads overseas*" <http://www.computerworld.com/s/article/9174132/China_s_Great_Firewall_spreads_overseas> » ou « "*Web traffic redirected to China in mystery mix-up*" <http://news.cnet.com/8301-27080_3-20001227-245.html> ». Si vous voulez un logiciel qui peut détecter certaines réécritures faites en Chine, il y a ScholarZhang <http://code.google.com/p/scholarzhang/> (ne me demandez pas de traduire le README !) Une version autonome a été publiée <https://lists.dns-oarc.net/pipermail/dns-operations/2010-March/005323.html>.

D'autre part, Jean-Marc Liotier a fait une très bonne traduction en anglais <http://serendipity.ruwenzori.net/index.php/2010/03/26/dns-spoofing-in-china-by-stephane-bortzmeyer> de cet article, pour ceux qui sont plus à l'aise avec la langue de Jasper Fforde.

Merci à Hauke Lampe et Marco Davids pour leur aide technique et bien sûr à Mauricio Vergara Ereche pour ses excellentes observations depuis Santiago.