

Un exemple d'empoisonnement DNS en vrai

Stéphane Bortzmeyer

<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 17 Janvier 2010

<http://www.bortzmeyer.org/empoisonnement-dns-en-vrai.html>

Depuis le temps qu'on parle d'empoisonnement DNS, par exemple suite à la faille Kaminsky <<http://www.bortzmeyer.org/comment-fonctionne-la-faille-kaminsky.html>>, je n'avais jamais eu l'occasion d'en observer un en vrai. Des essais, bien sûr, des résultats de tests, mais une vraie attaque menée dans le but de détourner du vrai trafic, j'en avais entendu parler mais jamais vu ça de mes propres digs. C'est désormais fait.

Tout a commencé sur Twitter : (17:07:09) oneeyed: whois.com hacked <http://bit.ly/7IaCfm>. Je regarde et <<http://whois.com/>>, service de recherche via whois, semble normal. D'autres personnes le voient normal. En fait, le site Web est intact, il n'a pas été défiguré, c'est le DNS du FAI Free qui a des problèmes. Je ne m'en étais pas aperçu car j'utilise mon propre résolveur DNS. Mais, en interrogeant ceux de Free, on trouve des données normales sur le serveur 212.27.40.241 mais pas sur l'autre résolveur que Free met à la disposition de ses clients :

```
% dig +short @212.27.40.240 A whois.com
94.102.7.12
```

Cette adresse IP 94.102.7.12 n'a rien à voir avec whois.com et la base du RIPE-NCC la situe chez un opérateur turc (la vraie adresse IP de whois.com est 67.225.139.191, aux États-Unis). À l'adresse en question, un serveur Web diffuse une image <<http://i.imgur.com/RgIZl.png>> de défiguration classique.

Donc, il semble bien qu'il y aie eu empoisonnement (par un moyen inconnu de moi) d'un des résolveurs DNS de Free. Pendant un certain temps (environ une heure, semble t-il), tous les clients de Free qui tombaient sur ce résolveur étaient envoyés au mauvais serveur. Le problème a ensuite disparu, probablement parce qu'un technicien de Free a redémarré le serveur.

Quelques leçons :

- Ce genre de problèmes n'est pas spécifique à Free : d'autres FAI peuvent l'avoir et rien n'indique qu'il soit dû à une erreur ou une défaillance de Free. On trouve plus facilement des rapports sur Free car ce fournisseur a des gens férus de techniques, alors qu'ils sont complètement absents chez d'autres FAI, qui peuvent donc faire n'importe quoi en étant sûrs de ne pas être observés.
- Je n'ai pas vu le serveur « pirate » et 94.102.7.12 ne le sert apparemment plus, donc je ne sais pas quel était le but poursuivi par l'attaquant.

Bien sûr, DNSSEC aurait détecté le problème. Mais DNSSEC soulève d'autres questions.

Merci à Samuel Lardieu pour m'avoir signalé le cas figolo. Voir aussi la discussion sur Reddit <http://www.reddit.com/r/reddit.com/comments/aqima/whoiscom_hacked/>.