Explorer le contenu du DNS dans le passé avec DNSDB

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 7 février 2013. Dernière mise à jour le 7 octobre 2013

https://www.bortzmeyer.org/dnsdb.html

Le DNS peut être vu comme une grande base de données répartie sur toute la planète. Cette base contient des données, les **enregistrements** ("*resource records*" dans la langue de George Martin, d'où le sigle RR que vous verrez plus bas). Ces enregistrements peuvent changer dans le temps, parfois assez vite, et on souhaiterait souvent revenir en arrière. L'adresse IP de `google.ro` a-t-elle changé le 28 novembre 2012 ? Qu'est-il arrivé à `meteofrance.com` le 20 novembre 2012 ? Quand est apparu l'enregistrement d'une adresse IPv6 pour `ovh.com` ? Le service DNSDB <https://www.dnsdb.info> de la société Farsight (créé originellement à l'ISC) permet de répondre à ces questions. C'est un véritable Internet Archive pour le DNS.

D'abord, un avertissement : DNSDB n'est pas ouvert publiquement. Les données que ce service contient peuvent être sensibles, et intéresser des "*pabos*". C'est pour cela que l'accès à DNSDB est soumis à une autorisation préalable <https://www.dnsdb.info/#Apply>. Il faut montrer patte blanche. Discuter autour d'une bière avec un employé de Farsight lors d'une réunion IETF ou OARC <https://www.dns-oarc.net/> peut aider aussi.

Une fois que votre candidature est approuvée, vous pouvez accéder au service, en parler publiquement (cet article dans mon blog ne viole donc pas les conditions d'utilisation) et même citer des exemples de données. Mais, évidemment, pas question de copier la base et de l'emporter (un avertissement technique au passage : la base est **grosse** et, même si on en avait une copie, il faudrait être un dieu de NoSQL pour arriver à y accéder en des temps raisonnables).

Bien, une fois qu'on a un accès, essayons d'abord avec l'interface Web : On va demander l'histoire de l'enregistrement de type A (adresse IPv4) `google.ro`. Il y a bien sûr de nombreuses réponses mais celle qui nous intéresse est celle du 28 novembre :

On voit que `google.ro`, pendant quelques heures, pointait vers l'adresse IP d'un hébergeur néerlandais qui n'a rien à voir avec Google. Apparemment, le registre du `.ro` avait été piraté et `google.ro` redirigé.

Mais d'où est-ce que DNSDB tire ces informations ? Il s'appuie sur plusieurs sources, notamment le SIE <https://sie.isc.org/>, un réseau de sondes DNS installées en divers endroits, qui capturent passivement le trafic DNS et l'envoient à DNSDB.

Naturellement, on n'est pas forcé d'utiliser le cliquodrome Web. Il existe une API REST. Il suffit de demander en ligne un mot de passe ("*API key*", évidemment non affichée ici). Testons-la avec curl pour regarder le problème de `meteofrance.com` :

```
% curl --header "X-API-Key: 1234" \
      https://api.dnsdb.info/lookup/rrset/name/meteofrance.com/NS
...
;;  bailiwick: com.
;;      count: 29
;; first seen: 2012-11-20 12:32:48 -0000
;;  last seen: 2012-11-20 15:38:22 -0000
meteofrance.com. IN NS ns1.pendingrenewaldeletion.com.
meteofrance.com. IN NS ns2.pendingrenewaldeletion.com.
...
;;; Returned 6 RRsets in 0.06 seconds
;;; ISC DNSDB
```

Ah, le problème est clair. Le 20 novembre, le domaine `meteofrance.com` a expiré (paiement non effectué) et le bureau d'enregistrement a mis le domaine sur ses propres serveurs de noms, le temps que le client se réveille (ce qui s'est passé trois heures plus tard, comme vous pouvez le voir).

Si on n'aime pas faire du curl directement, Farsight fournit des scripts qui permettent d'interroger l'API plus facilement. On met le mot de passe dans `/.isc-dnsdb-query.conf` et :

```
% isc-dnsdb-query rrset ovh.com/AAAA
;;  bailiwick: ovh.com.
;;      count: 10519
;; first seen: 2011-06-08 10:20:48 -0000
;;  last seen: 2011-08-19 16:40:23 -0000
ovh.com. IN AAAA 2001:41d0:1:1b00:213:186:33:34

;;; Returned 1 RRsets in 0.01 seconds
;;; ISC DNSDB
```

On peut voir qu'OVH a une adresse IPv6 en juin 2011 mais ne l'a pas conservée.

Attention au passage, si vous faites des analyses historiques, DNSD est un service récent. Essayons avec un domaine ancien et connu :

```
% isc-dnsdb-query rrset www.ripe.net
;;  bailiwick: ripe.net.
;;      count: 207148
;; first seen: 2010-06-24 06:30:27 -0000
...
```

Le RIPE existait évidemment avant 2010. Mais cette date est celle du plus ancien enregistrement dans la base.

DNSDB accepte aussi les jokers à l'extrémité d'un nom. Imaginons qu'on cherche tous les enregistrements DANE existants (RFC 6698 [1]). DNSDB ne connaît pas ce type mais on peut l'indiquer par son numéro :

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc6698.txt`

```
% isc-dnsdb-query rrset '_443._tcp.*/type52'
;;  bailiwick: torproject.org.
;;      count: 3
;; first seen: 2013-02-08 07:54:42 -0000
;;  last seen: 2013-02-10 07:29:16 -0000
_443._tcp.www.torproject.org. IN TYPE52 \# 67 03 01 02 4d f6 66 72 94 fc 1d fd 6a 95 da 7b d8 95 9b 71 7b 68 21
...
;;  bailiwick: os3sec.org.
;;      count: 9
;; first seen: 2013-01-19 22:57:17 -0000
;;  last seen: 2013-02-06 02:52:42 -0000
_443._tcp.os3sec.org. IN TYPE52 \# 35 03 00 01 18 e3 71 b8 ad 85 a1 7c ba a1 17 a8 af 44 10 1e 57 b8 8d 7a 99 44
...
```

Toutes les recherches ci-dessus ont été faites à partir du nom de domaine (la partie gauche d'un enregistrement DNS). Mais on peut aussi, depuis l'interface Web ou bien via l'API, chercher sur le **contenu**, sur la partie droite d'un enregistrement. Pour cela, il faut remplacer `rrset` par `rdata` et indiquer si on cherche une adresse IP ou un nom ou un contenu quelconque. Ici, je cherche tous les noms qui pointent vers l'adresse IP du serveur Web du ministère des Finances :

```
% isc-dnsdb-query  rdata ip 193.17.19.153
vae.gouv.fr. IN A 193.17.19.153
www.kezeco.economie.gouv.fr. IN A 193.17.19.153
taxepro.economie.gouv.fr. IN A 193.17.19.153
www.dpa.finances.gouv.fr. IN A 193.17.19.153
semaine.industrie.gouv.fr. IN A 193.17.19.153
www.semaine-industrie.gouv.fr. IN A 193.17.19.153
;;; Returned 6 RRs in 0.05 seconds
;;; ISC DNSDB
```

En pratique, cette option est très utile pour mesurer le degré de corruption d'une adresse IP. Si on prend une adresse IP citée dans un spam, on découvre en général plein de noms qui pointent vers la même adresse :

```
% isc-dnsdb-query  rdata  ip 83.206.207.181
tracking.cofidis.be. IN A 83.206.207.181
tr.service-mail.carrefour.fr. IN A 83.206.207.181
tr.denplan.co.uk. IN A 83.206.207.181
mp-dhrd.com. IN A 83.206.207.181
mail.dailyreduc.com. IN A 83.206.207.181
affiliates-solution.com. IN A 83.206.207.181
tr.affiliates-solution.com. IN A 83.206.207.181
www.affiliates-solution.com. IN A 83.206.207.181
tracking.bp01.net. IN A 83.206.207.181
trpreviews.bp01.net. IN A 83.206.207.181
tr1.bp06.net. IN A 83.206.207.181
bp08.net. IN A 83.206.207.181
bp09.net. IN A 83.206.207.181
bp10.net. IN A 83.206.207.181
bp11.net. IN A 83.206.207.181
...
```

(La liste continue pendant longtemps... Le spammeur avait manifestement enregistré une longue liste de domaines pour éviter les listes noires.)

Un service ressemblant à DNSDB (en moins riche) est `<http://dnshistory.org/>`.