PassiveDNS.cn, une autre base d'histoire du DNS

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 4 novembre 2014

https://www.bortzmeyer.org/passivedns-cn.html

Il existe plusieurs services « historique DNS » ou « *"passive DNS"* » qui permettent de remonter dans le temps et de consulter les données qui étaient associées à un nom de domaine. J'ai déjà parlé ici de DNSDB <https://www.bortzmeyer.org/dnsdb.html>, voici un nouveau, <https://PassiveDNS.cn>.

Tous ces services reposent sur le même principe : un ensemble de sondes écoute passivement le trafic DNS près de gros résolveurs, et stocke les réponses, avec leurs dates, dans une base de données, qu'il n'y a plus qu'à interroger. En ne stockant que le contenu des réponses (pas les requêtes, pas les adresses IP du requêtant), on évite pas mal de problèmes liés à la vie privée. Ces services se différencient par leurs conditions d'utilisation (aucun n'est public), par la quantité de données (qui dépend entre autres de la position des sondes), la géographie de leurs sondes (DNSDB <https://www.bortzmeyer.org/dnsdb.html> a l'air d'avoir surtout des sondes aux États-Unis) et leurs qualités logicielles. Ils sont des outils essentiels aux chercheurs et aux professionnels de la sécurité.

Ce <https://PassiveDNS.cn> a l'originalité d'être basé en Chine. Il faut demander un compte, après avoir expliqué pourquoi on le voulait et ce qu'on en ferait et, si le gestionnaire du service est d'accord, vous recevez de quoi vous connecter. Comme pour DNSDB, les recherches peuvent être faites par la partie gauche de la réponse DNS (*"owner name"*) ou par la partie droite (*"resource record data"*). On peut ainsi demander quelles ont été les adresses IPv6 successives de `www.bortzmeyer.org` :

```
2001:4b98:dc0:41:216:3eff:fece:1902
2605:4500:2:245b::42
Time begin: 2014-08-12 21:05:56
Time end: 2014-11-04 08:02:40
Count: 793
```

Le `Time begin` indique quand PassiveDNS.cn a commencé à stocker ses données (ce nom a une adresse IPv6 depuis des années).

Et on peut chercher par la partie droite, par le contenu. Qui a utilisé le serveur de noms `ns2.nic.fr` :

```
...
polytechnique.fr
press.ma
supelec.fr
telecom-bretagne.eu
u-bordeaux.fr
u-nancy.fr
...
```

(Notez que `press.ma` est une "*lame delegation*", une délégation faite à un serveur qui n'est pas au courant, comme le sont plusieurs délégations de cette zone.)

Il existe bien sûr une API. Curieusement, il faut demander une clé manuellement (on ne peut pas le faire depuis le site Web). Une fois obtenue, on a du REST classique. Une requête avec curl est un peu compliquée à faire (il faut ajouter deux en-têtes HTTP dont l'un est un condensat de l'URL demandé et de la clé). À défaut de curl en direct, on peut se programmer ça, ou bien on peut utiliser l'outil flint `<https://github.com/360netlab/flint>`.

```
% flint rrset www.bortzmeyer.org AAAA
www.bortzmeyer.org AAAA In rrset
-------
Record times: 2014-08-12 15:05:56 -- 2014-11-04 01:02:40
Count: 793
www.bortzmeyer.org AAAA 2001:4b98:dc0:41:216:3eff:fece:1902
www.bortzmeyer.org AAAA 2605:4500:2:245b::42
```

Et si on préfère le JSON, pour analyse ultérieure :

```
% flint -j rrset www.elysee.fr CNAME
[
    {
        "count": 1882,
        "time_first": 1407251470,
        "rrtype": "CNAME",
        "rrname": "www.elysee.fr",
        "rdata": "cdn.cdn-tech.com.c.footprint.net;",
        "time_last": 1415128869
    }
]
```

(Notez le curieux point-virgule à la fin du `rdata`.)

Bon, si vous tenez à le programmer vous-même, ce script shell marche (il faut lui passer `rrset/keyword/$DOMAI` en paramètre) :

```
#!/bin/sh

KEY='secret.key.for.you.only'
ID='guest.test'
# No / at the end
URL=https://www.passivedns.cn

query=/api/$1

hash=$(echo -n "$query$KEY" | md5sum | cut -d " " -f1)

curl -v -H "Accept: application/json" \
    -H "X-BashTokid: $ID" -H "X-BashToken: $hash" $URL$query
```

Comme tous les outils de ce genre, PassiveDNS.cn permet d'analyser des attaques. Ici, par exemple, on voit de fausses réponses pour le TLD `.us` :

```
% flint  rrset us NS
us NS In rrset
-------
Record times: 2014-08-20 09:17:03 -- 2014-11-04 01:29:31
Count: 102064
us NS a.cctld.us
us NS b.cctld.us
us NS c.cctld.us
us NS e.cctld.us
us NS f.cctld.us
us NS k.cctld.us

Record times: 2014-08-25 12:45:11 -- 2014-09-09 21:49:09
Count: 252
us NS ns1.360dns.cc
us NS ns1.360dns.net
us NS ns2.360dns.cc
us NS ns2.360dns.net

Record times: 2014-08-25 12:03:07 -- 2014-09-09 21:29:54
Count: 388
us NS ns1.unidns.x
us NS ns2.unidns.x
...
```

Le premier enregistrement est correct, les autres (notez leur durée plus courte) sont des empoisonnements de cache ou d'autres manipulations du DNS, dont la Chine est coutumière <https://www.bortzmeyer.org/detournement-racine-pekin.html> (on ne voit pas ces réponses anormales depuis DNSDB).

Ah, un dernier point, PassiveDNS.cn n'est pas très rapide ; soyez patient.