Sur les pannes de service-public.fr et impots.gouv.fr (et caf.fr)

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 16 avril 2023. Dernière mise à jour le 5 mai 2023

https://www.bortzmeyer.org/service-public-impots-dns.html

Après la grande panne de Météo-France <https://www.bortzmeyer.org/meteofrance-dns.html> le 12 avril, on a vu les sites Web et être en panne, les 14 et 15 avril. Le 16 avril, c'était le tour de . Sait-on ce qui s'est passé ?

Je divulgâche <https://fr.wiktionary.org/wiki/divulg%C3%A2cher> tout de suite, il n'y a pas d'informations fiables et précises. Tout au plus puis-je faire part de quelques observations, et ajouter quelques conseils.

Commençons par le 14 avril, la panne de l'excellent, très utile et très bien fait Service-public.fr. Je n'étais pas disponible au moment de la panne, mais j'ai pu effectuer un test avec les sondes RIPE Atlas <https://atlas.ripe.net/> peu après et il y avait bien un problème DNS :

```
% blaeu-resolve -r 100 --country FR --type A www.service-public.fr
[ERROR: NXDOMAIN] : 18 occurrences
[160.92.168.33] : 81 occurrences
Test #52236542 done at 2023-04-14T10:55:55Z
```

Dix-huit des sondes ont reçu de leur résolveur DNS <https://www.bortzmeyer.org/resolveur-dns.html> un NXDOMAIN ("*No Such Domain*" [Caractère Unicode non montré [1]] ce nom n'existe pas). Vous pouvez voir les résultats complets en ligne <https://atlas.ripe.net/measurements/52236542/#probes>. Ceci n'est évidemment pas normal : tout se passe comme si, pendant un moment, le domaine `service-public.fr` avait été modifié pour ne plus avoir ce sous-domaine `www`. Une erreur humaine ? Peu après, le problème avait disparu :

1. Car trop difficile à faire afficher par LaTeX

```
% blaeu-resolve -r 100 --country FR --type A www.service-public.fr
[160.92.168.33] : 100 occurrences
Test #52237120 done at 2023-04-14T11:32:53Z
```

Il avait en fait été réparé avant mon premier test mais rappelez-vous que les résolveurs DNS ont une mémoire et certains se souvenaient donc de la non-existence. Bref, sans pouvoir être certain (Service-public.fr ne semble pas avoir communiqué à ce sujet, à part via des tweets stéréotypés ne donnant aucun détail <https://twitter.com/servicepublicfr/status/1646826405236293635>), il semble bien qu'il y ait eu une erreur, vite corrigée.

Et le 15 avril, qu'est-il arrivé au site Web des impôts (c'était le lendemain de son ouverture pour les déclarations de revenus, moment qui se traduit en général par un trafic intense) ? Là encore, on voit un problème DNS, il ne s'agissait pas uniquement d'une surcharge du site Web :

```
% blaeu-resolve   --type A -r 100 --country FR www.impots.gouv.fr
[152.199.19.61] : 59 occurrences
[ERROR: SERVFAIL] : 36 occurrences
Test #52277291 done at 2023-04-15T07:20:04Z
```

Les sondes RIPE Atlas (résultats complets en ligne <https://atlas.ripe.net/measurements/52277291/#probes>) nous montrent cette fois qu'un certain nombre de résolveurs DNS ont mémorisé un SERVFAIL("*Server Failure*" [Caractère Unicode non montré] le résolveur n'a pas réussi à résoudre le nom). Les codes d'erreur DNS sont peu nombreux, malheureusement (le RFC 8914[2] propose une solution, mais encore peu déployée) et SERVFAIL sert à beaucoup de choses. Le plus vraisemblable est qu'il indiquait ici que le résolveur n'avait réussi à joindre aucun des serveurs faisant autorité <https://www.bortzmeyer.org/serveur-dns-faisant-autorite.html>. impots.gouv.fr n'a que deux serveurs faisant autorité <https://dns.bortzmeyer.org/impots.gouv.fr/NS>, tous les deux derrière l'AS 3215 <https://stat.ripe.net/ui2013/AS3215>, ce qui rend ce domaine vulnérable à des problèmes de routage ou à des attaques par déni de service. Voici les serveurs, testés par check-soa <https://framagit.org/bortzmeyer/check-soa> :

```
% check-soa impots.gouv.fr
dns1.impots.gouv.fr.
145.242.11.22: OK: 2023041301
dns2.impots.gouv.fr.
145.242.31.9: OK: 2023041301
```

On notera aussi que, même si on pouvait résoudre le nom de domaine, le serveur HTTP avait des problèmes :

```
% curl -v www.impots.gouv.fr.
*   Trying 152.199.19.61:80...
* Connected to www.impots.gouv.fr (152.199.19.61) port 80 (#0)
> GET / HTTP/1.1
> Host: www.impots.gouv.fr
> User-Agent: curl/7.81.0
```

2. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc8914.txt

```
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 504 Gateway Timeout
< Content-Type: text/html
< Date: Sat, 15 Apr 2023 07:18:41 GMT
< Server: ECAcc (paa/6F2E)
< X-EC-Proxy-Error: 14
< Content-Length: 357
<
<?xml version="1.0" encoding="iso-8859-1"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
         "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
<head>
<title>504 - Gateway Timeout</title>
</head>
...
```

On peut bien parler au serveur frontal mais il n'arrive pas à joindre le « vrai » serveur derrière, d'où l'erreur 504 <https://http.cat/504>.

Que s'est-il passé ? À ma connaissance, il n'y a pas eu de communication officielle des impôts à ce sujet mais des sources crédibles évoquent une attaque par déni de service, ce qui est en effet compatible avec ce qui a été observé.

Et les allocations familiales ? Le 16 avril, le domaine `caf.fr` est en panne :

```
% check-soa -i caf.fr
ns.caf.fr.
91.231.174.240: ERROR: read udp 192.168.2.4:45069->91.231.174.240:53: i/o timeout
ns1.caf.fr.
91.231.174.241: ERROR: read udp 192.168.2.4:48911->91.231.174.241:53: i/o timeout
% date -u
Sun 16 Apr 16:08:59 UTC 2023
```

Les deux serveurs répondent très épisodiquement (ce qu'on voit souvent lors des attaques par déni de service ; quelques requêtes passent). Un test sur les sondes RIPE Atlas <https://atlas.ripe.net/measurements/52345500/#probes> montre que c'est de partout :

```
% blaeu-resolve -r 100 --country FR --type NS caf.fr
[ERROR: SERVFAIL] : 68 occurrences
[ns.caf.fr. ns1.caf.fr.] : 8 occurrences
Test #52345500 done at 2023-04-16T15:39:40Z
```

Là encore, le domaine n'a que deux serveurs faisant autorité, tous les deux sous le même préfixe de longueur 24. C'est une configuration faible, qui rend le domaine vulnérable.

Enfin, le 16 avril, mais encore ensuite le 25 avril, puis le 4 mai, l'INSEE a eu un problème similaire, sur son domaine à seulement deux serveurs. Au début, un certain nombre de résolveurs avaient encore l'information en mémoire :

---

https://www.bortzmeyer.org/service-public-impots-dns.html

```
%   blaeu-resolve --requested 100 --country FR --type NS insee.fr
[ERROR: SERVFAIL] : 59 occurrences
[ns1.insee.fr. ns2.insee.fr.] : 21 occurrences
Test #52618361 done at 2023-04-25T09:55:20Z
```

Mais au plus fort de la crise :

```
% blaeu-resolve --requested 100 --country FR --type NS insee.fr
[ERROR: SERVFAIL] : 73 occurrences
[ns1.insee.fr. ns2.insee.fr.] : 2 occurrences
Test #52622678 done at 2023-04-25T12:02:12Z
```

Le problème a été réglé vers 1400 UTC. Il avait en effet en cascade, empêchant le fonctionnement des API de la base SIRENE et tous les services publics qui en dépendent. (Un arrêté du 14 juin 2017 <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000034944648> impose d'ailleurs un minimum de robustesse à un des services gérés par l'INSEE.)

Le fait que ns2 répondait parfois semble indiquer une attaque plutôt qu'une panne, qui aurait été totale. Un exemple d'un service planté par cascade (car il dépendait de l'INSEE) :

Conclusion ? On ne le rappelera jamais assez, le DNS est une infrastructure critique et qui doit être traitée comme telle. Puisque la très grande majorité des activités sur l'Internet dépend d'un DNS qui marche, un domaine important ne devrait pas se contenter de deux serveurs faisant autorité et connectés au même opérateur. Il est important d'avoir davantage de serveurs faisant autorité, et de les répartir dans plusieurs AS ; on ne met pas tous ses œufs dans le même panier.

Contrairement à ce qu'on lit souvent chez les lecteurs enthousiastes de la publicité des entreprises commerciales, cette robustesse ne nécessite pas forcément de faire appel à des prestataires chers, ni d'acheter des services qui ont peut-être leur utilité pour d'autres usages (comme HTTP) mais qui ne sont pas pertinents pour le DNS. De même qu'on peut faire un disque virtuel fiable à partir de plusieurs disques bon marché (le RAID), on peut faire un service DNS solide à partir de plusieurs hébergeurs même s'ils ne sont pas chers.

À cet égard, il est curieux que des services publics comme Météo-France, Service-public.fr et les impôts ne coopèrent pas davantage ; avoir des serveurs secondaires dans un autre établissement public devrait être la règle. (Je ne suis pas naïf et je me doute bien que la raison pour laquelle ça n'est pas fait n'a rien à voir avec la technique ou avec les opérations et tout à voir avec des problèmes bureaucratiques et des processus kafkaïens.)

Et puis, bien sûr, on souhaiterait voir davantage de communication de la part des organismes publics et donc des retex publics (une entreprise commerciale comme Cloudflare le fait souvent, mais les services publics français sont moins transparents ; Météo-France a communiqué <https://meteofrance.com/actualites-et-dossiers/actualites/meteo-france-victime-d1-attaque-informatique> mais avec quasiment aucun détail technique).

Un article du Parisien <https://www.leparisien.fr/economie/declaration-de-revenus-le-site-php> a été publié sur la panne des impôts.