RFC 8023 : Report from the Workshop and Prize on Root Causes and Mitigation of Name Collisions

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 27 novembre 2016

Date de publication du RFC : Novembre 2016

https://www.bortzmeyer.org/8023.html

Ce nouveau RFC est le compte-rendu d'un atelier qui s'était tenu du 8 au 10 mars 2014 à Londres sur le thème des « collisions ». Ce terme exagéré et sensationnaliste désigne le phénomène qui peut se produire quand un acteur de l'Internet a bêtement choisi de se créer un TLD à lui dans le DNS, et que ce TLD est ensuite créé par l'ICANN.

Supposons que l'entreprise Bidon décide de nommer ses ressources internes (site Web réservé aux employés, etc) sous le TLD inexistant `.bidon`. C'est une mauvaise idée <https://www.bortzmeyer.org/pourquoi-le-tld-local-n-est-pas-une-bonne-idee.html> mais elle est fréquente. L'entreprise Bidon compte sur le fait que ses employés utiliseront les résolveurs DNS internes, qui ont été configurés pour reconnaître `.bidon`. Par exemple, avec Unbound, et un serveur faisant autorité en `2001:db8:666::1:541f`, les résolveurs ont été configurés ainsi :

```
stub-zone:
 name:   "bidon"
 stub-addr: 2001:db8:666::1:541f
```

Si un employé tente accidentellement d'accéder à une ressource en `.bidon`, alors qu'il n'utilise pas les résolveurs de la boîte, la requête filera vers la racine du DNS, qui répondra `NXDOMAIN` ("*No Such Domain*"). C'est ainsi que la racine voit souvent des requêtes pour des noms se terminant en `.local`, `.home` ou `.belkin`. Si, quelques années après, l'ICANN délègue effectivement ce TLD à une autre organisation, ces requêtes à la racine donneront désormais un vrai résultat. Au lieu d'un message d'erreur, le malheureux employé sera peut-être redirigé vers un autre site Web que celui attendu. C'est ce phénomène que Verisign avait baptisé « collision » ("*name collision*"), terme conçu pour faire peur.

C'est dans ce contexte qu'il y a plus de deux ans s'était tenu le « "*Workshop on Root Causes and Mitigation of Name Collisions*" <http://namecollisions.net/> », dont ce RFC est le compte-rendu tardif. Le premier rapport de l'ICANN qui mentionnait ce phénomène était le SAC 045 <https://www.icann.org/en/system/files/files/sac-045-en.pdf> en 2010. Il pointait le risque que la délégation effective d'un nouveau TLD change la réponse obtenue, pour les clients mal configurés (qui interrogeaient à tort un résolveur extérieur, et donc la racine, au lieu de leurs résolveurs internes).

L'ICANN a même créé une page Web dédiée à cette question <https://www.icann.org/en/help/name-collision>, dont la source réelle est le recouvrement de deux espaces de noms, l'interne et l'externe. La bonne pratique idéale serait de ne pas utiliser de noms qui n'existent pas ou, pire, qui existent avec une autre signification dans l'arbre public des noms de domaine (et, là, relire le RFC 2826 [1] peut aider). Pour reprendre l'exemple de l'entreprise Bidon, si elle est titulaire de `bidon.fr`, elle devrait nommer ses ressources internes avec des noms se terminant en `privé.bidon.fr` ou `interne.bidon.fr`. Si on ne veut pas faire les choses proprement, et qu'on utilise quand même le TLD inexistant `.bidon`, alors il faut veiller très soigneusement à séparer les deux espaces de nommage et à éviter qu'ils ne se rencontrent un jour (ce qui est difficile à l'ère des mobiles, avec des appareils qui rentrent et qui sortent du réseau de l'entreprise). Sinon, on verra ces fameuses collisions.

En pratique, pas mal d'administrateurs système surestiment leurs compétences et croient qu'ils vont réussir à empêcher toute fuite vers le DNS public. C'est ce qui explique une partie des requêtes pour des noms inexistants que reçoit la racine (ces noms inexistants forment la majorité du trafic des serveurs racine du DNS). Un des problèmes de fond de l'Internet est en effet que l'administrateur de base ne se tient pas au courant et n'est pas informé des problèmes du monde extérieur. « Après moi, le déluge »

Autrefois, le problème était surtout théorique. Le nombre de TLD n'avait pas bougé depuis de très nombreuses années, et personne ne pensait que des TLD comme `.pizza` ou `.green` verraient le jour. Mais, en 2012, l'ICANN a lancé officiellement son programme d'ajout d'un grand nombre de TLD, et le risque est soudain devenu une question pratique. D'où l'atelier de 2014.

La section 2 du RFC revient en détail sur l'arrière-plan de ce problème de collision. Outre le rapport SAC 045 cité plus haut, il y avait eu une déclaration de l'IAB <https://www.iab.org/documents/correspondence-reports-documents/docs2008/2008-03-07-icann-new-gtlds/>, puis un autre rapport du SSAC ("*Security and Stability Advisory Committee*", un comité de l'ICANN), le SAC 046 <https://www.icann.org/en/system/files/files/sac-046-en.pdf>, une déclaration du RSSAC <https://www.icann.org/en/news/correspondence/murai-to-board-25nov10-en.pdf> et plein d'autres textes sur les conséquences d'un agrandissement important de la zone racine. Par exemple, le rapport SAC 057 <https://www.icann.org/en/system/files/files/sac-057-en.pdf> faisait remarquer que les AC attribuaient souvent des certificats pour des noms de domaine dans des TLD purement locaux. Cela montrait le déploiement de ces TLD privés et cela inquiétait. Si la société Bidon exploite `.bidon` et obtient d'une AC un certificat pour `www.compta.bidon`, après la délégation de ce même TLD dans la racine publique, ce certificat pourrait être utilisé pour usurper l'identité d'un autre serveur.

J'ai parlé plus haut des fuites vers le DNS public. Quelle est leur ampleur exacte ? Ce n'est pas si évident que cela de le savoir. Contrairement à un raccourci journalistique fréquent, l'ICANN ne gère pas la racine. Chaque opérateur d'un serveur DNS racine se débrouille indépendamment, supervise son serveur mais ne rend pas forcément compte à d'autres acteurs ou au public. En pratique, les opérateurs des serveurs racine ont un niveau d'ouverture très variable. (Cf. l'analyse de l'ICANN <https://www.icann.org/en/news/announcements/announcement-28may13-en.htm> à ce sujet.) Un

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc2826.txt`

des moments où plusieurs opérateurs de serveurs racine collectent en même temps de l'information est le "*Day in the Life of the Internet*" <http://www.caida.org/projects/ditl/> et c'est sur la base de ces données qu'a été fait le rapport d'Interisle « "*Name Collision in the DNS*" <https://www.icann.org/en/about/staff/security/ssr/name-collision-02aug13-en.pdf> ». Entre autres, ce rapport classait les futurs TLD selon qu'ils présentaient un risque de collision élevé ou faible (`.home`, `.corp` et `.site` se retrouvaient en tête du classement). L'ICANN a alors publié un plan <https://www.icann.org/en/about/staff/security/ssr/new-gtld-collision-mitigation-05aug13-en.pdf> pour gérer ce risque de collisions, notant que `.home` et `.corp` étaient de loin les plus « risqués », car ils sont fréquemment utilisés comme TLD locaux. Bien d'autres documents ont été publiés par l'ICANN, qui a une productivité extraordinaire lorsqu'il s'agit de faire de la paperasse. Le dernier <https://www.icann.org/en/about/staff/security/ssr/name-collision-mitigation-26feb14-en.pdf> mettait en place le système dit de « "*controlled interruption*" » qui, en gros, impose à tous les nouveaux TLD de résoudre, pendant les premiers temps de leur délégation, **tous** les noms de domaine vers l'adresse IP `127.0.53.53`. Voici l'exemple de `.box` en novembre 2016 (ce cas avait fait l'objet d'un article de Heise en allemand <https://www.heise.de/newsticker/meldung/Neue-Top-Level-Domain-box-bri html>, car le routeur Fritz!Box, très populaire en Allemagne, utilisait ce TLD) :

```
% dig ANY box.

; <<>> DiG 9.10.3-P4-Debian <<>> ANY box.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14573
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 24, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;box. IN ANY

;; ANSWER SECTION:
box. 3600 IN A 127.0.53.53
box. 3600 IN SRV 10 10 0 your-dns-needs-immediate-attention.box.
box. 3600 IN TXT "Your DNS configuration needs immediate attention see https://icann.org/namecollision"
box. 3600 IN MX 10 your-dns-needs-immediate-attention.box.
box. 900 IN SOA a.nic.box. support.ariservices.com. (
1478481375 ; serial
1800       ; refresh (30 minutes)
300        ; retry (5 minutes)
1814400    ; expire (3 weeks)
1800       ; minimum (30 minutes)
)
box. 172800 IN NS b.nic.box.
box. 172800 IN NS d.nic.box.
box. 172800 IN NS c.nic.box.
box. 172800 IN NS a.nic.box.
[...]
;; Query time: 89 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Nov 21 17:23:17 CET 2016
;; MSG SIZE  rcvd: 2938
```

Ces enregistrements ont pour but d'attirer l'attention des utilisateurs sur le risque de collision. Le TLD étant récent et pas encore peuplé, il ne devrait pas y avoir de requêtes DNS. S'il y en a quand même, c'est peut-être le résultat d'une collision avec un usage local. L'adresse IP `127.0.53.53` est une adresse locale à la machine. Si M. Michu tente de se connecter à `http://quelquechose.box/` aujourd'hui, il sera redirigé vers la machine locale. Il verra une erreur (pas de serveur HTTP qui écoute) ou bien la

page Web par défaut de sa machine (avec un message peu informatif comme « "*It works*" ») s'il y a un serveur HTTP. Si l'utilisateur regarde les enregistrements SRV, MX ou TXT, ou bien si un administrateur système regarde les requêtes DNS qui passent, ou bien les journaux du serveur de messagerie, peut-être comprendra-t-il qu'il doit agir. (Je trouve personnellement que la probabilité que cela arrive est assez faible.)

L'atelier lui-même, financé par Verisign (l'entreprise qui avait le plus crié « au loup » sur les "*name collisions*"), s'est donc tenu du 8 au 10 mars à Londres. Un site Web <http://namecollisions.net/> avait été mis en place pour cet atelier, et il contient les supports et les vidéos <http://namecollisions.net/program/index.html>.

Je ne vais pas décrire tous les exposés de l'atelier, la liste complète figure dans l'annexe C du RFC, et les supports sont en ligne <http://namecollisions.net/program/index.html>. Le RFC note qu'il y a eu plusieurs interventions sur la qualité des données du DITL ("*Day in the Life of the Internet*") : il est trivial de les polluer (le DITL est annoncé publiquement, et à l'avance) par des requêtes artificielles. Aucune preuve n'a été trouvée d'une manipulation délibérée. De toute façon, les données montrent surtout qu'il y a beaucoup de n'importe quoi dans le trafic que reçoivent les serveurs racine (par exemple des requêtes avec le bit RD - "*Recursion Desired*" - alors que les serveurs de la racine ne sont pas récursifs). Cela peut être le résultat de bogues dans les résolveurs, de tests ou bien d'attaques délibérées.

La question de l'éducation des utilisateurs est revenue plusieurs fois. Faut-il s'inspirer du téléphone ou du système postal, qui ont tous les deux connu des changements qui nécessitaient une adaptation de l'utilisateur, qui s'est faite par le biais d'importantes campagnes de sensibilisation et d'éducation ?

Le comité de programme avait conclu que le sujet était loin d'être épuisé. Manque de données, manque de théories explicatives, manque d'intérêt pour la question, en tout cas, celle-ci restait largement ouverte après l'atelier (et je ne suis personnellement pas sûr que cela soit mieux aujourd'hui, plus de deux ans après l'atelier de Londres).