Google détourné par Orange vers la place Beauvau

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 17 octobre 2016

https://www.bortzmeyer.org/google-detourne-par-orange.html

Aujourd'hui, bien des clients d'Orange ont eu la mauvaise surprise de ne pas pouvoir visiter Google. La plupart n'avaient pas de messages d'erreur précis, juste une longue attente et un message d'erreur vague du genre « "*timeout*" ». Certains avaient la désagréable surprise de voir apparaitre une page menaçante, les accusant d'avoir voulu se connecter à un site Web terroriste. À l'origine de ce problème, une erreur de configuration dans les résolveurs <https://www.bortzmeyer.org/resolveur-dns.html> DNS d'Orange, en raison de la fonction de censure administrative du Web.

D'abord, voyons l'étendue du problème. Il n'affectait que les clients d'Orange, et seulement ceux qui utilisaient les résolveurs <https://www.bortzmeyer.org/resolveur-dns.html> DNS de l'opérateur (voir plus loin pour une définition des termes techniques). Les sites inaccessibles incluaient , mais aussi , et quelques autres. Beaucoup d'utilisateurs ont imputé le problème à Google à tort (mot-croisillon #GoogleDown sur Twitter, ce qui était complètement erroné).

Il est rapidement apparu que le problème venait du DNS. Ce système permet d'associer à un nom de domaine (comme www.afnic.fr ou youtube.com) des données techniques, comme l'adresse IP de la machine serveuse. Cette adresse IP est indispensable au bon fonctionnement de l'Internet. Résoudre (traduire) un nom de domaine en adresse IP est le travail de deux sortes de serveurs DNS : les serveurs **faisant autorité <https://www.bortzmeyer.org/resolveur-dns.html>**, qui connaissent le contenu d'une partie du DNS (par exemple, les serveurs faisant autorité gérés par l'AFNIC connaissent le contenu de .fr, les serveurs faisant autorité pour cfeditions.com connaissent le contenu de cfeditions.com, etc), et les **résolveurs <https://www.bortzmeyer.org/resolveur-dns.html>**. Ces derniers ne connaissent rien mais, demandant aux serveurs faisant autorité, et mémorisant leur réponse (ce que les informaticiens appellent, bizarrement, « cacher »), ils obtiennent l'information qu'ils distribuent aux utilisateurs. Les résolveurs sont typiquement gérés par les FAI (comme Orange) mais il existe aussi des serveurs publics comme ceux de FDN <https://www.fdn.fr/actions/dns/>. L'utilisateur de l'Internet n'a en général pas à s'en soucier, son FAI lui indique automatiquement ses résolveurs et tout roule.

Normalement, donc, un résolveur n'a pas de données propres et se contente de relayer entre l'utilisateur et le serveur faisant autorité. Mais, comme quasiment toute communication Internet commence

par une requête DNS, il est tentant, lorsqu'on souhaite contrôler l'usage de l'Internet, de demander aux résolveurs de mentir <https://www.bortzmeyer.org/dns-menteur.html>, c'est-à-dire de donner une information qui n'est pas celle venue du serveur faisant autorité. C'est ce qui est prévu en France en application du décret n° 2015-125 du 5 février 2015 <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030195477&dateTexte=&categorieLien=id>. Le Ministère de l'Intérieur envoie aux principaux FAI une liste des domaines à bloquer (un article de Numérama détaille ce processus <http://www.numerama.com/tech/202058-orange-pourquoi-une-erreu html>) et ceux-ci déploient la configuration nécessaire dans leurs résolveurs.

Mais, ce lundi matin, lorsqu'on interrogeait les résolveurs d'Orange au sujet de l'adresse IP de www.google.fr, au lieu de répondre avec l'adresse contenue dans les serveurs faisant autorité pour google.fr (serveurs gérés par Google), par exemple 216.58.211.99, ils répondaient 90.85.16.52, une adresse appartenant à un sous-traitant du Ministère de l'Intérieur <https://www.bortzmeyer.org/censure-francaise.html>. Lorsqu'un navigateur Web se connecte à cette adresse, il obtient normalement une page l'avertissant que le nom de domaine fait partie de ceux qui sont bloqués, et un motif est indiqué (promotion du terrorisme, par exemple, comme dans l'image ci-dessus).

Mais ce serveur était bien trop faible pour encaisser l'énorme trafic de Google et de Wikipédia, et a vite cessé de fonctionner correctement. C'est ce qui explique l'absence de réponse fréquemment rencontrée, faisant croire aux utilisateurs que Google était en panne. (Une autre raison est que la plupart des accès à Google se font désormais en HTTPS et que le serveur du Ministère ne gère pas HTTPS, ne répondant pas, même pas par un refus de connexion.)

Comment une telle bavure a pu se produire ? L'erreur était-elle dans la liste envoyée par le Ministère de l'Intérieur ou bien uniquement chez Orange ? On n'a évidemment pas d'information à ce sujet (les pannes Internet ne font jamais l'objet d'analyses indépendantes et publiques, ce qui explique que la sécurité ne progresse guère). Tout est possible, y compris des erreurs humaines qui sembleraient invraisemblables (mais on voit vraiment de tout dans le monde réel). Une des hypothèses les plus intéressantes (elle explique notamment pourquoi il y a eu plusieurs noms touchés) est celle d'un fichier de test installé par erreur <http://www.macg.co/logiciels/2016/10/googlefr-bloque-par-orange-que-sest-il-p à la place du « bon ».

Au fait, comment sait-on que les clients d'Orange (et uniquement eux) recevaient cette fausse information ? En effet, dans l'Internet d'aujourd'hui, complexe et international, une observation faite en un point n'est pas suffisante. Les clients d'Orange peuvent s'exclamer en chœur « Google est planté » et ceux de Free répondre « non, tout va bien ici ». Et les deux groupes ont raison... de leur point de vue. J'ai utilisé, outre les mesures faites par des experts chez différents FAI (merci, merci, merci), le réseau des sondes RIPE Atlas <https://atlas.ripe.net/>. Ces petits boitiers très utiles <https://labs.ripe.net/Members/stephane_bortzmeyer/orange-blacklisting-a-case-for-measuring-censorsh permettent de mesurer un certain nombre d'indicateurs techniques depuis de nombreux points du réseau. (Des détails pour les techniciens figurent à la fin de cet article.)

La panne elle-même, c'est-à-dire l'envoi de fausses informations par les résolveurs DNS d'Orange, a duré environ une heure. Mais son effet avait été prolongé par la mémorisation (les fameux « caches ») des informations dans certains composants du réseau (par exemple la « "*box*" » chez l'utilisateur). Cela fait que, plusieurs heures après, Google ou Wikipédia étaient toujours inaccessibles pour certains utilisateurs.

Les leçons à en tirer ? Le DNS est un composant critique de l'Internet et sa résilience, sa capacité à résister aux pannes et à repartir ensuite, est donc cruciale. D'où l'importance de l'Observatoire de la résilience Internet <https://www.afnic.fr/fr/expertises/labs/projets-realises/l-observatoire-de-la-resilience-de-l-internet-en-france.html>. Toute interférence

avec le fonctionnement du DNS, que ce soit pour des raisons politiques ou autres, le met potentiellement en péril. C'est ce qu'avait analysé le rapport du Conseil Scientifique de l'AFNIC « Conséquences du filtrage Internet par le DNS <https://www.afnic.fr/fr/l-afnic-en-bref/actualites/actualites-generales/6573/show/le-conseil-scientifique-de-l-afnic-partage-sur-le-filtrage.html> », qui mettait bien en évidence le risque de tels filtrages ou blocages. Une bavure analogue à celle de Google était déjà arrivée au Danemark <http://www.computerworld.dk/art/214431/koks-hos-dansk-politi-spaerrer-for-8-000-websites> mais il semble que personne ne tire de leçons de l'expérience.

Que peuvent faire les utilisateurs face à de tels risques ? Le problème de fond est bien évidemment politique (la censure administrative, effectuée au mépris des contraintes opérationnelles) et doit donc être traité politiquement. Mais existe-t-il des solutions techniques ? Pour l'instant, la meilleure est d'avoir son propre résolveur DNS <https://www.bortzmeyer.org/son-propre-resolveur-dns.html>. Notez bien que je ne parle pas forcément d'un résolveur par machine à la maison. Cela peut être fait dans un équipement partagé, comme ce que permet le routeur Turris Omnia <https://www.turris.cz/en/>. Beaucoup de gens proposaient d'utiliser un résolveur DNS public. Ce n'est pas forcément une bonne solution. Google Public DNS <https://www.bortzmeyer.org/google-dns.html> a tous les inconvénients des services Google (bien expliqués dans le récent livre de Tristan Nitot <https://www.bortzmeyer.org/surveillance.html>). Cisco OpenDNS <https://www.bortzmeyer.org/opendns-non-merci.html> y ajoute le fait qu'il s'agit d'un résolveur menteur, comme ceux des principaux FAI français. Ceux d'OpenNIC <https://www.opennicproject.org/> marchent rarement et, de toute façon, sont une racine alternative <https://www.bortzmeyer.org/racines-alternatives.html>, avec les inconvénients que cela présente. Et les résolveurs de FDN <https://www.fdn.fr/actions/dns/> ? Ils sont honnêtes mais ils partagent un inconvénient commun avec presque tous les résolveurs DNS publics : ils n'offrent aucune authentification et rien ne garantit donc qu'on parle bien au résolveur qu'on veut. (C'est ainsi que Google Public DNS a déjà été détourné <https://www.bortzmeyer.org/dns-routing-hijack-turkey.html>.)

Quelques lectures sur cet incident :

— Le communiqué de presse du Ministère de l'Intérieur <http://www.interieur.gouv.fr/Actualites/L-actu-du-Ministere/Redirection-vers-la-page-de-blocage-des-sites-terrori> (avec une erreur sur la date), et une copie locale (en ligne sur https://www.bortzmeyer.org/files/ministere-interieur-censure-google.jpg) (au cas où le Ministère regrette d'avoir avoué qu'il collectait les adresses IP des visiteurs et ne change son communiqué),
— Très bon article sur NextInpact <http://www.nextinpact.com/news/101786-google-fr-bloque-pour-a> htm>,
— Bon résumé dans Numérama <http://www.numerama.com/tech/202005-google-est-parfois-bloque-> html>,
— L'article du Monde <http://www.lemonde.fr/pixels/article/2016/10/17/une-erreur-bloque-l-a> 5014900_4408996.html> rappelle le contexte politique,
— Un amusant fil de discussion sur un forum Orange <https://communaute.orange.fr/t5/ma-connexion/Impossible-de-faire-une-recherche-sur-internet-alors-que-je-suis/m-p/1090708>,
— Une discussion chez Reddit <https://www.reddit.com/r/france/comments/57wiv8/googlefr_bloqu%C3%A9_pour_apologie_du_terrorisme_suite/>.

Le reste de cet article est uniquement pour les techniciens, attention. Le script utilisé pour interroger les sondes Atlas est décrit ici <https://labs.ripe.net/Members/stephane_bortzmeyer/dns-censorship-dns-lies-seen-by-atlas-probes>. La commande exacte était `atlas-resolve --as 3215 --requested 100 www.google.fr`, l'AS 3215 étant celui d'Orange.

La panne semble avoir duré d'environ 07 :40 UTC à 08 :35. Un utilisateur d'Orange qui testait avec dig voyait :

```
% dig A +short @192.168.10.1 www.google.fr
90.85.16.52

% dig A +short @8.8.8.8 www.google.fr
172.217.20.35
```

Les sondes Atlas, elles, voyaient :

```
% atlas-resolve --as 3215 -r 100 www.google.fr
[74.125.24.94] : 1 occurrences
[216.58.208.195] : 2 occurrences
[74.125.206.94] : 2 occurrences
[216.58.210.35] : 2 occurrences
[216.58.210.227] : 3 occurrences
[216.58.211.67] : 3 occurrences
[172.217.16.67] : 2 occurrences
[216.58.213.35] : 1 occurrences
[216.58.211.99] : 2 occurrences
[172.217.18.227] : 2 occurrences
[216.58.204.3] : 1 occurrences
[90.85.16.52] : 75 occurrences
[216.58.208.227] : 2 occurrences
Test #6886264 done at 2016-10-17T08:06:14Z
```

Remarquez que certaines sondes, minoritaires, voient la vraie valeur, sans doute parce que le réseau où elles sont situées n'utilise pas les résolveurs DNS d'Orange. Mais la grande majorité voit le `90.85.16.52` mensonger. Un autre exemple avec les sondes Atlas, mais en leur demandant d'utiliser un autre résolveur (Google Public DNS) :

```
 % atlas-resolve --as 3215 -r 100 -e 8.8.4.4 www.google.fr
Nameserver 8.8.4.4
[172.217.18.227] : 3 occurrences
[216.58.219.67] : 1 occurrences
[172.217.23.67] : 1 occurrences
[216.58.210.3] : 1 occurrences
[216.58.211.67] : 8 occurrences
[172.217.16.67] : 3 occurrences
[216.58.210.163] : 1 occurrences
[172.217.16.163] : 2 occurrences
[172.217.19.131] : 8 occurrences
[216.58.201.35] : 4 occurrences
[74.125.206.94] : 4 occurrences
[216.58.213.99] : 1 occurrences
[172.217.23.99] : 1 occurrences
[172.217.20.35] : 5 occurrences
[216.58.208.227] : 10 occurrences
[216.58.210.131] : 1 occurrences
[216.58.204.67] : 2 occurrences
[216.58.211.99] : 11 occurrences
[216.58.210.227] : 8 occurrences
[216.58.212.99] : 2 occurrences
[172.217.23.3] : 1 occurrences
[216.58.204.3] : 1 occurrences
[216.58.208.163] : 1 occurrences
[216.58.210.195] : 6 occurrences
[216.58.192.99] : 1 occurrences
[216.58.208.195] : 10 occurrences
Test #6886273 done at 2016-10-17T08:13:06Z
```

Cette fois, personne ne voit le mensonge (notez que les serveurs DNS de Google servent des réponses très différentes, mais qui sont toutes dans un réseau Google). Notez aussi que d'autres services Google comme Gmail ou comme le "*spyware*" Analytics n'avaient aucun problème.

Wikipédia faisait partie des victimes, comme Google :

```
% atlas-resolve --as 3215 -r 100 fr.wikipedia.org
[91.198.174.192] : 21 occurrences
[90.85.16.52] : 73 occurrences
[208.80.154.224] : 1 occurrences
Test #6886283 done at 2016-10-17T08:22:22Z
```

Merci à tou[Caractère Unicode non montré [1]]te[Caractère Unicode non montré]s c[Caractère Unicode non montré]eux[Caractère Unicode non montré]elles qui m'ont envoyé des informations et des résultats de mesure. Ça, c'est l'Internet, la coopération, l'échange d'informations et la décentralisation.

1. Car trop difficile à faire afficher par LaTeX