Go Daddy planté, une des plus grosses pannes dans le DNS

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 10 septembre 2012. Dernière mise à jour le 5 octobre 2012

https://www.bortzmeyer.org/go-daddy-down.html

Go Daddy est de loin le plus gros bureau d'enregistrement de .com et de nombreux autres TLD. Il sert aussi d'hébergeur DNS. Ce soir, tous leurs serveurs de noms sont injoignables, entraînant l'impossibilité de joindre des millions de noms de domaine, et donc les serveurs situés derrière. C'est l'une des plus grandes pannes qu'ait jamais connu le DNS. Elle illustre une nouvelle fois l'importance de s'assurer de la **résilience** de son service DNS, notamment par le biais de la **redondance**.

Le lundi 10 septembre, il est 19h00 UTC et la panne dure depuis déjà un certain temps (premier signalement sur la liste "*outages*" vers 18h00 UTC). Prenons un hasard un nom de domaine hébergé chez Go Daddy, 1stoptr.com. Tentons une interrogation :

```
% dig A 1stoptr.com

; <<>> DiG 9.8.1-P1 <<>> A 1stoptr.com
;; global options: +cmd
;; connection timed out; no servers could be reached
```

Pas de réponse. Qu'arrive-t-il aux serveurs de noms ? Demandons au parent (VeriSign) les serveurs de noms de 1stoptr.com :

```
% dig @a.gtld-servers.net NS 1stoptr.com

; <<>> DiG 9.8.1-P1 <<>> @a.gtld-servers.net NS 1stoptr.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38711
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 3
;; WARNING: recursion requested but not available
```

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;1stoptr.com.                   IN      NS

;; AUTHORITY SECTION:
1stoptr.com.            172800  IN      NS      wsc1.jomax.net.
1stoptr.com.            172800  IN      NS      wsc2.jomax.net.
...
;; ADDITIONAL SECTION:
wsc1.jomax.net.         172800  IN      A       216.69.185.1
wsc2.jomax.net.         172800  IN      A       208.109.255.1
```

Ces deux serveurs sont bien chez Go Daddy comme on peut le vérifier avec whois :

```
% whois 216.69.185.1
#
# The following results may also be obtained via:
# http://whois.arin.net/rest/nets;q=216.69.185.1?showDetails=true&showARIN=false&ext=netref2
#

NetRange:       216.69.128.0 - 216.69.191.255
CIDR:           216.69.128.0/18
OriginAS:
NetName:        GO-DADDY-COM-LLC
NetHandle:      NET-216-69-128-0-1
Parent:         NET-216-0-0-0-0
NetType:        Direct Allocation
...
```

Et ils ne répondent pas :

```
%  dig @216.69.185.1  A 1stoptr.com

; <<>> DiG 9.7.3 <<>> @216.69.185.1 A 1stoptr.com
; (1 server found)
;; global options: +cmd
;; connection timed out; no servers could be reached
```

Et, surtout, c'est la même chose pour tous les serveurs de noms de Go Daddy. Le domaine de l'hébergeur lui-même, `godaddy.com` n'est pas davantage accessible :

```
% dig +nodnssec +nssearch godaddy.com

; <<>> DiG 9.7.3 <<>> +nodnssec +nssearch godaddy.com
;; global options: +short +cmd
;; connection timed out; no servers could be reached
```

Et comme pas de DNS égal pas de Web, ni d'autres services, on voit l'ampleur de la panne... Celle-ci a duré jusqu'à environ 20h40 UTC, où il y a eu une légère rémission, avant que cela ne re-plante. Finalement, le service a été rétabli quelques heures après (apparemment en migrant une partie de l'infrastructure sur la plate-forme de VeriSign). C'est donc assez long, même en cas de dDoS.

Que s'est-il passé ? Sur le moment, une personne se prétendant Anonymous a revendiqué l'action. Mais n'importe qui peut envoyer un tweet et, comme il ne donnait aucun détail technique, il était donc difficile de savoir si c'est vrai. La première déclaration officielle de Go Daddy <http://www.godaddy.com/newscenter/release-view.aspx?news_item_id=410> incriminait un problème technique interne dans leurs routeurs. L'hypothèse d'une attaque par déni de service distribué aussi réussie contre une infrastructure "*anycastée*" était certes possible mais, quand même, cela aurait en effet très difficile à réussir.

Au fait, pourquoi Anonymous aurait-il attaqué Go Daddy ? Peut-être parce qu'ils aiment les éléphants <http://www.huffingtonpost.com/2011/03/31/bob-parsons-godaddy-ceo-elephant-hunt_n_843121.html> ? Ou parce qu'ils sont choqués des publicités de mauvais goût de Go Daddy, à base de pinups vulgaires en bikini ? Mais Go Daddy est aussi connu pour son soutien à SOPA (voir Wikipédia), et pour être un des hébergeurs les plus rapides à censurer ses clients lorsque le gouvernement ou l'industrie du divertissement le demande (voir l'affaire JotForm <http://arstechnica.com/tech-policy/2012/02/secret-service-asks-for-shutdown-of-legit-website-over-user-content-g> ou celle de RateMyCop <http://www.wired.com/threatlevel/2008/03/godaddy-silence/>). Comme disent les policiers, il y a donc beaucoup trop de suspects...

Finalement, le 5 octobre, Go Daddy a publié un rapport technique très détaillé <http://inside.godaddy.com/inside-story-happened-godaddy-com-sept-10-2012/>. Le problème (si on prend ce rapport au pied de la lettre mais il semble cohérent avec les faits observés) était bien dans les routeurs. Une combinaison d'incidents avait entraîné l'apparition d'un très grand nombre de routes, dépassant la capacité de la table de routage. Ces routes ont été propagées en interne, plantant ainsi la totalité des routeurs. Même une fois le problème technique analysé, la correction a été longue car chaque fois qu'un des sites de Go Daddy repartait, tout le trafic se précipitait vers lui... et le replantait.

Autres articles :

- "*GoDaddy's DNS Servers Down, Taking Thousands of Sites With It*" <http://mashable.com/2012/09/10/godaddy-down/>
- "*GoDaddy Outage Takes Down Millions Of Sites, Anonymous Member Claims Responsibility* " <http://techcrunch.com/2012/09/10/godaddy-outage-takes-down-millions-of-sites/>
- "*GoDaddy Gone : Can the Domain Giant Recover Its Reputation ?*" <http://mashable.com/2012/09/10/godaddy-gone-recover-its-reputation/>
- Numérama, après qu'il semble bien qu'il ne s'agissait pas d'une attaque : GoDaddy dément toute attaque et parle d'un incident interne <http://www.numerama.com/magazine/23695-godaddy-dement-to html>,
- Un article de Wired, "*Amid Outage, GoDaddy Moves DNS to Competitor VeriSign*" <http://www.wired.com/wiredenterprise/2012/09/godaddy-moves-to-verisign/>, qui contient une énorme erreur dans le titre (VeriSign n'est pas bureau d'enregistrement et donc pas concurrent de GoDaddy).
- Bon article de synthèse d'Ars Technica, "*GoDaddy outage makes websites unavailable for many Internet users*" <http://arstechnica.com/security/2012/09/godaddy-outage-makes-websites-unavai>, gâché par la même erreur que celui de Wired,
- Le blogueur de DomainNameWire a raison de faire remarquer <http://domainnamewire.com/2012/09/11/like-i-was-saying-go-daddy-wasnt-hacked/> que les journalistes devraient avoir honte : tous ont négligé le problème réel (des millions de gens ne pouvant accéder à un service) et ont sauté sur l'hypothèse, certes plus juteuse, d'une attaque d'un "*hacker*". Et cela sur la base d'un seul et unique tweet !

— Un bon exemple de baratin intégral, avec quasiment aucun fait vérifié : "*Anonymous Hacker take down GoDaddy with IRC Bots*" <http://thehackernews.com/2012/09/anonymous-hacker-take-down
html>. Encore mieux, la proclamation par un neuneu total qu'il a publié le code source de Go Daddy <http://cylaw.info/?p=1133> alors que le fichier RAR téléchargé contient une copie d'un logiciel libre public <https://code.google.com/p/ttpython/source/browse/#svn%2Ftrunk%2Fgodaddy>, et une configuration bidon avec des serveurs dont l'adresse IP est en Chine (ce qui serait étonnant de la part de Go Daddy).

Une amusante ligne de script shell pour détecter si un de vos sites Web dépend de Go Daddy (merci à climagic <https://twitter.com/climagic/>). À exécuter dans le répertoire où se trouve la config Apache :

```
grep ServerName * | grep -io "[a-z0-9-]*\.[a-z]*$" | \
     sort -u | while read -r d; do whois $d | grep -q "GODADDY" &&echo $d; done # site check
```