Sur une panne DNS, et sur les leçons à en tirer (BNP Paribas)

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 20 juin 2017. Dernière mise à jour le 22 juin 2017

https://www.bortzmeyer.org/panne-dns-bnpparibas.html

Ce matin du 20 juin, plein de messages sur les réseaux sociaux pour se plaindre d'une impossibilité d'accéder aux services en ligne de BNP Paribas. Le CM a bien du mal <https://twitter.com/BNPParibas_SAV/status/877062495780864000> à répondre à tout le monde. À l'origine de cette panne, un problème DNS. Que s'est-il passé et pourquoi ?

Les noms de domaine utilisés par BNP Paribas sont tous dans le TLD `.bnpparibas`. On peut facilement vérifier que ce TLD va bien (un seul serveur ne répond pas) :

```
% check-soa -i bnpparibas
a0.nic.bnpparibas.
2a01:8840:3e::9: OK: 1000002072 (241 ms)
65.22.64.9: OK: 1000002072 (91 ms)
a2.nic.bnpparibas.
65.22.67.9: OK: 1000002072 (3 ms)
2a01:8840:41::9: OK: 1000002072 (3 ms)
b0.nic.bnpparibas.
2a01:8840:3f::9: OK: 1000002072 (19 ms)
65.22.65.9: OK: 1000002072 (27 ms)
c0.nic.bnpparibas.
2a01:8840:40::9: OK: 1000002072 (21 ms)
65.22.66.9: ERROR: read udp 10.10.86.133:33849->65.22.66.9:53: i/o timeout
```

Mais c'est en dessous qu'il y a des problèmes. En raison de règles ICANN absurdes, les noms publiés sont tous des sous-domaines de `.bnpparibas`, délégués à deux serveurs de noms :

```
% dig @a2.nic.bnpparibas. NS mabanqueprivee.bnpparibas
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51136
...
;; AUTHORITY SECTION:
mabanqueprivee.bnpparibas. 86400 IN NS sns5.bnpparibas.net.
mabanqueprivee.bnpparibas. 86400 IN NS sns6.bnpparibas.net.
...
;; SERVER: 2a01:8840:41::9#53(2a01:8840:41::9)
;; WHEN: Tue Jun 20 09:55:22 CEST 2017
```

Et, de ces deux serveurs de noms, l'un n'existe pas, l'autre est en panne (ou bien victime d'une attaque par déni de service) :

```
% check-soa -i -ns sns5.bnpparibas.net\ sns6.bnpparibas.net mabanqueprivee.bnpparibas
sns5.bnpparibas.net.
159.50.249.65: ERROR: read udp 10.10.86.133:57342->159.50.249.65:53: i/o timeout
sns6.bnpparibas.net.
Cannot get the IPv4 address: NXDOMAIN
```

On peut aussi tester avec dig, si vous préférez :

```
% dig @sns5.bnpparibas.net. NS mabanquepro.bnpparibas

; <<>> DiG 9.10.3-P4-Debian <<>> @sns5.bnpparibas.net. NS mabanquepro.bnpparibas
; (1 server found)
;; global options: +cmd
;; connection timed out; no servers could be reached

% dig @sns6.bnpparibas.net. NS mabanquepro.bnpparibas
dig: couldn't get address for 'sns6.bnpparibas.net.': not found
```

C'est assez étonnant. Un des deux serveurs n'existe même pas dans le DNS. D'après DNSDB <https://www.bortzmeyer.org/dnsdb.html>, il n'a même jamais existé ! Tous les noms de BNP Paribas (`mabanqueprivee.bnpparibas`, `mabanquepro.bnpparibas`, etc) dépendaient donc d'un seul serveur, qui a défailli ce matin.

Résultat, les utilisateurs ne pouvaient pas résoudre le nom en adresse et donc pas accéder au site Web ou à l'API. On le voit avec les sondes RIPE Atlas <https://atlas.ripe.net/> :

```
% atlas-resolve -r 100 mabanqueprivee.bnpparibas.
[ERROR: SERVFAIL] : 48 occurrences
[TIMEOUT(S)] : 50 occurrences
Test #8925333 done at 2017-06-20T07:55:45Z
```

La reprise a été partielle (plusieurs serveurs "*anycastés*" ? Attaque par déni de service qui se calme ?), un peu plus tard, on voit que certaines sondes réussissaient :

```
% atlas-resolve -r 100 mabanquepro.bnpparibas.
[159.50.188.21] : 3 occurrences
[ERROR: SERVFAIL] : 51 occurrences
[TIMEOUT(S)] : 40 occurrences
Test #8925337 done at 2017-06-20T07:58:24Z
```

Pour le serveur inexistant, l'explication m'a été donnée par un anonyme (que je remercie beaucoup) : le vrai nom est `sns6.bnpparibas.FR` (et pas `.NET`). Ce serveur existe bien, répond, et fait en effet autorité <`https://www.bortzmeyer.org/serveur-dns-faisant-autorite.html`> pour les zones de la banque. Lors de la délégation de la plupart des sous-domaines, c'est simplement un mauvais nom qui a été indiqué !

Tout ceci n'est pas très conforme aux bonnes pratiques (telles qu'elles sont régulièrement rappelées, par exemple, dans le rapport annuel sur la résilience de l'Internet français <`https://www.ssi.gouv.fr/agence/rayonnement-scientifique/lobservatoire-de-la-resilience-de-linternet-francais/`>) :

— Deux serveurs DNS faisant autorité, ce n'est en général pas assez (surtout si un des deux n'existe en fait pas),
— Les serveurs doivent être supervisés. Icinga ou Zabbix auraient prévenu depuis longtemps qu'un des deux serveurs ne marchait pas.
— Les configurations DNS doivent être testées, par exemple avec Zonemaster <`https://zonemaster.net/`>.
— Le TTL renvoyé par le serveur, lorsqu'il marche, est de seulement 30 secondes. C'est très insuffisant. En cas de panne imprévue, il faut facilement plusieurs heures pour réparer (l'essentiel du temps étant consacré à paniquer en criant).

Notez que, deux jours après la panne, rien n'a été réparé :

— Les zones n'ont toujours qu'un seul serveur (celui inexistant ne comptant évidemment pas),
— En prime, l'unique serveur répond incorrectement (il accepte les requêtes DNS de type A mais pas celles de types NS ou SOA).

Ces erreurs sont clairement visible sur les programmes de test DNS comme Zonemaster <`https://zonemaster.net/test/a8a67ef3f216b096`> ou bien DNSviz <`http://dnsviz.net/d/mabanqueprivee.bnpparibas/WUjr5A/dnssec/`>.