Le coupable d'un problème de réseau n'est pas toujours celui qu'on croit

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 19 octobre 2015

https://www.bortzmeyer.org/dnssec-qui-est-coupable.html

Le lancement raté d'un site Web gouvernemental (détails plus loin, analyse technique détaillée à la fin) est l'occasion de revenir sur un phénomène qui arrive assez souvent lorsqu'une partie de l'Internet est en panne : le coupable désigné sur les réseaux sociaux n'est pas toujours le bon (enfin, le méchant). Notamment, en cas de mauvaise configuration des techniques de sécurité, ceux qui appliquent ces techniques peuvent être « accusés » de la panne, puisque ça continue à marcher chez les « laxistes ».

Le dernier exemple que j'ai en tête s'est produit il y a quelques jours lors du lancement de http://www.images-art.f un site Web gouvernemental de distribution d'images. Ce site est un scandale <https://medium.com/@symac/la-vaste-blague-images-d-art-644e83124136> mais ce n'est pas le problème ici. Le problème est que les gérants du site Web avaient fait une erreur de configuration, et que ce site n'était donc pas visible depuis une partie de l'Internet, notamment depuis Free. La réaction de beaucoup d'utilisateurs avait été de reprocher ce problème à Free puisque « ça marche chez les autres ». Mais c'était injuste. En effet, Free est un des rares FAI français à déployer DNSSEC, une technique de sécurité qui vise à protéger les utilisateurs contre certaines attaques sur le réseau. Malheureusement, la plupart des autres FAI ne se soucient pas de sécurité et n'ont pas déployé cette technique. (Si vous préférez des exemples états-uniens, un incident similaire s'était produit lorsque la NASA avait cafouillé dans sa configuration, et que Comcast, principal FAI à utiliser DNSSEC, avait été accusé, bien à tort, de bloquer la NASA <http://www.internetsociety.org/deploy360/blog/2012/01/comcast-releases-detailed-analysis-of-nasa-gov-dnssec-validation-failure/>.)

Or, le nom de domaine images-art.fr avait un problème de configuration. Cela le rendait invisible depuis les opérateurs qui mettaient en œuvre DNSSEC (Free mais aussi Google Public DNS). En effet, ce problème de configuration était indistinguable d'une attaque.

Et c'est là un paradoxe fréquent de la sécurité : la sécurité gêne les utilisateurs. Imaginons un petit village qui n'a jamais connu de cambriolage. Les habitants ne ferment pas la porte à clé ou, quand ils le font, ils laissent la clé sous le pot de fleurs près de l'entrée. Maintenant, si la situation change et qu'il commence à y avoir quelques cambriolages, certains habitants vont commencer à faire plus attention. Et

les ennuis commenceront parce que, pour un cambriolage évité grâce à une porte fermée, il y aura dix ou vingt incidents dus à la sécurité : une personne claque la porte en laissant la clé dedans, une autre a oublié qu'un membre de sa famille devait passer et n'avait pas la clé, un troisième perd la clé dans la journée... Tous réagiront probablement au début en disant « la sécurité, c'est pénible » (ce qui est parfaitement exact).

Quittons notre histoire et revenons à l'Internet. `images-art.fr` a cafouillé (voir l'analyse technique détaillée plus loin). Mais ce cafouillage n'a eu aucune conséquence chez les FAI qui ne vérifient pas. Ils n'ont pas de quoi s'en vanter. Bien au contraire, ils laissent leurs utilisateurs vulnérables. Et ce sont donc Free ou Google qui avaient raison : les mesures de sécurité déployées étaient bonnes, la responsabilité de la panne n'était pas chez eux. Notons que ce problème n'a rien de spécifique à DNSSEC et que, par exemple, HTTPS (le petit cadenas et la barre verte...) connait largement autant de semblables « bavures ».

Pour les techniciens, voici maintenant quelques informations concrètes. La panne était due au fait que `images-art.fr` n'était **pas** signé par DNSSEC mais qu'il y avait dans la zone parente (`.fr`) un enregistrement DS ("*Delegation Signer*", un pointeur de la zone parente vers la clé de la zone fille, celui-ci pointait vers la clé 60840). Cet enregistrement DS est interprété par les résolveurs DNSSEC comme voulant dire « la zone est signée ». Si le résolveur découvre qu'elle ne l'est pas, il interprète cela comme une attaque. Pourquoi cette erreur ? On peut supposer plein de choses mais je note en examinant DNSDB <`https://www.bortzmeyer.org/dnsdb.html`> que le DS n'a jamais changé alors que les clés dans la zone (et les signatures) ne sont apparues que le 19 octobre dans l'après-midi. Il est donc probable que la zone était prévue pour être signée, mais que c'est la zone non signée qui a été publiée, sans que cela n'empêche l'administrateur système de publier le DS, sans avoir vérifié (la plupart des professionnels ne testent jamais la configuration qu'ils déploient). Une hypothèse proche était que le processus (signature + envoi du DS au registre) était automatisé mais que le programme avait une bogue : l'échec de la signature n'a pas suspendu la publication du DS.

Voici ce que montraient deux logiciels de débogage DNSSEC au moment de la panne : ZoneMaster <`https://zonemaster.net/test/40381`> (« "*Server at 46.105.206.200 sent 2 DNSKEY records, and 0 RRSIG records*" ») et DNSviz <`http://dnsviz.net/d/images-art.fr/ViTnig/dnssec/`>. Voici ce que voyait l'outil dig, d'abord avec Google Public DNS :

```
% dig @8.8.8.8 www.images-art.fr

; <<>> DiG 9.9.5-12-Debian <<>> @8.8.8.8 www.images-art.fr
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 11922
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;www.images-art.fr.     IN A

;; Query time: 24 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Mon Oct 19 15:30:06 CEST 2015
;; MSG SIZE  rcvd: 46
```

Le code `SERVFAIL` signifie "*Server Failure*". Si on demande à Google de ne **pas** valider avec DNSSEC (CD = "*Checking Disabled*") :

```
% dig +cd @8.8.8.8 www.images-art.fr

; <<>> DiG 9.9.5-12-Debian <<>> +cd @8.8.8.8 www.images-art.fr
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4472
;; flags: qr rd ra cd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;www.images-art.fr.     IN A

;; ANSWER SECTION:
www.images-art.fr.      3599 IN A 213.186.33.5

;; Query time: 15 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Mon Oct 19 15:30:09 CEST 2015
;; MSG SIZE  rcvd: 62
```

C'était une autre preuve que le problème avait un lien avec DNSSEC. Essayons ensuite chez Free avec le résolveur de la Freebox :

```
% dig www.images-art.fr

; <<>> DiG 9.10.2-P2 <<>> www.images-art.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 52045
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;www.images-art.fr.     IN A

;; Query time: 51 msec
;; SERVER: 192.168.2.254#53(192.168.2.254)
;; WHEN: Mon Oct 19 15:34:37 CEST 2015
;; MSG SIZE  rcvd: 46


% dig +cd www.images-art.fr

; <<>> DiG 9.10.2-P2 <<>> +cd www.images-art.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50409
;; flags: qr rd ra cd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;www.images-art.fr.     IN A

;; ANSWER SECTION:
www.images-art.fr.      3361 IN A 213.186.33.5

;; Query time: 8 msec
;; SERVER: 192.168.2.254#53(192.168.2.254)
;; WHEN: Mon Oct 19 15:34:40 CEST 2015
```

```
;; MSG SIZE  rcvd: 62
```

À noter que ce problème de « fausse alerte » ou de « faux positif » avec DNSSEC a été identifié il y a longtemps. Une des solutions possibles est le "*Negative Trust Anchor*" décrit dans le RFC 7646 [1].

Merci à Kanor pour avoir attiré mon attention sur ce problème <https://twitter.com/KanorUbu/status/656089317039706113>.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc7646.txt