DNSSEC peut-il aider en cas de piratage du registre de noms de domaines ?

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 5 juillet 2013

https://www.bortzmeyer.org/piratage-registre-dnssec.html

Le piratage du registre du .my le 1er juillet, survenant après des mésaventures analogues subies par d'autres registres de noms de domaine, a remis sur le tapis une vieille question : est-ce que DNSSEC peut aider dans un tel cas ? .my est en effet le premier TLD signé à être piraté.

Le bon sens dit que **non** : comme répété souvent par Peter Koch, « "*DNSSEC does not prove that the data is correct, just that it is authentic*" ». Les signatures DNSSEC sont calculées par le registre, sur ses machines, à partir des données contenues dans sa base. Si le pirate a pris le contrôle du système, il a pu modifier la base et, dans ce cas, DNSSEC signera des données incorrectes. DNSSEC protège contre bien des attaques (dont la fameuse attaque Kaminsky <https://www.bortzmeyer.org/comment-fonctionne-la-faille-html>) mais pas contre toutes. Si les données sont fausses, signer prouvera juste que les données fausses étaient bien celles dans la base. GIGO ("*Garbage In, Garbage Out*"). C'est un point important lorsqu'on évalue la sécurité des noms de domaine <http://www.pulsar-informatique.com/Blog/Entry/journee-du-conseil-scientifique-de-lafnic-jcsa-securite-des-noms-de-domaine.html>.

Mais, en creusant un peu la question, on voit que c'est plus compliqué que cela. Gardez bien en tête un rappel, un point important du DNS : les données peuvent rester dans les caches (les résolveurs, sur le réseau local ou chez le FAI) pendant un certain temps, borné par le TTL. Par exemple, ici, je demande à mon résolveur la clé de .fr :

```
% dig DNSKEY fr.
fr. 39110 IN DNSKEY 256 3 8 AwEAA...
fr. 39110 IN DNSKEY 257 3 8 AwEAA...
fr. 39110 IN DNSKEY 257 3 8 AwEAA...
fr. 39110 IN DNSKEY 257 3 8 AwEAA...
```

Et je vois qu'elle va encore rester en mémoire du résolveur pendant 39 110 secondes, plus de 10 heures. Comme le note Olivier Auber, avec DNSSEC, il faut toujours avoir une perspective temporelle. (Revoir quelques épisodes de Doctor Who peut aider.)

Or, mettons nous à la place de l'attaquant : il est maître du système du registre, il a l'accès à la base de données, il peut faire des `UPDATE` ou des `INSERT` tant qu'il veut. Si le domaine qu'il veut modifier est signé, que peut-il faire ? L'attaquant typique, aujourd'hui, ne connait probablement pas DNSSEC, qui est encore trop peu déployé. Il va donc probablement l'ignorer (comme cela avait été fait pour `.my`), et changer les enregistements NS pour les domaines visés. Par exemple, dans le cas de `.my`, DNSdb <https://www.bortzmeyer.org/dnsdb.html> nous montrait ce changement :

```
bailiwick coca-cola.com.my.
count 3
first seen 2013-07-01 04:23:36 -0000
last seen 2013-07-01 07:06:04 -0000
coca-cola.com.my. NS ns1.jealousdesigns.com.
coca-cola.com.my. NS ns2.jealousdesigns.com.
```

Pendant quelques heures, ce domaine avait été redirigé vers d'autres serveurs de noms contrôlés par le méchant (les bons serveurs sont en `ko.com`). Ces serveurs servaient une zone **non signée** où le nom `coca-cola.com.my` avait une adresse qui était celle d'une machine du pirate. La zone étant non signée, si un enregistrement DS avait été dans `com.my` (en fait, `com.my` est bien signé mais `coca-cola.com.my` ne l'est pas ; la suite de mon raisonnement est fait en regardant ce qui se serait passé si `coca-cola.com.my` avait été signé), la zone non signée aurait été considérée comme invalide et les résolveurs validant avec DNSSEC auraient rejeté son contenu. Donc, l'attaquant n'aurait pas atteint son but (qui était de diriger vers une page Web de hameçonnage, ou bien une page Web proclamant ses objectifs politiques ou simplement son ego). À la place, le détournement serait devenu un « simple » déni de service. Donc, dans ce cas (attaquant ignorant), DNSSEC aurait pu aider.

Bon, mais les attaquants vont progresser. Ils vont suivre des cours DNSSEC et faire plus attention la prochaine fois. Quelles sont les possibilités d'un attaquant qui s'y connait ? La première idée est de ne pas seulement modifier les NS mais aussi les DS **et** de servir, sur les serveurs de noms « pirates », une zone signée (avec les clés indiquées par le nouveau DS). Cela va marcher... sauf que le TTL va s'interposer. Voici le DS de `bortzmeyer.fr` dans mon cache :

```
% dig DS bortzmeyer.fr
bortzmeyer.fr. 42507 IN DS 3445 8 2 7CC...
bortzmeyer.fr. 42507 IN DS 44461 8 2 56A...
```

Et on voit qu'il va rester encore 11 heures. L'ancien DS étant dans un certain nombre de caches, la résolution va donc échouer pour ces caches, puisque l'ancien DS pointe vers la zone du pirate, pas signée avec la bonne clé. Ce sera l'équivalent d'un remplacement de clé ("*key rollover*") raté parce qu'on n'a pas bien fait ses calculs de TTL (voir le RFC 6781 [1], mon expérience <https://www.bortzmeyer.org/key-rollover.html> et l'étude montrant que les erreurs existent <https://www.bortzmeyer.org/satin.html>.) **La seule chose que le pirate ne contrôle pas, c'est le Temps.** Et c'est ainsi qu'on peut détecter ses plans diaboliques.

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc6781.txt`

Bon, changement de stratégie. Pourquoi ne pas tout simplement supprimer le DS, attendre que le contenu dans les caches expirent, puis changer les NS ? Cela peut marcher... si le titulaire de la zone fille ne fait pas de surveillance de ses noms de domaine et ne s'aperçoit donc pas que la zone est désormais neutre (non signée). D'où l'importance de la supervision dans tout projet DNSSEC. C'est d'ailleurs également le cas pour l'attaque précédente : si personne ne supervise et ne s'aperçoit du problème avant que les données ne disparaissent des caches, DNSSEC n'aura servi à rien.

Merci à Peter Koch, Antoin Verschuren, Edward Lewis et Klaus Darilion pour une intéressante discussion à ce sujet.

Un autre article sur la sécurité des noms de domaine était celui de Pierre Col <http://www.zdnet.fr/actualites/securite-des-noms-de-domaines-un-tutoriel-indispensable-39774232.htm>.

---

https://www.bortzmeyer.org/piratage-registre-dnssec.html