Un intéressant problème de DoS spontané avec DNSSEC

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 11 février 2010

https://www.bortzmeyer.org/rollover-and-die.html

Le 16 décembre 2009, le RIPE-NCC a procédé au remplacement de ses clés DNSSEC. Ce changement a eu des conséquences ennuyeuses comme d'invalider DNSSEC dans Fedora <https://lists.dns-oarc.net/pipermail/dns-operations/2010-February/004931.html> mais aussi de provoquer une mini-DoS sur les serveurs secondaires des domaines du RIPE-NCC.

Le RIPE-NCC étant un RIR, les domaines les plus importants qu'il gère sont les domaines de résolution inverse (d'adresse IP en nom de domaine). Ces domaines sont tous signés avec DNSSEC, pour permettre l'authentification de l'origine de ces données. Les clés de signature (KSK pour "*Key Signing Key*" sont remplacées régulièrement <https://www.ripe.net/rs/reverse/dnssec/key-maintenance-procedure.html>, et très fréquemment dans le cas du RIPE-NCC. Ce dernier remplacement, le 16 décembre, a entrainé un brusque bond des requêtes sur les serveurs de l'APNIC, ce qui a donné l'alarme.

Quatre chercheurs, George Michaelson, Patrik Wallstr[Caractère Unicode non montré [1]]m, Roy Arends et Geoff Huston ont enquêté sur le problème dans leur article « Roll Over and Die ? <http://www.potaroo.net/ispcol/2010-02/rollover.html> ». Excellent article, très touffu, plein de détails techniques et de beaux graphiques. Les auteurs ont établi que le problème venait de certains résolveurs, notamment BIND, s'ils avaient en local une clé (une "*trust anchor*") qui avait été retirée. Lorsque la clé (DNSKEY) récupérée dans le DNS est invalide, ces résolveurs pensent à un empoisonnement de cache et réessayent à toute vitesse d'obtenir une bonne clé. Quête vaine lorsque la "*trust anchor*" locale est invalide, et source d'innombrables paquets inutiles...

L'ISC s'est engagée à modifier BIND <https://www.isc.org/announcement/response-to-concerns10Feb>
mais pas immédiatement <https://www.isc.org/community/blog/201002/surprise-bugs-and-release-sc
La correction a été annoncée le 2 mars <https://www.isc.org/community/blog/201003/analysis-dnskey-que

Moralité : en matière de sécurité, il n'y a pas de solution parfaite, uniquement des compromis. En voulant se protéger contre un danger, on tombe souvent sur un autre.

1. Car trop difficile à faire afficher par LaTeX