# Davantage de cloche à vache : la NSA espionne aussi le DNS

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 24 janvier 2015

https://www.bortzmeyer.org/morecowbell.html

---

Quelques jours après le FIC <https://www.forum-fic.com/2015/> (Forum International sur la Cybersécurité, où on avait beaucoup parlé de méchants hackers, forcément djihadistes), un article du Monde <http://www.lemonde.fr/economie/visuel/2015/01/24/cowbells-nouvelles-revelations-sur-4561547_3234.html> nous rappelle que les plus grandes attaques contre la sécurité de l'Internet viennent des États. L'article révèle l'existence du programme MoreCowBell (« davantage de cloche à vache <http://vimeo.com/91715361> ») de la NSA, programme d'espionnage du DNS. L'article du Monde est assez flou, questions détails techniques, donc voici quelques explications supplémentaires.

Vous pouvez également en trouver, et jusqu'à saturation, dans « "*NSA[Caractère Unicode non montré ]s MORECOWBELL : Knell for DNS*" <https://gnunet.org/sites/default/files/mcb-en.pdf> »[1], écrit par les personnes qui ont préparé l'article du Monde (Grothoff est l'auteur de GNUnet, Ermert est une excellente journaliste connaissant bien l'Internet, Appelbaum travaille sur Tor). Dans cet article en anglais (il y a une traduction en français <https://gnunet.org/sites/default/files/mcb-fr.pdf>, vous aurez tous les détails sur MoreCowBell mais aussi sur les travaux de l'IETF pour améliorer le DNS, sur les systèmes alternatifs de nommage comme GNUnet, etc. Au cas où vous n'ayez pas envie de changer de page Web, voici mes informations à moi.

Pour résumer l'article du Monde, la NSA espionne le DNS de deux façons :

— Récolte **passive** de données, probablement via une écoute directe du trafic Internet (quelque chose que la NSA fait souvent), suivie d'une dissection automatique des paquets DNS et stockage dans une base de données. Rien d'extraordinaire, le trafic DNS étant en clair, et des services moins secrets le font depuis longtemps, comme DNSDB <https://www.bortzmeyer.org/dnsdb.html> ou PassiveDNS.cn <https://www.bortzmeyer.org/passivedns-cn.html>.

1. Car trop difficile à faire afficher par LaTeX

— Récolte **active** de données par des attaques par dictionnaire, où une sonde (dans le cas de la NSA, la sonde passe par des résolveurs DNS ouverts <https://www.bortzmeyer.org/fermer-les-recursif html>, comme Google Public DNS <https://www.bortzmeyer.org/google-dns.html>, pour mieux dissimuler ses traces) interroge des serveurs DNS sur des noms possibles ou vraisemblables (en utilisant tous les mots du dictionnaire, par exemple). C'est ce que le Monde, curieusement, appelle « adresses fictives mais plausibles ». Les serveurs DNS reçoivent ce genre d'attaques très souvent (ce sont en général des spammeurs qui cherchent à se constituer des listes de noms de domaine).

Comme toujours avec la NSA, rien de surprenant (seuls les naïfs seront étonnés), des techniques classiques, mais déployées à grande échelle.

Maintenant, sur quelques points obscurs de l'article du Monde :

— « Serveur DNS interne » est apparemment un néologisme du Monde pour **résolveur**.
— « Les numéros IP "en chiffres", correspondant aux adresses "en mots", sont gérés par l[Caractère Unicode non montré ]Internet Assigned Numbers Authority (IANA) » C'est tellement résumé que c'est quasiment faux : si l'IANA attribue bien les préfixes (et encore, c'est fini depuis longtemps en IPv4 <https://www.bortzmeyer.org/epuisement-adresses-ipv4.html>), ce sont les RIR qui font le gros du travail et définissent les politiques d'attribution.
— La phrase « quand ils reçoivent une demande pour une adresse qui n[Caractère Unicode non montré ]existe pas, ils renvoient un message d[Caractère Unicode non montré ]erreur accompagné de deux suggestions » est probablement une allusion aux possibilités d'énumération liées à l'ancienne technologie NSEC, possibilités décrites (avec la solution) dans mon article sur le RFC 5155 [2].
— MoreCowBell, si on se fie aux PowerPoint de la NSA, n'utilise pas que le DNS, mais aussi HTTP. Quand le Monde écrit « quand une attaque est déclenchée, l[Caractère Unicode non montré ]interrogation des serveurs DNS va servir à évaluer son efficacité en temps réel. Grâce à MoreCowBells [sic], la NSA saura si le service attaqué continue à fonctionner ou s[Caractère Unicode non montré ]il a été coupé », il confond probablement ces deux protocoles. Le DNS ne peut pas servir à savoir si un serveur a cessé de fonctionner.
— En revanche, « s[Caractère Unicode non montré ]il a été déplacé vers un autre serveur par mesure de protection, elle va le repérer à nouveau, ce qui permettra de reprendre l[Caractère Unicode non montré ]attaque » peut en effet se faire avec le DNS mais cela n'a rien d'extraordinaire : bien des attaquants qui font des dDoS font pareil.

Par-delà ces détails dans les explications, voilà pourquoi il est essentiel de travailler à améliorer la protection de la vie privée dans le DNS (il faut aussi travailler à mettre fin aux délirants pouvoirs de la NSA, une menace pour tout le monde, mais c'est une autre histoire). À l'IETF, le principal effort, dans la lignée du RFC 6973, est fait dans le groupe de travail DPRIVE <http://datatracker.ietf.org/wg/dprive/>. Son premier RFC sera sans doute le document de description du problème <https://tools.ietf.org/html/draft-ietf-dprive-problem-statement>. Pour le chiffrement des requêtes DNS, afin d'assurer leur confidentialité, ma proposition préférée est T-DNS <http://datatracker.ietf.org/doc/draft-hzhwm-dprive-start-tls-for-dns/> mais l'idée d'utiliser l'ALPN de TLS <http://datatracker.ietf.org/doc/draft-hoffman-dprive-dns-tls-alpn> est également tentante. Une partie de l'effort IETF est également faite dans le groupe de travail DNSOP <http://datatracker.ietf.org/wg/dprive/>, où se fait l'élaboration de la proposition de minimisation des données envoyées <https://tools.ietf.org/html/draft-ietf-dnsop-qname-minimisation>.

Et, bien sûr, une autre solution serait d'utiliser des systèmes alternatifs au DNS, prenant mieux en compte le respect de la vie privée. Ils existent (Namecoin <https://www.bortzmeyer.org/namecoin.html>, Tor / dot-onion <https://www.bortzmeyer.org/blog-tor-onion.html>, etc) mais ils posent de redoutables problèmes <https://www.bortzmeyer.org/no-free-lunch.html>.

Un autre article en français sur ce programme est dans 01 Net <http://www.01net.com/editorial/642838/comment-la-nsa-denature-le-dns-pour-espionner-particuliers-et-entreprises/>.

2. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc5155.txt