Vulnérabilités DNS du mois

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 5 mai 2006

https://www.bortzmeyer.org/dns-vulnerabilites.html

Le mois d'avril 2006 a été marqué par l'intérêt médiatique pour les vulnérabilités du DNS. Mais cet intérêt a peut-être créé une certaine confusion entre des problèmes très différents, qui n'ont été rapprochés que par les hasards de la chronologie.

La plus médiatisée (même la BBC en a parlé <http://news.bbc.co.uk/1/hi/technology/4954208.stm>) est l'étude du groupe Beehive <http://www.cs.cornell.edu/people/egs/beehive/> (menée notamment par Emin Gun Sirer), intitulée "*A Survey of DNS Security : Most Vulnerable and Valuable Assets*" <http://www.cs.cornell.edu/people/egs/beehive/dnssurvey.html>, présentée à RIPE 52 <http://www.ripe.net/ripe/meetings/ripe-52/>.

En résumé, cette étude rappelle qu'un nom de domaine dépend d'autres domaines pour sa résolution. Par exemple, sarkozy.fr dépend de .net puisque les serveurs de noms de sarkozy.fr sont dans deviantnetwork.net. Le responsable de ce domaine doit donc tenir compte de ces autres serveurs et la liste des dépendances peut être étonemment longue (le programme (en ligne sur https://www.bortzmeyer.org/files/dependency-domain.py) peut être utilisé pour afficher la liste et le programme (en ligne sur https://www.bortzmeyer.org/files/ns2dot.py) peut produire un joli graphe Graphviz des dépendances). Si ceux-ci trahissent ou bien sont piratés (l'étude mentionne longuement les vulnérabilités de certaines mises en œuvre du DNS), le domaine peut être modifié.

Certains TLD sont, selon cette étude, plus vulnérables car ils dépendent de davantage de serveurs (ainsi, il y a 248 serveurs de noms dans le graphe de dépendance de .fr).

Cette étude soulève un grand nombre de questions. D'abord, elle ne découvre pas grand'chose de nouveau : la question du graphe de dépendance est discutée depuis longtemps (on peut regarder le graphe de dépendance d'un domaine sur l'l'outil du registre polonais <http://www.dns.pl/cgi-bin/dnsexplorer.pl>). Et cette discussion n'a jamais permis d'arriver à un consensus entre les deux écoles, celle qui pense qu'il faut répartir les risques (avec des serveurs de noms dans des domaines différents), et celle qui pense qu'il faut mettre tous ses œufs dans le même panier (en concentrant les serveurs de noms dans un petit nombre de domaines). Certains gros hébergeurs comme UltraDNS <http://www.ultradns.org/> ont même changé de politique (les serveurs de noms de .org étaient tous dans .org mais ils sont désormais dans plusieurs TLD).

Ensuite, l'étude mélange un problème de base du DNS, les relations de dépendance entre serveurs, avec les vulnérabilités des logiciels. Il y a bien d'autres moyens d'attaquer le DNS que de pirater un serveur de noms : par exemple la trahison des administrateurs de ce serveur : il faut avoir confiance dans les administrateurs de ses serveurs secondaires.

Le vrai but de l'étude semble être la promotion de la solution du groupe Beehive : CoDoNS <http://www.cs.cornell.edu/people/egs/beehive/codons.php>, un système de résolution de noms bâtie sur les tables de hachages distribuées. CoDoNS est une approche très intéressante, et je me félicite que des chercheurs courageux se lancent dans des grands projets comme celui-ci mais la comparaison avec le DNS est tout à fait injuste. Le DNS fonctionne depuis presque vingt ans et a affronté d'innombrables problèmes alors que CoDoNS est encore un prototype de laboratoire qui, dès qu'on l'examine de plus près, révèle un grand nombre de problèmes qui restent à résoudre avant qu'il puisse prétendre remplacer le DNS.

Ceux qui s'intéressent aux questions de gouvernance de l'Internet noteront que CoDoNS ne s'attaque qu'à la question de la résolution des noms de domaine, et ne change rien à leur structure, donc à la hiérarchie d'allocation de ces noms, hiérarchie qui culmine au gouvernement états-unien, via l'ICANN.

D'autre part, et sans qu'il y aie de relation avec l'étude de Beehive, le 28 avril, le NISCC annonçait son étude "*Vulnerability Issues in Implementations of the DNS Protocol*" <http://www.niscc.gov.uk/niscc/docs/re-20060425-00312.pdf?lang=en>. Menée en envoyant à divers clients et serveurs DNS des paquets délibérement incorrects, elle a mené à la découverte de vulnérabilités dans plusieurs logiciels, souvent très utilisés.

Il s'agit là de vulnérabilités classiques de logiciels écrits de manière un peu négligente, pas de problèmes du DNS en général.