Attaque sur plusieurs systèmes d'enregistrement de noms de domaines

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 18 mai 2009

https://www.bortzmeyer.org/attaques-registres-noms.html

Vous avez sans doute vu un des nombreux articles publiés depuis deux semaines, sur les attaques portant sur les systèmes d'enregistrement de noms de domaines : les ccTLD de la Nouvelle-Zélande <http://www.zone-h.org/news/id/4708>, de Porto-Rico <http://news.cnet.com/8301-1009_3-10228436-83.html> et du Maroc <http://www.marocinfo.net/to/index.php/Sciences-et-Technologi Google-Maroc-deface.cfm> ont été touchés.

Le rythme semble s'accélerer et d'autres attaques sont signalées (Tunisie, Ouganda, Équateur). Comme le domaine de Google était souvent visé, Google a publié un texte expliquant que c'était la faute du DNS <http://www.infoworld.com/t/authentication-and-authorization/google-blames-dns-insecurity

C'est donc l'occasion de faire un petit point. Je n'ai pas d'informations « de l'intérieur » sur ces attaques, je relaie simplement des informations publiques. La plupart des articles cités ci-dessus étant « garantis 0 % information », il faut prendre tout cela avec beaucoup de pincettes. Pour la même raison, ce message n'est pas officiel, il n'a pas été validé par le Ministère de l'Intérieur, etc.

— il n'est pas certain qu'il s'agisse d'une attaque coordonnée. C'est évidemment tentant que penser que les Illuminati visent tous les registres de ccTLD en même temps mais ce n'est pas prouvé, il peut s'agir d'un simple effet de mode (un peu comme les voitures qui brûlent en banlieue).
— sauf peut-être dans le cas d'un FAI kenyan, qui pourrait avoir été victime d'une attaque de style Kaminsky <https://www.bortzmeyer.org/comment-fonctionne-la-faille-kaminsky.html>, aucune de ces attaques ne semble mériter le nom d'attaque DNS. Toutes ont porté sur le système d'enregistrement, en amont du DNS. Le "*modus operandi*" le plus fréquent semble la traditionnelle injection SQL <https://www.bortzmeyer.org/sql-injection.html>, qui marche toujours très bien contre des sites Web écrits en PHP ou en VB.net par un stagiaire. Une fois l'injection réussie, le craqueur insère de fausses données dans la base et le DNS publie aveuglément ces données.
— pour la même raison, les techniques de signature cryptographiques comme DNSSEC n'auraient servi à rien, contrairement à ce que raconte bêtement le marketing de PIR <http://blog.pir.org/?p=335>. En effet, DNSSEC signe les données de la base ; si celle-ci est corrompue, DNSSEC signe des données fausses.

— l'attaque a parfois porté sur le registre (cas de .PR), parfois sur un bureau d'enregistrement (« "*registrar*" », cas de .MA).

Tout ceci forme une leçon très classique en sécurité : les experts se focalisent sur les attaques de haute technologie, rigolotes, comme la faille Kaminsky et ignorent les attaques bêtes, simples et classiques comme l'injection SQL (voire l'ingéniérie sociale).

Terminons en rendant hommage aux malawites qui sont les premiers à avoir publié un rapport technique sur les attaques <https://lists.afrinic.net/pipermail/africann/2009-May/001438.html>. Deux ans après, les porto-ricains ont à leur tour rendu publiques les informations <http://svsf40.icann.org/meetings/siliconvalley2011/presentation-domain-system-threat-landscap pdf>. Un rapport détaillé sur les problèmes d'attaques sur les systèmes d'enregistrement des registres de noms est le "*SAC 40 : Measures to Protect Domain Registration Services Against Exploitation or Misuse*" <https://www.icann.org/en/committees/security/sac040.pdf>.
