Détournement d'un nom de domaine via le domaine des serveurs de noms

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 29 octobre 2012

https://www.bortzmeyer.org/detournement-via-ns.html

Lorsqu'on analyse la sécurité de ses noms de domaine, on pense à des choses comme surveiller l'expiration et ne pas oublier de renouveller, ou bien on pense au piratage du registre ou du bureau d'enregistrement par le premier "*hacker*" chinois islamiste pédophile venu (comme vu récemment dans `.ie`) ou alors on pense à des attaques d'encore plus haute technologie comme l'attaque Kaminsky <https://www.bortzmeyer.org/comment-fonctionne-la-faille-kaminsky.html>. Mais on pense rarement à un risque courant : un domaine trébuche parce que le domaine de ses serveurs de noms a trébuché. C'est ce qui vient de se produire dans deux cas, `duckworksmagazine.com` et `ben.edu`.

Les deux cas ont été publiés et discutés ce mois-ci sur la liste dns-operations <https://lists.dns-oarc.net/mailman/listinfo/dns-operations> de l'OARC <https://www.dns-oarc.net/>. Prenons le deuxième domaine, `ben.edu`, domaine de Benedictine University (qui n'a apparemment rien à voir avec la boisson française). Ce domaine a deux serveurs de noms :

```
% dig NS ben.edu

; <<>> DiG 9.8.1-P1 <<>> NS ben.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29134
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;ben.edu. IN NS

;; ANSWER SECTION:
ben.edu. 37533 IN NS ns2.bobbroadband.com.
ben.edu. 37533 IN NS ns1.bobbroadband.com.

;; Query time: 0 msec
;; SERVER: ::1#53(::1)
;; WHEN: Mon Oct 29 10:11:02 2012
;; MSG SIZE  rcvd: 88
```

Or, le point important est que ces serveurs sont dans un autre domaine, géré par une autre organisation et passant par un bureau d'enregistrement (BE) qui n'a pas de rapport avec Benedictine University (`.edu` n'utilise pas de bureaux d'enregistrement). En changeant ce domaine `bobbroadband.com`, on peut changer le contenu de `ben.edu`. C'est apparemment ce qui s'est produit à partir du 25 octobre 2012 (merci à Robert Edmonds pour l'analyse) : au lieu de son adresse IP habituelle, `38.100.120.100`, `ben.edu` avait tout à coup `208.91.197.132` (sur certains sites, les autres ayant l'ancienne adresse dans les caches). Le domaine `bobbroadband.com` avait expiré (ses serveurs de noms sont passés dans le domaine `pendingrenewaldeletion.com` qu'utilise le BE Network Solutions comme purgatoire pour les domaines non renouvelés), quelqu'un l'a apparemment acheté, a changé les serveurs de noms (`ns1432.ztomy.com`). Contrôlant alors le contenu de `bobbroadband.com`, il pouvait changer toutes les zones dont les serveurs de noms étaient dans `bobbroadband.com`. C'est ce qui est arrivé à `ben.edu`. `208.91.197.132` (qui est aussi l'adresse de `ns1432.ztomy.com`) est enregistré... aux Îles Vierges, paradis fiscal connu.

Le premier cas, quelques jours plus tôt, était celui de `duckworksbbs.com` (et `duckworksmagazine.com`), qui vend des équipements pour bateaux <`http://www.duckworksbbs.com/`>. Les serveurs de noms étaient dans le domaine `crystaltech.com`, qui a un BE différent de celui de `duckworksbbs.com`. Ce domaine a expiré le 18 octobre (merci à Andrew Sullivan pour l'analyse). Pour pouvoir supprimer le domaine auprès du registre de `.com` (les contraintes d'intégrité du registre interdisent normalement de supprimer un domaine qui est utilisé par d'autres), le BE a renommé les serveurs de noms (`webterminator1.crystaltech.com` est devenu `doesnotexistwebterminator1.crystaltech.com.hu`...) La sortie de la commande whois pour `duckworksbbs.com` ne montrait pas ce changement, puisque le BE de `duckworksbbs.com`, différent de celui de `crystaltech.com`, n'était pas au courant... Les nouveaux serveurs de noms n'existant pas dans le DNS, le domaine `duckworksbbs.com` ne marchait plus (ce qui est moins grave que d'être détourné).

La morale de ces deux histoires ? Lorsqu'on analyse la sécurité d'un nom de domaine, il faut aussi regarder celle du nom utilisé pour les serveurs de noms. Le maillon faible est peut-être là. Essayez avec quelques domaines connus, vous verrez que le domaine sensible est souvent celui du fournisseur, pas celui du titulaire.

`https://www.bortzmeyer.org/detournement-via-ns.html`