

Piratage de trois domaines de premier niveau

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 8 octobre 2026

<https://www.bortzmeyer.org/piratage-trois-cctld.html>

Du 22 au 27 septembre, un inconnu a piraté trois registres de noms de domaine. L'occasion de rappeler, face à plusieurs commentaires erronés, que si un attaquant prend le contrôle du nom de domaine, il peut **tout** faire (et, non, TLS ne protège pas).

Les faits, d'abord, tels que résumés dans cet article d'Ars Technica <<https://arstechnica.com/security/2026/10/hackers-obtain-counterfeit-tls-certificates-for-google-and-other-large-s>>. Un attaquant a piraté, par des moyens inconnus, trois ccTLD, .gh, .sl et .as. Ayant apparemment le contrôle complet de la base de données, il pouvait modifier les noms qu'il voulait, notamment google.TLD. (Voir le communiqué de Google <<https://blog.google/security/chromes-response-to-recent>>.)

On peut confirmer indépendamment cet article avec DNSDB <<https://www.bortzmeyer.org/dnsdb.html>> ou un autre service présentant l'historique du DNS. Par exemple pour la Sierra Leone :

```
% isc-dnsdb-query rrset google.sl/NS
;; bailiwick: sl.
;; count: 105533
;; first seen: 2010-07-09 12:58:00 -0000
;; last seen: 2026-10-07 03:41:01 -0000
google.sl. IN NS ns1.google.com.
google.sl. IN NS ns2.google.com.
google.sl. IN NS ns3.google.com.
google.sl. IN NS ns4.google.com.

;; bailiwick: sl.
;; count: 12
;; first seen: 2026-09-25 04:37:33 -0000
;; last seen: 2026-09-25 04:47:46 -0000
google.sl. IN NS betty.ns.cloudflare.com.
google.sl. IN NS edward.ns.cloudflare.com.
```

Notez le *"bailiwick"* montrant que c'est bien le TLD qui était piraté. On voit dans le premier groupe, les serveurs de noms normaux <<https://www.bortzmeyer.org/serveur-dns-faisant-autorite.html>>, chez Google, le deuxième groupe étant le piratage. Il a été très vite détecté et corrigé, les pirates devraient savoir que quand on pirate un registre, il ne faut **surtout pas** toucher à `google.TLD`, c'est le plus surveillé et Google est très réactif.

Et aux Samoa?

```
% isc-dnsdb-query rrset google.as/NS
;; bailiwick: as.
;;      count: 10000346
;; first seen: 2010-06-24 04:28:33 -0000
;; last seen: 2026-10-08 02:20:05 -0000
google.as. IN NS ns1.google.com.
google.as. IN NS ns2.google.com.
google.as. IN NS ns3.google.com.
google.as. IN NS ns4.google.com.

;; bailiwick: as.
;;      count: 549
;; first seen: 2026-09-27 03:18:09 -0000
;; last seen: 2026-09-27 05:30:26 -0000
google.as. IN NS duke.ns.cloudflare.com.
google.as. IN NS mckinley.ns.cloudflare.com.
```

Même chose, deux jours plus tard. (Et `google.com.gh`, puisque ce TLD enregistre au troisième niveau, le 22 septembre. Merci à Rémy Grünblatt du rappel.)

Certaines personnes, par exemple dans les commentaires à l'article d'Ars Technica <<https://arstechnica.com/security/2026/10/hackers-obtain-counterfeit-tls-certificates-for-google>> n'ont pas compris les conséquences du piratage et se sont demandés pourquoi c'est grave puisque TLS aurait protégé de toute façon. (Notons qu'un commentaire confond registre de noms de domaine et AC... Il ne faut pas lire les commentaires <<https://www.bortzmeyer.org/no-comment.html>> si on ne veut pas devenir misanthrope.) TLS n'aurait pas protégé tout simplement parce que, quand on contrôle le DNS, on contrôle **tout** et on peut obtenir facilement et automatiquement un certificat (il y a bien longtemps que les certificats alloués « manuellement », avec examen par un humain, ne sont presque plus utilisés). C'est ce que dit l'article d'Ars Technica et on peut le vérifier avec les journaux *"Certificate Transparency"* (RFC 9162¹). Si on a la chance de tomber à un moment où fonctionne (c'est rare), on peut trouver les certificats créés (je n'en vois pas pour `google.com.gh`) :

Cette difficulté de certains à comprendre l'ampleur des choses qu'on peut faire une fois qu'on a le contrôle d'un TLD est en partie liée au cliché souvent répété « Le DNS, c'est pour traduire des noms en adresses IP ». Ce n'est en fait qu'une partie de son rôle mais le DNS sert à bien d'autres choses. Par exemple, un commentaire a cité la possibilité, pour Google, de mettre un enregistrement CAA (RFC 8659), sans comprendre que cela n'aurait servi à rien pendant le détournement. (Modulo la mémorisation du CAA dans certains résolveurs <<https://www.bortzmeyer.org/resolveur-dns.html>>.) Bref, la sécurité des TLD contre ce genre de piratage est cruciale.

1. Pour voir le RFC de numéro NNN, <https://www.ietf.org/rfc/rfcNNN.txt>, par exemple <https://www.ietf.org/rfc/rfc9162.txt>