Détournement du nom de domaine eth.limo

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 20 avril 2026

https://www.bortzmeyer.org/eth-limo-detourne.html

Le 18 avril, le nom de domaine eth.limo a été victime d'un détournement (une attaque où le méchant prend le contrôle du nom et change les informations).

Les détournements sont le deuxième plus gros problème de sécurité des noms de domaine, avec les attaques par déni de service. Des articles de bilan sur celui-ci ont été produits aussi bien par le titulaire du nom <https://x.com/eth_limo/status/2045552916157563148> (nom qui est utilisé en rapport avec la cryptomonnaie Ethereum) que par le revendeur EasyDNS <https://easydns.com/blog/2026/04/18/we-screwed-up-and-we-own-it-the-eth-limo-shtshow-is-on-us/> (dont on notera la franchise « nous avons merdé »). On ne sait pas exactement comment s'est fait le détournement (l'article d'EasyDNS parle juste d'« ingénierie sociale). Mais voyons les changements faits dans le DNS, et quelques leçons à tirer.

Le domaine a été enregistré via EasyDNS, un revendeur du BE Tucows. Il est hébergé sur AWS. Voici l'information obtenue via RDAP :

```
% rdap eth.limo
...
Nameserver: ns-814.awsdns-37.net
Nameserver: ns-1689.awsdns-19.co.uk
Nameserver: ns-48.awsdns-06.com
Nameserver: ns-1382.awsdns-44.org
Delegation Signed: yes
...
Last Changed: 2026-04-18T15:31:54.163Z
...
Role: registrar
Name: Tucows Domains Inc.
```

(Notez qu'on ne peut pas utiliser whois, celui-ci n'est plus obligatoire dans les TLD ICANN et, en effet, .limo ne semble plus en avoir.)

Enregistrés par DNSDB <https://www.bortzmeyer.org/dnsdb.html>, voici la délégation DNS normale de eth.limo :

```
;;  bailiwick: limo.
;;      count: 1371
;; first seen in zone file: 2022-07-15 00:15:27 -0000
;;  last seen in zone file: 2026-04-19 00:11:22 -0000
eth.limo. IN NS ns-48.awsdns-06.com.
eth.limo. IN NS ns-814.awsdns-37.net.
eth.limo. IN NS ns-1382.awsdns-44.org.
eth.limo. IN NS ns-1689.awsdns-19.co.uk.
```

Et pendant le détournement (deux jeux de serveurs de noms <https://www.bortzmeyer.org/serveur-dns-faisant-autorite.html> utilisés, comme noté par le tweet du titulaire) :

```
;;  bailiwick: limo.
;;      count: 495
;; first seen: 2026-04-18 06:31:38 -0000
;;  last seen: 2026-04-18 08:06:34 -0000
eth.limo. IN NS joan.ns.cloudflare.com.
eth.limo. IN NS garrett.ns.cloudflare.com.

;;  bailiwick: limo.
;;      count: 1363
;; first seen: 2026-04-18 08:06:57 -0000
;;  last seen: 2026-04-18 11:59:02 -0000
eth.limo. IN NS dns1.namecheaphosting.com.
eth.limo. IN NS dns2.namecheaphosting.com.
```

Il est amusant de constater que deux jours après, Cloudflare (et Namecheap) continuent à servir la mauvaise information :

```
% dig @joan.ns.cloudflare.com. eth.limo NS
...
;; ANSWER SECTION:
eth.limo.  86400 IN NS garrett.ns.cloudflare.com.
eth.limo.  86400 IN NS joan.ns.cloudflare.com.
...
;; WHEN: Mon Apr 20 14:02:13 BST 2026
```

Qu'est-ce que le méchant a changé dans la zone ? Il a modifié l'adresse IP, pointant vers un hébergement Web chez Namecheap. On le voit aussi avec DNSDB :

```
;;      count: 206
;; first seen: 2026-04-18 07:36:35 -0000
;;  last seen: 2026-04-18 11:50:19 -0000
eth.limo. IN A 162.213.253.76
```

Mais notez que les serveurs faisant autorité <https://www.bortzmeyer.org/serveur-dns-faisant-auto
html> de Cloudflare et Namecheap continuent de servir la mauvaise info. Comparez avec la vraie :

———————

https://www.bortzmeyer.org/eth-limo-detourne.html

```
% dig eth.limo A
...
;; ANSWER SECTION:
eth.limo.  60 IN A 35.71.142.77
eth.limo.  60 IN A 52.223.52.2
...
;; WHEN: Mon Apr 20 13:18:39 UTC 2026

% dig @dns1.namecheaphosting.com eth.limo A
...
;; ANSWER SECTION:
eth.limo.  14400 IN A 162.213.253.76
...
;; WHEN: Mon Apr 20 13:19:06 UTC 2026
```

Et en mettant `162.213.253.76 eth.limo` dans son `/etc/hosts`, on peut voir le site « pirate », qui n'a pas été supprimé. Il ressemble tout à fait au vrai, sauf qu'il n'a pas de HTTPS. Puisqu'on parle de HTTPS, notons que l'attaquant ne semble pas avoir demandé de certificat (il aurait pu). Le dernier certificat alloué date du 11 avril. C'est en tout cas ce qu'on voit en regardant les journaux Certificate Transparency.

Le domaine était signé et l'attaquant, bêtement, n'a pas changé l'enregistrement DS, ce qui fait que tous les gens utilisant (à raison) un résolveur <https://www.bortzmeyer.org/resolveur-dns.html> validant n'ont pas pu voir le site pirate. (Personne ne semble avoir testé le domaine avec DNSviz <https://dnsviz.net/d/eth.limo/dnssec/> pendant le détournement mais les tests anciens montrent que le DS était là depuis bien avant.)

Il ne semble pas (mais ce n'est pas visible de l'extérieur) que `eth.limo` était protégé par un verrou au registre (je ne sais pas si `.limo` a un tel service, l'équivalent du "*FR lock*" <https://www.afnic.fr/produits-services/services-associes/fr-lock/> de `.fr`; Patrick Mevzek a cherché et n'a pas trouvé trace de ce service en `.limo`). C'est pourtant une très bonne protection contre les détournements mais aucun des deux articles n'en parle.