Un cas rigolo d'oubli d'un nom de domaine

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 30 mars 2022

https://www.bortzmeyer.org/attaque-sous-domaine-caisse-epargne.html

---

Il est fréquent qu'une organisation utilise un sous-domaine de son domaine principal pour mettre une adresse IP qui est celle d'un hébergeur plus ou moins distant. Pas de problème avec cela. Sauf que, parfois, lorsqu'on arrête d'utiliser le serveur chez l'hébergeur, on oublie de supprimer le nom de domaine. Et cela peut ouvrir des failles de sécurité.

Le cas a été détecté par Thomas Citharel <https://social.tcit.fr/@tcit/108012090476028890>. Le nom de domaine societaires.caisse-epargne.fr pointe vers une adresse IP qui semble être utilisée par un particulier sans lien avec la Caisse d'Épargne. Regardons :

```
% dig A societaires.caisse-epargne.fr

; <<>> DiG 9.16.1-Ubuntu <<>> A societaires.caisse-epargne.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2803
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;societaires.caisse-epargne.fr. IN A

;; ANSWER SECTION:
societaires.caisse-epargne.fr. 86400 IN A 5.39.72.65

;; Query time: 183 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Fri Mar 25 07:50:02 CET 2022
;; MSG SIZE  rcvd: 74
```

L'adresse IP est `5.39.72.65` (au fait, vous pouvez regarder vous-même si cela a changé depuis cet article, avec dig, ou bien via le DNS Looking Glass <https://dns.bortzmeyer.org/societaires.caisse-epargne.fr>). L'adresse en question indique une machine chez OVH (vu avec whois). Rien d'extraordinaire à ce que la Caisse d'Épargne utilise des machines dans le "*cloud*". Ce qui est plus curieux, c'est que le serveur HTTP sur la machine renvoie un code de retour 403 (accès interdit) :

```
% curl -v  societaires.caisse-epargne.fr
*   Trying 5.39.72.65:80...
* Connected to societaires.caisse-epargne.fr (5.39.72.65) port 80 (#0)
> GET / HTTP/1.1
> Host: societaires.caisse-epargne.fr
...
< HTTP/1.1 403 Forbidden
< Server: nginx
< Date: Wed, 30 Mar 2022 07:54:37 GMT
...
<html>
<head><title>403 Forbidden</title></head>
...
```

Pourquoi avoir ce nom de domaine si ça ne marche pas ? En fait, le serveur HTTP répond à un autre nom. Une façon de le trouver est dans le certificat. Réessayons en HTTPS :

```
%  curl -v https://societaires.caisse-epargne.fr
*   Trying 5.39.72.65:443...
...
* Server certificate:
*  subject: CN=cloud.sevenn.fr
...
```

Donc, la machine indique plutôt `cloud.sevenn.fr` comme identité. Et, là, ça marche, ce nom <https://dns.bortzmeyer.org/cloud.sevenn.fr> pointe vers la meme adresse IP :

```
% dig A cloud.sevenn.fr
...
;; ANSWER SECTION:
cloud.sevenn.fr. 300 IN CNAME sevenn.fr.
cloud.sevenn.fr. 300 IN RRSIG CNAME 13 3 300 (
20220326075016 20220324055016 34505 sevenn.fr.
YZKUrmJudhUmG/iOu1GKsei510JBZVS2Bn+2z2pmO8fC
aXJbbgb66XTJsyCkMZ7oaPzaKdgJI8UldHhZ/1ErHg== )
sevenn.fr. 300 IN A 5.39.72.65
sevenn.fr. 300 IN RRSIG A 13 2 300 (
20220326075016 20220324055016 34505 sevenn.fr.
gk3v1r2/dJTc0/jqL4ZQqH6xQh7xvYLcCSNhQNq5yrvM
ubQ3WYuv3Pu1Yw7MoxVrJjNOqP9NlVdzmo3L/FK8ag== )

...
```

En visitant le site Web, on voit un service Nextcloud. (On notera que le domaine du particulier est signé avec DNSSEC, alors que celui de l'établissement financier ne l'est pas…)

Le plus probable est donc qu'à une époque, la Caisse d'Épargne avait un serveur chez OVH. Elle a supprimé le serveur, mais a gardé le nom de domaine. Plus tard, un particulier a loué un serveur chez OVH, et récupéré l'adresse IP. Il contrôle donc une machine vers laquelle pointe un nom de la Caisse d'Épargne. Quelles conséquences cela peut avoir ? Il peut y avoir des problèmes de sécurité. Par exemple, le locataire de la machine pourrait désormais obtenir un certificat pour le nom `societaires.caisse-epargne.fr` (et peut-être pour le nom au-dessus). Il pourrait également placer des "*cookies*" pour ce nom. C'est pour cela que j'ai évidemment écrit aux adresses de contact du domaine `caisse-epargne.fr` (obtenues via whois) avant de publier cet article. Inutile de dire que, comme pour la plupart des signalements de sécurité, je n'ai jamais eu de réponse, et que rien n'a été fait.

Bien sûr, ici, il ne s'agit pas d'une attaque, le nouveau titulaire de l'adresse IP est parfaitement de bonne foi. Mais de telles attaques sont possibles : on parle d'« attaque par le sous-domaine <`https://labs.detectify.com/2014/10/21/hostile-subdomain-takeover-using-herokugithubdesk-more/`> ». Le principe est de repérer un sous-domaine de votre cible qui pointe vers une adresse IP d'un hébergeur et qui n'est plus affectée, puis de créer des serveurs chez l'hébergeur en question jusqu'à tomber sur la bonne adresse. Avec les API, cela s'automatise et peut donc être rapide et pas trop coûteux.

Un dernier détail : si vous visitez l'URL `http://societaires.caisse-epargne.fr` avec certaines versions de Firefox (et peut-être d'autres navigateurs), cela « marchera » car le navigateur, recevant le code d'erreur 403, ré-essaiera ensuite avec `www.societaires.caisse-epargne.fr` (qui est associé à une toute autre adresse IP, chez Online). Cela rappelle qu'il ne faut **pas** déboguer les problèmes de réseau avec un navigateur Web, logiciel compliqué et qui fait plein de choses qu'on ne lui a pas demandé.

(Ces problèmes d'« attaque » par sous-domaine ne sont pas nouveaux, Marc Framboisier m'a retrouvé un article de 2009 <`https://www.numerama.com/politique/11639-le-site-du-tgi-de-bonneville-html`> touchant un tribunal de la même façon.)

`https://www.bortzmeyer.org/attaque-sous-domaine-caisse-epargne.html`