AXA et le redirecteur

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 29 octobre 2017

https://www.bortzmeyer.org/axa-redirecteur.html

La société AXA (assurance et autres services financiers) utilise souvent pour sa communication des URL où le nom de domaine est go.axa.fr. On le trouve dans les messages envoyés aux clients, par exemple. Quel est le problème de sécurité et d'éducation que cela pose ?

Si vous voulez voir de tels URL, demandez simplement à un moteur de recherche un truc du genre inurl:go.axa.fr et vous en trouverez plein, apparemment utilisés dans des campagnes de promotion (« téléchargez une application permettant de mieux gérer votre compte AXA Banque » ou bien voir la page Facebook officielle d'AXA Banque <https://www.facebook.com/axabanque/photos/a.378967568810200.87222.149396658433960/1781580115215598/?type=3&theater>). Prenons par exemple http://go.axa.fr/promium/, « le programme d'AXA France destiné aux Professionnels ». Normalement, le client, même méfiant, n'hésitera pas à suivre ce lien : il est bien situé sous le domaine d'AXA, axa.fr. Si on suit les conseils habituels <https://www.ssi.gouv.fr/particulier/precautions-elementaires/5-reflexes-a-avoir-lors-de-la-reception-dun-courriel/> « En passant la souris au-dessus du lien proposé, vous pouvez repérer s[Caractère Unicode non montré [1]]il pointe bien vers l[Caractère Unicode non montré]adresse du site annoncée dans le message. Si l[Caractère Unicode non montré]adresse est différente, soyez méfiant, et évitez de cliquer sur le lien. De manière générale, il est préférable de saisir manuellement l[Caractère Unicode non montré]adresse dans le navigateur. », on ne devrait pas se faire avoir. (Oui, je sais que, dans le monde réel, personne ne suit ces conseils.)

Sauf que...Le nom go.axa.fr pointe vers <https://dns.bortzmeyer.org/go.axa.fr/ADDR> l'adresse IP 74.217.253.90. Hébergée aux États-Unis chez Internap, elle ne semble pas a priori avoir de relation avec AXA. Pourtant, s'y connecter en HTTP redirige bien vers la bonne page :

1. Car trop difficile à faire afficher par LaTeX

```
% curl -v http://go.axa.fr/promium/
*   Trying 74.217.253.90...
* TCP_NODELAY set
* Connected to go.axa.fr (74.217.253.90) port 80 (#0)
> GET /promium/ HTTP/1.1
...
< HTTP/1.1 301 Moved Permanently
< Server: post/2.0
< Location: https://mediazone.axa/communique-de-presse/axa-programme-promium#
```

On est bien renvoyé vers une page d'AXA, dans le TLD `.axa`. Mais, minute, il y a une chose bizarre dans la réponse, le champ `Server:`. Il indique `post` qui identifie le serveur de redirection utilisé par le service `po.st`, un moteur de redirection comme `bit.ly`. D'ailleurs, si on visite `http://go.axa.fr/` (sans rien après la dernière barre oblique), on arrive bien chez `po.st` :

```
% curl -v http://go.axa.fr/
*   Trying 74.217.253.90...
* TCP_NODELAY set
* Connected to go.axa.fr (74.217.253.90) port 80 (#0)
> GET / HTTP/1.1
...
< HTTP/1.1 302 Found
< Server: post/2.0
< Location: https://www.po.st
```

Si vous voulez un autre signe, vous pouvez essayer en HTTPS, `https://go.axa.fr/promium/`. Le certificat ne sera pas accepté car il ne couvre que `po.st`, pas `go.axa.fr`.

Bon, donc, en fait, AXA utilise `po.st`. Est-ce grave ? En tout cas, c'est ennuyeux, car ces redirecteurs/raccourcisseurs d'URL ont deux problèmes <`https://www.bortzmeyer.org/probleme-raccourcisseu` `html`> :

— Ils peuvent changer à leur guise la redirection et donc emmener les clients d'AXA où ils veulent,
— Ils peuvent enregistrer les informations sur le client (son adresse IP et surtout l'empreinte du navigateur <`https://panopticlick.eff.org/`>, grâce aux nombreuses données que celui-ci envoie).

Paranoïa complète de ma part ? `po.st` est propriété de RadiumOne (source : `https://www.po.st/about/post`), société états-unienne, et ces derniers ne cachent pas leurs activités : « "*a company that generates first-party data about actual customers – from their behaviors, actions and interests demonstrated across the web and mobile. We access tens of billions of real-time impressions each day across the Web, video, social and mobile to reach consumers in real-time no matter where they are. Our intelligent software and methodologies increase the relevance and personalization of ads through sophisticated algorithms that find valuable characteristics, gauge consumer behaviors, and target ads with laser focus to the right audiences*" ». Bref, rediriger à travers `po.st`, c'est donner plein d'informations à une enterprise états-unienne, non tenue par le RGPD. Le but de surveillance à des fins marketing est encore plus clair sur l'image en `https://www.po.st/assets/img/sharing/sharing-brand` ou sur la page `https://www.po.st/sharing/brands`.

(Concernant le RGPD, des juristes m'ont fait remarquer que `po.st` est bien tenu de respecter le RGPD, du moment que les données concernées sont celles de citoyens européens, ce qui est le cas ici (principe d'extra-territorialité du RGPD). Ils ont bien sûr raison, mais la question est plutôt « en pratique, que se passera-t-il ? » Je doute fort qu'AXA soit inquiété pour ces traitements.)

Je ne cherche pas spécialement à taper sur AXA. Des tas d'entreprises font cela. En général, le service communication ignore complètement tous les conseils de sécurité. Ainsi, on s'inscrit à la "*newsletter*" d'une société dont le domaine est `mabanque.example` et on reçoit ensuite des messages envoyés depuis un tout autre domaine. Impossible dans ces conditions de mettre en pratique les conseils de l'ANSSI indiqués plus haut !

Mais, ici, le cas est un peu plus original dans le mesure où le nom affiché au client (`go.axa.fr`) est conçu pour inspirer confiance, dissimulant à l'usager qu'il verra ses données être enregistrées par `po.st`. Ce genre de pratiques met donc en péril toutes les tentatives d'éducation à la sécurité qui ont été faites depuis des années, et qui encourageaient à faire attention au nom de domaine dans les URL.

(Notons qu'utiliser un nom de domaine à soi pour rediriger via `po.st` nécessite l'accord de `po.st`. Si, dans `http://go.axa.fr/promium/`, vous remplacez `go.axa.fr` par `po.st`, cela ne marchera pas.)

Et puis c'est dommage que cette utilisation d'un redirecteur étranger et peu soucieux de protection des données personnelles soit le fait d'une société qui s'était permis de promouvoir un « permis Internet <`https://www.permisinternet.fr/`> » qui avait été, à juste titre, fortement critiqué <`https://www.nextinpact.com/news/87433-le-permis-internet-au-cm2-pedagogie-par-peur.htm`>.

Mes remerciements à Philippe Meyer pour avoir attiré mon attention sur cet intéressant cas.