Détails techniques sur les récentes attaques contre les noms de domaine

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 27 février 2019

https://www.bortzmeyer.org/dnspionage.html

Au cours du dernier trimestre 2018, mais peut-être depuis plus longtemps, un certain nombre d'attaques contre les noms de domaine ont eu lieu, apparemment toutes perpétrées par le même groupe. Dans un autre article <https://www.bortzmeyer.org/attaques-noms-domaine-explications.html>, j'ai essayé d'expliquer à un public assez large ce qu'étaient ces attaques et leurs conséquences. Dans l'article que vous êtes en train de lire, je détaille un certain nombre de points techniques. Au contraire du premier, cet article est fait pour un public de technicien·ne·s.

Quelques avertissements sont sans doute utiles :

— L'auteur de cet article (moi) ne sait pas tout. Autant que possible, j'ai essayé de ne parler que de ce qui était public, et que chacun pouvait vérifier mais, en sécurité, ça n'est pas toujours possible. Et, évidemment, vous ne trouverez pas ici d'informations confidentielles.
— Les gens qui savent quelque chose, et qui connaissent le sujet sont presque toujours employés par une organisation qui ne leur permet pas de tout raconter à l'extérieur.
— Le monde de la cybersécurité est très fermé, les informations ne circulent que dans des cercles restreints. Ce qui est publié n'est souvent que de vagues résumés, parfois délibérement déformés à des fins commerciales ou politiques. C'est une des raisons pour lesquelles la cybersécurité progresse si lentement, et pourquoi les légendes ont la vie dure : le baratin est libre alors que la vérité a les mains liées.

Cet article est basé en grande partie sur les rares articles techniques sérieux publiés sur le sujet (dans l'ordre chronologique) :

— L'article de Talos <https://blog.talosintelligence.com/2018/11/dnspionage-campaign-targets-
html>, qui fut apparemment le premier, à un moment où l'ampleur de la campagne n'était pas encore évidente,
— Celui de Fireye <https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijackin
html> (que je trouve peu détaillé, et dont les explications DNS sont confuses),
— Celui de CrowdStrike <https://www.crowdstrike.com/blog/widespread-dns-hijacking-activity-
> qui, sauf erreur, a été le premier à donner des IOC (élements précis qu'on peut vérifier, les adresses IP utilisées, par exemple), IOC que j'utilise par la suite,
— L'article de Brian Krebs <https://krebsonsecurity.com/2019/02/a-deep-dive-on-the-recent-wide
>, le plus complet.

Cet article sera malheureusement assez décousu, sautant d'un sujet à l'autre. l'idée est d'expliquer en français quelques points techniques subtils sur ces attaques.

Donc, d'abord, un résumé. La série d'attaques qui a eu lieu au moins d'octobre à décembre 2018 reposait en grande partie sur le **détournement de noms de domaine**. Le détournement ("*hijacking*", d'ailleurs un collègue me dit que ça peut s'écrire "*highjacking*") de noms de domaine consiste à usurper l'identité d'un titulaire ou d'un autre responsable d'un nom de domaine pour changer les informations associées à un nom. Voici par exemple le panneau de contrôle Web de Gandi :

Ce panneau est protégé par un mot de passe, auquel on peut ajouter un deuxième facteur d'authentification. Si quelqu'un peut mettre la main sur ces mécanismes d'authentification, il peut se faire passer pour le vrai responsable du nom, et changer les informations. On voit que cette attaque n'est **pas** une attaque DNS, le protocole DNS n'y ayant joué aucun rôle. Il s'agit d'une attaque contre le système d'**avitaillement** des noms de domaine (leur création et modification). Par contre, elle va avoir des conséquences sur le DNS. Et c'est encore plus vrai si le nom détourné est le nom d'un serveur de noms faisant autorité. On voit également que cette attaque n'était pas de haute technologie, et reposait probablement sur des méthodes de hameçonnage et d'ingénierie sociale classiques.

Les attaques par détournement de nom de domaine sont classiques et anciennes. Sur ce blog, j'avais déjà parlé en détail de celle contre le New York Times <https://www.bortzmeyer.org/attaques-sea.html> en 2013 et de celle contre Wikileaks <https://www.bortzmeyer.org/observations-wikileaks.html> en 2017. Il y en a eu d'autres commes celles contre Canal + et Météo France en 2016. La nouveauté des attaques de 2018, si nouveauté il y a, est dans leur caractère plus systématique et professionnel, probablement au sein d'un groupe unique. (Ne me demandez pas qui ; je n'en sais rien.)

Je m'aperçois que je m'emballe, j'ai déjà parlé du DNS alors que je voulais garder cela pour plus tard. Le DNS est à la fois une technologie indispensable de l'Internet, et une des plus mal connues. La lecture des articles qui parlent de DNS est souvent déprimante, en raison du nombre d'erreurs. Donc, pour lire la suite de cet article, il vaut mieux être au courant du vocabulaire des noms de domaine et du DNS, tel que compilé dans le RFC 8499 [1]. Il est notamment **crucial** de noter que parler de « serveur DNS » tout court est fortement déconseillé. Il y a les **résolveurs** et il y a les **serveurs faisant autorité** et ce sont deux choses très différentes. Dans le RFC 8499, vous allez également devoir réviser les notions de **bailliage** et de **colle <https://www.afnic.fr/observatoire-ressources/papier-expert/le-dns-ca-colle-ou-ca-ne-colle-pas/>**.

Après les préliminaires, lançons-nous dans les attaques de 2018. D'abord, peut-on vérifier les faits mentionnés dans les articles cités plus haut, ou bien devons-nous faire une confiance aveugle ? L'article de Crowdstrike ou celui de Krebs donnent des détails techniques précis, qu'on peut vérifier. (Je classe automatiquement les articles qui ne donnent aucun nom, aucune adresse IP, dans la catégorie « pas sérieux ».) Comme ces articles concernent des événements passés, on ne peut pas utiliser les clients DNS comme dig aujourd'hui, il faut faire appel à des outils historiques comme DNSDB <https://www.bortzmeyer.org/dnsdb.html>, qui ne sont pas toujours accessibles publiquement. Prenons l'exemple du ministère des affaires étrangères égyptien. DNSDB nous montre :

```
;;  bailiwick: gov.eg.
;;      count: 3
;; first seen: 2018-11-14 18:41:30 -0000
;;  last seen: 2018-11-14 20:05:40 -0000
mail.mfa.gov.eg. IN A 188.166.119.57
```

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc8499.txt

On y voit que le 14 novembre 2018, et peut-être également avant et après (DNSDB ne voit pas tout le trafic DNS, loin de là), `mail.mfa.gov.eg` avait comme adresse IP `188.166.119.57`, une des adresses listées dans les IOC de CrowdStrike. (L'adresse IP habituelle de ce serveur, avant et après, est `41.191.80.13`.) L'adresse IP utilisée par les attaquants est hébergée chez DigitalOcean, ce qu'on peut voir avec whois.

DNSDB permet également de chercher par le contenu. On peut voir ainsi les autres noms pointant (ou ayant pointé, parfois longtemps avant) vers cette adresse :

```
mail.mfa.gov.eg. IN A 188.166.119.57
sm2.mod.gov.eg. IN A 188.166.119.57
mail.mod.gov.eg. IN A 188.166.119.57
mail.noc.ly. IN A 188.166.119.57
embassy.ly. IN A 188.166.119.57
egypt.embassy.ly. IN A 188.166.119.57
...
```

Si nous faisons ce même exercice de recherche avec une autre adresse trouvée dans la liste de CrowdStrike :

```
ns0.idm.net.lb. IN A 139.59.134.216
sa1.dnsnode.net. IN A 139.59.134.216
fork.sth.dnsnode.net. IN A 139.59.134.216
plinkx.info. IN A 139.59.134.216
...
```

On trouve de vieilles informations (`plinkx.info` n'existe plus depuis 2017) mais aussi d'autres noms comme `ns0.idm.net.lb`, au Liban. Comme son nom l'indique, c'est un serveur DNS, et on voit qu'il fait autorité pour le domaine :

```
% dig @ns0.idm.net.lb NS idm.net.lb
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54194
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 4
...
;; ANSWER SECTION:
idm.net.lb.  3600 IN NS sf.idm.net.lb.
idm.net.lb.  3600 IN NS ns0.idm.net.lb.
...
;; SERVER: 2a00:1590:3c::2#53(2a00:1590:3c::2)
;; WHEN: Tue Feb 26 20:40:26 CET 2019
;; MSG SIZE  rcvd: 134
```

DNSDB nous indique que cette adresse a changé pendant le moment où l'attaque était à son maximum :

```
;;  bailiwick: lb.
;;      count: 2
;; first seen: 2018-12-18 15:00:27 -0000
;;  last seen: 2018-12-18 15:00:27 -0000
ns0.idm.net.lb. IN A 139.59.134.216
```

Cela illustre un point important de cette attaque : elle ne visait pas que des serveurs « finaux » (serveur HTTP ou SMTP) mais aussi des serveurs DNS, afin de pouvoir envoyer de fausses réponses aux requêtes DNS.

Notez aussi la ligne marquée "*bailiwick*" (bailliage). L'information mensongère n'était pas dans la zone elle-même, mais dans la zone parente (`.lb` pour `ns0.idm.net.lb`). Cela montre que l'attaquant est bien passé par le bureau d'enregistrement et pas par l'hébergeur DNS, puisqu'il a pu modifier les informations au registre « du dessus ».

Et si vous n'avez pas accès à DNSDB ou pas confiance dans leurs résultats ? Vous pouvez essayer aussi avec PassiveDNS.cn <https://www.bortzmeyer.org/passivedns-cn.html>, qui nous trouve :

```
mail.mfa.gov.eg A In rrset
-------
Record times: 2018-10-22 17:27:09 -- 2019-02-26 18:45:45
Count: 807
mail.mfa.gov.eg A 41.191.80.13

Record times: 2014-08-19 13:08:27 -- 2018-10-22 11:27:47
Count: 1398
mail.mfa.gov.eg A 41.191.80.12

Record times: 2017-11-21 00:39:59 -- 2018-10-21 10:42:56
Count: 951
mail.mfa.gov.eg A 41.191.80.12
mail.mfa.gov.eg A 41.191.80.13
```

Ah, oui, le monde est cruel. Le service chinois de "*passive DNS*" a beaucoup moins de points de mesure, et n'a pas vu le court moment du détournement. Même problème avec `circl.lu`, qui, pour le serveur de noms libanais, voit juste :

```
{"count": 1724, "origin": "https://www.circl.lu/pdns/", "time_first": 1477641718, "rrtype": "A", "rrname": "
```

Bref, difficile de se passer de DNSDB.

Si vous avez bien regardé plus haut les noms qui ont pointé vers `139.59.134.216`, vous avez peut-être remarqué `fork.sth.dnsnode.net`. C'est encore un serveur de noms, appartenant à un hébergeur important, Netnod. Cette société a publiquement communiqué <https://www.netnod.se/news/statement-on-man-in-the-middle-attack-against-netnod> à propos de cette attaque. La machine en question est également un serveur de noms, et c'est une nouvelle illustration de l'utilisation de serveurs de noms pour une attaque très indirecte, où le pirate change l'adresse IP du serveur de noms pour ensuite pouvoir répondre ce qu'il veut. `fork.sth.dnsnode.net` est utilisé par des TLD comme `.ps` ou `.lb` (mais aussi par des TLD sans lien avec le Moyen-Orient comme `.aq`). DNSDB montre au moins deux détournements :

```
;;  bailiwick: net.
;;      count: 9308
;; first seen: 2018-12-14 12:09:32 -0000
;;  last seen: 2018-12-24 12:17:24 -0000
fork.sth.dnsnode.net. IN A 82.196.11.127

;;  bailiwick: dnsnode.net.
;;      count: 63
;; first seen: 2018-12-24 15:21:49 -0000
;;  last seen: 2018-12-27 19:24:23 -0000
fork.sth.dnsnode.net. IN A 139.59.134.216
```

82.196.11.127 est également DigitalOcean, un hébergeur grand-public où le pirate était perdu au milieu d'autres utilisateurs. (Rien n'indique que cet hébergeur ait quoi que ce soit à voir avec l'attaque ; ils ont juste été utilisés par le pirate.) Notez que les deux adresses mensongères venaient de bailliage différents : la zone parente dans le premier cas, et la zone fille dans le second.

Outre les adresses IP, l'article de CrowdStrike nous apprend que les attaquants ont également utilisé des noms comme cloudnamedns.com. Si le domaine n'existe plus, on retrouve son nom dans le détournement des services de renseignement jordanien :

```
;;  bailiwick: gov.jo.
;;      count: 67
;; first seen: 2017-02-07 08:17:10 -0000
;;  last seen: 2017-02-12 23:27:29 -0000
gid.gov.jo. IN NS ns1.cloudnamedns.com.
gid.gov.jo. IN NS ns2.cloudnamedns.com.
```

(Notez la date : c'était bien avant que l'affaire soit publique.) Ce cas illustre le fait que les attaquants ont tantôt changé des adresses IP (enregistrements DNS de type A), tantôt des listes de serveurs de noms (enregistrements DNS de type NS). Dans le cas de gov.eg, on ne trouve pas de trace de changement des NS, alors que, pour gid.gov.jo, on voit ci-dessus le changement de NS. Changer les NS dans la zone parente nécessite d'avoir accès au bureau d'enregistrement. Changer les adresses IP nécessite un accès à l'hébergeur DNS, ou bien au bureau d'enregistrement s'il s'agit d'enregistrements dits de colle <https://www.afnic.fr/observatoire-ressources/papier-expert/le-dns-ca-colle-ou-ca-ne-colle-pas/>. (Notez que l'hébergeur DNS peut être également le bureau d'enregistrement, ou bien être le titulaire lui-même, ou encore être un tiers.)

DNSSEC a souvent été mentionné comme une technique à déployer, voire comme une solution qui aurait empêché cette attaque. Ce sont en fait deux questions distinctes. Oui, DNSSEC, normalisé dans le RFC 4033 et suivants, est une bonne solution, et devrait être déployé partout depuis longtemps. (Vous pouvez voir l'arborescence DNSSEC du domaine de ce blog sur DNSviz <http://dnsviz.net/d/bortzmeyer.org/dnssec/>.) Mais, comme toutes les techniques de sécurité, DNSSEC ne résout pas **tous** les problèmes. DNSSEC signe les enregistrements DNS. Un résolveur DNS **validant** (qui vérifie les signatures) peut alors détecter les enregistrements modifiés et les rejeter. DNSSEC protège, par exemple, contre un serveur secondaire faisant autorité qui serait malhonnête ou piraté. Il protège également contre les attaques de type Kaminsky <https://www.bortzmeyer.org/comment-fonctionne-la-faille-kaminsky.html>.

Normalisé depuis longtemps (le RFC 4033 date de quatorze ans) et déployé dans la racine du DNS et dans les TLD importants comme .fr et .com depuis 2009-2011, DNSSEC devrait aujourd'hui être présent partout. Les zones DNS importantes devraient être signées, et les résolveurs devraient valider. Bien sûr, mieux vaut tard que jamais. Si, suite aux attaques du moment, davantage d'organisations déploient DNSSEC, c'est parfait.

Mais DNSSEC aurait-il aidé **dans ces cas précis** ? DNSSEC, on l'a vu, permet de s'assurer que les données n'ont pas été modifiées entre l'origine (l'endroit où sont gérées les données) et le résolveur validant. Mais si les données sont fausses dès l'origine ? Le bon sens nous dit qu'il ne sert à rien de signer des données fausses. Si l'attaquant a le contrôle de l'origine (par exemple le serveur DNS maître), il peut modifier les données et signer des données mensongères. Ou bien il peut simplement retirer l'enregistrement DS dans la zone parente, indiquant ainsi que la zone n'est pas signée. Pour citer Paul Ebersman, « "*DNSSEC isn't useless but it solves one specific problem*" ».

Ça, c'est la théorie, mais la pratique est plus compliquée. D'abord, les attaquants ne sont pas parfaits. Il y a des amateurs, des professionnels, et des professionnels compétents. Et même ces derniers font des erreurs. Lors de détournements de noms signés avec DNSSEC, il a déjà été observé que les attaquants, bien qu'ils ont acquis le pouvoir de changer également les informations DNSSEC, n'y pensent pas toujours. Et même s'ils y pensent, le temps n'est pas sous leur contrôle, ce qui peut rendre DNSSEC efficace, même en cas de piratage d'un registre <https://www.bortzmeyer.org/piratage-registre-dnssec.html>. L'article de Krebs cité plus haut <https://krebsonsecurity.com/2019/02/a-deep-dive-on-the-r> donne d'ailleurs le témoignage de l'hébergeur PCH, qui explique comment DNSSEC a partiellement empêché l'exploitation par le pirate de ses succès antérieurs. Il faut faire très attention, en sécurité, à ne pas se braquer exclusivement sur des solutions théoriquement parfaites. Ce qu'on cherche à faire, ce n'est pas à rendre impossible toute attaque (c'est irréaliste), mais à gêner le plus possible l'attaquant. La plupart des serrures ne résistent pas longtemps à un cambrioleur professionnel, équipé de matériel de qualité. Mais on ne renonce pas à mettre des serrures pour autant : elles bloquent le cambrioleur amateur, et elles gênent même les plus compétents, ce qui peut les empêcher d'aller jusqu'au bout. Pour citer Paul Ebersman, « *"we are in a world now where every layer of security we can add is probably a good idea and having a day to notice could be handy"* ».

Bref, attaques du moment ou pas, ce serait une bonne chose que pousser le déploiement de DNSSEC. Comme DNSSEC consiste en la **signature** des zones et leur **validation**, deux catégories d'acteurs doivent agir : les gérants des zones (cela peut être l'hébergeur DNS, ou bien le titulaire de la zone), et les gérants des résolveurs (typiquement le FAI ou le service informatique de votre organisation). Pourquoi n'ont-ils pas encore agi ? Les raisons sont variées, mais c'est l'occasion de rappeler que la sécurité, ce n'est pas juste pousser des cris quand une attaque spectaculaire est révélée. Cela nécessite du temps, et des efforts constants. Une des raisons du déploiement insuffisant est peut-être l'étonnante quantité de nimportequoi qu'on trouve dans les médias au sujet de DNSSEC. Comme quand un article <https://business.lesechos.fr/directions-numeriques/technologie/cybersecurite/0600763925658-ale> php> explique que DNS chiffre (non) et « rend les données illisibles » (certainement pas).

Arrivé·es là, mes lecteurices, qui sont très compétent·e·s, se disent probablement : « mais on s'en moque du détournement DNS, tout est protégé par TLS de nos jours, donc le détournement ne servira à rien ». Précisons : ce n'est pas tant TLS qui pourrait permettre de détecter un détournement, mais l'authentification fournie par PKIX/X.509 (ce que les médias appellent « certificat SSL », même si SSL est officiellement abandonné depuis trois ans - RFC 7568 - et que, de toute façon, ces certificats peuvent servir à d'autres usages). Normalement, en cas de détournement DNS, les visiteurs du serveur pirate auraient dû se heurter à un mauvais certificat, et la communication être coupée, non ?

Eh bien non, comme l'ont montré ces attaques. D'abord, il y a des services qui n'utilisent pas TLS ou une technique équivalente (c'est le cas du DNS, malgré le RFC 7858). Ensuite, il n'y a pas que les navigateurs Web. Les autres applications clientes oublient parfois <http://doi.acm.org/10.1145/2382196.2382204> de vérifier les certificats, ou bien ne coupent pas la communication si le certificat est invalide. Mais, surtout, ce qui relativise sérieusement la protection offerte par PKIX, c'est que, si on contrôle un nom de domaine, on peut avoir un certificat. Cela n'est certes pas vrai pour les certificats EV mais les DV, eux, peuvent être obtenus dès qu'on contrôle le domaine.

Et c'est bien ce qu'ont fait les pirates ! On peut le savoir grâce au fait qu'il existe plusieurs journaux stockant les certificats émis, et accessibles publiquement (RFC 6962). Prenons `crt.sh` pour y accéder, et un domaine égyptien cité plus haut :

```
;;  bailiwick: gov.eg.
;;      count: 3
;; first seen: 2018-11-14 18:41:30 -0000
;;  last seen: 2018-11-14 20:05:40 -0000
mail.mfa.gov.eg. IN A 188.166.119.57
```

Pendant cette courte période, l'attaquant a obtenu un certificat via Let's Encrypt, le 03 :d9 :d3 :e5 :a6 :2c :dc :87 :1c :b8 :0f :1
<https://crt.sh/?id=946136592>. L'attaquant avait donc un certificat parfaitement valable et reconnu par beaucoup de logiciels. TLS, PKIX et X.509 ne protégeaient plus.

Un autre exemple est celui d'un domaine albanais. DNSDB montre le détournement :

```
;;  bailiwick: asp.gov.al.
;;      count: 8
;; first seen: 2018-11-08 09:49:18 -0000
;;  last seen: 2018-11-08 10:06:17 -0000
mail.asp.gov.al. IN A 199.247.3.191
```

Et l'attaquant a eu un certificat <https://crt.sh/?id=929142682>. On notera que, contrairement à ce qui a parfois été écrit, il n'y a pas que Let's Encrypt qui a été utilisé par les pirates, ce dernier certificat venait d'une autre AC, Comodo. Puisqu'on parlait de DNSSEC, on notera que Comodo ne valide pas les domaines à travers un résolveur DNS validant...Pire, Comodo n'a pas révoqué les certificats émis pendant les détournements, alors qu'ils sont valables un an. (Ceux de Let's Encrypt, d'une durée de validité de trois mois, sont pour la plupart expirés.)

Une autre technique qui aurait pu aider est celle du verrouillage. L'idée est de demander au registre de ne pas accepter les modifications (changement des serveurs de noms, par exemple), sans une procédure additionnelle de déverrouillage (envoi de SMS à N contacts, auxquels au moins M d'entre eux doivent répondre, par exemple). La plupart des registres offrent cette possibilité (par exemple .fr <https://www.afnic.fr/fr/produits-et-services/services/fr-lock-par-l-afnic-3.html>), mais elle reste peu utilisée. Notez que vous ne pouvez pas voir, de l'extérieur, si un domaine est ainsi verrouillé. whois ne l'affiche pas, par exemple.

Outre DNSSEC et le verrouillage, un autre outil de sécurité important, mais souvent négligé, est la **supervision**. On a vu plus haut que les certificats émis étaient publics, et il est donc utile de superviser l'émission de certificats pour ses noms de domaine, pour voir si un méchant n'a pas réussi à en obtenir un.

Dommage, crt.sh n'a apparemment pas d'API mais, comme me le conseille Valentin Robineau, on peut utiliser celle de CertStream <https://medium.com/cali-dog-security/introducing-certstream-3fc13
Ici, j'utilise leur bibliothèque Python <https://github.com/CaliDog/certstream-python/>
avec un petit script (en ligne sur https://www.bortzmeyer.org/files/test-certstream.py)
qui n'affiche que les certificats pour des noms en .fr (le flux complet est évidemment très bavard) :

```
[2019-02-28T08:35:30] www.ilovemypet.fr (SAN: )
[2019-02-28T08:35:34] www.manaturopatheetmoi.fr (SAN: )
[2019-02-28T08:35:34] cdns.nicolaschoquet.fr (SAN: )
[2019-02-28T08:35:36] bmv-verre.fr (SAN: www.bmv-verre.fr)
[2019-02-28T08:35:36] www.armand-martin-osteo.fr (SAN: )
[2019-02-28T08:35:37] www.chiropracteur-thiais-nabe.fr (SAN: )
[2019-02-28T08:35:37] hekafrance.fr (SAN: www.hekafrance.fr)
[2019-02-28T08:35:50] mail.topocad-tech.fr (SAN: )
[2019-02-28T08:35:53] cherchons-trouvons.fr (SAN: cherchons-trouvons.odazs.com, cpanel.cherchons-trouvons.fr, ma
```

(Dans la réalité, bien sûr, on ne regarderait que les noms de ses domaines.)

Mais il n'y a pas que les certificats qu'on peut superviser. On peut aussi regarder son domaine avec whois et/ou avec le DNS pour être prévenu immédiatement d'un changement. C'est assez facile à programmer soi-même, pour intégration dans un système de supervision comme Icinga. Pour le DNS, il existe même des services tout faits comme l'excellent DNSspy <https://dnsspy.io/> (si vous en connaissez d'autre, merci de me les signaler).

La supervision ne peut que détecter le détournement, pas l'empêcher. À la base, le problème principal est de suivre les bonnes pratiques de sécurité, ce qui est toujours plus facile à dire qu'à faire. On peut déjà éviter de mettre le mot de passe de l'interface Web du BE sur un Post-It affiché dans l'"*open space*". (Ne riez pas : ça existe.) Au-delà, il faut envisager de durcir tous les mécanismes d'authentification. Lors des débats suivant cette attaque, pas mal de gens ont cité l'authentification à deux facteurs. C'est une bonne idée dans l'absolu mais son déploiement est freiné par la variété des solutions fermées et incompatibles. Si on n'avait à protéger que l'interface du BE ou de l'hébergeur DNS, ce serait simple, mais l'administrateur réseaux typique gère beaucoup de choses et, s'il activait l'authentification à deux facteurs partout, il devrait se trimbaler avec un grand nombre de dispositifs matériels. Il existe bien un protocole ouvert, décrit dans le RFC 6238, mais ce n'est pas celui qui est utilisé par tout le monde. Il ne suffit pas de crier « il faut faire du 2FA ! », il faut aussi accepter de discuter les problèmes pratiques de déploiement.

Quelques lectures qui peuvent vous intéresser, outre les articles techniques sérieux cités au début de cet article :

— De bons textes, plein de sages avis, sur la sécurisation de vos noms de domaine : le guide des bonnes pratiques de l'ANSSI <https://www.ssi.gouv.fr/guide/bonnes-pratiques-pour-lacquis> et le dossier de l'AFNIC sur la même question <https://www.afnic.fr/fr/ressources/publications/dossiers-thematiques/securiser-la-gestion-des-noms-de-domaine.html>.
— Le communiqué de l'ICANN <https://www.icann.org/news/announcement-2019-02-22-en>.
— Un bon communiqué de SIDN <https://www.sidnlabs.nl/a/weblog/nl-not-affected-by-globa language_id=2&langcheck=true>, le registre de .nl, décrivant calmement le problème (avec de bons conseils dans l'avant-dernier paragraphe.)
— Un court communiqué <https://blog.verisign.com/domain-names/revisiting-how-registran> du registre de .com.
— Pour les gens pressés, Ars Technica a fait un résumé pas trop mauvais <https://arstechnica.com/information-technology/2019/02/inside-the-dnspionage-hacks-that-hijack-domain>.
— Des semaines après, Talos a publié un rapport <https://blog.talosintelligence.com/2019/04/seaturtle.html> avec peu d'informations nouvelles, et des grosses erreurs sur la notion de registre.
— Beaucoup d'articles sensationnalistes, voire ridicules, ont été publiés. Un exemple est cet article <https://www.estrepublicain.fr/faits-divers/2019/02/23/gigantesque-cyberattaque-i> mais il est loin d'être le seul ; méfiez-vous des médias.
— Beaucoup d'articles contiennent des erreurs, parfois sérieuses. C'est le cas de cet article <https://www.developpez.com/actu/248286/Internet-est-en-proie-a-une-vague-d-attaques-in>, qui invente que l'ICANN aurait été « reconnue d'utilité publique » (par qui ???), qui cite une attaque dDoS sans aucun rapport avec l'attaque actuelle, et qui mélange détournement de noms de domaine et attaques par réflexion <https://www.bortzmeyer.org/attaques-reflexion.html>. De même, cet autre article <https://www.latribune.fr/opinions/tribunes/une-attaque-qui-vise-le-coeur-d-internet-serait-en-cours-808677.html> prétend qu'on ne peut pas utiliser TCP pour le DNS (les auteurs auraient dû lire le RFC 7766), prétend que DNSSEC « introduit de l'aléatoire dans les requêtes » (!!!), ajoute que DNSSEC chiffre (!!!) et finit par ajouter des certificats imaginaires dans DNSSEC. Un autre exemple est cet autre article

<https://www.futura-sciences.com/tech/actualites/securite-tout-ce-vous-devez-savoir-
> : contrairement à ce qu'il dit, l'ICANN n'a pas été piratée (et n'a pas signalé un tel piratage, le gestionnaire de mots de passe n'a absolument rien à voir avec ce piratage, utiliser Cisco OpenDNS n'aurait protégé, puisque l'attaque portait sur le domaine lui-même, et la publicité pour le VPN à la fin est non seulement indication de malhonnêteté mais est absurde : utiliser un VPN n'aurait rien changé ici. La médiocrité de l'information que reçoit le lecteur ou la lectrice ordinaire a de quoi inquiéter, car on n'améliorera pas la sécurité de l'Internet sans un minimum de compréhension du problème.

— En français, plusieurs articles ont présenté une vue plus informée du problème : l'article de Next Inpact <https://www.nextinpact.com/brief/non--internet-n-est-pas-mort-ce-week-end--mai
htm>, celui du Monde <https://www.lemonde.fr/pixels/article/2019/02/25/non-une-attaque-ma
5427997_4408996.html> ou cet interview sur France TV info <https://www.francetvinfo.
fr/internet/securite-sur-internet/une-attaque-identifiee-et-pratiquee-depuis-des-ann
3204117.html>.

---

https://www.bortzmeyer.org/dnspionage.html