Saisie de noms de domaine par Microsoft

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 9 décembre 2021

https://www.bortzmeyer.org/saisie-domaines-par-microsoft.html

---

Il y a quelques jours, la justice étatsunienne a saisi, sur demande de Microsoft, un certain nombre de domaines, et les a transférés à cette société. Quelques informations techniques concrètes suivent pour celles et ceux qui seraient intéressé[Caractère Unicode non montré [1]]es.

D'abord, le jugement du 2 décembre (trouvé par Rayna Stamboliyska, merci beaucoup) : une copie en ligne <https://www.documentcloud.org/documents/21138969-nickel_bc_order-granting-tro>. En gros, Microsoft a identifié des noms de domaine utilisés par un groupe de délinquants nommé Nickel (apparemment entre autres pour contrôler des botnets composés de machines Microsoft Windows). La société a donc demandé à la justice de saisir ces noms. Cela marche car ces domaines étaient dans les TLD `.com` et `.org`, TLD gérés par des registres étatsuniens (alors que beaucoup de gens croient qu'ils ont un statut « international »). La justice a donné raison à Microsoft et ordonné le transfert des noms. Techniquement, c'est l'équivalent d'un détournement de nom de domaine ; Microsoft, ayant désormais le contrôle du nom, peut changer les informations associées et, par exemple, envoyer le trafic vers un serveur qu'ils contrôlent. La liste de ces noms figure dans l'annexe A du jugement.

Prenons un de ces noms au hasard, `optonlinepress.com`. Une requête whois nous montre le nouveau titulaire (on admire la célérité de l'opération, effectuée le lendemain du jugement) :

```
% whois optonlinepress.com
...
Updated Date: 2021-12-03T21:42:26Z
...
Registrant Name: Digital Crimes Unit Digital Crimes Unit
Registrant Organization: Microsoft Corporation
Registrant Street: One Microsoft Way,
Registrant City: Redmond
Registrant State/Province: WA
Registrant Postal Code: 98052
Registrant Country: US
...
```

1. Car trop difficile à faire afficher par LaTeX

(Attention, .com est un registre mince, et les informations au registre peuvent être différentes de celles au BE, notamment si l'injonction judiciaire a visé le registre sans prévenir le BE. Mais, ici, tout est cohérent.)

Le domaine est désormais délégué <https://dns.bortzmeyer.org/optonlinepress.com/NS> aux serveurs DNS faisant autorité <https://www.bortzmeyer.org/serveur-dns-faisant-autorite.html> de Microsoft (ici, avec l'outil check-soa <https://framagit.org/bortzmeyer/check-soa>) :

```
% check-soa optonlinepress.com
NS104A.microsoftinternetsafety.net.
13.107.222.41: OK: 1
NS104B.microsoftinternetsafety.net.
13.107.206.41: OK: 1
ns001.microsoftinternetsafety.net.
13.107.222.41: OK: 1
ns002.microsoftinternetsafety.net.
13.107.206.41: OK: 1
```

(On notera que la liste des serveurs n'est pas la même dans la zone parente, .com et dans la zone optonlinepress.com. C'est une erreur de configuration fréquente et Zonemaster <https://zonemaster.fr> proteste à juste titre <https://zonemaster.fr/result/999ab87c10fd6bb5>. Ici, encore plus rigolo, les serveurs supplémentaires ont la même adresse IP.)

DNSDB <https://www.bortzmeyer.org/dnsdb.html> nous montre l'ancienne configuration :

```
;;  bailiwick: com.
;;      count: 136
;; first seen: 2020-06-17 19:04:12 -0000
;;  last seen: 2021-12-01 16:37:44 -0000
optonlinepress.com. IN NS ns67.domaincontrol.com.
optonlinepress.com. IN NS ns68.domaincontrol.com.
```

La nouvelle étant :

```
;;  bailiwick: com.
;;      count: 4
;; first seen in zone file: 2021-12-04 22:50:22 -0000
;;  last seen in zone file: 2021-12-07 22:50:26 -0000
optonlinepress.com. IN NS ns104a.microsoftinternetsafety.net.
optonlinepress.com. IN NS ns104b.microsoftinternetsafety.net.
```

L'adresse IP pour le nom optonlinepress.com est désormais 40.83.198.93 (chez Microsoft) alors qu'elle était auparavant 172.105.98.76 (chez le gros hébergeur Linode), qui ne répond plus aujourd'hui. D'ailleurs, les anciens serveurs faisant autorité répondent toujours pour ce nom (ce qui est courant en cas de saisie judiciaire, l'ancien hébergeur n'ayant pas été prévenu) :

```
%  dig +norecurse @ns67.domaincontrol.com. ANY optonlinepress.com

; <<>> DiG 9.16.22-Debian <<>> +norecurse @ns67.domaincontrol.com. ANY optonlinepress.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1600
;; flags: qr aa; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1472
;; QUESTION SECTION:
;optonlinepress.com. IN ANY

;; ANSWER SECTION:
optonlinepress.com. 600 IN A 172.105.98.76
optonlinepress.com. 3600 IN NS ns67.domaincontrol.com.
optonlinepress.com. 3600 IN NS ns68.domaincontrol.com.
optonlinepress.com. 3600 IN SOA ns67.domaincontrol.com. dns.jomax.net. (
2020111802 ; serial
28800      ; refresh (8 hours)
7200       ; retry (2 hours)
604800     ; expire (1 week)
600        ; minimum (10 minutes)
)

;; Query time: 12 msec
;; SERVER: 2603:5:2174::2c#53(2603:5:2174::2c)
;; WHEN: Thu Dec 09 10:53:43 CET 2021
;; MSG SIZE  rcvd: 164
```

L'affaire a fait l'objet d'un article sur ArsTechnica <https://arstechnica.com/information-technology/2021/12/microsoft-seizes-domains-used-by-highly-sophisticated-hackers-in-china/> qui semble essentiellement reprendre l'article officiel de Microsoft <https://blogs.microsoft.com/on-the-issues/2021/12/06/cyberattacks-nickel-dcu-china/>, qui est très médiocre (utilisant au hasard des termes comme "*server*" et "*website*", et mélangeant tout).