Attaques de la Syrian Electronic Army contre les noms de domaines

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 27 août 2013. Dernière mise à jour le 28 août 2013

https://www.bortzmeyer.org/attaques-sea.html

Mardi 27 août, la « "*Syrian Electronic Army*" » a attaqué plusieurs noms de domaines importants, comme ceux du New York Times et de Twitter. Voici mon résumé, ainsi que des éléments concrets que j'avais recueilli sur le moment.

L'attaque a porté sur le bureau d'enregistrement Melbourne IT. Une fois cet intermédiaire piraté, la SEA a pu modifier à sa guise les données et notamment les serveurs de noms des domaines visés.

Ces données ont été récoltées entre 21 et 22 h UTC le 27 août. D'abord, le piratage du domaine `nytimes.com`. Mon Unbound sur ma machine (qui fait suivre les requêtes aux résolveurs de Free) voit :

```
% dig SOA nytimes.com.

; <<>> DiG 9.9.2-P1 <<>> SOA nytimes.com.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8602
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;nytimes.com. IN SOA

;; ANSWER SECTION:
nytimes.com. 86308 IN SOA ns1.syrianelectronicarmy.com. admin.sea.sy. 2013082701 86400 7200 3600000 86400

;; AUTHORITY SECTION:
nytimes.com. 86374 IN NS ns1.syrianelectronicarmy.com.
nytimes.com. 86374 IN NS ns2.syrianelectronicarmy.com.

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Aug 27 22:59:11 2013
;; MSG SIZE  rcvd: 145
```

À ce stade, on ne peut pas encore dire s'il y a empoisonnement DNS ou piratage du registre ou du bureau d'enregistrement ?

Quelques minutes après, en demandant directement au registre :

```
; <<>> DiG 9.9.2-P1 <<>> @d.gtld-servers.net. NS nytimes.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2190
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 3
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;nytimes.com. IN NS

;; AUTHORITY SECTION:
nytimes.com. 172800 IN NS ns27.boxsecured.com.
nytimes.com. 172800 IN NS ns28.boxsecured.com.
```

Ces `boxsecured.com` (un hébergeur états-unien) sont suspects : l'un répond `REFUSED`, l'autre donne un SOA étrange :

```
; <<>> DiG 9.9.2-P1 <<>> @212.1.211.141 SOA nytimes.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61161
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;nytimes.com. IN SOA

;; ANSWER SECTION:
nytimes.com. 86400 IN SOA ns5.boxsecured.com. ssuliman.hotmail.co.uk. 2013082703 86400 7200 3600000 86400

;; AUTHORITY SECTION:
nytimes.com. 86400 IN NS ns6.boxsecured.com.
nytimes.com. 86400 IN NS ns5.boxsecured.com.
```

whois semble indiquer que le domaine a bien été changé au registre (regardez la "*Updated Date*") :

```
Domain Name: NYTIMES.COM
Registrar: MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
Whois Server: whois.melbourneit.com
Referral URL: http://www.melbourneit.com
Name Server: NS27.BOXSECURED.COM
Name Server: NS28.BOXSECURED.COM
Status: serverDeleteProhibited
Status: serverTransferProhibited
Status: serverUpdateProhibited
Updated Date: 27-aug-2013
Creation Date: 18-jan-1994
Expiration Date: 19-jan-2014
```

Et Twitter ? `twitter.com` dans whois montre un piratage (le TLD `.sy` est la Syrie) :

```
Admin Name.......... SEA SEA
  Admin Address........ 1355 Market Street
  Admin Address........ Suite 900
  Admin Address........
  Admin Address. San Francisco
  Admin Address........ 94103
  Admin Address........ CA
  Admin Address........ UNITED STATES
  Admin Email.......... sea@sea.sy
  Admin Phone.......... +1.4152229670
  Admin Fax............ +1.4152220922
```

Même bureau d'enregistrement que `nytimes.com`, Melbourne IT. Par contre, les serveurs de noms n'ont pas été changés. Pourquoi ? Manque de temps pour la SEA ? Ou peut-être une protection spéciale, un « super-verrou » contre les modifications, soit au registre, soit au bureau d'enregistrement. Ce qui fait que, dans le cas de Twitter, l'utilisateur ordinaire ne voit rien. Par contre, `twimg.com` (hébergement d'images pour Twitter) a un whois analogue mais des serveurs de noms changés.

Une heure après, le registre de `.com` servait à nouveau la bonne information :

```
% dig @a.gtld-servers.net NS nytimes.com

; <<>> DiG 9.9.2-P1 <<>> @a.gtld-servers.net NS nytimes.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57384
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 3
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;nytimes.com. IN NS

;; AUTHORITY SECTION:
nytimes.com. 172800 IN NS dns.ewr1.nytimes.com.
nytimes.com. 172800 IN NS dns.sea1.nytimes.com.
CK0POJMG874LJREF7EFN8430QVIT8BSM.com. 86400 IN NSEC3 1 1 0 - CK0RFQAOES8CTVNVNH4G6Q85NOQAQ8I9 NS SOA RRSIG DNSKE
CK0POJMG874LJREF7EFN8430QVIT8BSM.com. 86400 IN RRSIG NSEC3 8 2 86400 20130903044137 20130827033137 8795 com. j5+
O6B9DUFQLHV3BU9UG6OASLHH80ECTS95.com. 86400 IN NSEC3 1 1 0 - O6C0FKNFS7M5TK0HI5HN4O5JKU9PTV22 NS DS RRSIG
O6B9DUFQLHV3BU9UG6OASLHH80ECTS95.com. 86400 IN RRSIG NSEC3 8 2 86400 20130903110913 20130827095913 8795 com. YE2

;; ADDITIONAL SECTION:
dns.ewr1.nytimes.com. 172800 IN A 170.149.168.134
dns.sea1.nytimes.com. 172800 IN A 170.149.173.133

;; Query time: 144 msec
;; SERVER: 192.5.6.30#53(192.5.6.30)
;; WHEN: Tue Aug 27 23:57:25 2013
;; MSG SIZE  rcvd: 603
```

(Le `sea1` dans `dns.sea1.nytimes.com` n'a rien à voir avec la SEA, il indique la ville, Seattle.) Mais il est amusant de noter que le whois au bureau d'enregistrement indiquait toujours la mauvaise information, ce qui semble indiquer que le registre a modifié l'information directement, en ignorant le bureau d'enregistrement :

```
% whois nytimes.com

Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

   Server Name: NYTIMES.COM
   IP Address: 141.105.64.37
   Registrar: MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
   Whois Server: whois.melbourneit.com
   Referral URL: http://www.melbourneit.com

   Domain Name: NYTIMES.COM
   Registrar: MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
   Whois Server: whois.melbourneit.com
   Referral URL: http://www.melbourneit.com
   Name Server: DNS.EWR1.NYTIMES.COM
   Name Server: DNS.SEA1.NYTIMES.COM
   Status: serverDeleteProhibited
   Status: serverTransferProhibited
   Status: serverUpdateProhibited
   Updated Date: 27-aug-2013
   Creation Date: 18-jan-1994
   Expiration Date: 19-jan-2014

>>> Last update of whois database: Tue, 27 Aug 2013 21:58:26 UTC <<<

[...]

Domain Name.......... nytimes.com
  Creation Date........ 1994-01-18
  Registration Date.... 2011-08-31
  Expiry Date.......... 2014-01-20
  Organisation Name.... SEA
  Organisation Address. 620 8th Avenue
  Organisation Address.
  Organisation Address.
  Organisation Address. New York
  Organisation Address. 10018
  Organisation Address. NY
  Organisation Address. UNITED STATES

Admin Name........... SEA SEA
  Admin Address........ SEA
  Admin Address........ 620 8th Avenue
  Admin Address........
  Admin Address. Syria
  Admin Address........ 10018
  Admin Address........ SY
  Admin Address........ SYRIAN ARAB REPUBLIC
  Admin Email.......... sea@sea.sy
  Admin Phone.......... +1.2125561234
  Admin Fax............

Tech Name............ NEW YORK TIMES DIGITAL
  Tech Address......... 229 West 43d Street
  Tech Address.........
  Tech Address.........
  Tech Address......... New York
  Tech Address......... 10036
  Tech Address......... NY
  Tech Address......... UNITED STATES
  Tech Email........... hostmaster@NYTIMES.COM
  Tech Phone........... +1.2125561234
  Tech Fax............. +1.1231231234
  Name Server.......... ns27.boxsecured.com
```

```
  Name Server.......... ns28.boxsecured.com
```

À noter que sharethis.com a aussi été attaqué <http://blogs.cisco.com/security/syrian-electronic-a
> mais qu'il est chez un bureau d'enregistrement différent et qu'il n'est pas sûr que la même méthode ait été employée.

Des rapports fiables signalent également un détournement de huffingtonpost.co.uk (un registre différent mais le même bureau d'enregistrement) mais je n'ai pas pu l'observer moi-même. Mais il est sûr que le problème ne frappait pas que .com. Voici la sortie du whois de twitter.co.uk, vingt minutes après que le .com ait été réparé :

```
% whois twitter.co.uk

    Domain name:
        twitter.co.uk

    Registrant:
        Twitter Inc

    Registrant type:
        Non-UK Corporation

    Registrant's address:
        1355 Market Street Suite 900
        San Francisco
        CA
        94103
        United States

    Registrar:
        Melbourne IT t/a Internet Names Worldwide [Tag = MELBOURNE-IT]
        URL: http://www.melbourneit.com.au/contacts

    Relevant dates:
        Registered on: 05-Mar-2005
        Expiry date:  05-Mar-2015
        Last updated:  27-Aug-2013

    Registration status:
        Registered until expiry date.

    Name servers:
        ns1.syrianelectronicarmy.com
        ns2.syrianelectronicarmy.com

    WHOIS lookup made at 23:20:51 27-Aug-2013

[...]
```

Cela plaide donc encore plus pour un piratage du bureau d'enregistrement, Melbourne IT, qui a été confirmé par Melbourne IT quelques heures après.

Quelques articles intéressants sur ce piratage :

— L'article officiel du New York Times <http://www.nytimes.com/2013/08/28/business/media/hacking-attack-is-suspected-on-times-web-site.html>
— Et celui de Twitter <http://status.twitter.com/post/59528478030/twitter-service-issue>

— L'étude de CloudFlare <http://blog.cloudflare.com/details-behind-todays-internet-hacks qui inclut la reconnaissance du piratage par Melbourne IT (dans un message qui a été envoyé à leurs clients mais pas rendu public)
— Mon interview par PCinpact <http://www.pcinpact.com/news/82014-detournement-nyt-et-twit htm>, discutant notamment de comment on pourrait améliorer la sécurité des noms de domaines.

Et c'est l'occasion de relire et revoir :

— Le Rapport sur la résilience de l'Internet en France <http://www.ssi.gouv.fr/fr/menu/actualites/l-observatoire-sur-la-resilience-de-l-internet-francais-publie-son-ra html>
— Mon tutoriel à la Journée du Conseil Scientifique de l'AFNIC <http://www.afnic.fr/fr/l-afnic-en-bref/actualites/actualites-generales/6132/show/succes-pour-la-journee- html> sur « La sécurité des noms de domaines »
— Duane Wessels a fait une excellente étude sur la réjuvenation <https://www.bortzmeyer.org/dns-propagation.html> des caches des serveurs DNS après la correction, présentée, à l'OARC en octobre 2013 <https://indico.dns-oarc.net/indico/materialDisplay.py?contribId=7&materialId=slides&confId=1>.