Le mystère DNS Free rebondit

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 24 avril 2016

https://www.bortzmeyer.org/free-dnssec-reloaded.html

J'ai déjà parlé ici <https://www.bortzmeyer.org/free-noblogs-dnssec.html> de la bogue DNS de Free affectant certains domaines signés avec DNSSEC. Six mois après, elle n'a pas été réparée et le problème se montre en fait encore plus complexe qu'à première vue.

Le problème a été signalé sur la liste FRnog et analysé par Rémy Duchet. En gros, certains usagers de Free n'arrivent pas à aller en . Si on regarde avec dig, on voit bien un problème DNS (ici, j'interroge explicitement un des résolveurs DNS officiels de Free, puisque j'ai un résolveur local <https://www.bortzmeyer.org/son-propre-resolveur-dns.html>) :

```
% dig @212.27.40.240 test-yann.myshopify.com

; <<>> DiG 9.9.5-9+deb8u6-Debian <<>> @212.27.40.240 test-yann.myshopify.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 393
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;test-yann.myshopify.com. IN A

;; Query time: 27 msec
;; SERVER: 212.27.40.240#53(212.27.40.240)
;; WHEN: Sun Apr 24 17:00:03 CEST 2016
;; MSG SIZE  rcvd: 52
```

Ah, en effet, nous avons un problème (SERVFAIL = "*Server Failure*"). Avec d'autres résolveurs de Free, pas de problème. Et ça varie dans le temps (en d'autres termes, des fois, ça marche, des fois, ça marche pas). On peut également tester avec les sondes RIPE Atlas <https://www.bortzmeyer.org/atlas-udm.html>, dans l'AS de Free, 12322 :

```
% atlas-resolve -r 500 --as 12322 -t A test-yann.myshopify.com
[ERROR: SERVFAIL] : 61 occurrences
[23.227.38.68 23.227.38.69 23.227.38.70 23.227.38.71] : 133 occurrences
[TIMEOUT(S)] : 1 occurrences
Test #3682131 done at 2016-04-24T14:57:13Z
```

Cela montre bien que certains résolveurs de Free ont le problème `SERVFAIL` mais pas tous.

Si on essaie avec l'option `+cd` (*"Checking Disabled"*, couper la validation DNSSEC), tout marche :

```
% dig +cd @212.27.40.240 test-yann.myshopify.com

; <<>> DiG 9.9.5-9+deb8u6-Debian <<>> +cd @212.27.40.240 test-yann.myshopify.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18276
;; flags: qr rd ra cd; QUERY: 1, ANSWER: 22, AUTHORITY: 4, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;test-yann.myshopify.com. IN A

;; ANSWER SECTION:
test-yann.myshopify.com. 1800 IN CNAME shops.shopify.com.
test-yann.myshopify.com. 1800 IN RRSIG CNAME 5 2 600 (
20160519013040 20160419013040 12663 myshopify.com.
K3oRwkmXUkzNYbFO1jNLGLrSkhaRRBnKeGvld9YdcZo+
nUOpJzGUECTzrzOTBGpbGXdJB5M3nJ6pebAGpr46m5Rk
HfG3+FOdgCRS+CG5lpu0+KC8w80718ywOFO8LROdIjwm
h4swblM+0Aft4o1lj5ChnCBefWgn2Cs4qSqMT0g= )
test-yann.myshopify.com. 1800 IN RRSIG CNAME 5 2 600 (
20160519013040 20160419013040 39852 myshopify.com.
lBsyv5zrQ4twd4LNzLrdQpHWyxL9SQGM2wfhVR/GfnWE
TXNV3wyW5bIwRDySbmdRg9RLiz9h1sBFByIeITYEJeKv
7daLBZSwoI7551mz0jJX5fMgEuW7FEFOP25pYb6p5o1r
lVFvc47+X8qTLaV5j0Uz+PXJjFBvF7GB4i3gFb0= )
test-yann.myshopify.com. 1800 IN CNAME shops.shopify.com.
test-yann.myshopify.com. 1800 IN RRSIG CNAME 5 2 600 (
20160519013040 20160419013040 12663 myshopify.com.
K3oRwkmXUkzNYbFO1jNLGLrSkhaRRBnKeGvld9YdcZo+
nUOpJzGUECTzrzOTBGpbGXdJB5M3nJ6pebAGpr46m5Rk
HfG3+FOdgCRS+CG5lpu0+KC8w80718ywOFO8LROdIjwm
h4swblM+0Aft4o1lj5ChnCBefWgn2Cs4qSqMT0g= )
test-yann.myshopify.com. 1800 IN RRSIG CNAME 5 2 600 (
20160519013040 20160419013040 39852 myshopify.com.
lBsyv5zrQ4twd4LNzLrdQpHWyxL9SQGM2wfhVR/GfnWE
TXNV3wyW5bIwRDySbmdRg9RLiz9h1sBFByIeITYEJeKv
7daLBZSwoI7551mz0jJX5fMgEuW7FEFOP25pYb6p5o1r
lVFvc47+X8qTLaV5j0Uz+PXJjFBvF7GB4i3gFb0= )
test-yann.myshopify.com. 1800 IN CNAME shops.shopify.com.
test-yann.myshopify.com. 1800 IN RRSIG CNAME 5 2 600 (
20160519013040 20160419013040 12663 myshopify.com.
K3oRwkmXUkzNYbFO1jNLGLrSkhaRRBnKeGvld9YdcZo+
nUOpJzGUECTzrzOTBGpbGXdJB5M3nJ6pebAGpr46m5Rk
HfG3+FOdgCRS+CG5lpu0+KC8w80718ywOFO8LROdIjwm
h4swblM+0Aft4o1lj5ChnCBefWgn2Cs4qSqMT0g= )
test-yann.myshopify.com. 1800 IN RRSIG CNAME 5 2 600 (
20160519013040 20160419013040 39852 myshopify.com.
lBsyv5zrQ4twd4LNzLrdQpHWyxL9SQGM2wfhVR/GfnWE
TXNV3wyW5bIwRDySbmdRg9RLiz9h1sBFByIeITYEJeKv
7daLBZSwoI7551mz0jJX5fMgEuW7FEFOP25pYb6p5o1r
```

```
1VFvc47+X8qTLaV5j0Uz+PXJjFBvF7GB4i3gFb0= )
test-yann.myshopify.com. 1800 IN CNAME shops.shopify.com.
test-yann.myshopify.com. 1800 IN RRSIG CNAME 5 2 600 (
20160519013040 20160419013040 12663 myshopify.com.
K3oRwkmXUkzNYbFO1jNLGLrSkhaRRBnKeGvld9YdcZo+
nUOpJzGUECTzrzOTBGpbGXdJB5M3nJ6pebAGpr46m5Rk
HfG3+FOdgCRS+CG5lpu0+KC8w80718ywOFO8LROdIjwm
h4swblM+0Aft4o1lj5ChnCBefWgn2Cs4qSqMT0g= )
test-yann.myshopify.com. 1800 IN RRSIG CNAME 5 2 600 (
20160519013040 20160419013040 39852 myshopify.com.
lBsyv5zrQ4twd4LNzLrdQpHWyxL9SQGM2wfhVR/GfnWE
TXNV3wyW5bIwRDySbmdRg9RLiz9h1sBFByIeITYEJeKv
7daLBZSwoI7551mz0jJX5fMgEuW7FEFOP25pYb6p5o1r
1VFvc47+X8qTLaV5j0Uz+PXJjFBvF7GB4i3gFb0= )
test-yann.myshopify.com. 1800 IN CNAME shops.shopify.com.
test-yann.myshopify.com. 1800 IN RRSIG CNAME 5 2 600 (
20160519013040 20160419013040 12663 myshopify.com.
K3oRwkmXUkzNYbFO1jNLGLrSkhaRRBnKeGvld9YdcZo+
nUOpJzGUECTzrzOTBGpbGXdJB5M3nJ6pebAGpr46m5Rk
HfG3+FOdgCRS+CG5lpu0+KC8w80718ywOFO8LROdIjwm
h4swblM+0Aft4o1lj5ChnCBefWgn2Cs4qSqMT0g= )
test-yann.myshopify.com. 1800 IN RRSIG CNAME 5 2 600 (
20160519013040 20160419013040 39852 myshopify.com.
lBsyv5zrQ4twd4LNzLrdQpHWyxL9SQGM2wfhVR/GfnWE
TXNV3wyW5bIwRDySbmdRg9RLiz9h1sBFByIeITYEJeKv
7daLBZSwoI7551mz0jJX5fMgEuW7FEFOP25pYb6p5o1r
1VFvc47+X8qTLaV5j0Uz+PXJjFBvF7GB4i3gFb0= )
test-yann.myshopify.com. 1800 IN CNAME shops.shopify.com.
test-yann.myshopify.com. 1800 IN RRSIG CNAME 5 2 600 (
20160519013040 20160419013040 12663 myshopify.com.
K3oRwkmXUkzNYbFO1jNLGLrSkhaRRBnKeGvld9YdcZo+
nUOpJzGUECTzrzOTBGpbGXdJB5M3nJ6pebAGpr46m5Rk
HfG3+FOdgCRS+CG5lpu0+KC8w80718ywOFO8LROdIjwm
h4swblM+0Aft4o1lj5ChnCBefWgn2Cs4qSqMT0g= )
test-yann.myshopify.com. 1800 IN RRSIG CNAME 5 2 600 (
20160519013040 20160419013040 39852 myshopify.com.
lBsyv5zrQ4twd4LNzLrdQpHWyxL9SQGM2wfhVR/GfnWE
TXNV3wyW5bIwRDySbmdRg9RLiz9h1sBFByIeITYEJeKv
7daLBZSwoI7551mz0jJX5fMgEuW7FEFOP25pYb6p5o1r
1VFvc47+X8qTLaV5j0Uz+PXJjFBvF7GB4i3gFb0= )
shops.shopify.com. 1800 IN A 23.227.38.71
shops.shopify.com. 1800 IN A 23.227.38.69
shops.shopify.com. 1800 IN A 23.227.38.70
shops.shopify.com. 1800 IN A 23.227.38.68

;; AUTHORITY SECTION:
shopify.com. 6458 IN NS ns4.p19.dynect.net.
shopify.com. 6458 IN NS ns3.p19.dynect.net.
shopify.com. 6458 IN NS ns1.p19.dynect.net.
shopify.com. 6458 IN NS ns2.p19.dynect.net.

;; Query time: 41 msec
;; SERVER: 212.27.40.240#53(212.27.40.240)
;; WHEN: Sun Apr 24 17:44:13 CEST 2016
;; MSG SIZE  rcvd: 2376
```

On a la réponse mais on voit bien qu'il y a un problème : ces enregistrements DNS `CNAME` ("*Canonical Name*") répétés ne sont pas normaux. Il ne sont pas dans les serveurs faisant autorité pour le domaine :

```
%  dig @ns1.p19.dynect.net test-yann.myshopify.com

; <<>> DiG 9.9.5-9+deb8u6-Debian <<>> @ns1.p19.dynect.net test-yann.myshopify.com
; (2 servers found)
```

```
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7499
;; flags: qr aa rd; QUERY: 1, ANSWER: 3, AUTHORITY: 3, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;test-yann.myshopify.com. IN A

;; ANSWER SECTION:
test-yann.myshopify.com. 600 IN CNAME shops.shopify.com.
test-yann.myshopify.com. 600 IN RRSIG CNAME 5 2 600 (
20160519013040 20160419013040 12663 myshopify.com.
K3oRwkmXUkzNYbFO1jNLGLrSkhaRRBnKeGvld9YdcZo+
nUOpJzGUECTzrzOTBGpbGXdJB5M3nJ6pebAGpr46m5Rk
HfG3+FOdgCRS+CG5lpu0+KC8w80718ywOFO8LROdIjwm
h4swblM+0Aft4o1lj5ChnCBefWgn2Cs4qSqMT0g= )
test-yann.myshopify.com. 600 IN RRSIG CNAME 5 2 600 (
20160519013040 20160419013040 39852 myshopify.com.
lBsyv5zrQ4twd4LNzLrdQpHWyxL9SQGM2wfhVR/GfnWE
TXNV3wyW5bIwRDySbmdRg9RLiz9h1sBFByIeITYEJeKv
7daLBZSwoI7551mz0jJX5fMgEuW7FEFOP25pYb6p5o1r
1VFvc47+X8qTLaV5j0Uz+PXJjFBvF7GB4i3gFb0= )

;; AUTHORITY SECTION:
test-winkel.myshopify.com. 60 IN NSEC test1012345.myshopify.com. CNAME RRSIG NSEC
test-winkel.myshopify.com. 60 IN RRSIG NSEC 5 3 60 (
20160519013040 20160419013040 12663 myshopify.com.
BHS+QE4Pdu0qFdTW2XHN4Z6mbiqu3eb89UhwO3f5/C7W
vpQmlNEmuYNlUlAHgUWbXvCwmDr+9k0bVZuiZh0UuSCp
pveXWvYzr6nJjCRy5CZoUJy6C60Dyt1LfW2kCNTXUdjX
Vp8HwMlKN0np6jxe2o/ryU/BphzdYA1OEmqp9/0= )
test-winkel.myshopify.com. 60 IN RRSIG NSEC 5 3 60 (
20160519013040 20160419013040 39852 myshopify.com.
I8LqnvjOSLhivVteqv6gqeeytZ9YZU9heYIj/hNfYUz+
vOQ2PQBCk7N0ujbI9vWpFkj+3YSNnsxBshxjVZfWQoLp
Cpde8Ir+zP8WK95/04VQBpU1HjI7QBAARkPCD0YCnTBY
U/hTVe6gcB43c9CFAUaJ5qynRmnTZFIsvtcGBz8= )

;; Query time: 22 msec
;; SERVER: 2001:500:90:1::19#53(2001:500:90:1::19)
;; WHEN: Sun Apr 24 17:45:54 CEST 2016
;; MSG SIZE  rcvd: 831
```

Donc, ce sont les résolveurs de Free qui les ont inventé. La bogue est clairement de la responsabilité de Free.

Dans mon article précédent <https://www.bortzmeyer.org/free-noblogs-dnssec.html>, j'avais émis l'hypothèse que le problème était lié à l'utilisation de `NSEC3` (RFC 5155[1]) et des jokers. Ici, la zone est signée avec `NSEC`, pas `NSEC3` (ce qui est curieux, d'ailleurs, puisque cela permet de connaitre la liste des clients de `shopify.com`), donc `NSEC3` ne semble pas responsable. On retrouve par contre les jokers, dont l'interaction avec DNSSEC est régulièrement une source d'ennuis. D'une façon ou d'une autre, une combinaison de caractéristiques de la zone `myshopify.com` déclenche la bogue, multiplie les `CNAME` (la réponse du résolveur de Free a une taille supérieure à la MTU d'Ethernet...), l'enregistrement `NSEC` obligatoire est supprimé, et paf.

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc5155.txt`

En résumé, je ne sais pas quel logiciel résolveur utilise Free (aucun des logiciels que je connais, comme Unbound ou BIND, ne montre ce comportement) mais il est bogué et devrait impérativement être réparé, si on veut que DNSSEC soit plus largement utilisé.

Et du côté de l'utilisateur ordinaire, que peut-on faire ? Le client final peut utiliser son propre résolveur <https://www.bortzmeyer.org/son-propre-resolveur-dns.html> (ce qui est une bonne idée, de toute façon), le webmestre qui veut publier des choses accessibles aux utilisateurs de Free ne peut pas grand'chose, à part peut-être configurer sa zone DNS de manière plus conservatrice (les jokers sont presque toujours une mauvaise idée).