Hijacking of public DNS servers in Turkey, through routing

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

First publication of this article on 29 March 2014. Last update on of 30 March 2014

http://www.bortzmeyer.org/dns-routing-hijack-turkey.html

A new step in the fight between the Turkish government and the Internet occurred recently when the access providers in Turkey started, not only to install lying DNS resolvers, but also to hijack the IP addresses of some popular open DNS resolvers, like Google Public DNS.

The first attempt of censorship by the Turkish government was to request (around 20 March) the IAP (Internet Access Providers), who typically provide a recursive DNS service to their users, to configure these recursors to lie, providing false answers when queried about censored names like `twitter.com`. This is a very common censorship technique, which is used sometimes for business reasons (lying about non-existing domain names, to direct the user to an advertisement page) and sometimes for plain censorship (this was done in France <http://pro.clubic.com/legislation-loi-internet/telechargement-illegal/actualite-604000-allostreaming-consorts-justice-ordonne-blocage.html>, Bulgaria, Ireland <http://www.independent.ie/business/technology/high-court-orders-six-in html>, etc).

An obvious workaround to this technique is to use other resolvers than the IAP's ones. Hence the calls on the walls of many Turkish cities to use a service like Google Public DNS, with the IP addresses of its resolvers

Now, the Turkish governement, replying to the reply, went apparently further. Before discussing what they have done, let's see the facts. We will use the network of RIPE Atlas probes <https://atlas.ripe.net> to query Google Public DNS from various places, in the world and in Turkey, since the excellent RIPE Atlas interface allows you to select probes based on many criteria, including the country. The probe can resolve names (like `twitter.com`, the first censored name) with its local DNS resolver (typically configured by a DHCP reply when the probe starts) but we won't use this possibility, we already know the the IAP's DNS resolvers in Turkey lie. We will instead instruct the Atlas probes to query Google Public DNS, at its IP address `8.8.4.4` (it is less known than `8.8.8.8` but Atlas have an automatic rate-limiter and, since so many people are currently investigating Turkish censorship, Atlas does not accept queries to `8.8.8.8`.)

First, to see the ground truth, let's ask a hundred probes worldwide to resolve `twitter.com`. The measurement ID is #1605067 for those who want to check (most Atlas measurements are public, anyone can download the results as a big JSON file and analyze them by themselves). Since Twitter is implemented by many machines, the IP addresses vary and it's normal. Here is an excerpt :

```
...
[199.59.148.10 199.59.149.198 199.59.150.7] : 2 occurrences
[199.16.156.38 199.16.156.6 199.16.156.70] : 8 occurrences
[199.59.149.230 199.59.150.39 199.59.150.7] : 5 occurrences
...
```

All IP addresses do belong to Twitter (checked with whois), which makes sense. Now, let's query only Turkish probes. There are ten available Atlas probes in Turkey. This is measurement #1605068. Here is the full result :

```
10 probes reported, 10 successes
[199.16.156.230 199.16.156.6 199.16.156.70] : 1 occurrences
[195.175.254.2] : 8 occurrences
[199.16.156.198 199.16.156.230 199.16.156.70] : 1 occurrences
Test done at 2014-03-29T16:57:38Z
```

Two probes give normal results, with three IP addresses, all in Twitter space. The majority of probes, eight, give an IP address at a Turkish provider ("*Turk Telekomunikasyon Anonim Sirketi*" alias `ttnet.com.tr`). So, there is clearly something fishy : **even when you request specifically Google Public DNS**, you get a lie.

We can measure with another censored name, `youtube.com` and we get similar results. In Turkey, measurement #1606453 reports :

```
10 probes reported, 10 successes
[173.194.34.160 173.194.34.161 173.194.34.162 173.194.34.163 173.194.34.164 173.194.34.165 173.194.34.166 17
[195.175.254.2] : 8 occurrences
[195.22.207.20 195.22.207.24 195.22.207.25 195.22.207.29 195.22.207.30 195.22.207.34 195.22.207.35 195.22.20
Test done at 2014-03-30T15:16:22Z
```

The same IP address is obtained, and of course it is not possible that the real Twitter and the real YouTube are hosted at the same place.

[All measurements show that two Atlas probes in Turkey do not see the hijacking. Why are they spared ? According to the manager of one of these probes, his entire network was tunneled to a foreign server, to escape filtering, which explains why the probe on the network saw normal DNS replies.]

If you try another well-known DNS resolver, such as OpenDNS, you'll get the same problem : a liar responds instead.

So, someone replies, masquerading as the real Google Public DNS resolver. Is it done by a network equipment on the path, as it is common in China where you get DNS responses even from IP addresses where no name server runs ? It seems instead it was a trick with routing : the IAP announced a route to the IP addresses of Google, redirecting the users to an IAP's own impersonation of Google Public DNS, a lying DNS resolver. Many IAP already hijack Google Public DNS in such a way, typically for business reasons (gathering data about the users, spying on them). You can see the routing hijack on erdems' Twitter feed <https://twitter.com/erdems/status/449922833070960641>, using Turkish Telecom looking glass : the routes are no normal BGP routes, with a list of AS numbers, they are injected locally, via the IGP (so, you won't see it in remote BGP looking glasses, unless someone in Turkey does the same mistake that Pakistan Telecom did with YouTube in 2008). Test yourself <http://lg.turktelekom.com.tr/> :

```
u*>? 8.8.4.4/32 100 None
212.156.250.157 None -
No As-Path
```

while a normal route wil look like :

```
u*>i 74.82.42.0/24 100 1
212.156.100.1 None -
6939
*i 74.82.42.0/24 100 1
212.156.100.1 None -
6939
```

(6939 being the origin AS of the remote route, here a foreign one, while `8.8.4.4/32` is local)

Another indication that the hijacking is not done by a man in the middle mangling any DNS reply (as it is done in China) is that, if you try a little-known open DNS resolver, there is no problem, even from Turkey, you get correct results (measurement #1605104).

Also, a traceroute to Google Public DNS shows the user is going to Turkish servers, unrelated to the Californian corporation (see this example `<https://twitter.com/esesci/status/449902883933126659/photo/1>`). RIPE Atlas probes can do traceroutes, too, but for the probes I used, the traceroute gets lost in the network of TTNET Turk Telekomunikasyon Anonim Sirketi, the lying DNS resolver, unlike the real Google Public DNS, does not reply to UDP traceroutes :

```
From:  212.58.13.159    8685    DORUKNET Doruk Iletisim ve Otomasyon Sanayi ve Ticaret A.S.,TR
Source address:  212.58.13.159
Probe ID:  3506
1    212.58.13.253    8685    DORUKNET Doruk Iletisim ve Otomasyon Sanayi ve Ticaret A.S.,TR    [3.98, 3.235, 3.
2    82.151.154.193    8685    DORUKNET Doruk Iletisim ve Otomasyon Sanayi ve Ticaret A.S.,TR    [3.15, 3.044, 3
3    212.156.133.117    9121    TTNET Turk Telekomunikasyon Anonim Sirketi,TR    [4.146, 4.807, 4.157]
4    [u'*', u'*', 'late', u'*']
5    81.212.204.205    9121    TTNET Turk Telekomunikasyon Anonim Sirketi,TR    [11.185, 10.657, 10.67]
6    81.212.204.149    9121    TTNET Turk Telekomunikasyon Anonim Sirketi,TR    [10.864, 11.007, 10.685]
7    ['late', u'*', 'late', u'*', u'*']
8    [u'*', u'*', u'*']
9    [u'*', u'*', u'*']
10    [u'*', u'*', u'*']
11    [u'*', u'*', u'*']
255    [u'*', u'*', u'*']
```

But RIPE Atlas probes are able to do traceroute with ICMP and, this time, it works :

```
From:  212.58.13.159    8685    DORUKNET Doruk Iletisim ve Otomasyon Sanayi ve Ticaret A.S.,TR
Source address:  212.58.13.159
Probe ID:  3506
1    212.58.13.253    8685    DORUKNET Doruk Iletisim ve Otomasyon Sanayi ve Ticaret A.S.,TR    [3.866, 3.13, 3.
2    82.151.154.193    8685    DORUKNET Doruk Iletisim ve Otomasyon Sanayi ve Ticaret A.S.,TR    [3.316, 3.012,
3    212.156.133.117    9121    TTNET Turk Telekomunikasyon Anonim Sirketi,TR    [4.362, 5.976, 4.394]
4    [u'*', u'*', 'late', u'*']
5    81.212.204.205    9121    TTNET Turk Telekomunikasyon Anonim Sirketi,TR    [13.922, 13.574, 13.753]
6    81.212.204.149    9121    TTNET Turk Telekomunikasyon Anonim Sirketi,TR    [13.933, 17.873, 13.571]
7    8.8.4.4    15169    GOOGLE - Google Inc.,US    [11.689, 11.761, 11.897]
```

Is the lying resolver a full standalone resolver or does it just proxy requests to the real servers, after censoring some names? To be sure, we ask the Atlas probes to query Google Public DNS with the name `whoami.akamai.net`, which is delegated to special Akamai servers in order to reply with the IP address of their DNS client (thanks to Alexander Neilson for the idea). Measurement #1606450 shows :

```
10 probes reported, 10 successes
[74.125.18.80] : 2 occurrences
[195.175.255.66] : 8 occurrences
Test done at 2014-03-30T14:49:39Z
```

We learn with whois that `74.125.18.80` is Google, `195.175.255.66` Turkish Telecom. So, no, Google Public DNS is not proxied but replaced by an impostor which is a full recursor.

There is no other easy way to be sure we talk to the real Google Public DNS or not : Google's servers, unfortunately, do not support the NSID identification system and, anyway, even if they did, it is easy to forge. The only real solution to be sure is the resolver you use, is cryptography. OpenDNS implements DNScrypt <http://www.dnscrypt.org/> but Google DNS has nothing.

Of course, DNSSEC would solve the problem, **if and only if** validation were done on the user's local machine, something that most users don't do today.

About censoring with DNS, I recommend the comprehensive report of AFNIC Scientific Council <http://www.afnic.fr/medias/documents/conseilscientifique/SC-consequences-of-DNS-based pdf>. Thanks to Sedat Kapano[Caractère Unicode non montré [1]]lu <https://twitter.com/esesci> for his measurements. Some other articles on this issue :

- My talk at the RIPE meeting in Warsaw in may : the slides (en ligne sur `http://www.bortzmeyer.org/files/bortzmeyer-google-dns-turkey.pdf`) (also hosted at RIPE <https://ripe68.ripe.net/presentations/158-bortzmeyer-google-dns-turkey.pdf>), and the video <https://ripe68.ripe.net/archives/video/177> (Flash unfortunately required),
- At BGPmon <http://www.bgpmon.net/turkey-hijacking-ip-addresses-for-popular-global >,
- At Google <http://googleonlinesecurity.blogspot.fr/2014/03/googles-public-dns-inter html>,
- At Renesys <http://www.renesys.com/2014/03/turkish-internet-censorship/>,
- At RIPE Labs <https://labs.ripe.net/Members/emileaben/a-ripe-atlas-view-of-internet- > (with a new proof of the hijacking, based on the latency),
- At the Internet Society <http://www.internetsociety.org/deploy360/blog/2014/04/turkish-hijacking-of-dns-providers-shows-clear-need-for-deploying-bgp-and-dns-se >, with an emphasis on the possible solutions (I disagree with the emphasis they put on BGP security since this hijacking was not done with BGP).

On the political side, see the good statement by Internet Society <http://www.internetsociety.org/blog/institutional-tech-matters/2014/03/internet-society-turkey%E2%80%99s-internet (the previous one was technical).

1. Car trop difficile à faire afficher par LaTeX