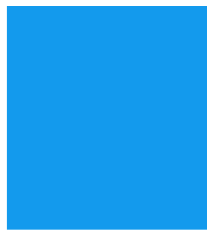
Hijacking through routing in Turkey

Stéphane Bortzmeyer

bortzmeyer@nic.fr

Context

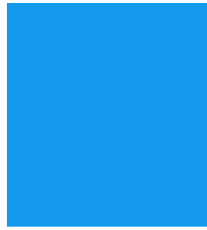
Criticisms against the turkish government on Twitter and YouTube...



Context

Criticisms against the turkish government on Twitter and YouTube...

...First, the government requests IAPs to censor, through lying DNS resolvers, sending false results for `twitter.com` (21 march)...



Context

. . . First, the government requests IAPs to censor, through lying DNS resolvers, sending false results for `twitter.com` (21 march). . .

. . . Users switch to other resolvers, such as Google Public DNS. . .

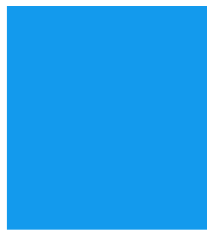
Context - 2

. . . Governement blocks some of the alternative resolvers, breaking Internet access for their users (25 march). . .

afnic

Facts

Turkish IAPs inject routes (29 march) for the important public resolvers (`8.8.8.8/32`)...



Facts

Turkish IAPs inject routes (29 march) for the important public resolvers (`8.8.8.8/32`)...

...An actual DNS server listens on these addresses (like `8.8.8.8`). It lies about `twitter.com` and `youtube.com`, to send users to `195.175.254.2`...

Facts

Turkish IAPs inject routes (29 march) for the important public resolvers (`8.8.8.8/32`)...

...An actual DNS server listens on these addresses (like `8.8.8.8`). It lies about `twitter.com` and `youtube.com`, to send users to `195.175.254.2`...

It is no longer "simple" censorship, it is now hijacking by the State.

afnic

Aftermath

1. Lying apparently stopped (4 april)
2. Hijacking apparently stopped (7 april)

afnic

Proofs

1. (No NSID or `hostname.bind` for Google Public DNS but they are easy to forge, anyway)
2. Turk Telecom's Looking Glass,
3. DNS requests from RIPE Atlas probes (when the probe is connected to a network which is tunneled outside, the problem disappears),
4. DNS requests by human users in Turkey,
5. Traceroutes,
6. Latency to `8.8.8.8`, measured by Atlas probes and Renesys probes (unlike many other things, like traceroute, latency is hard to fake).

afnic

Solutions

DNSSEC would help if done properly (validation on the user's own machine) and if `twitter.com` were signed.

. . . Authentication of the resolver (with TSIG, SIG(0) or DNScrypt - like OpenDNS does) would help (the security of a very long "last mile"). . .

. . . RPKI would not help: hijacking was internal, inside the IGP. No routing security solution here. . .

. . . Detecting the lie is one thing, working around it is another issue. . .

afnic

For the regular user

1. Switch to another public resolver (many were not blocked),
2. Local DNS resolver (port 53 was not blindly blocked),
3. tunnels, Tor. . .

afnic

References

- http://www.renesys.com/2014/03/turkish-internet-censorship/
- https://labs.ripe.net/Members/emileaben/a-ripe-atlas-view-of-internet-meddling-in-turkey
- http://www.bgpmon.net/turkey-hijacking-ip-addresses-for-popular-global-dns-p
- http://www.bortzmeyer.org/dns-routing-hijack-turkey.html
- http://www.afnic.fr/medias/documents/conseilscientifique/SC-consequences-of-DNS-based-Internet-filtering.pdf
- http://www.internetsociety.org/deploy360/blog/2014/04/turkish-hijacking-of-dns-providers-shows-clear-need-fo

afnic

Merci !

www.afnic.fr
contact@afnic.fr