Observations on a DNSSEC incident: the russian TLD (1/8)

Stéphane Bortzmeyer

bortzmeyer@nic.fr

The problem

The problem

- 30 january 2024 : many users in the world cannot use services whose name is under `.ru` (the russian Top-Level Domain),

The problem

- 30 january 2024 : many users in the world cannot use services whose name is under `.ru`,
- But it still works for some,

The problem

- 30 january 2024 : many users in the world cannot use services whose name is under `.ru`,
- But it still works for some,
- Problem lasts a few hours.

The analysis

The analysis

- As usual, confusion and wild speculation,

The analysis

- As usual, confusion and wild speculation,
- Many reports on the social networks blame one Web site or the other,

The analysis

- As usual, confusion and wild speculation,
- Many reports on the social networks blame one Web site or the other,
- Many persons decide it has something to do with the war,

The analysis

- As usual, confusion and wild speculation,
- Many reports on the social networks blame one Web site or the other,
- Many persons decide it has something to do with the war,
- Or the russian censorship.

DNSviz, the best tool for DNSSEC issues
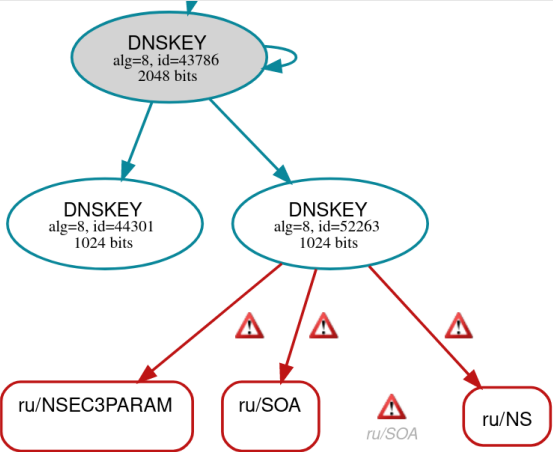
The reality

The reality

- DNSSEC issue at the `.ru` domain name registry,

The reality

- DNSSEC issue at the `.ru` domain name registry,
- Signatures invalid,

The reality

- DNSSEC issue at the `.ru` domain name registry,
- Signatures invalid,
- Breaks if you use a validating resolver.

The lessons

The lessons

- Almost every activity involves DNS,

The lessons

- Almost every activity involves DNS,
- DNS is therefore critical,

The lessons

- Almost every activity involves DNS,
- DNS is therefore critical,
- Domain names are a tree : when the parent breaks, everything underneath breaks.

The lessons

- Almost every activity involves DNS,
- DNS is therefore critical,
- Domain names are a tree : when the parent breaks, everything underneath breaks.
- Cryptography is hard,

The lessons

- Almost every activity involves DNS,
- DNS is therefore critical,
- Domain names are a tree : when the parent breaks, everything underneath breaks.
- Cryptography is hard,
- Every security technique can lead to denials of service.

Free software is great

Free software is great

- The Internet depends on free software (free as in free speech, not free as in free beer),

Free software is great

- The Internet depends on free software,
- Without DNSviz `https://dnsviz.net/` , debugging such problems would be much harder,

Free software is great

- The Internet depends on free software,
- Without DNSviz, debugging such problems would be much harder,
- RIPE Atlas probes `https://atlas.ripe.net/` are also critical (not entirely free but quite open).

Merci !

www.afnic.fr
contact@afnic.fr