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

Stéphane Bortzmeyer
bortzmeyer@nic.fr
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 lasts a few hours.
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.
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.
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

DNSKEY
alg=8, id=43786
2048 bits

DNSKEY
alg=8, id=44301
1024 bits

DNSKEY
alg=8, id=52263
1024 bits

ru/NSEC3PARAM
ru/SOA
ru/SOA
ru/NS

(2024-01-30 16:50:42 UTC)
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

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.
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 !