The Root Canary
Quantifying the Quality of DNSSEC Validation in the Wild
Canary in the virtual coalmine

• Goals:

  • **Track operational impact** of the root KSK rollover, act as a warning signal that validating resolvers are failing to validate with the new key

  • **Measure validation during** the KSK rollover from a global perspective to learn from this type of event
Measurement methodology

- Use four perspectives:
  - Online perspectives:
    - RIPE Atlas
    - Luminati
    - APNIC DNSSEC measurement
      (current thinking: use data during evaluation)
  - “Offline” perspective (analysed after measuring)
    - Traffic to root name servers (multiple letters)
Measurement methodology

- We have **signed and bogus** records for **all algorithms** and **most DS algorithms**

- This gives us one of three outcomes:
  - Resolver **validates correctly**
  - Resolver **fails to validate** (SERVFAIL)
  - Resolver **does not validate**
    - (yes, there are **corner cases** probably **not covered** by these three options)

- **Side-effect**: measure support for algorithms

https://rootcanary.org/
Measurement methodology

- **Luminati**: HTTP(s) proxy service

  - 2.3 Million exit nodes - usually of residential users
    - Allows us to send HTTP(s) traffic via a central Luminati server through the exit nodes
    - This HTTP request triggers a DNS query
  
  - Covers > 15,000 ASes
  
  - Of which > 14,000 are not covered by RIPE Atlas

https://rootcanary.org/
Canary in the virtual coalmine

- Preliminary Findings after 2017-09-19:
Canary in the virtual coalmine

- Preliminary Findings after 2017-09-19: Root

TCP and UDP Replies at B-Root (MIA)

New ZSK in Zone

https://rootcanary.org/
Canary in the virtual coalmine

- Preliminary Findings after 2017-09-19: Root
Beyond the Root Canary Project

- **Tooling for key roll overs**: develop generic measurement methodology that can also be applied at TLD level or below

- **Know your resolvers**: measure use of DNSSEC algorithms and resolver implementations

- **But first**: the real root key roll over

https://rootcanary.org/
You can help!

- Run small shell script that uses `dig` to query our test domains from within your network
  - Using your default resolvers
  - Once every hour

- Please come talk to me if you’re interested
More info

- Project webpage: https://rootcanary.org/
- Online algorithm test: https://rootcanary.org/test.html
- Current results for RIPE Atlas-based measurement: https://portal.rootcanary.org/rcmstats.html