The Root Canary

Measuring the (postponed) rollover of the Root KSK
Canary in the virtual coalmine

picture from academia.dk

https://rootcanary.org/
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)
1414 byte DNSKEY

- Does it break stuff?

# Servfail responses for valid signed domains (except RSAMD5)

Failed Responses per 60 min

- New ZSK in Zone

https://rootcanary.org/
From the perspective of the root servers

1414 byte DNSKEY
1414 byte DNSKEY

- From the perspective of the root servers
Improving our Measurements

• Would you be willing to help us improving our measurements?

• Proposal:
  
  • Run small shell scripts that uses `dig` to query our test domains from within your network
  
  • Using the default resolvers
  
  • Every hour or more frequently

https://github.com/moritzcm/root-canary-custom-msm
More info

• Current results for RIPE Atlas-based measurement: https://portal.rootcanary.org/rcmstats.html

• Live feed for RIPE Atlas-based measurement: https://monitor.rootcanary.org/live.html

• BASH measurement script: https://github.com/moritzcm/root-canary-custom- MSM

• moritz.muller@sidn.nl | @moritzcm_ |