The Root Canary

The Evolution of a Measurement
What’s the goal of this talk?

• Some of you may have already heard about the Root Canary project

• So why present about it again at the MAPRG?

• We want to tell the story of an evolving measurement, where we started measuring one thing, but…
  • We measure other things as a side effect
  • We make brilliant mistakes
  • The measurement results in new ways to monitor DNS operations useful for, e.g., TLD operators

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

- **Recap**: why did we start this project?
  - **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

https://rootcanary.org/
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)

https://rootcanary.org/
Measurement methodology

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

- **Millions of exit nodes** - usually **residential users**
  - Allows us to send HTTP(S) traffic via a central server that egresses through the exit nodes
  - Our **HTTP** requests **trigger DNS** queries

- **Covers > 15,000 ASes**

- Of which **> 14,000** are **not covered by RIPE Atlas**

https://rootcanary.org/
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)
Live results

https://portal.rootcanary.org/rcmstats.html

https://rootcanary.org/
Live results

CDF of time spent in state; longer == more stable (> 80% of probes)

DS: SHA-256, signed with RSA-SHA256

Current probe status for all probes

CDF for current time

All probes (24h)

All probes (7 days)

https://rootcanary.org/
No sh*t, RIPE Atlas is biased ;-)  

Luminati vs. RIPE Atlas: SHA256-RSA-SHA1

Luminati

~ 13,000 VPs
7% validating

RIPE Atlas

~ 9,000 VPs
42% validating

https://rootcanary.org/
Excitement?

The first moment things could go wrong; let’s see what happened
So what happened?

- Preliminary Findings after 2017-09-19:

  One vantage point glitching, likely not related to measured event

https://rootcanary.org/
What about traffic to the root?

No noticeable increase in TCP traffic

No noticeable increase in truncated responses

with thanks to Wes Hardaker (USC/ISI) for preliminary access to B-root traffic

https://rootcanary.org/
Nothing *exciting* happened.
And then...

- **Phase I**: Introduction of new KSK
- **Phase II**: DNSKEY size increases due to ZSK rollover
- **Phase III**: New KSK becomes active
- **Phase IV**: Start of revocation of old KSK
- **Phase V**: Old KSK removed
- **Phase VI**
And then...

- So did we do **all this work for nothing?**

https://rootcanary.org/
Spin-offs (1)

- First spin off: **online algorithm test**

https://portal.rootcanary.org/
Spin-offs (2)

• We **test** algorithm support for **all probes over time**

Also allows rough fingerprinting of resolvers — Can anybody guess what resolver this is?

https://monitor.rootcanary.org/
Spin-offs (3)

- **Oops, we forgot to re-sign** our test domains…
Spin-offs (3)

- Oops, we forgot to re-sign our test domains…

What you would expect to happen
Spin-offs (3)

- **Oops, we forgot to re-sign** our test domains…

But what’s happening here?!

What you would expect to happen
Spin-offs (3)

• **Oops, we forgot to re-sign** our test domains…

Resolvers have a (configurable) grace period for expired signatures

We believe that’s what we’re seeing here

Future work:
How long is the grace period?
Rööt Cånåry

https://rootcanary.org/
• The good folks at IIS are performing a KSK and algorithm rollover for the .se ccTLD*

• Asked if Root Canary team could measure this event and signal problems to them

• Much more “agile” timescale than Root KSK — entire process takes less than two weeks

*https://www.iis.se/se-tech/se-ksk-algorithm-rollover/
• Developed **new methodology** for this project, to also cover **issues specific to algorithm rollover**

• **.se** was **first TLD to sign** its domain in **2005** — this is well **pre-signed root**, consequently **resolvers with separate .se trust anchors may exist in the wild**

• **Tests** show many **resolver implementations** give precedence to local trust anchor, so a **rollover** may result in **SERVFAIL**s for those resolvers (!)

*Discussion about this initiated by Moritz from our team: https://www.ietf.org/mail-archive/web/dnsop/current/msg21179.html*
Rööt Cånåry

- Approached by .se at DNS-OARC
- .se performing algo + KSK rollover
- .se interesting position: resolvers may have fixed trust anchors as .se was first signed TLD (2005 — check)
- Will measure specific aspects of algorithm rollover (signature publication, key publication, …)
- Spin-off: methodology for operators that want to perform similar rollovers
- Learning about what resolvers do if they have a separate TA, thread on DNSOP

https://rootcanary.org/
Conclusions

• We **started measuring** the Root KSK rollover **as** a sort-of **ad-hoc project**

• As our **thinking** about the measurement **evolved**, many **spin-offs developed**

• Example **case study** of why **measuring rare events** that hit **corner cases** are (extremely) useful

• **Measurements —> Better understanding —> Better protocols, (hopefully) fewer failures.**
Open data

• The Root Canary measurement data performed by RIPE Atlas is publicly available through the Atlas API.

• Our aggregate results can be monitored as a live stream over Websockets (https://monitor.rootcanary.org:443/new_ripe_msm).

• We will release datasets for publications coming out of this work as open data, but if you want data now, come talk to me!
Thank you for your attention!
Questions?

acknowledgments: with thanks to Willem Toorop, Taejoong Chung and Moritz Müller

nl.linkedin.com/in/rolandvanrijswijk
@reseauxsansfil
roland.vanrijswijk@surfnet.nl
r.m.vanrijswijk@utwente.nl