

Roll, Roll, Roll Your Root

A Comprehensive Analysis of the First Ever DNSSEC Root KSK Rollover

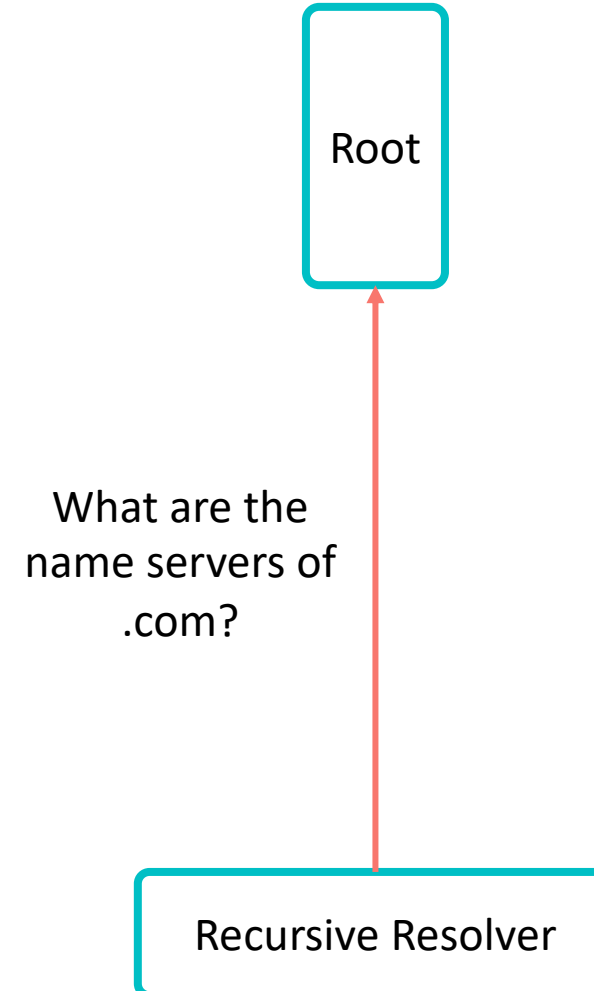
RIPE 79 – Rotterdam, 2019-10-15

Moritz Müller^{3,4}, Matthew Thomas⁶, Duane Wessels⁶, Wes Hardaker⁵, Taejoong Chung², Willem Toorop¹,
Roland van Rijswijk-Deij^{1,4}

¹NLnet Labs, ²Rochester Institute of Technology, ³SIDN Labs, ⁴University of Twente, ⁵USC/Information Sciences Institute, ⁶Verisign

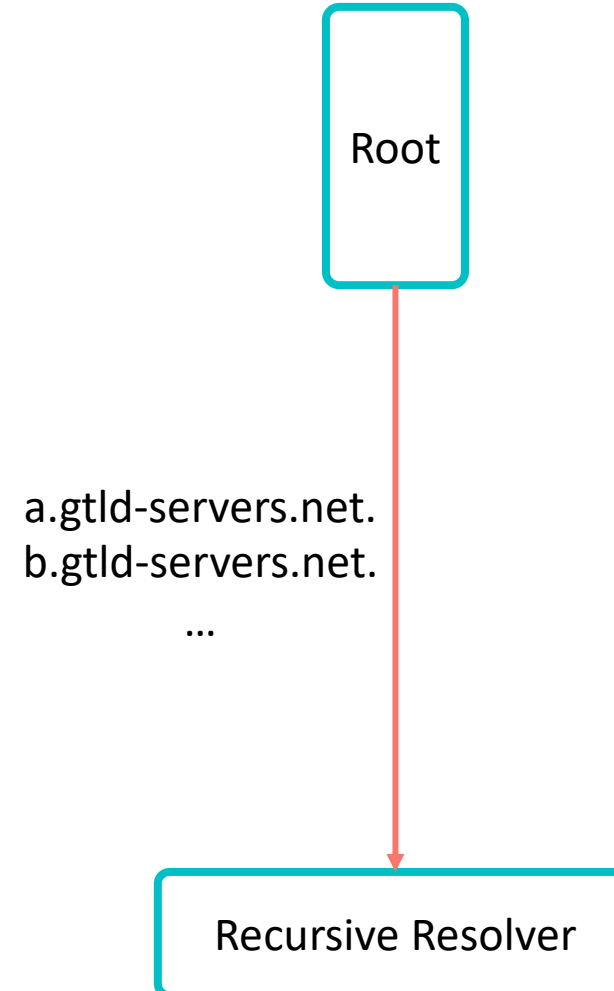
Introduction

- DNSSEC brings **integrity** to the DNS
- Validators need the public key of the Root and configure it as *trust-anchor*
- In 2018, the trust-anchor was replaced (or “*rolled*”) for the *first time*
- The old key: **KSK-2010**
- The new key: **KSK-2017**



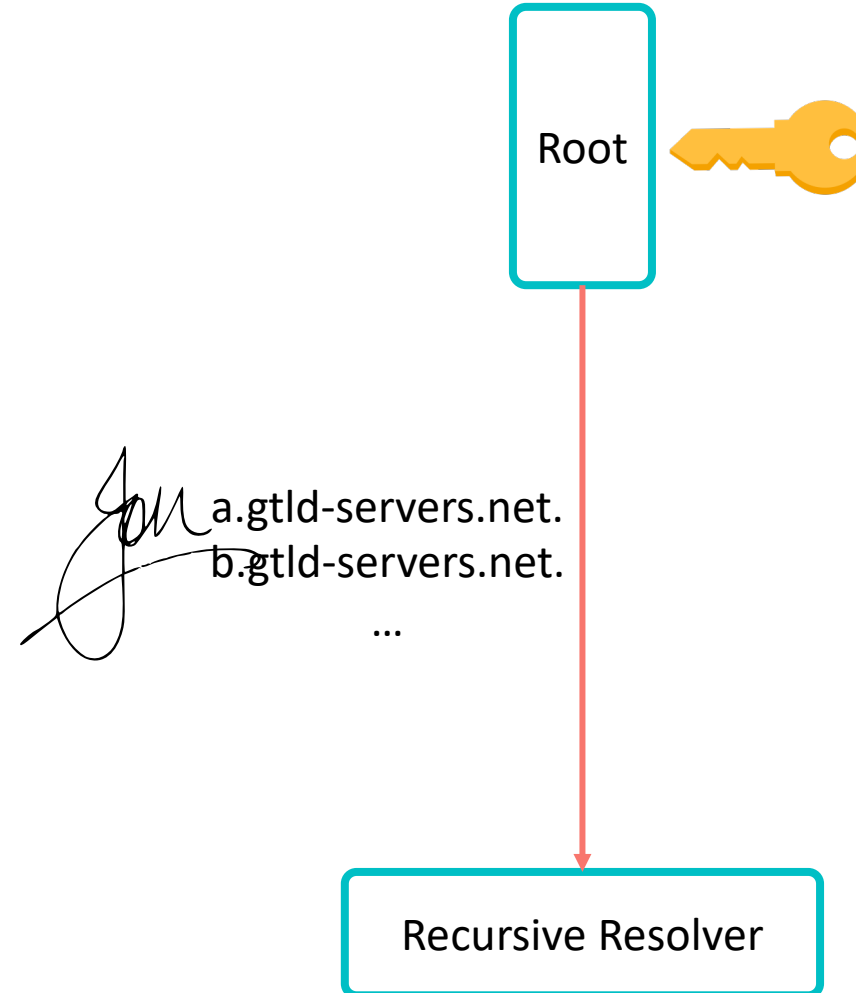
Introduction

- DNSSEC brings **integrity** to the DNS
- Validators need the public key of the Root and configure it as *trust-anchor*
- In 2018, the trust-anchor was replaced (or “*rolled*”) for the *first time*
- The old key: **KSK-2010**
- The new key: **KSK-2017**



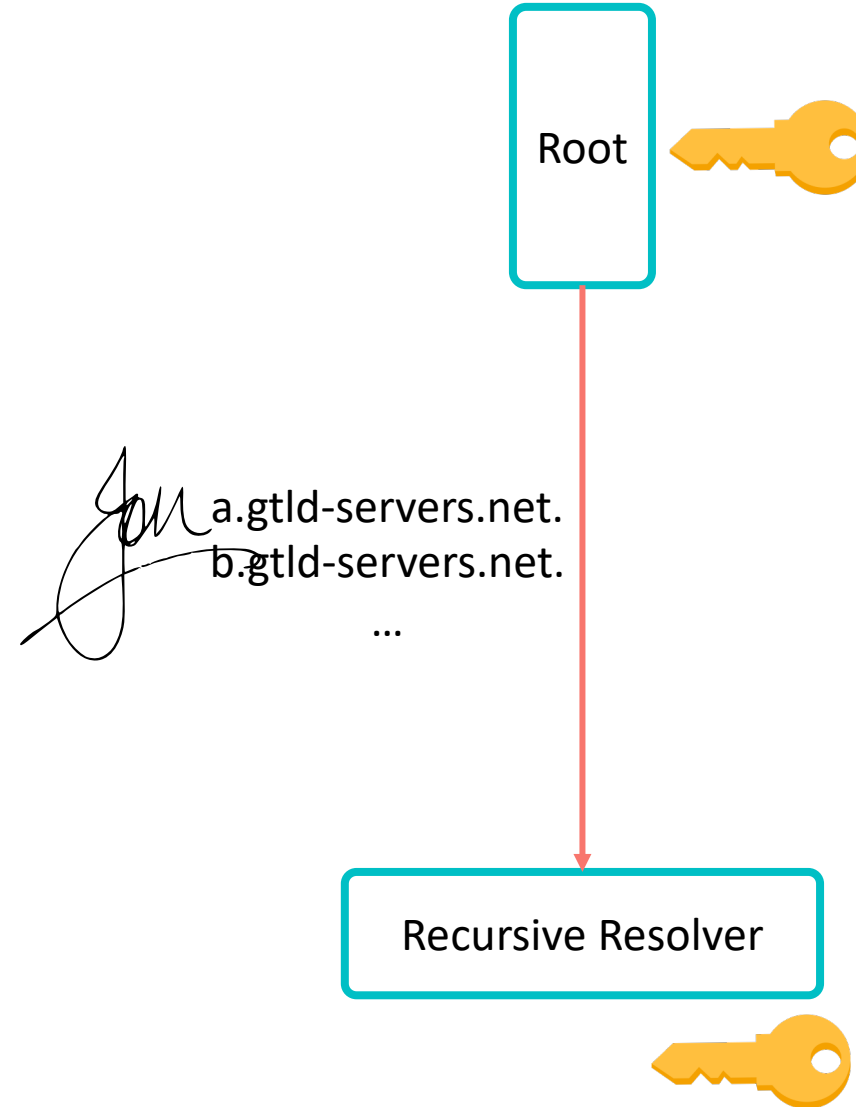
Introduction

- DNSSEC brings **integrity** to the DNS
- Validators need the public key of the Root and configure it as *trust-anchor*
- In 2018, the trust-anchor was replaced (or “*rolled*”) for the *first time*
- The old key: **KSK-2010**
- The new key: **KSK-2017**



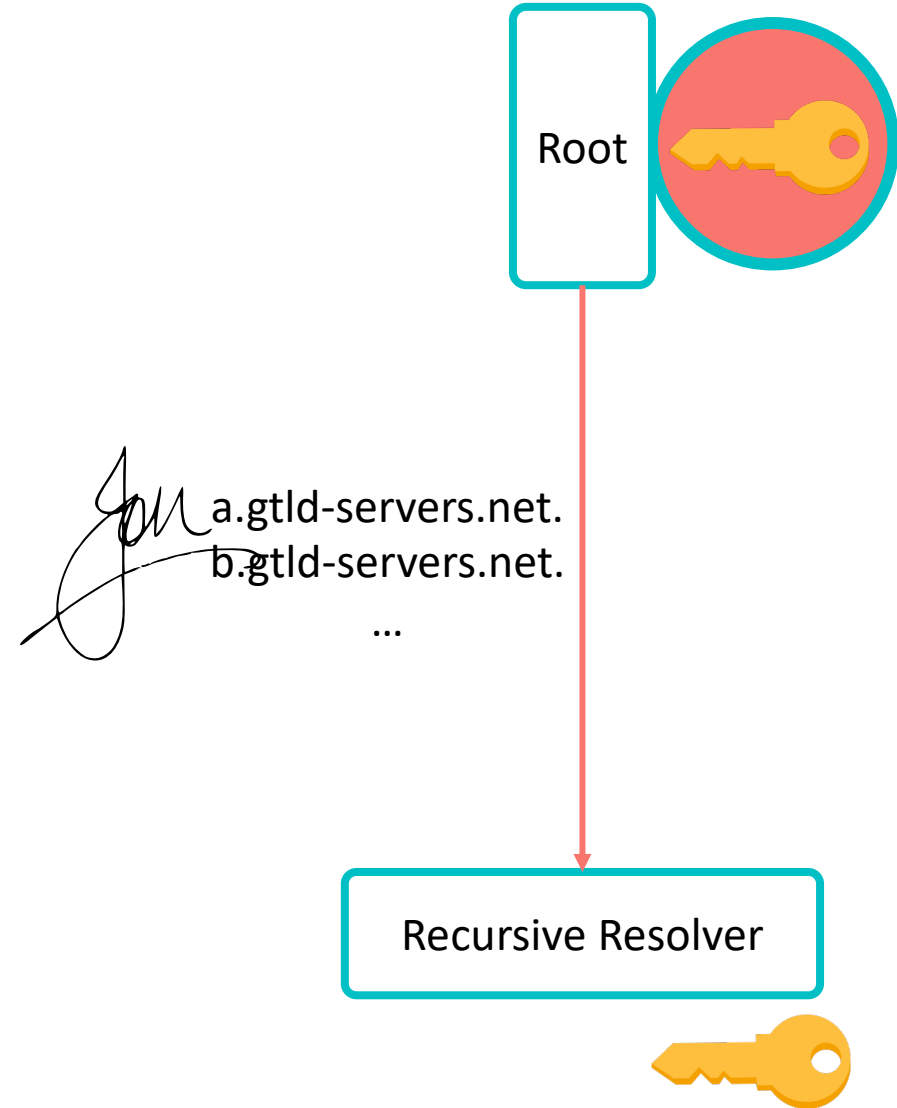
Introduction

- DNSSEC brings **integrity** to the DNS
- Validators need the public key of the Root and configure it as *trust-anchor*
- In 2018, the trust-anchor was replaced (or “*rolled*”) for the *first time*
- The old key: **KSK-2010**
- The new key: **KSK-2017**



Introduction

- DNSSEC brings **integrity** to the DNS
- Validators need the public key of the Root and configure it as *trust-anchor*
- In 2018, the trust-anchor was replaced (or “*rolled*”) for the *first time*
- The old key: **KSK-2010**
- The new key: **KSK-2017**



Why is rolling hard?

- No key → No validation → No DNS responses
- **Every** validator needs to have KSK-2017, but:
 - Validators use hard-coded keys
 - Containers challenge key update
 - People tend to forget about DNS

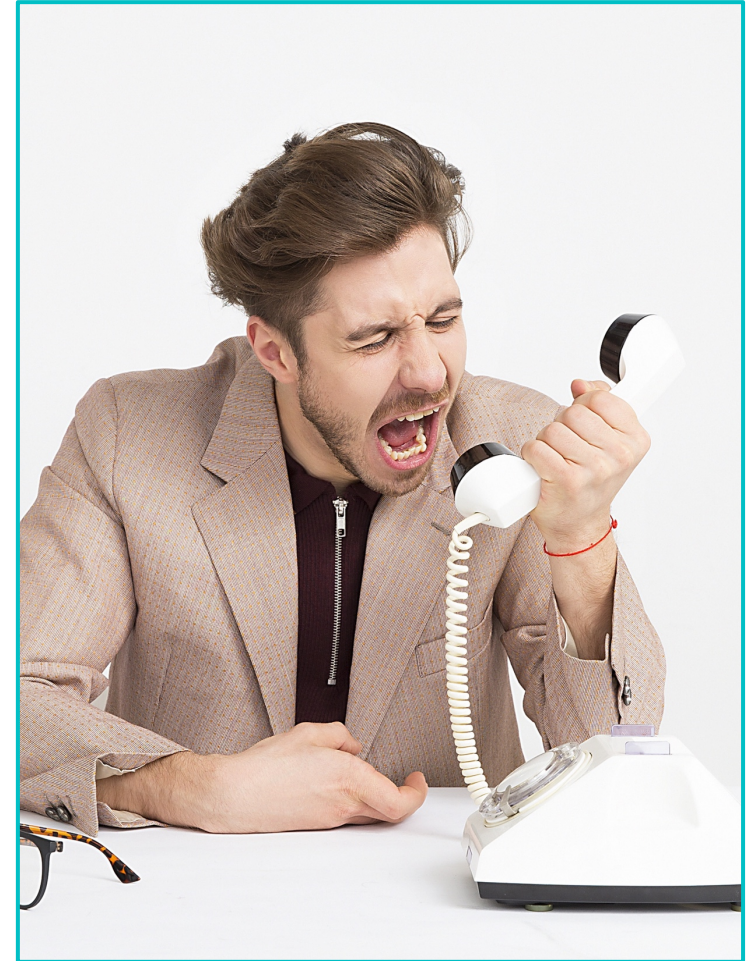
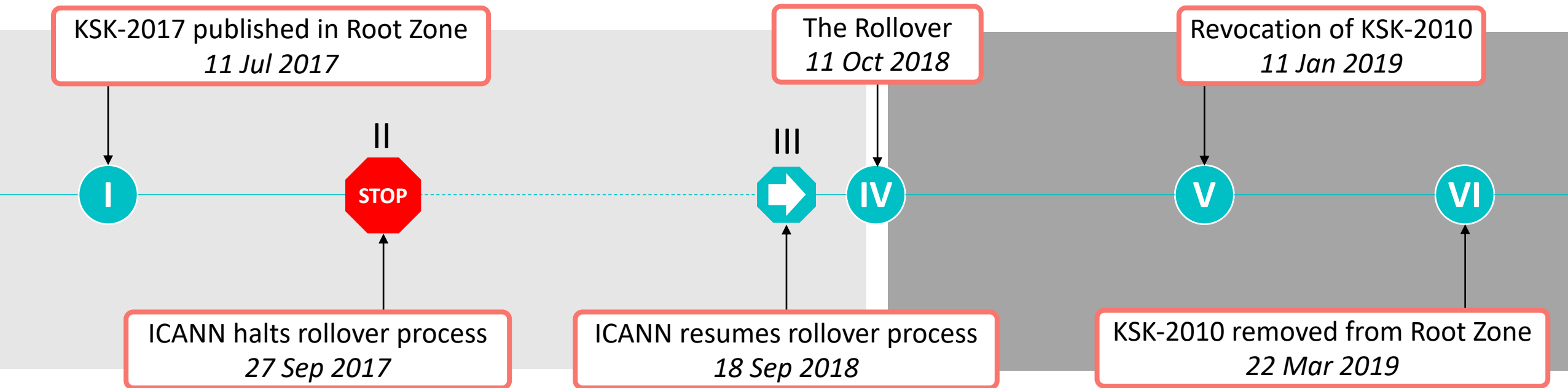
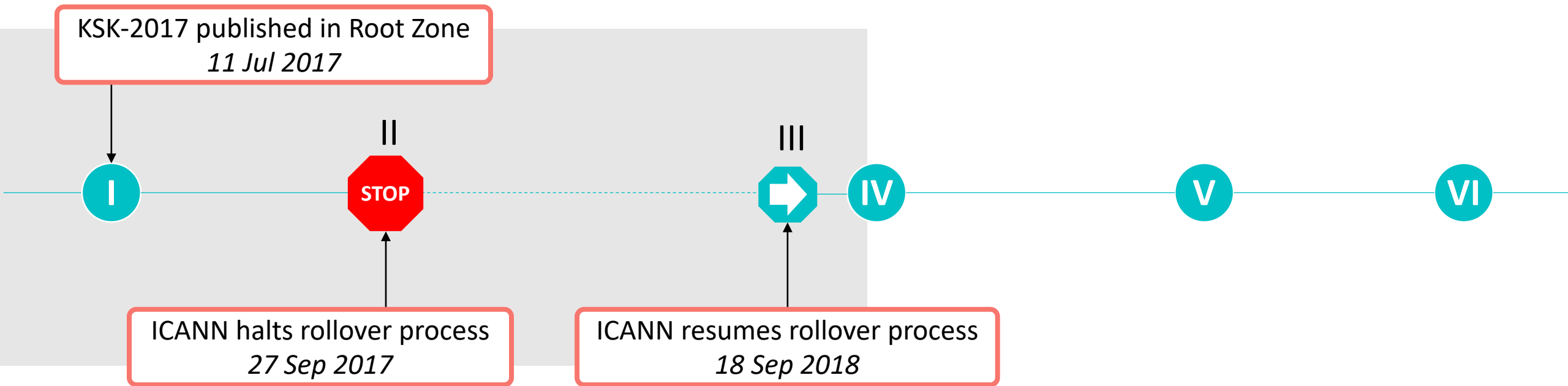


Photo by Icons8 team on Unsplash

Timeline

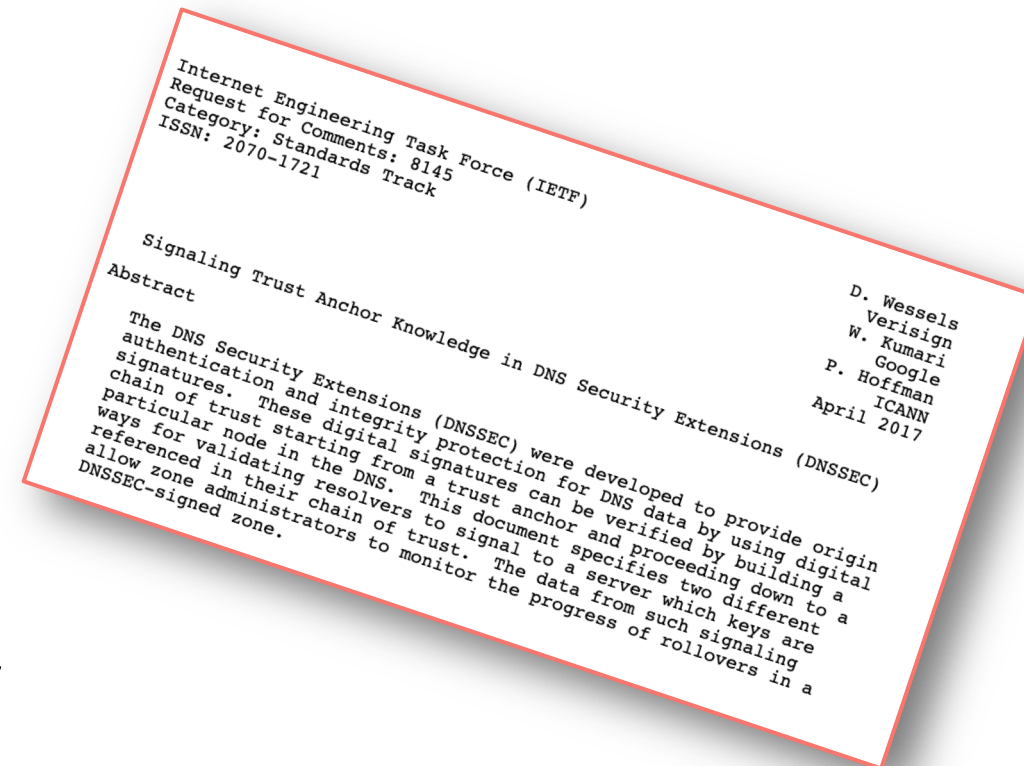


Before the Rollover

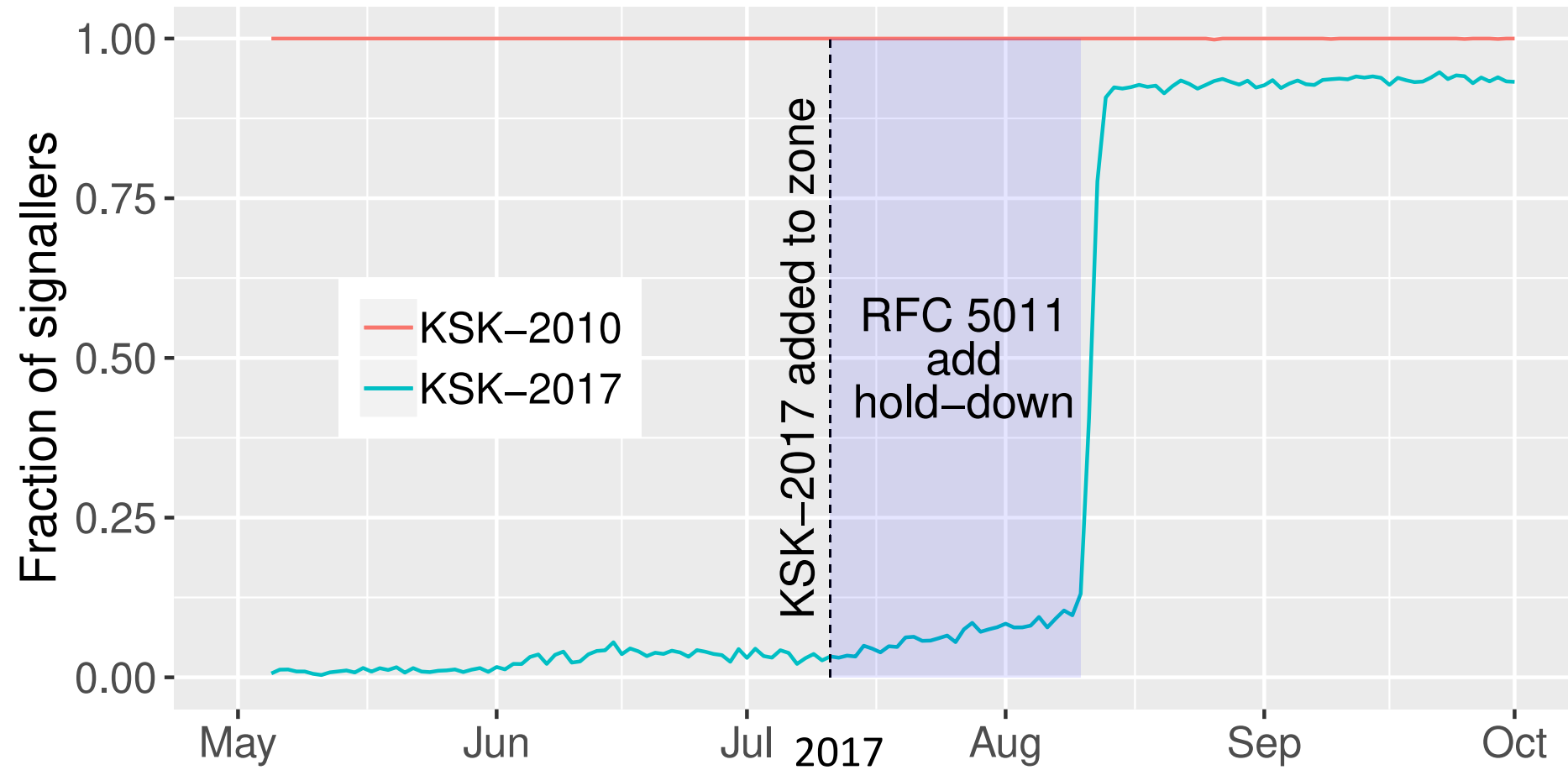


Resolver Telemetry: RFC 8145

- The goal: estimating how many validators had KSK-2017
- The solution: resolvers signal to the root which keys they trust
- Data from ICANN from A, B, and J root
- Signals from up to 100,000 validators daily



Uptake of KSK-2017



I

STOP

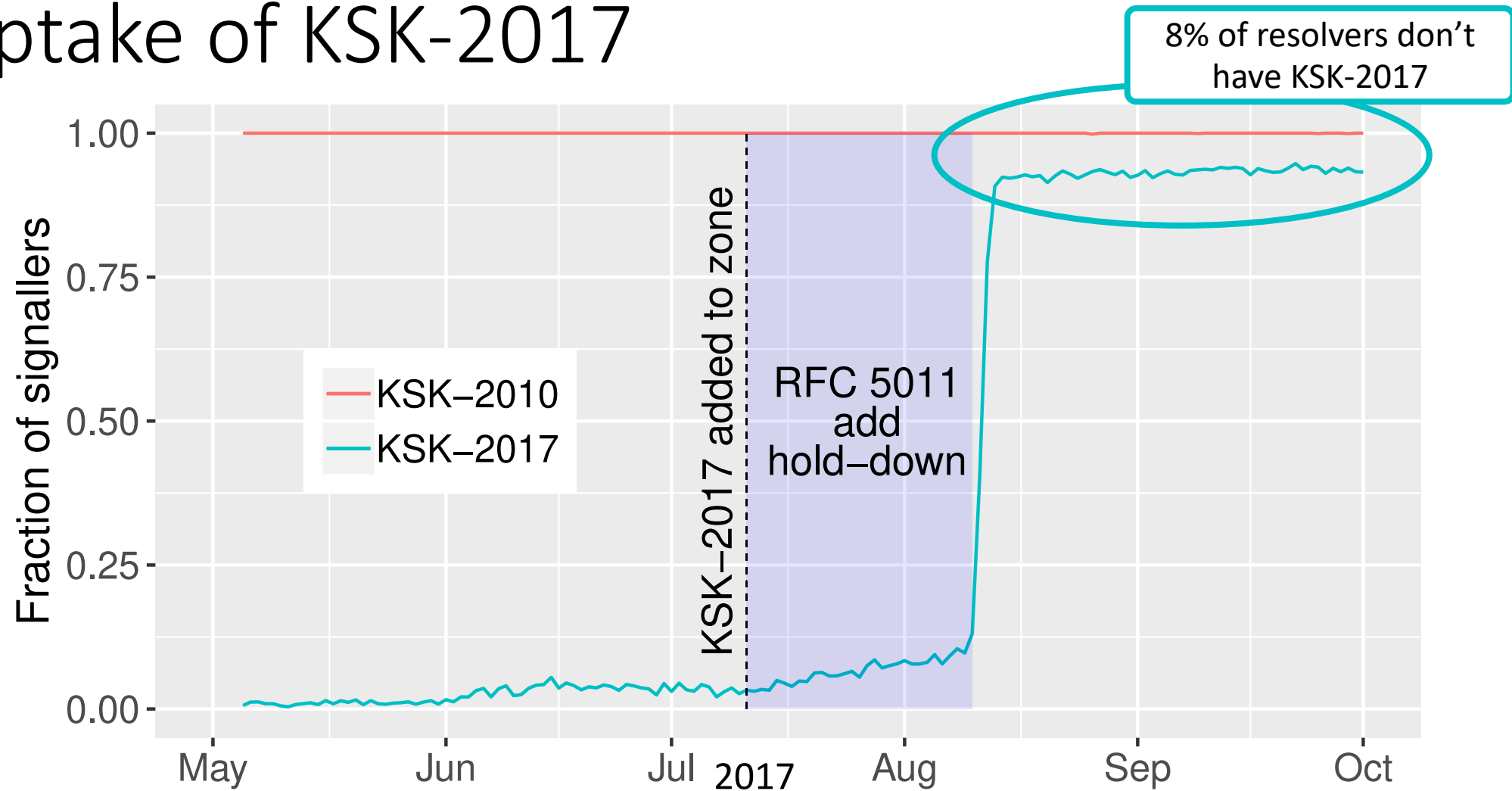


IV

V

VI

Uptake of KSK-2017



I

STOP



IV

V

VI

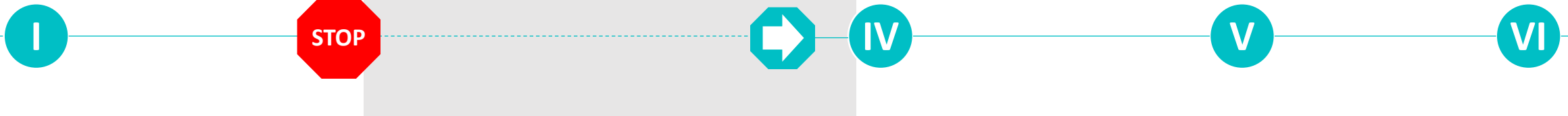


Zooming in on resolvers that only have KSK-2010

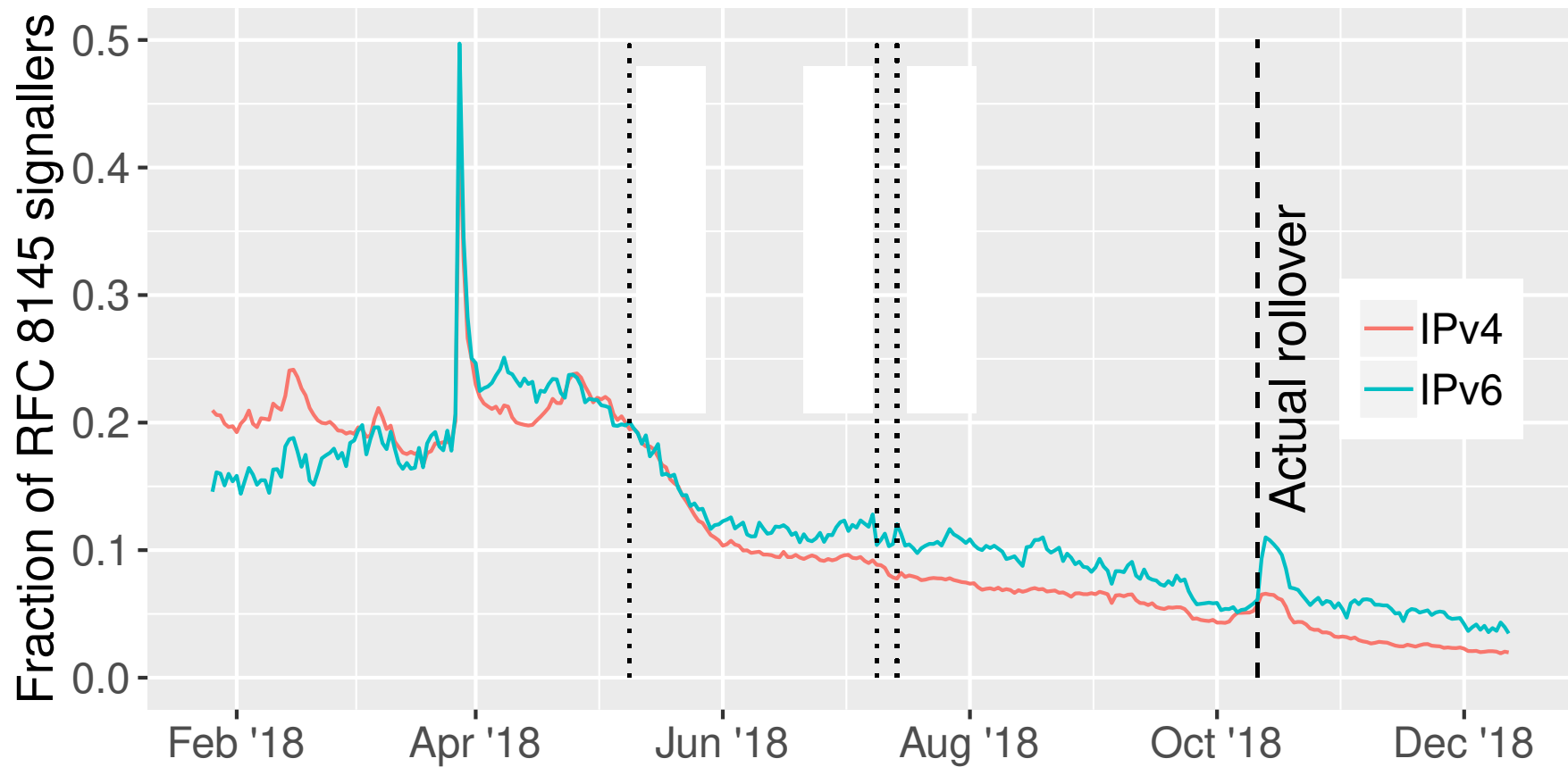
- Lots of RFC 8145 sources sent only one signal
- Many sent only a few queries

Query	Count
_ta-4a5c	15,447
.	9,182
VPN domain	3,156
VPN alternate domain	415
_sip._udp.otherdomain	86

Domains, queried by resolvers



Zooming in on resolvers that only have KSK-2010



I

STOP

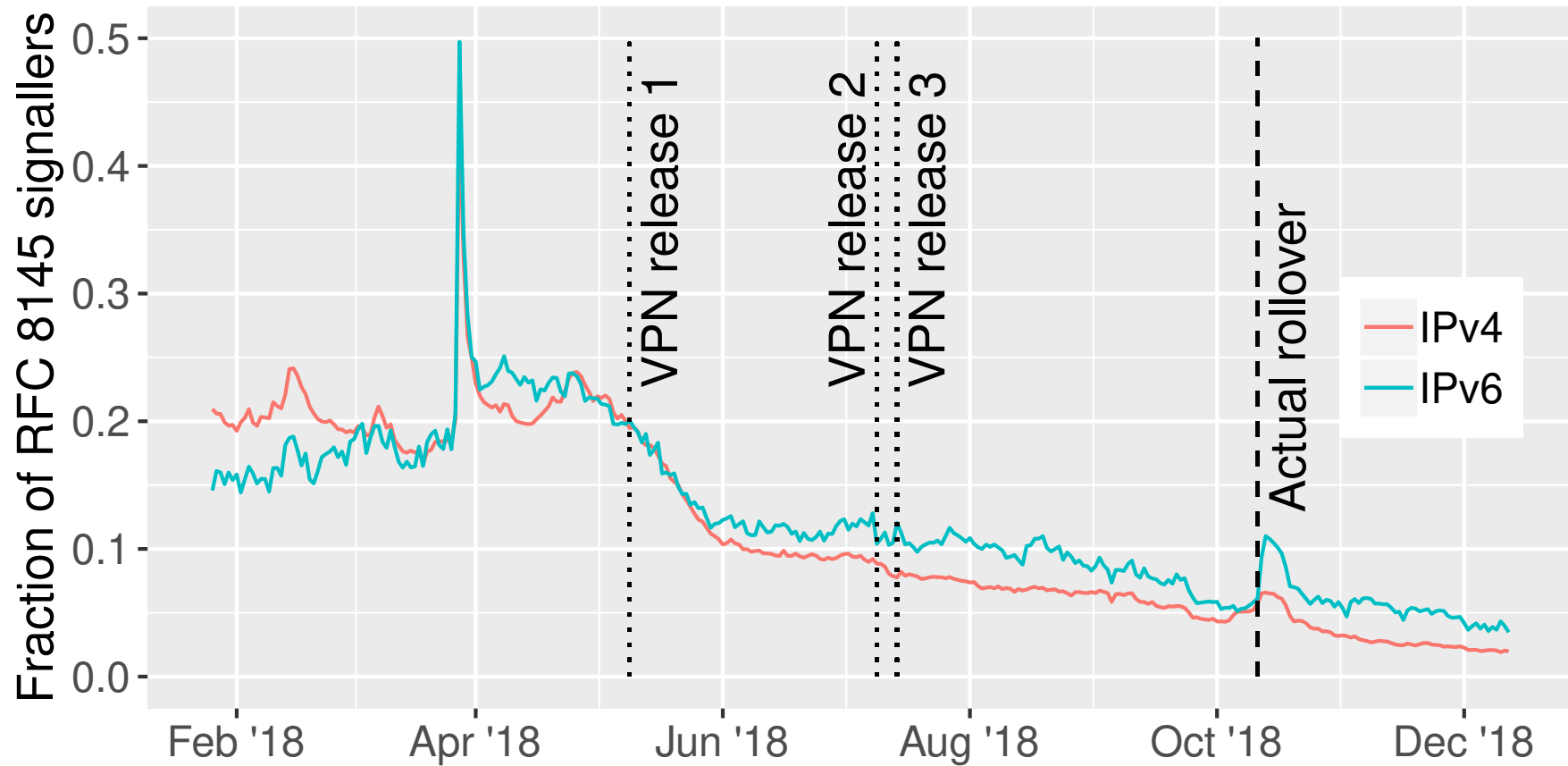


IV

V

VI

Zooming in on resolvers that only have KSK-2010



I

STOP



IV

V

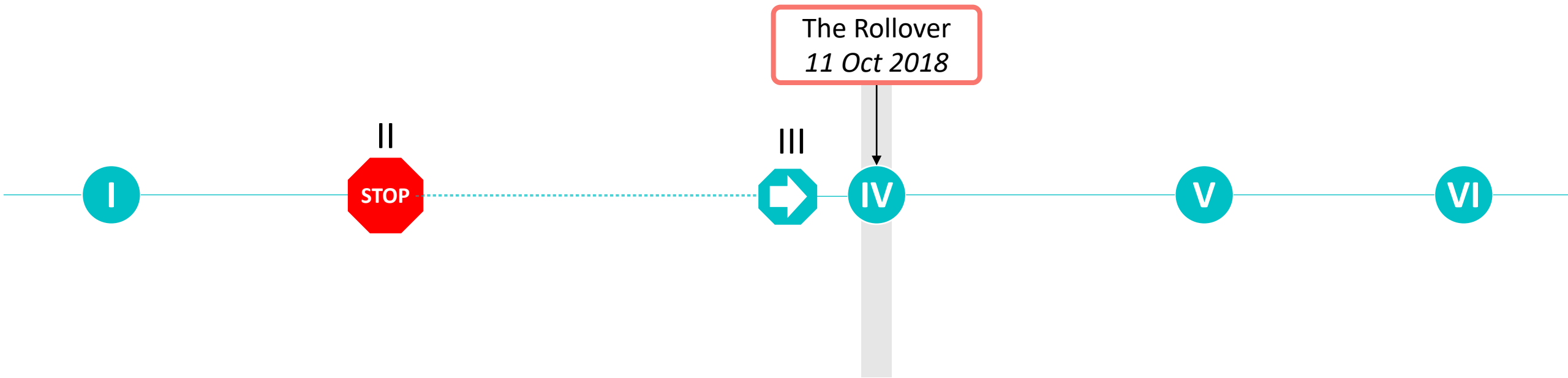
VI

Takeaways from *before* the Rollover

- **Most** validators correctly picked up KSK-2017
- But **one single application** can influence the trust-anchor signal
- Validation in applications might become more common
→ **Influence on telemetry**



During the Rollover

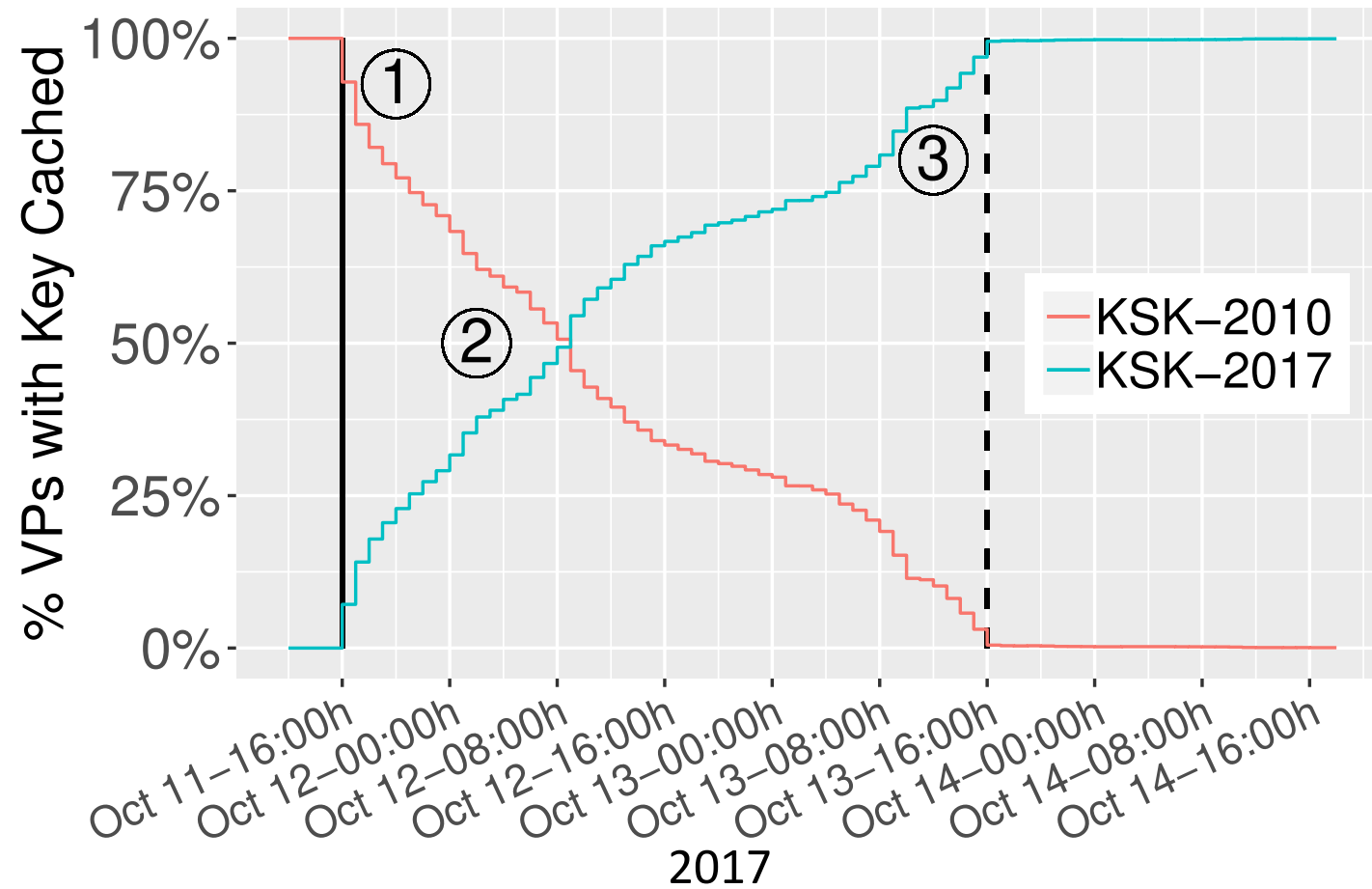


The User's Perspective: RIPE Atlas

- The goal: measuring how **users** perceive the rollover
- The approach: Measuring with all RIPE Atlas probes once per hour
 - a) If they have cached KSK-2017
 - b) If they validate correctly
- We observed **35,719 resolver addresses** in **3,141 ASes** and correlated failing resolvers with DNSKEY queries with DITL data



Activating KSK-2017



I

STOP

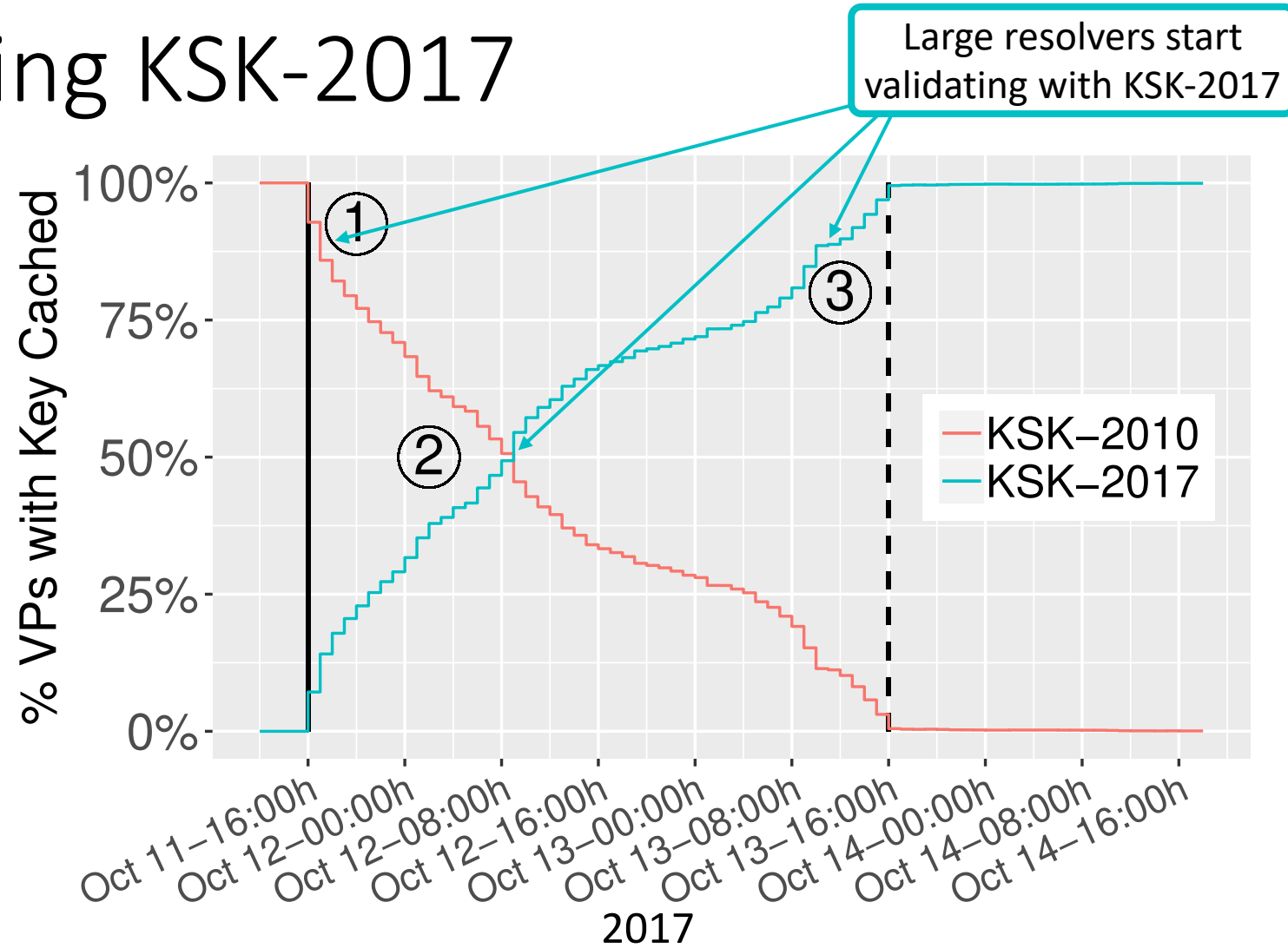


IV

V

VI

Activating KSK-2017



I

STOP

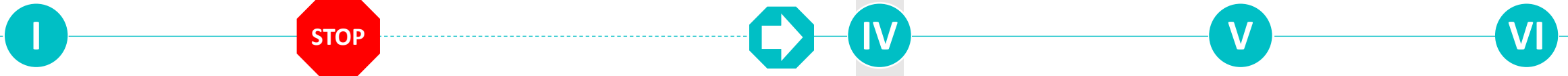
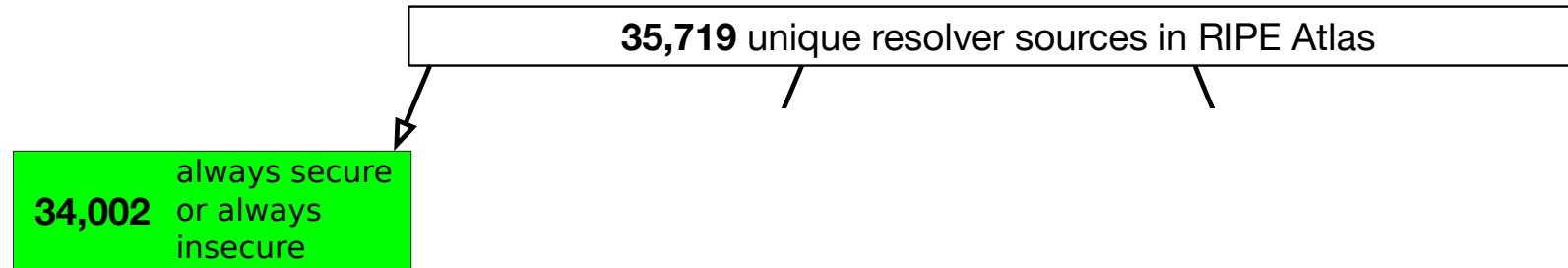


IV

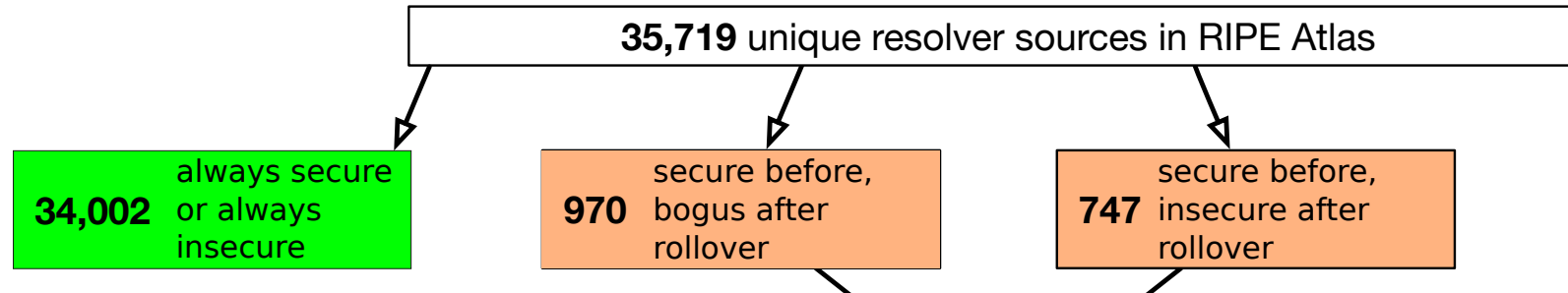
V

VI

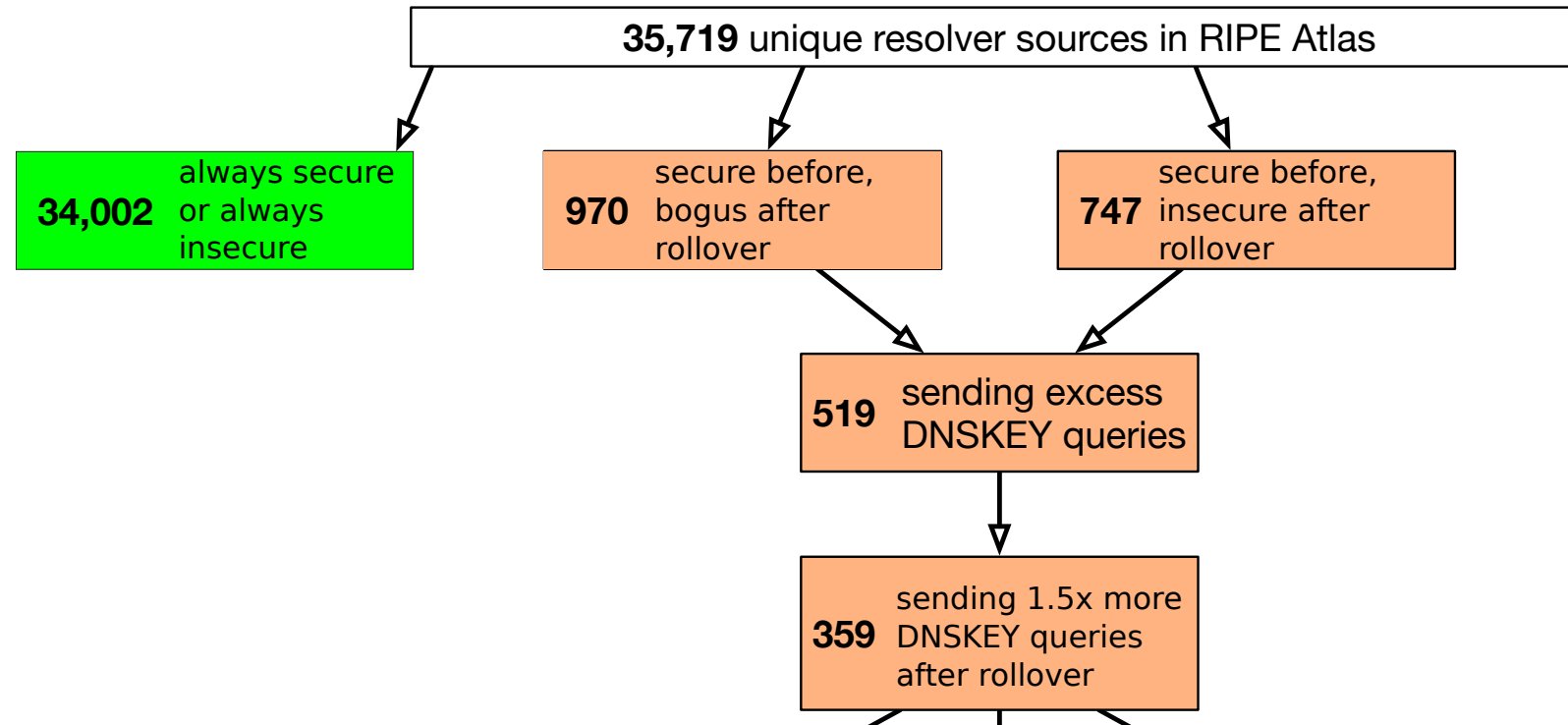
Reaction to Validation Failures



Reaction to Validation Failures



Reaction to Validation Failures



I

STOP

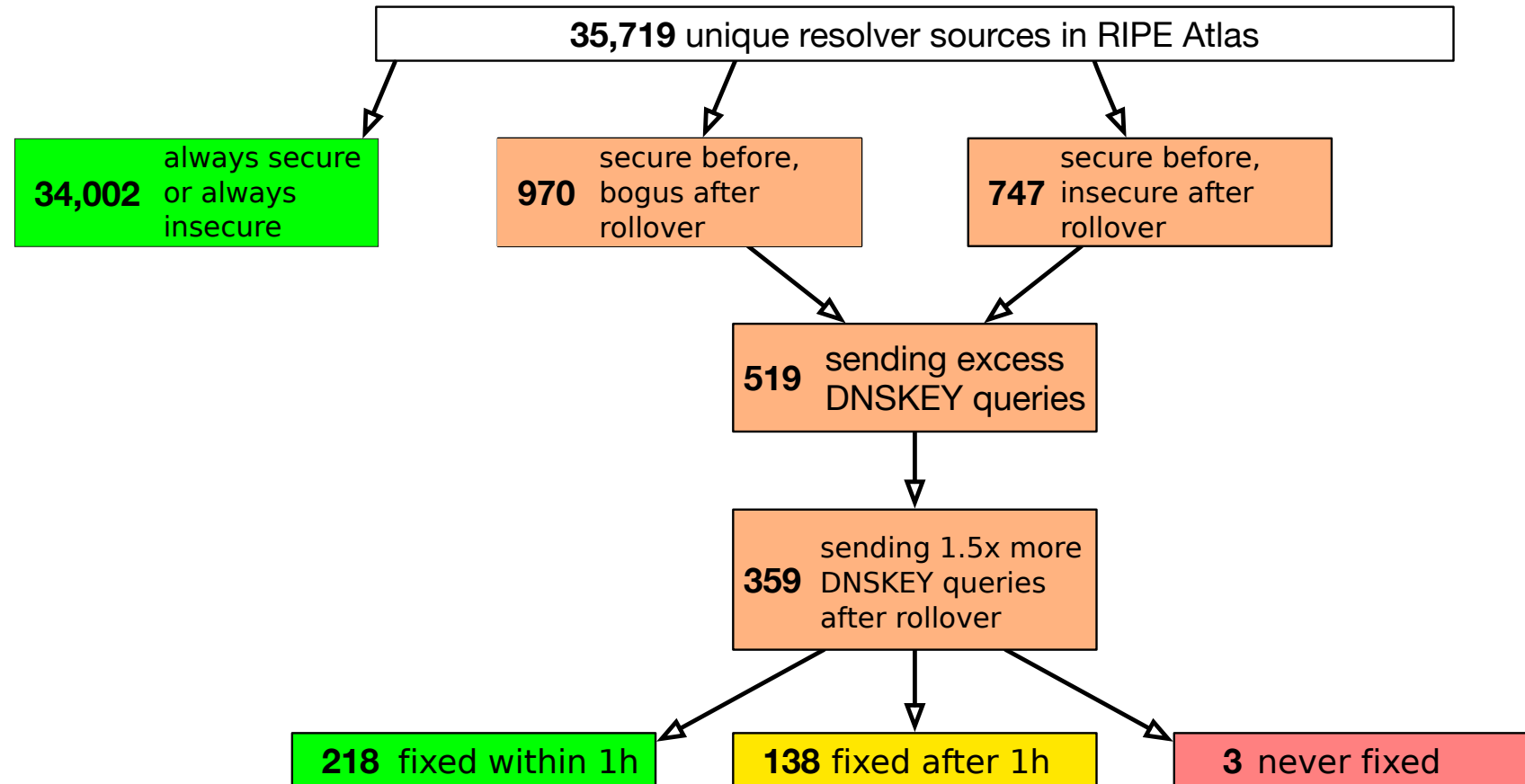


IV

V

VI

Reaction to Validation Failures



Broadband restored to Eir customers after outage

Company says problem with DNS server led to outage across the country

© Sat, Oct 13, 2018, 21:23

Updated: Sun, Oct 14, 2018, 07:55



File photograph: Maxwells

<https://www.irishtimes.com/business/technology/broadband-restored-to-eir-customers-after-outage-1.3663004>

I

STOP

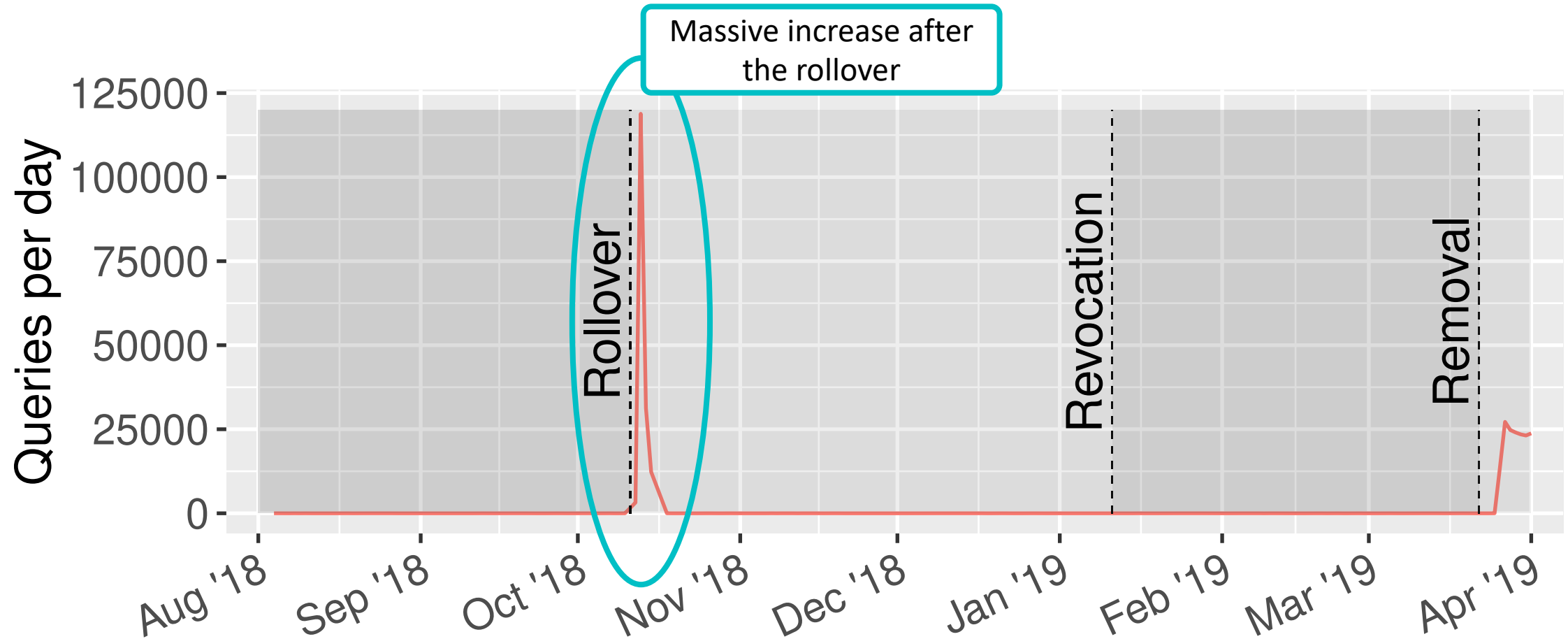


IV

V

VI

EIR Outage - Was it DNS(SEC)?



I

STOP

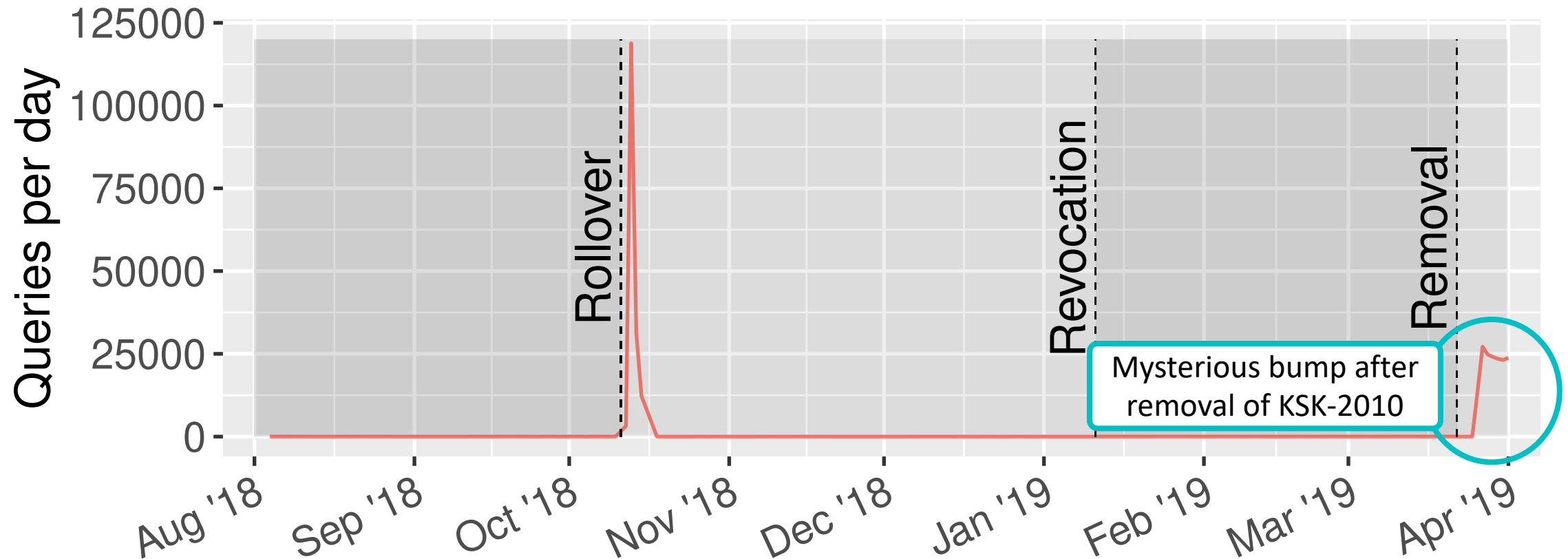


IV

V

VI

EIR Outage - Was it DNS(SEC)?



I

STOP



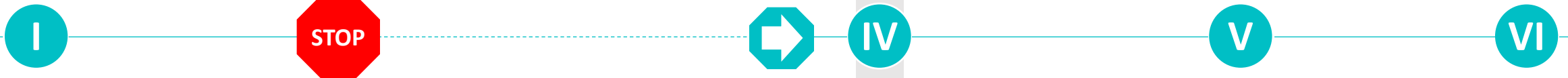
IV

V

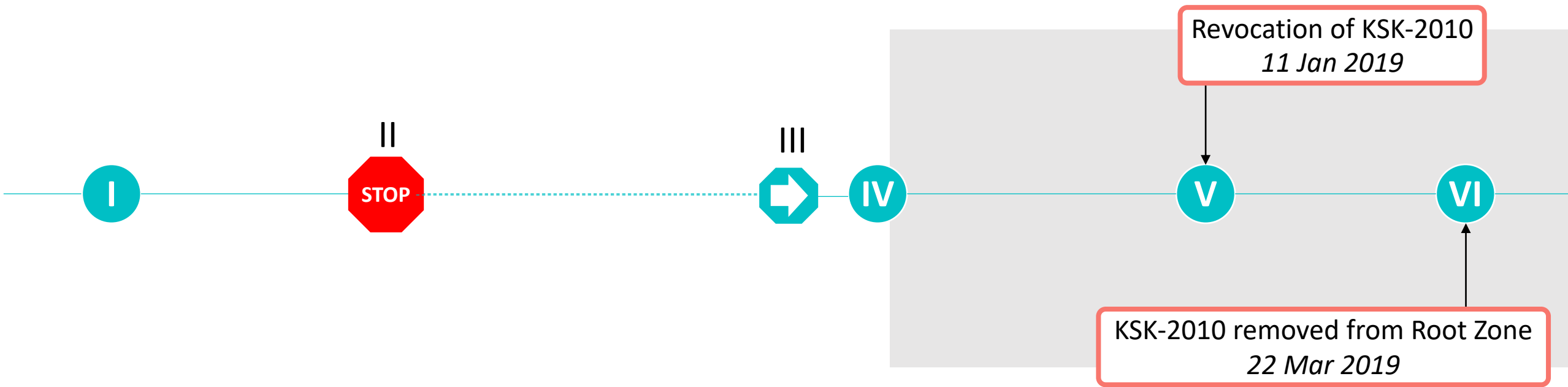
VI

Takeaways from *during* the Rollover

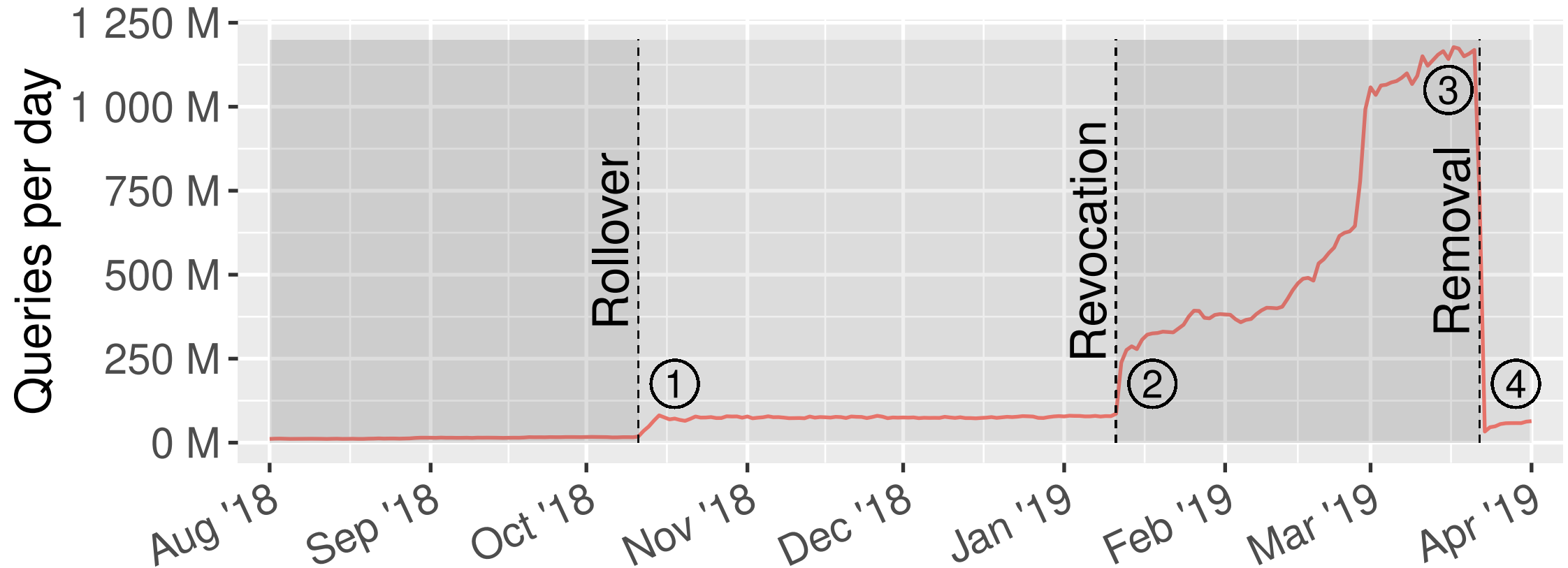
- **Few** resolvers had **serious problems**
- The ones that had problems **recovered fast**
- Less than **0.01%** of the resolvers we monitored experienced problems



After the Rollover



Increase in DNSKEY queries



I

STOP

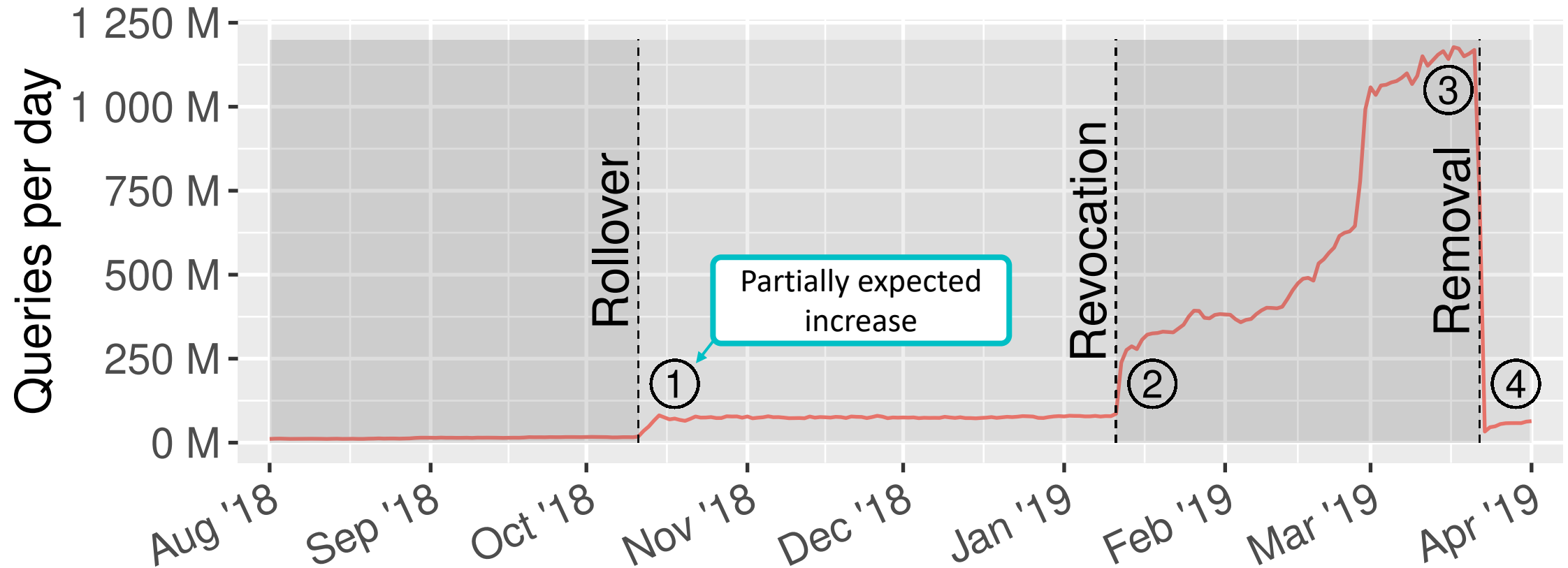


IV

V

VI

Increase in DNSKEY queries



I

STOP

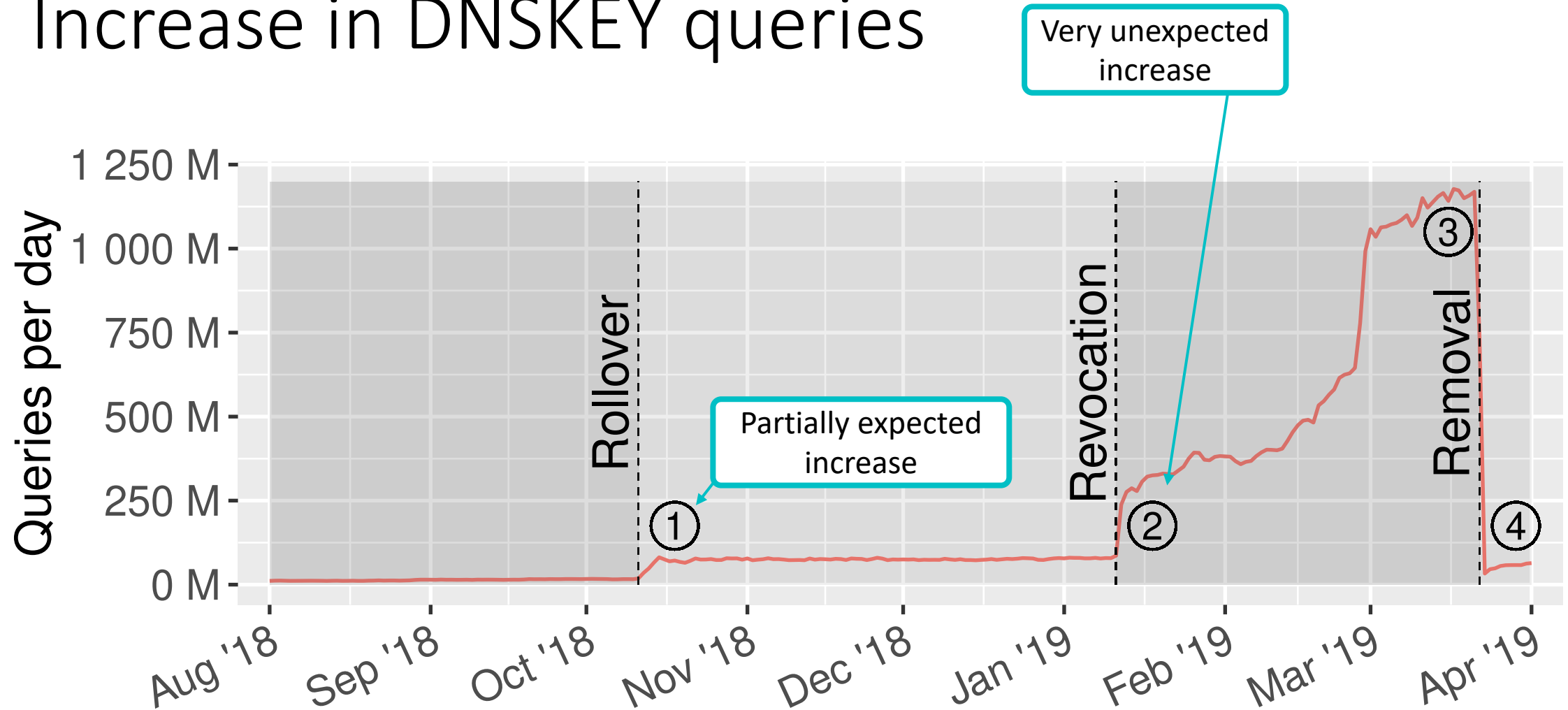


IV

V

VI

Increase in DNSKEY queries



I

STOP

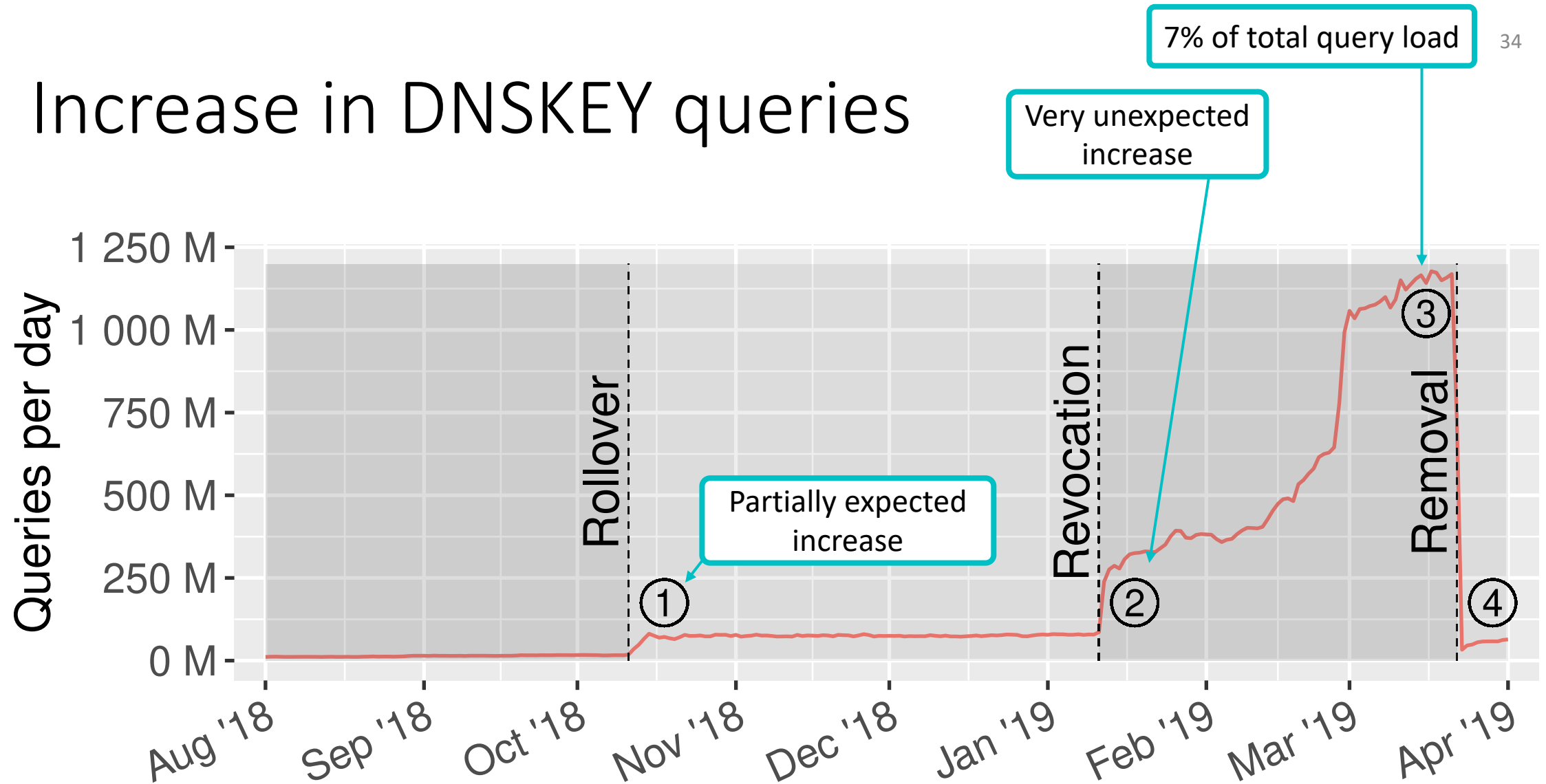


IV

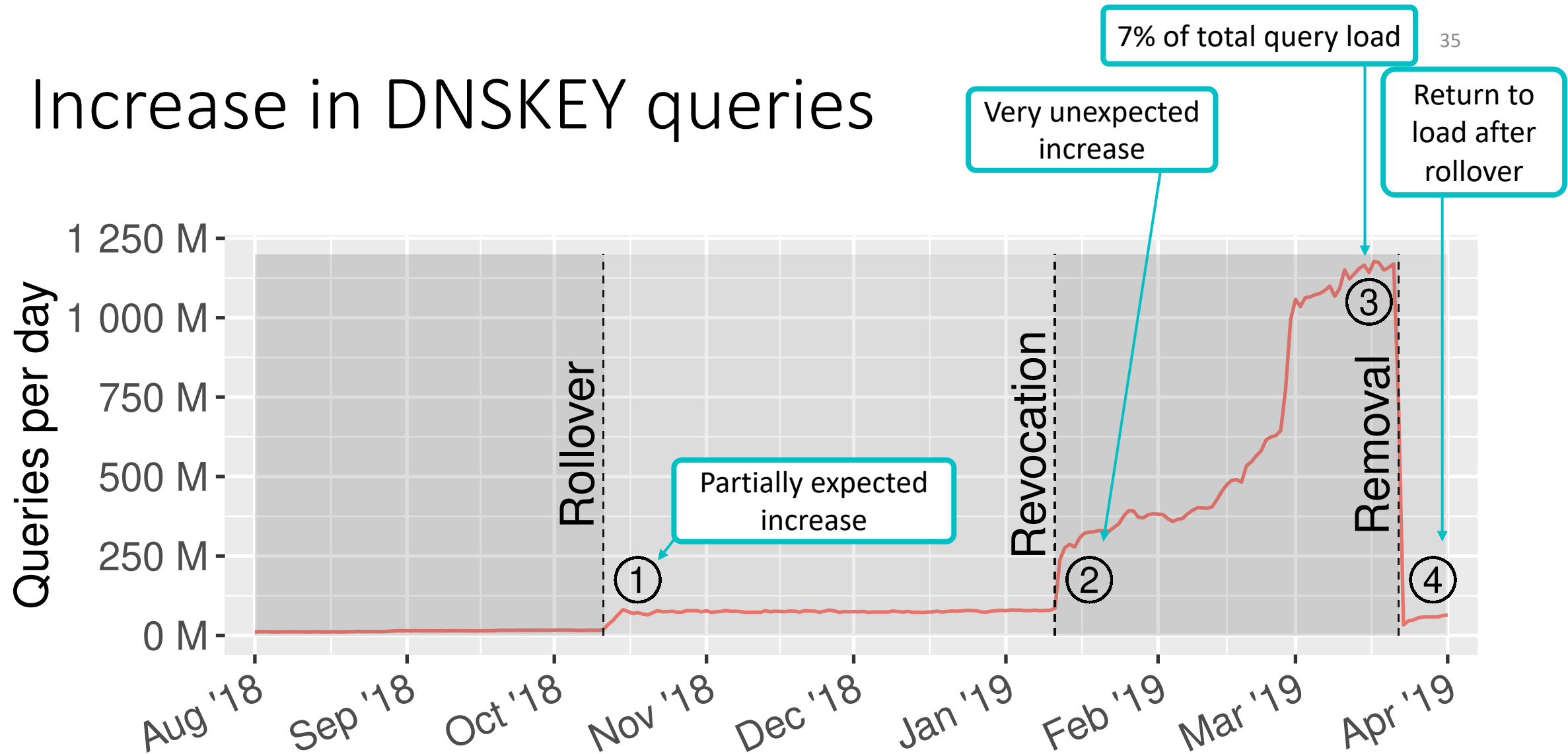
V

VI

Increase in DNSKEY queries



Increase in DNSKEY queries



I

STOP



IV

V

VI

Who's behind the query floods?

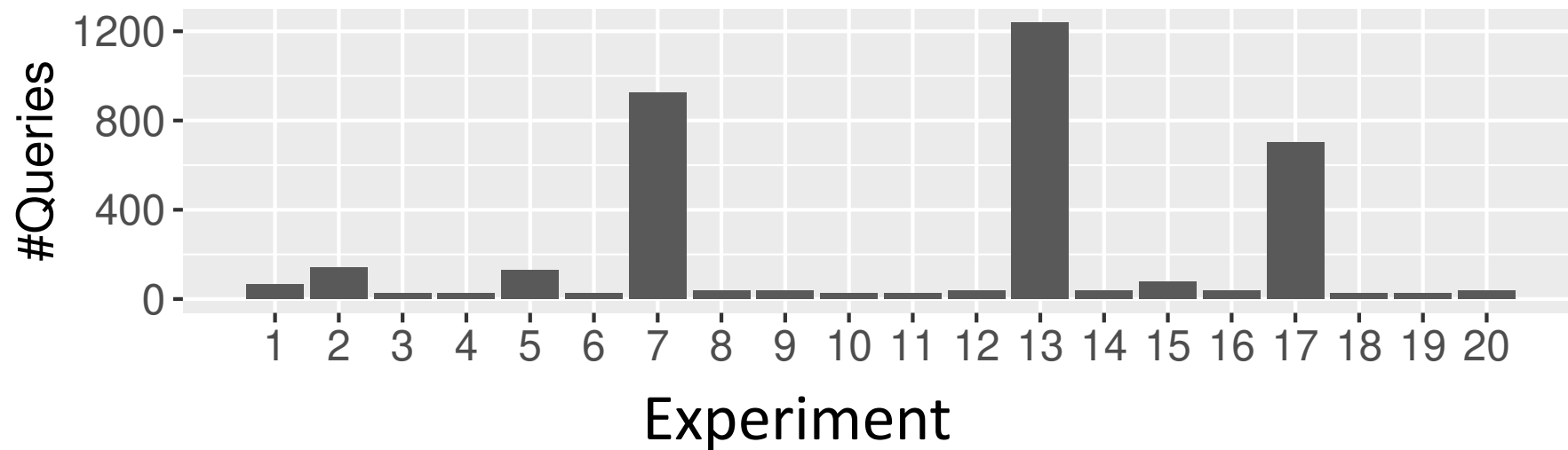
- DNS CHAOS queries to sources reveal mostly older versions of BIND
- Outreach
 - A large French cloud hosting provider confirmed a source running BIND 9.8.2 on CentOS
 - Large midwestern university confirmed DNS lab exercise and provided BIND config

Photo by Kelly Sikkema on Unsplash



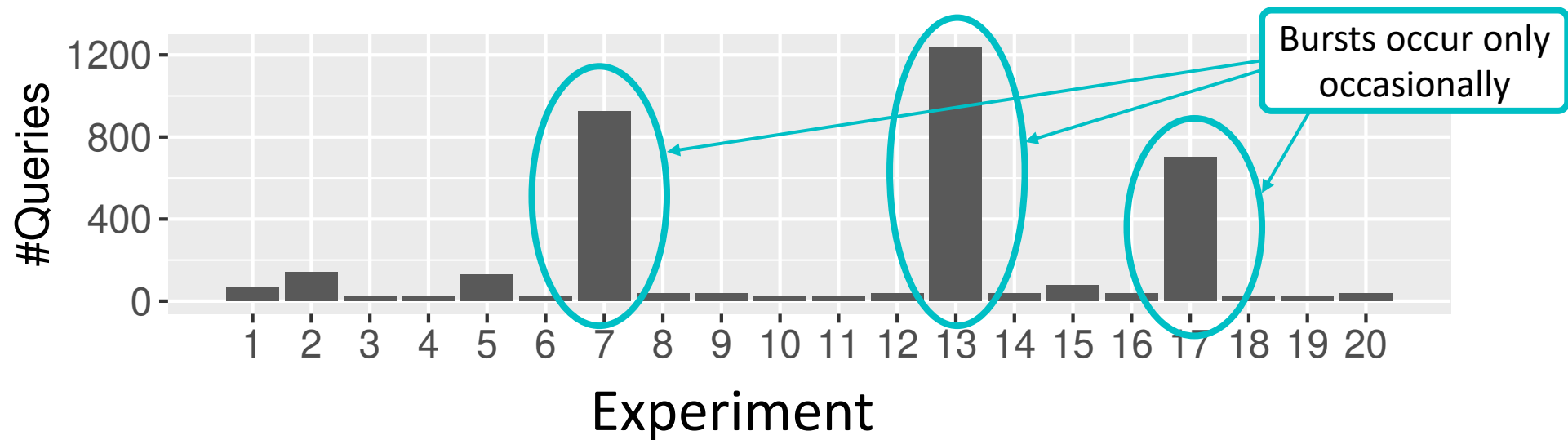
Reproducing Key Floods with BIND

- Conditions for reproducing DNSKEY floods with BIND:
 - DNSSEC managed keys contains KSK-2010, but not KSK-2017
 - The dnssec-enable flag was set to false
 - The dnssec-validation flag was unset, leaving it in its default state of “yes.”



Reproducing Key Floods with BIND

- Conditions for reproducing DNSKEY floods with BIND:
 - DNSSEC managed keys contains KSK-2010, but not KSK-2017
 - The dnssec-enable flag was set to false
 - The dnssec-validation flag was unset, leaving it in its default state of “yes.”



I

STOP

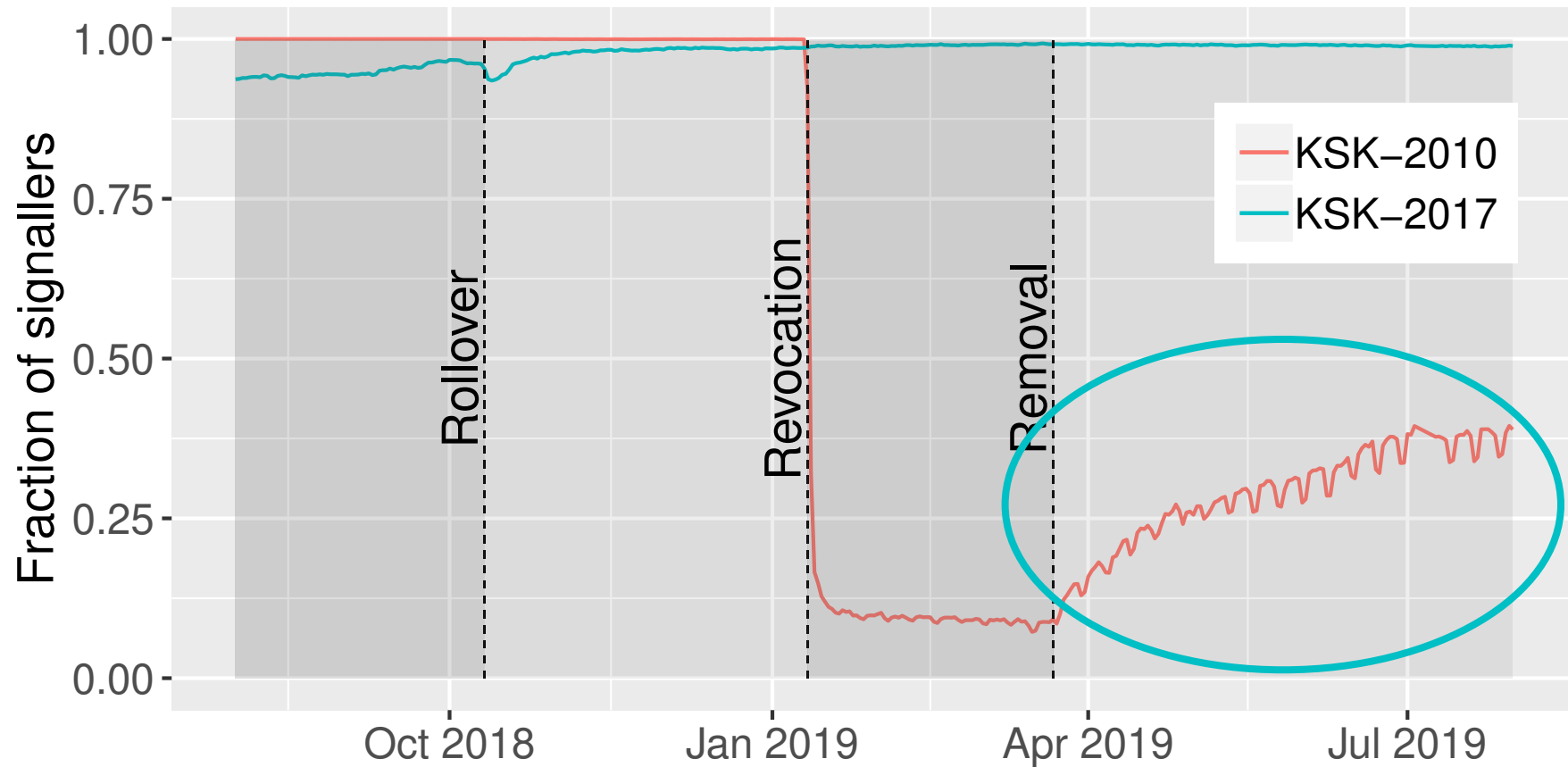


IV

V

VI

Resolver Telemetry: The return of KSK-2010



I

STOP



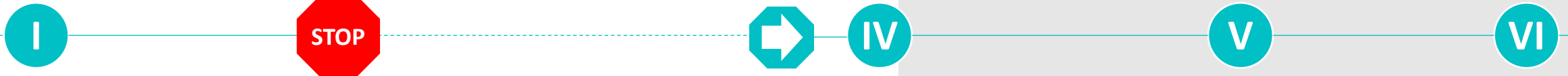
IV

V

VI

Takeaways from *after* the Rollover

- **No one** expected the massive flood of DNSKEY queries
- Trust anchor management comes in **different shapes and colors**
- Shipping trust anchors with software has **long-lasting effects**



Discussion

Do we need to improve telemetry?

- RFC 8145 and RFC 8509 are useful but should be improved
 - Allowing to identify the true source of a signal
 - Provide an estimate for how many users a signal represents

Photo by Chunlea Ju on Unsplash



Do we need to improve telemetry?

- RFC 8145 and RFC 8509 are useful but should be improved
 - Allowing to identify the true source of a signal
 - Provide an estimate for how many users a signal represents

Photo by Chunlea Ju on Unsplash

Do we need to change trust anchor management?

E.g. shipping TAs centrally in OSes?



Conclusions and broader Lessons

- The rollover was a **success**
 - **Independent analysis** and measurements on the internet are valuable
 - Telemetry must be kept in mind **at an early stage** of protocol development
 - Trust anchors should be **managed centrally**
-

Conclusions and broader Lessons

- The rollover was a **success**
- **Independent analysis** and measurements on the internet are valuable
- Telemetry must be kept in mind **at an early stage** of protocol development
- Trust anchors should be **managed centrally**

Questions, suggestions, comments?

Data available at

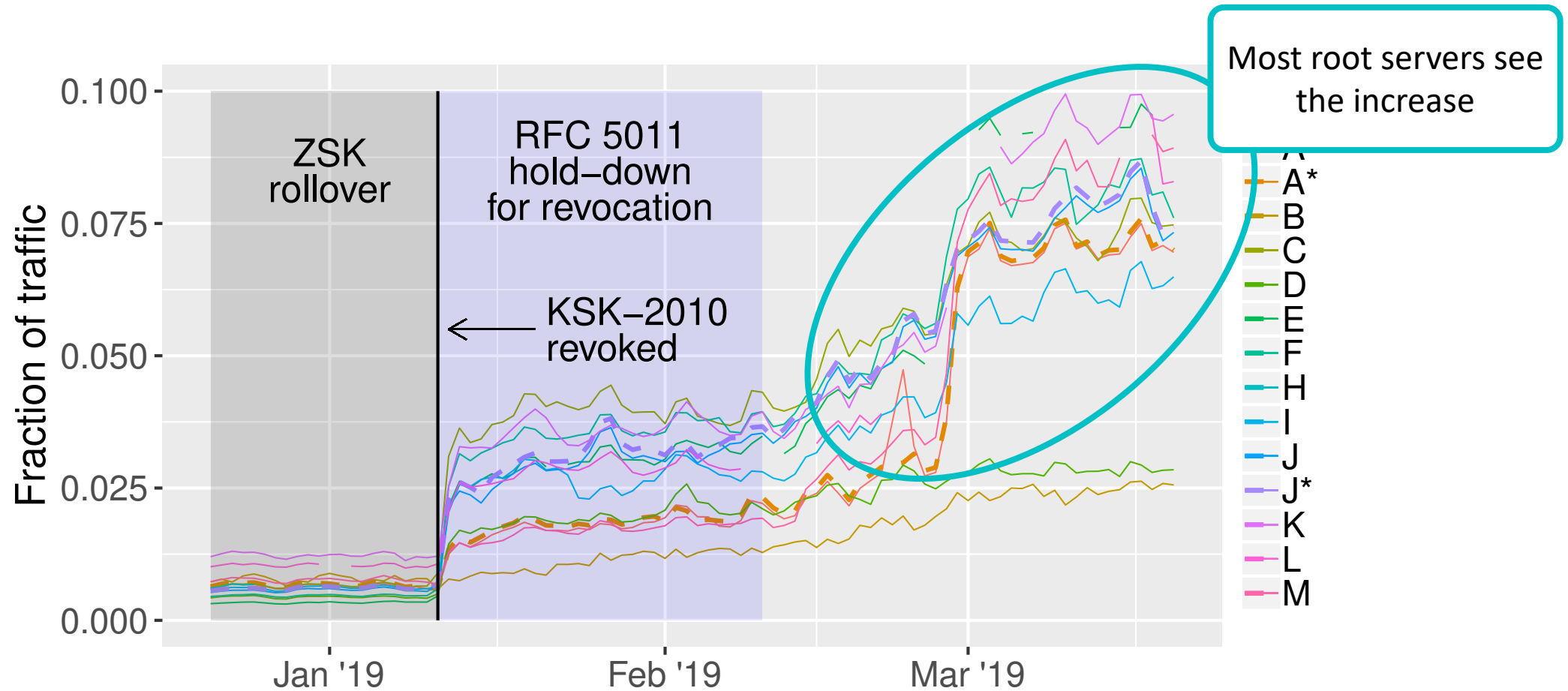
<https://github.com/SIDN/RollRollRollYourRoot>

Contact

Moritz Müller | moritz.muller@sidn.nl | sidnlabs.nl

Bonus Slides

Increase in DNSKEY queries after revocation



I

STOP

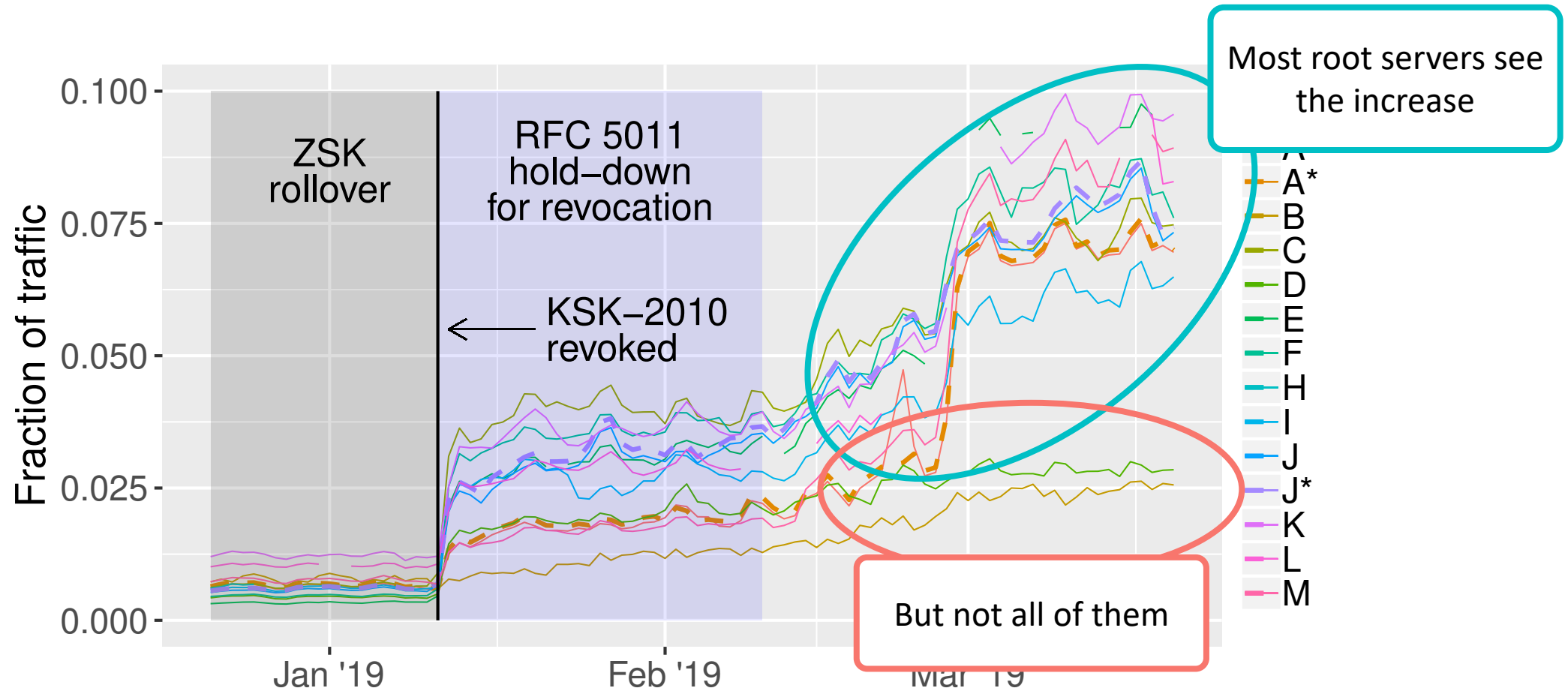


IV

V

VI

Increase in DNSKEY queries after revocation



I

STOP

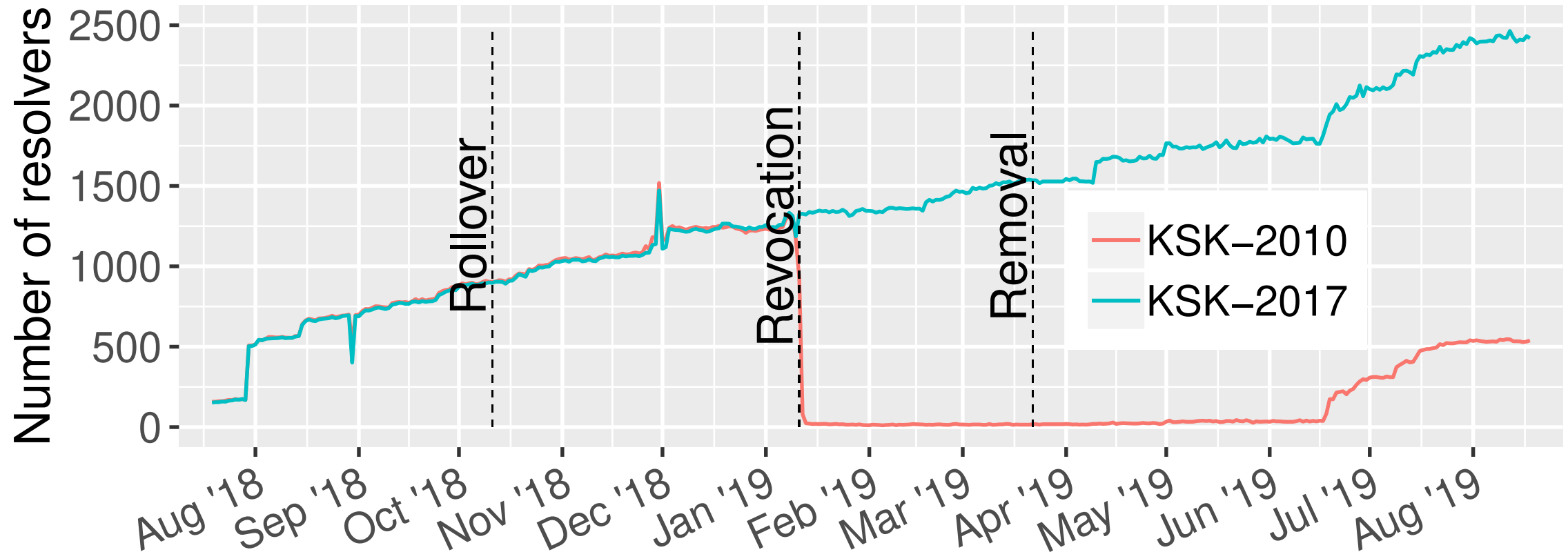


IV

V

VI

Resolver Telemetry: RFC 8509 “Root Sentinel”



I

STOP

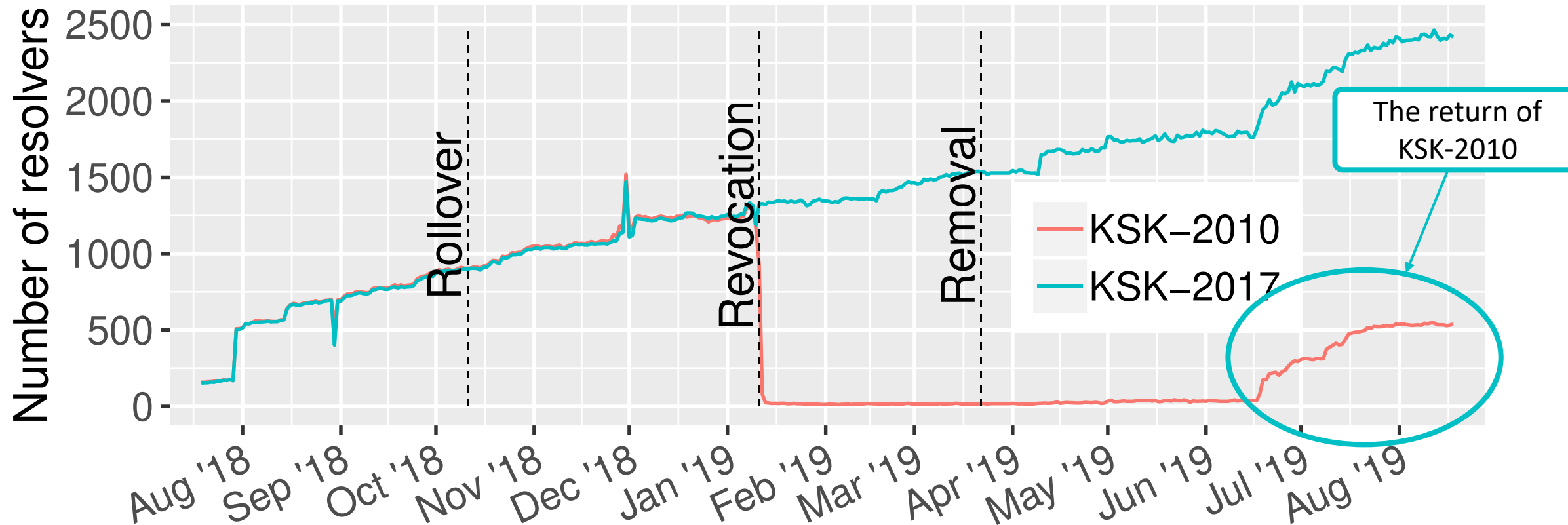


IV

V

VI

Resolver Telemetry: RFC 8509 “Root Sentinel”



I

STOP



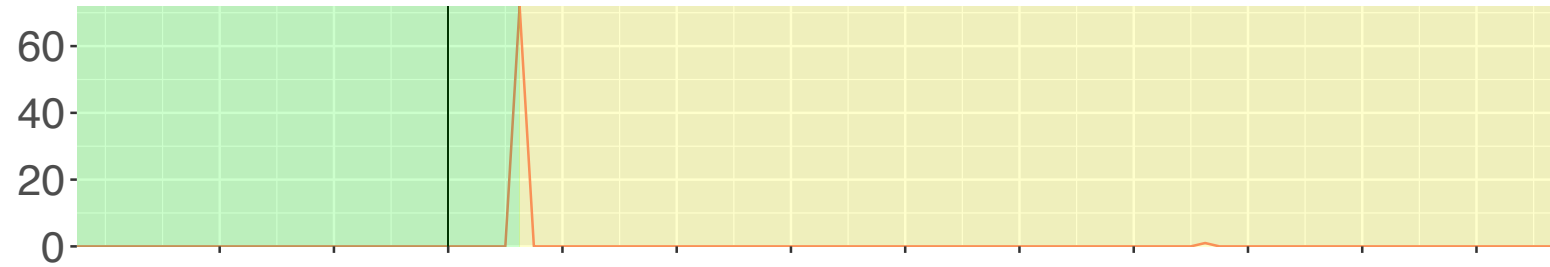
IV

V

VI

Failure Modes

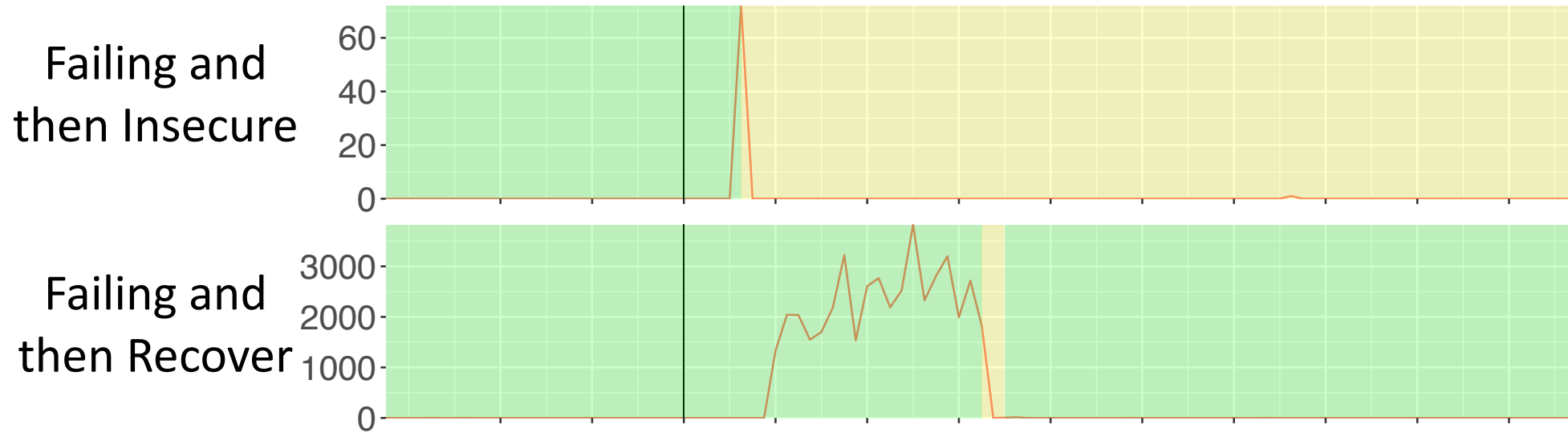
Failing and
then Insecure



Oct 11 - 00:00
Oct 11 - 08:00
Oct 11 - 16:00
Oct 12 - 00:00
Oct 12 - 08:00
Oct 12 - 16:00
Oct 13 - 00:00
Oct 13 - 08:00
Oct 13 - 16:00
Oct 14 - 00:00
Oct 14 - 08:00
Oct 14 - 16:00



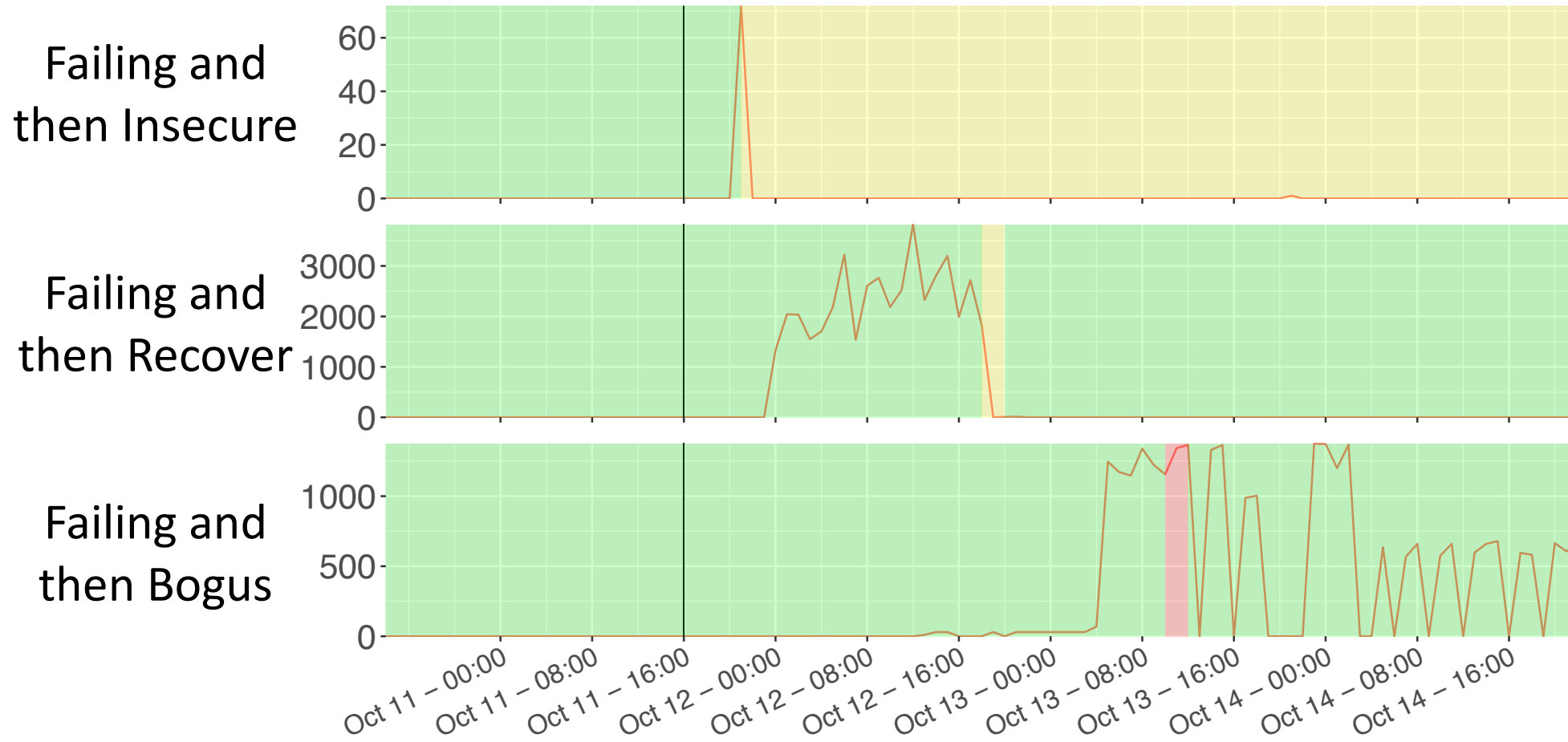
Validation Failure Modes



Oct 11 - 00:00
Oct 11 - 08:00
Oct 11 - 16:00
Oct 12 - 00:00
Oct 12 - 08:00
Oct 12 - 16:00
Oct 13 - 00:00
Oct 13 - 08:00
Oct 13 - 16:00
Oct 14 - 00:00
Oct 14 - 08:00
Oct 14 - 16:00



Validation Failure Modes



I

STOP



IV

V

VI