KSK Rollover 2015-2019

What We've Learned So Far

Edward lewis

APRICOT 2019
26 February 2019

Agenda

- KSK Rollover Project
  - Where it is
  - Audience "action"
- Reflections on Managing the Rollover
  - Role of Communications
  - Monitoring
  - Measurements
- Lessons/Questions for the Next Time

KSK Rollover Project

- Goal: Replace the key (KSK) used to sign the DNS root zone's DNSSEC key set since 2010 without disruption

- Passed many milestones, a few more to go
  - Next up: removing the revocation record for the out-going KSK on March 22

Where It Is

2015	2016	2017	2018	2019
Design Team	Plans Made; Key Created	Publicize; The "Pause"	Publicize; Change Key	Revoke; Clean Up

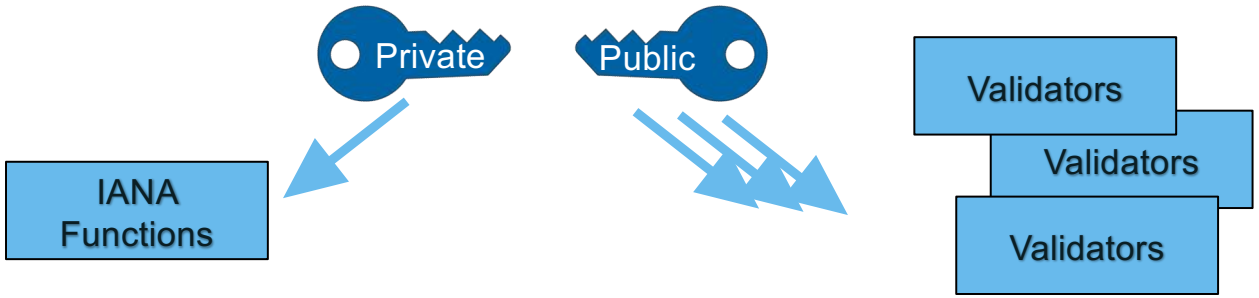
- A key rollover can be done more quickly, but "going fast" has never been the goal

Audience "Actions"

- Have you done nothing so far and have seen no problems?
  - Continue what you are doing!
- Have you been relying on *Automated Updates* (RFC 5011)?
  - Continue what you are doing!
- Are you manually managing the configuration of DNSSEC trust anchors?
  - Remove the old key (2010) from trust anchors.

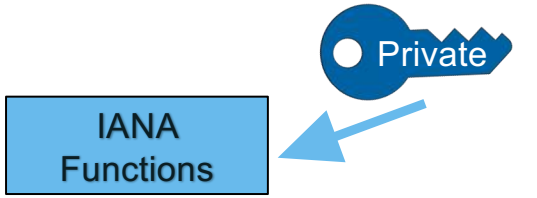
Project Considerations

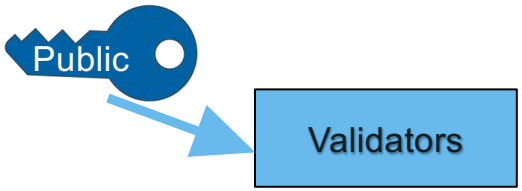
- The KSK is a private-public key pair
- IANA Functions Operator uses the **private key** to sign the "top" of the DNSSEC hierarchy
- Validator operators configure their DNSSEC validating servers with the **public key**

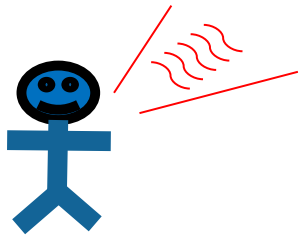


The Project's "Problem to Solve"

- Rolling the Private Key
  - Simple
- Rolling the Public Key
  - Simple
- Coordinating the actions
  - Difficult
  - An exercise in communications







Technical Tools

- *Automated Updates of DNSSEC Trust Anchors*
  - Also known as "RFC 5011"
  - Some don't like idea of self-configuring edge devices, others rely on the convenience
- A functional but difficult to manage protocol
  - Proven (albeit in few cases)
  - DNS lacks measurement hooks
  - DNS lacks testing hooks
  - Requires attentive operators

The Permission-less Internet

- *Permission-less* means operators make their own choices and are responsible for their actions
- This has enabled DNS to scale very well
- But
  - *Automated Updates* is a choice, not required
  - No list of operators configuring the key
  - Not easy to "snoop", no pervasive monitoring

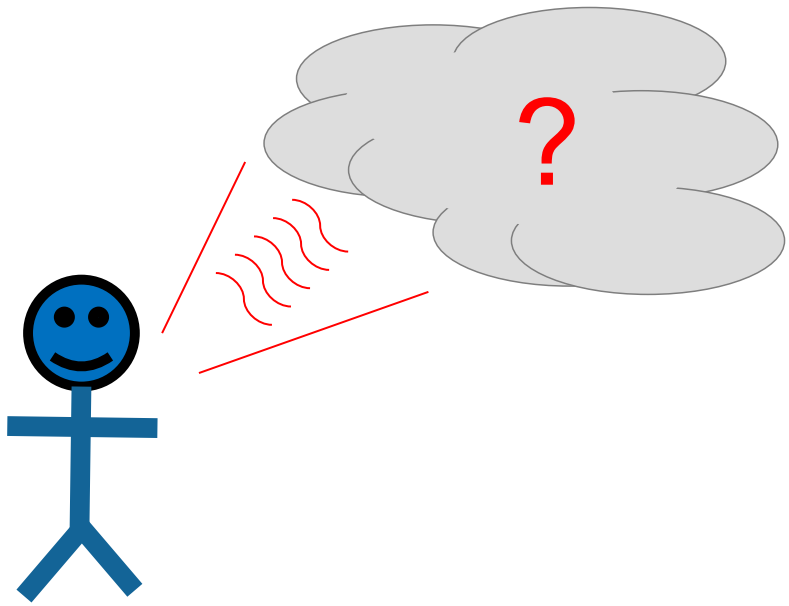
Approach to the Rollover

- Communications

- Technical management
  - Testing
  - Monitoring
  - Measurement

Communications to/with an Unknown Audience

- Permission-less: No list of audience members
- Timing of messages
  - Different skill sets
  - Different focus
  - Different forums
- Conferences
- Media engagements
  - Interviews
- Letters



Adventures in Testing

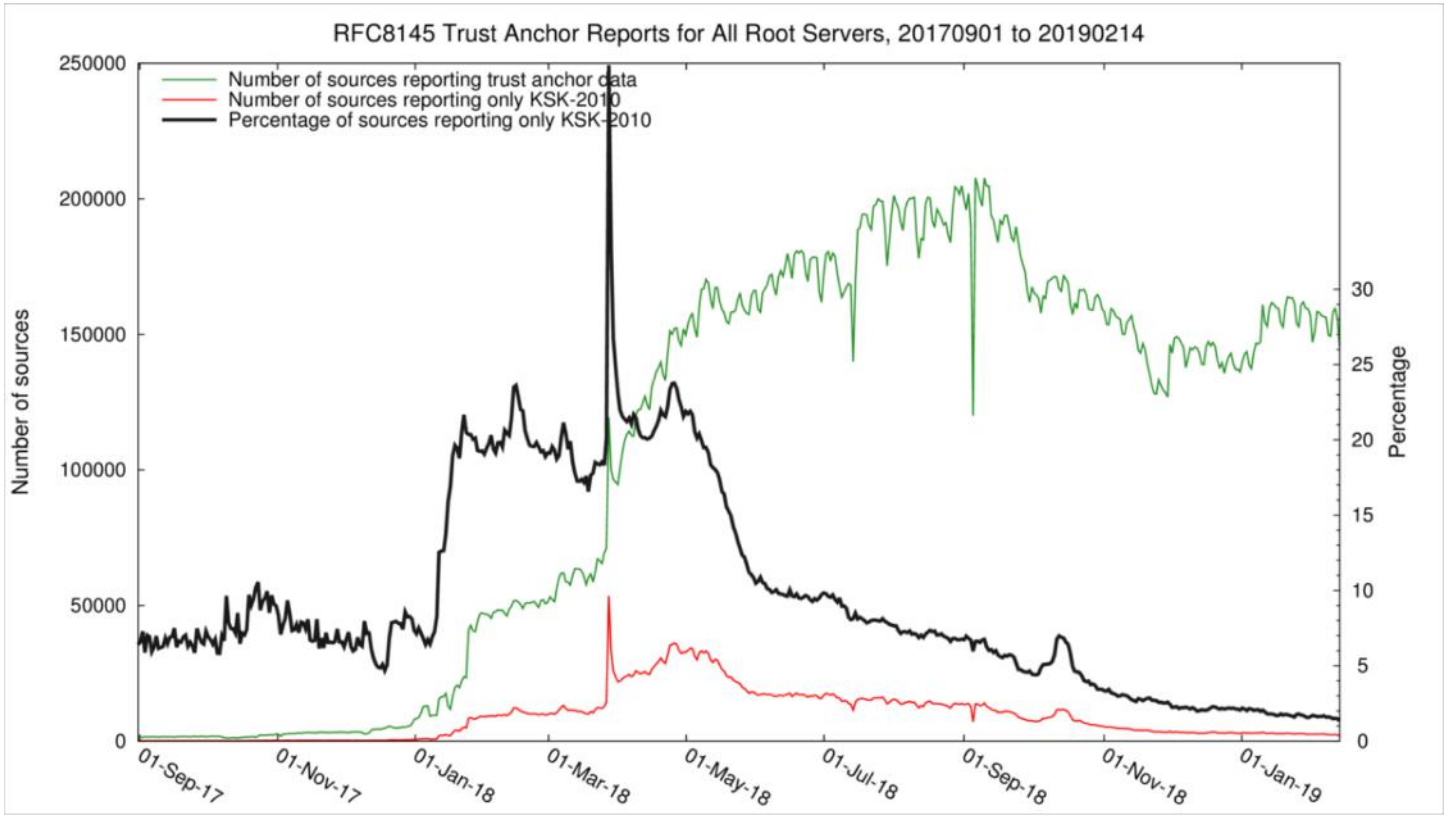
- The live system is very constrained
  - Can't use the key outside it's production use
  - DNSSEC is not favorable to test cases
    - Cannot isolate use of a specific key for specific data
- Test beds for software 'capabilities' benefits developers
- Test beds for configurations was not too popular

Adventures in Monitoring

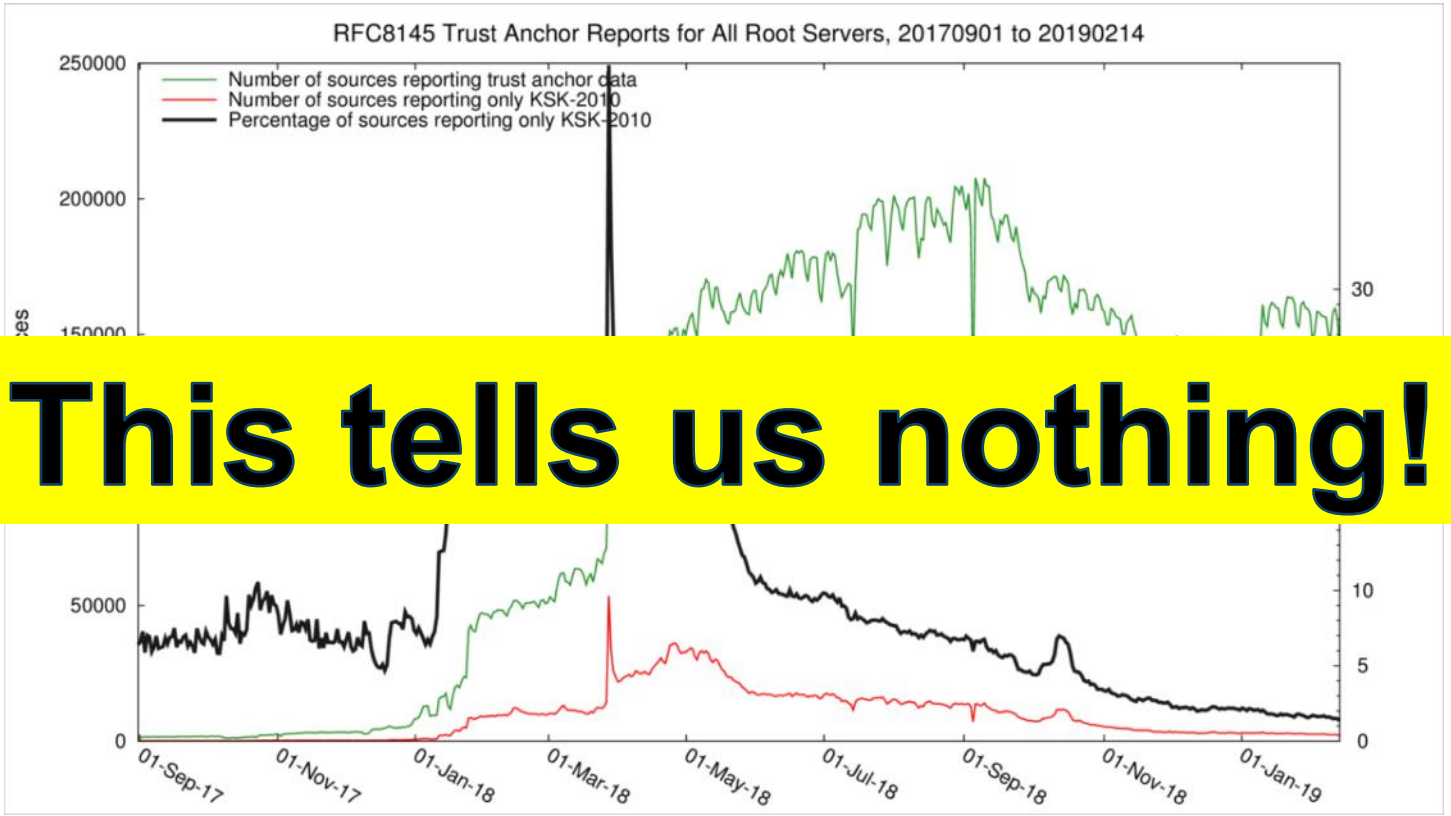
- Many tried to design a way to "third-party" test operator readiness
  - No promising efforts
  - Rising concerns of pervasive monitoring and desires for privacy, we are getting further from this

- Nevertheless, IETF rushed to define "Signaling Trust Anchor Knowledge in DNS Security Extensions (DNSSEC)" (RFC 8145)
  - And then a replacement for that...

Key Tag Reports, 01 September 2017- 14 February 2019



Key Tag Reports, 01 September 2017- 14 February 2019



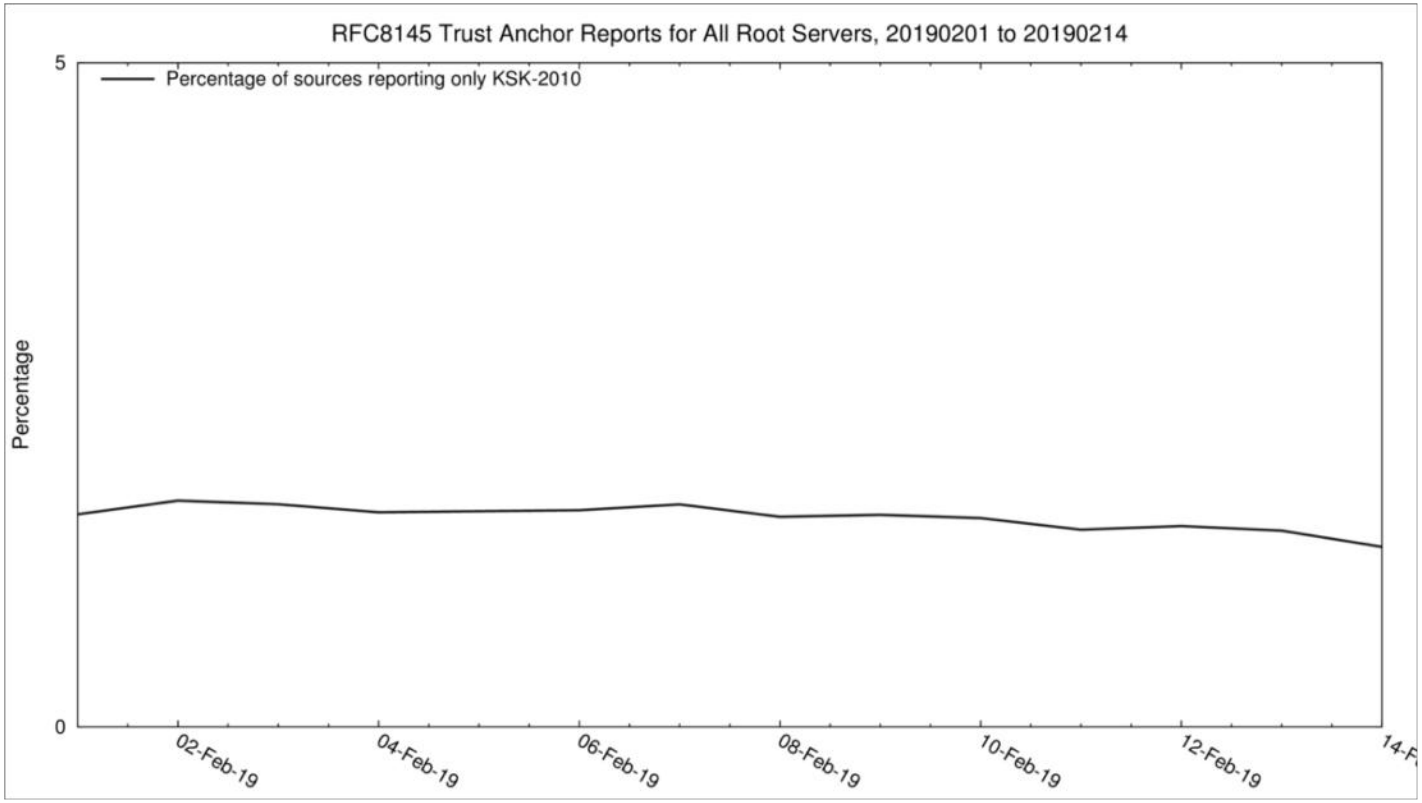
This tells us nothing!

Experience with *Signaling Trust Anchor Knowledge in DNSSEC*

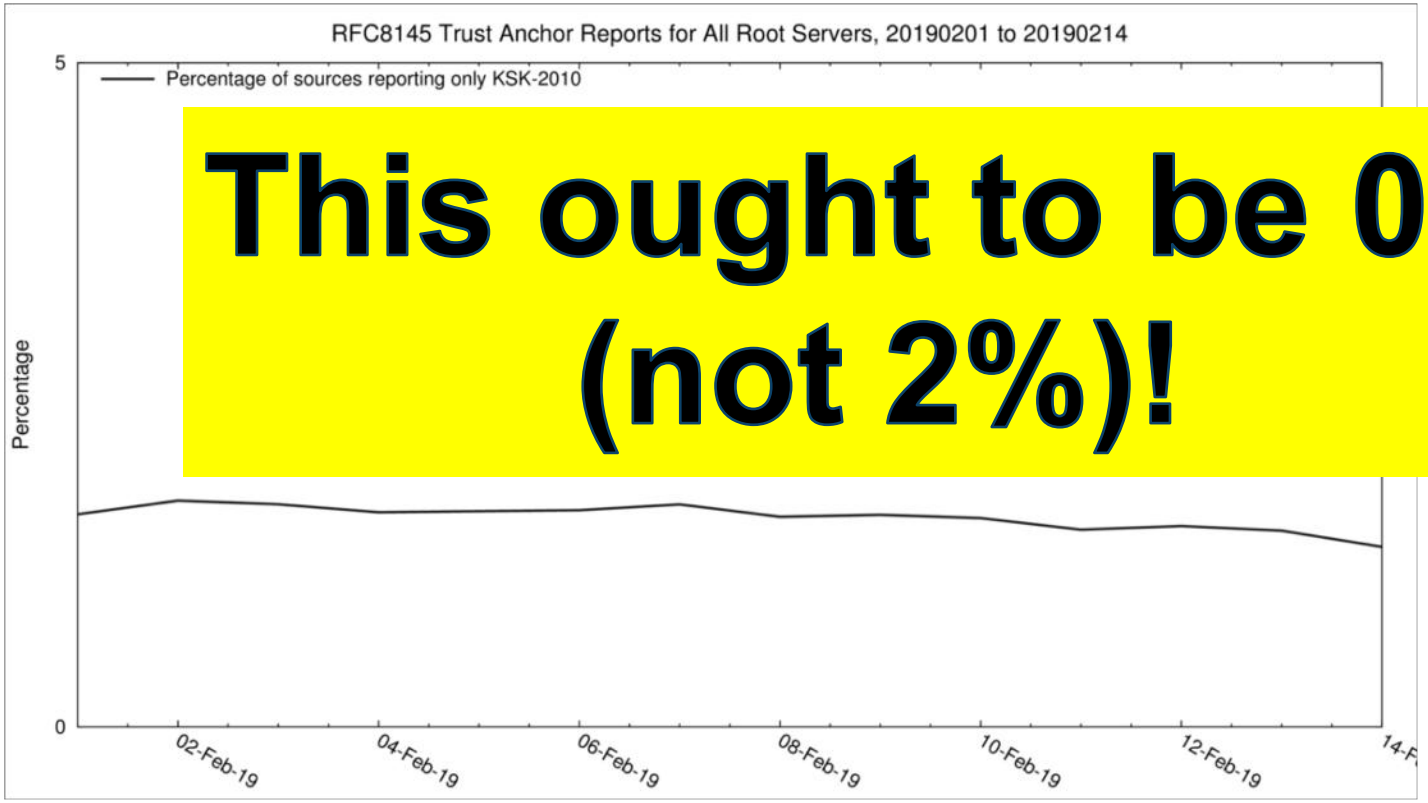
- Due to "newness" : biased towards "new code only"
- Represents small population of operators
  - Large in number, small in percentage
- Buggy implementation(s) skew results significantly

- Still, the statistics were discouraging and led to a 1 year delay
- Looking back, this measurement is not reliable

Key Tag Reports, 1 February 2019 - 14 February 2019, "Percent" only



Key Tag Reports, 1 February 2019 - 14 February 2019, "Percent" only



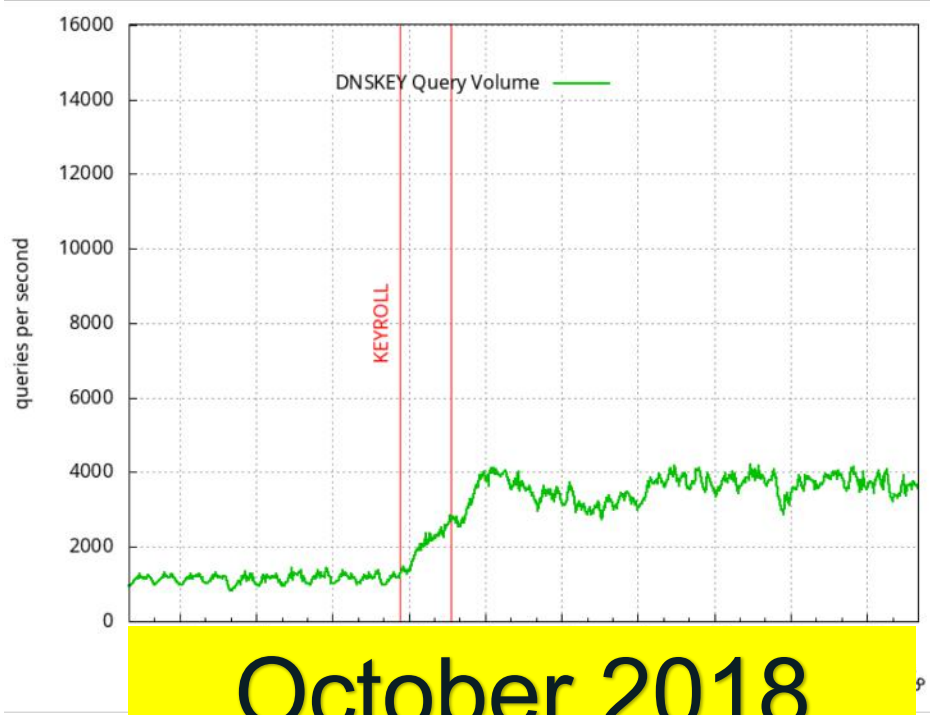
Adventures in Measurement

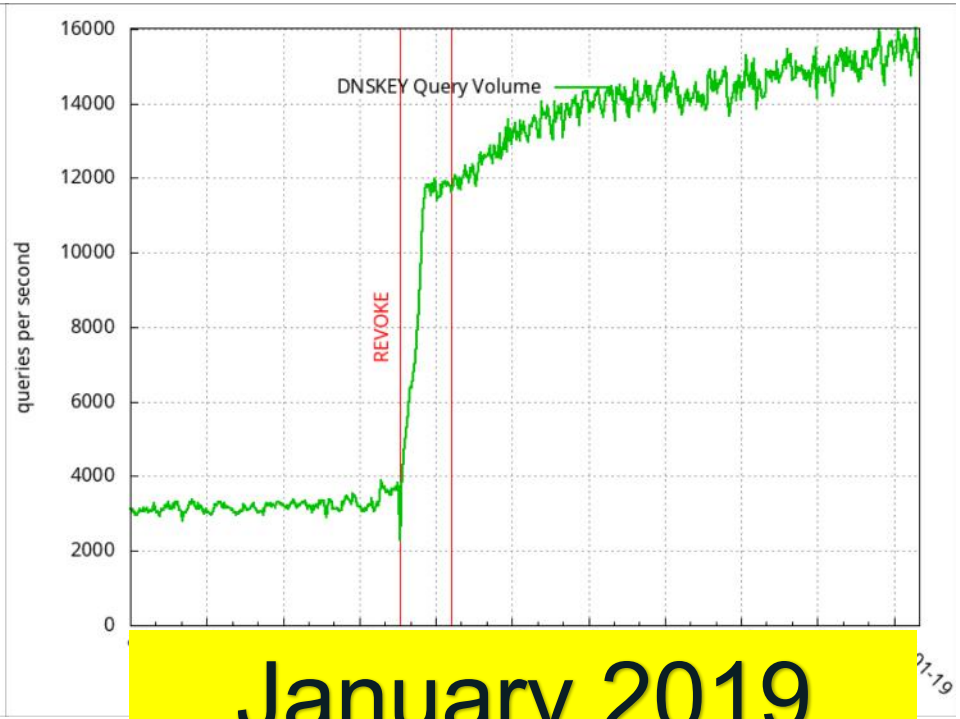
- Measuring impact
- Queries seen at the DNS root servers for DNSKEY records
- In theory we shouldn't see a sustained change from event to event in the roll – perhaps brief rises during transitions
  - But we are seeing something different

Counting Queries

- Next slides show the counts of queries for the root zone's DNSKEY set
  - A measure of resolvers doing DNSSEC and needing to update the key set
  - First – simple counts during the months of the Rollover (October 2018) and Revocation (January 2019)
  - Second – comparing individual resolver's query rates before and after some event (changed behavior is a symptom)

DNSKEY queries seen at "most of" the DNS Root Servers

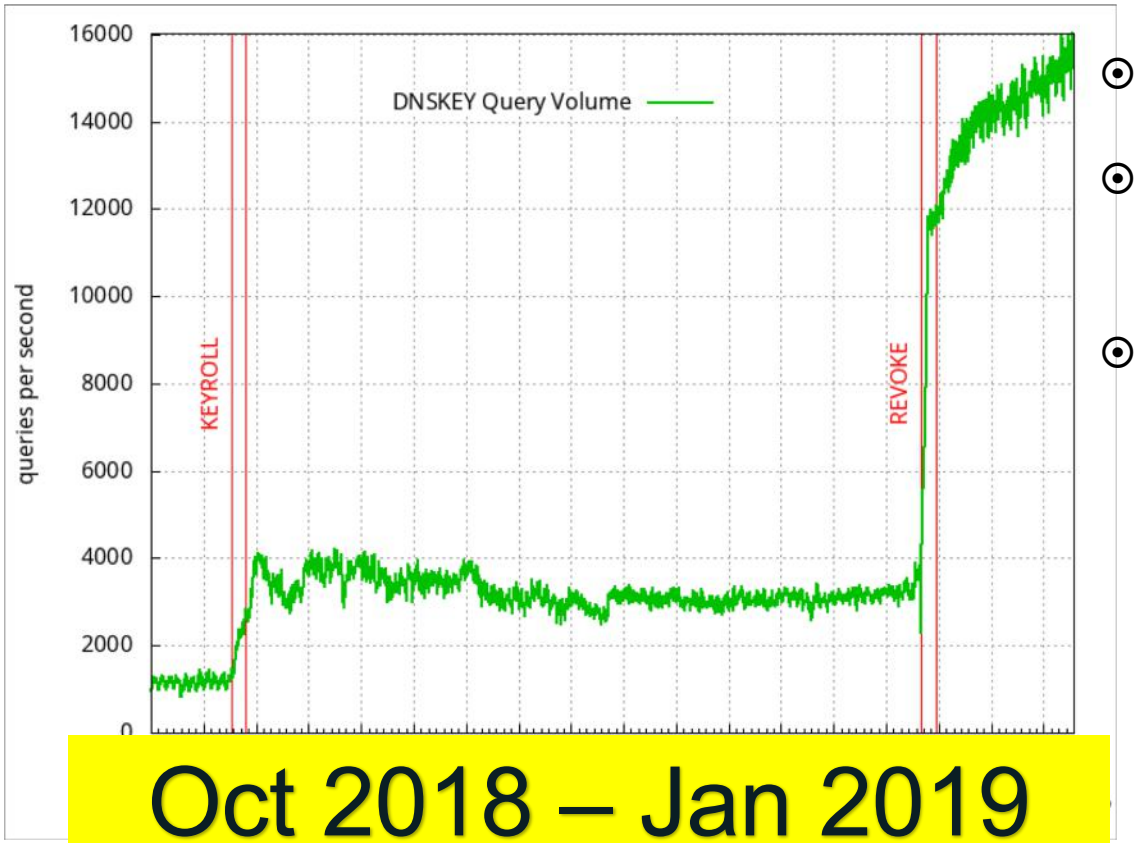




October 2018
Key Change/Roll

January 2019
Revocation

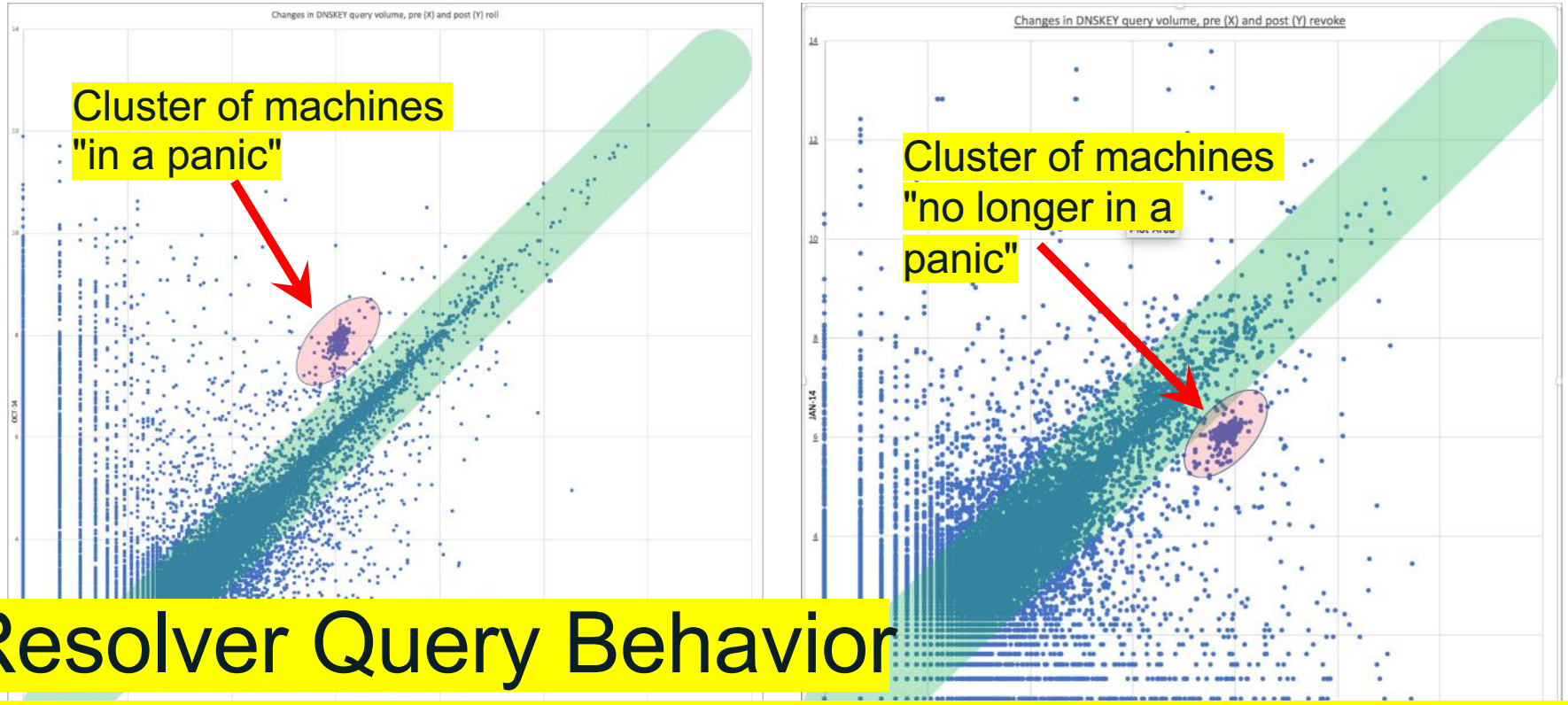
DNSKEY queries seen at "most of" the DNS Root Servers



Oct 2018 – Jan 2019

- Surprising
- No seeming impact (no complaints)
- We may not have the whole story yet
  - Note how the data settled in November

Oct 10 vs. Oct 14 and Oct 14 vs. Jan 14 ("problem" to "fixed")



Resolver Query Behavior Before and After the Rollover (Key Change)

Oct 10 vs. Jan 14 (same total span of time)

- This simply shows a return to "normalcy"
- No sustained "shift" around the change in signing key

Before and After the Rollover (Key Change)

Before and After the Revocation (10 Jan vs. 14 Jan)

- However...
- Around the revocation (11 January) there seems to be a lot of machines "in a panic"
- It may be too early to tell the "shape" of this

Before and After introducing the Revocation

Next Steps

- We need to collect data for a longer timespan
  - In March the revocation DNSKEY record is removed
  - Will we return to the old "normal" levels?
  - Premature to draw conclusions
- Should understand changes when none is expected
- Common assumption: unused/ignored machines? That many?

Other Observations of the Rollover

- In 2015, discussions were theoretical, academic
  - Nature of "trust", what is the true "top key"
  - Preferred ways to get new key
  - Design measurements, testbeds
- Doing it made it real
- By 2018, practical considerations
  - Include the new key in DNS software
  - Use email and surveys to reach operators
  - "Get it done"

The Future of Measurement/Monitoring

- Why aren't there effective tests or measures?
  - Knowledgeable people tried
  - The DNS is not built to make this easy
- What then?
  - Look for alternatives
  - Different expectations
  - Innovate/change coordination model

Lessons in perspective

- The rollover effort once again highlights the continuing need of out-of-band ("people") coordination to make the DNS work
- Variations of code and of configurations still are an issue
  - Noted in *Development of the Domain Name System* (1988)
- There remain fundamental issues with achieving a manageable and secure distributed, federated system

Engage with ICANN

Thank You and Questions

Visit us at **icann.org**
Email: edward.lewis@icann.org

@icann

linkedin/company/icann

facebook.com/icannorg

slideshare/icannpresentations

youtube.com/icannnews

soundcloud/icann

flickr.com/icann

instagram.com/icannorg