Root Zone KSK Rollover update

Roy Arends
Principal Research Scientist, Office of the CTO, ICANN

FOSDEM 2019

3 February 2019

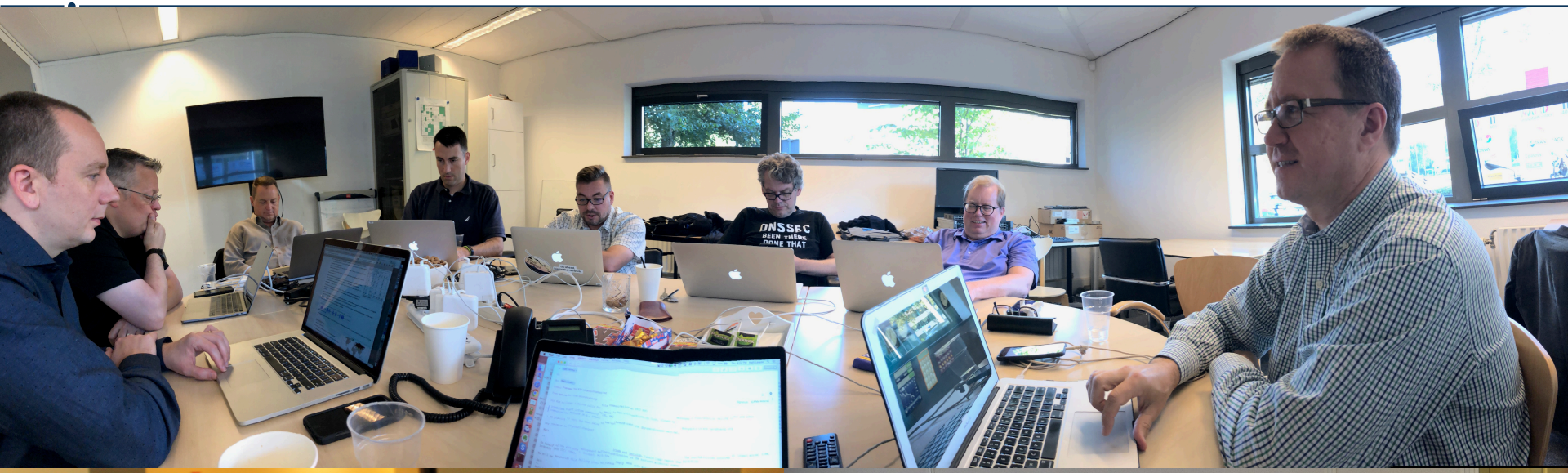
The KSK rollover has happened!

- The KSK rollover occurred on time as planned at 1600 UTC on 11 October 2018 with the publication of a root zone with KSK-2017 signing the root zone DNSKEY RRset for the first time.

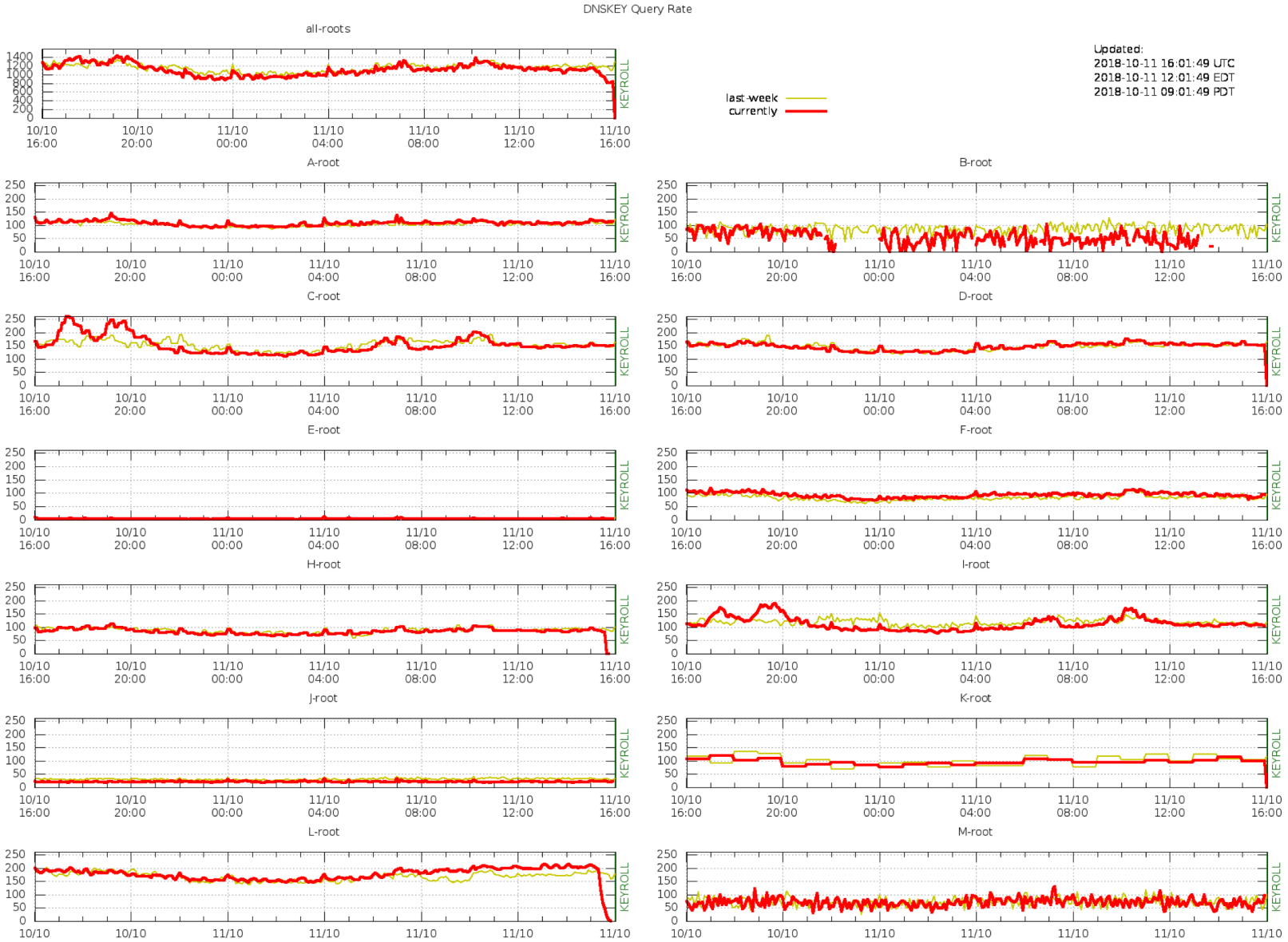
Timeline of events (UTC)

- 13:00 Root Zone Management Partners join conference bridge
- 13:00 Verisign generates root zone file
- 13:15 Verisign inspects root zone file
- 13:30 Verisign sends root zone file to ICANN
- 13:30 ICANN inspects root zone file
- 15:30 ICANN Go/No-go call
- 15:45 ICANN approves the zone for publication
- 15:45 Verisign reminds root server operators of scheduled zone push
- **16:00 Verisign approves root zone file push**
- 16:05 Verisign informs root server operators zone file has pushed

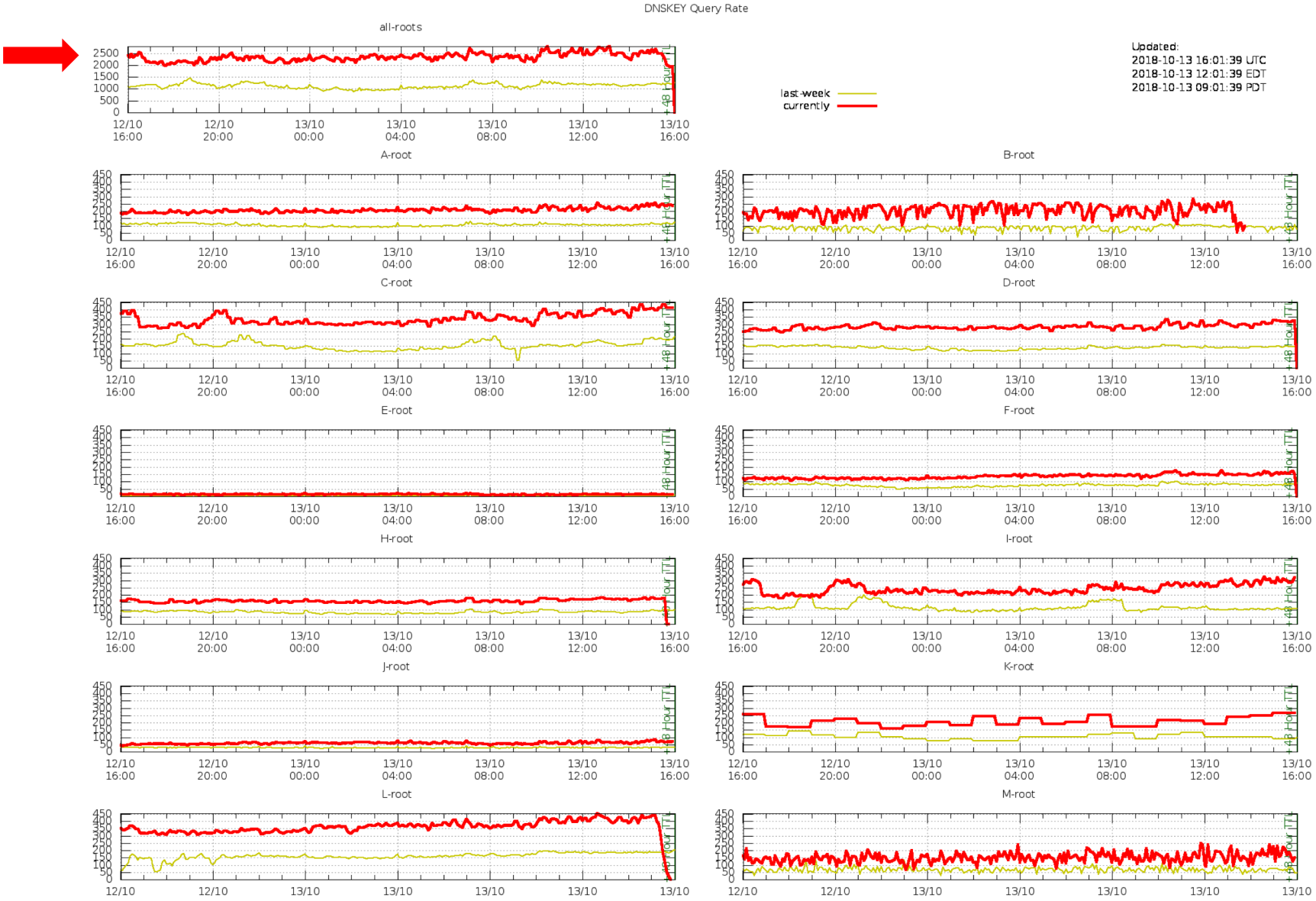
Amsterdam team



Monitoring: ./IN/DNSKEY queries at the root (just before the roll)



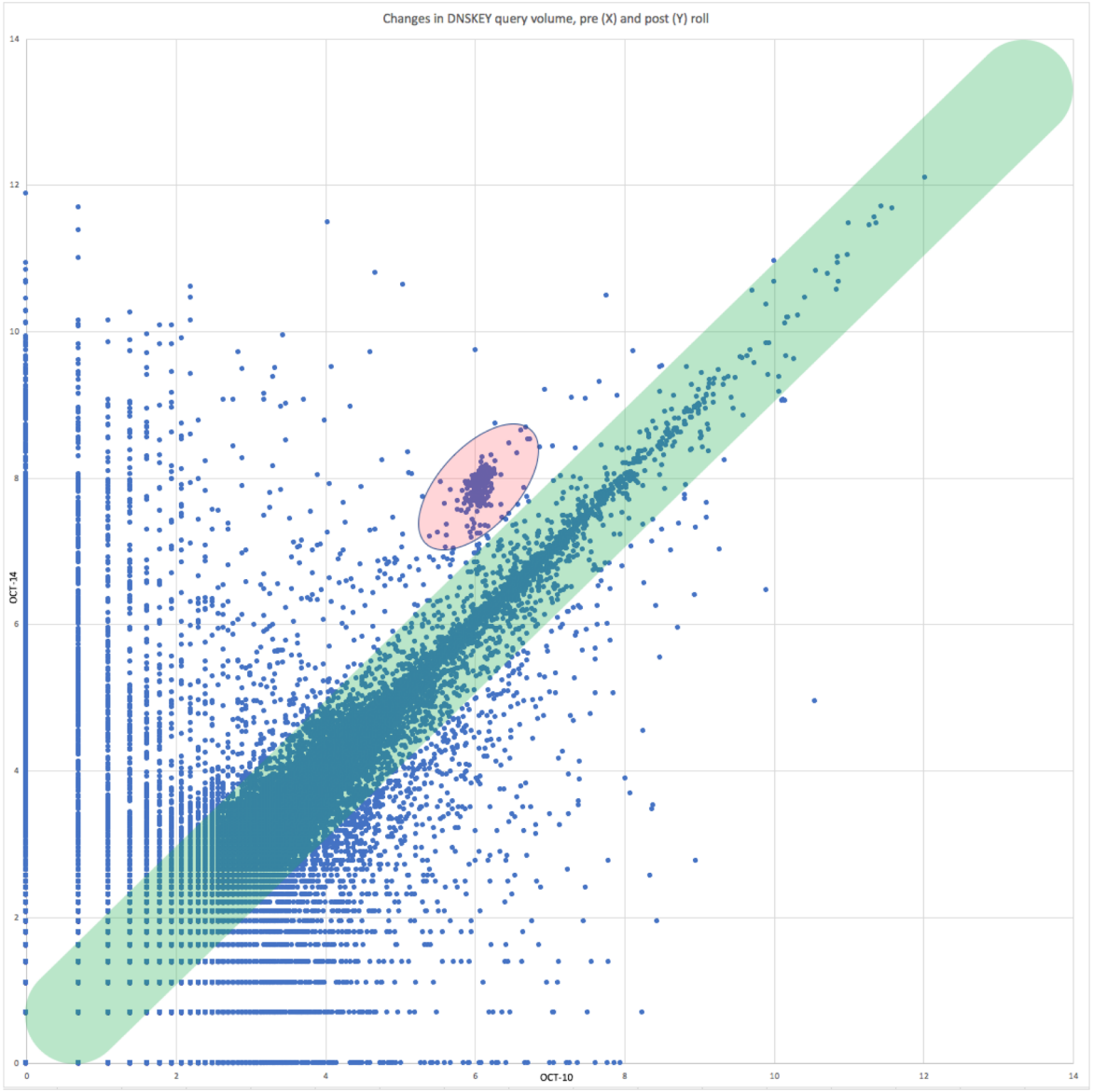
Monitoring: ./IN/DNSKEY queries at the root (48 hours after the roll)



Analysis of DNSKEY queries

- Testing proved that stale trust anchors cause an increase in DNSKEY queries
- OCTO compared DNSKEY query behavior before and after the roll
  - October 10 and 14
- We've observed a total of 1,091,215 unique resolvers asking for a DNSKEY over four days
- 155,117 unique resolvers observed on both 10 October and 14 October
  - 85,531 resolvers sent a DNSKEY request at least once a day between the 10 October and 14 October
  - Vantage point was IMRS/L-root
  - Resolvers might talk to other root letters
- OCTO tracked each of the 155,117 resolvers for change in query behavior

DNSKEY queries (10 October vs. 14 October)



DNSKEY scatter plot

- The X axis represents query volume on 10 October in log scale
- The Y axis represents query volume on 14 October in log scale
- Each blue dot represents an observed resolver, plotted (X,Y) on the graph
- Expected behavior is in the green diagonal band, showing changes within the same order
- Anything above the green band is O(1) increased query volume
- Anything below the green band is O(1) decreased query volume
- The red represents an unexpected clustering that we're actively investigating

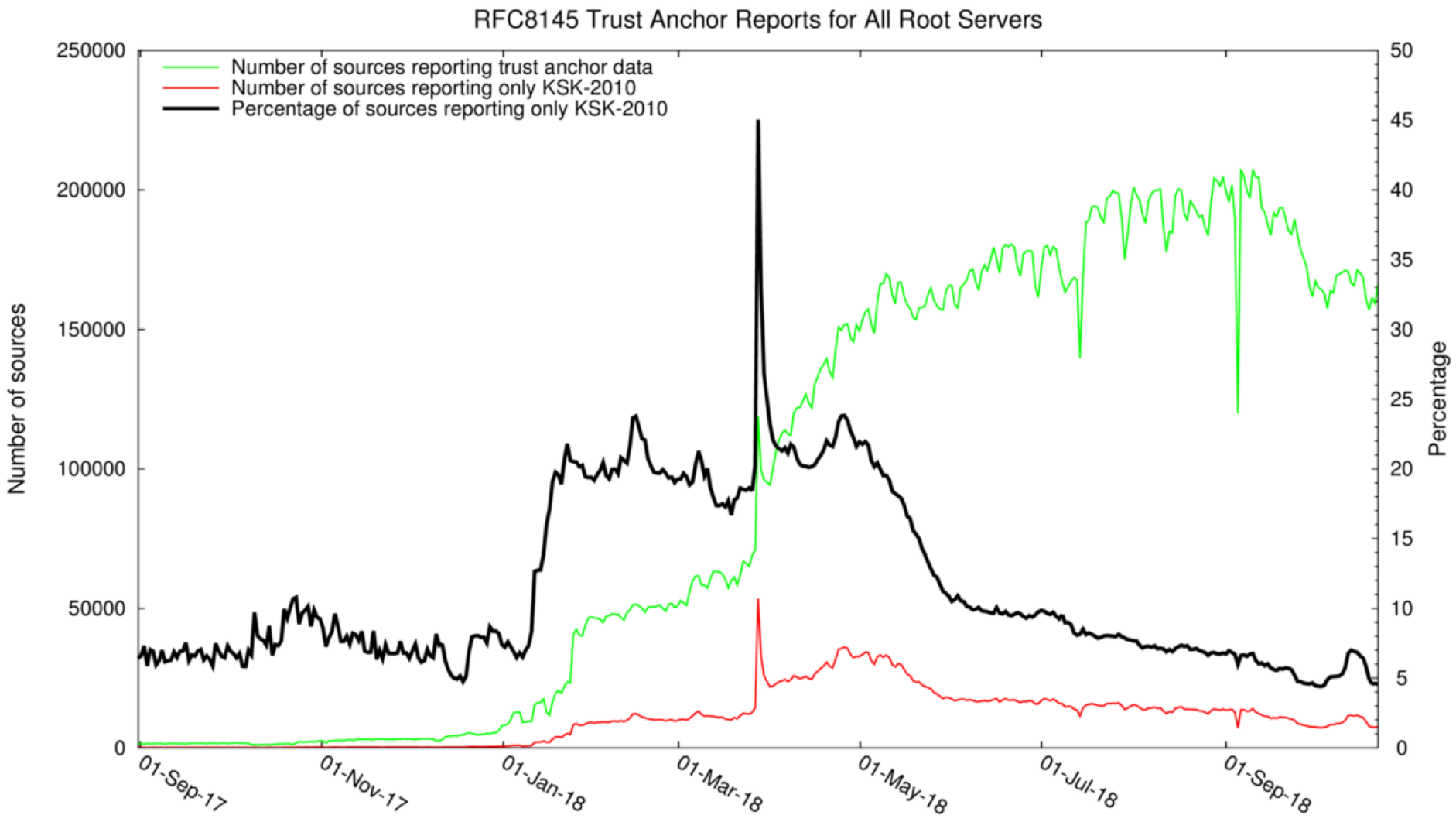
Resolvers per order change

Resolvers per order change

- The X axis represents buckets of “volume order change”
- The Y axis represents the number of resolvers in a bucket
- The bulk of resolvers lie between -1 and 1
  - Less than an order of magnitude change in the number of queries issued

- Between -1 and 1: 148,502 resolvers or 95.7% of the total observed
  - Relatively little change in volume
- Great than 1: 2,084 resolvers or 1.34% of the total observed
  - They see their volume increase significantly
- Less than -1: 4,531 or 2.92% of the total observed
  - They see their volume decrease significantly

root-trust-anchor-reports.research.icann.org



Known issues

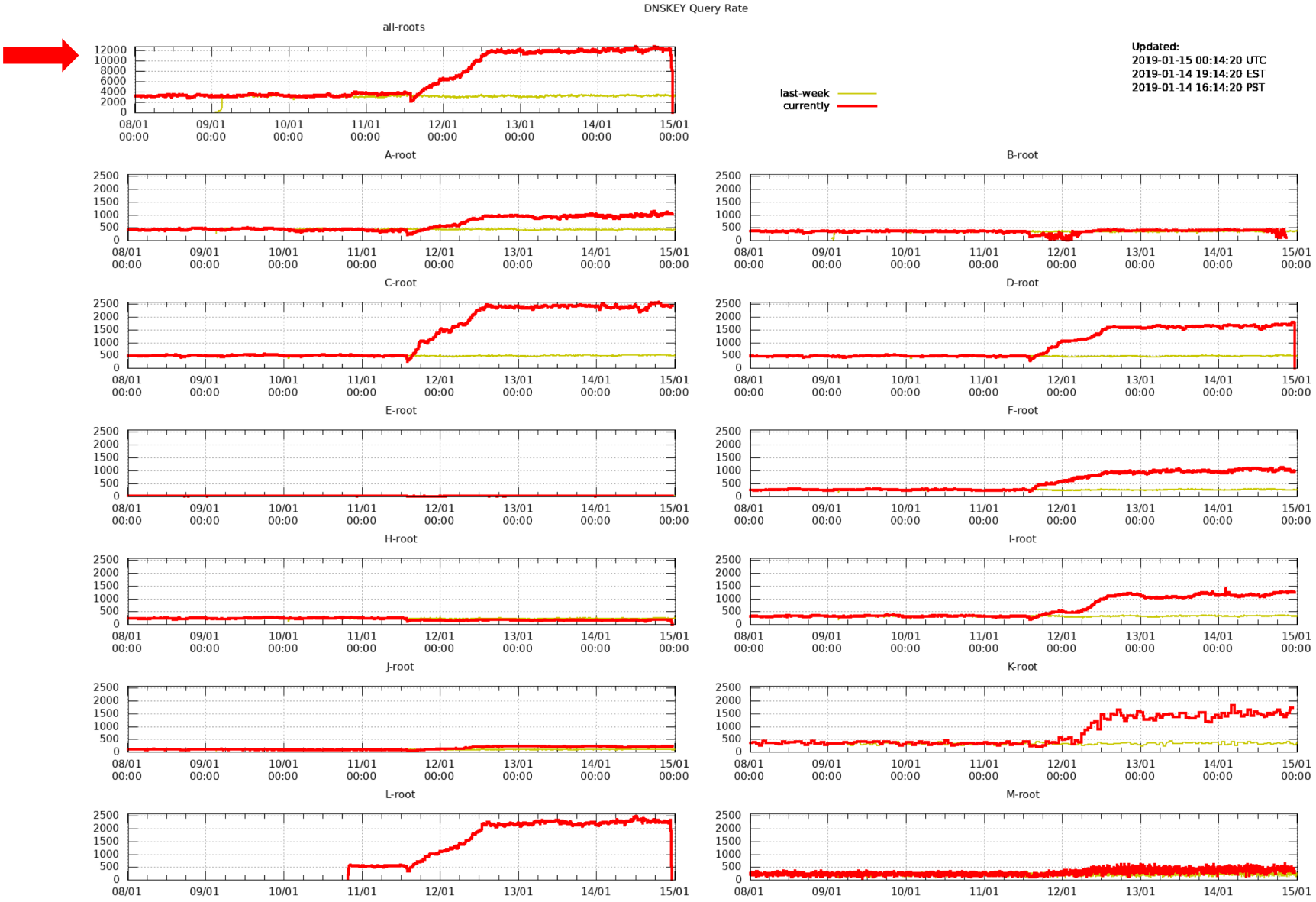
- Only one very minor report of trouble to ICANN
- A small number of reports of issues (<10) via Twitter, mailing lists and operational forums
  - Mostly individual administrators relating minor issues
  - No reports of significant number of issues affected
- Two outages may potentially be the result of the KSK rollover. We are trying to reach the ISPs involved to get more information.
  - eir (Irish ISP): https://www.rte.ie/news/2018/1013/1002966-eir-outage/
  - Consolidated Communications (Vermont, US ISP): https://www.wcax.com/content/news/Consolidated-Communications-scrambles-to-fix-Vt-internet-outage-497030071.html

The KSK revoke has happened!

- The KSK rollover occurred on time as planned at 1600 UTC on 11 October 2018 with the publication of a root zone with KSK-2017 signing the root zone DNSKEY RRset for the first time.

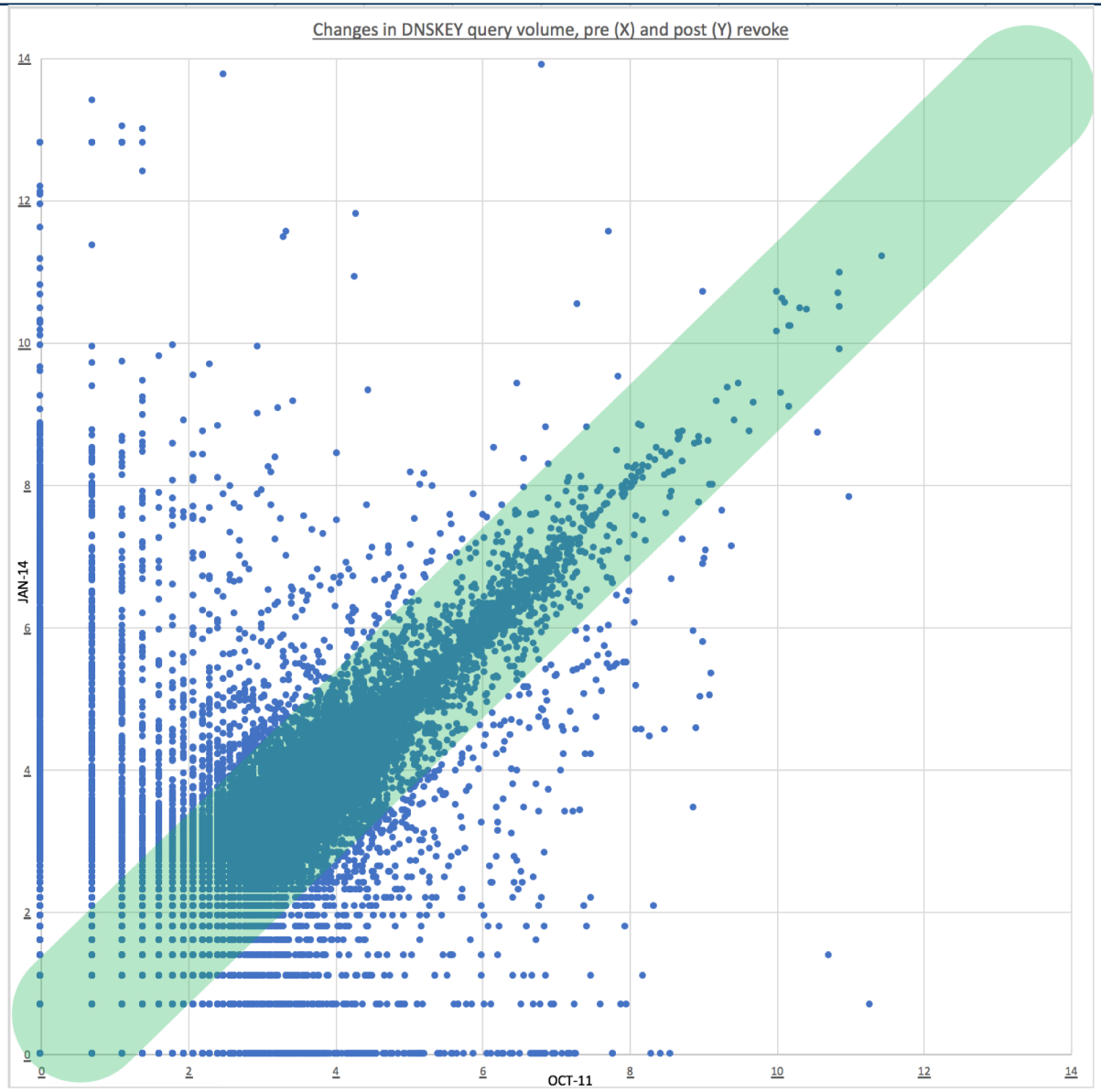
- The KSK revoke occurred on time as planned at 1400 UTC on 11 January 2019 with the publication of a root zone with KSK-2010 marked as revoked.

Monitoring: ./IN/DNSKEY queries at the root (48 hours after the revoke)

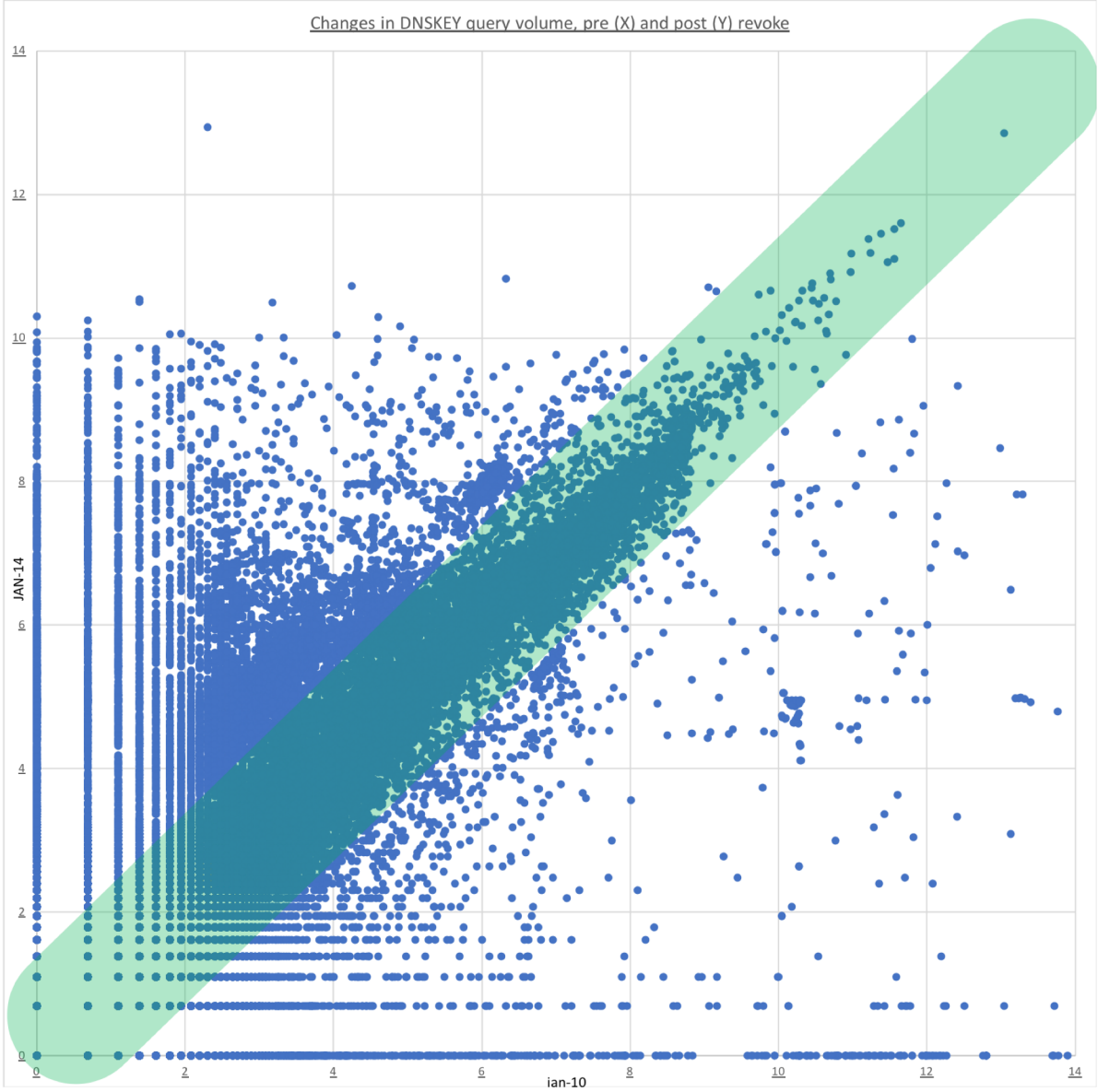


DNSKEY queries (14 October vs. 14 January)

DNSKEY queries (11 October vs. 14 January)

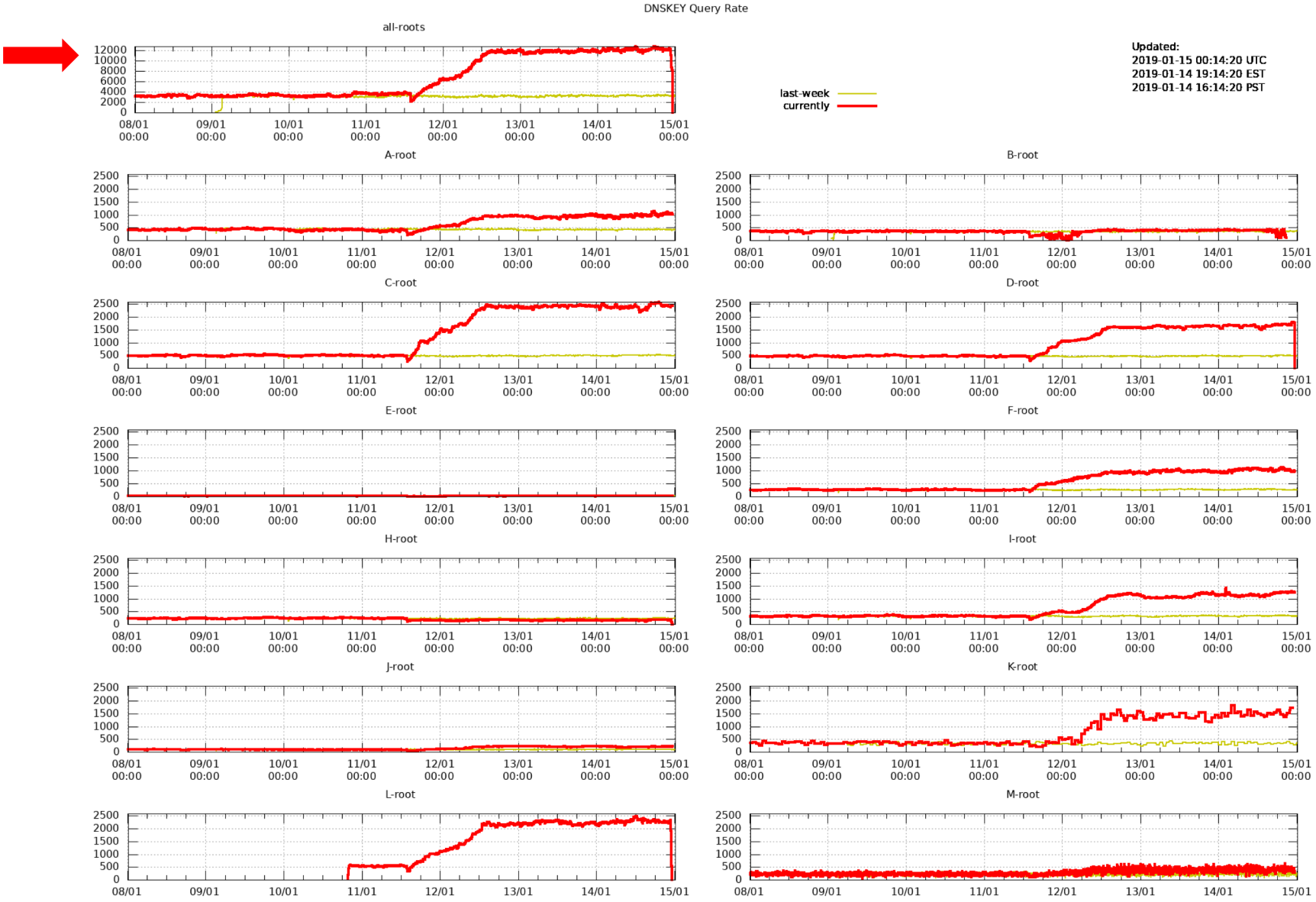


DNSKEY queries (10 January vs. 14 January)

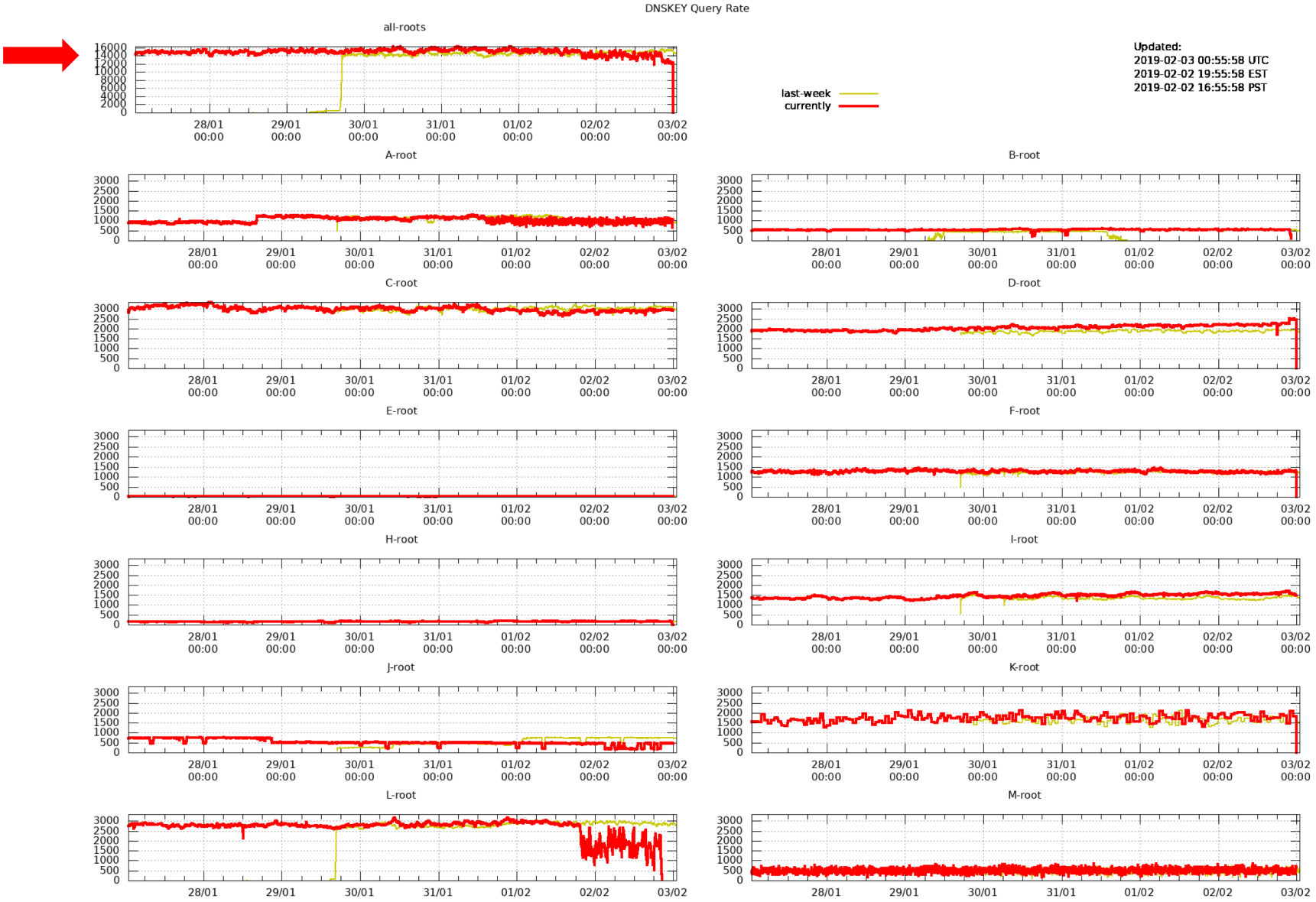


DNSKEY queries (10 January vs. 14 January)

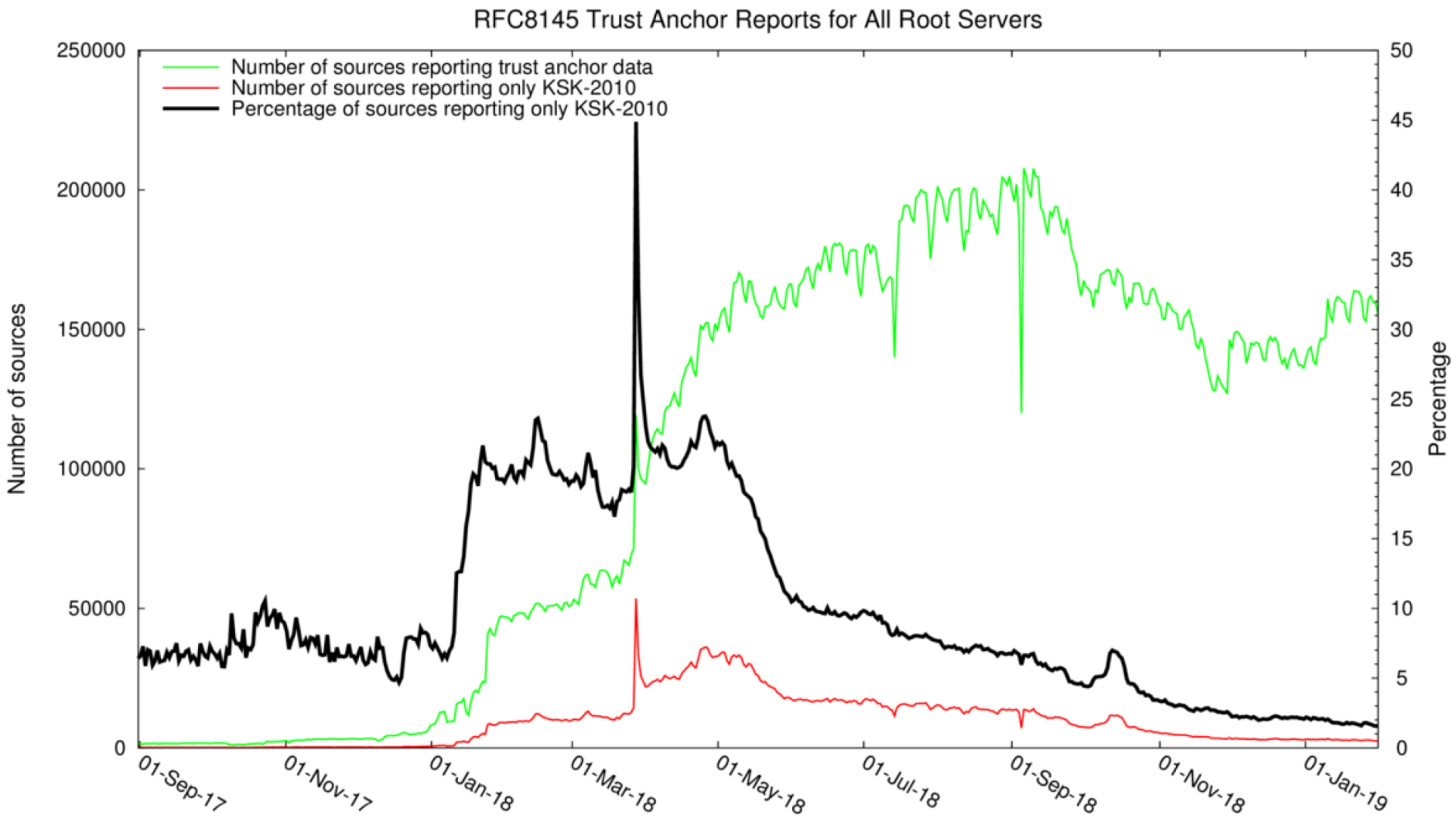
Monitoring: ./IN/DNSKEY queries at the root (48 hours after the revoke)



Monitoring: ./IN/DNSKEY queries at the root (now)



root-trust-anchor-reports.research.icann.org



Upcoming milestones

- Q4 Root KSK Ceremony
  - Signatures are generated in advance that, when published, will revoke KSK-2010 via the RFC 5011 automated update protocol
- 11 January 2019
  - The root zone is published with the RFC 5011 revoke bit set on KSK-2010
- 22 March 2019
  - The root zone is published without KSK-2010 for the first time
  - Only KSK-2017 remains published
- Q3 Root KSK Ceremony
  - KSK-2010 is deleted from the HSMs in the U.S. East Coast Key Management Facility
- Q4 Root KSK Ceremony
  - KSK-2010 is deleted from the HSMs in the U.S. West Coast Key Management Facility

More maintenance is needed

- The community has highlighted the desire to roll the key regularly
  - Extremes are: every three months … only when there is a need.
- The community has highlighted the desire for a standby-key
  - This makes sure that DNSSEC deployment follows RFC5011 spec.
- The community has highlighted the desire for an algorithm rollover
  - We need to know how to do it, in case RSA becomes weak.
- All of the above are related, and each is a significant amount of work.
  - We are listening, tell us your thoughts and join the discussions at

ksk-rollover@icann.org