Joint Meeting:
RSSAC & OCTO

ICANN 63

23 Oct 2018
Barcelona, ES
13:30 – 15:00

Agenda

1. Response to RSSAC questions (David)
2. Root Server Strategy Resolution (David)
3. KSK Rollover: Observations and Future Planning (Matt)
4. RSSAC038 (David)

Questions and Answers

Question 1: In OCTO's interpretation, is the scope of the resolution the root server system as a whole or the IMRS/L-root?

- OCTO's interpretation is that the resolution has two components:
  1. Development of a consensus strategy with the community aimed at reducing the risk to the confidentiality, integrity, and availability of root service due to continued growth/evolution of attacks
  2. Implementation of that strategy for the root server managed by ICANN.
- We (OCTO) believe the intent was to direct staff to work with the community to finalize a strategy to address the increased risk of attack. Since it is not realistic for ICANN org, as the operator of one of the root servers, to alone develop and implement a strategy that would address the increased risk, the Board has asked staff to engage with RSSAC, the root operators, and the rest of the community to develop a strategy aimed at reducing the effects of attacks that would impact root service.
- ICANN org, as a root server operator, can choose to implement that strategy (or not) just like any other root server operator.

Questions and Answers

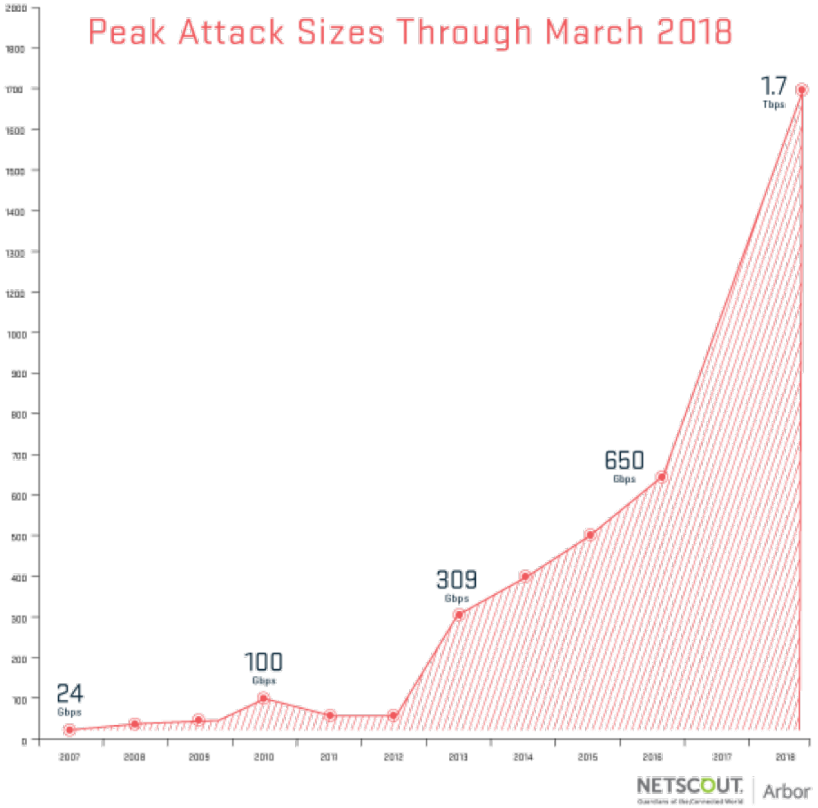
Question 2: There appears to be an inherent conflict between "increase[ing] observation and monitoring of the system as a whole" and a much more distributed "hyper-local root-esque" solution that has been championed by OCTO. There are RSSAC and SSAC statements as well as the CDAR report which provide a clear indication of the need for additional monitoring, and it is certain that any level of monitoring will only get more challenging with a more distributed resolution system. How does OCTO intend to reconcile implementing both and what measures have been taken thus far for each?

- Monitoring the system as a whole does not mean monitoring all queries that might have gone to a root server. Resolver configuration currently allows for functionality such as aggressive NSEC and QNAME minimization and RFC 7706, so increasingly, queries are already not being monitored at the root.
- Given increased interest in privacy in the Internet, the board believes that over time, the monitoring vantage points provided by the root servers will become less effective. In particular, the implementation of query name minimization, TTL stretching, cache pre-fetching, etc. will tend to reduce the effectiveness of monitoring done at the root servers. As such, while increased hyperlocal deployment is likely to impact the ability for monitoring to be done at the root, we must already take into account and prepare for this loss of this visibility into DNS operations.

Questions and Answers

Question 3: Can OCTO explain what research informed the ICANN Board that the "long-term outlook for the traditional approach appears bleak," when this is the current approach?

- The traditional approach of dealing with attacks against the root system has been to increase the number of and bandwidth to root server instances. However, as this approach has non-trivial costs and those costs are and will likely continue to be significantly higher than the costs associated with mounting attacks. In particular, the rate of growth of recent attacks suggests we're seeing exponential growth in attack capacity.



Questions and Answers

Question 4: Can OCTO be more specific on what "new technological advances and methodologies" are envisaged to "enhance existing root server operator practices" that are not occurring organically and require ICANN org shepherding?

- Nothing in the resolution says anything about requiring ICANN org shepherding. For hyperlocal, which has appeared organically, some community members have suggested that it may be appropriate for ICANN org to organize/coordinate a reliable zone availability service, but other organizations could certainly organize parallel reliable services as well.
- In keeping with ICANN's mandate of working to ensure the security and stability of the DNS, ICANN may facilitate deployment of various other technologies being developed within the IETF and elsewhere aimed at addressing confidentiality, integrity, and availability of the DNS, e.g., DNS privacy enhancement, query name minimization, NSEC aggressive use, etc.

Questions and Answers

Question 5: What are the priorities for OCTO in the coming year?

⊙ Not in Order

- Develop implementation plan for RSSAC 37/38
- Studies on DNS abuse using DAAR
- Publishing revised SSR Framework
- Improve engagement with Operational Security Communities
- Produce a plan to implement root server strategy
- Continue work on ITHI
- Transition Open Data to Operations and E&IT
- RZM Studies
- Study Resolver Behavior
- Finish KSK rollover
- Enhance Capacity Building
- BTC Coordination
- Increase/improve Technical Content

Questions and Answers

Question 6: Can OCTO share any internal organizational changes regarding ownership and operation of both the IANA and IMRS?

- Executive ownership of IANA Functions has been temporarily assigned to the CTO during the search for Akram's replacement
  - May or may not be a permanent assignment
- ICANN org's root server strategy has been assigned to OCTO
  - OCTO has "contracted" internally with E&IT's DNS Engineering group to implement that strategy

Agenda

1. Response to RSSAC questions (David)
2. Root Server Strategy Resolution (David)
3. KSK Rollover: Observations and Future Planning (Matt)
4. RSSAC038 (David)

Strawman Plan

Assumption 1: It is permissible for ICANN org as an operator of a root server to propose a strategy to address increased risks of attack against root service.

Assumption 2: It is impossible for ICANN org, by ourselves, to increase the security of the one root server we operate to address the increased risk caused by the growth in attack capacity/modalities.

1. Provide a draft root strategy paper to RSSAC for their review, requesting RSSAC members forward to their respective root operators (as appropriate)
2. After some period of time, revise the paper as a result of input received from RSSAC/root operators
3. Post the paper to the community and initiate a public comment
4. Revise the paper based on input from the public comment
5. Finalize the strategy
6. Develop an implementation plan along with resource requirements for the Board's review.

Agenda

1. Response to RSSAC questions (David)
2. Root Server Strategy Resolution (David)
3. KSK Rollover: Observations and Future Planning (Matt)
4. RSSAC038 (David)

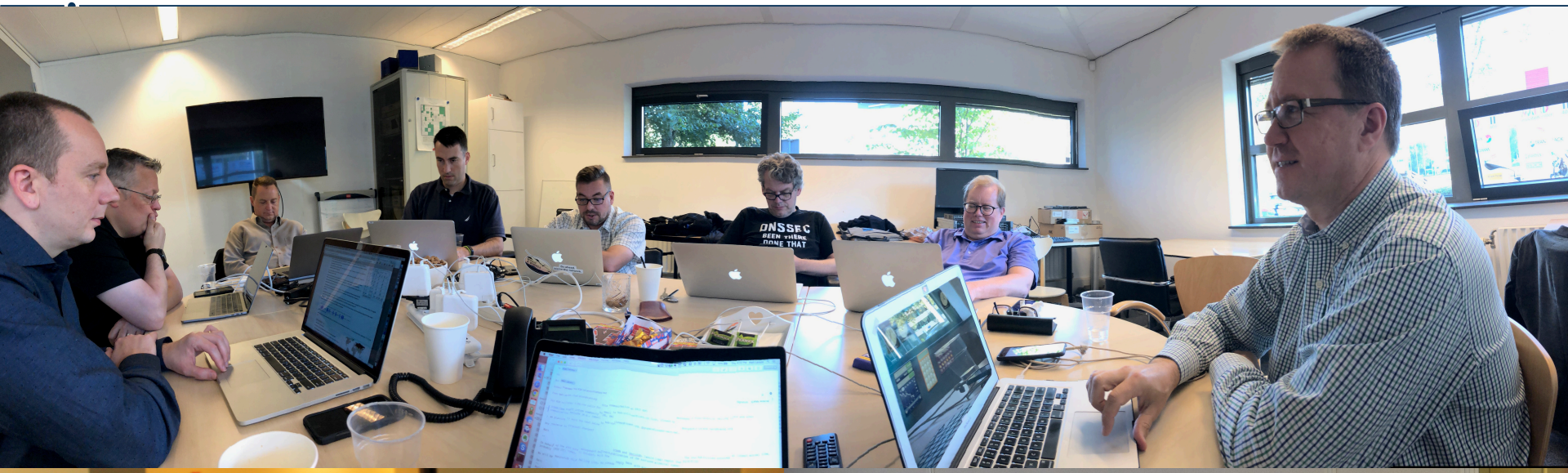
The KSK rollover has happened!

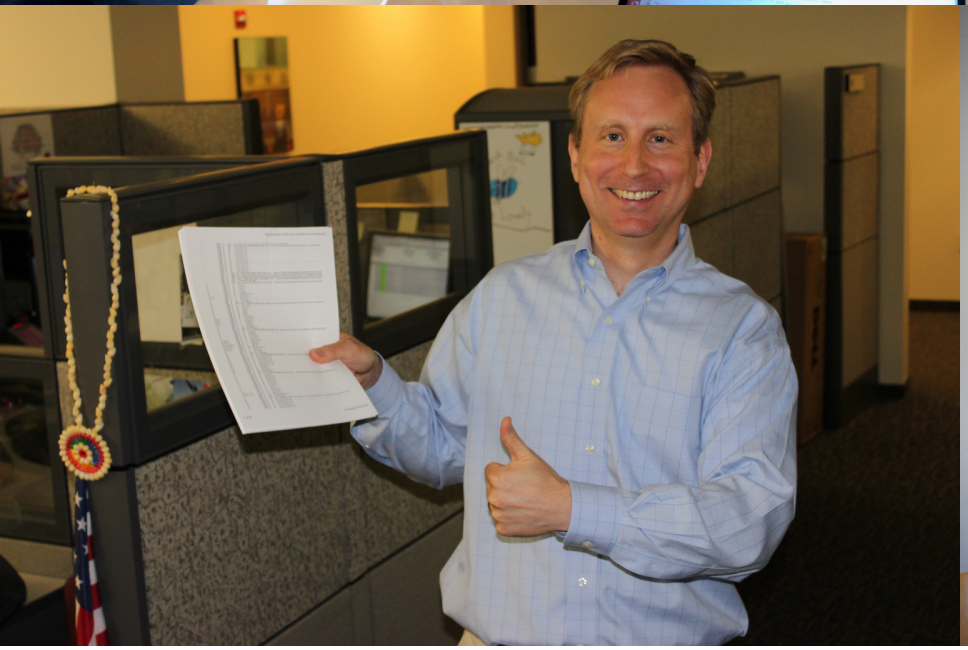
- The KSK rollover occurred on time as planned at 1600 UTC on 11 October 2018 with the publication of a root zone with KSK-2017 signing the root zone DNSKEY RRset for the first time.

Timeline of events (UTC)

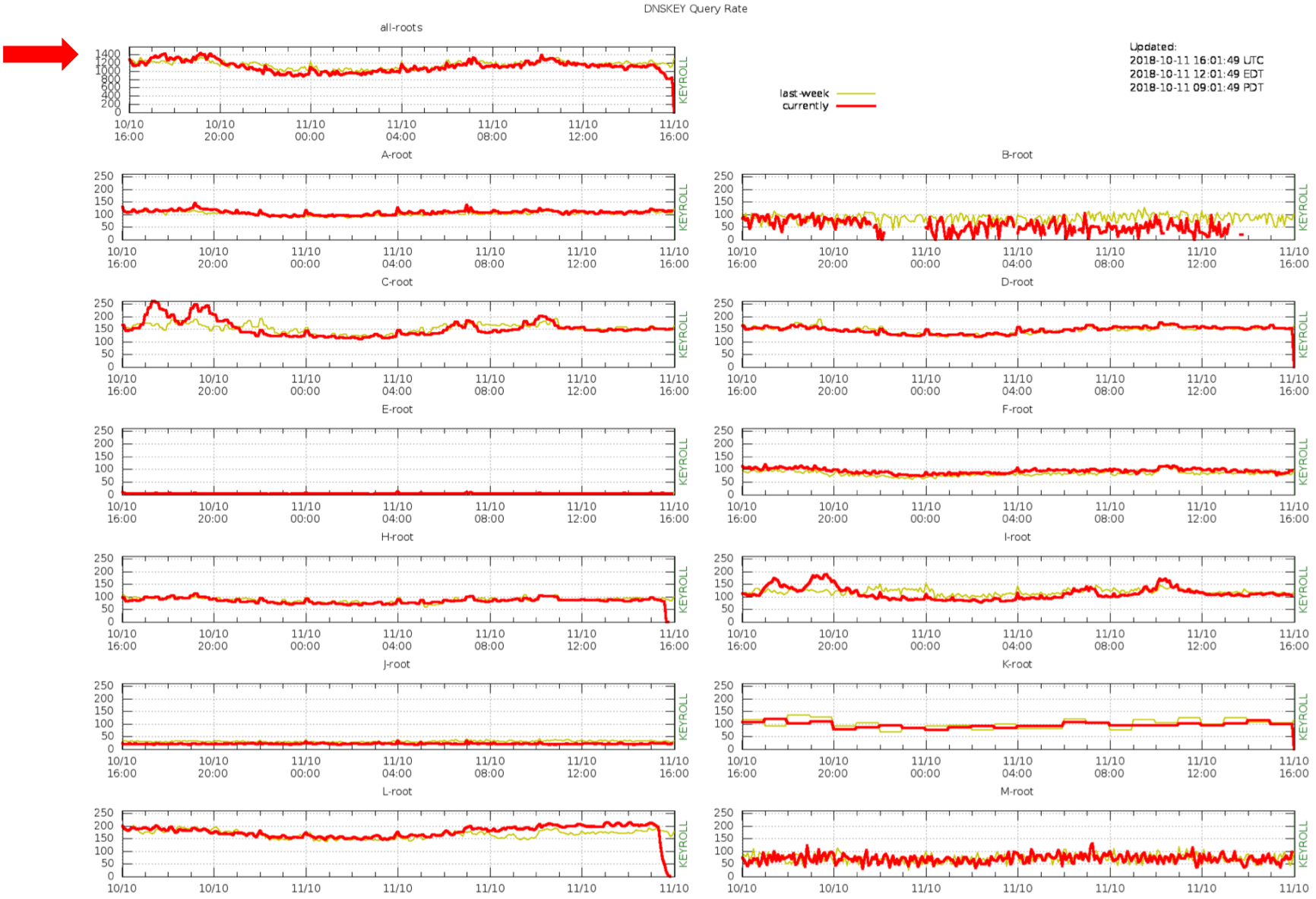
- 13:00 Root Zone Management Partners join conference bridge
- 13:00 Verisign generates root zone file
- 13:15 Verisign inspects root zone file
- 13:30 Verisign sends root zone file to ICANN
- 13:30 ICANN inspects root zone file
- 15:30 ICANN Go/No-go call
- 15:45 ICANN approves the zone for publication
- 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

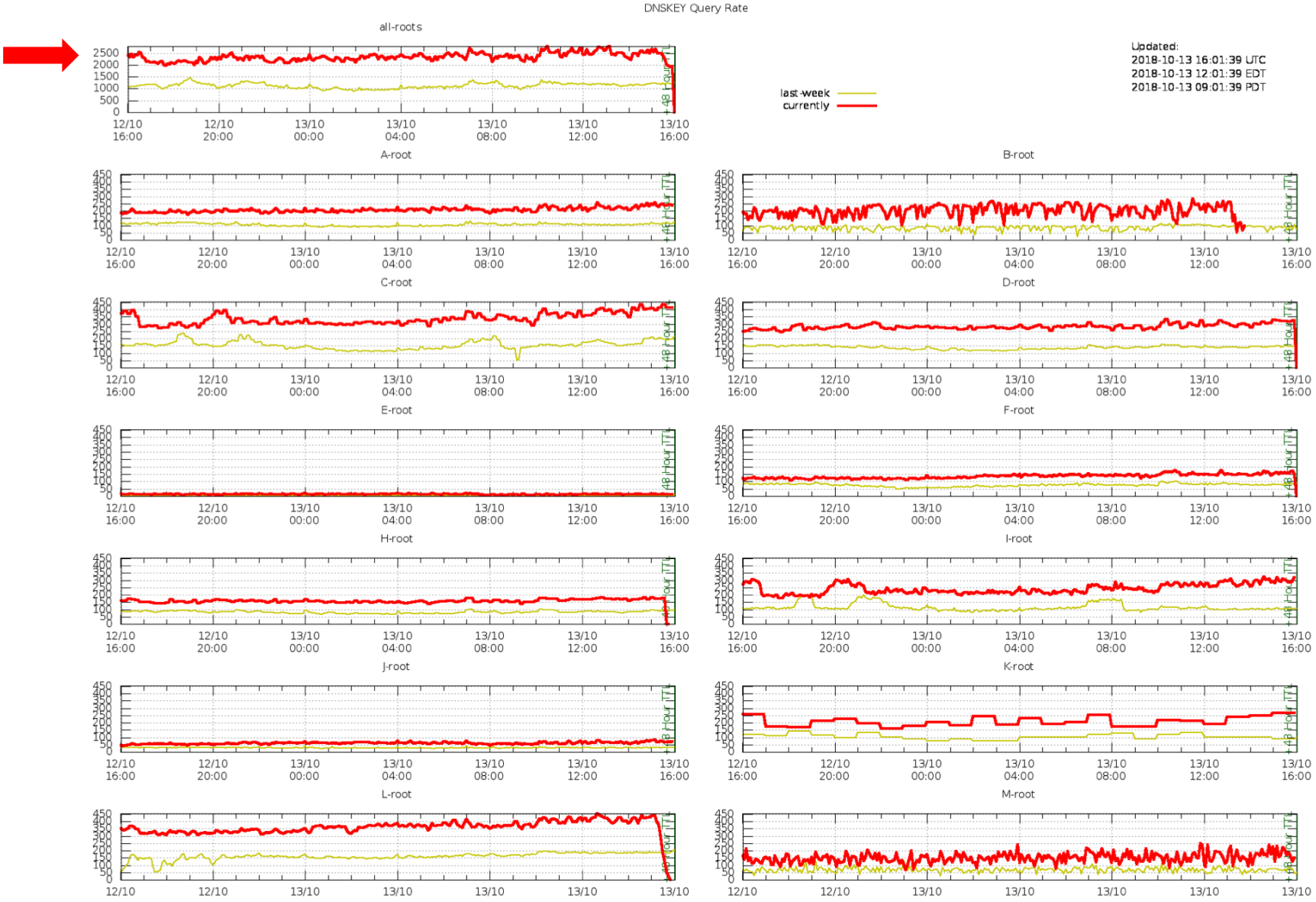




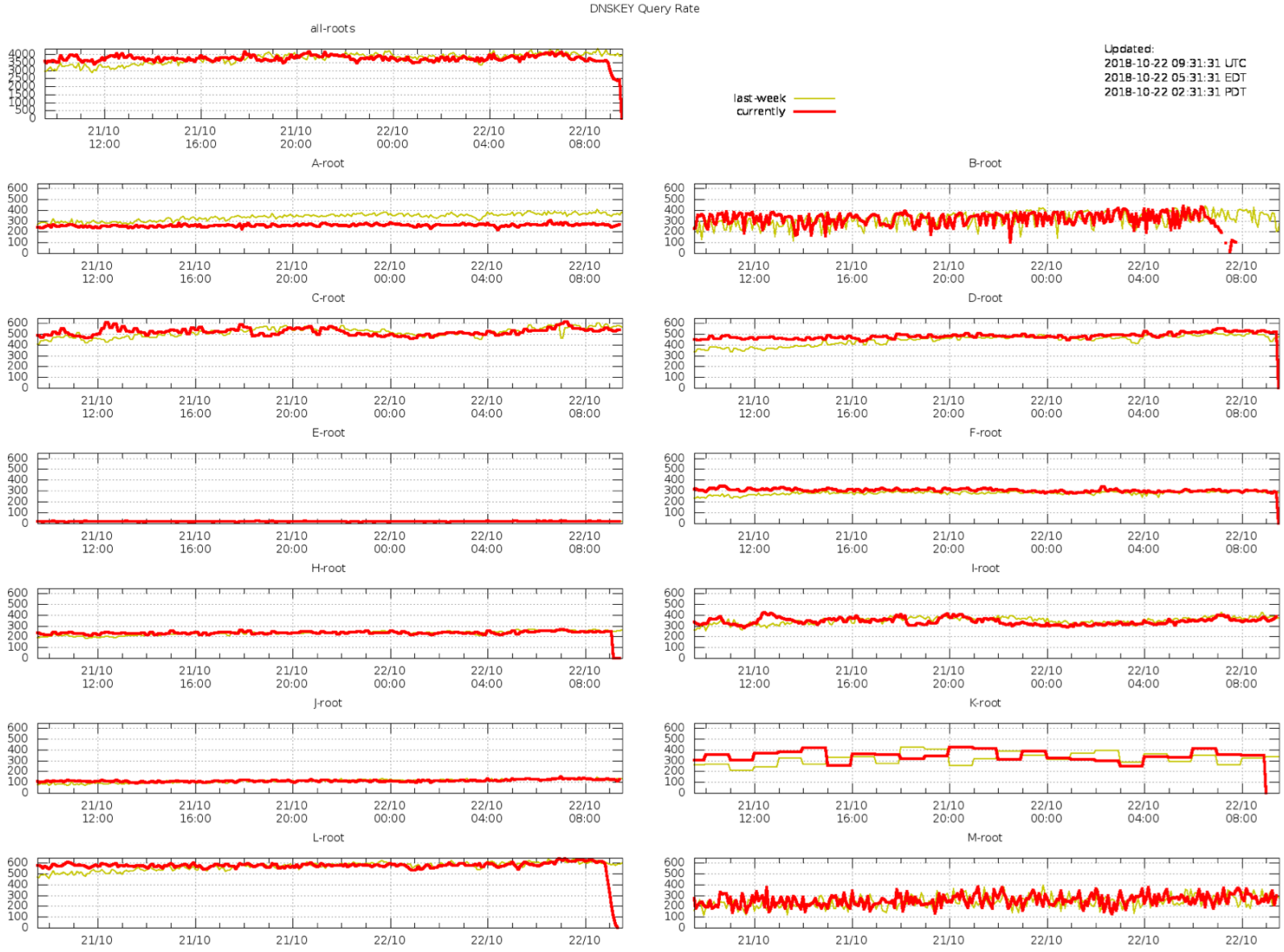
Monitoring: ./IN/DNSKEY queries at the root (just before the roll)



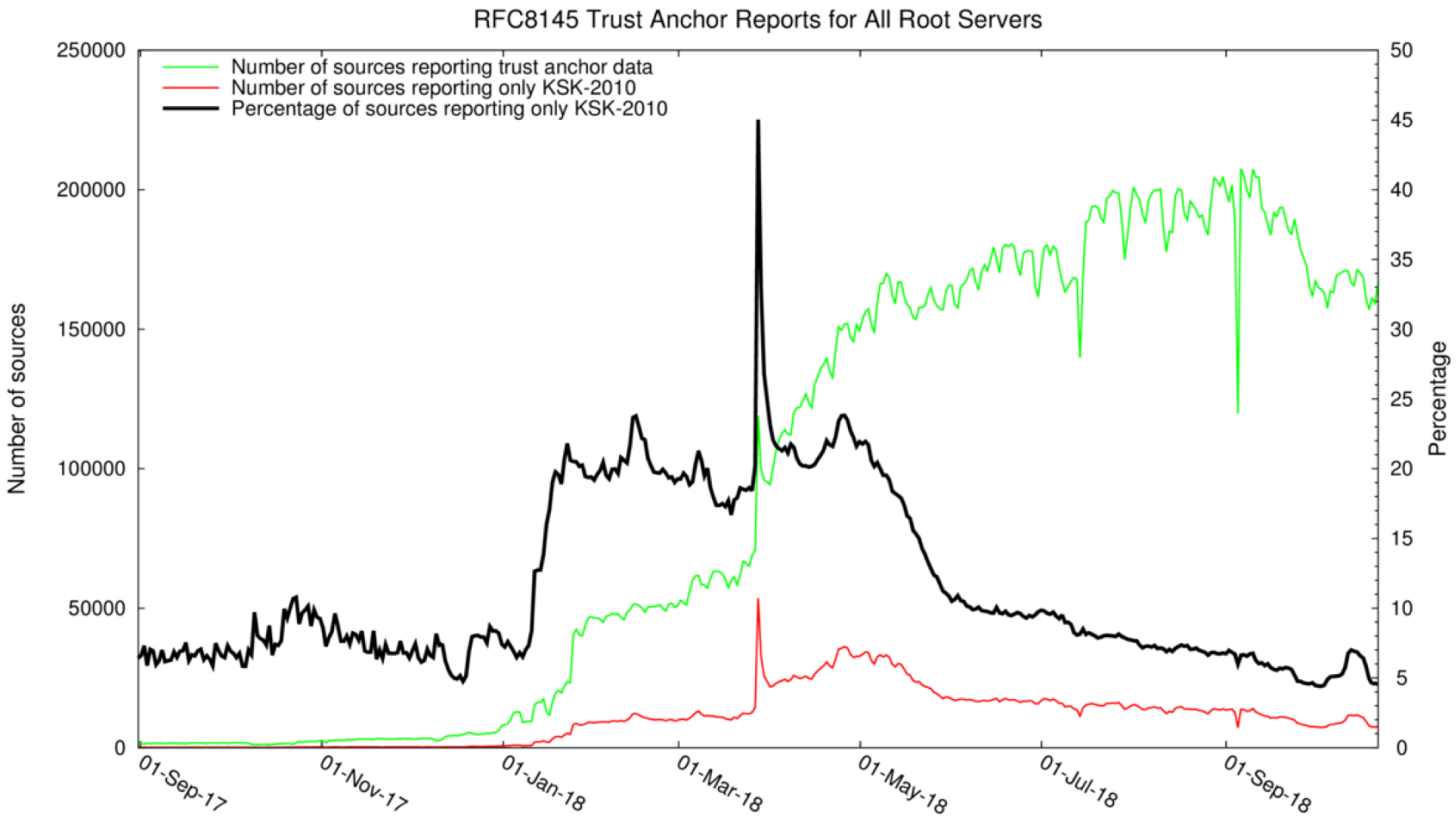
Monitoring: ./IN/DNSKEY queries at the root (48 hours after the roll)



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



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

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

Agenda

1. Response to RSSAC questions (David)
2. Root Server Strategy Resolution (David)
3. KSK Rollover: Observations and Future Planning (Matt)
4. RSSAC038 (David)

Advisory on a proposed governance model for the root server system

- **Recommendation (1):** The RSSAC recommends that the ICANN Board initiate a process to **produce a final version of the Model** for implementation based on RSSAC037.
- **Recommendation (2):** The RSSAC recommends that the ICANN Board refer to RSSAC037, section 5.5.3 to **estimate the costs** of the RSS and developing the Model. Initial efforts should focus on developing a timeline for costing these. The RSSAC estimates the suggested costing effort should not take more than six months.
- **Recommendation (3):** The RSSAC recommends that the ICANN Board and community **implement the final version** of the Model based upon the principles of accountability, transparency, sustainability, and service integrity.

Planning Status

- Identified ICANN org resources / executive sponsorship
  - Team will assess, manage, plan, and track the work associated with Board response to RSSAC038
  - Drafting Advice Roadmap Plan to assess organizational feasibility, using established Board advice process
- Board and RSSAC to continue discussions on RSSAC037 model
  - Board Committee oversight/shepherd to be identified
- Possible future resolution based on ICANN org's assessment:
  - Direct ICANN org to undertake consultations and produce cost estimates
  - Direct ICANN org to seek public comment on Advice Roadmap Plan and process to develop final model