Root KSK Roll Update Webinar

Matt Larson, VP of Research

11 October 2017

Who has KSK-2017 configured as a trust anchor?

- Until recently, there was no way to know which trust anchors validators have configured
- *Signaling Trust Anchor Knowledge in DNS Security Extensions (DNSSEC)* is a recent protocol extension that can provide that information
  - Reports trust anchor key tags via EDNS option or DNS query
  - *draft-ietf-dnsop-edns-key-tag-00* (December 2015)
  - Published as RFC 8145 (April 2017)
- Implementations
  - BIND 9.11 starting with 9.11.0b3 (28 July 2016)
  - BIND 9.10 starting with 9.10.5b1 (11 January 2017)
  - Unbound 1.6.4 (27 June 2017)

  - On by default in BIND, off by default in Unbound

Looking for key tag signaling

- RFC 8145 is so new and validator support so limited that the root KSK roll project team did not expect to get enough data to help with the first root KSK Roll
- Duane Wessels (Verisign) started looking at A & J root traffic in May 2017 for RFC 8145 signaling
- *Presentation from Duane, who joins us today on the webinar*

Further analysis by OCTO Research

- ICANN OCTO Research did an analysis similar to Duane's
  - Analyzed query data from B, D, F and L
  - Combined with Verisign's A & J data
  - For 1 September 2017 through 25 September 2017
- Results:
  - Total number of unique addresses reporting key tag data: **11,692**
  - Total number that only ever reports KSK-2010: **577**
  - **4.93% of reporting validators are not ready for the KSK roll on 11 October 2017**
- Analysis is complicated
  - Dynamic IPs make the situation look worse by inflating true number of sources
  - Forwarders make the situation look better if they obscure multiple validators behind the forwarder
  - BIND reports trust anchors even if not validating

Why do validators report just KSK-2010?

- Multiple reasons suspected or confirmed:
  1. BIND reports trust anchors even if not validating
  2. Old configurations pre-dating automatic update support
     - E.g., BIND's *trusted-keys* instead of *managed-keys* or *dnssec-validation auto*
  3. Bugs in automatic update or key tag signaling support
  4. Operator error
     - E.g., Docker container keeps booting up with only KSK-2010 and starts 5011 all over again
- We always knew old configurations would be an issue but never had objective data until now
- We worried bugs and operator error were possible but didn't have evidence until now
- Analysis is ongoing

Issues and thoughts

- We do not know how representative the set of validators reporting key tag data is compared to the set of all validators
- Validators != end users (or “end systems”), and the impact on end users is what is most important
  - The design team recognized this
- Determining number of end users/systems for a given resolver is hard
  - APNIC’s data will help
  - Query data from TLD or other popular zones would also help
- Mitigation is hard
  - We’ve already had a multi-year campaign to reach operators
  - Implementation-specific problems don’t make the problem easier

What we just announced

- We postponed the root KSK roll until we can gather more information and understand the situation better
- The delay will be at least one quarter
- We have not yet determined how many quarters to delay
- We will at least partially mitigate

Next steps: you can help

- Please work with us to identify and investigate sources reporting only KSK-2010
  - We will publish the list of autonomous systems with sources publicly
  - Want to track down as many as possible to understand behavior
    - Old configuration, bug, operator error, something else?
- If you run a resolver that forwards, please start logging RFC 8145 queries
  - We want to talk with you
- Please help us as we reduce the number of sources reporting only KSK-2010
  - We recognize not all validators are equal
- We have already been working with vendors to get issues addressed
  - If you are familiar with a 5011 or 8145 implementation, please look carefully at that code for edge cases

Engage with ICANN – Thank You and Questions

One World, One Internet

Visit us at **icann.org**

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

slideshare/icannpresentations

soundcloud/icann