# A Look at RFC 8145 Trust Anchor Signaling for the 2017 KSK Rollover – The Good Parts

ICANN 60 DNSSEC Workshop

Duane Wessels

November 1, 2017

# RFC 8145 -- Signaling Trust Anchor Knowledge in DNS Security Extensions (DNSSEC)

# RFC 8145 – Key Tag Signaling

- Validators periodically report trust anchor key tags.
- What's a key tag?
  - A 16-bit integer that identifies and enables efficient selection of DNSSEC public keys. Much like a ones' complement checksum.
  - 19036 – key tag for KSK-2010
  - 20326 – key tag for KSK-2017
- Reported to a zone's authoritative name servers.
- Should be transmitted about as frequently as DNSKEY expire.

# Two Forms of Key Tag Signaling

- edns-key-tag option.
  - An appended option code in the ENDS0 / OPT record
- Separate key tag query.
- Key tag encoded in query name, using hexadecimal representation.
  - 19036 = hex 4a5c
  - 20326 = hex 4f66

# Timeline & Implementations

| When | What |
|---|---|
| 2015 December | draft-ietf-dnsop-edns-key-tag-00 |
| 2016 July | First implementation in BIND |
| 2017 February | draft-ietf-dnsop-edns-key-tag-05 |
| 2017 April | RFC 8145 |
| 2017 April | First implementation in Unbound |
| 2017 May | Start collecting data |

BIND: ‘trust-anchor-telemetry’ defaults to ‘yes’

Unbound: initially ‘trust-anchor-signaling’ defaults to ‘no’, changed to ‘yes’ around October 1, 2017

# Data

# Data Sources

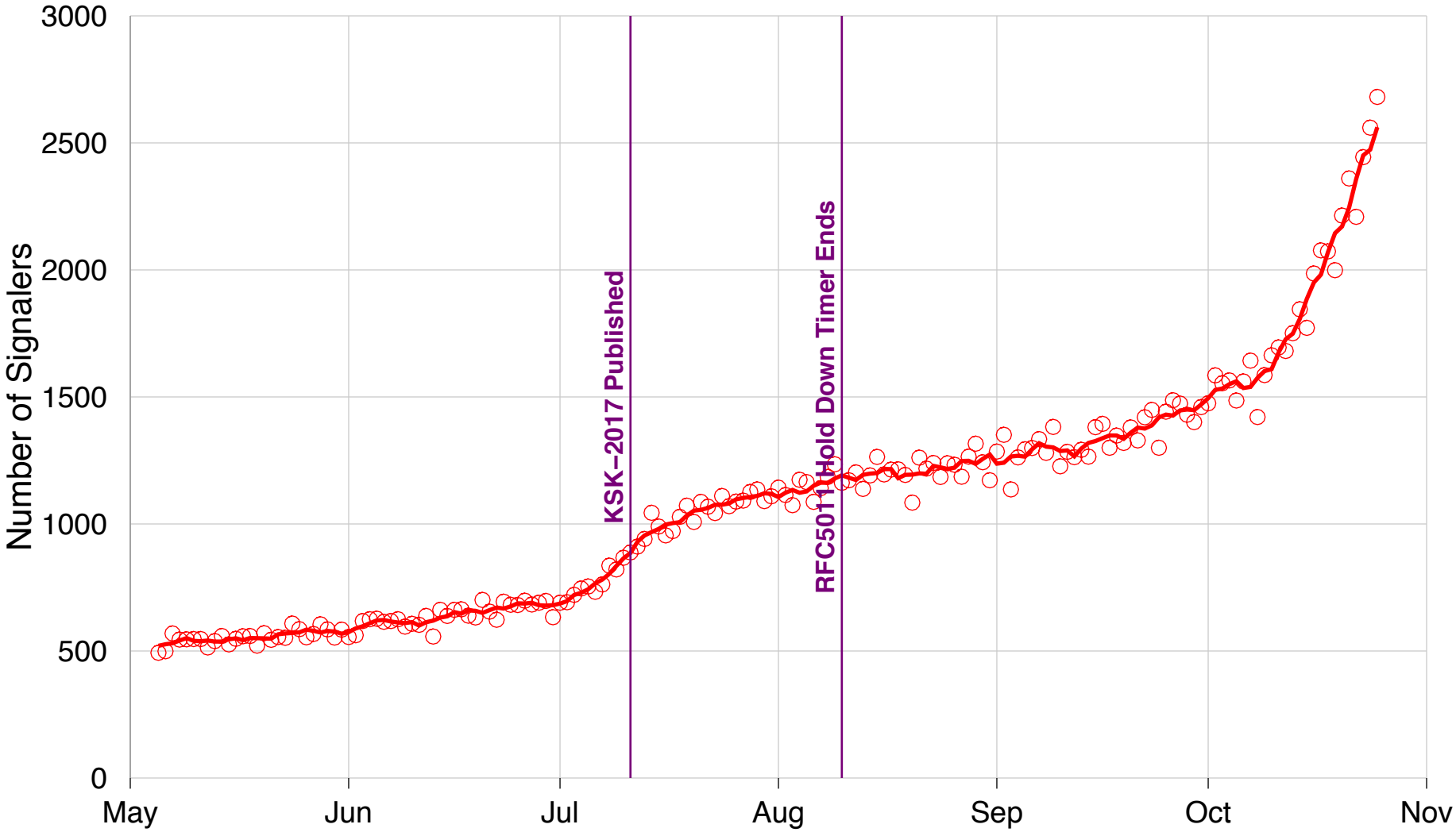
- Key Tag signals are sent to the name servers authoritative for the key they represent.
- In this case, the root zone.
- This data comes from A-root and J-root.
- Selection bias caveat: data provided by only relatively recent implementations.

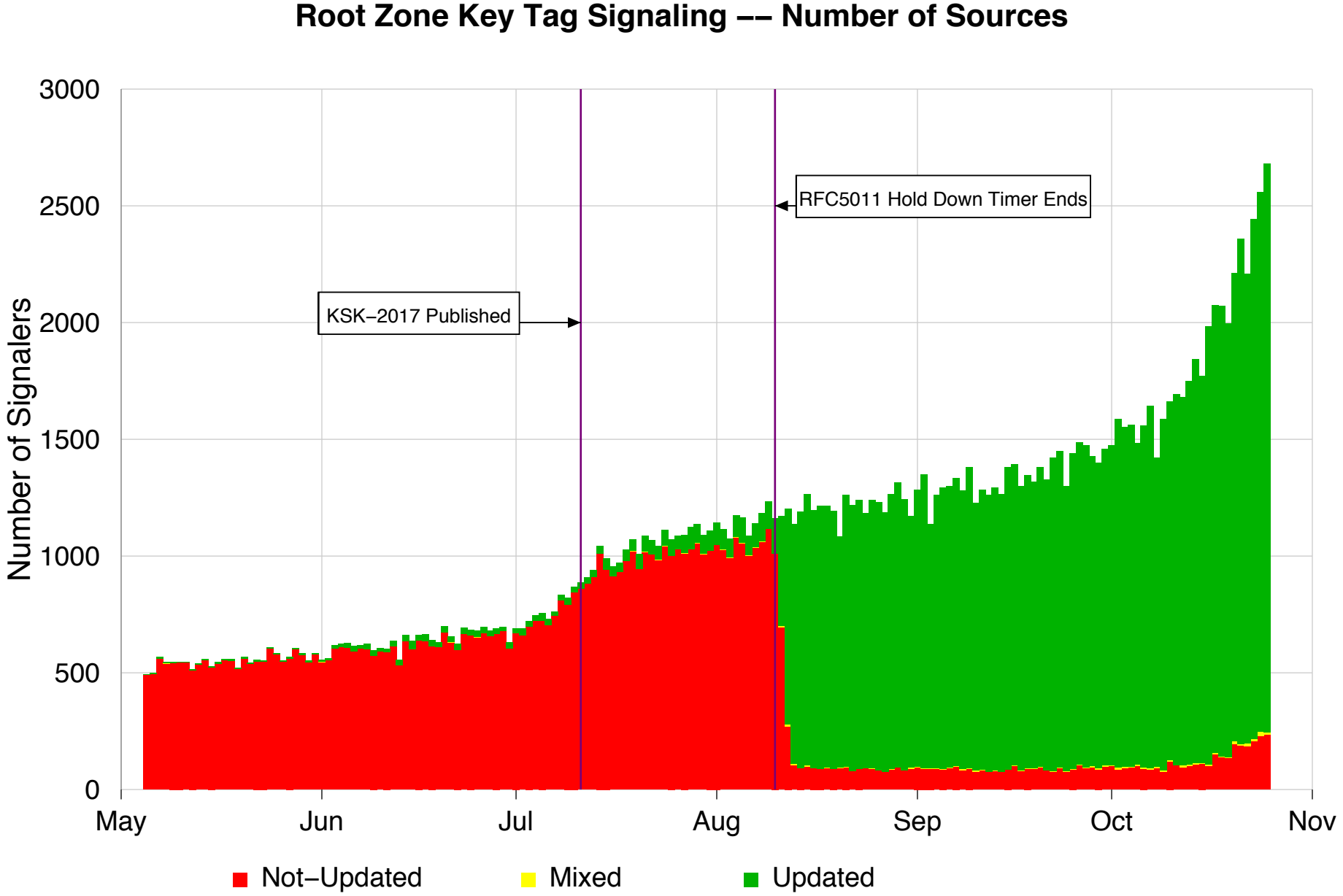
# Data Sample

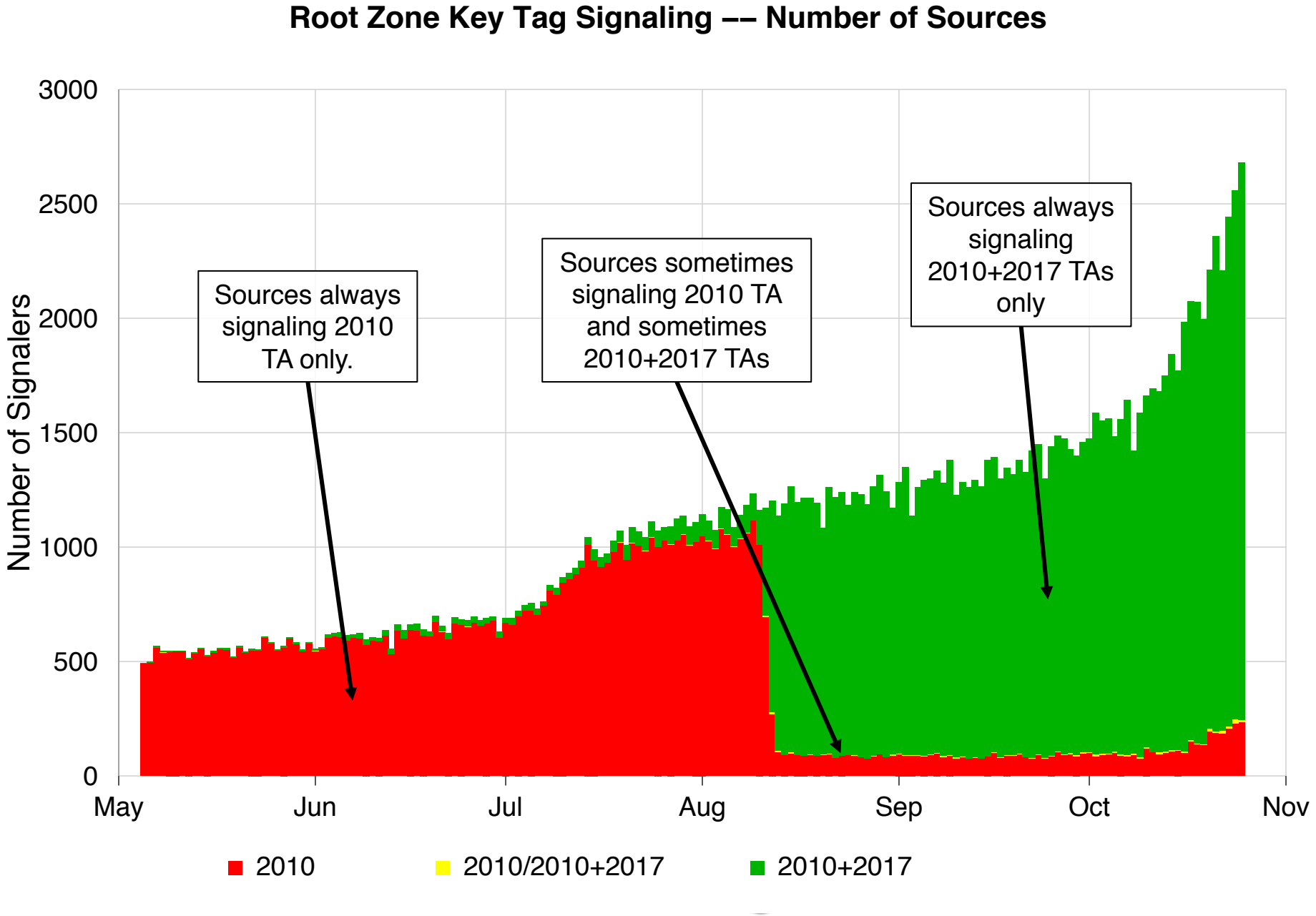
```
SELECT `timestamp`,lower(qname),dstip,srcip,year,month,day
FROM some_hadoop_hive_table
WHERE lower(qname) rlike '^_ta-'
AND qtype = 10
AND product = 'root';
```

```
1500479443  _ta-4a5c       128.x.x.x    192.58.128.30        2017 7 19
1500439539  _ta-4a5c       2a00:x:x::x  2001:503:ba3e::2:30  2017 7 19
1500476401  _ta-4a5c       2001:x:x::x  2001:503:c27::2:30   2017 7 19
1500476401  _ta-4a5c       2001:x:x::x  2001:503:c27::2:30   2017 7 19
1500495841  _ta-4a5c-4f66  188.x.x.x    198.41.0.4           2017 7 19
1500464521  _ta-4a5c       5.x.x.x      192.58.128.30        2017 7 19
1500476401  _ta-4a5c       2001:x:x::x  2001:503:c27::2:30   2017 7 19
1500476401  _ta-4a5c       194.x.x.x    198.41.0.4           2017 7 19
1500476401  _ta-4a5c       2001:x:x::x  2001:503:c27::2:30   2017 7 19
1500476401  _ta-4a5c       194.x.x.x    198.41.0.4           2017 7 19
1500495841  _ta-4a5c-4f66  188.x.x.x    198.41.0.4           2017 7 19
```

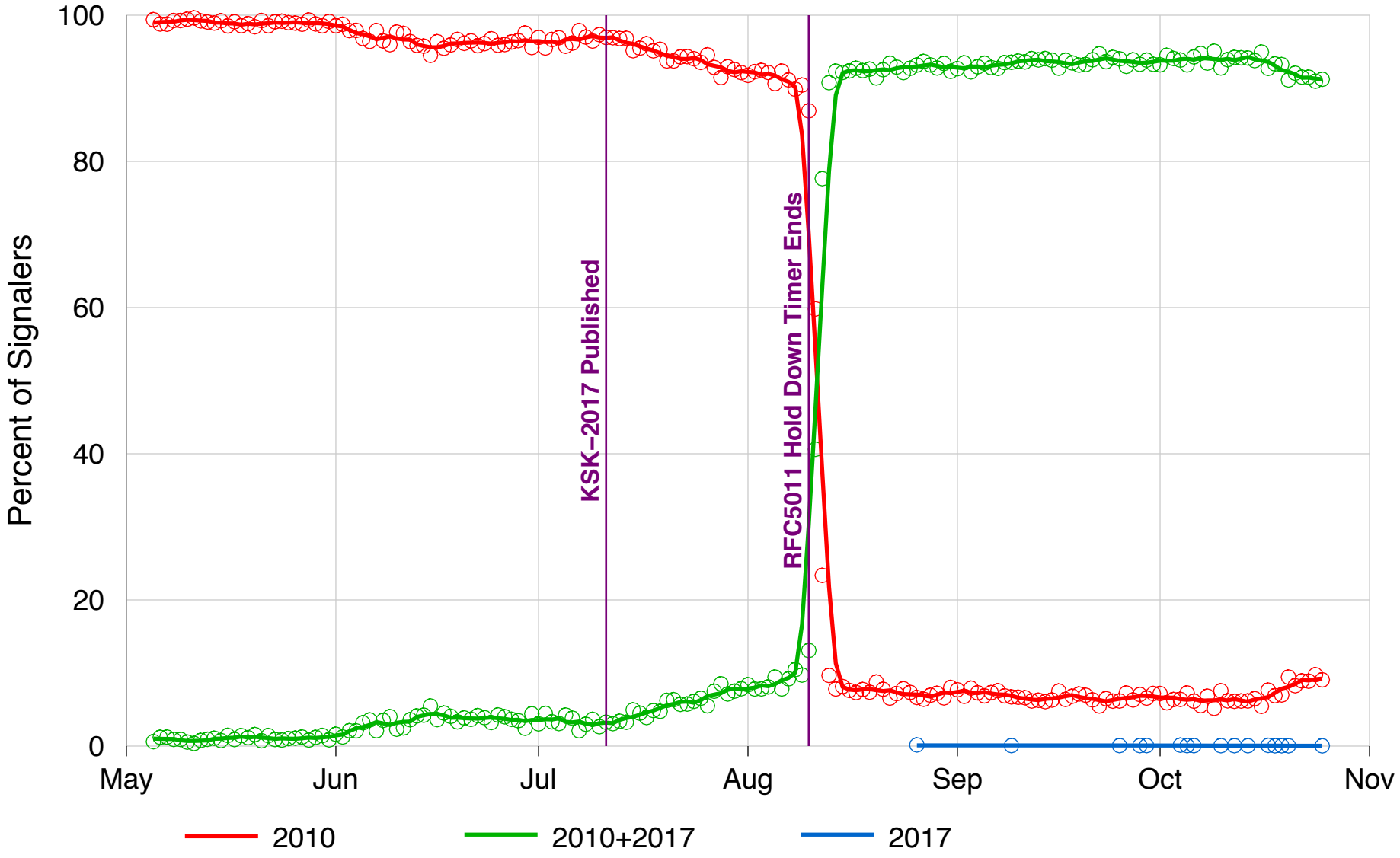
# Root Zone Key Tag Signaling –– Number of Sources




Root Zone Key Tag Signaling –– Number of Sources
Number of Signalers
3000
2500
2000
1500
1000
500
0
May
Jun
Jul
Aug
Sep
Oct
Nov
KSK–2017 Published
RFC5011 Hold Down Timer Ends
Not–Updated
Mixed
Updated


Root Zone Key Tag Signaling –– Number of Sources
Number of Signalers
3000
2500
2000
1500
1000
500
0
May
Jun
Jul
Aug
Sep
Oct
Nov
Sources always signaling 2010 TA only.
Sources sometimes signaling 2010 TA and sometimes 2010+2017 TAs
Sources always signaling 2010+2017 TAs only
2010
2010/2010+2017
2010+2017

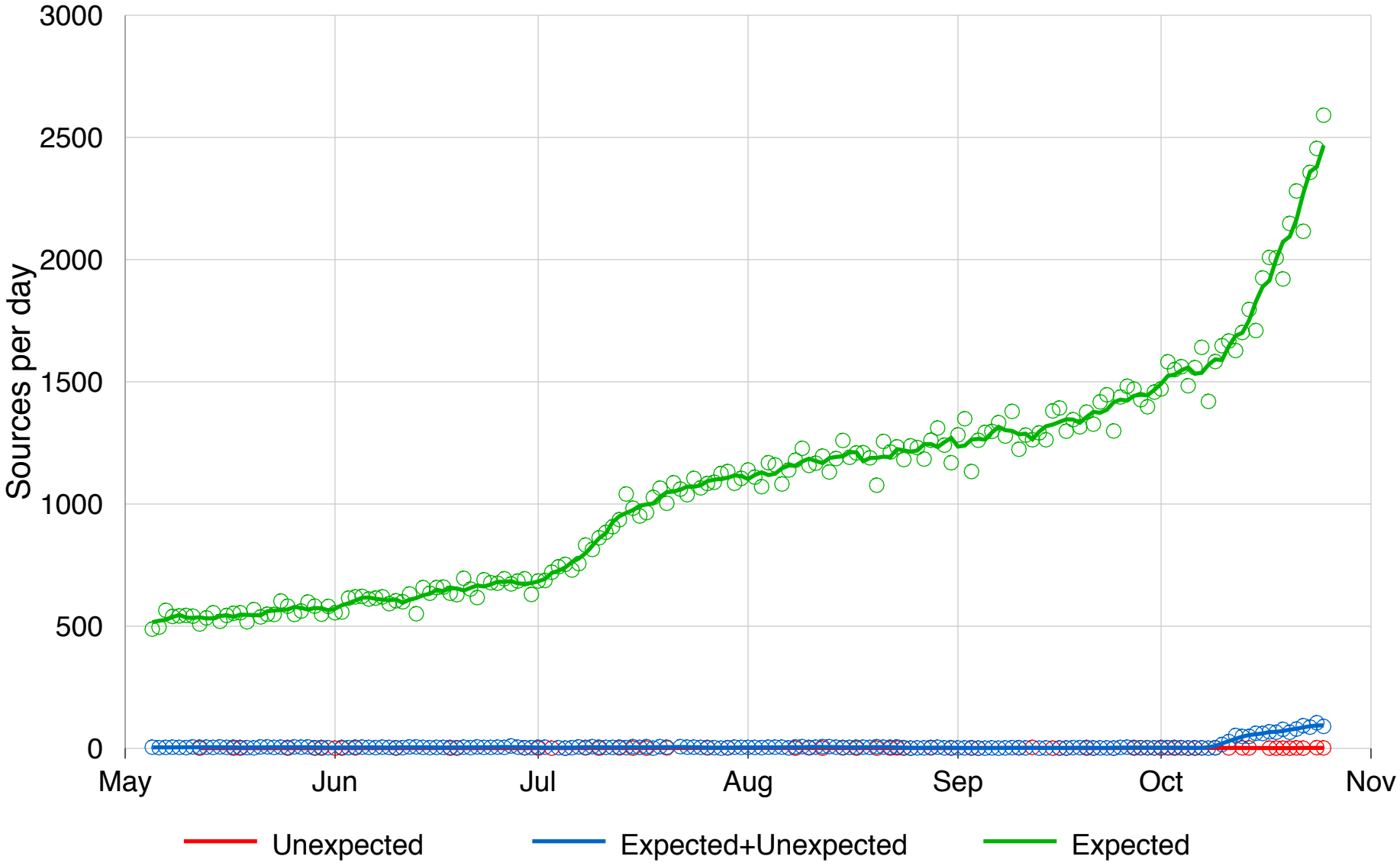
# Root Zone Key Tag Signaling –– TA Update Evidence



# Non-IANA Key Tags

- How often do we see ”unexpected” key tags?
- Observed ~~19~~ 29 key tags for root other than 19036 and 20326.
- From less than ~~10~~ 100 distinct source IPs per day.

# Root Zone Key Tag Signaling –– Unexpected Key Tags



# Conclusions

- Signals from BIND (and Unbound?) appear to be of reasonably good quality.
- NATs, forwarding, dynamic IPs, and partial views complicate analysis.
- Something strange with new signalers on Oct 10.

- ISC, Thank you!
- NLnet Labs, thanks for changing trust-anchor-signaling to ‘yes’ by default.
- Other vendors, please consider implementing RFC 8145.

powered by

VERISIGN™