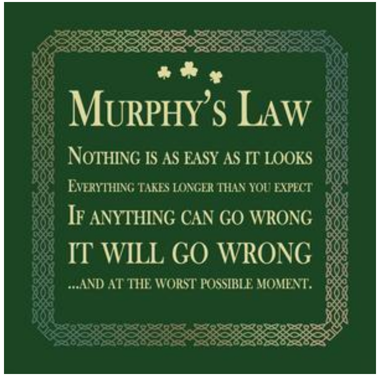
DNSKEY Flood - What does it tell us about resolvers?

Ray Bellis
Olafur Gudmundsson
Vasco Asturiano

Motivation for this Research

- Concerns prior to the roll-over
  - Will resolvers cope? (RFC 5011 timing)
  - Packet Size issues
- Do different resolvers behave differently?
  - Different vendors’ implementations
  - Different versions from the same vendor
    - Derivatives thereof
  - Configuration options
- Accuracy of RFC 8145 signalling from different operational models?
  - E.g. local forwarders / proxies / ALGs, ISP forwarders



Murphy’s Law

Nothing is as easy as it looks

Everything takes longer than you expect

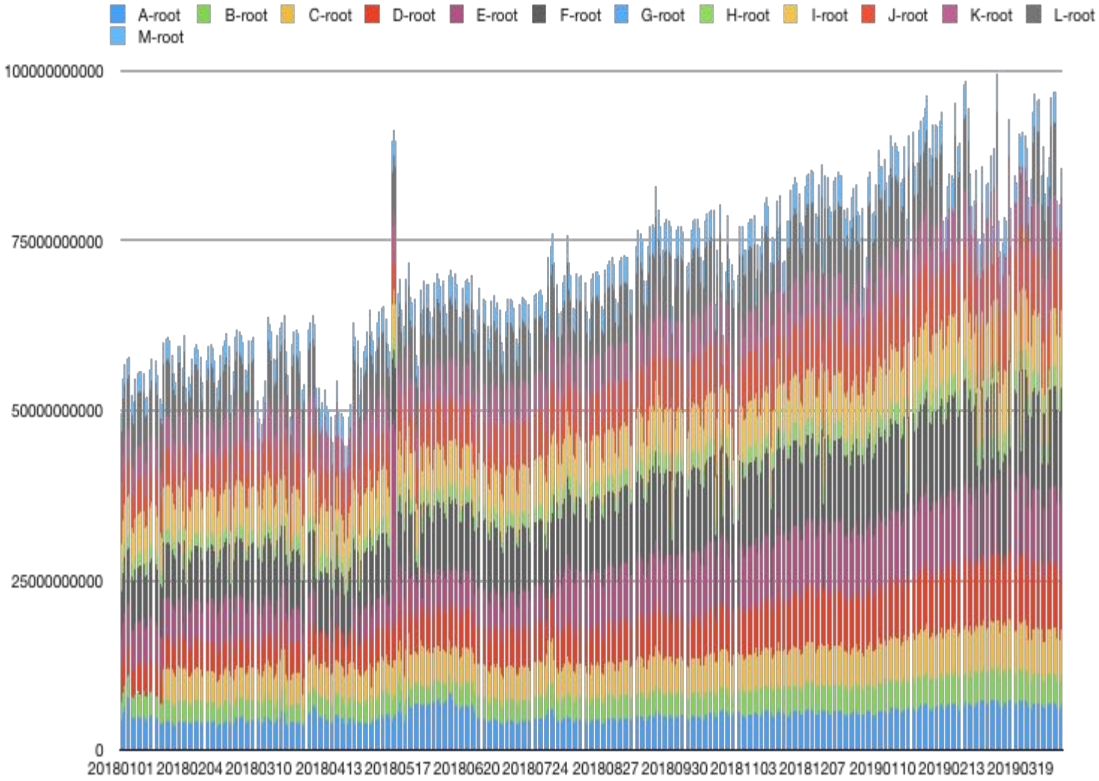
If anything can go wrong

IT WILL GO WRONG

...AND AT THE WORST POSSIBLE MOMENT.

Data sources:

- F-root and E-root aggregate traffic seen by Cloudflare
- Root traffic statistics (RSSAC002)
  - **50%**+ query growth 2018/Jan - 2019/Apr
  - More than **1 Mqps**
- ICANN OCTO _ta signal reports (RFC 8145)



RFC 8145 Reporting

- ICANN OCTO published **daily** summary data on received telemetry
- Two different formats were used
    - Phase 1 format somewhat verbose and included records for all Key IDs
    - Phase 2 format only provided ASN and IP address, and only for addresses still reporting the old Key ID
        - One record per IP address, no counts included

Phase 1 format report - single IP address

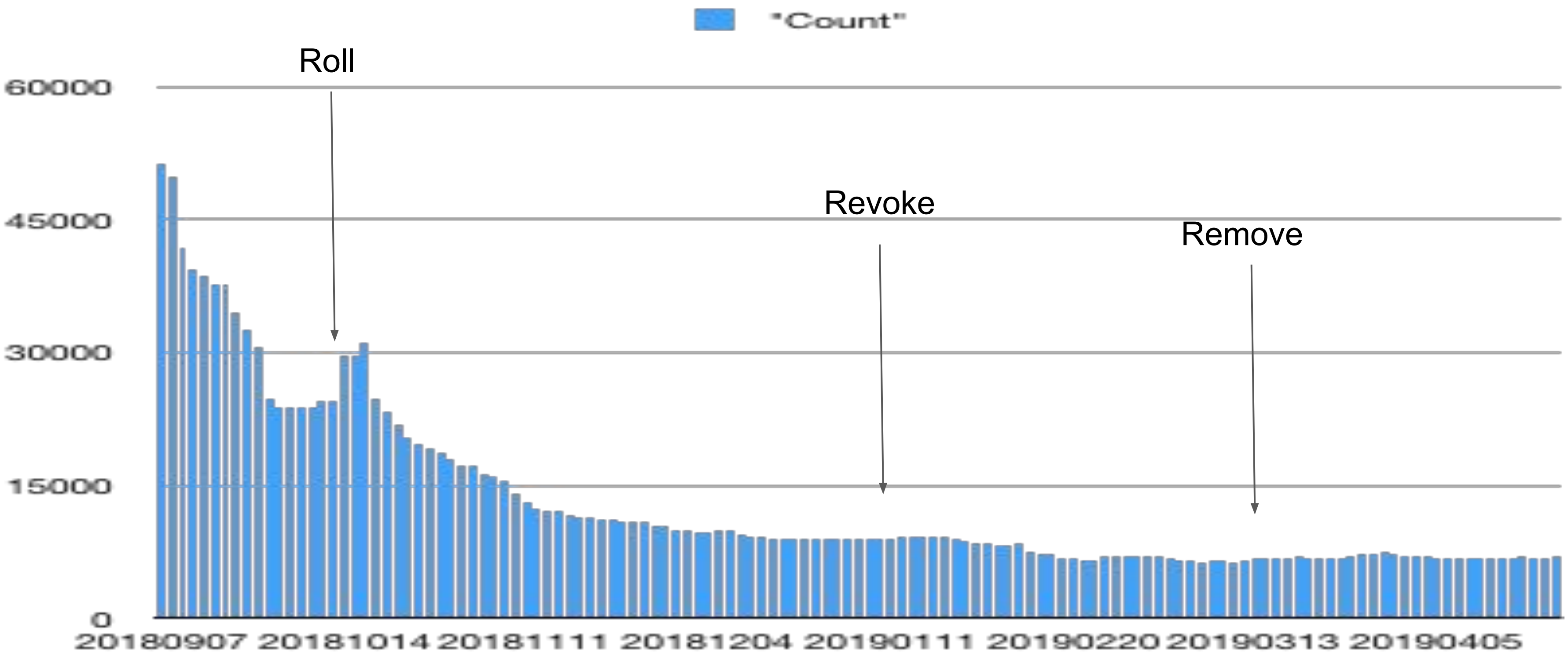
Date	**Address**	**ASN**	**30 Day Count**	**Saw Both Keys**	**Spamhaus PBL**
2018-06-01	210.94.72.x	9318	27	**False**	True
2018-06-03	210.94.72.x	9318	27	**True**	True
2018-06-04	210.94.72.x	9318	27	**False**	True
2018-06-10	210.94.72.x	9318	27	**True**	True
2018-06-11	210.94.72.x	9318	27	**True**	True
2018-06-13	210.94.72.x	9318	27	**False**	True
2018-06-18	210.94.72.x	9318	27	**False**	True

Interpretation of that Data

- AS9318 is SK Broadband, Korea
- Count of 27: shows up all the time ⇒ **ISP Resolver**
- Both keys seen - flipping between True and False

  ⇒ it is *forwarding* **`_ta`** signal from other resolvers (possibly end users)
- Conclusion: Lots of noise, hard to draw conclusions

Phase 2 data - Unique addresses per day (KSK-2010)



Roll

Revoke

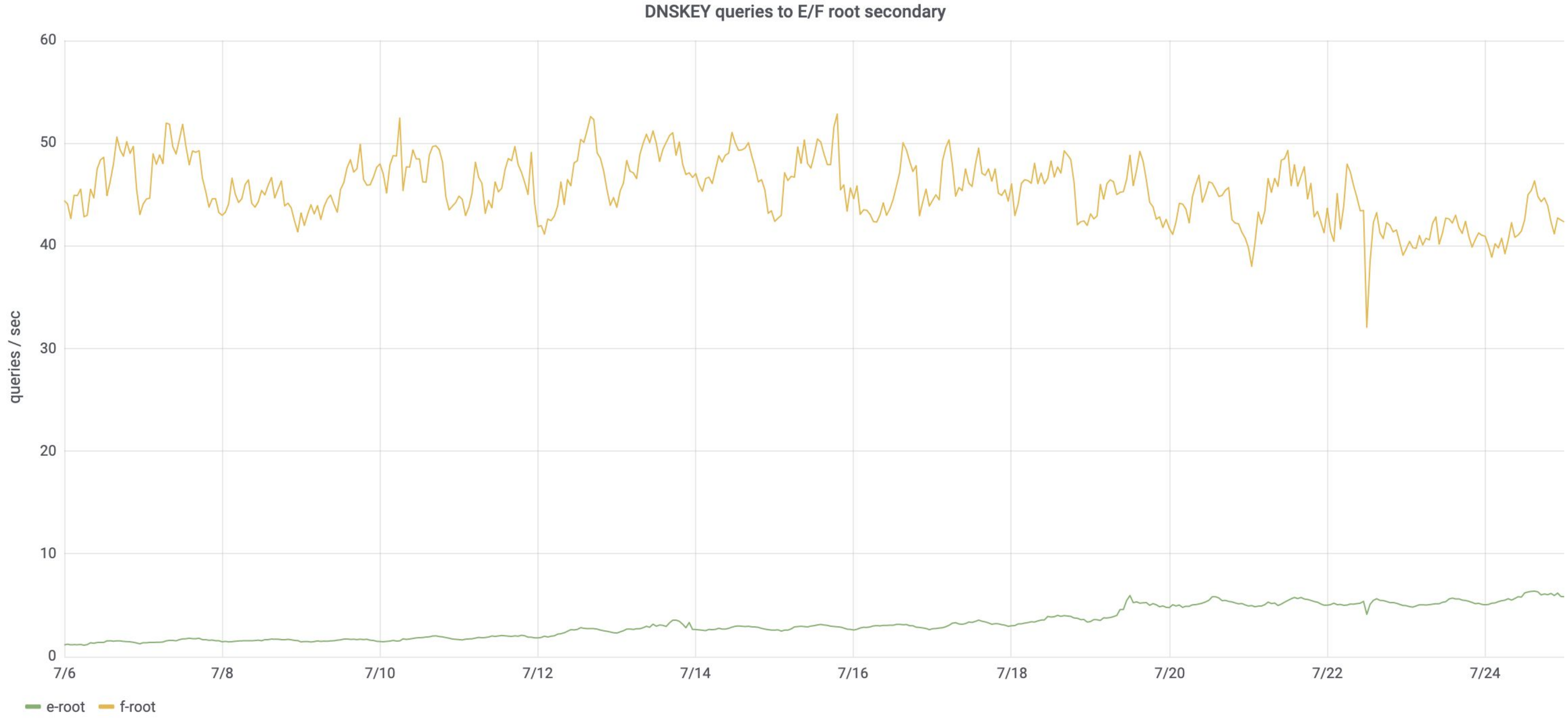
Remove

Summary on _ta signal

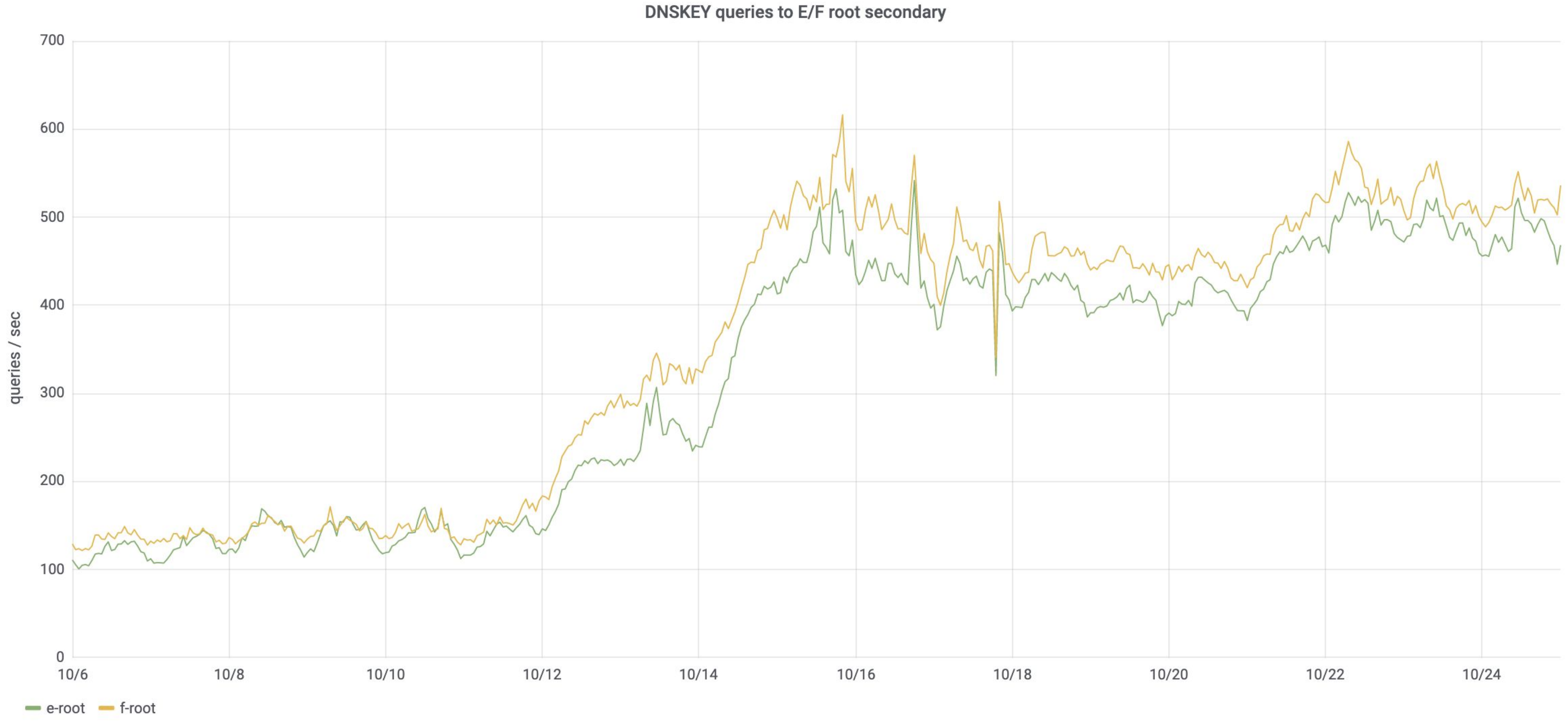
- Mostly Noise:
  - Known-good ISP resolvers sending “bad” signals
    - actual system is masked by resolver
- No signal from sites with Local Root / RFC 7706
- Not all Root Server instances represented
- No way to correlate IPv4 and IPv6 reports from the same instance
- Some ASNs contain a large number of sporadic reporters
  - Cloud computing instances spin up and down repeatedly (perhaps on different addresses)
  - Cellular and broadband connections may have unstable addresses
  - Carrier Grade NAT

DNSKEY Traffic Observations

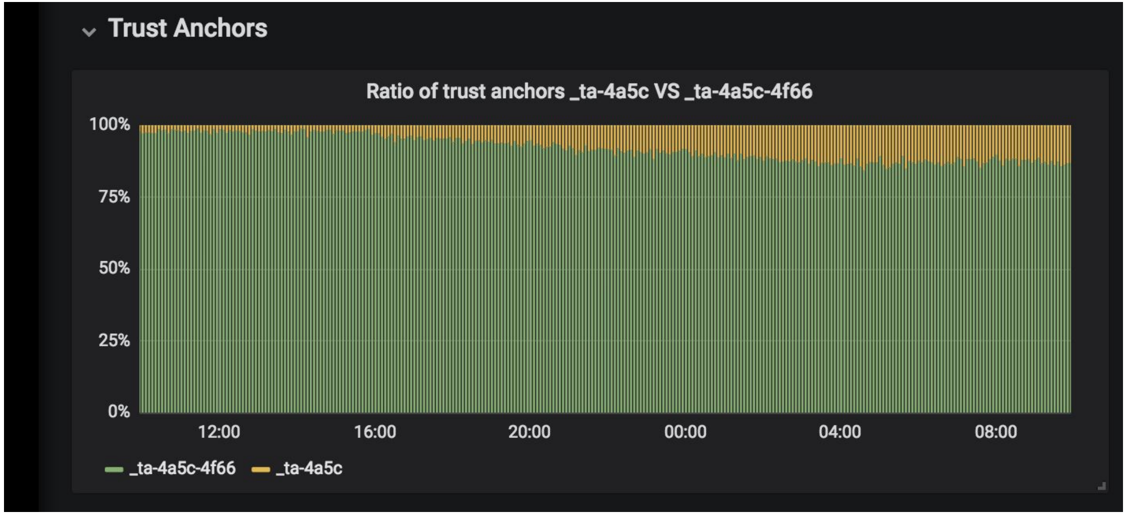
2017-07-11: KSK-2017 added



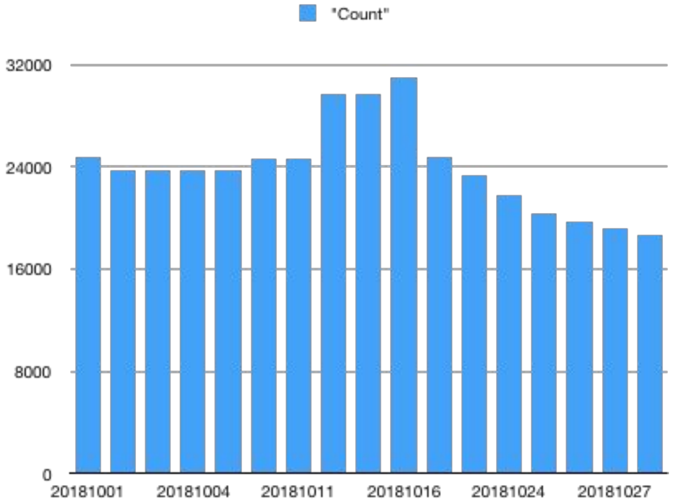
2018-10-11: KSK-2017 takes over



What about _ta Signal:

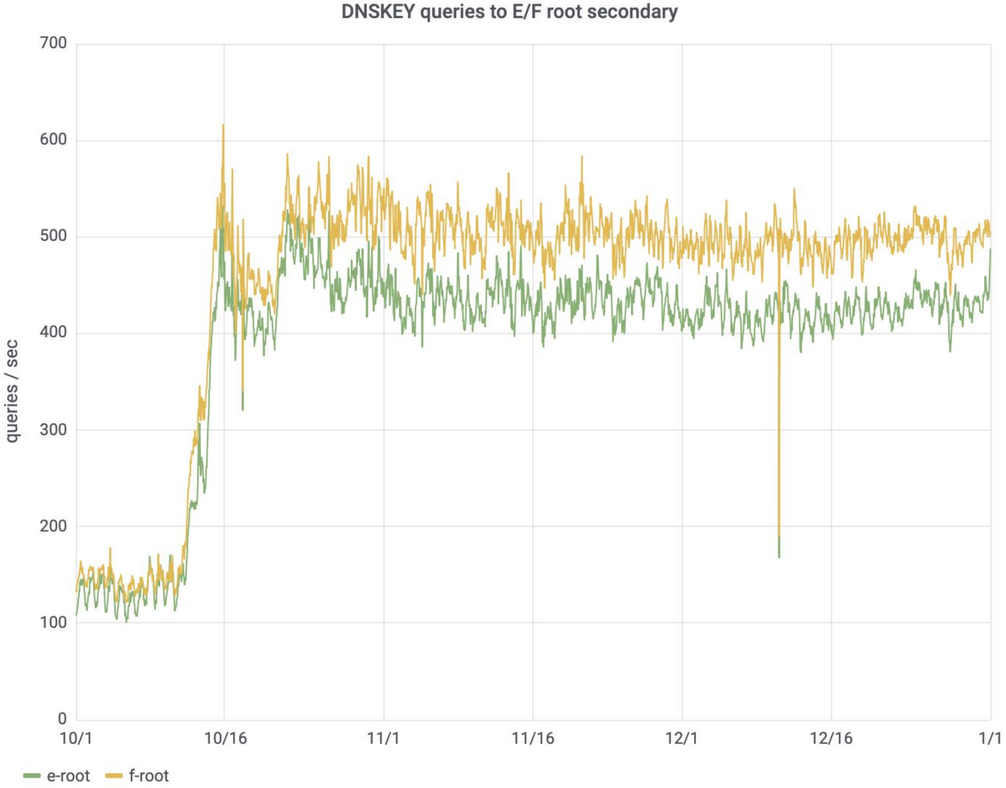


Increase in <KSK2010 Only>
⇒ indicates some resolvers are having problems



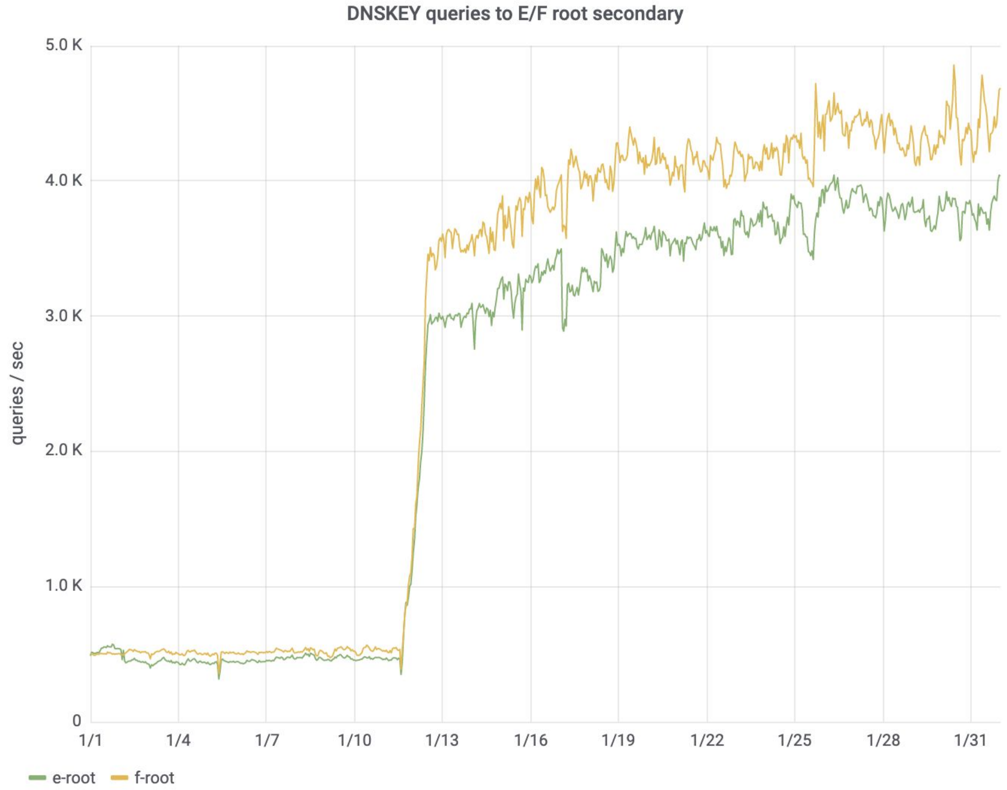
Medium Term Impact

- 3x increase in DNSKEY queries
- Unexpected, but not operationally concerning



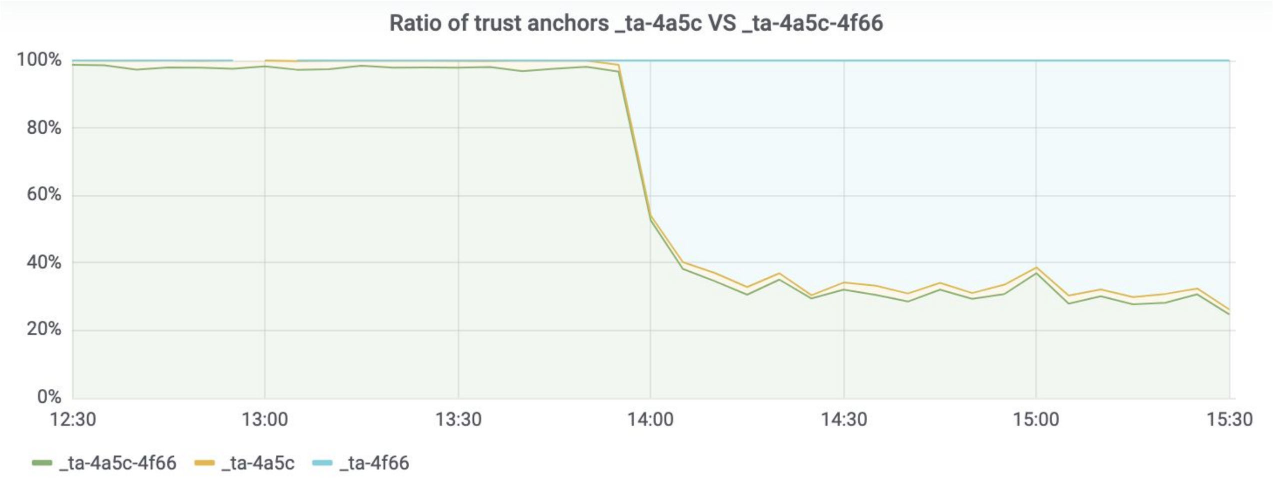
2019-01-11:: KSK-2010 Revoked

- A sudden further 5x increase
- And rising…
- (Still) not operationally concerning



_ta signal changes as seen by Cloudflare

- Rapid change to only new Key
  ⇒ RFC5011 working when the revoke bit was added to the key on 2019-01-11
- Much faster than expected



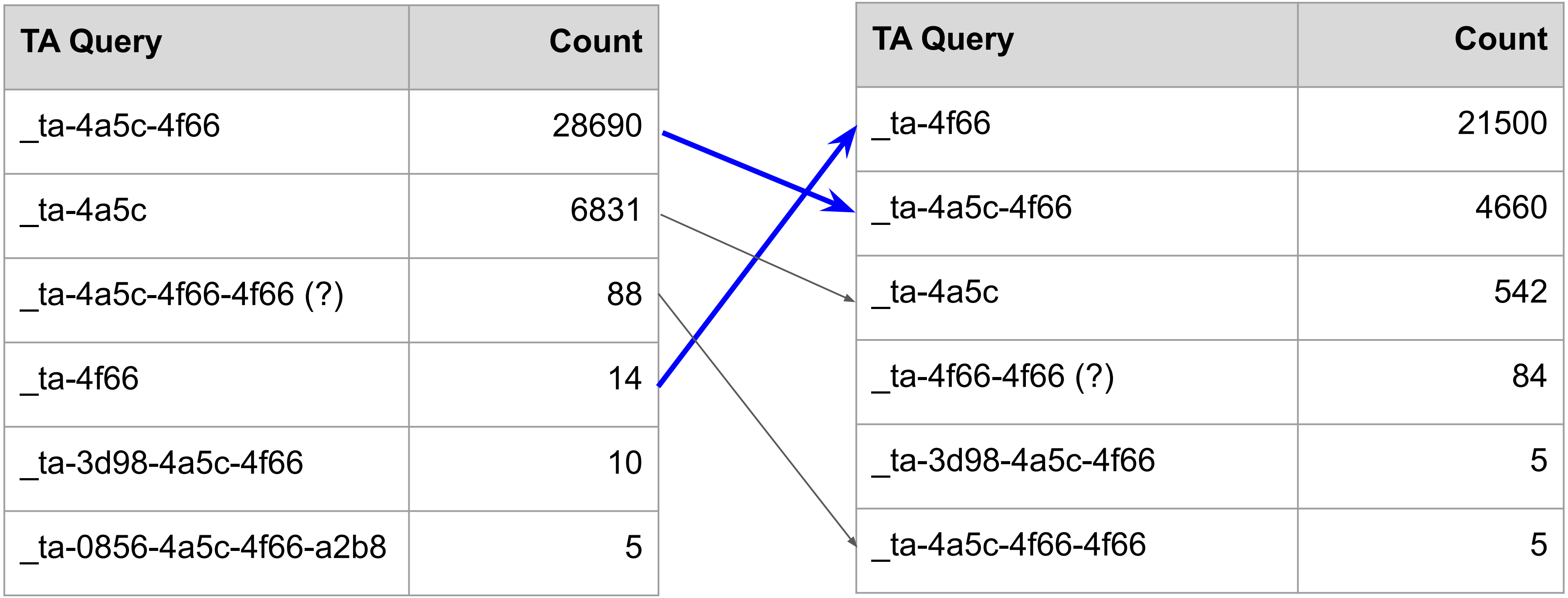
Sources of TA signal

- Not all sources have the same frequency
- Some report on every DNSKEY query

  ⇒ if one forwarder is "broken" it sends lots of DNSKEY queries biasing the counts

Query Source	**Total Queries**
200.179.223.x	6490
45.231.28.x	4810
1.10.193.x	737
153.92.184.x	703
84.198.213.x	628
12.151.164.x	599

Evidence of RFC 5011 working



2019-01-10 12:00 - 13:00 UTC

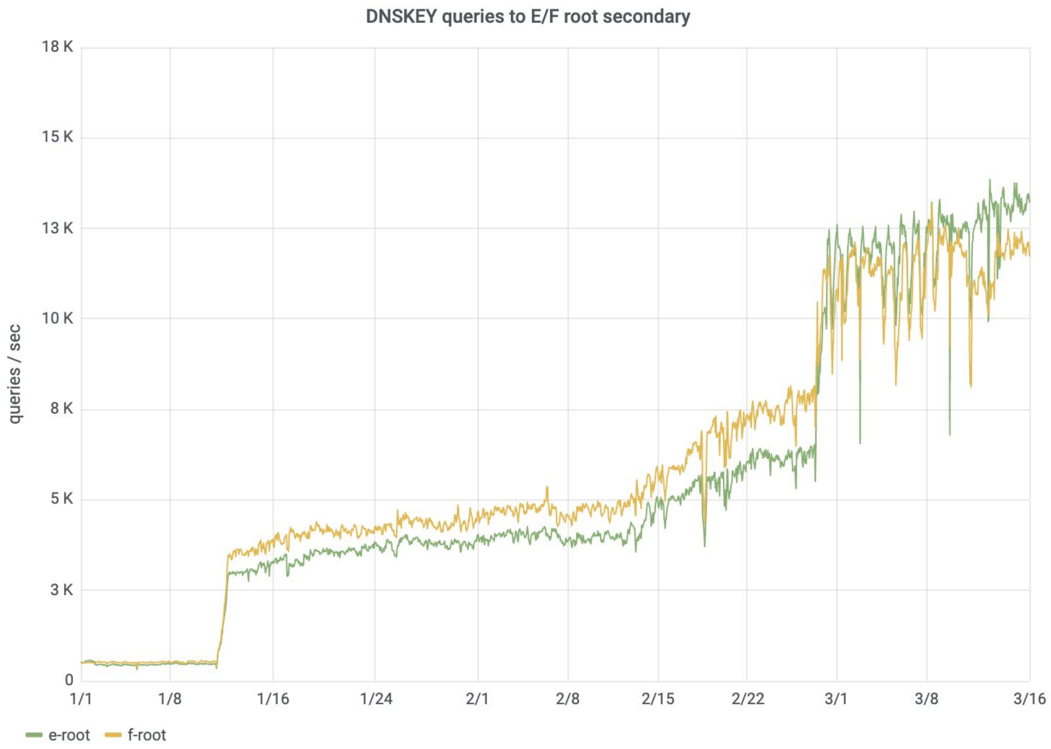
TA Query	Count
_ta-4a5c-4f66	28690
_ta-4a5c	6831
_ta-4a5c-4f66-4f66 (?)	88
_ta-4f66	14
_ta-3d98-4a5c-4f66	10
_ta-0856-4a5c-4f66-a2b8	5

2019-01-15 12:00 - 13:00 UTC

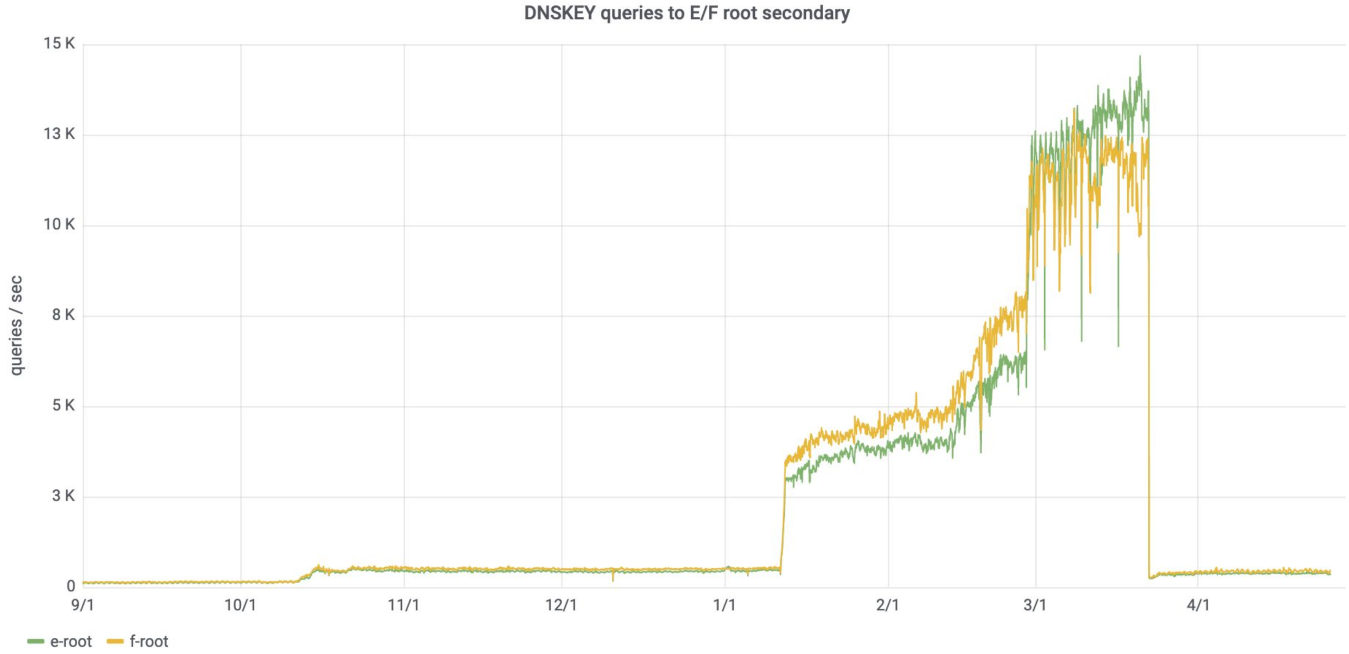
TA Query	Count
_ta-4f66	21500
_ta-4a5c-4f66	4660
_ta-4a5c	542
_ta-4f66-4f66 (?)	84
_ta-3d98-4a5c-4f66	5
_ta-4a5c-4f66-4f66	5

Long Term Impact

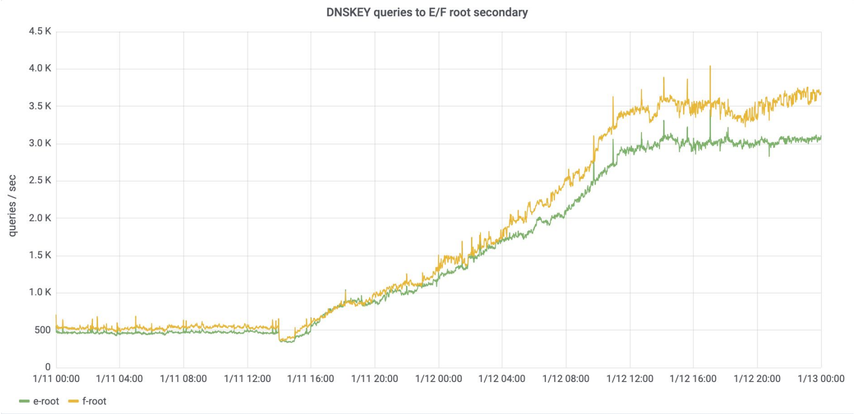
- Not steady
- Four separate growth phases
- (Still) not a problem
- 26 kQPS globally (E+F)



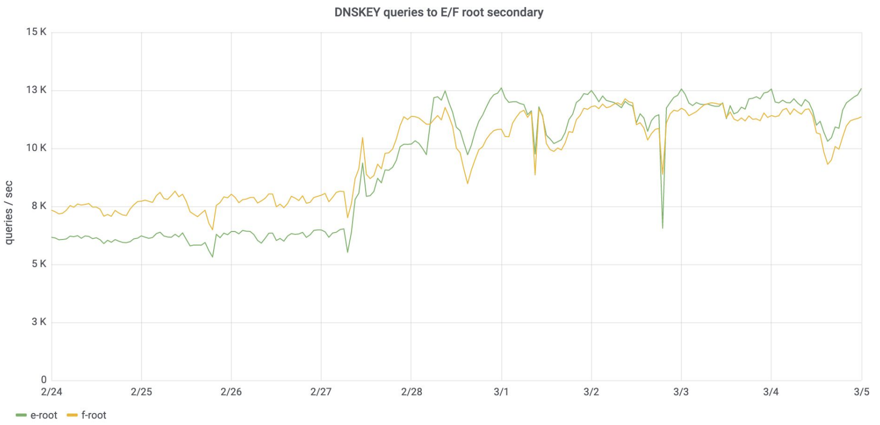
Entire Key Roll Life Cycle



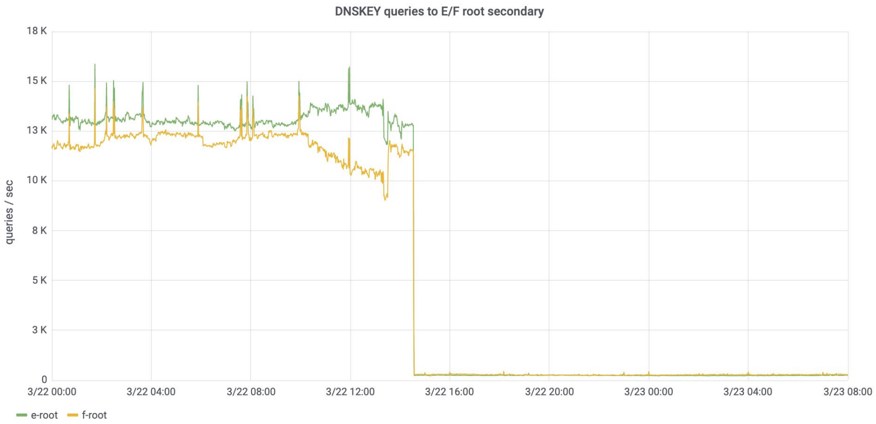
Revoke KSK-2010 (2019-01-11)



2nd rise (Feb 27 - Mar 1, 2019):

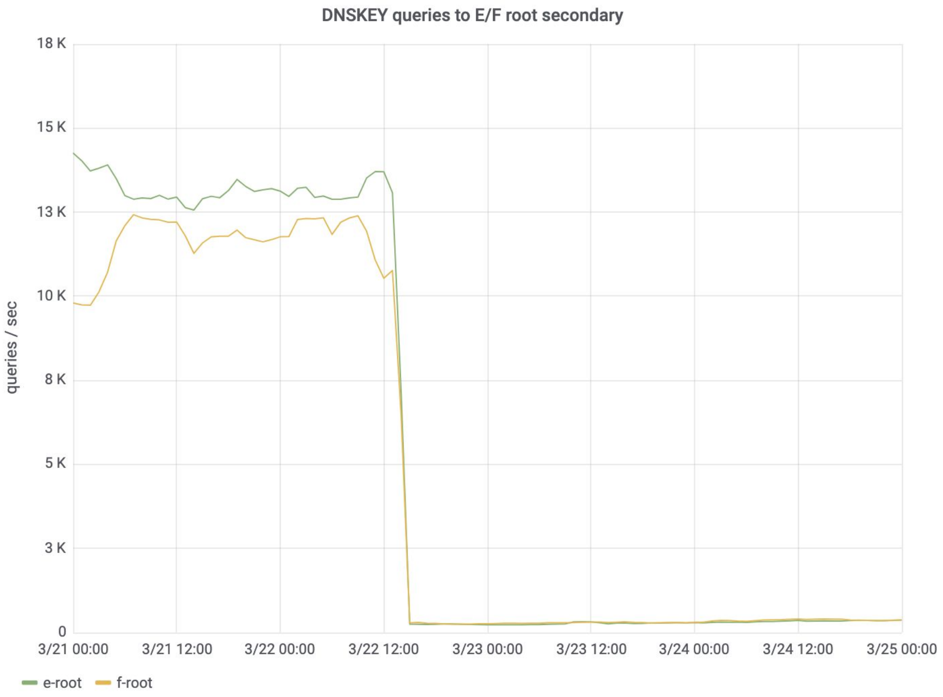


Remove KSK-2010 (2019-03-22)

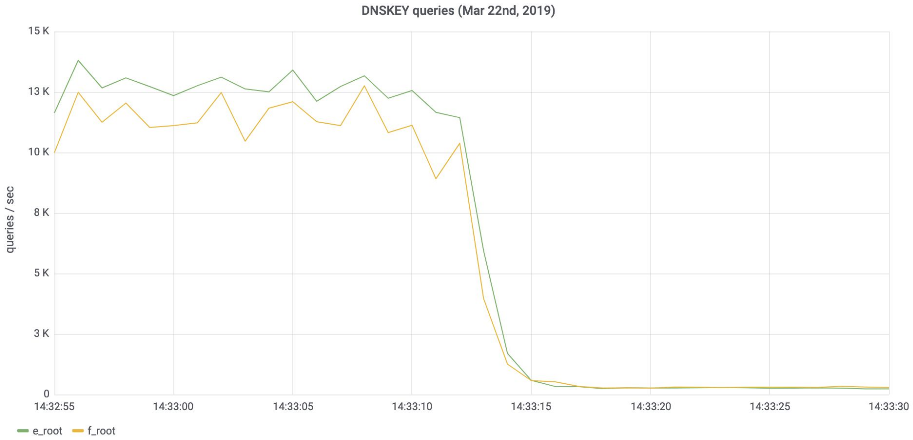


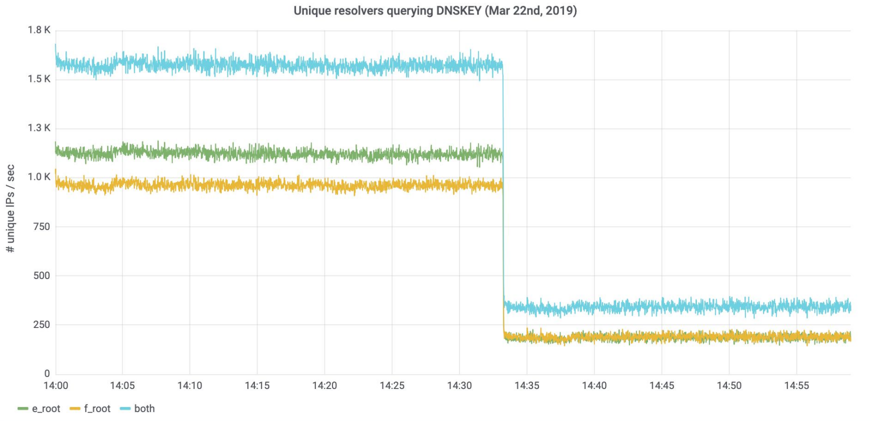
2019-03-22: KSK-2010 removal

- Incredibly sharp drop (< 2 seconds)



2019-03-22: KSK-2010 removal (Detail)





Current State

- DNSKEY traffic remains at post-roll levels

- TA Signal Counts for 2019-05-10 (1 hour sample)

  < 100 addresses reporting KSK-2010 (1.6%)
  > 4300 addresses reporting KSK-2017
  > 1500 addresses still reporting both ⇐ This is fine

Questions?