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
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

<table>
<thead>
<tr>
<th>Date</th>
<th>Address</th>
<th>ASN</th>
<th>30 Day Count</th>
<th>Saw Both Keys</th>
<th>Spamhaus PBL</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018-06-01</td>
<td>210.94.72.x</td>
<td>9318</td>
<td>27</td>
<td>False</td>
<td>True</td>
</tr>
<tr>
<td>2018-06-03</td>
<td>210.94.72.x</td>
<td>9318</td>
<td>27</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>2018-06-04</td>
<td>210.94.72.x</td>
<td>9318</td>
<td>27</td>
<td>False</td>
<td>True</td>
</tr>
<tr>
<td>2018-06-10</td>
<td>210.94.72.x</td>
<td>9318</td>
<td>27</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>2018-06-11</td>
<td>210.94.72.x</td>
<td>9318</td>
<td>27</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>2018-06-13</td>
<td>210.94.72.x</td>
<td>9318</td>
<td>27</td>
<td>False</td>
<td>True</td>
</tr>
<tr>
<td>2018-06-18</td>
<td>210.94.72.x</td>
<td>9318</td>
<td>27</td>
<td>False</td>
<td>True</td>
</tr>
</tbody>
</table>
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)
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

<table>
<thead>
<tr>
<th>Query Source</th>
<th>Total Queries</th>
</tr>
</thead>
<tbody>
<tr>
<td>200.179.223.x</td>
<td>6490</td>
</tr>
<tr>
<td>45.231.28.x</td>
<td>4810</td>
</tr>
<tr>
<td>1.10.193.x</td>
<td>737</td>
</tr>
<tr>
<td>153.92.184.x</td>
<td>703</td>
</tr>
<tr>
<td>84.198.213.x</td>
<td>628</td>
</tr>
<tr>
<td>12.151.164.x</td>
<td>599</td>
</tr>
</tbody>
</table>
## Evidence of RFC 5011 working

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

<table>
<thead>
<tr>
<th>TA Query</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>_ta-4a5c-4f66</td>
<td>28690</td>
</tr>
<tr>
<td>_ta-4a5c</td>
<td>6831</td>
</tr>
<tr>
<td>_ta-4a5c-4f66-4f66 (?)</td>
<td>88</td>
</tr>
<tr>
<td>_ta-4f66</td>
<td>14</td>
</tr>
<tr>
<td>_ta-3d98-4a5c-4f66</td>
<td>10</td>
</tr>
<tr>
<td>_ta-0856-4a5c-4f66-a2b8</td>
<td>5</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>TA Query</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>_ta-4f66</td>
<td>21500</td>
</tr>
<tr>
<td>_ta-4a5c-4f66</td>
<td>4660</td>
</tr>
<tr>
<td>_ta-4a5c</td>
<td>542</td>
</tr>
<tr>
<td>_ta-4f66-4f66 (?)</td>
<td>84</td>
</tr>
<tr>
<td>_ta-3d98-4a5c-4f66</td>
<td>5</td>
</tr>
<tr>
<td>_ta-4a5c-4f66-4f66</td>
<td>5</td>
</tr>
</tbody>
</table>
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?