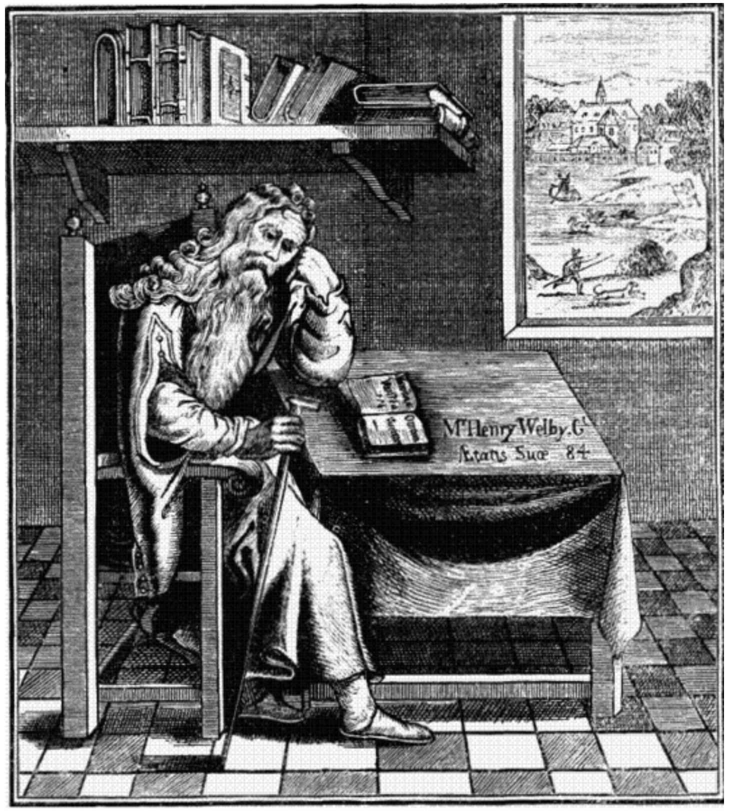
Measuring the KSK Roll

Geoff Huston
APNiC Labs

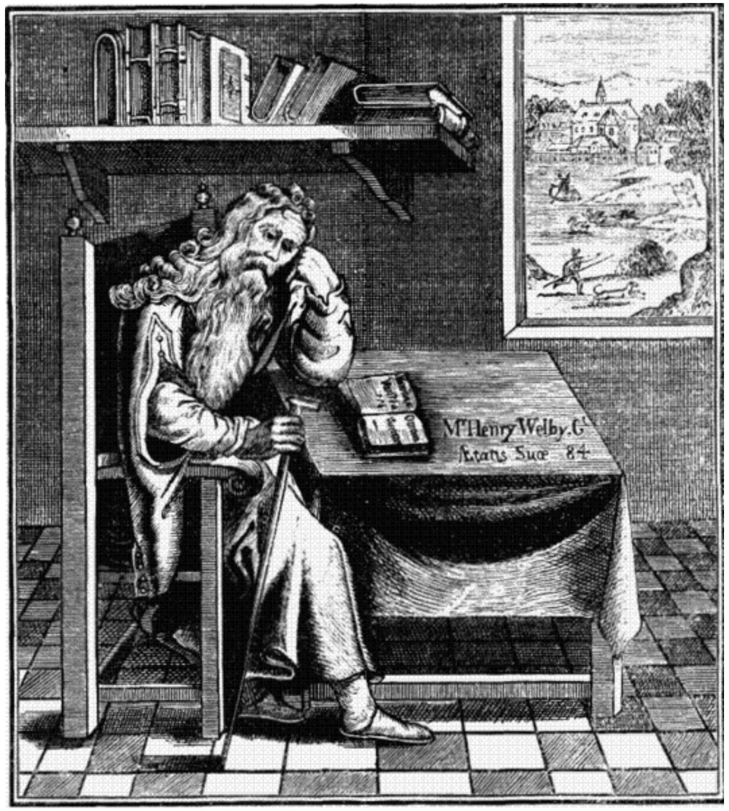
KSK Roll Measurement Objective

What number of users are at risk of being impacted by the KSK Roll?

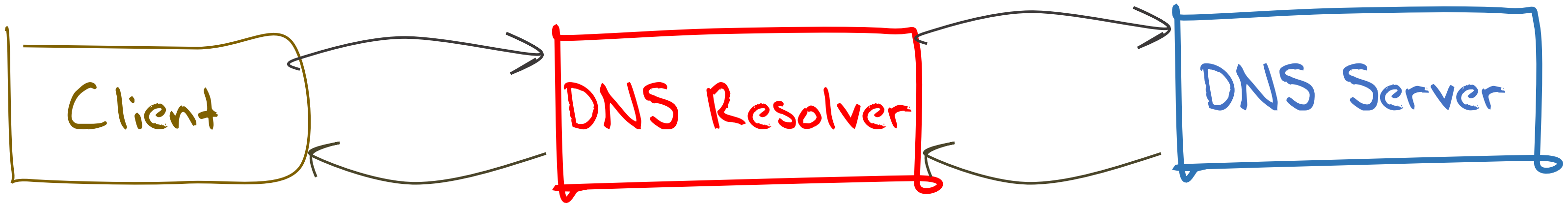


KSK Roll Measurement Objective

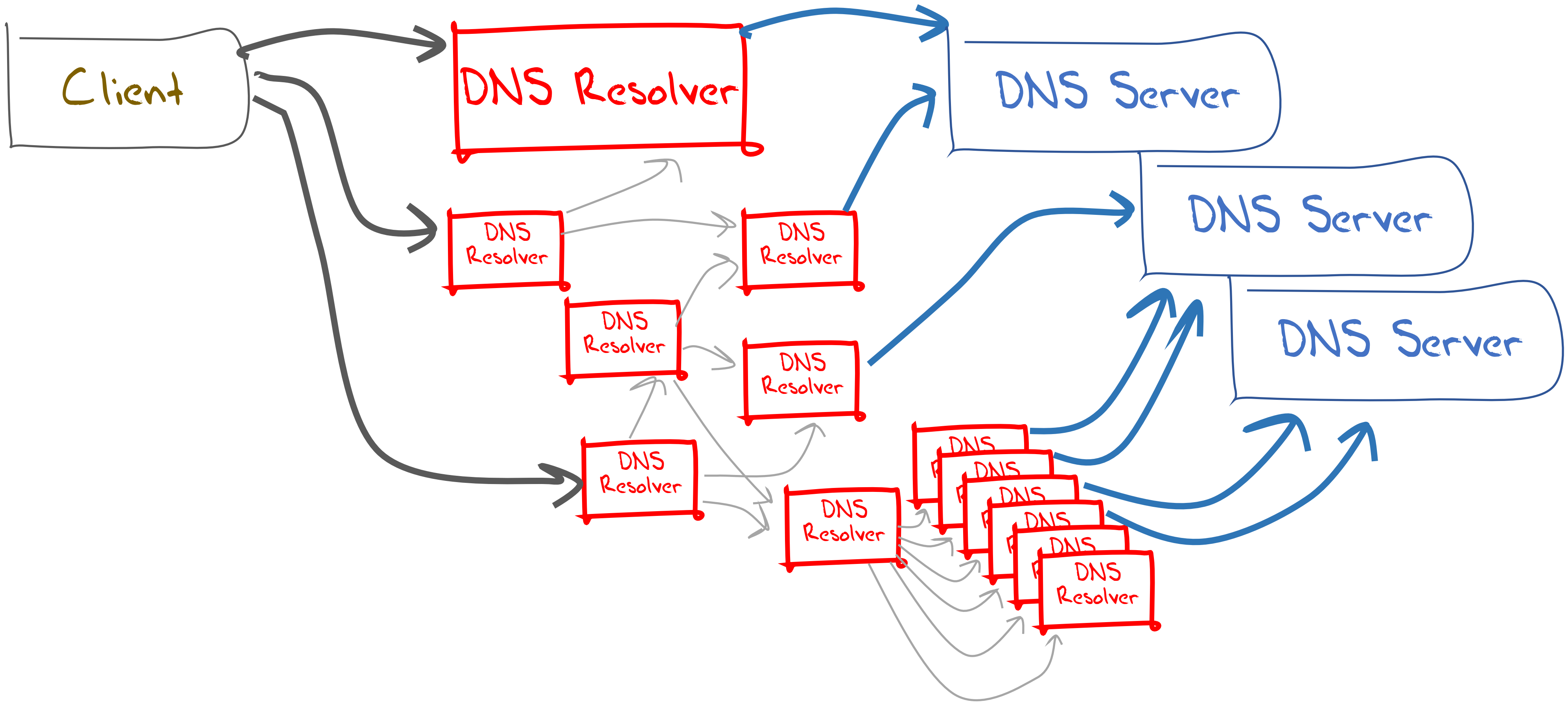
What number of users ~~are at risk of being~~ were impacted by the KSK Roll?



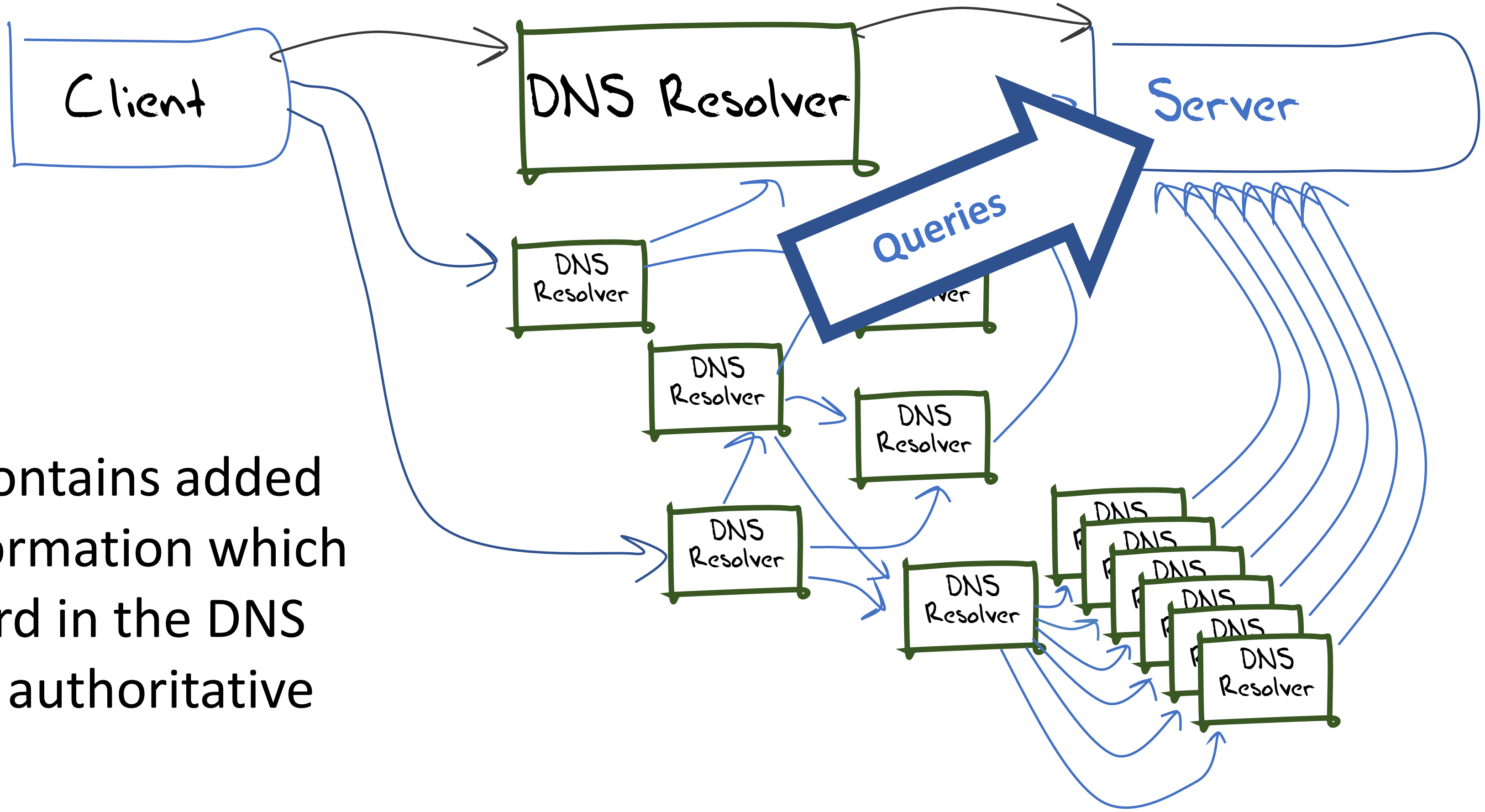
What we would like the DNS to be



What we suspect is in the DNS

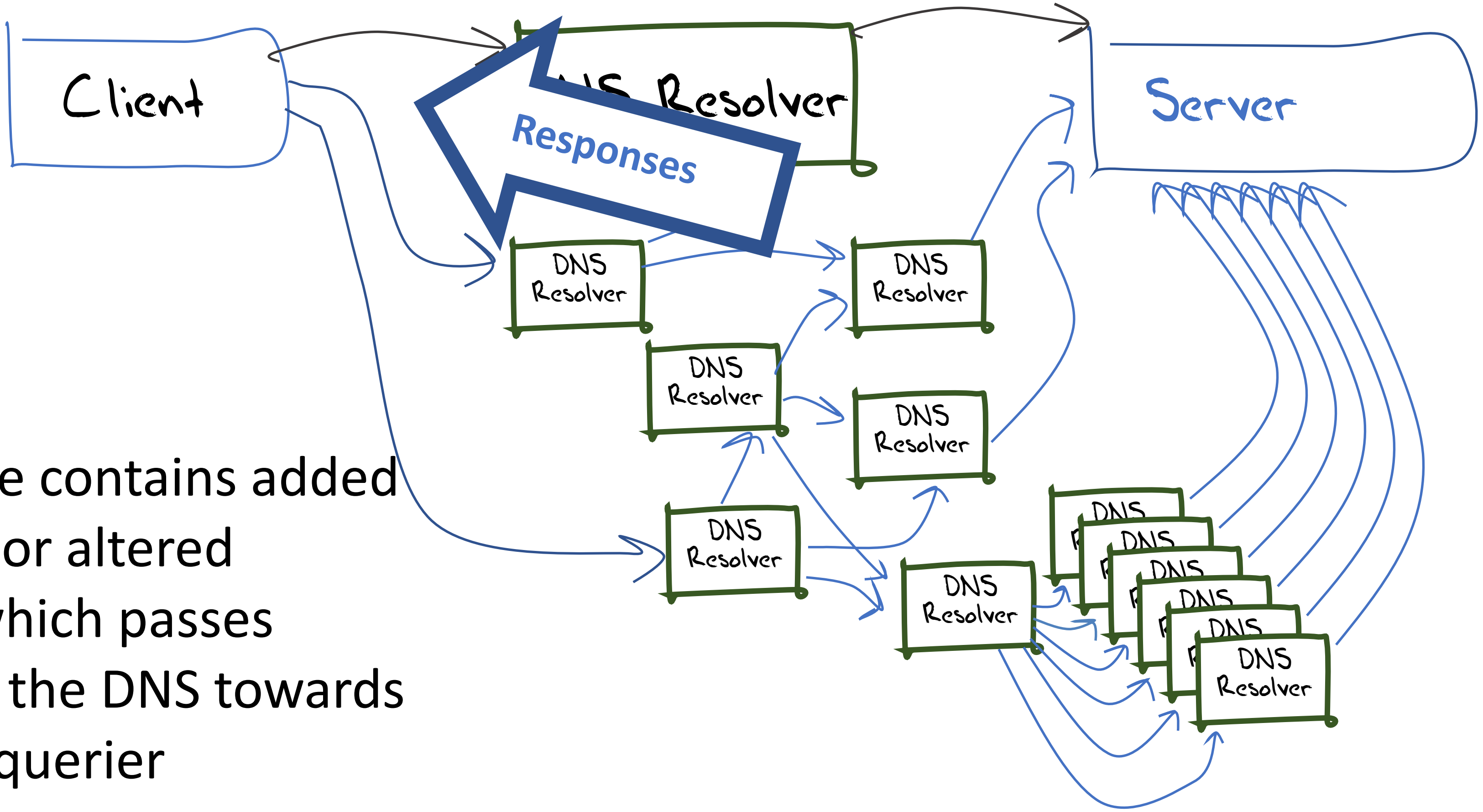


Signalling via Queries



The query contains added resolver information which passes inward in the DNS towards the authoritative server(s)

Signalling via Responses

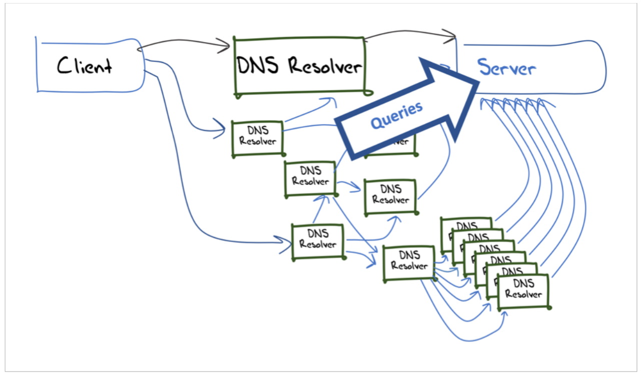


The response contains added information or altered behavious which passes backward in the DNS towards the original querier

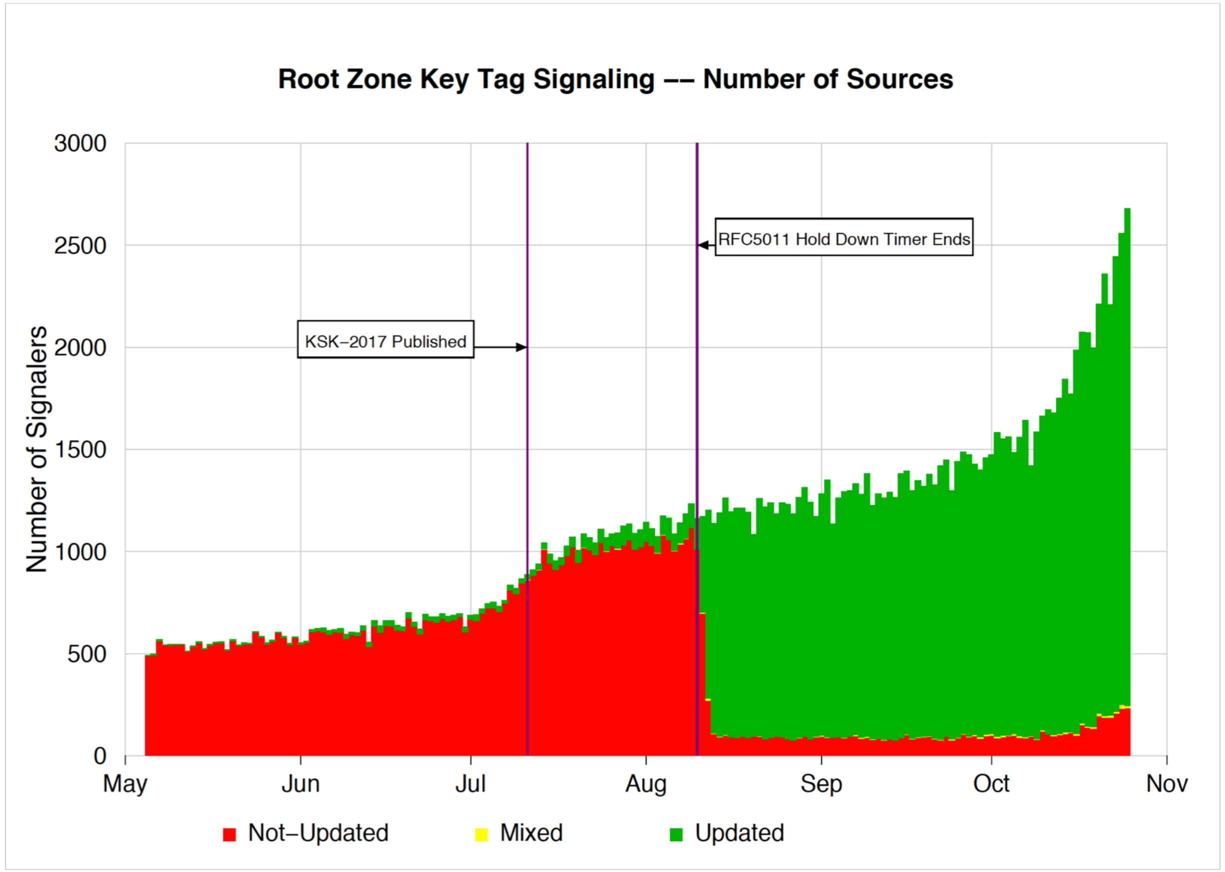
Measuring Resolvers with RFC 8145

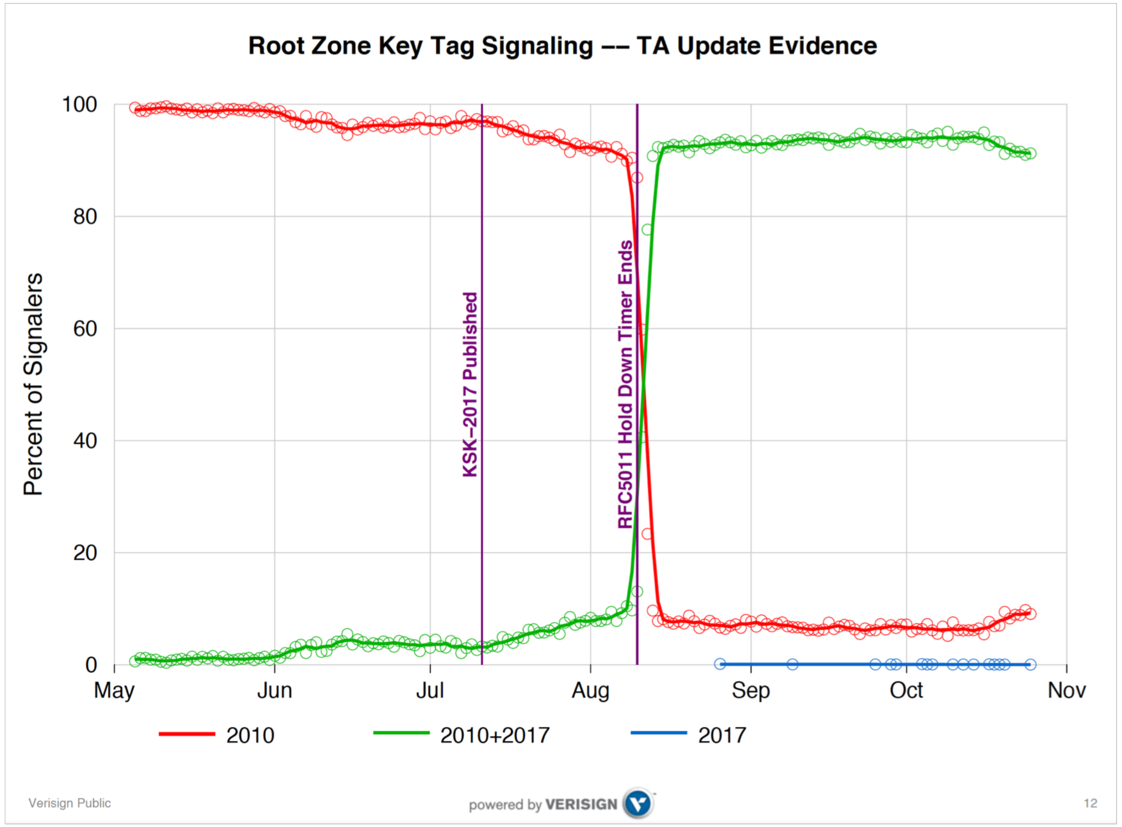
Getting resolvers to report on their local trusted key state

- A change to resolver behavior that requires deployment of new resolver code
- Resolvers that support the RFC 8145 signal mechanism periodically include the key tag of their locally trusted keys into a query directed towards the root servers



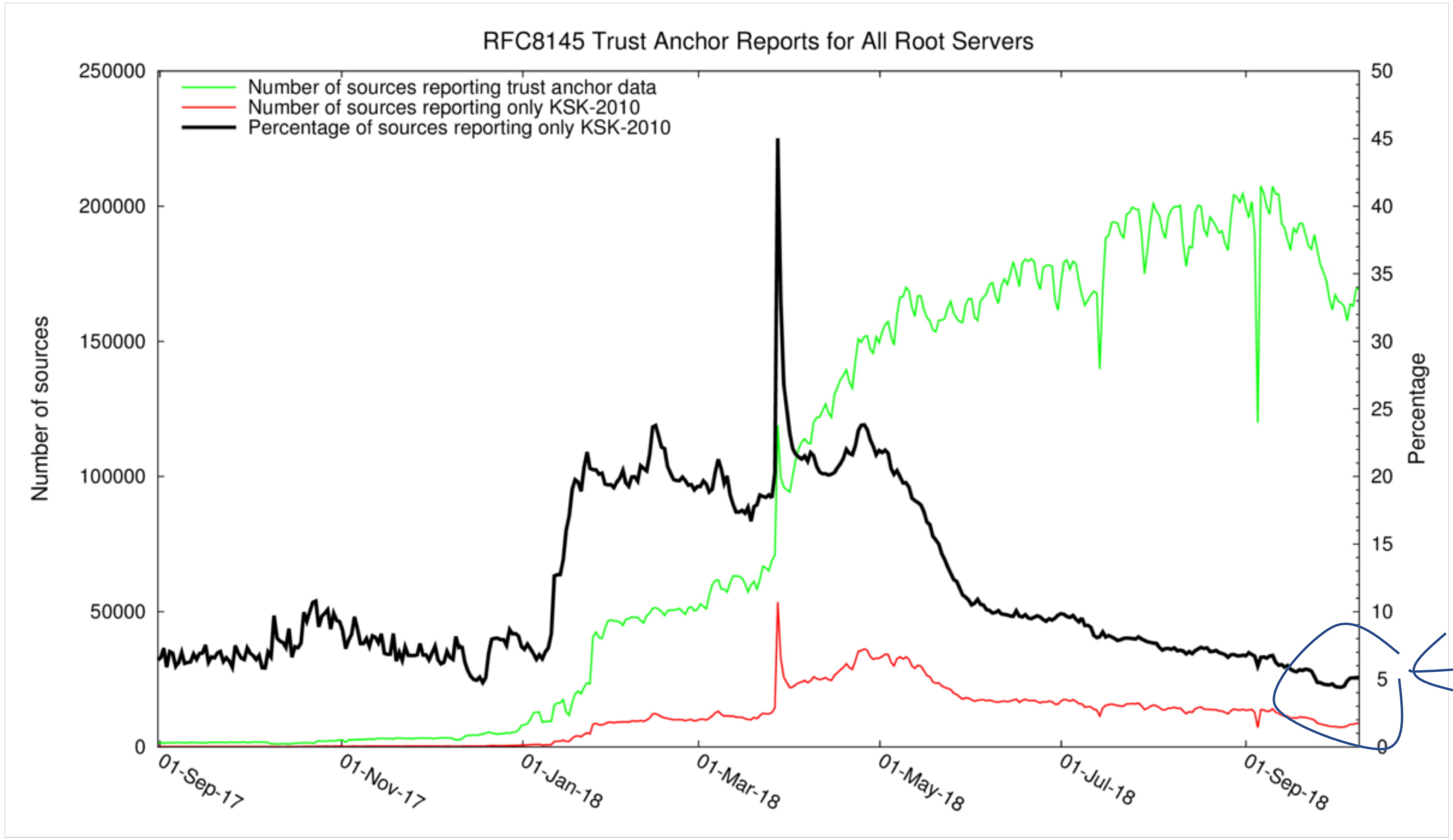
What did we see at the roots?





Duane Wessels VeriSign RFC 8145 Signaling Trust Anchor Knowledge In DNS Security Extensions
Presentation to DNSSEC Workshop @ ICANN 60 – 1 Nov 2017
https://schd.ws/hosted_files/icann60abudhabi2017/ea/Duane%20Wessels-VeriSign-RFC%208145-Signaling%20Trust%20Anchor%20Knowledge%20in%20DNS%20Security%20Extensions.pdf

12 months of RFC8145 signalling



Yes, with just a few days to go this mechanism was still reporting 5% 'breakage'

http://root-trust-anchor-reports.research.icann.org

What is this saying?

It’s clear that there is some residual set of resolvers that are signalling that they have not yet learned to trust the new KSK key

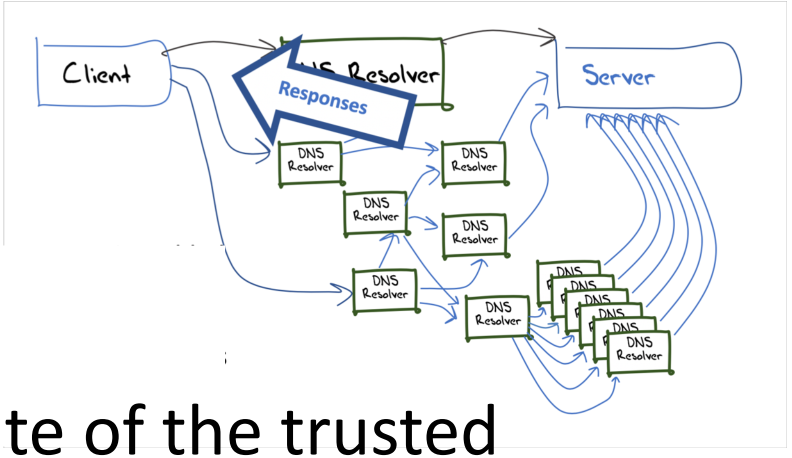
But its **not** clear if:

- This is an accurate signal about the state of this resolver
- This is an accurate signal about the identity of this resolver
- How many users sit ‘behind’ this resolver
- Whether these uses rely solely on this resolver, or if they also have alternate resolvers that they can use
- What proportion of all users are affected

Why?

- Because the DNS does not disclose the antecedents of a query
  - If A forwards a query to B, who queries a Root Server then if the query contains an implicit signal (as in this case) then it appears that B is querying, not A
  - At no time is the user made visible in the referred query
- Because caching
  - If A and B both forward their queries via C, then it may be that one or both of these queries may be answered from C’s cache
  - In this case the signal is being suppressed
- Because its actually measuring a cause, not the outcome
  - Its measuring resolvers’ uptake of the new KSK, but is not able to measure the user impact of this

User-Side Measurement



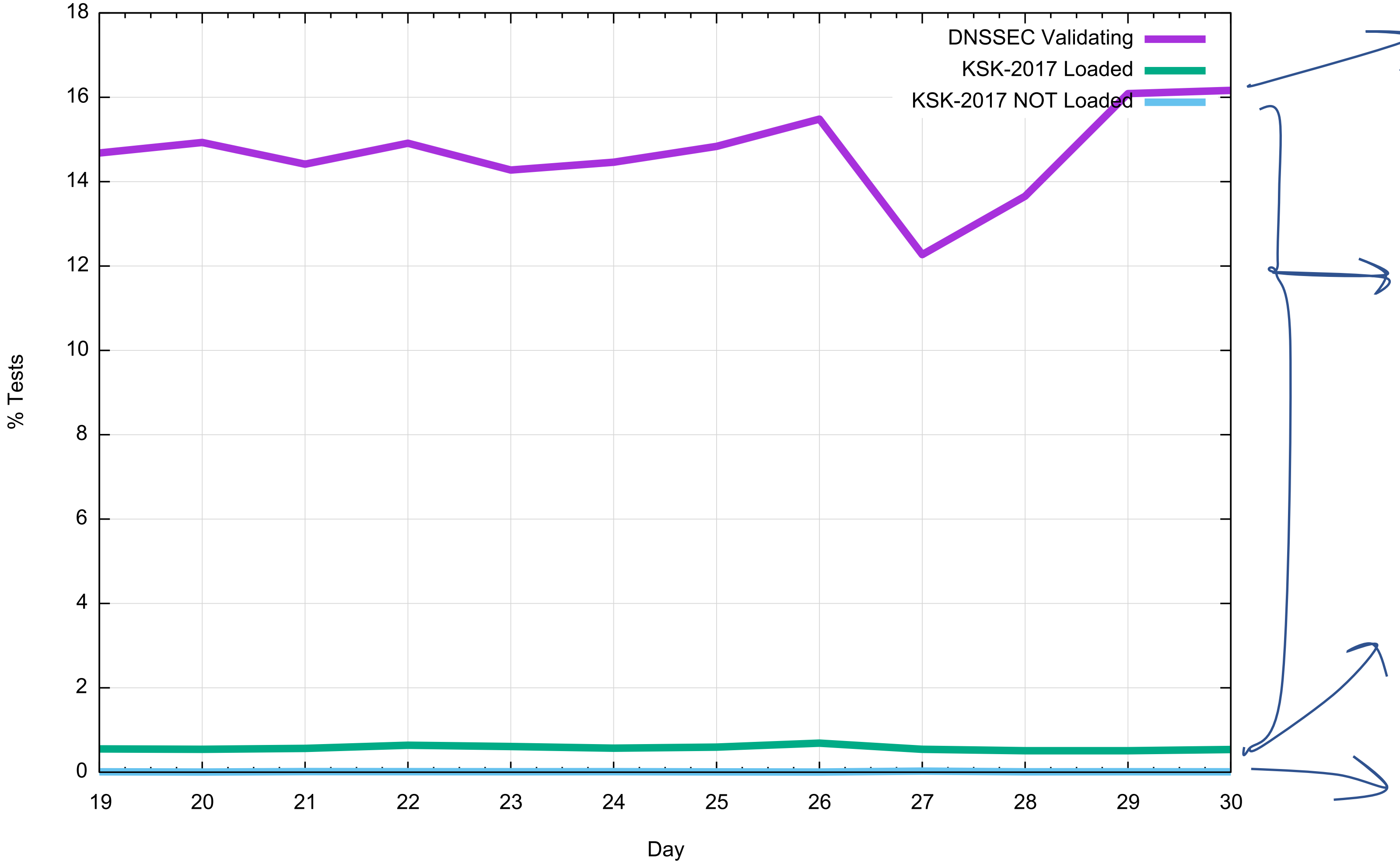
Can we devise a DNS query that could reveal the state of the trusted keys of the resolvers back to the user?

- What about a change to the resolver's reporting of validation outcome depending on the resolver's local trusted key state?
    - If a query contains the label **"root-key-sentinel-is-ta-<key-tag>**" then a validating resolver will report validation failure if the key is NOT in the local trusted key store
    - If a query contains the label **"root-key-sentinel-not-ta-<key-tag>"** then a validating resolver will report validation failure if the key IS in the local trusted key store

DNS + Web

- How can you tell if a user is able to resolve a DNS name?
  - Be the user (get the user to run a script of some sort)
  - Look at the DNS server AND the Web server
    - The Web object is fetched only when the DNS provides a resolution answer
    - But the opposite is not necessarily the case, so there is a noise component in such an approach

Prior to the KSK Roll



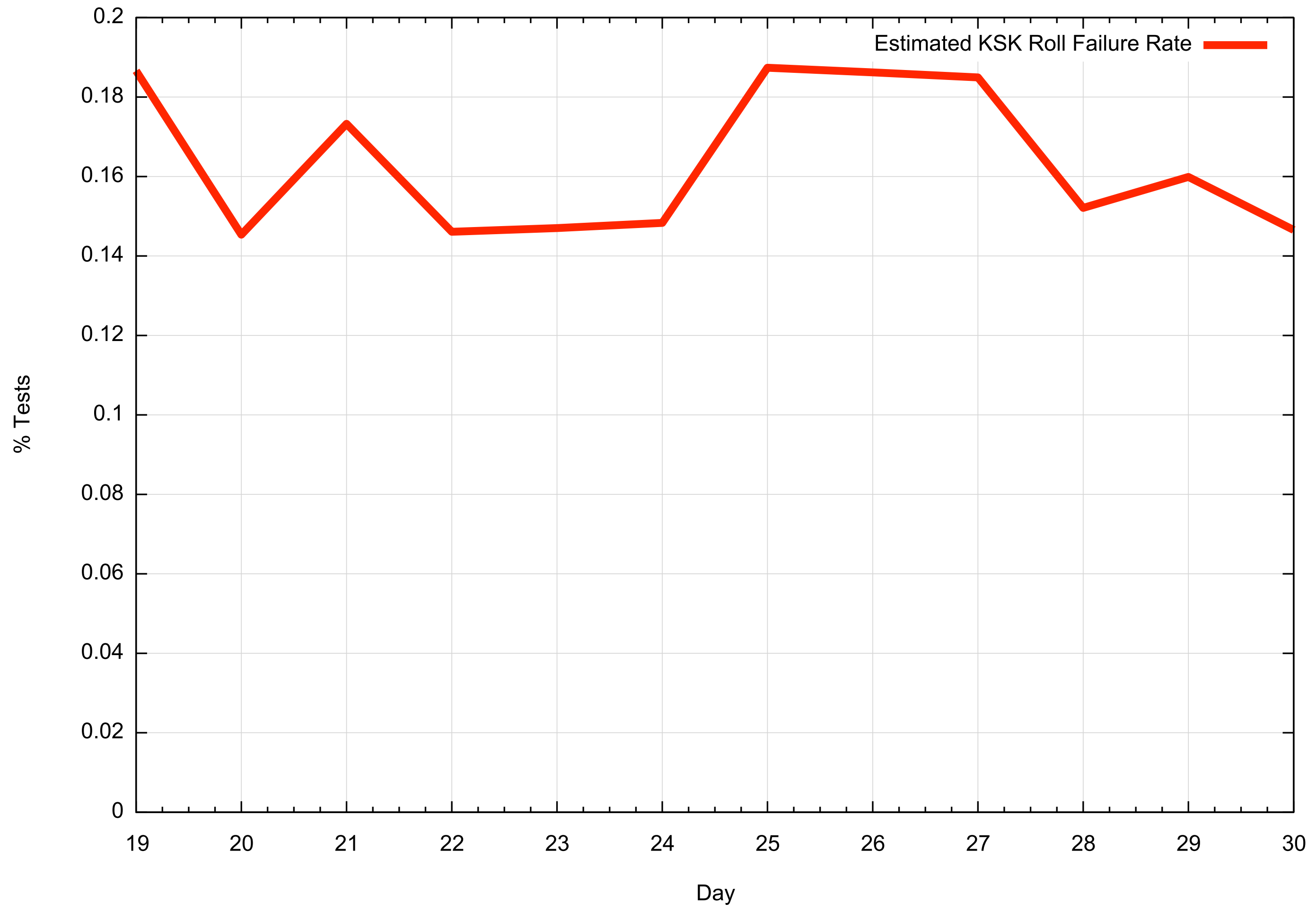
16% of users use DNSSEC-validating resolvers

15% of users do not report their KSK trust-state

0.5% of users report KSK-2017 loaded

0.005% of users report KSK-2017 NOT loaded

Possibly Affected Users



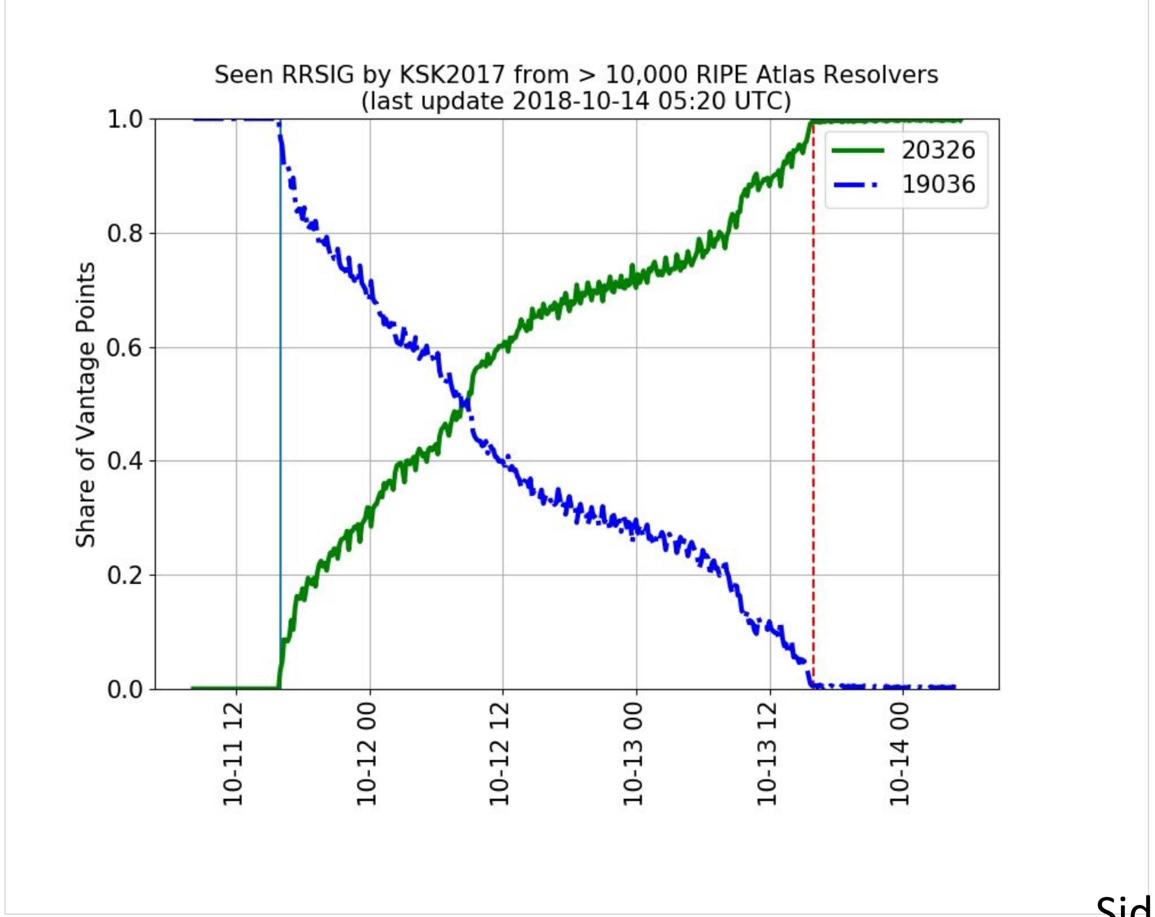
Between 0.1% to 0.2% of users are reporting that their resolvers have not loaded KSK-2017 as a trust anchor

The measurement has many uncertainties and many sources of noise so this is an upper bound of the pool of users who may encounter DNS failure due to to the KSK roll

But

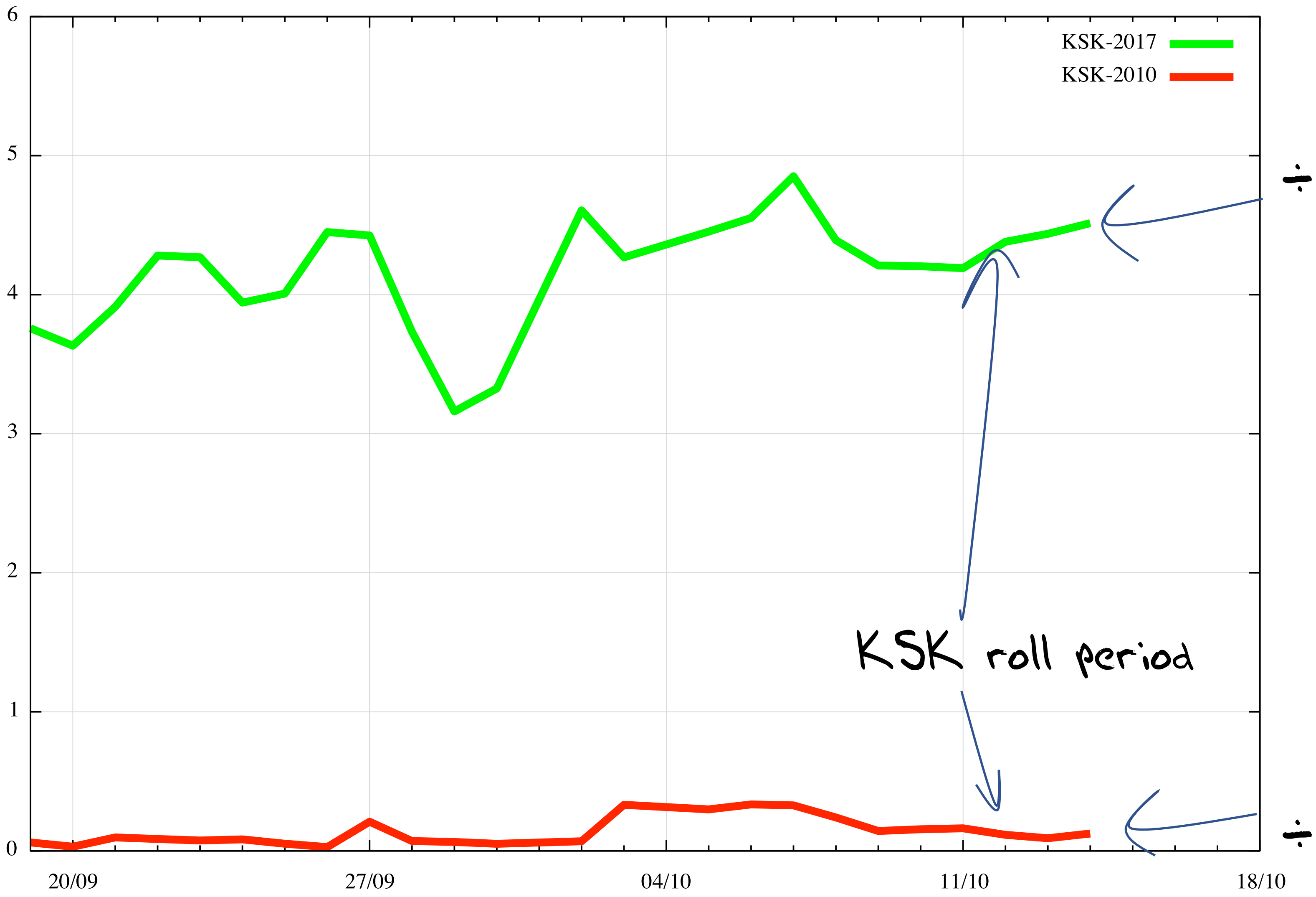
- Not all resolvers will pre-provision KSK-2017 using RFC 5011 automated trust mechanisms – they may elect to load the new trsut anchor at the time of the roll manually
  - And we cannot measure the difference between a resolver that has a broken implementation of RFC5011 and a resolver that is being managed manually
- Only recently upgraded resolvers have this test behaviour included
  - But the resolvers we worry about are the crufty ones at the bottom of the rack that have been all but forgotten!

What happened



Sidn Labs Atlas Measurement

What we saw

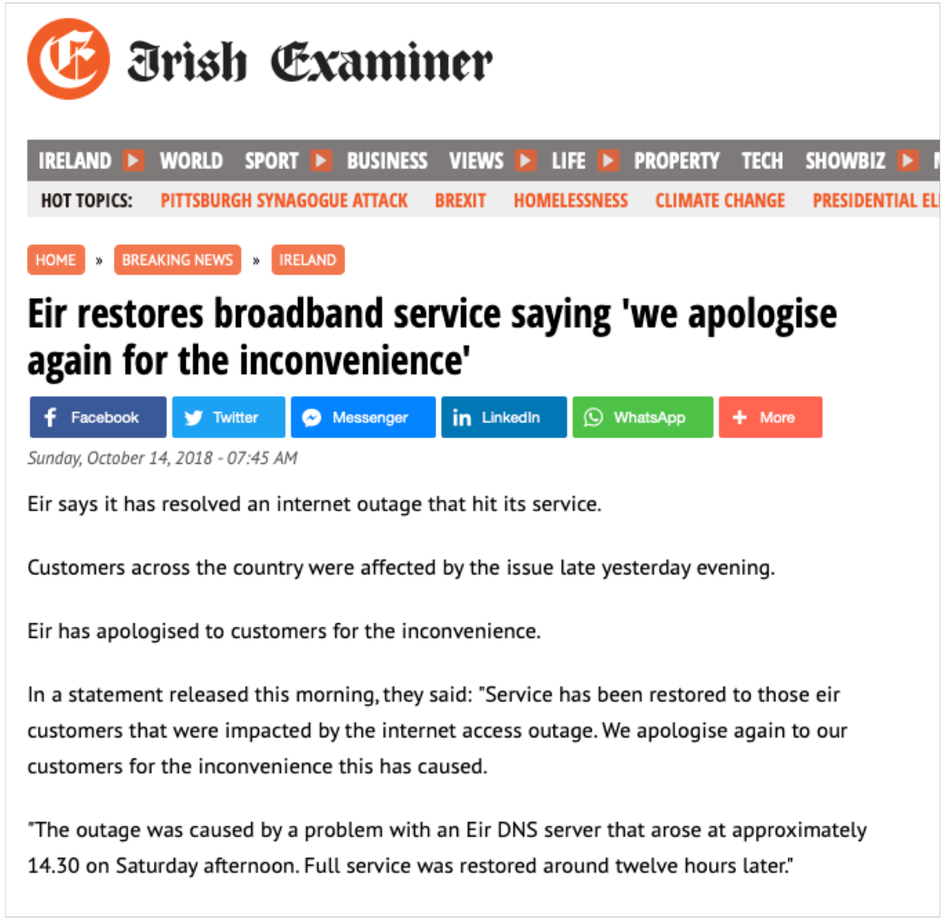


KSK roll period

÷ of folk that reported "good"

÷ of folk that reported "bad"

What we heard


Irish Examiner
IRELAND WORLD SPORT BUSINESS VIEWS LIFE PROPERTY TECH SHOWBIZ
HOT TOPICS: PITTSBURGH SYNAGOGUE ATTACK BREXIT HOMELESSNESS CLIMATE CHANGE PRESIDENTIAL EL
HOME » BREAKING NEWS » IRELAND
Facebook Twitter Messenger LinkedIn WhatsApp More

Eir restores broadband service saying 'we apologise again for the inconvenience'

Sunday, October 14, 2018 - 07:45 AM

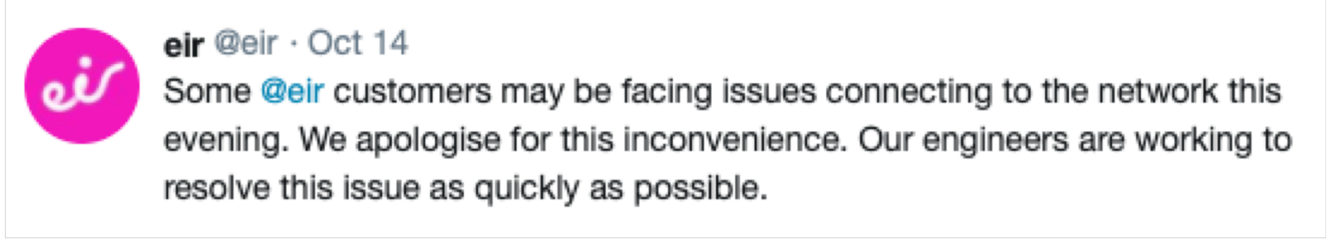
Eir says it has resolved an internet outage that hit its service.

Customers across the country were affected by the issue late yesterday evening.

Eir has apologised to customers for the inconvenience.

In a statement released this morning, they said: "Service has been restored to those eir customers that were impacted by the internet access outage. We apologise again to our customers for the inconvenience this has caused.

"The outage was caused by a problem with an Eir DNS server that arose at approximately 14.30 on Saturday afternoon. Full service was restored around twelve hours later."



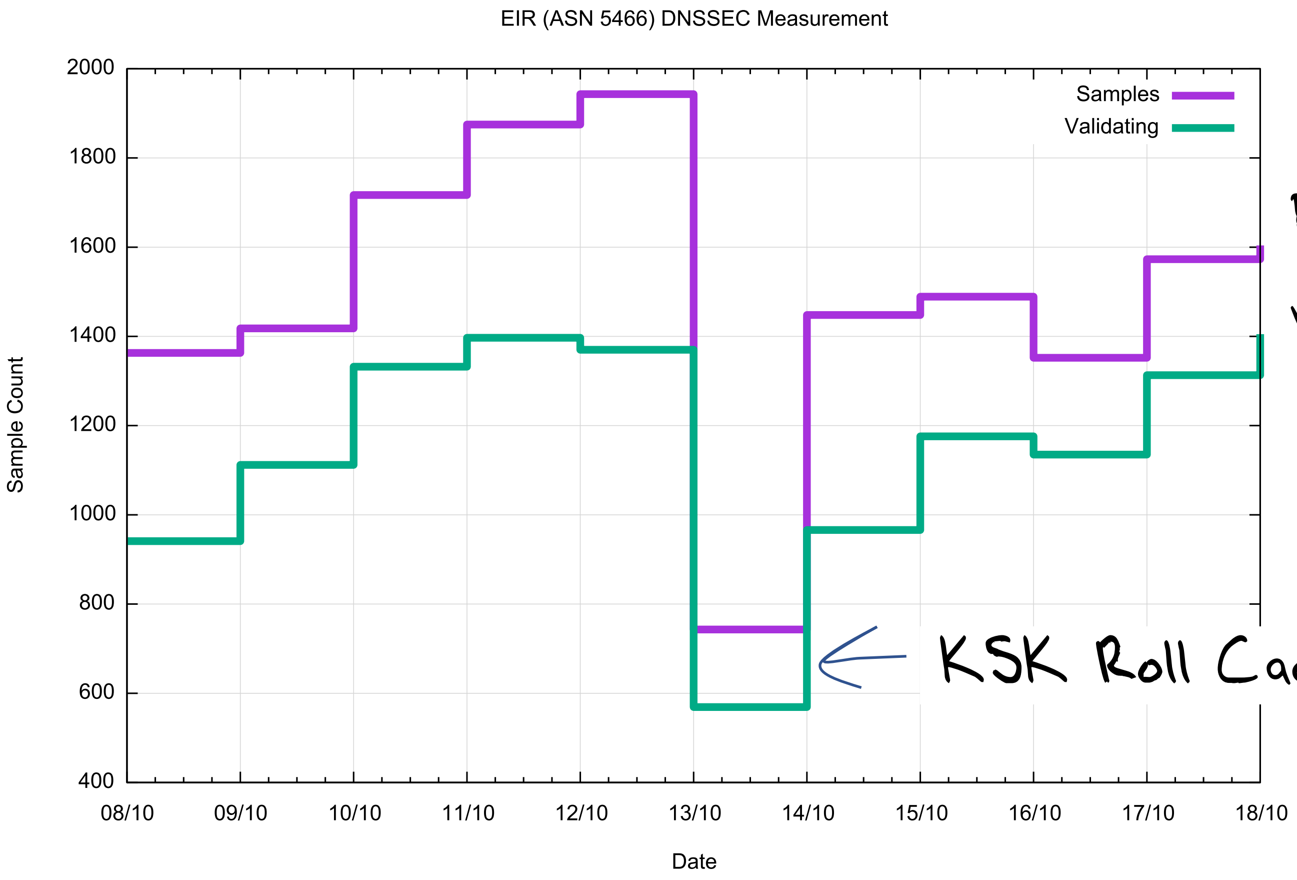
eir @eir · Oct 14

Some @eir customers may be facing issues connecting to the network this evening. We apologise for this inconvenience. Our engineers are working to resolve this issue as quickly as possible.

What happens when you lose track of the KSK?

Everything goes black

EIR - AS5466 DNSSEC Data

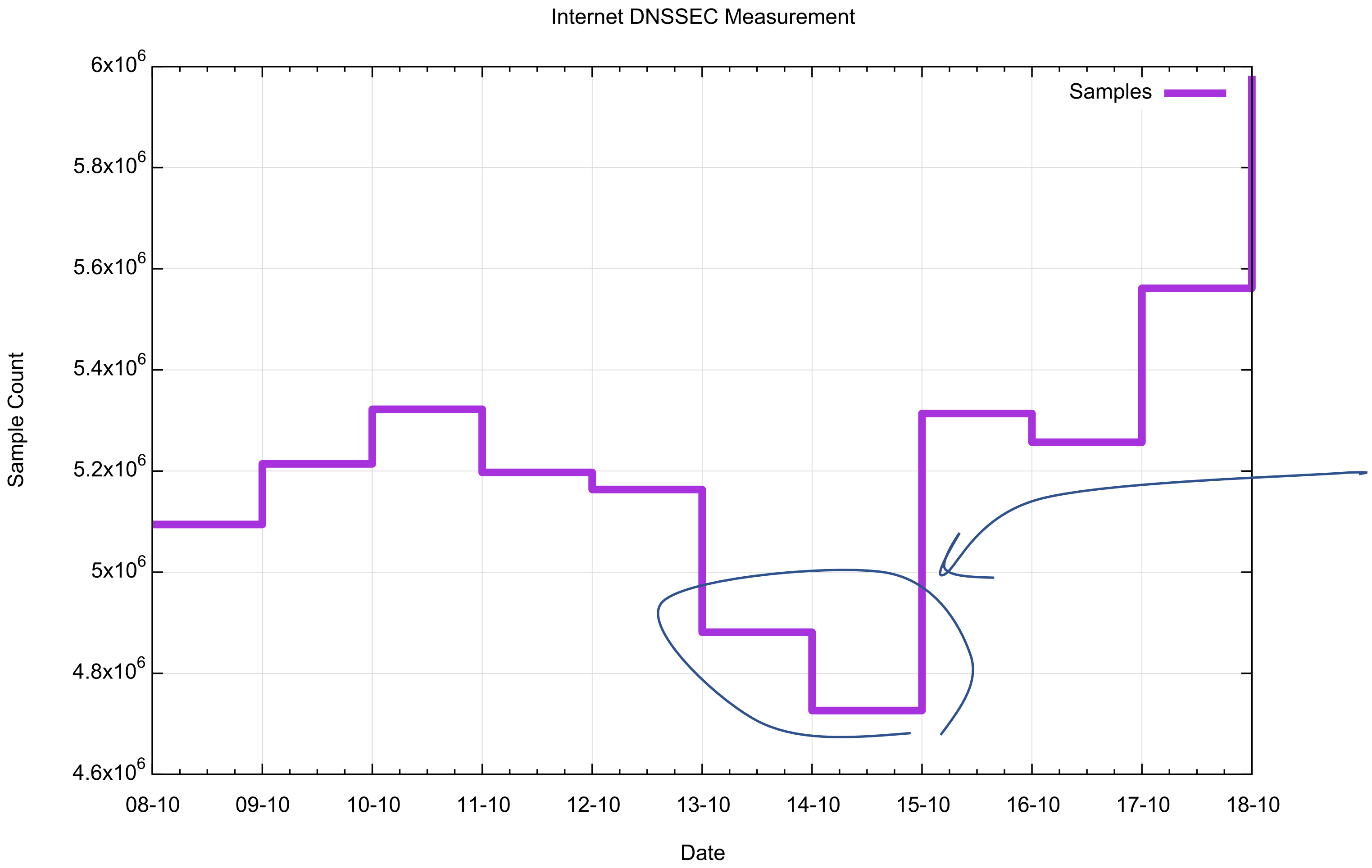


Daily Sample Count

Validating Sample Count

KSK Roll Cache Expiry

Internet DNSSEC Data



is this part-related to
the KSK Roll?

Looking for Affected Networks

- Lets use the following filter:
  - More than 400 samples / day in the lead up to the KSK roll (using weighted sample count)
  - DNSSEC validation level more than 30% prior to the KSK roll
  - Drop of more than 33% in DNSSEC validation during the KSK roll

Rank	AS	CC	Seen			Validating			As Name
			Before	During	After	Before	During	After	
1	AS2018	ZA	1,858	1,122	1,473	694	220	288	TENET, South Africa
2	AS10396	PR	1,789	1,673	1,988	1,647	276	33	COQUI-NET - DATACOM CARIBE, Puerto Rico
3	AS45773	PK	1,553	388	1,393	606	178	540	HECPERN-AS-PK PERN, Pakistan
4	AS15169	IN	1,271	438	1,286	1,209	438	1,242	GOOGLE - Google LLC, India
5	AS22616	US	1,264	503	1,526	883	377	1,014	ZSCALER- SJC, US
6	AS53813	IN	1,213	689	1,862	1,063	582	1,419	ZSCALER, India
7	AS1916	BR	1,062	94	991	326	37	277	Rede Nacional de Ensino e Pesquisa, Brazil
8	AS9658	PH	931	281	842	440	136	404	ETPI-IDS-AS-AP Eastern Telecoms, Philippines
9	AS37406	SS	888	486	972	582	365	599	RCS, South Sudan
10	AS263327	BR	882	345	438	776	289	359	ONLINE SERVICOS DE TELECOMUNICACOES, Brazil
11	AS17557	PK	835	430	777	431	277	413	Pakistan Telecommunication, Pakistan
12	AS36914	KE	834	476	937	583	354	670	KENET , Kenya
13	AS327687	UG	802	473	834	390	189	332	RENU, Uganda
14	AS680	DE	773	966	1,332	268	117	289	DFN Verein zur Foerderung, Germany
15	AS201767	UZ	761	538	729	461	200	371	UZMOBILE, Uzbekistan
16	AS37682	NG	695	401	728	593	274	568	TIZETI, Nigeria
17	AS7470	TH	674	214	507	219	94	182	True Internet, Thailand
18	AS51167	DE	670	378	479	214	78	156	CONTABO, Germany
19	AS15525	PT	600	260	593	287	125	284	MEO-EMPRESAS, Portugal
20	AS14061	GB	594	468	672	260	169	313	DigitalOcean, United Kingdom
21	AS37130	ZA	585	5	464	414	0	260	SITA, South Africa
22	AS30998	NG	583	264	484	192	54	143	NAL, Nigeria
23	AS135407	PK	569	227	457	419	207	344	TES-PL-AS-AP Trans World, Pakistan
24	AS16814	AR	565	235	456	258	120	208	NSS, Argentina
25	AS132335	IN	563	17	30	538	17	23	NETWORK-LEAPSWITCH-IN LeapSwitch Networks, India
26	AS5438	TN	559	532	579	526	171	27	ATI,Tunisia
27	AS5466	IE	547	240	401	419	184	329	EIRCOM Internet House, IE Ireland
28	AS18002	IN	538	467	614	277	176	242	WORLDPHONE-IN AS, India
29	AS37209	NG	532	109	438	269	45	194	HYPERIA, Nigeria
30	AS37100	ZA	454	161	401	168	95	131	SEACOM-AS, South Africa
31	AS5588	CZ	453	175	430	186	102	162	GTSCE GTS Central Europe, Czechia
32	AS1103	NL	446	38	363	189	7	132	SURFnet, The Netherlands
33	AS17563	PK	402	117	359	207	64	199	Nexlinx, Pakistan
34	AS327724	UG	401	120	538	208	103	266	NITA, Uganda
35	AS7590	PK	400	122	329	266	84	224	COMSATS, Pakistan

Rank	AS	CC	Seen			Validating			As Name
			Before	During	After	Before	During	After	
1	AS2018	ZA	1,858	1,122	1,473	694	220	288	TENET, South Africa
2	AS10396	PR	1,789	1,673	1,988	1,647	276	33	COQUI-NET - DATACOM CARIBE, Puerto Rico
3	AS45773	PK	1,553	388	1,393	606	178	540	HECPERN-AS-PK PERN, Pakistan
4	AS15169	IN	1,271	438	1,286	1,209	438	1,242	GOOGLE - Google LLC, India
5	AS22616	US	1,264	503	1,526	883	377	1,014	ZSCALER- SJC, US
6	AS53813	IN	1,213	689	1,862	1,063	582	1,419	ZSCALER, India
7	AS1916	BR	1,062	94	991	326	37	277	Rede Nacional de Ensino e Pesquisa, Brazil
8	AS9658	PH	931	281	842	440	136	404	ETPI-IDS-AS-AP Eastern Telecoms, Philippines
9	AS37406	SS	888	486	972	582	365	599	RCS, South Sudan
10	AS263327	BR	882	345	438	776	289	359	ONLINE SERVICOS DE TELECOMUNICACOES, Brazil
11	AS17557	PK	835	430	777	431	277	413	Pakistan Telecommunication, Pakistan
12	AS36914	KE	834	476	937	583	354	670	KENET , Kenya
13	AS327687	UG	802	473	834	390	189	332	RENU, Uganda
14	AS680	DE	773	966	1,332	268	117	289	DFN Verein zur Foerderung, Germany
15	AS201767	UZ	761	538	729	461	200	371	UZMOBILE, Uzbekistan
16	AS37682	NG	695	401	728	593	274	568	TIZETI, Nigeria
17	AS7470	TH	674	214	507	219	94	182	True Internet, Thailand
18	AS51167	DE	670	378	479	214	78	156	CONTABO, Germany
19	AS15525	PT	600	260	593	287	125	284	MEO-EMPRESAS, Portugal
20	AS14061	GB	594	468	672	260	169	313	DigitalOcean, United Kingdom
21	AS37130	ZA	585	5	464	414	0	260	SITA, South Africa
22	AS30998	NG	583	264	484	192	54	143	NAL, Nigeria
23	AS135407	PK	569	227	457	419	207	344	TES-PL-AS-AP Trans World, Pakistan
24	AS16814	AR	565	235	456	258	120	208	NSS, Argentina
25	AS132335	IN	563	17	30	538	17	23	NETWORK-LEAPSWITCH-IN LeapSwitch Networks, India
26	AS5438	TN	559	532	579	526	171	27	ATI,Tunisia
27	AS5466	IE	547	240	401	419	184	329	EIRCOM Internet House, IE Ireland
28	AS18002	IN	538	467	614	277	176	242	WORLDPHONE-IN AS, India
29	AS37209	NG	532	109	438	269	45	194	HYPERIA, Nigeria
30	AS37100	ZA	454	161	401	168	95	131	SEACOM-AS, South Africa
31	AS5588	CZ	453	175	430	186	102	162	GTSCE GTS Central Europe, Czechia
32	AS1103	NL	446	38	363	189	7	132	SURFnet, The Netherlands
33	AS17563	PK	402	117	359	207	64	199	Nexlinx, Pakistan
34	AS327724	UG	401	120	538	208	103	266	NITA, Uganda
35	AS7590	PK	400	122	329	266	84	224	COMSATS, Pakistan

These networks
turned DNSSEC
validation off!

Impact of the KSK Roll

- The immediate impact appears to be some 0.2% - 0.3% of users
- In 33 cases service was restored with DNSSEC validation enabled
- In 2 cases DNSSEC validation was turned off

We were using WEIGHTED counts

- In order to compare one AS to another we ‘normalize’ the sample counts to align withg national user populations to correct for any skew in reporting
- For the sake of completeness here is the same thresholds applied to the ‘raw’ numbers

```
 Rank AS    CC   Seen                    Validating          Weight   As Name
                Before During After    Before During After

 1 AS9541   PK 10,201  4,953  6,273    4,651  2,644  2,773 0.480   CYBERNET-AP Cyber Internet Services (Pvt) Ltd., PK Pakistan
 2 AS38264  PK  6,001  2,464  3,123    2,794  1,309  1,443 0.480   WATEEN-IMS-PK-AS-AP National WiMAX/IMS environment, PK Pakistan
 3 AS45773  PK  4,736    732  2,568    1,850    336    996 0.480   HECPERN-AS-PK PERN AS Content Servie Provider, Islamabad, Pakistan, PK Pakistan
 4 AS22616  US  3,212  1,225  3,539    2,244    918  2,351 0.414   ZSCALER-SJC1 - ZSCALER, INC., US United States of America
 5 AS17557  PK  2,555    811  1,430    1,318    522    759 0.480   PKTELECOM-AS-PK Pakistan Telecommunication Company Limited, PK Pakistan
 6 AS9231   HK  2,056  1,300  3,277    1,973  1,277  3,193 0.211   IPEOPLESNET-AS-AP China Mobile Hong Kong Company Limited, HK Hong Kong
 7 AS5438   TN  1,745  1,924  2,082    1,646    717    100 0.291   ATI-, TN Tunisia
 8 AS135407 PK  1,742    429    845    1,282    391    636 0.480   TES-PL-AS-AP Trans World Enterprise Services (Private) Limited, PK Pakistan
 9 AS9658   PH  1,723    453  1,193      814    220    575 0.612   ETPI-IDS-AS-AP Eastern Telecoms Phils., Inc., PH Philippines
10 AS5466   IE  1,670    743  1,471    1,280    569  1,208 0.301   EIRCOM Internet House, IE Ireland
11 AS24691  TG  1,458    808  1,608      466    257    554 0.590   TOGOTEL-AS TogoTelecom, Togo, TG Togo
12 AS23956  BD  1,438    568  1,016      956    480    855 0.409   AMBERIT-BD-AS AmberIT Limited, BD Bangladesh
13 AS9381   HK  1,403    338  1,241      891    251    832 0.211   WTT-AS-AP WTT HK Limited, HK Hong Kong Special Administrative Region of China
14 AS10396  PR  1,383  1,110  1,320    1,272    248     20 1.433   COQUI-NET - DATACOM CARIBE, INC., PR Puerto Rico
15 AS37228  RW  1,262    279    909      398    117    241 1.291   Olleh-Rwanda-Networks, RW Rwanda
16 AS17563  PK  1,225    222    663      632    121    368 0.480   NEXLINX-AS-AP Autonomous System Number for Nexlinx, PK Pakistan
17 AS7590   PK  1,218    231    606      810    160    413 0.480   COMSATS Commission on Science and Technology for, PK Pakistan
18 AS15964  CM  1,159    583  1,868      464    241    731 1.376   CAMNET-AS, CM Cameroon
19 AS37425  SO  1,148    957  1,114      521    343    517 0.069   Somcable, SO Somalia
20 AS45588  BD  1,013    444    776      517    188    350 0.409   BTCL-ISP-AS Bangladesh Telecommunications Company (BTCL), Nationwide, BD Bangladesh
21 AS38026  BD    961    203    671      355     68    241 0.409   MNBL-TRANSIT-AS-AP MetroNet Bangladesh Limited,, BD Bangladesh
22 AS5408   GR    959    180    937      421     86    376 0.080   GR-NET http://www.grnet.gr, GR Greece
23 AS24435  PK    926    222    466      485    141    254 0.480   SUPERNET-PAKISTAN-AS-AP Supernet Limited Transit Autonomous System Number, PK Pakistan
24 AS15525  PT    861    382    827      413    184    396 0.714   MEO-EMPRESAS, PT Portugal
25 AS31313  RO    829     27    453      323     14    159 0.389   STS Bucharest, 323A Splaiul Independentei,Sector 6,060044,Romania, RO Romania
26 AS25605  US    823    234    924      302     91    376 0.414   SCANSAFE - SCANSAFE SERVICES LLC, US United States of America
27 AS9387   PK    815    327    399      275    113    156 0.480   AUGERE-PK AUGERE-Pakistan, PK Pakistan
28 AS45326  BD    799    199    637      269    109    222 0.409   BBTS-AS-AP Broad Band Telecom Services Ltd, BD Bangladesh
29 AS38713  PK    780    200    474      401     96    243 0.480   CONNECT2B-AS-PK Broadband ISP, FTTH and Cable Service Provider, PK Pakistan
30 AS38229  LK    766    428    640      324    210    263 0.302   LEARN-LK Lanka Education & Research Network, NREN, LK Sri Lanka
31 AS21219  UA    738    422    591      389    250    325 0.570   DATAGROUP, UA Ukraine
32 AS5588   PL    735    239    550      274     59    121 0.538   GTSCE GTS Central Europe / Antel Germany, CZ Czech Republic
33 AS17911  PK    719    169    346      488    139    240 0.480   BRAINPK-AS-AP Brain Telecommunication Ltd., PK Pakistan
34 AS4922   US    712    523    635      517    310    374 0.414   SHENTEL - Shentel Communications, LLC, US United States of America
35 AS7470   TH    706    244    604      230    107    218 0.876   TRUEINTERNET-AS-AP TRUE INTERNET Co.,Ltd., TH Thailand
36 AS4515   HK    680    238    552      272    113    256 0.211   ERX-STAR HKT Limited, HK Hong Kong Special Administrative Region of China
```

Rank	AS	CC	Seen			Validating			Weight	As Name
			Before	During	After	B	D	A		
37	AS17469	BD	660	185	549	226	63	176	0.409	ACCESSTEL-AS-AP Access Telecom (BD) Ltd., BD Bangladesh
38	AS17494	BD	658	141	521	336	69	280	0.409	BTTB-AS-AP Telecom Operator & Internet Service Provider as well, BD Bangladesh
39	AS53813	US	636	194	580	513	171	487	0.414	ZSCALER-INC - ZSCALER, INC., US United States of America
40	AS40285	US	625	420	502	515	229	306	0.414	NORTHLAND-CABLE - NORTHLAND CABLE TELEVISION INC., US United States of America
41	AS1955	HU	624	290	548	275	118	217	0.521	HBONE-AS HUNGARNET, HU Hungary
42	AS23473	US	621	342	439	566	296	388	0.414	PAVLOVMEDIA - PAVLOV MEDIA INC, US United States of America
43	AS55501	PK	619	205	336	480	181	263	0.480	CONNECTEL-PK 141-143 Maulana Shaukat Ali Road, PK Pakistan
44	AS38511	ID	602	345	671	331	196	375	0.464	TACHYON-AS-ID PT Remala Abadi, ID Indonesia
45	AS58923	BD	547	137	449	316	92	218	0.409	INTERCLOUDLTD-AS-AP InterCloud ltd, BD Bangladesh
46	AS12578	LV	531	188	474	257	126	229	0.550	APOLLO-AS Latvia, LV Latvia
47	AS36879	DZ	528	271	478	176	101	151	0.086	SLC1-AS, DZ Algeria
48	AS38203	BD	523	150	357	346	117	249	0.409	ADNTELECOMLTD-BD ADN Telecom Ltd., BD Bangladesh
49	AS17747	IN	523	299	1,152	390	199	729	3.080	SITINETWORS-IN-AP SITI NETWORKS LIMITED, IN India
50	AS9832	BD	518	167	449	234	83	200	0.409	ISN-AS-AP ISN, Internet Service Provider, BD Bangladesh
51	AS24556	BD	513	125	437	235	64	219	0.409	BIJOY-BD-AS-AP Bijoy Online Ltd. , BD Bangladesh
52	AS680	DE	504	799	987	172	93	212	1.385	DFN Verein zur Foerderung eines Deutschen Forschungsnetzes e.V., DE Germany
53	AS2018	ZA	500	223	367	191	55	70	4.147	TENET-1, ZA South Africa
54	AS55406	BD	494	143	381	292	82	244	0.409	HRCTECH-01-AS-AP 26 Shyamoli, Bir Uttam A. W., BD Bangladesh
55	AS17547	SG	487	182	482	342	149	344	0.323	M1NET-SG-AP M1 NET LTD, SG Singapore
56	AS9441	BD	480	283	428	308	202	285	0.409	NEXT-BD Next Online Limited., BD Bangladesh
57	AS3326	UA	467	257	427	302	189	302	0.570	AS3326-BLINKING-MEGABIT AS3326-BLINKING-MEGABIT, UA Ukraine
58	AS62044	FR	463	73	431	385	68	344	0.630	ZSCALER-EMEA, CH Switzerland
59	AS5588	CZ	462	193	448	190	113	169	0.955	GTSCE GTS Central Europe / Antel Germany, CZ Czech Republic
60	AS16178	BA	459	214	386	290	178	236	0.202	LOGOSOFT-AS Logosoft d.o.o., BA Bosnia and Herzegovina
61	AS9821	PH	458	66	405	151	29	112	0.612	DOST-PH-AP Department of Science and Technology, PH Philippines
62	AS30990	DJ	448	268	449	356	214	385	0.442	ADJIB-AS, DJ Djibouti
63	AS22709	US	446	217	328	359	199	241	0.414	NSTELCO - North State Telephone Co., US United States of America
64	AS16814	AR	445	168	362	205	86	164	1.342	NSS S.A., AR Argentina
65	AS9557	PK	442	87	281	157	40	90	0.480	PKTELECOM-AS-PK Paknet Limited Merged into PTCL, PK Pakistan
66	AS12764	KG	433	320	501	186	122	225	1.501	AKNET-AS, KG Kyrgyzstan
67	AS51167	DE	430	301	353	141	62	116	1.385	CONTABO, DE Germany
68	AS133443	BD	427	248	338	278	177	235	0.409	COMILLA-AS-AP Comilla Online, BD Bangladesh
69	AS16657	US	420	88	253	140	28	36	0.414	FIBERTECH-NETWORKS-AS-ROC-NY-US - Fibertech Networks, LLC, USA
70	AS15169	IN	408	107	607	384	107	587	3.080	GOOGLE - Google LLC, US United States of America
71	AS20412	US	405	222	246	340	181	185	0.414	CLARITY-TELECOM - Clarity Telecom LLC, US United States of America

Lessons Learned

- Yes, we can roll the KSK!
- Yes, the extensive contact campaign helped
- Yes, we should now look at an Elliptical Curve algorithm roll
- Yes, we should now look at backup KSK provision
- Yes, we should review both RFC 8145 and Key Sentinel and improve them or kill them off
- Maybe, we should look at a KSK bootup chain to automate synching old KSK configs into current production state

Keep It Rolling

Maybe we just need to keep rolling every year

- That way we train the manual loaders to keep up!

Thanks!