DNS Observatory: Monitoring Global DNS for Performance and Security

Paweł Foremski

Farsight Security / IITiS PAN
pjf@fsi.io

Oliver Gasser

Technical University of Munich
gasser@net.in.tum.de

The telescope: top-N in passive DNS

- ~200K/sec passive DNS cache miss traffic
- Diverse set of resolvers world-wide
- Completely new machinery vs. DNSDB
- Tracking only the top-N objects
- 1 min -> 10 mins -> 1 hour -> 1 day -> 1 month

This talk: Jan-Mar 2019 (>1 trillion DNS queries)

Goal: preview + what would you like to see?

The galaxies: tracked DNS objects

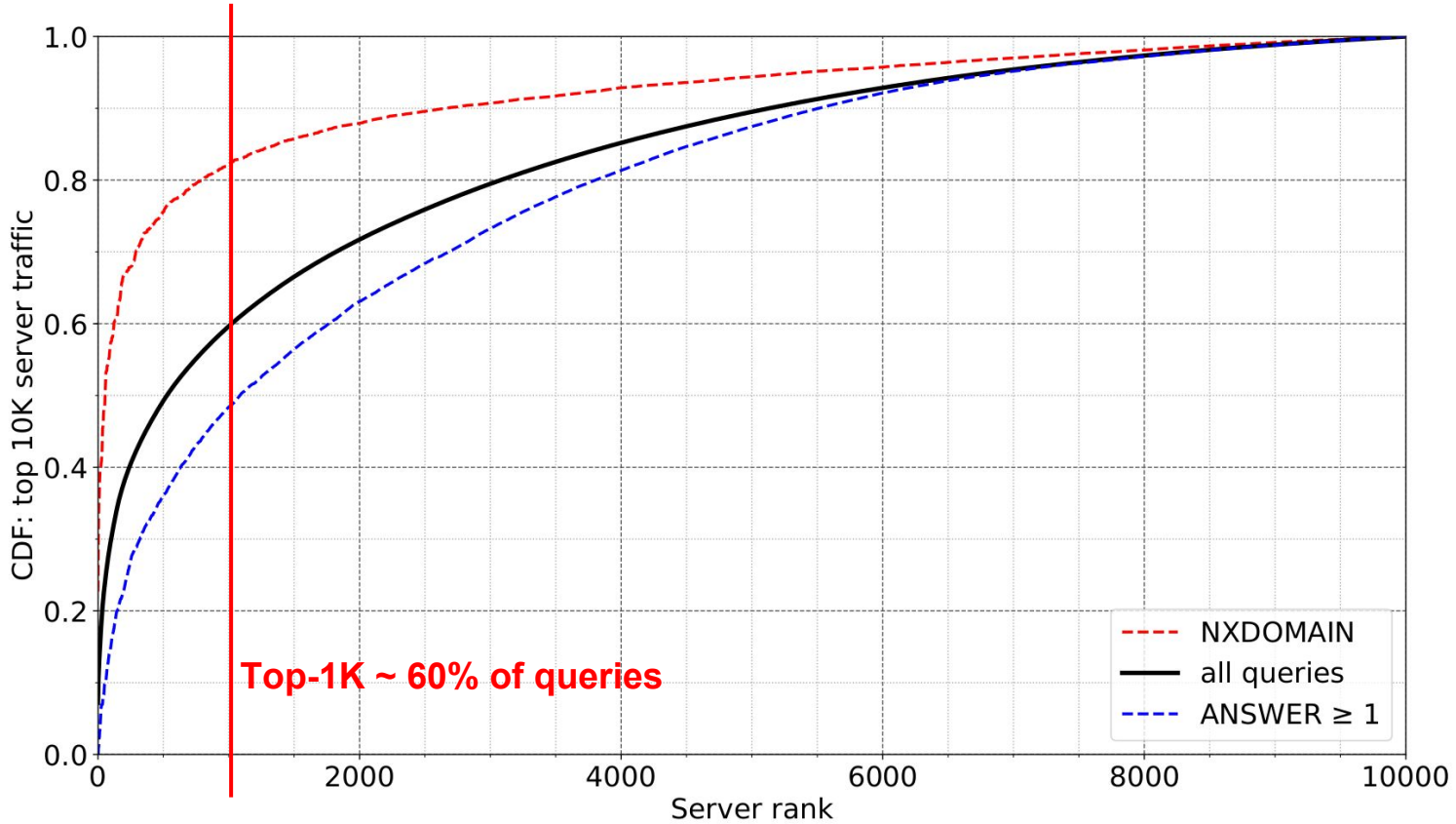
- Authoritative DNS servers
  (aggregated by IP address)
- Effective TLDs (Public Suffix List)
- Effective Second-Level Domains
- Fully-Qualified Domain Names
- QTYPE values (A, AAAA, MX, RRSIG, …)
- IPv4 and IPv6 answers (A, AAAA, ANY)

~Top-10K for each minute

NASA / ESA (public domain)

The stars: traffic features

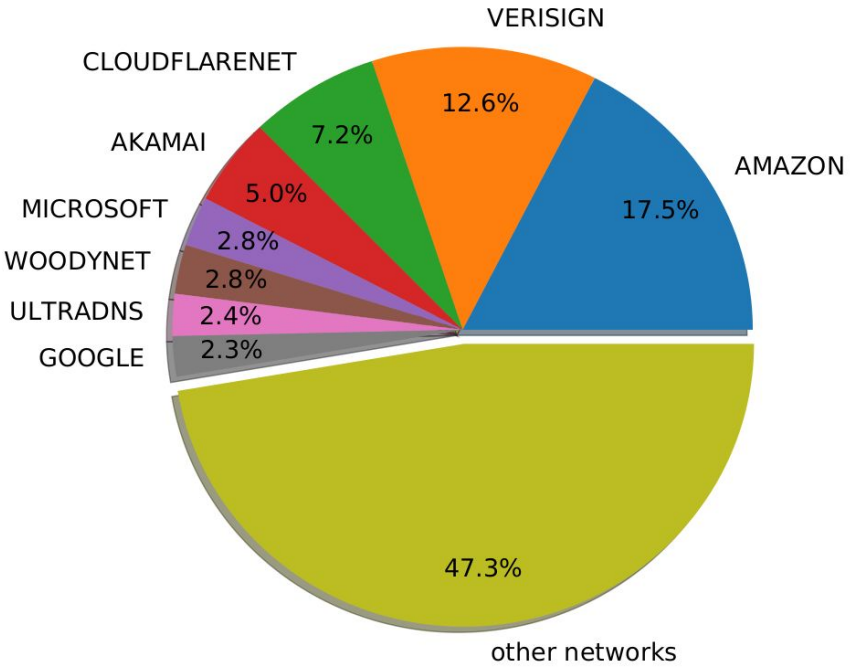
- 30+ features per each object, e.g.
  - **Counters of DNS queries and responses**: all, answered, SUCCESS, NXDOMAIN, non-empty ANSWER, NS records in AUTHORITY, DNSSEC-signed, empty AAAA answers, etc.
  - **Cardinality estimates** (incl. HyperLogLog): number of distinct FQDNs, TLDs, SLDs, QTYPEs, IP addresses seen in ANSWER, auth. server IPs
  - **Histogram estimates** (percentiles, top-k, means): server response delay, number of network hops, response size, record TTLs, est. hierarchy level



Q1 2019 Top-10k servers: DNS traffic distribution

FARSIGHT SECURITY

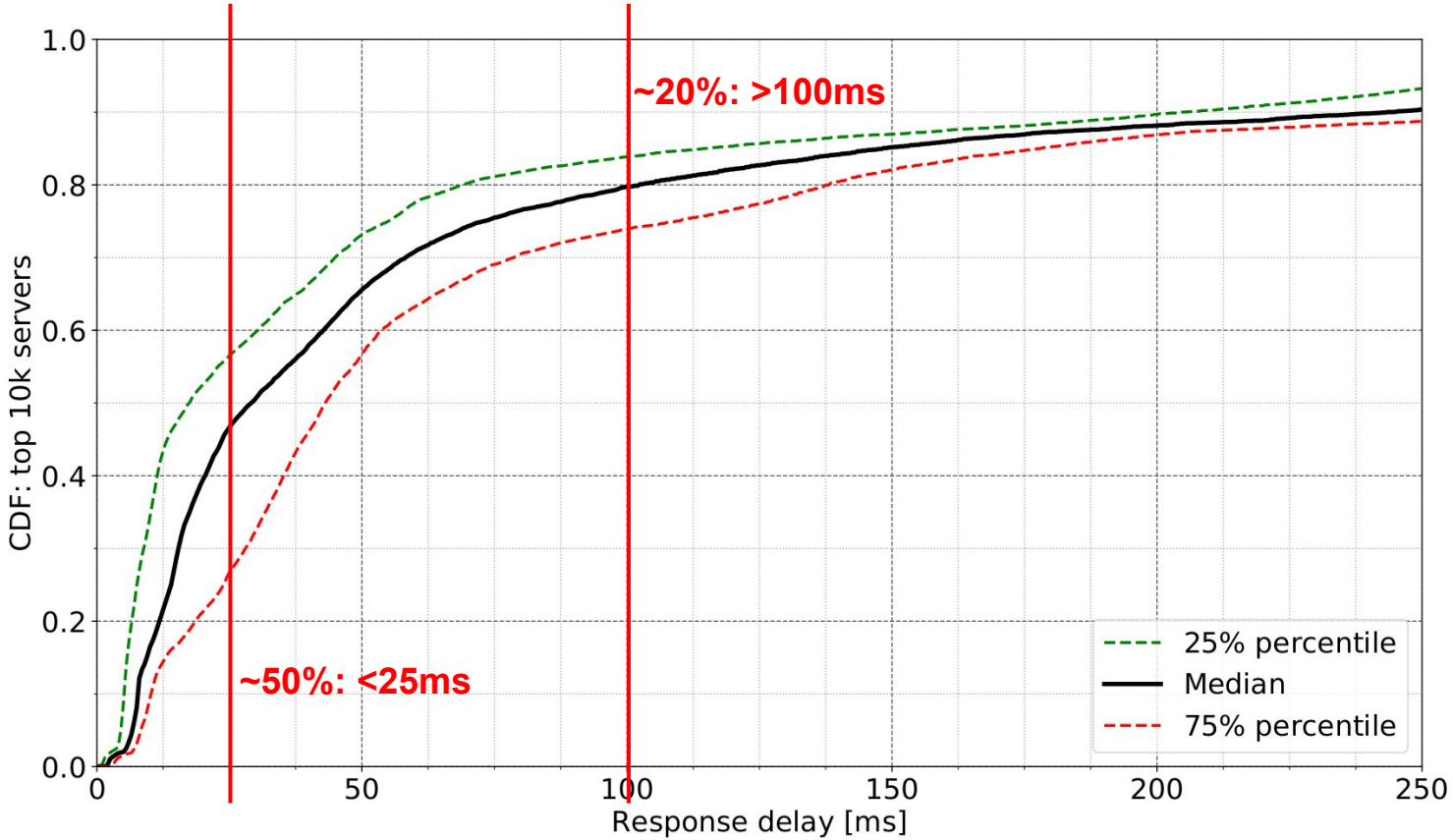
Is DNS *really* distributed in practice?



DNS queries

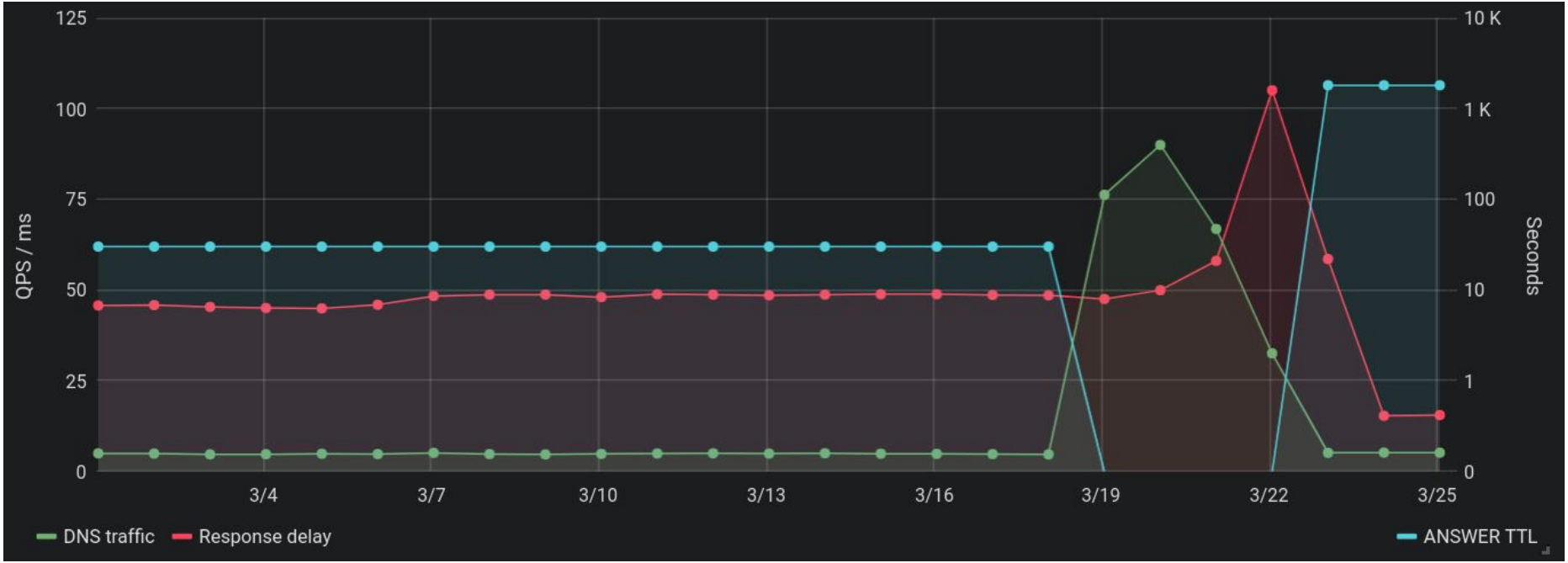
Q1 2019 Top-10k servers

FARSIGHT SECURITY



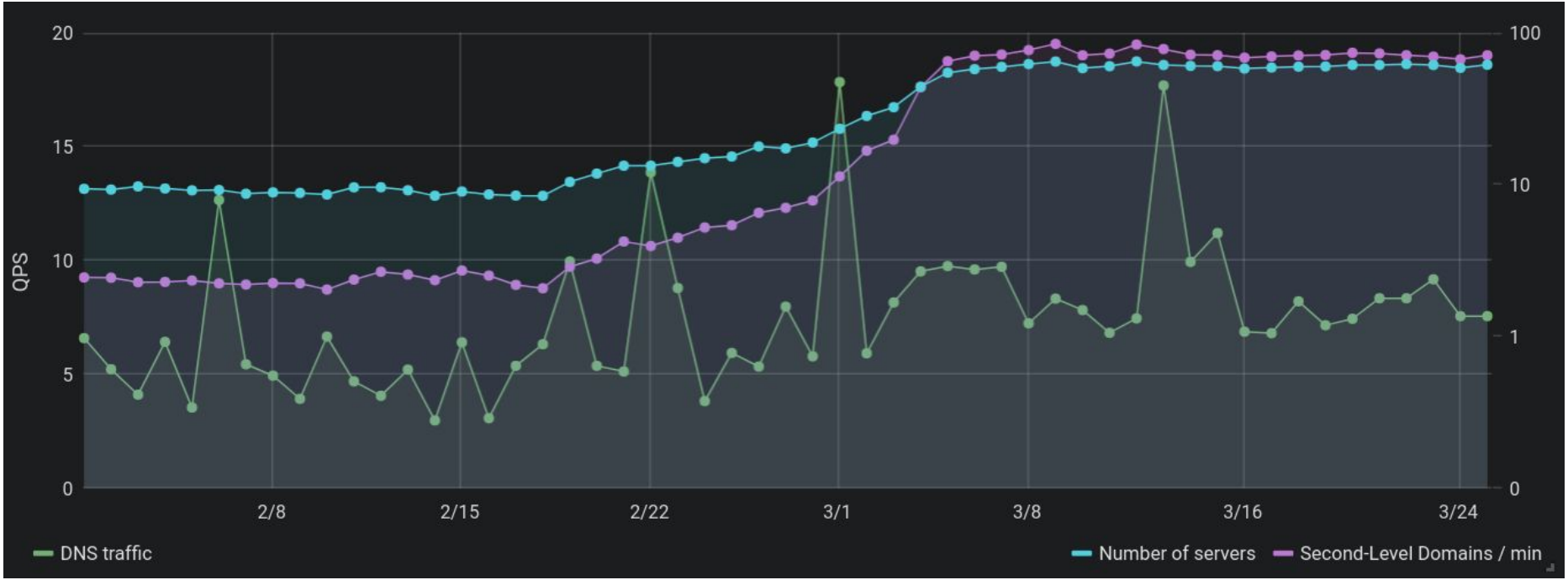
Median response delay

1 server == 1 IP address; 20% space for improvement; popular servers are faster (less hops), but…



Playing with TTLs: large hardware vendor (a .com SLD)

...plus added a few servers to accomodate more traffic



A new shiny gTLD

Spikes show big days, but new domains didn't bring more traffic (yet)

Happy Eyeballs + Negative Caching

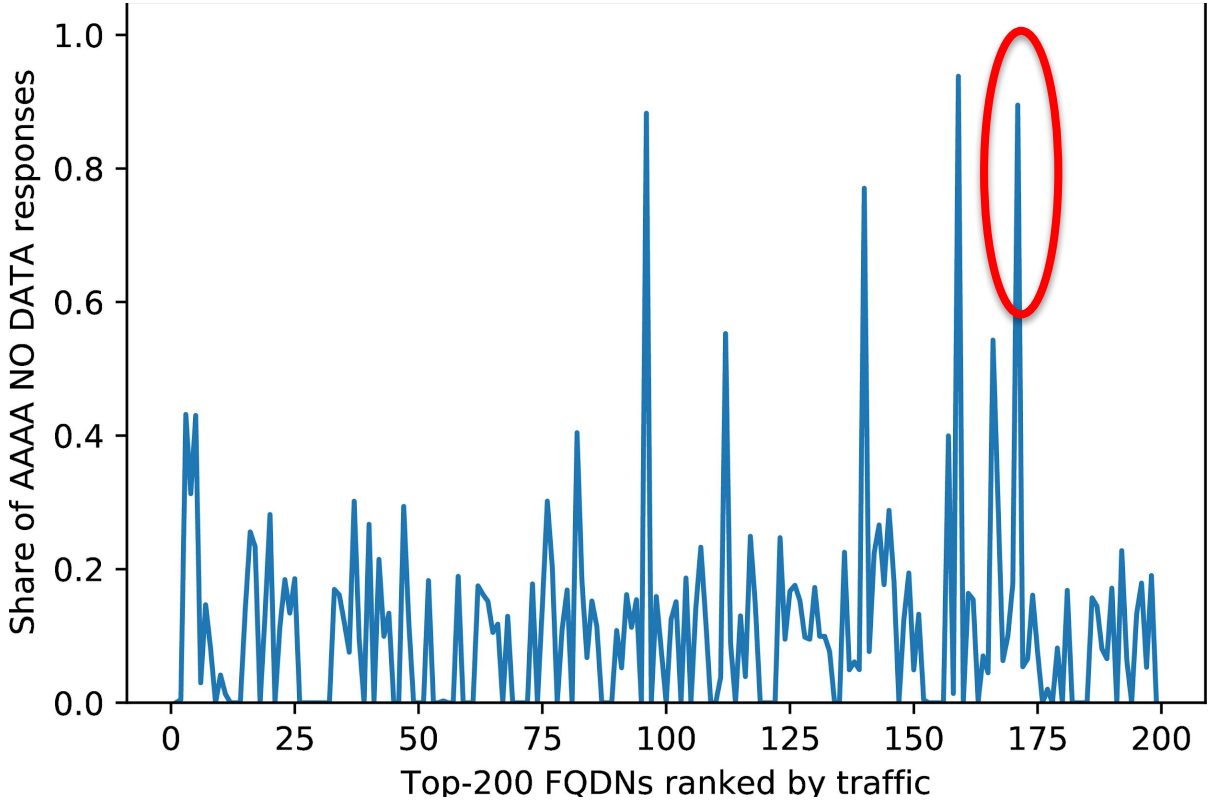
- Happy Eyeballs (RFC 8305)
  - Send A and AAAA queries for each domain name
  - Results in a lot of AAAA queries at name servers, also for v4-only domains

- Negative caching
  - Regular DNS RR are sent with a TTL for caching purposes
  - Negative responses (NXDOMAIN or NO DATA) use SOA's negative caching TTL

- Some ISP resolvers do not cache NO DATA AAAA responses at all

- Some FQDNs have a very large percentage of NO DATA AAAA responses

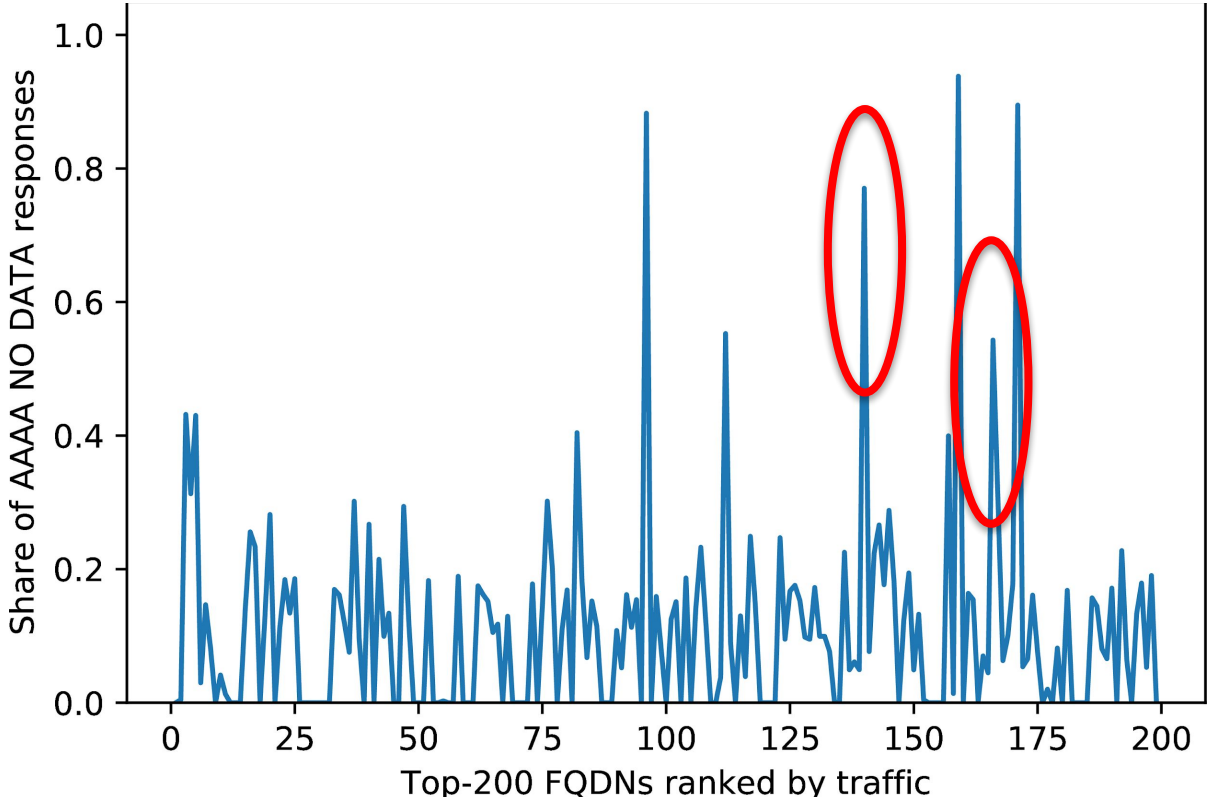
Happy Eyeballs + Negative Caching



CDN for OS updates

- A RR TTL of 1 hour
- Negative caching TTL of 15 minutes
- 89% of all responses are AAAA NO DATA

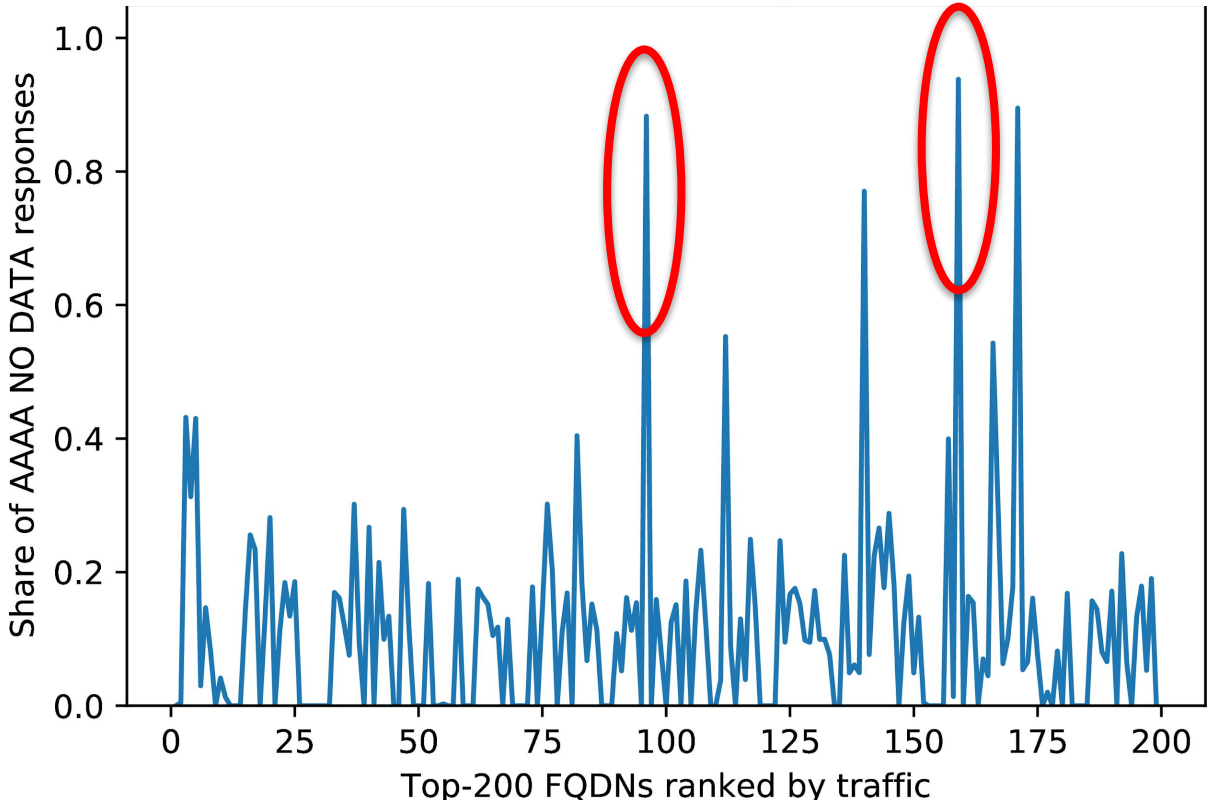
Happy Eyeballs + Negative Caching



Ad server

- A RR TTL of 5 minutes
- Negative caching TTL of 60 seconds
- 66% of all responses are AAAA NO DATA

Happy Eyeballs + Negative Caching



OS time server

- A RR TTL of 15 minutes
- Negative caching TTL of 15 seconds
- 90% of all responses are AAAA NO DATA

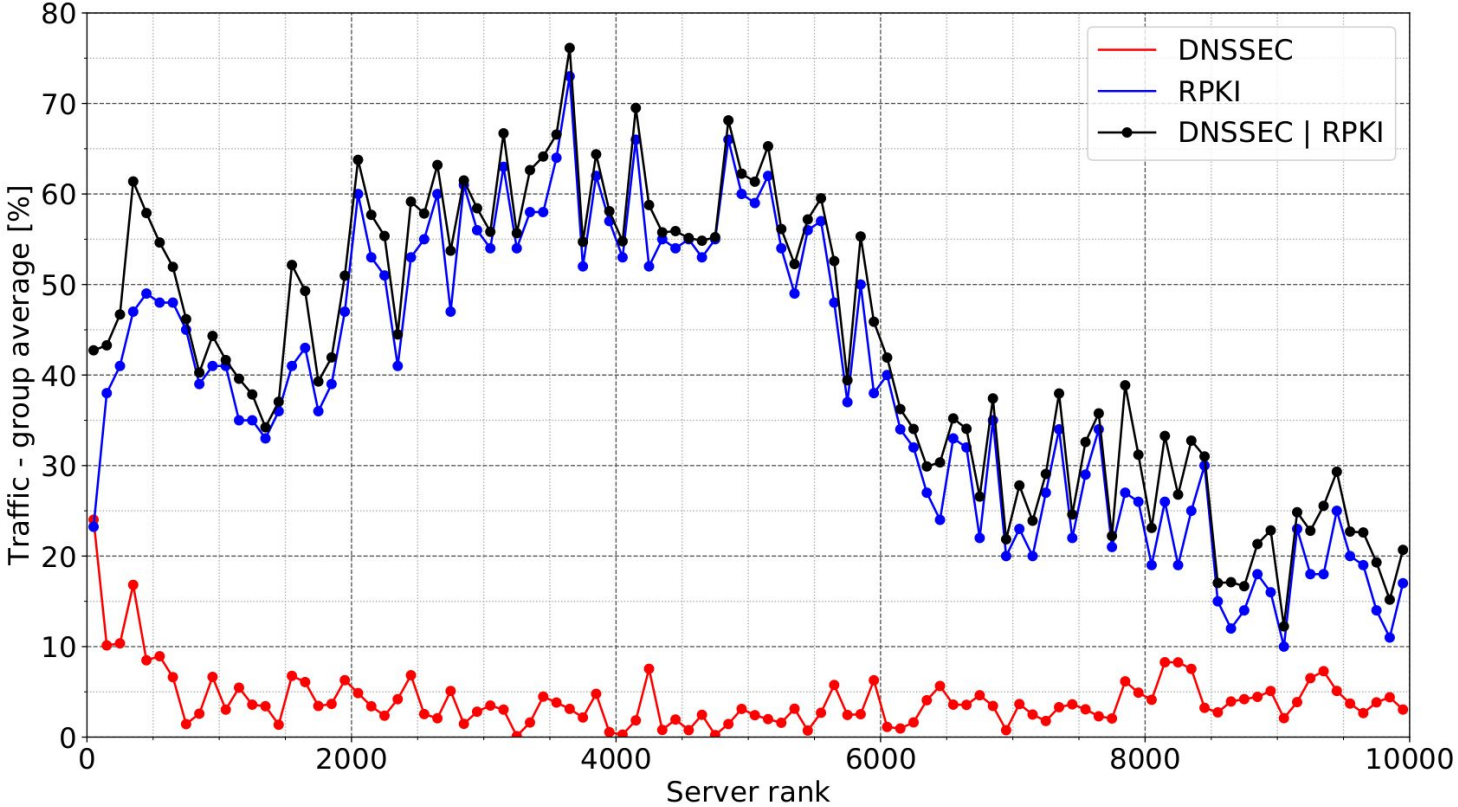
DNSSEC and RPKI

https://www.zdnet.com/article/iranian-hackers-suspected-in-worldwide-dns-hijacking-campaign/

In April 2018, we detailed a brazen BGP hijack of Amazon's authoritative DNS service in order to redirect users of a crypto currency wallet service to a fraudulent website ready to steal their money.

In the past month, we have observed additional BGP hijacks of authoritative DNS servers with a technique similar to what was used in April. This time the targets included US payment processing companies.

https://dyn.com/blog/bgp-dns-hijacks-target-payment-systems/



Top-10K DNS server security: DNSSEC, RPKI, and both combined

DNSSEC server/traffic adoption: 4% / 16%; RPKI: 39% / 36%; DNSSEC|RPKI: 44% / 49%

Dots are groups of 100 IPs. See also: https://stats.labs.apnic.net/dnssec/XA?c=XA&x=1&g=1&r=1&w=7&g=0

FARSIGHT SECURITY

DNS Observatory

- Provides aggregated view of global DNS in time
- Top DNS infrastructure need more work on performance & security
- Interested in getting the data? Drop us an email.

Paweł Foremski

Farsight Security / IITiS PAN

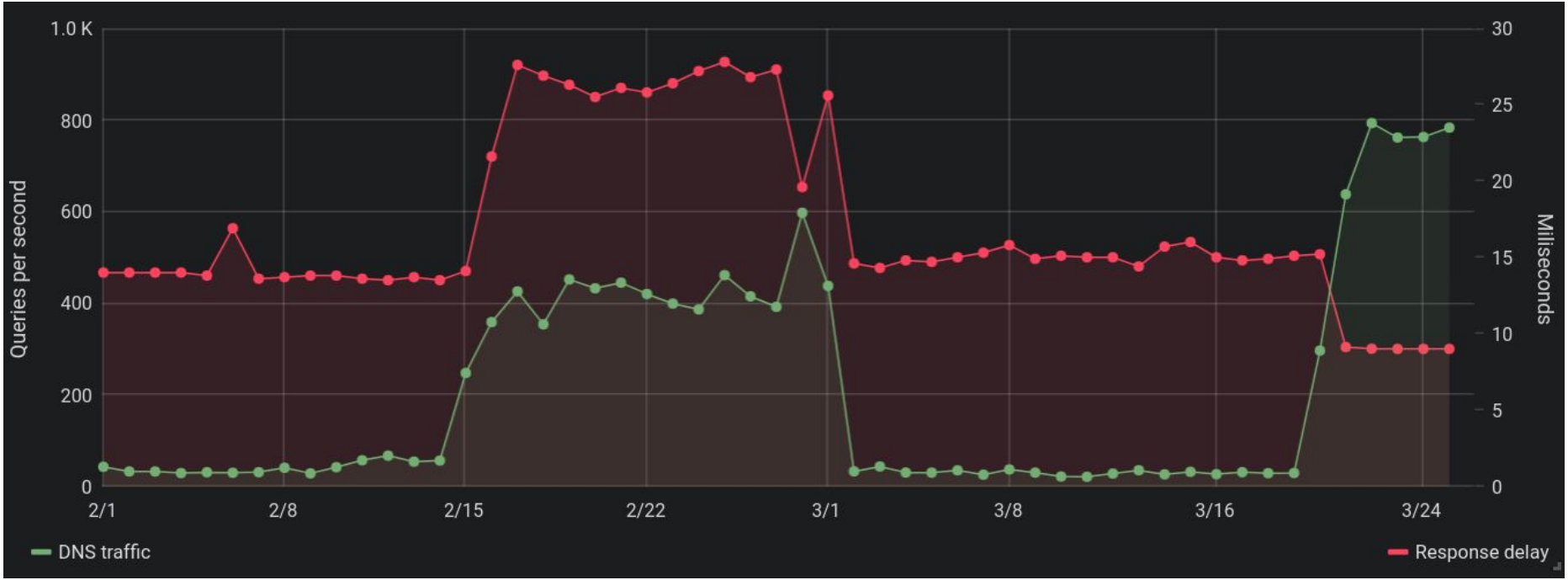
pjf@fsi.io @pforemski

Oliver Gasser

Technical University of Munich

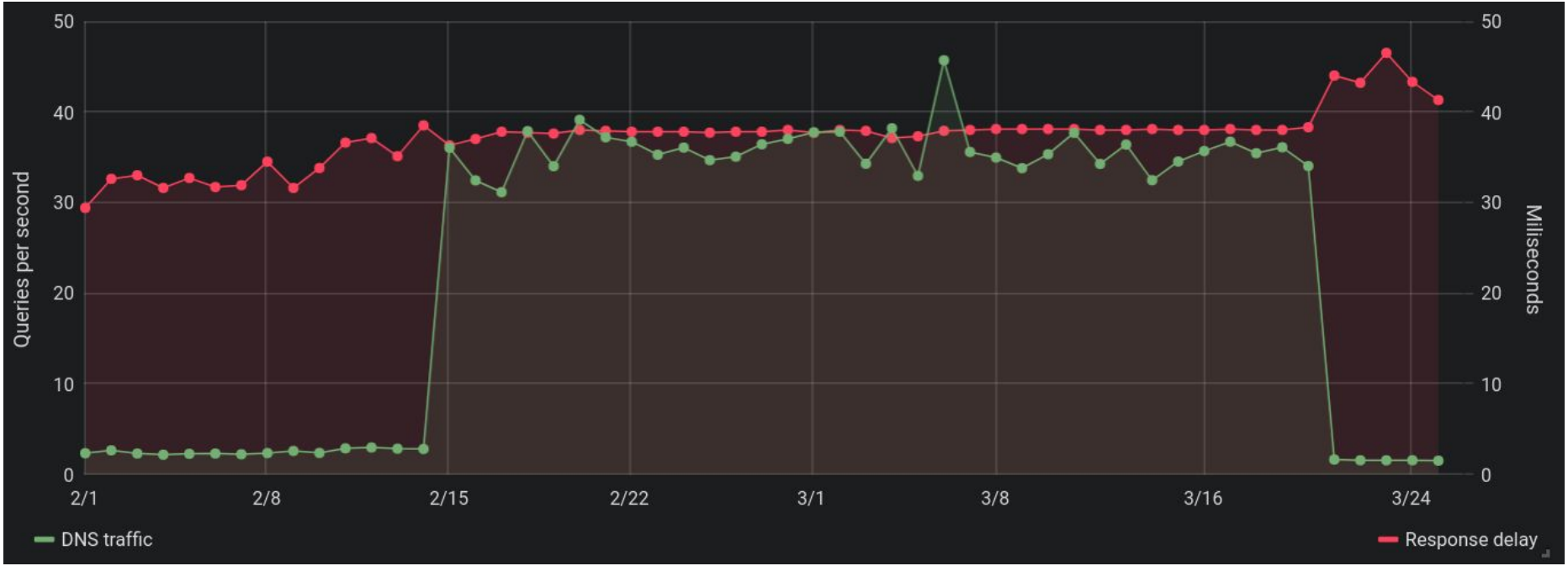
gasser@net.in.tum.de

Backup slides



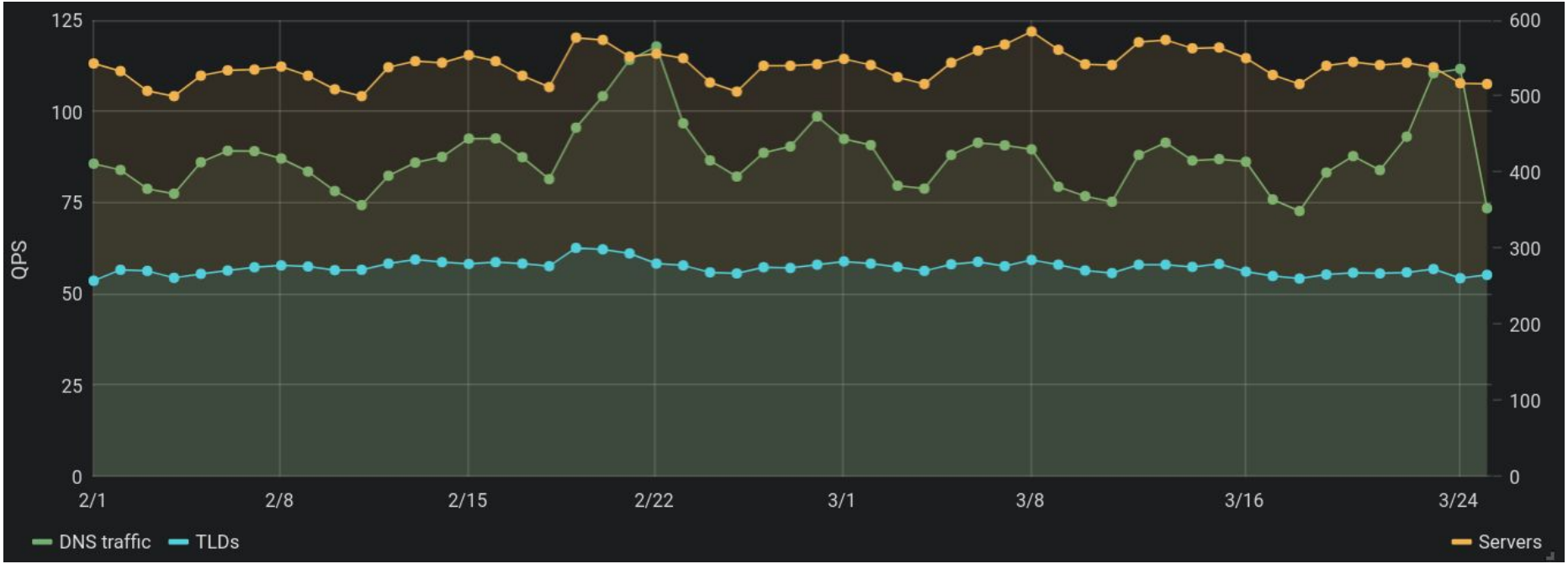
Feb/March for a specific ccTLD server

Feb 2019: traffic means delay / Mar 2019: success



Server on/off: another ccTLD

+median response delay increased



World's 2nd most frequently seen IPv4 address in DNS is…? ;-)

1st is a VOD anycast

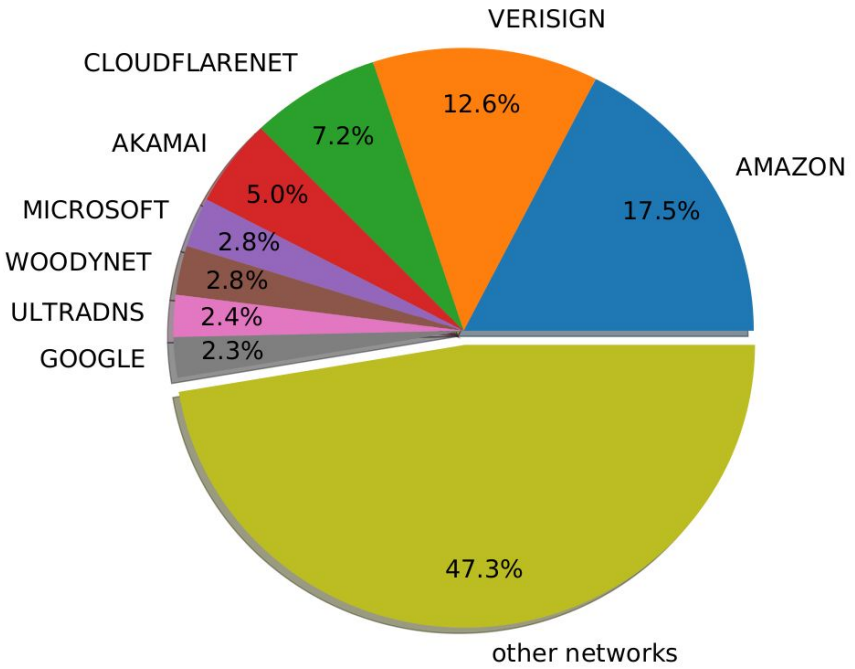
	B	F	G	I	L	M	O	P	S	T	U	V	X	Y	Z	AA	AB	AC	AD
1	server	hits	unans	nxd	ok_ans	ok_ns	ok_nil	ok_sec	qnamesa	qtypes	tlds	eslds	ip4s	ip6s	lvl	nslvl	resp_delays	network_hops	resp_size
2	192.33.1	507631	64.1	292447	58.5	200969	14150	158391	258347	15.8	4.01	148956	0	0	1.91	2	5.58|8.07|15.0	6.00|7.00|8.02	236|665|1006
3	193.232.	69879	43.6	17444	122	50423	1968	35575	46378	15.1	6.32	27758	10.7	2.24	3.93	2	4.42|6.91|8.01	6.00|7.00|8.60	385|609|824
4	199.7.83	52349	23.8	50887	21.4	1324	87.1	487	41032	13.6	437	1028	0	0.02	0.35	1	2.95|5.27|8.00	5.00|6.00|7.04	117|463|991
5	194.146.	46989	50	44476	3.94	2448	10.3	2150	46540	8.86	1.37	1767	0.08	0.07	1.91	2	8.00|9.00|10.1	8.00|9.89|11.6	945|998|1021
6	216.239.	36423	74.4	1852	29777	278	3538	0	19507	13	138	276	6611	3360	3.62	3.08	14.8|18.3|24.0	19.0|21.1|23.1	80.4|106|117
7	216.239.	35326	79.1	1768	28874	277	3424	0	19062	12.9	132	268	6482	3327	3.63	3.08	15.4|18.7|29.4	18.1|20.9|23.2	80.4|106|117
8	204.61.2	33641	24.7	12523	20.9	20039	1035	15637	27444	8.15	1	57.3	0	0	2.29	3.86	37.7|39.8|42.0	5.95|7.40|9.84	303|334|727
9	88.221.8	31389	19.7	0.21	30059	0	1310	0	5337	6	1	5.21	9232	2684	4.01	?	14.3|30.2|47.2	4.00|5.00|6.00	67.1|71.0|82.2
10	205.251.	30491	11.9	393	19854	19871	10205	0	4087	7.64	7.4	36.1	7594	206	5	3.98	12.9|20.8|32.7	7.00|8.03|9.03	172|255|288
11	184.85.2	27195	23.1	90.2	22132	0	4949	0	2534	7.23	1	1	1916	19.6	5.33	?	15.6|22.0|25.0	4.80|5.99|7.02	82.2|106|125
12	205.251.	26171	149	339	16314	16319	9360	0	4062	7.68	9.57	40.6	7113	222	4.99	3.96	16.3|28.6|33.2	7.00|8.00|9.81	171|253|281
13	205.251.	26113	14.2	338	16394	16396	9364	0	3960	7.33	4.18	29.3	7164	210	5	3.98	6.25|12.7|28.7	7.00|8.00|9.01	171|253|281
14	69.171.2	25942	49.1	77.5	25039	25039	776	0	3608	4.28	2	5.58	3207	1566	4.44	2.89	18.9|25.1|36.8	7.15|31.8|40.3	196|199|206
15	69.171.2	25805	53.2	76.8	24901	24901	774	0	3604	4.28	2	5.62	3200	1564	4.44	2.89	14.3|23.0|35.7	7.28|32.1|39.0	196|199|206
16	192.71.5	25611	0.77	25243	0.36	366	0.8	317	25577	5.75	1.13	300	0.01	0.03	1.71	2	7.07|8.11|9.41	5.00|6.00|8.00	999|1037|1052
17	205.251.	25047	96.5	321	15485	15489	9126	0	3929	7.21	5.42	26.5	6955	198	5.01	3.98	6.39|12.9|20.6	7.18|8.59|10.2	171|252|279
18	192.38.7	24416	0.93	23871	0.09	542	1.14	402	24373	6.66	1.03	439	0.02	0.02	2.07	2	15.2|17.9|19.9	4.82|5.94|9.64	1197|1332|1401
19	192.58.1	23901	26.3	23349	18.4	477	30.1	166	21295	11.7	217	376	0	0.01	0.24	1	6.79|22.6|66.8	6.00|7.37|8.37	116|126|759
20	192.203.	22976	56.7	22190	73	626	30.5	377	20604	11.5	213	492	0.02	0.01	0.07	1	4.84|7.29|9.96	4.49|6.04|8.11	116|125|688
21	199.249.	21802	31.8	15170	5.78	6329	267	3630	12101	12	2.22	4714	1.38	0.02	1.68	2	32.1|39.1|41.6	6.10|7.24|9.44	113|684|1007
22	199.249.	20709	33.8	14392	5.73	6021	258	3338	11638	12	2.23	4506	1.28	0.02	1.62	2	31.1|38.8|41.7	6.06|7.17|9.61	109|666|1006
23	192.35.5	19896	73.5	4858	2.44	14620	344	5239	18782	11.8	3.74	13716	0	0	1.48	2	26.0|38.3|61.3	6.22|7.72|8.87	143|252|570
24	192.42.9	19862	66.5	4545	2.62	14893	357	5496	18725	11.8	3.76	13968	0	0	1.48	2	25.9|38.0|61.1	6.14|7.60|8.69	140|253|574
25	192.12.9	19681	78.4	4934	2.43	14325	344	4960	18576	11.8	3.76	13432	0	0	1.45	2	26.0|38.7|61.5	6.22|7.74|8.89	142|244|565
26	216.239.	18347	77.8	615	14713	255	1636	0	11396	11.2	166	273	3461	2306	3.74	3.02	23.6|42.6|49.8	17.7|19.0|20.0	75.2|94.1|116
27	194.146.	18129	24.8	12824	1.02	5261	18.6	5026	17510	7.18	1.29	4117	0.57	0.11	2.45	2.01	8.00|9.01|10.2	8.00|10.1|12.4	1054|1191|1327
28	216.239.	17578	28.6	571	14094	255	1581	0	11090	11	164	269	3234	2228	3.75	3.02	17.1|29.6|38.0	17.6|19.0|20.0	75.2|93.8|116
29	204.61.2	17227	12.1	3664	14.4	13116	431	10580	15652	7.89	1.99	90.2	3.04	2.29	3.26	3.43	34.4|39.6|41.9	6.09|7.47|10.2	300|338|400
30	13.107.1	17064	39.4	1465	11043	1.83	4514	0	3046	7.61	5	15	1939	32.3	3.49	3.99	28.4|42.4|50.5	8.18|9.25|10.3	75.0|86.2|134

Sample: Top-30 nameservers (subset)

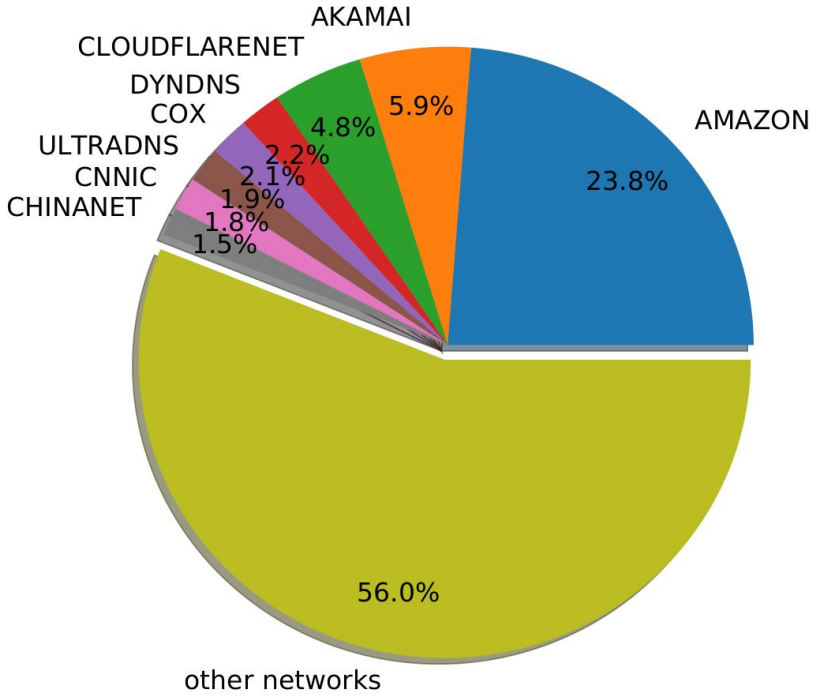
eTLD	srvips	hits	unans	nxd	rfs	fail	ok_ans	ok_ns	ok_add	ok_nil	ok_sec	ok6	ok6nil	qnamesa	qtypes	eslds	qnames	ip4s	ip6s	lvl	nslvl
.com	61693	3549339	183761	473661	209777	20909	1725563	1261262	403869	587169	160532	843753	525172	843638	27.5	263847	616726	255056	29642	3.57	2.44
.net	25506	1709317	61308	111263	34809	13410	1151387	516708	167486	241006	31717	402705	226705	255252	20.9	34192	208154	117283	42866	4.09	2.62
.in-addr.arpa	20241	477099	44870	123417	74626	10014	97993	192033	52666	4020	54640	40	15.7	204969	9.91	222	118047	1.57	0	5	3.64
.org	10870	211318	17309	53039	13565	1304	75944	49085	17834	26321	9619	35829	22744	52647	20.2	16761	31783	16928	2140	3.32	2.09
.biz	2275	63482	5882	35939	1891	72	11694	7862	2581	3011	3633	4220	2397	17312	10.9	4083	6924	3928	839	2.64	2.07
.nl	1787	61828	1343	49862	434	10.2	4997	5631	3618	853	4866	1610	683	53287	10.5	2737	3575	2446	150	2.92	2.01
.info	3292	61525	4921	16909	4211	150	20663	11811	2740	8055	3595	9875	6839	19093	12.8	6855	10409	5836	1107	2.69	2
.se	931	55284	202	49551	644	9.76	2552	2908	1610	503	1777	902	435	50954	10.6	1191	1724	943	83	3.03	2.09
.tv	2068	52218	1610	557	824	33	42314	22805	1646	4115	824	16070	3837	10265	8.95	1564	9499	7760	4657	3.6	2.59
.io	2671	52065	340	2397	3074	17.7	36983	32167	550	5907	846	11701	5456	7884	11.3	2158	6458	4842	779	3.4	2.22
.it	2654	48585	302	25767	360	114	10453	13613	5345	1785	8450	2068	1236	33028	9.95	6950	9582	3773	62.6	2.9	2.01
.me	1737	46973	1050	25411	1026	15.5	12914	7355	1134	4452	800	6166	3983	9633	9.98	2191	4851	2869	480	2.9	2.03
.cn	1347	43254	5189	7346	6019	32.8	14426	14281	2713	3959	4874	5091	3032	15031	9.8	5095	7088	3413	49.5	3.07	2.05
.be	787	37277	536	27746	209	3.58	6828	6641	951	694	1105	1037	583	33560	10.7	931	5854	718	62.1	4.55	2.58
.cz	764	37234	282	27285	208	2.89	6452	3744	3099	531	2393	1031	459	29164	11.4	1329	1911	1211	107	3.53	2.03
.edu	2990	36917	15706	5845	1040	358	7331	6538	4974	3634	1095	4905	3383	10277	11.6	1261	6213	2833	76.7	3.45	2.39
.de	3339	36033	676	2050	890	186	18592	20619	7287	3341	8228	4965	2763	15833	14.2	7270	14549	6213	373	3.61	2.25
.in	1317	35548	2163	25405	631	12.5	4023	4366	1043	1213	1407	1522	1009	7184	8.78	1584	2271	1189	76.8	2.93	2.04
.dk	679	32464	238	27183	410	96.6	2570	2395	1069	487	1096	715	428	29283	10.2	1376	2109	1121	39.5	3.29	2.04
.xyz	1430	31122	941	11033	3162	102	9543	5612	696	2018	3120	3996	1281	11984	16.7	4206	5199	2978	1276	2.26	1.99
.cc	1016	30171	821	22750	360	126	3952	2819	275	1376	411	1684	1055	5961	9.9	884	1505	962	179	2.75	1.99
.top	817	29247	1278	12370	4151	3.02	5330	5710	341	1470	3970	1936	770	11400	8.13	3304	4353	1792	285	2.35	1.97
.us	1960	27582	677	1233	2557	4762	13822	14499	8014	1672	1052	5769	1486	3773	11.5	1688	2881	2726	186	2.95	2.47
.co.uk	3599	27177	629	1943	1582	62.9	13153	15400	7252	1862	4957	3820	1631	8433	9.98	5083	7281	4087	242	3.04	2.07
.gov	956	25663	2368	4226	6627	13.7	5348	5227	1564	3169	718	3916	2112	5397	12.2	471	2905	1067	175	3.56	2.74
.co	2151	25539	460	790	1493	32.4	16152	10549	608	2900	1051	6297	2380	4888	10.4	2349	4446	2894	522	2.86	2.01
.local	18.1	24941	31.9	24909	0	0	0	0	0	0	0	0	0	18955	0	0	0	0	0	?	?
.sk	367	24919	74.8	146	118	3.31	22976	1402	1112	187	7.5	321	176	18193	6.5	511	18088	412	16.6	4.75	2.05
.hu	645	23273	310	19653	19.9	9.39	1540	2367	1736	350	1142	530	328	21072	7.85	959	1291	845	30.4	2.93	2.02
.win	302	22337	73.5	11931	524	4.54	6679	2778	33.3	1017	1931	1412	660	10060	6.3	2231	3560	910	425	2.35	1.98
.pt	416	21974	436	15560	70.4	5.42	4698	1234	775	522	508	623	423	17504	7.37	422	1765	418	23.4	3.84	2.04
.com.mx	537	19219	283	17256	37.6	1.97	908	1033	316	134	396	357	125	17832	6.92	466	588	378	26.7	2.86	2.05
.com.br	3091	19010	852	1706	343	81.8	8073	10597	6902	958	5935	1510	656	7661	10	5316	6746	3470	98.6	2.87	2.06
.ip6.arpa	268	18772	4878	10159	307	1503	364	488	273	1329	70.4	6.8	6.55	11030	5.55	3.74	431	0.01	0	32.8	11.2

Sample: Top-30+ effective TLDs (subset)

Where does the DNS traffic flow to?

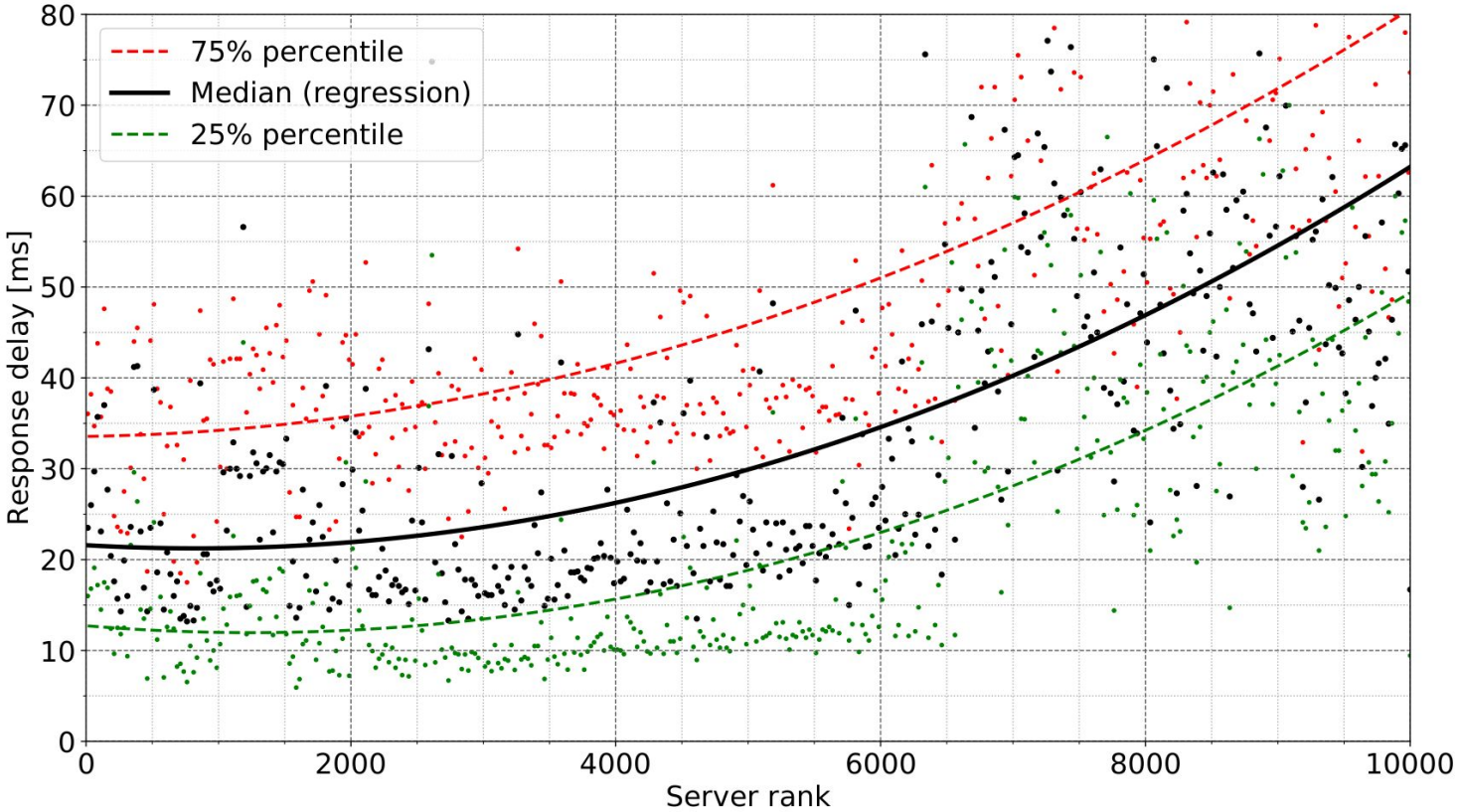


DNS queries



DNS servers

Top 10k auth. servers Q1 2019



Do popular servers respond faster?

Note: DNS recursive resolvers prefer faster servers.