Measuring DNSSEC

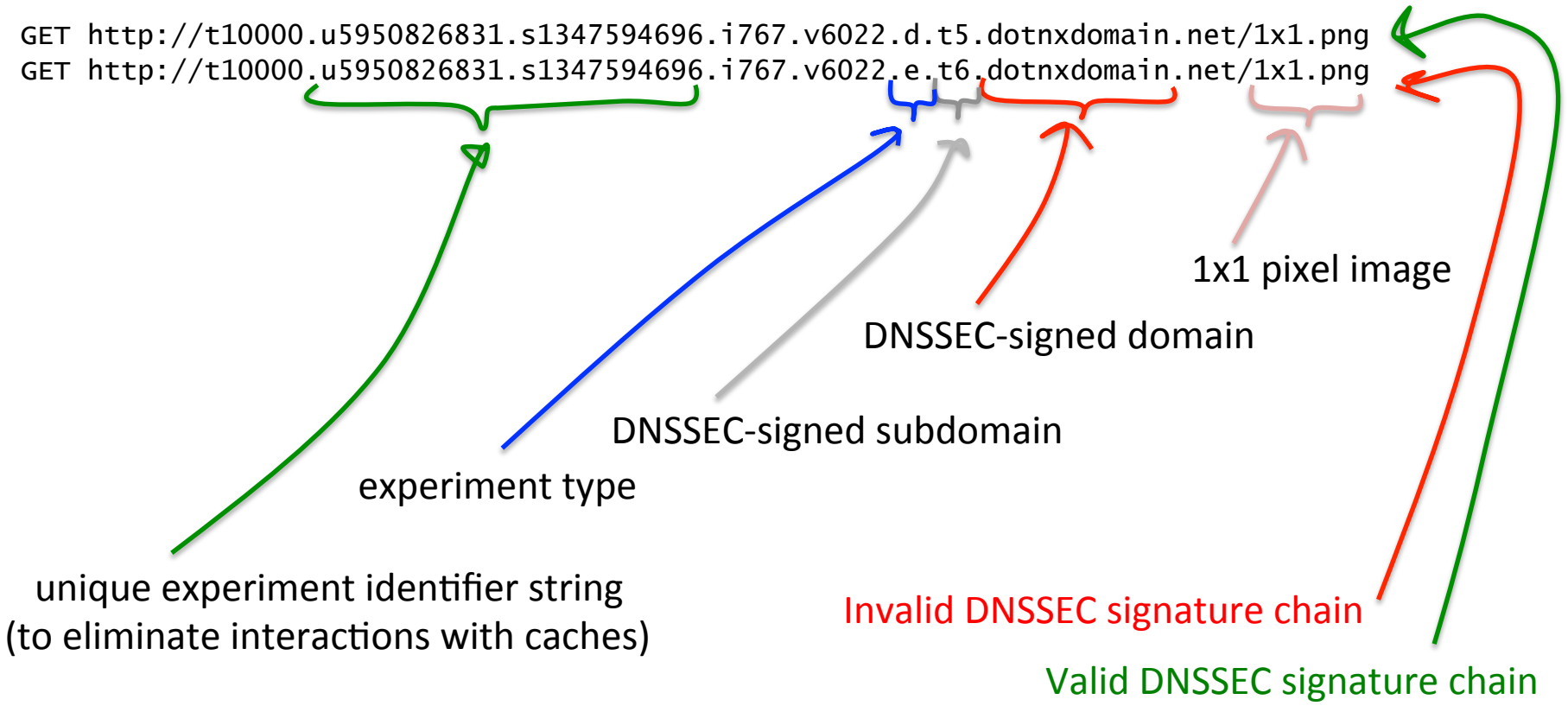
Geoff Huston & George Michaelson
APNIC Labs
October 2012

What are the questions?

1. What proportion of DNS resolvers are DNSSEC-capable?
2. What proportion of users are using DNSSEC-validating DNS resolvers?
3. Where are these users?

Experimental Technique

- Use code embedded in an online ad to perform two simple DNSSEC tests



The Experiment

- Embed the unique id generation and the ad control in flash code
  - Use a 10 second timer to POST results to the server
- Enrol an online advertisement network to display the ad
- The underlying code and the retrieval of the image is executed as part of the ad display function
  - No click is required!

    (or wanted!)

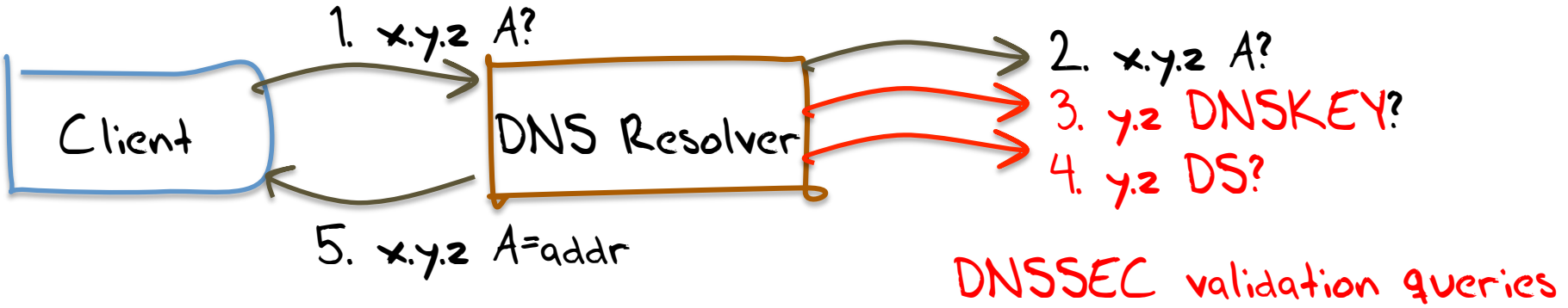
Experiment Run

10 – 27 September 2012

2,831,780 experiments were executed

DNSSEC-Validating Resolver

```
23-Sep-2012 00:09:40.747 queries: client 201.6.x.y#28672:
                         query: t10000.u356944218.s1348355380.i767.v6022.d.t5.dotnxdomain.net IN A -EDC (203.133.248.110)
23-Sep-2012 00:09:41.118 queries: client 201.6.x.y#11321:
                         query: t5.dotnxdomain.net IN DNSKEY -EDC (203.133.248.6)
23-Sep-2012 00:09:41.494 queries: client 201.6.x.y#59852:
                         query: t5.dotnxdomain.net IN DS -EDC (203.133.248.110)
```



DNS Resolvers

- How many unique IP addresses queried for experiment domains in dotnxdomain.net?

- How many of these DNS resolvers also queried for the DNSKEY RR of dotnxdomain.net?

DNS Resolvers

- How many unique IP addresses queried for experiment domains in dotnxdomain.net?

  126,780

- How many of these DNS resolvers also queried for the DNSKEY RR of dotnxdomain.net?

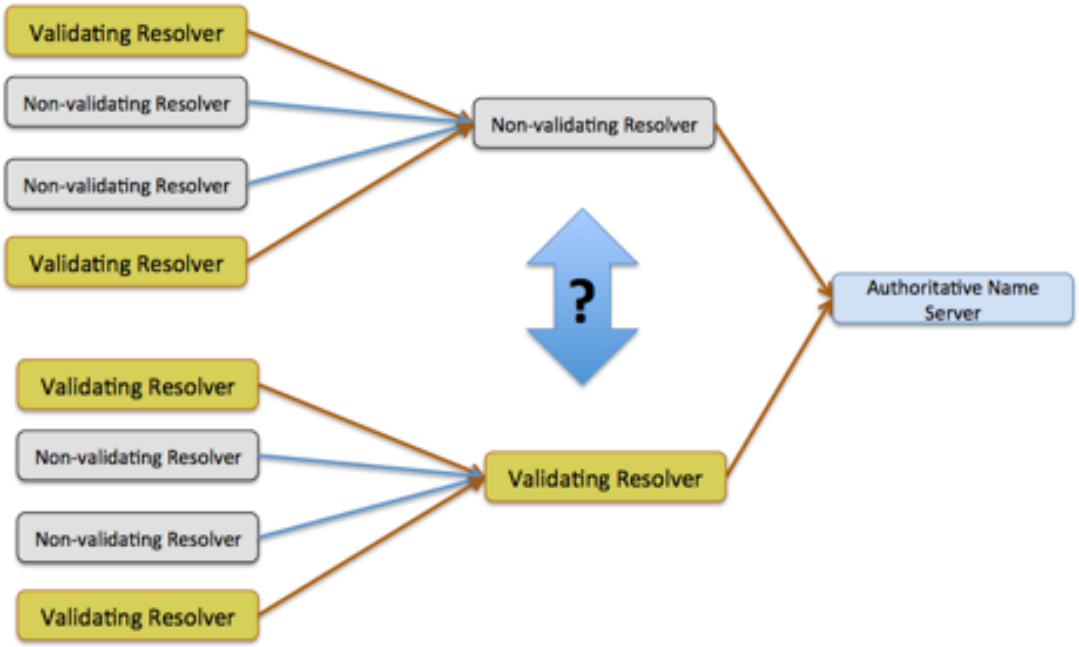
  3,367

Q1: What proportion of DNS resolvers are DNSSEC-capable?

2.6% of visible DNS resolvers appear to be performing DNSSEC validation

Hang on...

How can we tell the difference between a DNSSEC-capable DNS recursive resolver and a DNS forwarder?



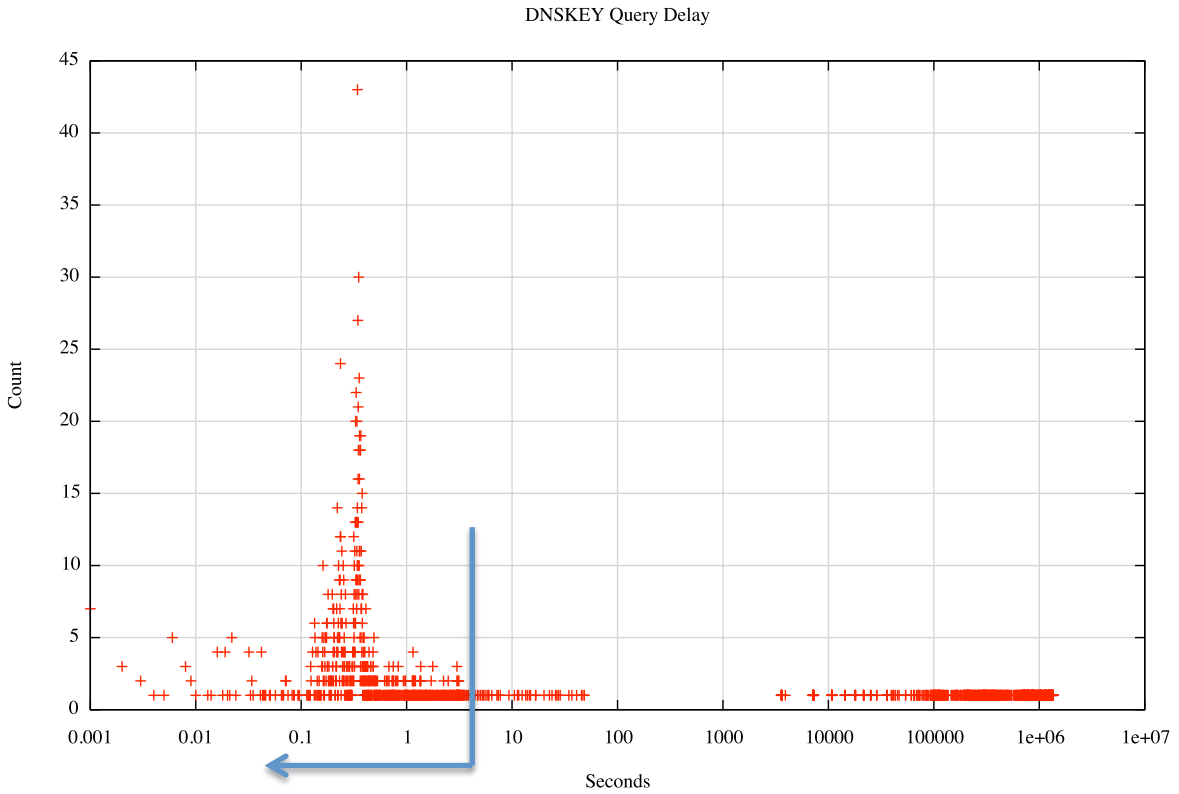
Hang on...

How can we tell the difference between a DNSSEC-capable DNS recursive resolver and a DNS forwarder?

Look for a DNSKEY query within 3 seconds of the initial DNS query. If the DNSKEY query “follows” the initial query within 3 seconds it is more likely we are seeing a DNSSEC-validating DNS recursive resolver.

A DNSSEC-validating resolver will perform validation as part of the query resolution process. This implies that the resolver will submit a DNSKEY query “very soon” after the first A query.

So if we look at the time gap between the first A query and the first DNSKEY query we might be able to distinguish between recursive resolvers and forwarders



Resolvers:

- How many unique IP addresses queried for experiment domains in dotnxdomain.net?

  126,780

- How many of these DNS resolvers also (immediately) queried for the DNSKEY RR of dotnxdomain.net?

  2,277

Thats **1.7%** of the seen resolver set

Hang on again...

- We are getting each client to fetch two URLs:
  - One is DNSSEC-valid
  - One is not
- If a client fetches the DNSSEC-invalid URL _and_ if the only resolver used by the client is a supposedly DNSSEC-validating recursive resolver then we can infer that the resolver is not in fact a DNSSEC-validating recursive resolver

Resolvers:

- How many unique IP addresses queried for experiment domains in dotnxdomain.net?

  126,780

- How many of these DNS resolvers also (immediately) queried for the DNSKEY RR of dotnxdomain.net AND returned an error for DNSSEC-invalid queries?

  2,123

That's **1.6%** of the seen DNS resolver set

Infrastructure Resolvers:

Filter out all resolvers that are associated with just 10 or fewer end clients

How many “big” resolvers are left: **26,825**

How many perform DNSSEC validation: **819**

What’s the DNSSEC-active proportion of these resolvers: **3.1%**

"small scale" Resolvers

How many “small” resolvers were seen: **68,806**

How many perform DNSSEC validation: **692**

What’s the DNSSEC-active proportion of these resolvers: **1.0%**

The Biggest Resolvers by Origin AS

DNSSEC?	Clients	AS	AS NAME	Country
no	976241	AS4766	KIXS-AS-KR Korea Telecom	Republic of Korea
no	472735	AS15169	GOOGLE - Google Inc.	USA
no	411220	AS16880	TRENDMICRO Global IDC and Backbone of Trend Micro	USA
no	330663	AS3462	HINET Data Communication Business Group	Taiwan
no	294053	AS3786	LGDACOM LG DACOM Corporation	Republic of Korea
no	274418	AS5384	EMIRATES-INTERNET Emirates Telecommunications Corp	United Arab Emirates
no	228905	AS4134	CHINANET-BACKBONE No.31,Jin-rong Street	China
no	194865	AS9318	HANARO-AS Hanaro Telecom Inc.	Republic of Korea
no	145429	AS4837	CHINA169-BACKBONE CNCGROUP China169 Backbone	China
yes	140211	AS7922	COMCAST-7922 - Comcast Cable Communications, Inc.	USA
no	120056	AS4788	TMNET-AS-AP TM Net, Internet Service Provider	Malaysia
no	113965	AS3356	LEVEL3 Level 3 Communications	USA
no	107524	AS9050	RTD ROMTELECOM S.A	Romania
no	100527	AS45595	PKTELECOM-AS-PK Pakistan Telecom Company Limited	Pakistan
no	87825	AS6799	OTENET-GR Ote SA (Hellenic Telecommunications Orga	Greece
no	86182	AS7470	TRUEINTERNET-AS-AP TRUE INTERNET Co.,Ltd.	Thailand
no	85917	AS17676	GIGAINFRA Softbank BB Corp.	Japan
no	83349	AS4713	OCN NTT Communications Corporation	Japan
no	82349	AS25019	SAUDINETSTC-AS Autonomus System Number for SaudiNe	Saudi Arabia
no	82146	AS8781	QA-ISP Qatar Telecom (Qtel) Q.S.C.	Qatar
no	78339	AS9737	TOTNET-TH-AS-AP TOT Public Company Limited	Thailand
no	75510	AS9299	IPG-AS-AP Philippine Long Distance Telephone Compa	Philippines
no	71499	AS15557	LDCOMNET Societe Francaise du Radiotelephone S.A	France
no	69071	AS45758	TRIPLETNET-AS-AP TripleT Internet Internet service	Thailand
no	67079	AS8452	TE-AS TE-AS	Egypt

The Biggest DNSSEC-validating Resolvers by Origin AS

DNSSEC?	Clients	AS	AS NAME	Country
yes	140211	AS7922	COMCAST-7922 - Comcast Cable Communications, Inc.	USA
yes	11355	AS5466	EIRCOM Eircom Limited	Ireland
yes	9804	AS9299	IPG-AS-AP Philippine Long Distance Telephone Compa	Philippines
yes	9327	AS3301	TELIANET-SWEDEN TeliaSonera AB	Sweden
yes	9005	AS22047	VTR BANDA ANCHA S.A.	Chile
yes	7390	AS16276	OVH OVH Systems	France
yes	5313	AS28573	NET Servicos de Comunicao S.A.	Brazil
yes	4758	AS1257	TELE2	European Union
yes	3762	AS7657	VODAFONE-NZ-NGN-AS Vodafone NZ Ltd.	New Zealand
yes	3684	AS23700	BM-AS-ID PT. Broadband Multimedia, Tbk	Indonesia
yes	3649	AS5713	SAIX-NET	South Africa
yes	3448	AS15735	DATASTREAM-NET GO p.l.c.	Malta
yes	3411	AS2519	VECTANT VECTANT Ltd.	Japan
yes	3177	AS29562	KABELBW-ASN Kabel BW GmbH	Germany
yes	2927	AS4134	CHINANET-BACKBONE No.31,Jin-rong Street	China
yes	2180	AS28725	CZ-EUROTEL-AS AS of Eurotel Praha	Czech Republic
yes	1897	AS39651	COMHEM-SWEDEN Com Hem Sweden	Sweden
yes	1849	AS11992	CENTENNIAL-PR - Centennial de Puerto Rico	Puerto Rico
yes	1832	AS12912	ERA Polska Telefonia Cyfrowa S.A.	Poland
yes	1809	AS12301	INVITEL Invitel Tavkozlesi Zrt.	Hungary
yes	1798	AS11814	DISTRIBUTEL-AS11814 - DISTRIBUTEL COMMUNICATIONS L	Canada
yes	1781	AS2119	TELENOR-NEXTEL Telenor Norge AS	Norway
yes	1444	AS34779	T-2-AS AS set propagated by T-2, d.o.o.	Slovenia
yes	1220	AS44034	HI3G Hi3G Access AB	Sweden
yes	947	AS23752	NPTELECOM-NP-AS Nepal Telecommunications Corporati	Nepal

Now lets look at Clients:

- How many unique IP addresses completed web fetches for objects named in the experiment?

- How many clients exclusively used DNSSEC-validating resolvers?

Clients:

- How many unique IP addresses completed web fetches for objects named in the experiment?

  1,717,906

- How many clients **exclusively** used DNSSEC-validating resolvers?

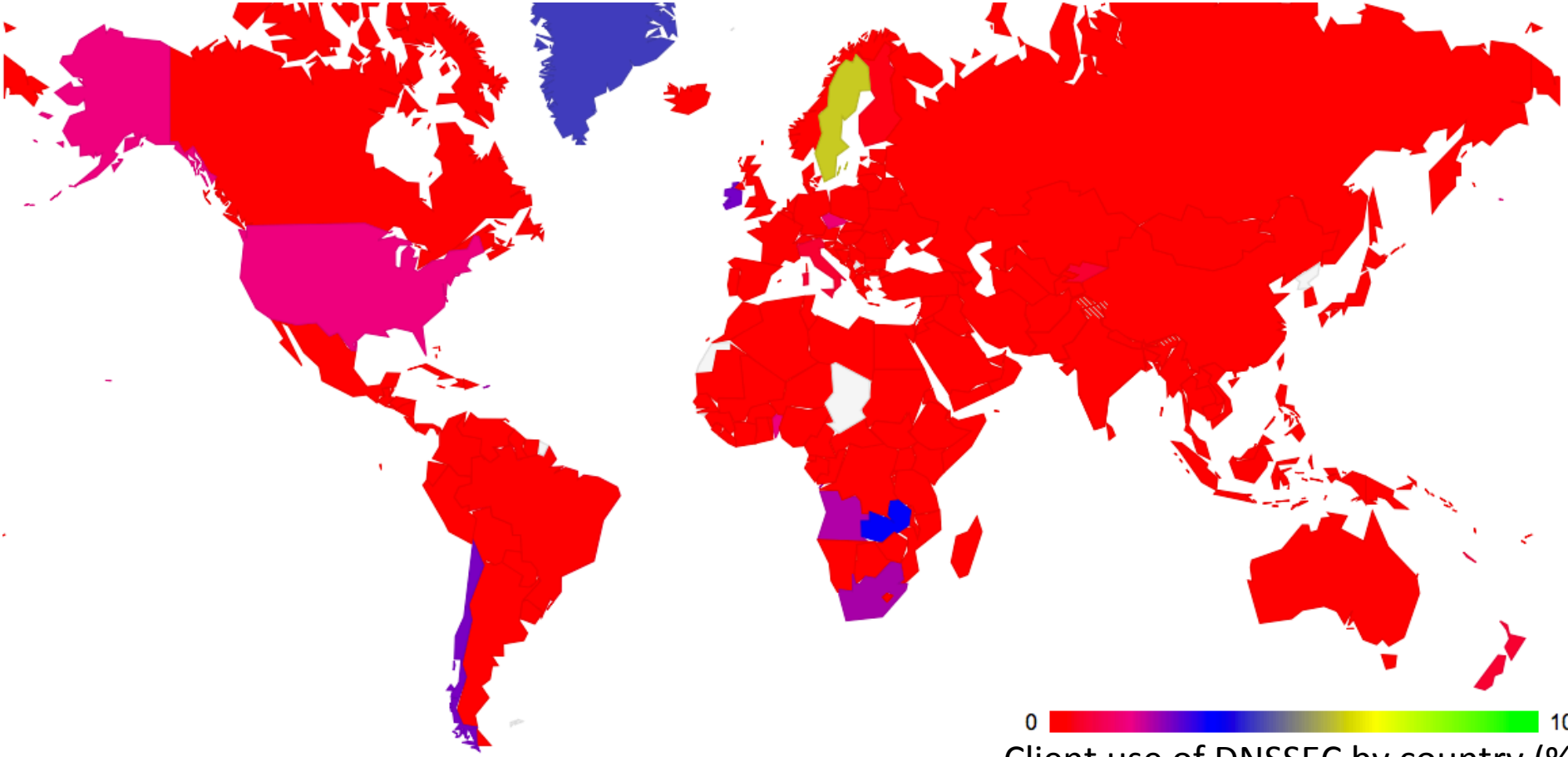
  27,838

Q2: What proportion of users are DNSSEC-validating resolvers?

1.6% of end client systems are using **only** DNS resolvers that appear to be performing DNSSEC validation

Q3: Where can we find DNSSEC-validating clients?

Q3: Where can we find DNSSEC-validating clients?



Client use of DNSSEC by country (%)
September 2012

The top of the country list

% who validate DNSSEC		Validate DNSSEC	Total	
63.44%	AG	177	279	Antigua and Barbuda
59.48%	SE	1982	3332	Sweden
42.31%	GL	11	26	Greenland
32.31%	ZM	158	489	Zambia
25.17%	IE	1632	6484	Ireland
24.88%	CL	2068	8313	Chile
21.95%	PR	570	2597	Puerto Rico
21.40%	ZA	782	3655	South Africa
20.88%	AO	62	297	Angola
16.00%	BB	135	844	Barbados
15.75%	US	9149	58074	United States of America
15.66%	BJ	13	83	Benin
14.74%	CZ	858	5820	Czech Republic
8.00%	NC	16	200	New Caledonia
7.07%	NZ	569	8045	New Zealand
6.85%	KG	23	336	Kyrgyzstan
6.79%	IT	1917	28228	Italy
6.63%	LB	62	935	Lebanon
4.82%	MT	171	3545	Malta
4.69%	FI	93	1981	Finland
3.75%	CH	171	4562	Switzerland
3.37%	BR	1411	41906	Brazil
3.03%	LI	1	33	Liechtenstein
2.83%	DE	484	17105	Germany
2.09%	UA	329	15711	Ukraine

The top of the country list

% who validate DNSSEC		Validate DNSSEC	Total	
59.48%	SE	1982	3332	Sweden
25.17%	IE	1632	6484	Ireland
24.88%	CL	2068	8313	Chile
21.95%	PR	570	2597	Puerto Rico
21.40%	ZA	782	3655	South Africa
15.75%	US	9149	58074	United States of America
14.74%	CZ	858	5820	Czech Republic
7.07%	NZ	569	8045	New Zealand
6.79%	IT	1917	28228	Italy
4.82%	MT	171	3545	Malta
4.69%	FI	93	1981	Finland
3.75%	CH	171	4562	Switzerland
3.37%	BR	1411	41906	Brazil
2.83%	DE	484	17105	Germany
2.09%	UA	329	15711	Ukraine
1.98%	CA	543	27405	Canada
1.97%	SK	62	3140	Slovakia
1.89%	PL	799	42284	Poland
1.65%	HU	255	15432	Hungary
1.65%	JP	792	48089	Japan
1.41%	UY	35	2485	Uruguay
1.21%	LT	105	8658	Lithuania
1.15%	CO	73	6331	Colombia
1.15%	SI	41	3573	Slovenia
1.11%	RS	133	11963	Serbia
0.94%	ID	308	32891	Indonesia
0.78%	TR	91	11656	Turkey

Ranking only those CCs with more than 1000 sample points in this experiment run (106 CC's)

The bottom of the country list

% who validate DNSSEC		Validate DNSSEC	Total	
59.48%	SE	1982	3332	Sweden
25.17%	IE	1632	6484	Ireland
24.88%	CL	2068	8313	Chile
21.95%	PR	570	2597	Puerto Rico
21.40%	ZA	782	3655	South Africa
15.75%	US	9149	58074	United States of America
14.74%	CZ	858	5820	Czech Republic
7.07%	NZ	569	8045	New Zealand
6.79%	IT	1917	28228	Italy
4.82%	MT	171	3545	Malta
4.69%	FI	93	1981	Finland
3.75%	CH	171	4562	Switzerland
3.37%	BR	1411	41906	Brazil
2.83%	DE	484	17105	Germany
2.09%	UA	329	15711	Ukraine
1.98%	CA	543	27405	Canada
1.97%	SK	62	3140	Slovakia
1.89%	PL	799	42284	Poland
1.65%	HU	255	15432	Hungary
1.65%	JP	792	48089	Japan
1.41%	UY	35	2485	Uruguay
1.21%	LT	105	8658	Lithuania
1.15%	CO	73	6331	Colombia
1.15%	SI	41	3573	Slovenia
1.11%	RS	133	11963	Serbia
0.94%	ID	308	32891	Indonesia
0.78%	TR	91	11656	Turkey

% who validate DNSSEC		Validate DNSSEC	Total	
0.01%	GR	6	70060	Greece
0.01%	SA	3	36156	Saudi Arabia
0.01%	CY	1	11523	Cyprus
0.00%	AE	0	28475	United Arab Emirates
0.00%	QA	0	16413	Qatar
0.00%	LK	0	10401	Sri Lanka
0.00%	DZ	0	6574	Algeria
0.00%	KW	0	6192	Kuwait
0.00%	OM	0	4317	Oman
0.00%	KZ	0	4153	Kazakhstan
0.00%	JO	0	4177	Jordan
0.00%	EC	0	3868	Ecuador
0.00%	BH	0	3135	Bahrain
0.00%	YE	0	2526	Yemen
0.00%	MO	0	2287	Macao
0.00%	PS	0	2321	Occupied Palestine
0.00%	MU	0	2098	Mauritius
0.00%	LV	0	1945	Latvia
0.00%	PA	0	1617	Panama
0.00%	NG	0	1394	Nigeria
0.00%	ZW	0	1392	Zimbabwe
0.00%	SD	0	1273	Sudan
0.00%	ME	0	1244	Montenegro
0.00%	SV	0	1182	El Salvador
0.00%	GT	0	1127	Guatemala
0.00%	TT	0	1058	Trinidad and Tobago
0.00%	JM	0	1088	Jamaica

Ranking only those CCs with more than 1000 sample points in this experiment run (106 CC's)

DNSSEC-Validating Clients by AS - the top AS's

% who validate DNSSEC		Validate DNSSEC	Total		
97.54%	AS44143	119	122	RS	VIPMOBILE-AS Vip mobile d.o.o., Serbia
97.26%	AS27831	71	73	CO	Colombia M?vil, Colombia
97.03%	AS44034	261	269	SE	HI3G Hi3G Access AB, Sweden
96.83%	AS28725	61	63	CZ	CZ-EUROTEL-AS AS of Eurotel Praha, Czech Republic
96.49%	AS15600	55	57	CH	FINECOM Finecom Telecommunications AG, Switzerland
96.26%	AS20776	180	187	FR	OUTREMER-AS Outremer Telecom, France
94.93%	AS12912	712	750	PL	ERA Polska Telefonia Cyfrowa S.A., Poland
94.30%	AS31343	248	263	UA	INTERTELECOM Intertelecom Ltd, Ukraine
91.87%	AS29518	113	123	SE	BREDBAND2 Bredband2 AB, Sweden
90.86%	AS5466	1631	1795	IE	EIRCOM Eircom Limited, Ireland
90.79%	AS38484	69	76	AU	VIRGIN-BROADBAND-AS-AP Virgin Broadband VISP, Australia
88.06%	AS22047	2066	2346	CL	VTR BANDA ANCHA S.A., Chile
87.83%	AS11992	570	649	PR	CENTENNIAL-PR - Centennial de Puerto Rico, Puerto Rico
87.74%	AS3737	93	106	US	PTD-AS - PenTeleData Inc., United States of America
87.40%	AS17711	111	127	TW	NDHU-TW National Dong Hwa University, Taiwan
86.25%	AS3301	508	589	SE	TELIANET-SWEDEN TeliaSonera AB, Sweden
85.19%	AS3245	46	54	BG	DIGSYS-AS Digital Systems Ltd, Bulgaria
83.78%	AS41833	62	74	LB	MOSCANET Moscanet (WISE), Lebanon
82.26%	AS8473	102	124	SE	BAHNHOF Bahnhof Internet AB, Sweden
80.43%	AS7922	8855	11010	US	COMCAST-7922 - Comcast Cable Communications, Inc., United States of America
80.27%	AS4704	118	147	JP	SANNET SANYO Information Technology Solutions Co., Ltd., Japan
80.09%	AS5713	744	929	ZA	SAIX-NET, South Africa
80.00%	AS41749	100	125	RO	NETCOMPUTERS-AS Net & Computers SRL, Romania
79.44%	AS24852	85	107	LT	VINITA VINITA Internet Services, Lithuania
76.16%	AS1257	409	537	EU	TELE2, European Union

Ranking only those ASs with more than 50 sample points in this experiment run (15,134 AS's)

The Sort-of-Good News

1.6% of clients appear to use DNSSEC-validating resolvers - that's almost twice the amount DNSSEC validation coverage for the Internet than the amount of users who have IPv6!

And finally...

The “Mad Resolver” prize goes to the pair of resolvers:

217.73.15.39

217.73.15.38

who successfully queried for the same A RR from our server for a total of 93,237 times over eight hours

Thanks guys! Great achievement!

Thank you!