


EDNS (in) Compatibility

October, 2015
DNS-OARC, Montreal, Canada
Vicky Risk, ISC

New Applications introduce new (unknown) options

IETF Draft of edns-client-subnet

Below is a copy of the most recent [IETF draft for edns-client-subnet](#).

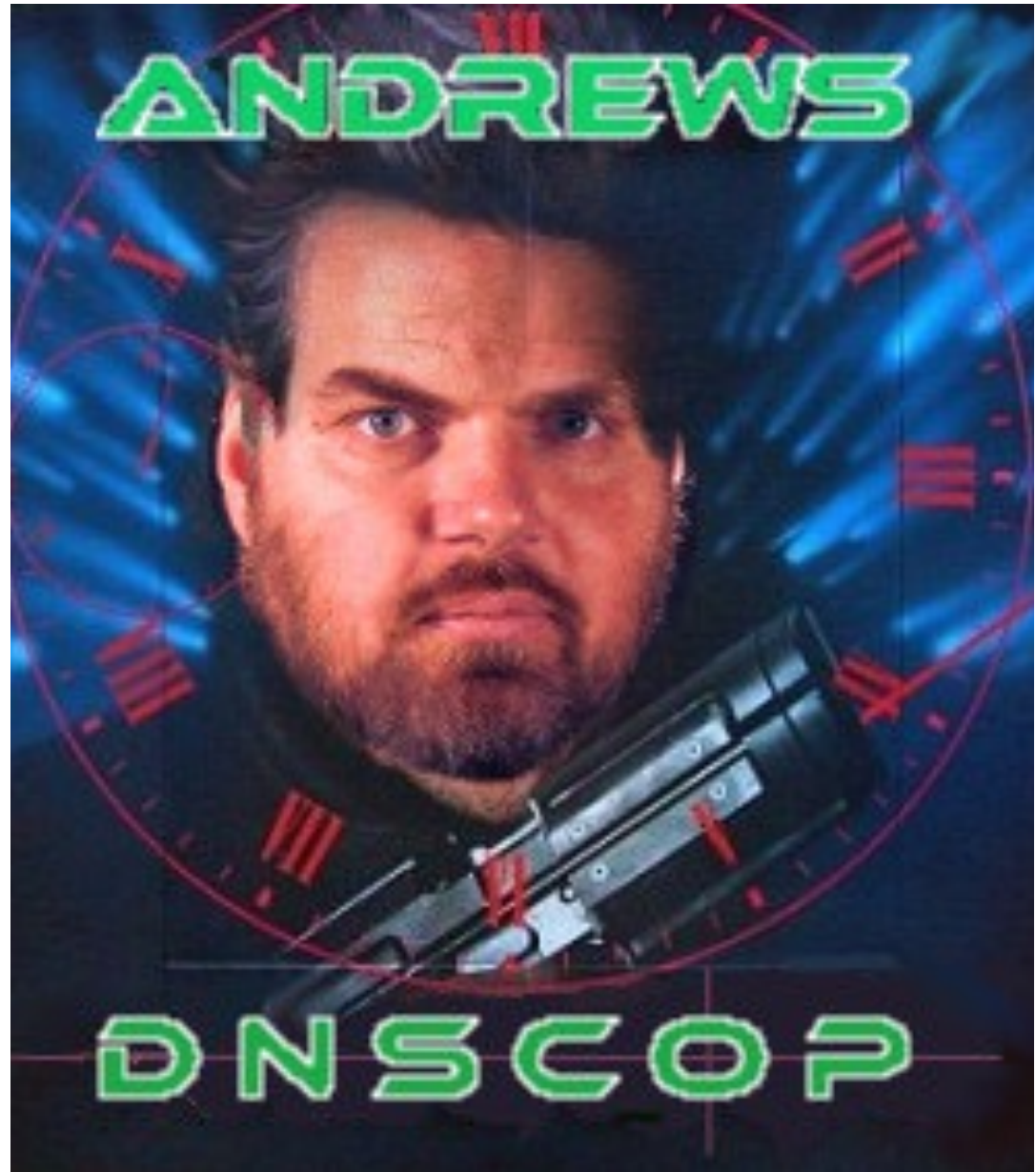
dnsop
Internet-Draft
Intended status: Informational
Expires: May 19, 2015

C. Contavalli
M. van der Gaast



EDNS Version 1 (expired draft)

“It is impracticable to deploy new EDNS options, with EDNS version 0, on a global scale due to inconsistent server behaviour in deployed servers when a EDNS option is present in the query.”

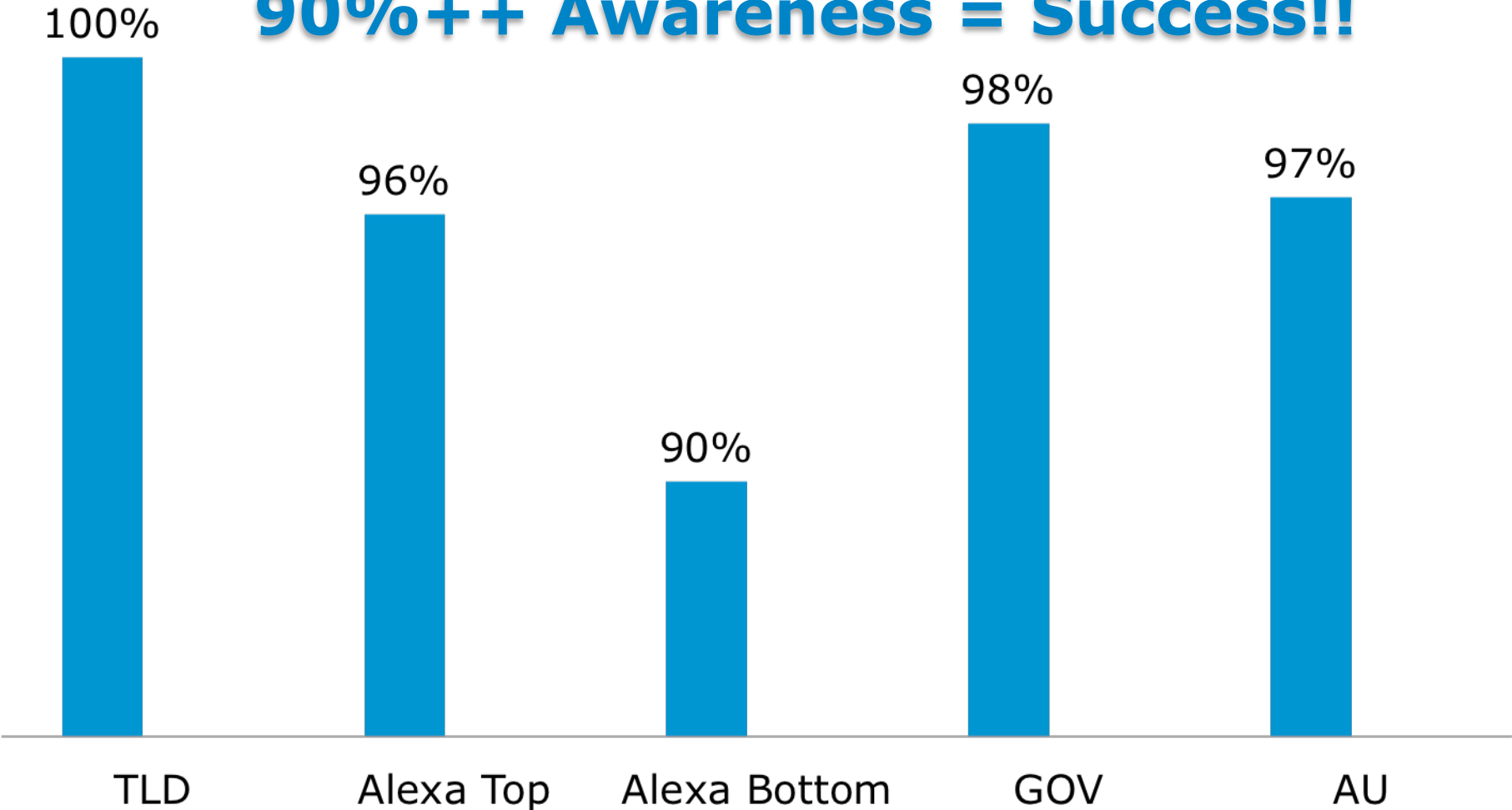


Experiment surveyed ...

1. Root and TLD servers using a series of dig queries
 2. DNS servers for Alexa Top 1000 sites
 3. DNS servers for Alexa Bottom 1000 of the top 1M sites
 4. GOV servers in the Alexa Top 1M sites
 5. AU servers in the Alexa Top 1M sites
- see ednscomp.isc.org for details of queries + expected results

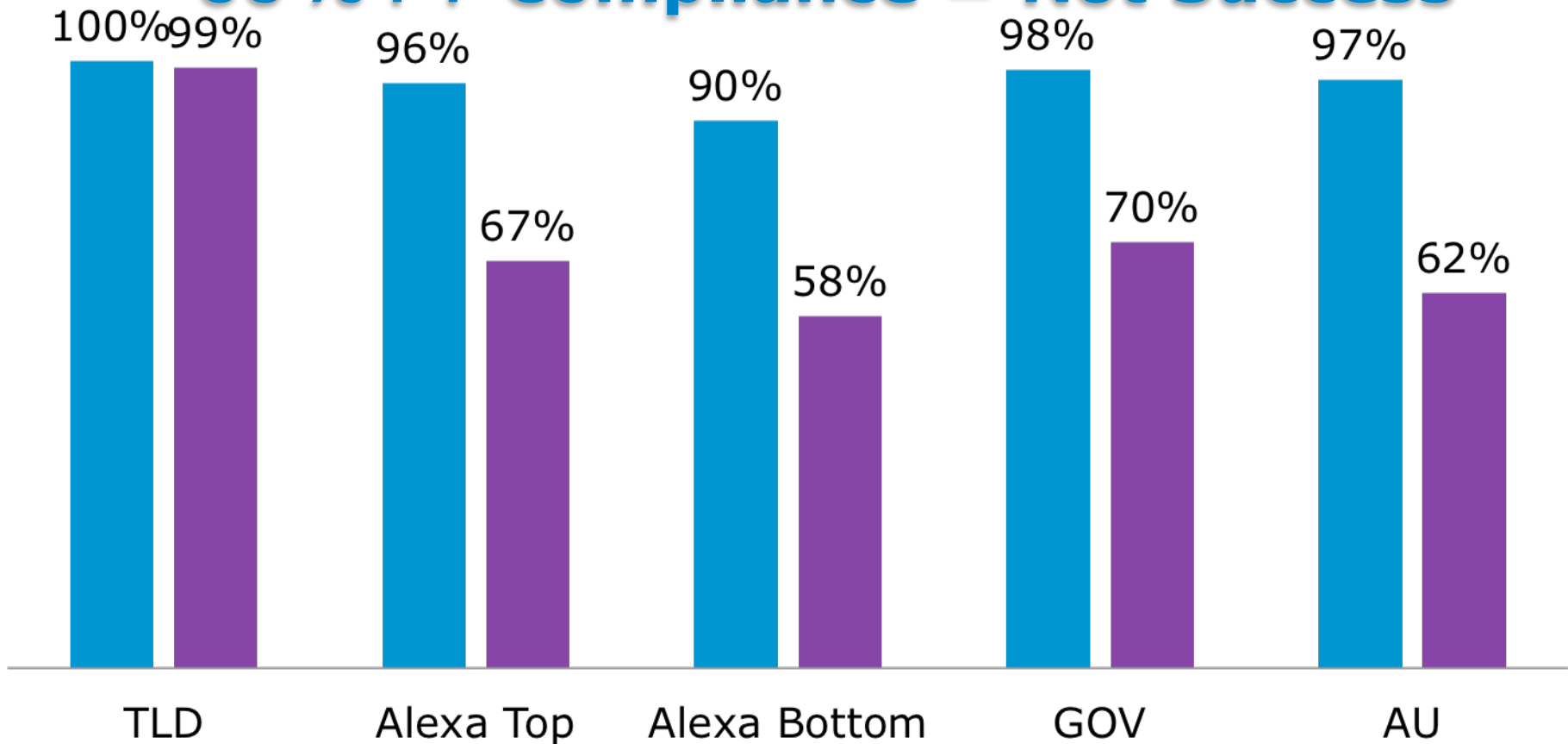
EDNS Aware Servers
(Sept 30, 2015)

90%++ Awareness = Success!!



**EDNS Aware Servers and
Full EDNS Compliance
(Sept 30, 2015)**

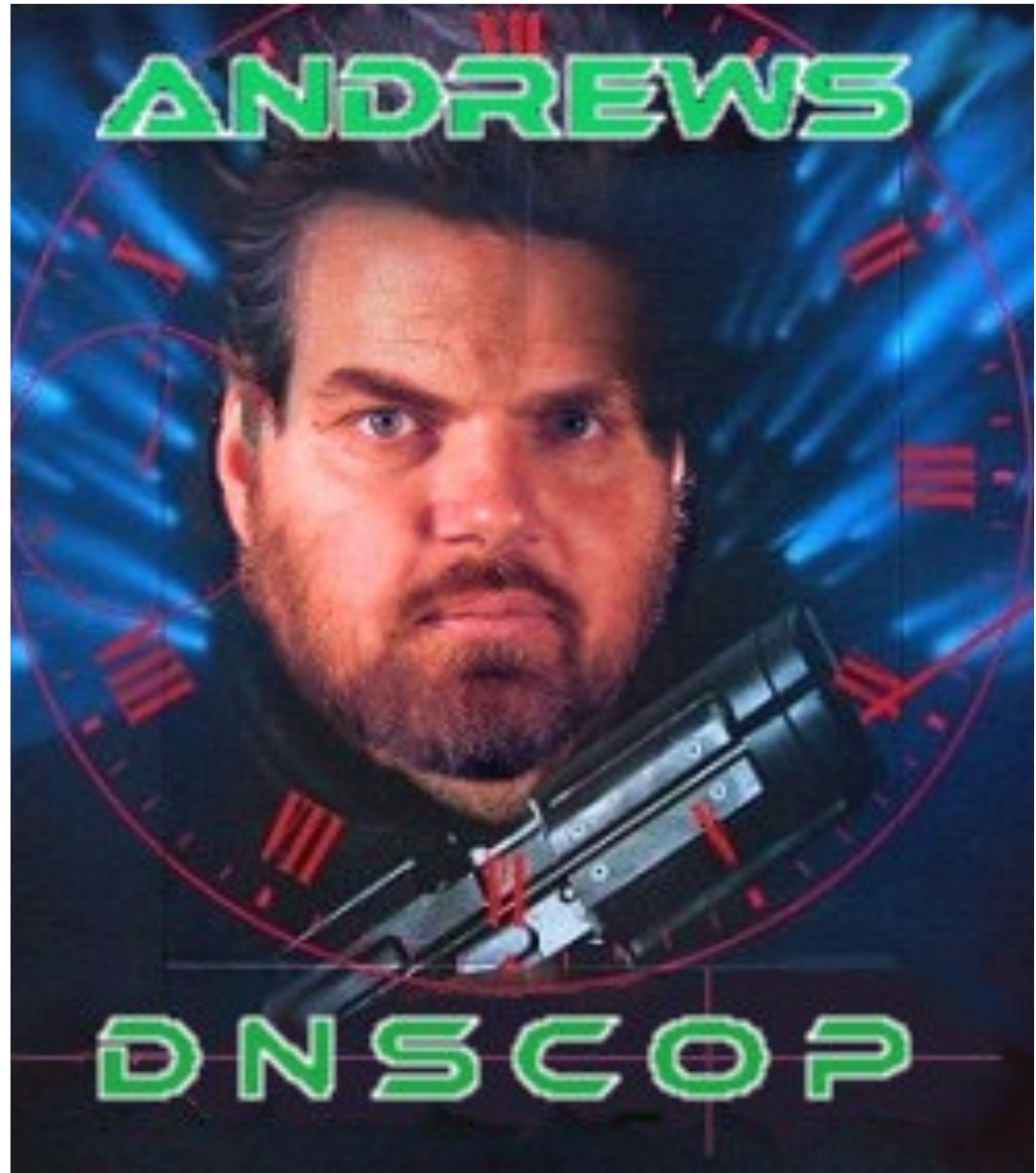
60%++ Compliance = Not Success



Problems seen

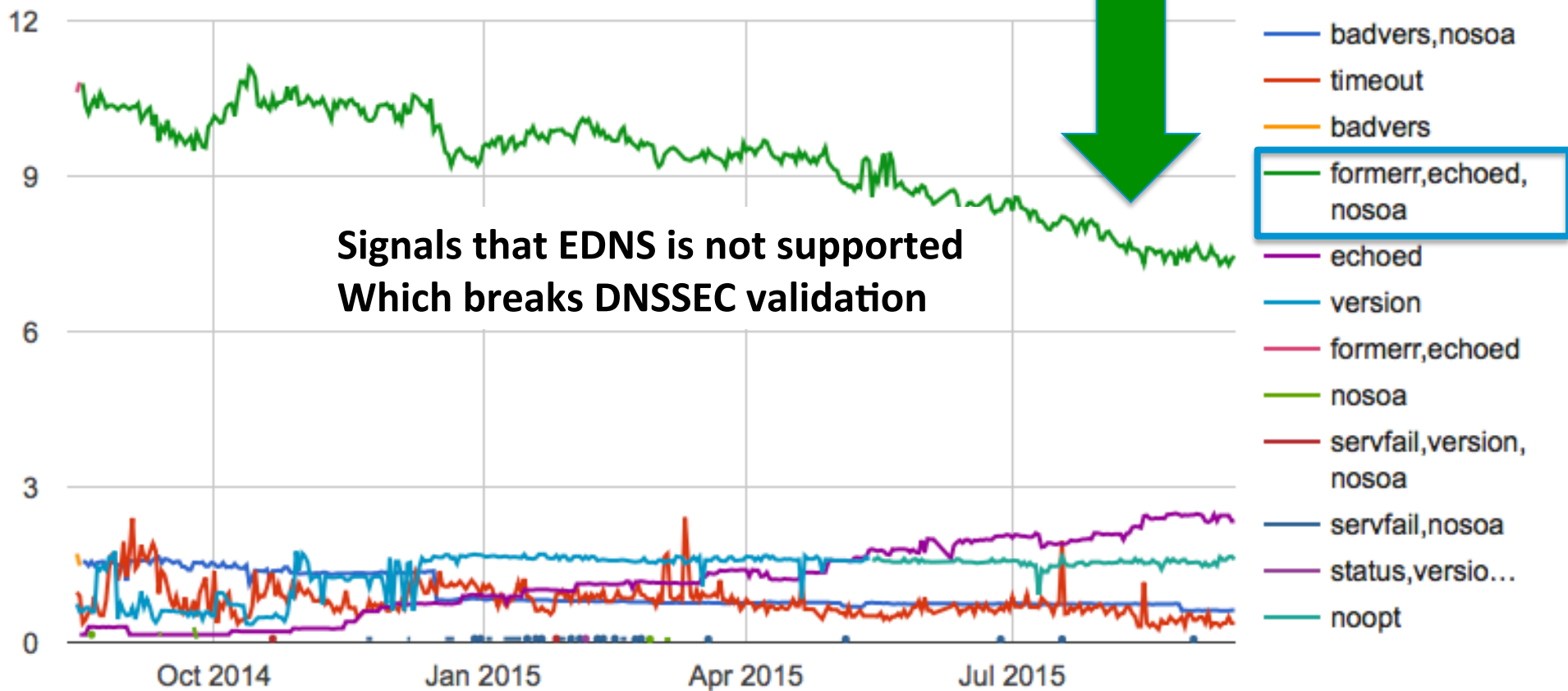
- OPT only returned when DO=1 is present in the request
- BADVER not returned to EDNS (1)
- NOTIMP, FORMERR, BADVERS returned when a EDNS option is present
- NOTIMP, FORMERR, BADVERS returned when a EDNS Z flag is present
- EDNS (1) queries being dropped
- EDNS queries with a Z bit being dropped
- EDNS Z bits in queries echoed back
- TCP response size limited to EDNS UDP response size
- DO=1 not returned by DNSSEC aware servers

“dropping packets is just plain anti-social and always has been”



Unknown option -> disable EDNS

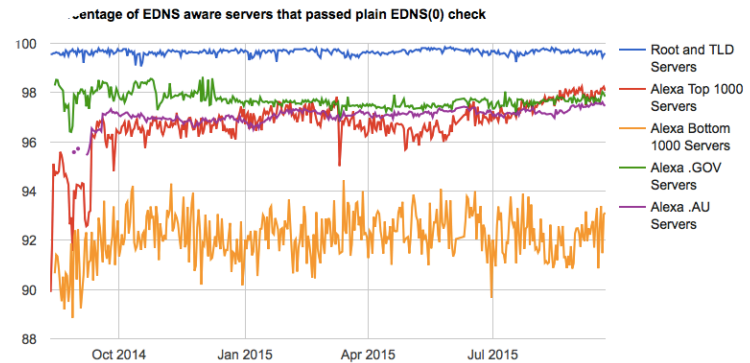
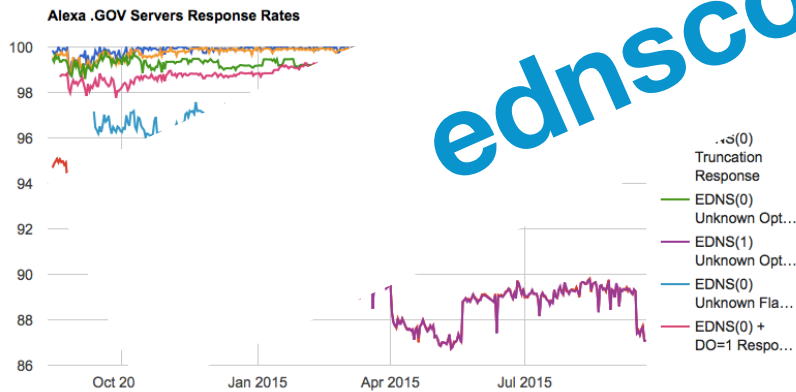
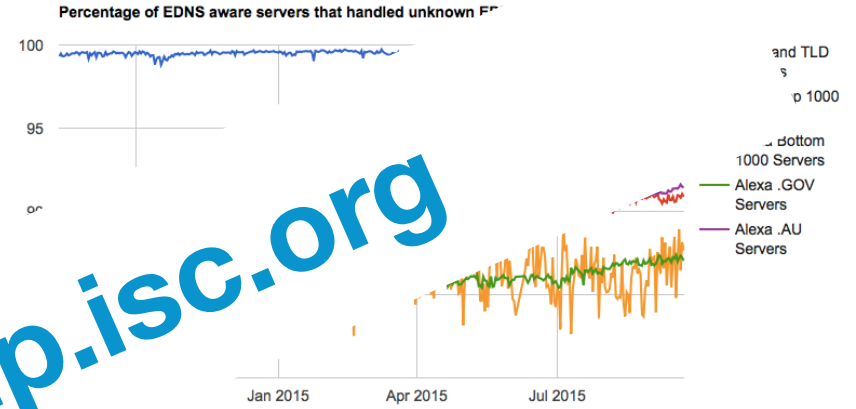
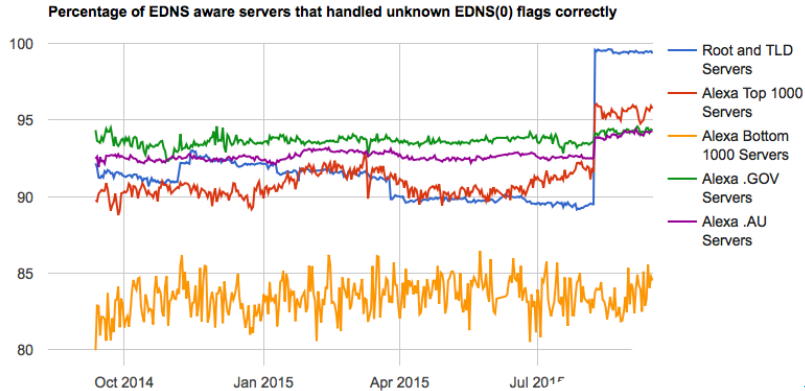
Alexa .GOV Servers EDNS(0) Unknown Option Failure Reasons



TRENDS

September 2014 vs September 2015

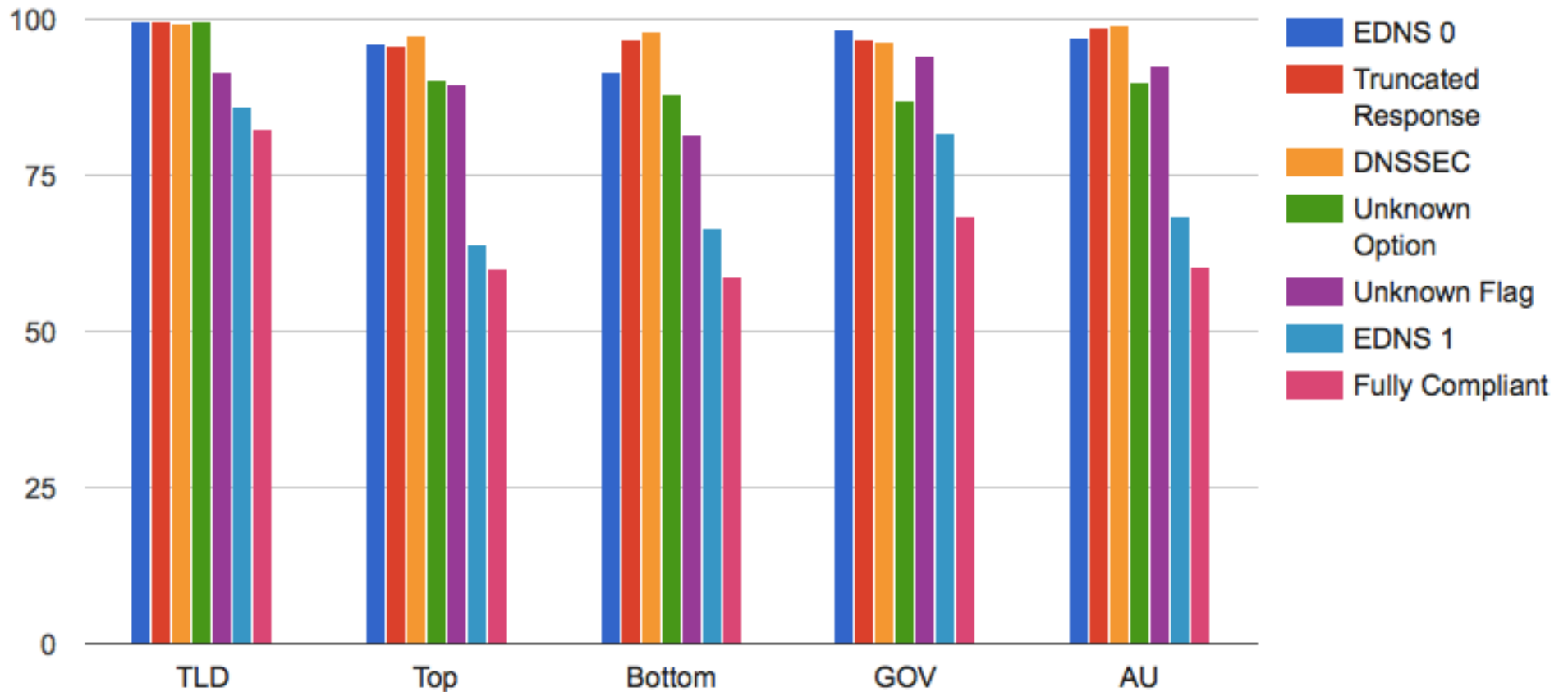
Historical Data



ednscmp.isc.org

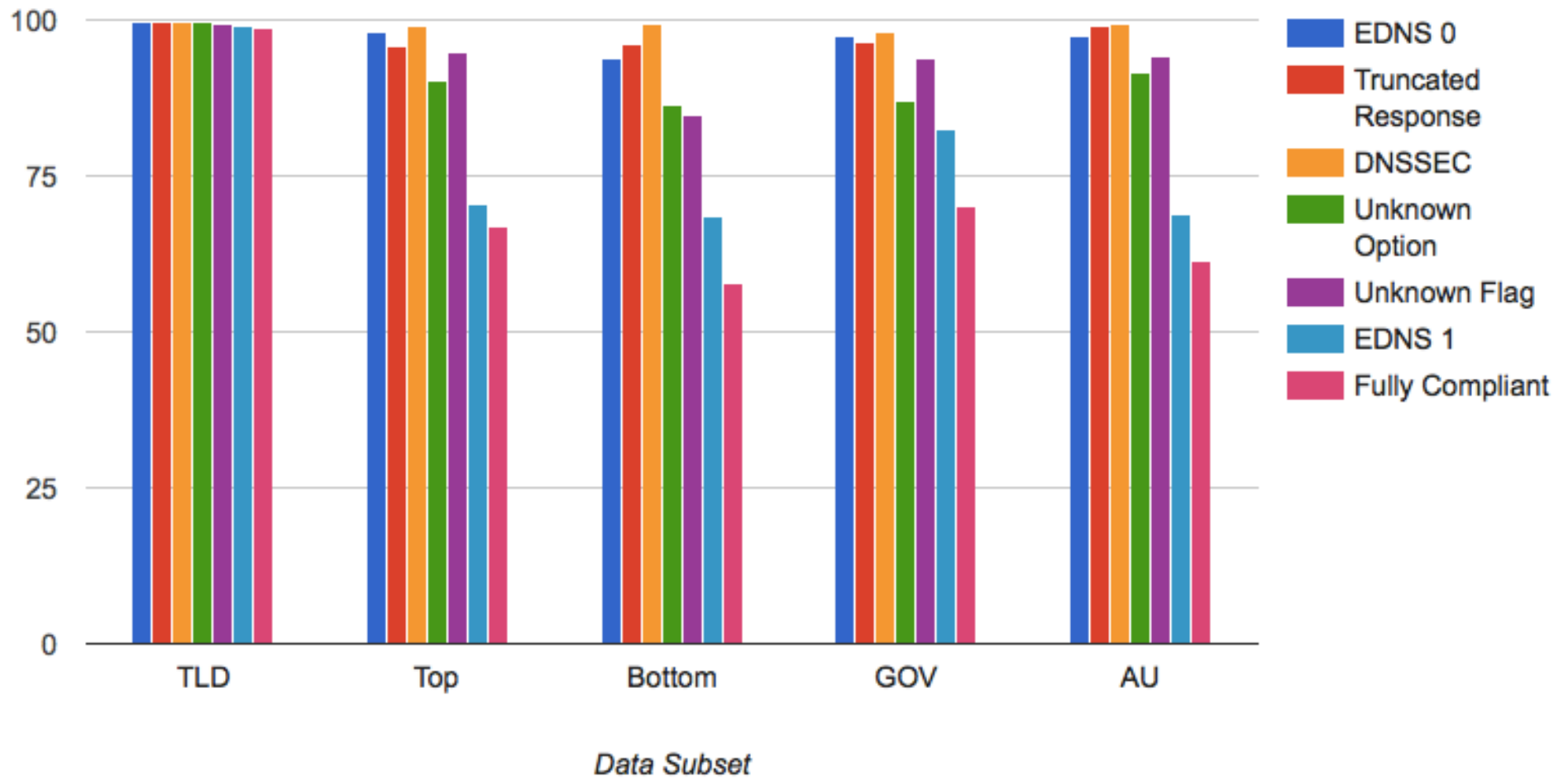
2014

EDNS Compliance by Function of EDNS Aware Servers - 21 Sep 2014










2015

EDNS Compliance by Function of EDNS Aware Servers - 30 Sep 2015

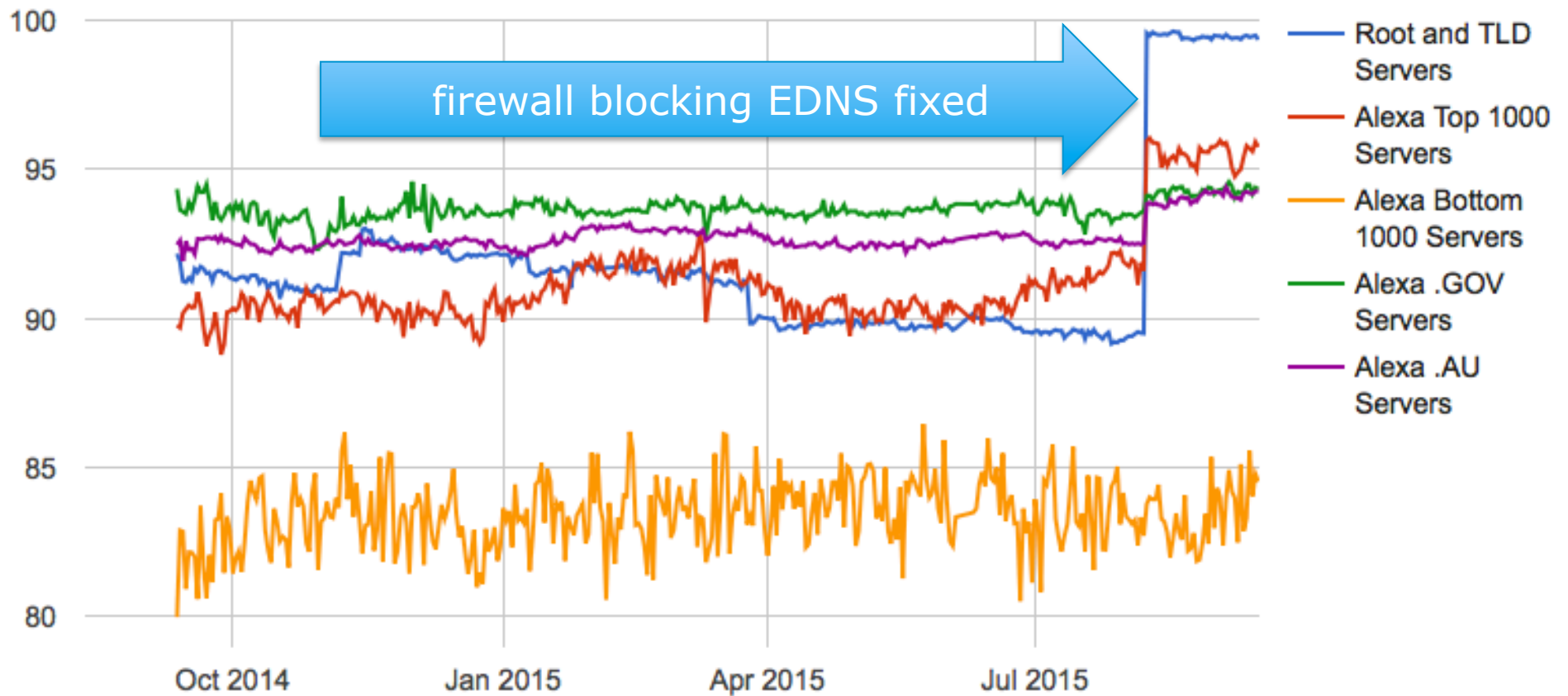


Trend by Problem

Issue		Trend 2014 - 2015
EDNS0		flat, slight decline in .AU
Truncated Response		4 of 5 improved slightly
DNSSEC		all improved
Unknown Option		3 of 5 improved slightly
Unknown Flag		significant improvement – esp in TLDs by 8%
EDNS1		significant recent improvement
Fully Compliant		significant improvement est. in TLD and Alexa top 1000

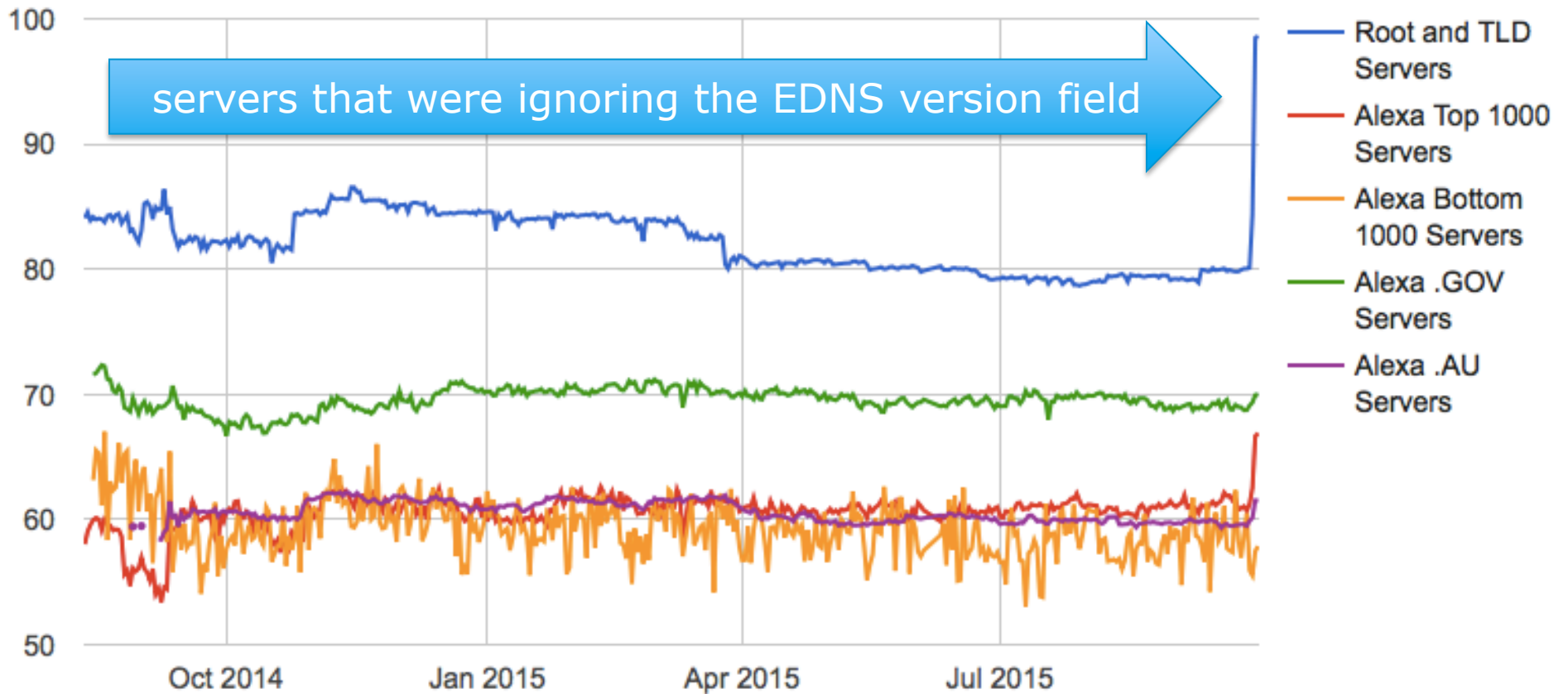
August 7th

Percentage of EDNS aware servers that handled unknown EDNS(0) flags correctly



Sept 30th

Percentage of EDNS aware servers that passed all EDNS compliance tests



Why should you care?

1. Most recursive resolvers now support EDNS. Lack of EDNS support in authoritative servers results in additional queries being made as the recursive servers need to retry with plain DNS **and results in slower DNS resolution.**
2. Not answering EDNS queries is particularly bad as that is indistinguishable from **packet loss.**
3. Incorrect EDNS behaviour when presented with unknown EDNS versions and EDNS options can result in **DNS resolution failures and/or DNSSEC validation failures.**
4. Failure to run fully EDNS compliant nameservers will make it **hard to deploy developments like DNS COOKIES.**

What we have done so far

- Put up a self-test web site at **www.ednscomp.isc.org**
- Contacted various operators who seemed to have problems, based on our testing
- Asked Casey Deccio to add this test to DNSViz
 - <https://github.com/dnsviz/dnsviz/releases/tag/v0.4.0-beta4>
- Presented at IETF on this problem (3/15)
- NOW – presenting at OARC and NANOG

Please

Test your nameserver to ensure it:

1. Supports EDNS version negotiation.
2. Handles unknown EDNS options
3. Handles unknown EDNS flags.

(Switch has put up a site to measure compliance in .ch and .li)

Summary

- DNS cookies are disabled by default in BIND 9.10. We plan to enable them in 9.11, by default.
- Is there anything further the community wants to do to prevent DNSSEC failures?



References

- <http://ednscomp.isc.org>
- <https://www.ietf.org/proceedings/92/slides/slides-92-dnsop-7.pdf>
- <https://www.isc.org/blogs/partial-edns-compliance-hampers-deployment-of-new-dns-features/>