

EDNS Compliance

Mark Andrews
marka@isc.org

DataSets

- Root and TLD servers
- Alexa Top 1000
- Alexa Bottom 1000 of Top 1Million
- GOV servers from Alexa Top 1Million
- AU servers from Alexa Top 1Million

Methodology

dig +norec +noedns soa zone @server

dig +norec +edns=0 soa zone @server

dig +norec +edns=1 +noednsneg soa zone @server

dig +norec +ednsopt=100 soa zone @server

dig +norec +ednsflags=0x80 soa zone @server

dig +norec +dnssec soa zone @server

dig +norec +dnssec +bufsize=512 +ignore dnskey zone @server

dig +norec +edns=1 +noednsneg +ednsopt=100 soa zone @server

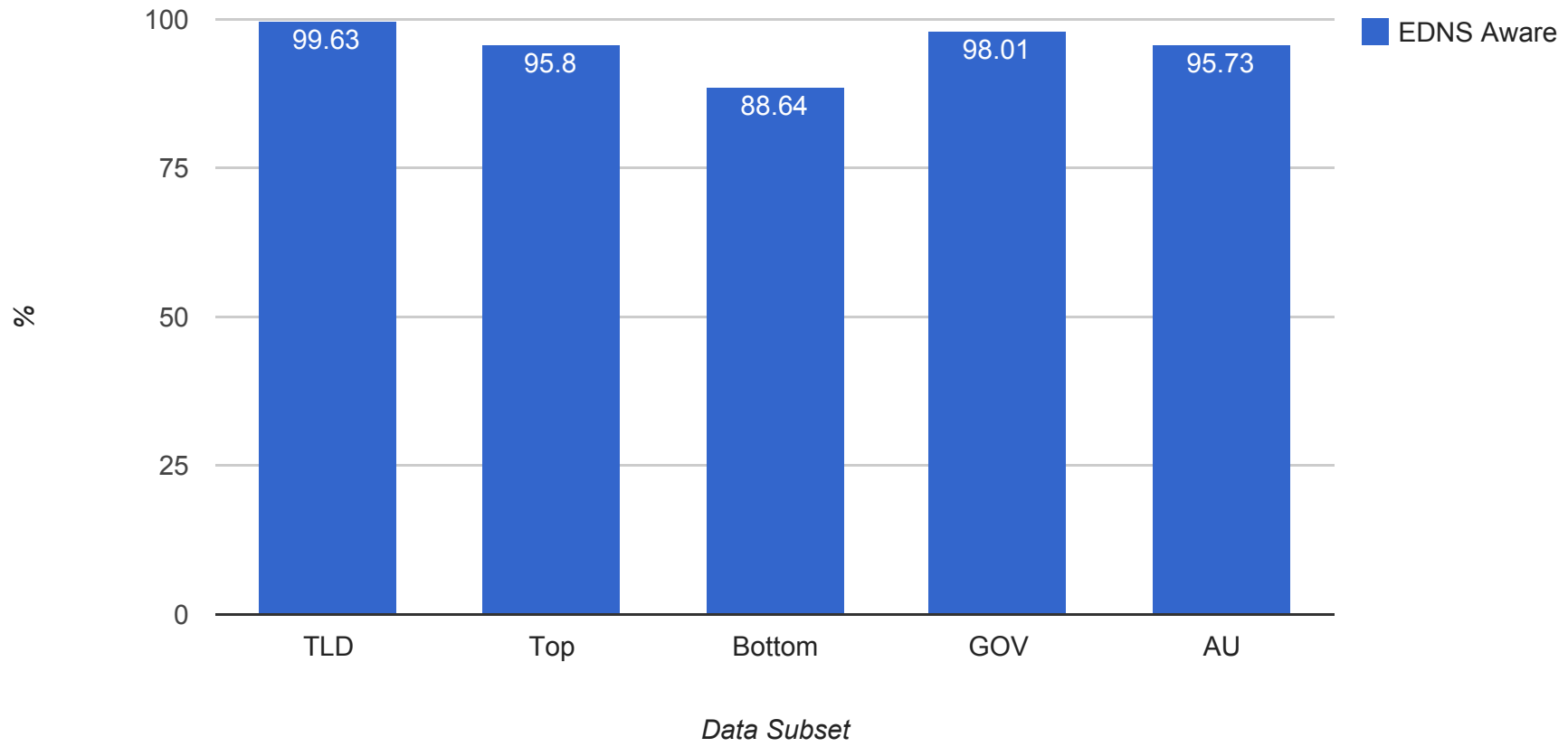
Faults Detected 1/2

- OPT only returned when DO=1 is present in the request
- BADVER not returned to EDNS (1)
- NOTIMP returned when a EDNS option is present
- FORMERR returned when a EDNS option is present
- BADVERS returned when a EDNS option is present
- NOTIMP returned when a EDNS Z flag is present
- FORMERR returned when a EDNS Z flag is present
- BADVERS returned when a EDNS Z flag is present
- EDNS option echoed back

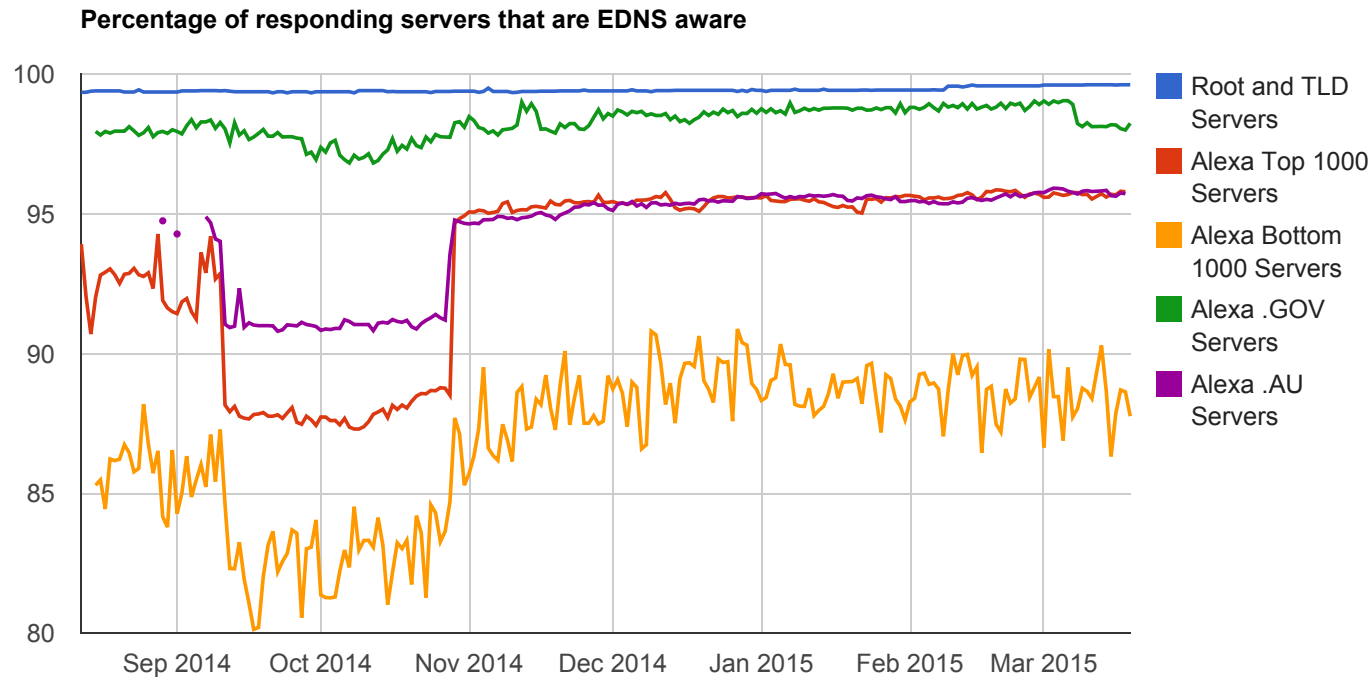
Faults Detected 2/2

- OPT not returned in truncated response
- 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
- Truncated UDP response when send when response will not fit
- Fragmented responses being blocked
- DO=1 not returned by DNSSEC aware servers

EDNS Aware Servers - 18 Mar 2015



EDNS Compliance Report: 2015-03-19T05:19:26Z



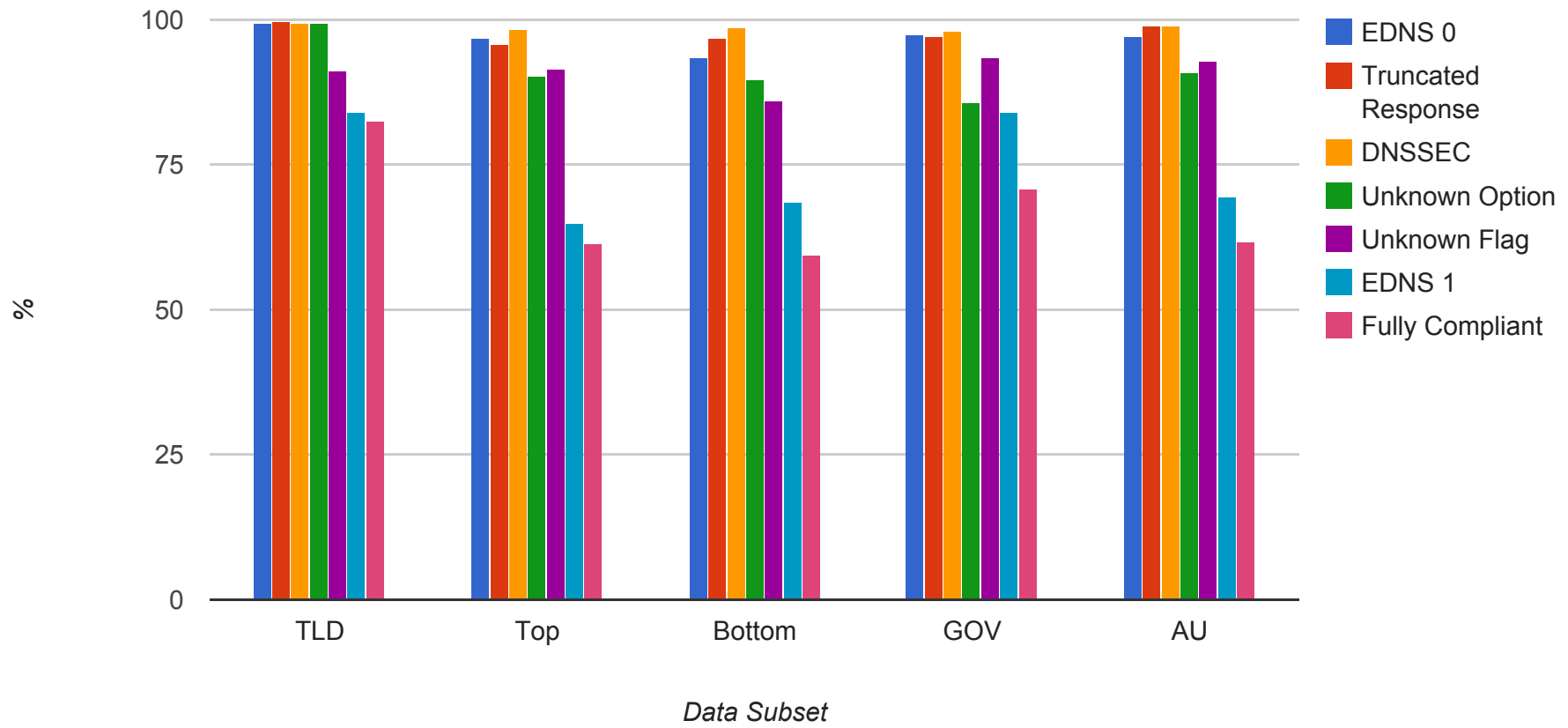
A EDNS aware server is one which returns a EDNS response to at least one of the test queries. A active server is one which returns a response to one of the test queries. Inactive servers are discarded when calculating the EDNS aware percentages.

2014-09-11: Cloudflare replaced server software which only returned a EDNS response when DO was set to one in the request to a server which ignores EDNS in the request.

2014-10-10: Stopped setting AD=1 in test queries.

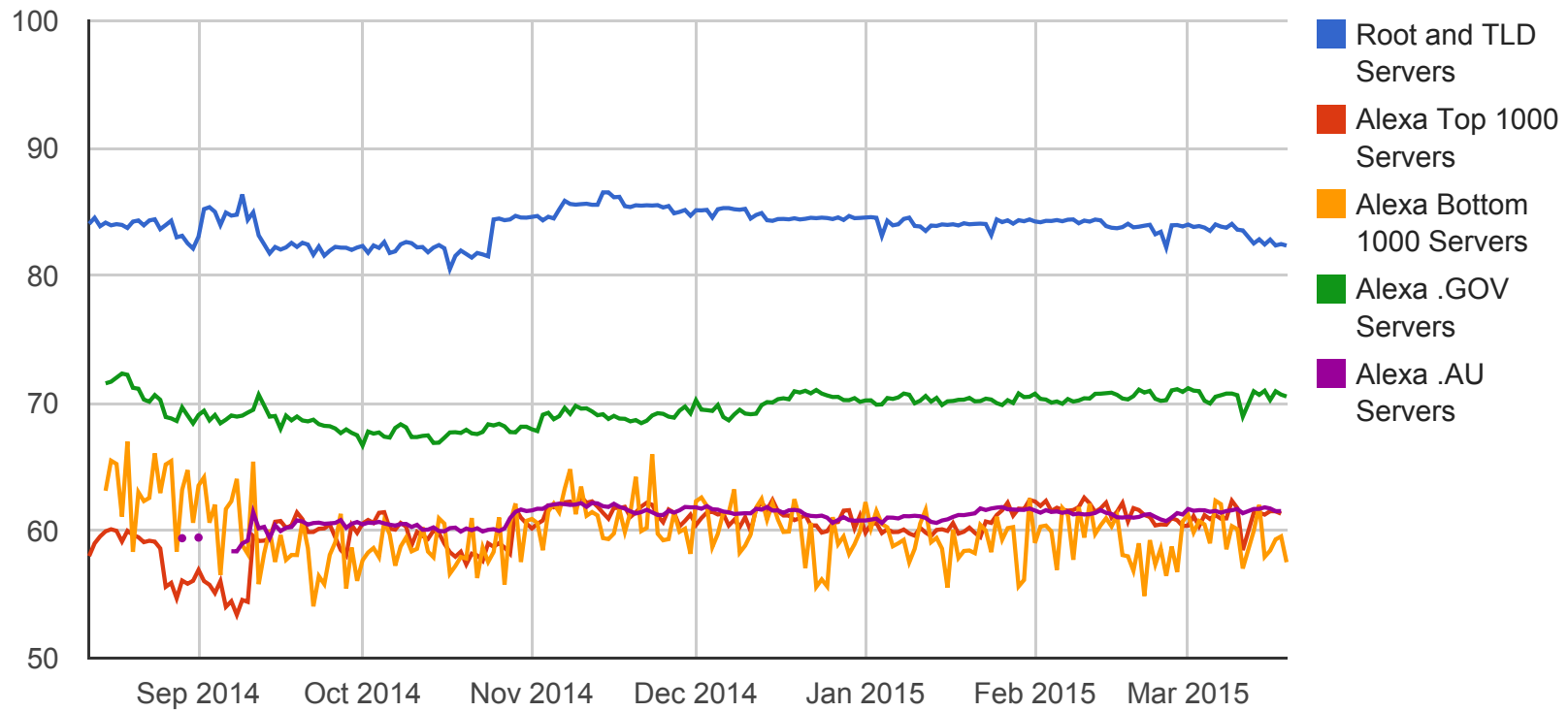
2014-10-29: Cloudflare restored EDNS support.

EDNS Compliance by Function - 18 Mar 2015

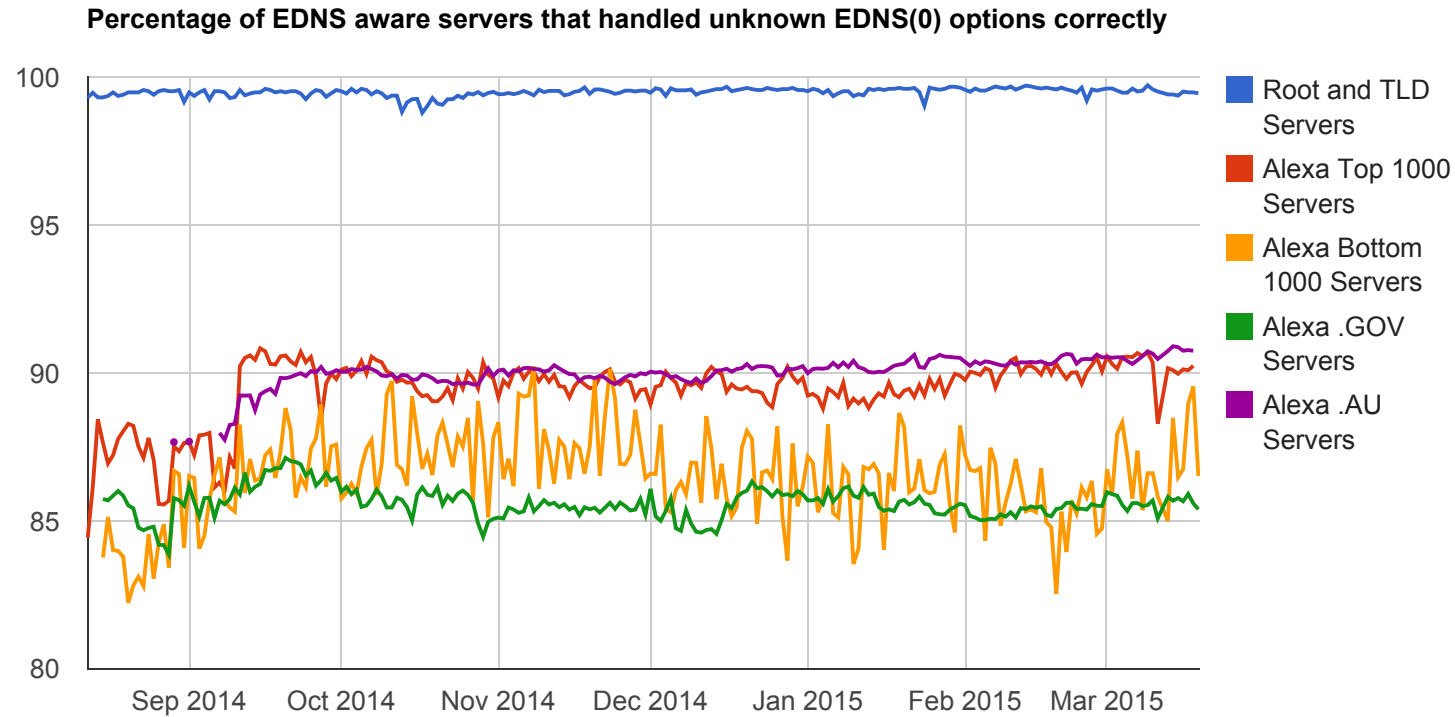


EDNS Compliance Report: 2015-03-19T07:46:51Z

Percentage of EDNS aware servers that passed all EDNS compliance tests



EDNS Compliance Report: 2015-03-19T05:19:26Z



(dig +ednsopt=100 +norec soa \$zone @\$server)

expect: status: NOERROR

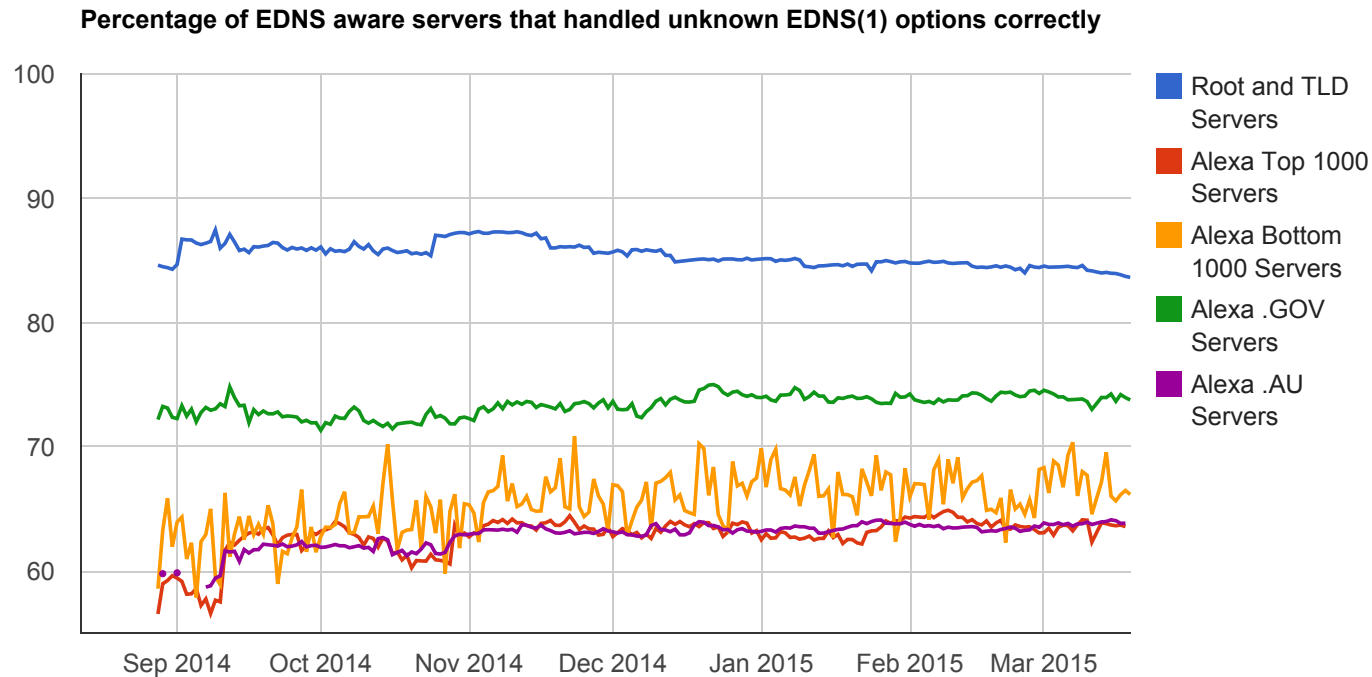
expect: SOA record to be present

expect: OPT record to be present

expect: OPT=100 to not be present

[See RFC6891, 6.1.2 Wire Format](#)

EDNS Compliance Report: 2015-03-19T07:46:51Z



(dig +ednsopt=100 +edns=1 +norec soa \$zone @\$server)

expect: status: BADVERS

expect: SOA record to NOT be present

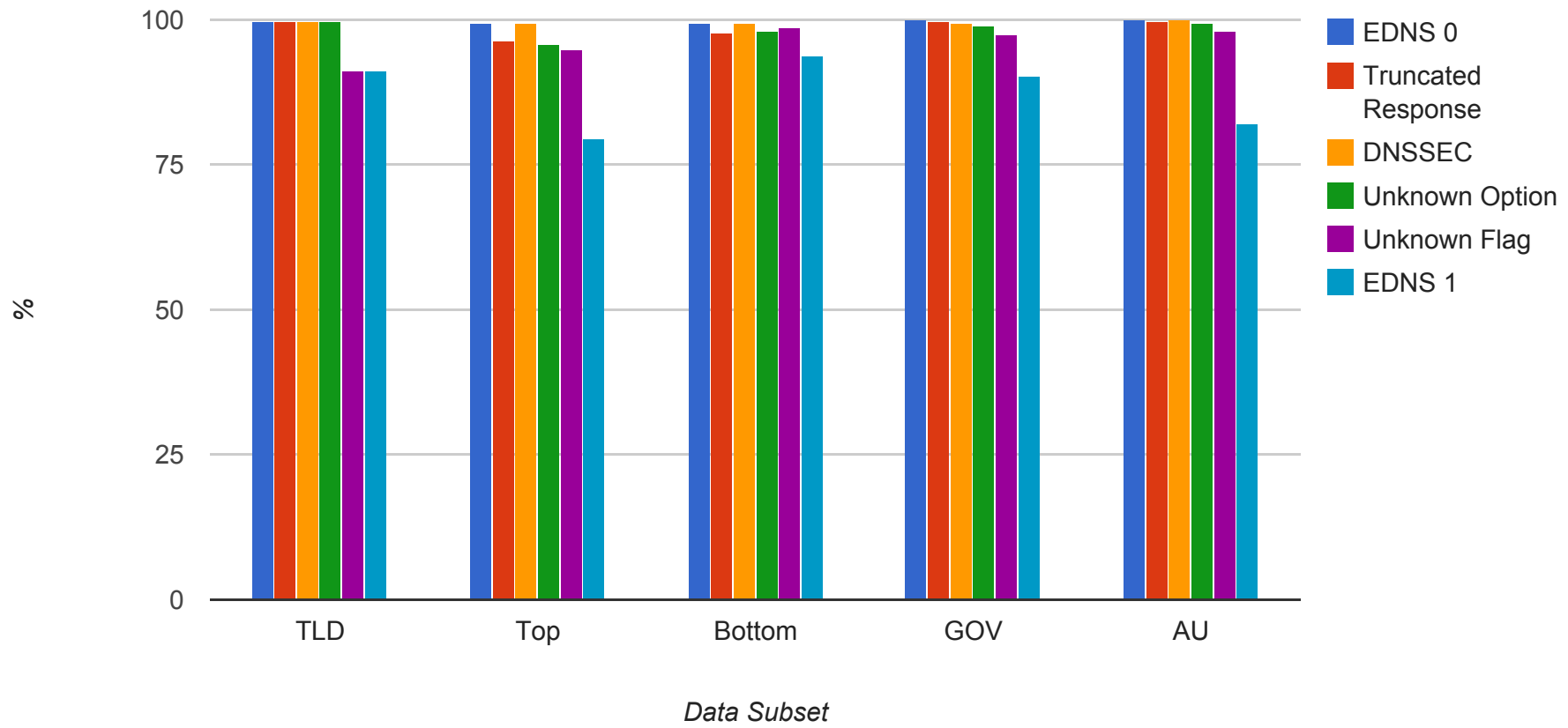
expect: OPT record to be present

expect: OPT=100 to not be present

expect: EDNS Version 0 in response

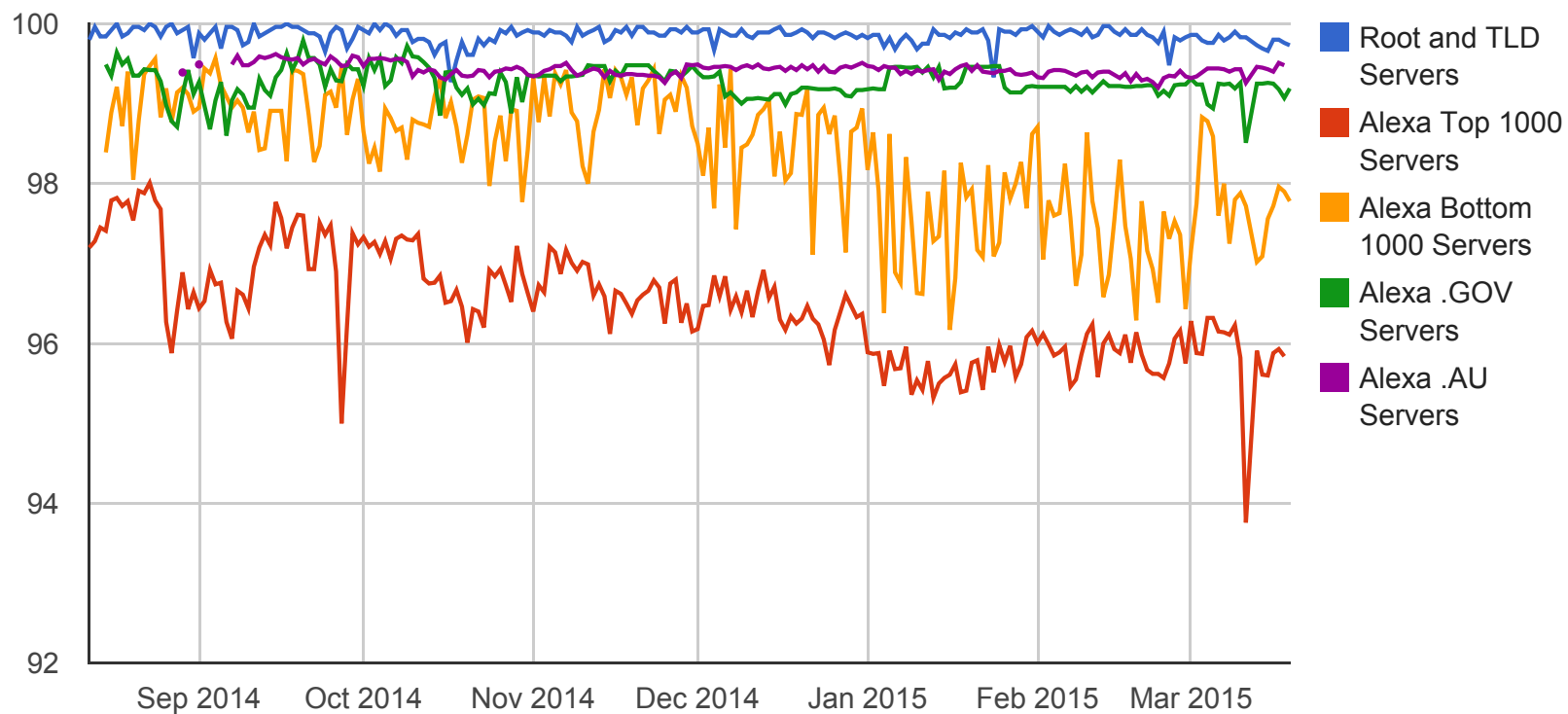
[See RFC6891](#)

EDNS Response Rate by Function - 18 Mar 2015

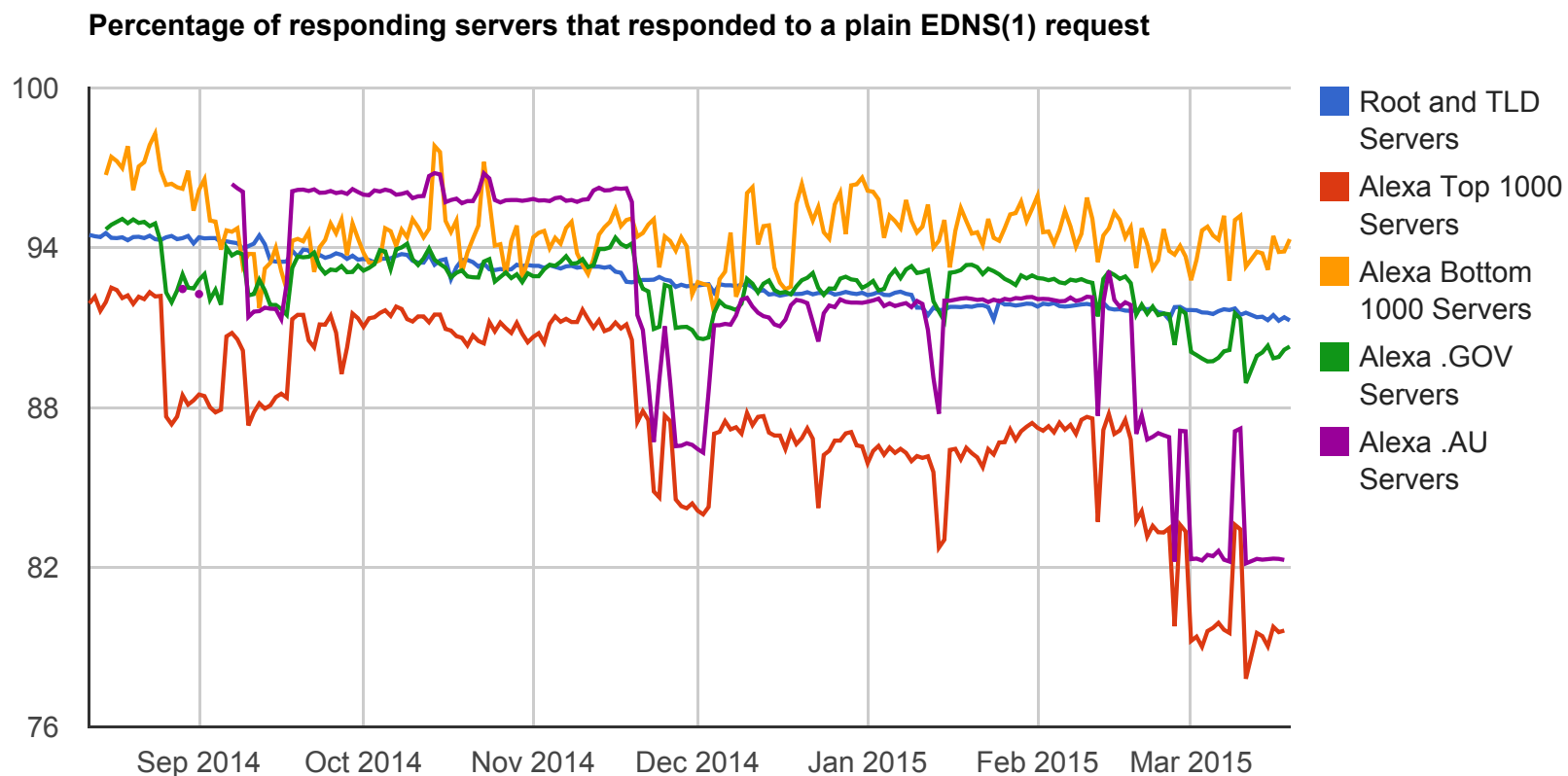


EDNS Compliance Report: 2015-03-19T05:19:26Z

Percentage of responding servers that responded to a EDNS(0) request with a unknown option



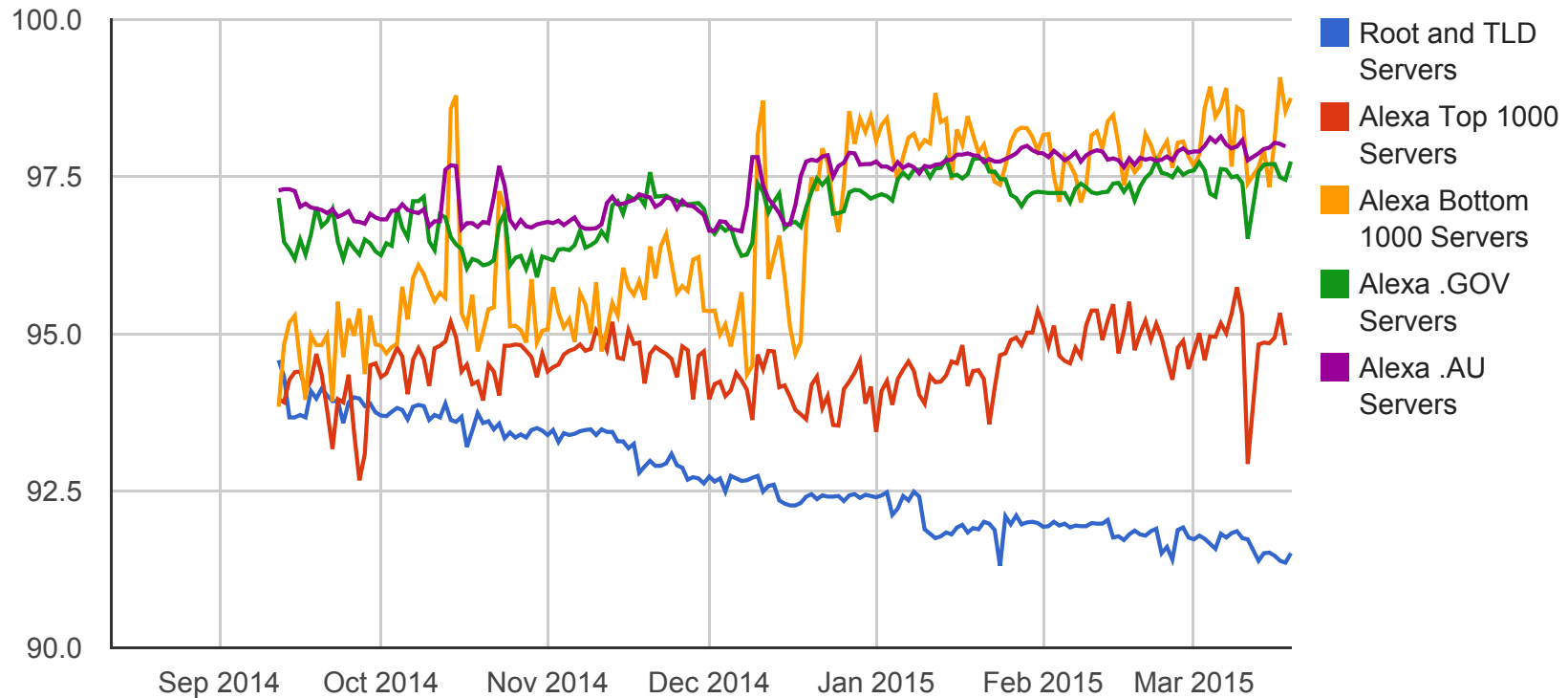
EDNS Compliance Report: 2015-03-19T05:19:26Z



2014-10-12 - 2014-10-15: Domaincontrol removed the firewall blocking EDNS version 1 and EDNS flags.

EDNS Compliance Report: 2015-03-19T05:19:26Z

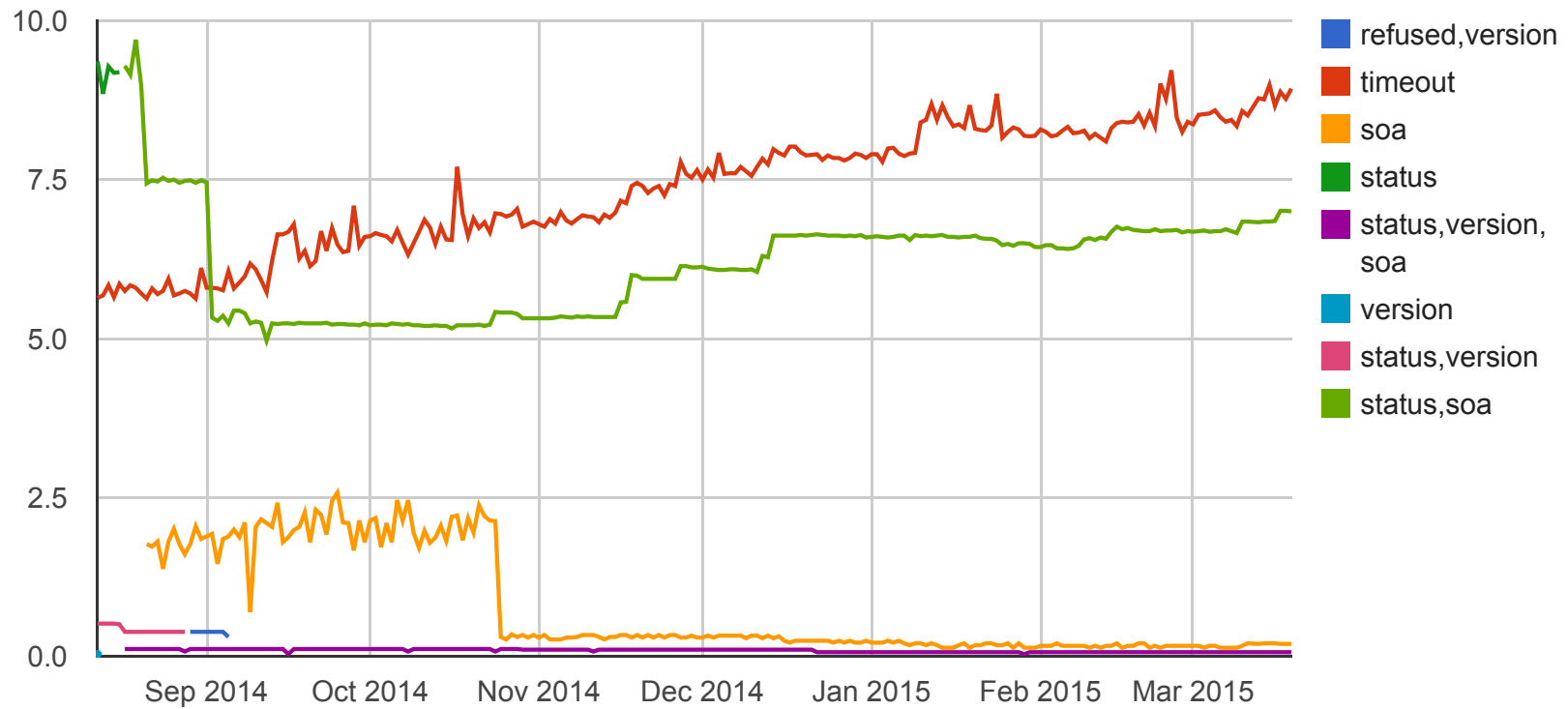
Percentage of responding servers that responded to a EDNS(0) request with a unknown flags



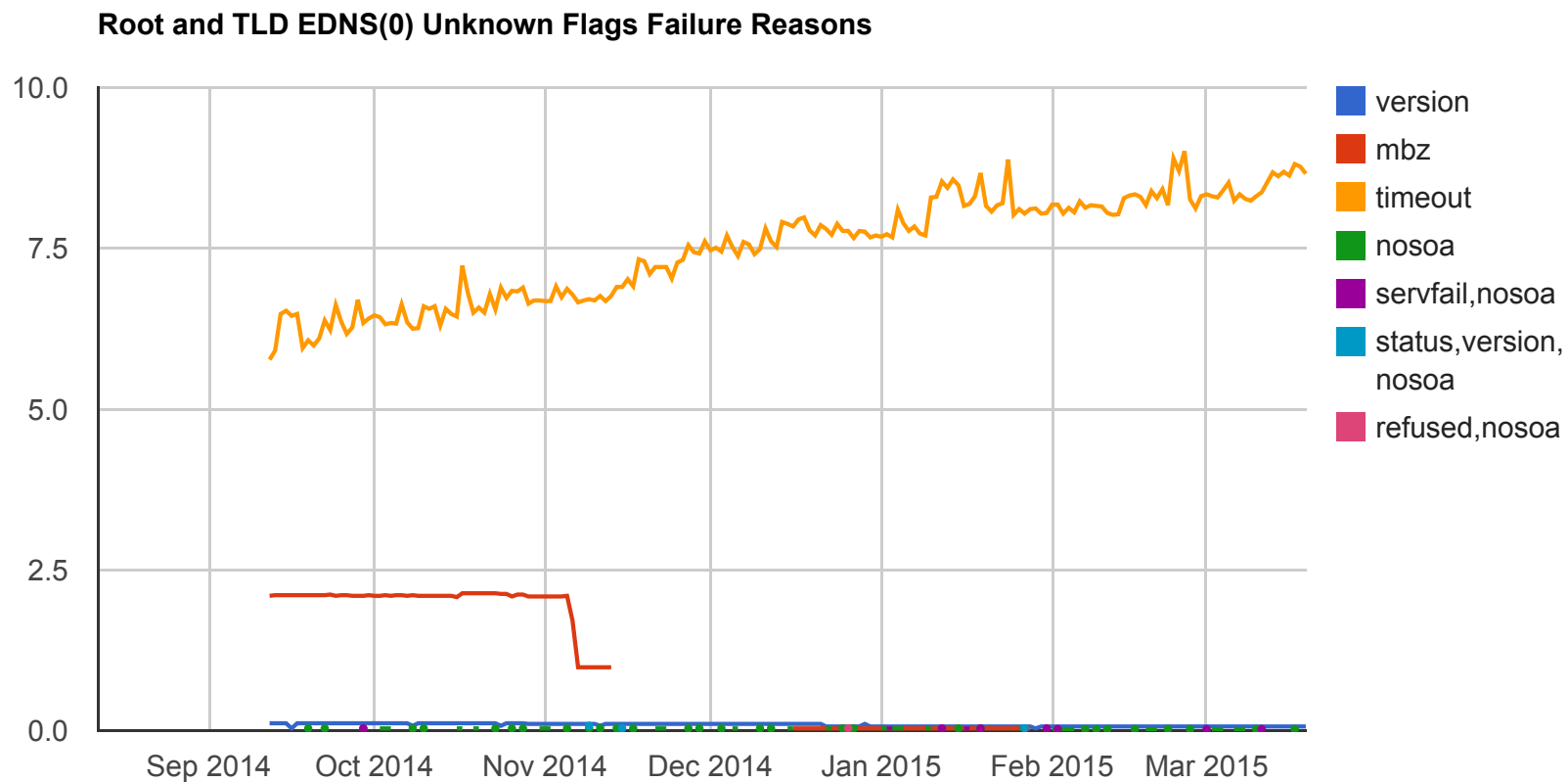
2014-10-12 - 2014-10-15: Domaincontrol removed the firewall blocking EDNS version 1 and EDNS flags.

EDNS Compliance Report: 2015-03-19T05:19:26Z

Root and TLD EDNS(1) Failure Reasons



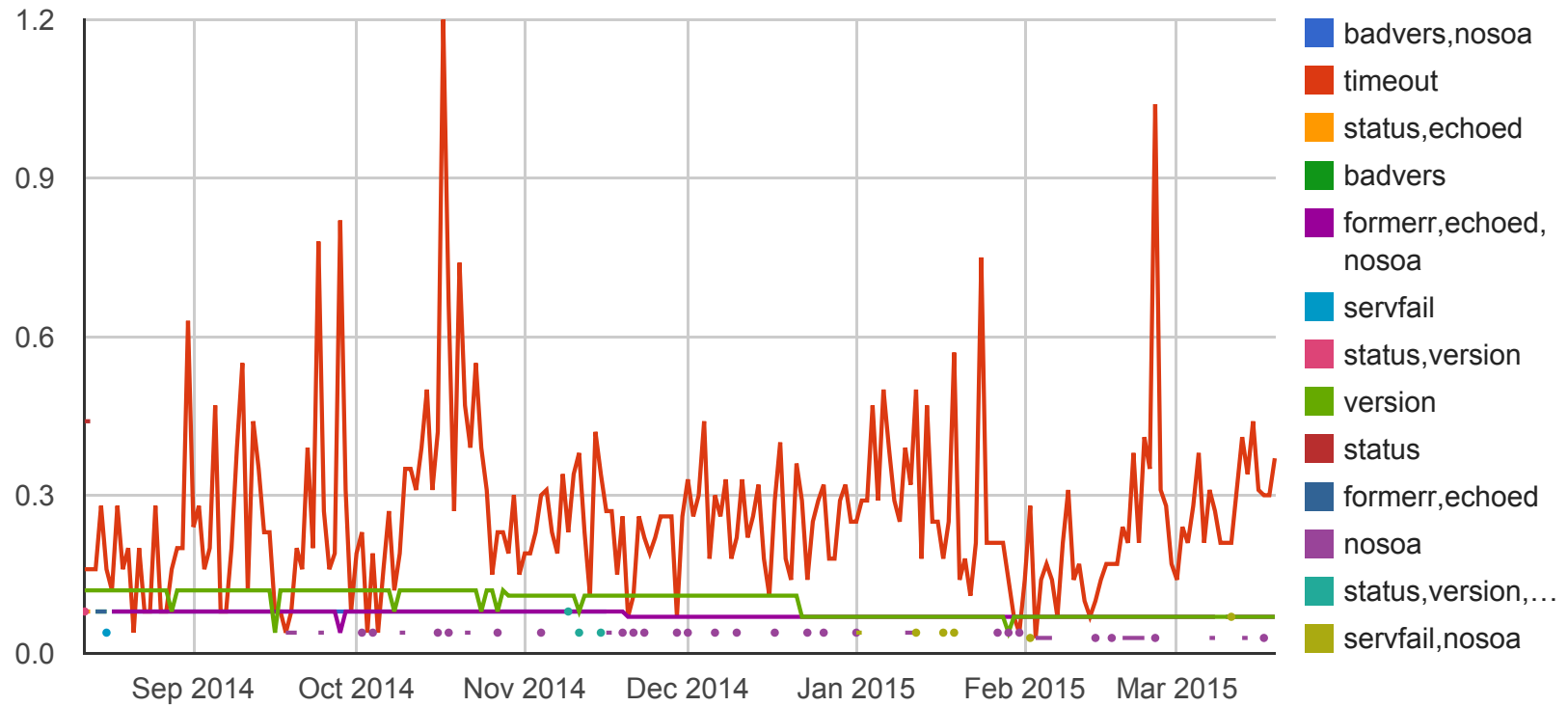
EDNS Compliance Report: 2015-03-19T05:19:26Z



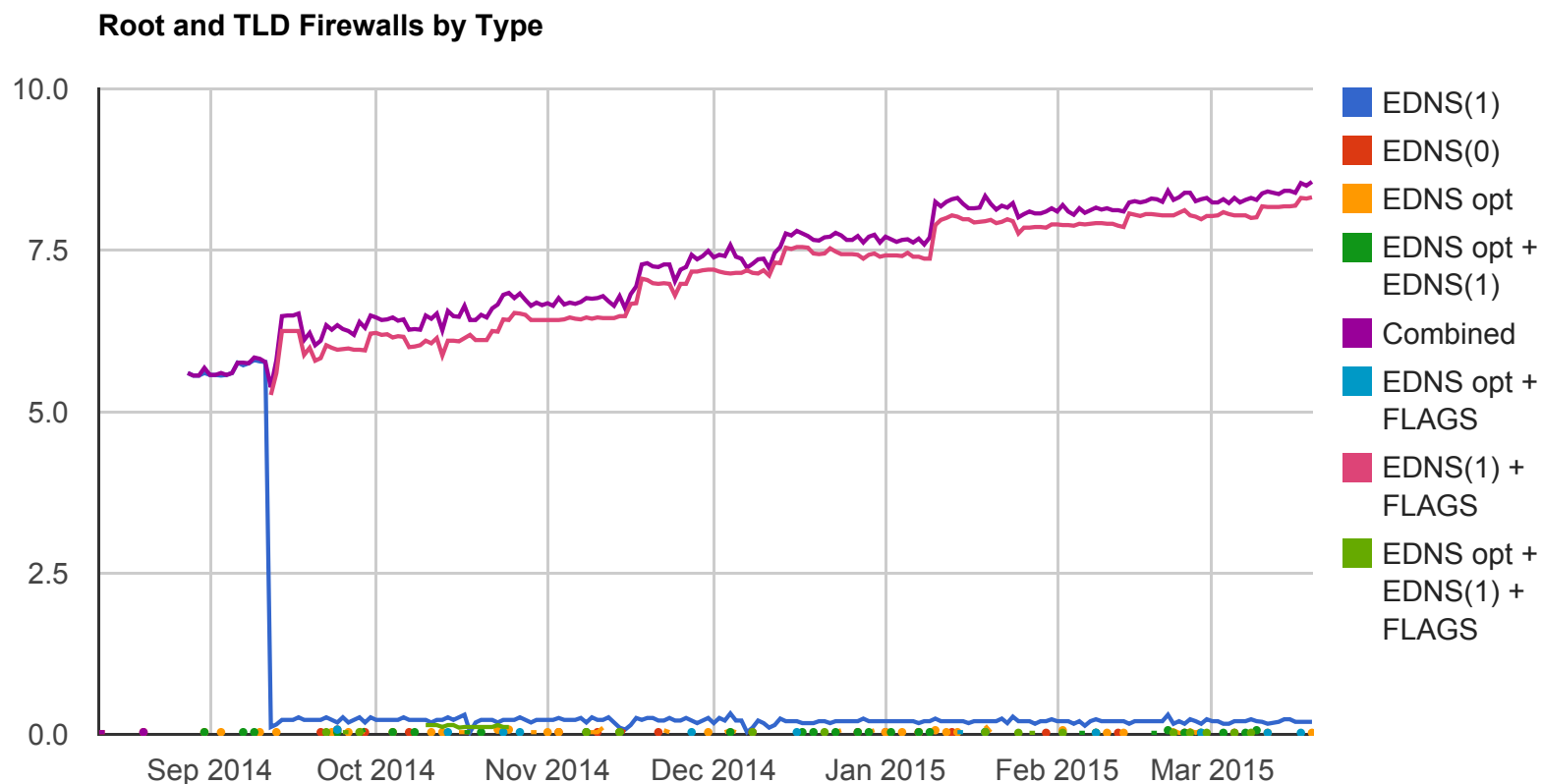
2014-09-14: operators returning unknown flags informed.

EDNS Compliance Report: 2015-03-19T05:19:26Z

Root and TLD EDNS(0) Unknown Option Failure Reasons



EDNS Compliance Report: 2015-03-19T05:19:26Z



EDNS(0) all EDNS queries have timeout and there was a response to the plain DNS query

EDNS(1) only the two EDNS version 1 queries timeout

EDNS(1) + FLAGS the two EDNS version 1 queries timeout as well as the unknown EDNS flags query

Where Next

- Extend draft-andrews-no-response-issue
(Working group adoption?)
- Contact Firewall Vendors
- Contact Nameserver Vendors
- Contact Zone Owners / DNS hosters
- Convince TLD/SLD operators to run regular checks
- Add to online DNS checkers.

More Information

- <http://users.isc.org/~marka/ts.html>
- <http://users.isc.org/~marka/tld-report.html>
- <http://users.isc.org/~marka/gov-report.html>
- <http://users.isc.org/~marka/au-report.html>
- <http://users.isc.org/~marka/alexa-report.html>
- <http://users.isc.org/~marka/bottom-report.html>
- <https://source.isc.org>