What roots do resolvers use

Looking under rocks

Roy Arends

IEPG
18 March 2018

Overview

- Queries recent list of public open resolvers for the root SOA record.
- Expected SOA was the most recent root SOA.
- results
- Some conjecture
- Conclusion
- Future work

What?

- Public-dns.info has a list containing 25881 open resolvers
- This site endorse the use of open resolvers
  - Lists them grouped by country
- You can add your own resolvers
  - Or others
- Their tests are straightforward.
  - Response must arrive within 3 seconds
  - No nxdomain re-write
  - Correct answer for wikileaks.org, youporn.com, archive.org, rotten.com and thepiratebay.org.
  - Check for AD bit

How?

- By sending a simple query for the root SOA record
- Compare the results with the latest SOA.
- TTL of the root SOA record is 1 day
- Tolerate at least two days of version numbering
  - Caching is a bit funky...
- This was a quick test with a limited set of resolvers. I have not
  - Checked for responses with AA or AD bit cleared or set
  - Checked for TTL values (or if they were decreasing)
  - Checked if multiple address had a single server
  - Checked if resolver’s address is the querying address
  - Checked the nameserver names and addresses

Why?

- To measure which roots these resolvers use.
- To measure how stale locally configured roots get.
- Most of all, if the results of this limited test warrant further study.

Results

- Of the 25881 addresses
  - 16835 returned a response (65%)
  - 13826 returned the expected SOA record
  - Of these expected SOA records:
    - 13800 returned expected SOA serial (at most 2 days off)
    - 5 had a different formatted SOA serial number (1520976703)
    - 21 had a serial number than was out of date (eldest is 2012041813)
- 3009 returned an unexpected (completely different mname, etc) SOA record.
- from those that responded, 22% (3009 out of 13826) have other roots configured.

Results

- many of these unexpected SOA root resolvers are registrar related
- Many of these are based in China
- 23 were opennic resolvers
- Some were signed.

Future work

- Expand the list of addresses
  - Naïve method: scan v4 space for open resolvers
    - Many non-production setups might skew the data
  - Naïve method: look at the topN root-server queries
    - They're obviously ask the IANA root.
  - Look at the topN addresses that query popular zone
    - See which are open.
  - Smart method:
    - Use RIPE ATLAS to send root-soa queries.
- Expand the list of tests
  - Check for AD / AA, check for single server multiple addresses, proxies, cache strategies, etc.

Top NXDOMAINs to the root

Quest for potential collisions

Roy Arends

IEPG
18 March 2018

Overview

- Fully automated daily aggregation of NXDOMAIN responses
- Group them by TLD string
- Order by Volume
- Order by unique address count
- Filter Applicant Guidebook compliant strings.
  - (3 ASCII letters or more)

Overview

TLD	Volume
local	113,549,380
home	78,920,086
openstacklocal	22,955,903
internal	22,921,636
localdomain	19,744,707
lan	13,521,890
dhcp	11,024,672
dlink	10,095,743
backnet	9,350,620
invalid	7,761,471

Overview

TLD	Volume
local	113,549,380
home	78,920,086
openstacklocal	22,955,903
internal	22,921,636
localdomain	19,744,707
\131	19,452,576
lan	13,521,890
dhcp	11,024,672
dlink	10,095,743
dhcp\032host	9,591,403

Overview

TLD	Unique Addresses
local	323,840
localdomain	122,075
home	90,185
lan	80,133
internal	56,522
corp	47,085
wpad	44,230
invalid	43,271
belkin	33,936
adsl	33,681

Overview

TLD	Unique Addresses
local	323,840
localdomain	122,075
home	90,185
lan	80,133
internal	56,522
corp	47,085
1	46,818
wpad	44,230
invalid	43,271
_tcp	_ 36,122

Engage with ICANN

Thank You and Questions

Visit us at **icann.org**
Email: email@icann.org

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

slideshare/icannpresentations

soundcloud/icann