Root Cause Analysis of ICANN Name Collisions Reports

Update: Feb 9, 2022

TLDs Associated with ICANN Name Collisions Reports

network
ads
prod
dev
cloud
google
school
anz

(in order of most frequently occurring)

app
cpa
csc
goo
kitchen
nyc
off
office
orange
Site
tech

As of Dec 1:

- For all (885) gTLDs delegated between August 2014 and June 2021
  - Extracted 100 days of DNS responses since its delegation (i.e., controlled interruption period) using Farsight security's DNSDB
  - Identified "suffixes" using:
    - chrome NXDOMAIN probing
    - wpad as first label
    - isatap as first label
- Result:
  - 2761 suffixes
    - 2300 (86%) of which are longer than a TLD - this means that there is more identifying information to go on
  - There was a high correlation between the number of suffixes seen for a TLD and the number of ICANN reports for a TLD

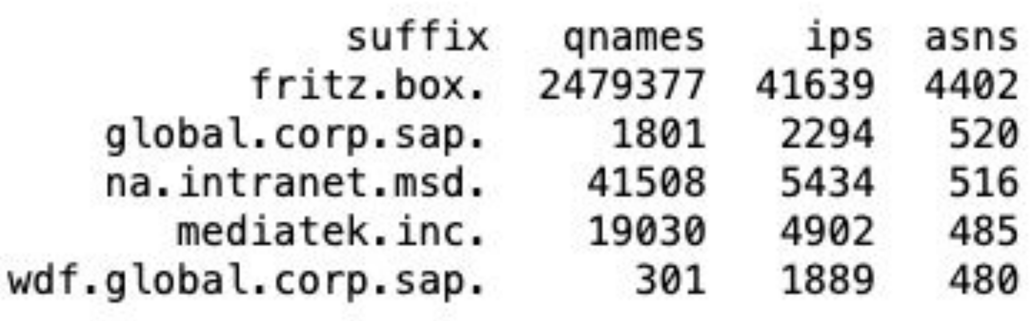
Questions to Answer

- Can we use query data at root servers to learn whether the suffixes queried during controlled interruption period are still being issued?
- Has the quantities of queries changed over time?
- Has the diversity of queries changed over time?
- Can we use query data to identify specific organizations that might be affected by delegation of new gTLD?

Methodology

- Extracted query information (qname, IP address) for (most) TLDs having suffixes in the list of suffixes identified with Chome, wpad, isatap
    - DITL 2014, 2016, 2017 (others in progress)
- Further filtered query information:
    - Only include non-TLD suffixes (i.e., the 86%)
- Further filtered to just a sample, to hone code and methodology:
    - Only include 1M queries from 2016 a-root data
- Results:
    - 1,609 (70%) of suffixes appear in this data set
    - Suffixes from 16 (80%) of reported TLDs appear in the data set
    - 1,097 (68%) of suffixes in queries are associated with reported TLDs

Examples



```
             suffix   qnames    ips  asns
          fritz.box. 2479377  41639  4402
    global.corp.sap.    1801   2294   520
    na.intranet.msd.   41508   5434   516
       mediatek.inc.   19030   4902   485
wdf.global.corp.sap.     301   1889   480
```