# NCAP Case Study Report

Prepared for ICANN NCAP

by John Kristoff and Steve Sheng

# The NCAP Discussion Group Case Study Report

**Introduction and Background**

**Data and Methodology**

**Results**

**Analysis**

**Conclusions**

# Introduction

SSAC led study on data and analysis of DNS name collisions

Name Collision Analysis Project (NCAP) discussion group formed

Initial study submitted to ICANN board on 2020-06-19

Revised Study 2 described in SSAC2021-02 asked for case studies

This report presents case studies for the following TLDs:

.CORP .HOME .INTERNAL .LAN .LOCAL .MAIL

# Background - Interisle study

Evaluated the consequences collisions on the 6 names

2013 report drawn from the following sources:

- 2012 and 2013 DITL data
- 2012 request stream from resolver operator
- Data related to internal names in CA issued X.509 certs

Concluded there was potential risk of harm for the 6 strings

# Background - JAS study

Focused on the collision mitigation and reducing risk

Report drawn from DITL 2012 and 2013 data

Produced a number of recommendations including:

- Publish RFC 1918 equivalent for .corp, .mail, .home
- Formalize ICANN's DNS emergency response procedures
- Consider collecting and analyzing NXDOMAIN responses

# Data and Methodology

Multi-year longitudinal A-ROOT and J-ROOT query data

- Query volume (daily)
- QTYPE distribution
- Unique daily query source IPv4 and IPv6 addresses
- Geographic distribution
- ASN distribution
- Label (analysis) distribution
- SLD overlap between roots
- ASN overlap between roots

# Limitations

Focused on aggregate view

- As opposed to regional/local patterns

Changes to technology limit visibility

- Such as QNAME minimization, DNS over ??? transports

Limited vantage points

- e.g. queries arriving at resolvers unexamined

# Results

Generally graphs of volume are up and to the right

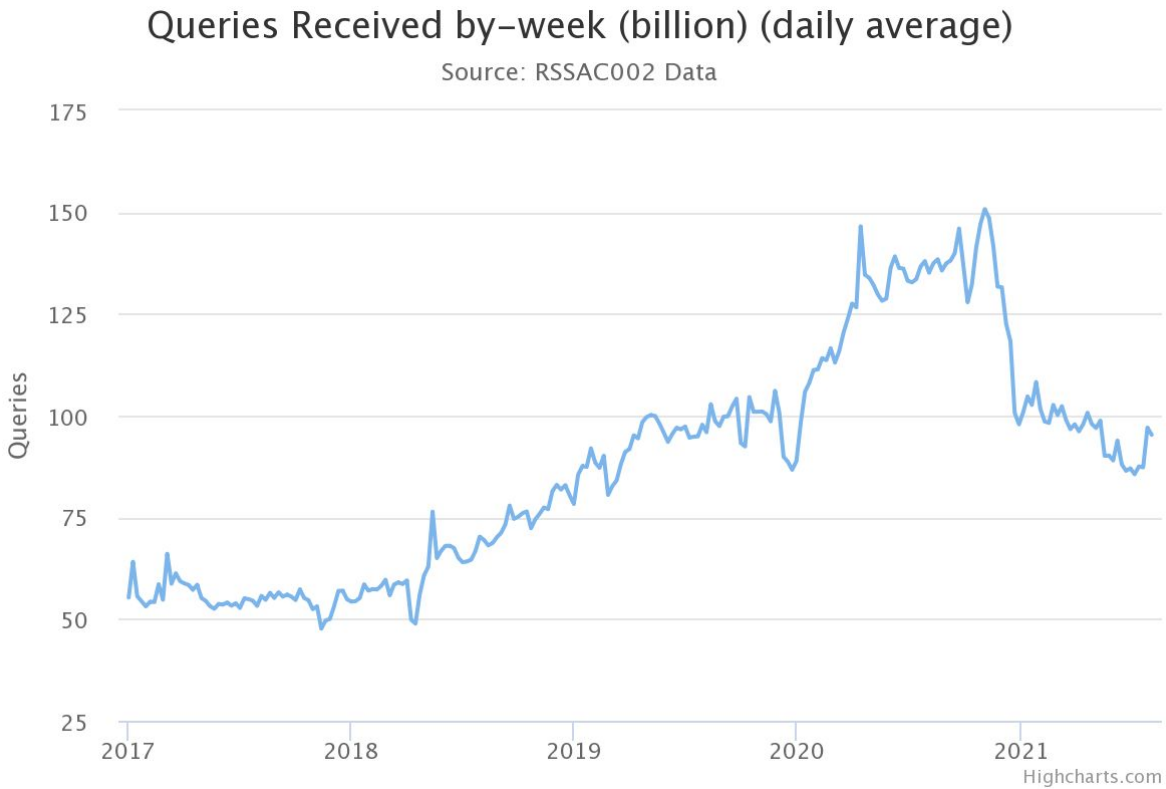
Some obvious anomalies

e.g. end of 2020 drop due to Chromium change

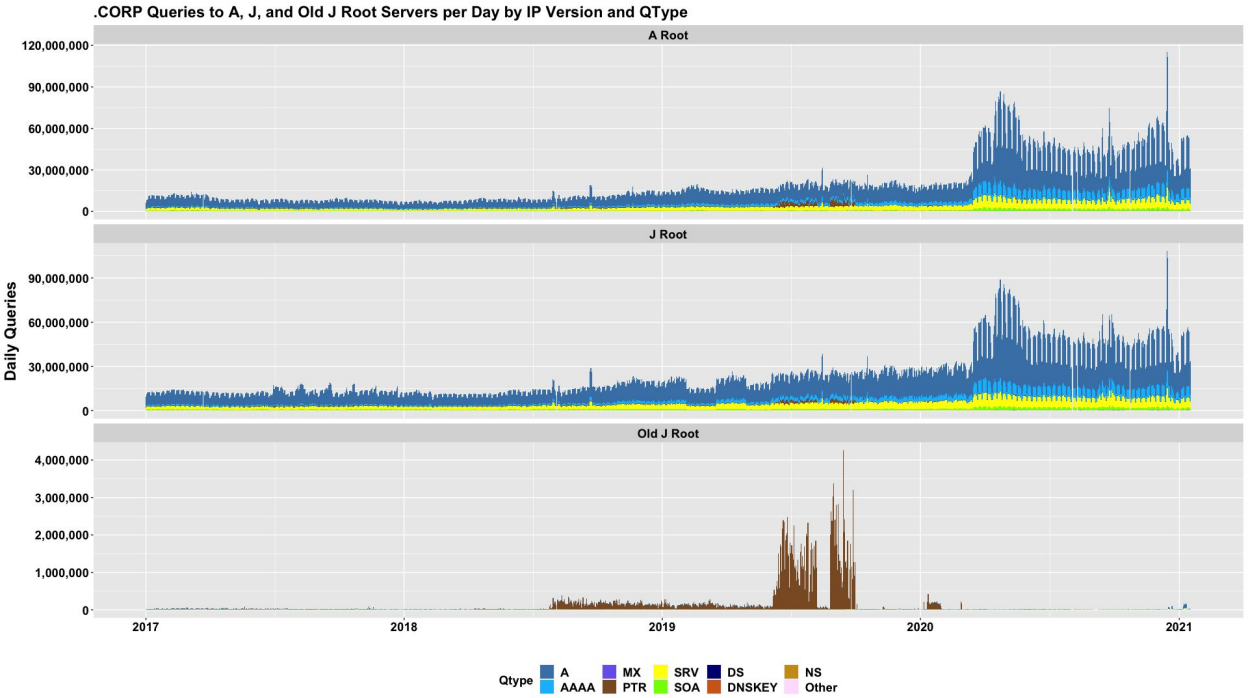
Query source diversity continues to expand

Label analysis provides rich basis for understanding behavior

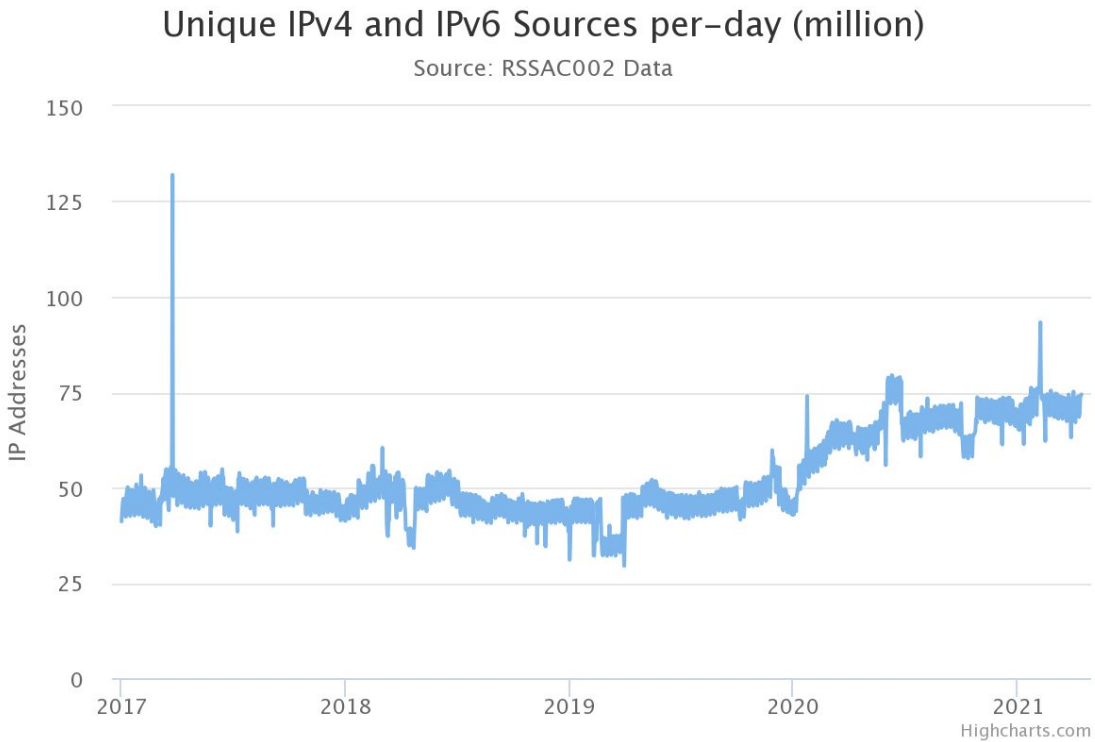
# Query Volume



# QTYPE Distribution



# Query Source Address Diversity



# Label Analysis (.mail)

| | SLD | % |
|---|---|---|
| 1 | g | 8.2588799 |
| 2 | _ | 6.7988669 |
| 3 | yahoo | 6.2023317 |
| 4 | antivirusufv | 4.5026149 |
| 5 | www | 4.0041403 |

| | Third label | % |
|---|---|---|
| 1 | wpad | 19.8957231 |
| 2 | winhexbemig15 | 6.4311622 |
| 3 | winhexbemig16 | 6.3125283 |
| 4 | _ldap | 3.6859604 |
| 5 | winhexbemig13 | 3.2862324 |

# Analysis

*Critical Diagnostic Measurements*: properties that best determine the scope, impact, and potential harm of name collisions.

Query Volume - DNS query count
Query Origin Diversity - IP address and ASN distribution
Query Type Distribution
Label Diversity
Other Characteristics - OSINT of string being used

# Conclusions

These case studies have provided invaluable insight

Precise accounting of potential harm is extremely difficult

Additional analysis from other vantage points may be helpful

Controlled experiments could help, but tricky to perform

New technologies (e.g. DNS over ???) need to be considered

There would be impact if .CORP/.HOME/.MAIL are delegated