

WeirDNS: Measuring Bogon Address Exposure in DNS

Fariba Osali, Iman Alipour, Carlos H. Gañán
Anja Feldmann, Tobias Fiebig



DNS OARC 47 (Vancouver, BC)
Nov 8-11, 2026



MAX-PLANCK-INSTITUT
FÜR INFORMATIK



UNIVERSITÄT
DES
SAARLANDES



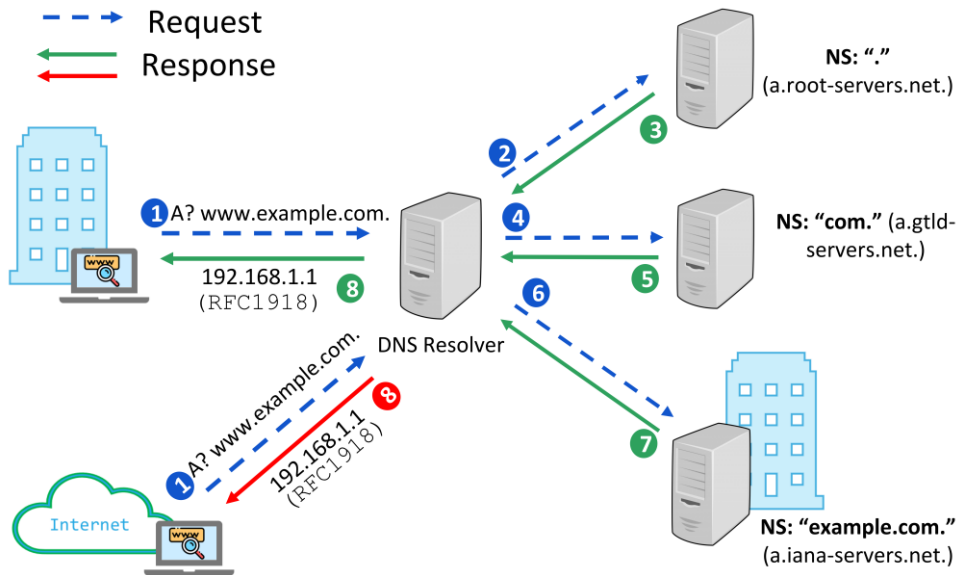
TECHNISCHE
UNIVERSITÄT
WIEN





Introduction

- Split-view DNS
- Bogon addresses are generally not intended for global routing.





Motivation

- The network operations community called for such a study at RIPE 88
- Shortage of private IP address space
- Emerging use of 240.0.0.0/4 and other reserved IP address ranges in GKE and AWS.
- Reserved IPv6 addresses are a notable problem for assessing IPv6 readiness in DNS.

Dataset



DNS Dataset
Jan 2015 to
Apr 2025



Data Filtering



DNS Dataset
Jan 2015 to
Apr 2025

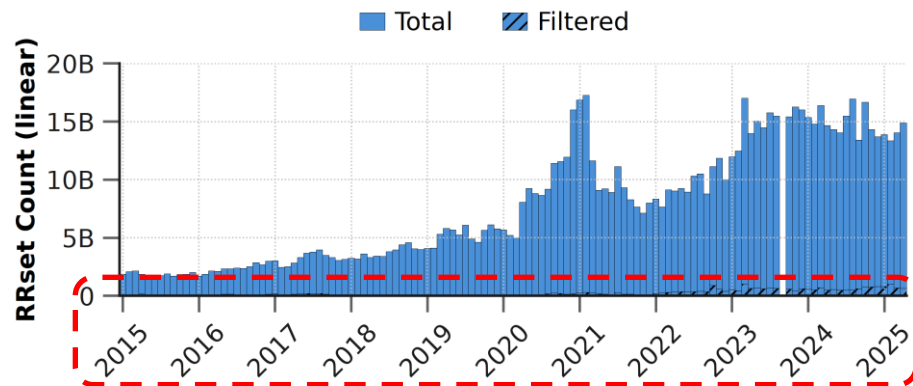


Resource Record
sets filtering

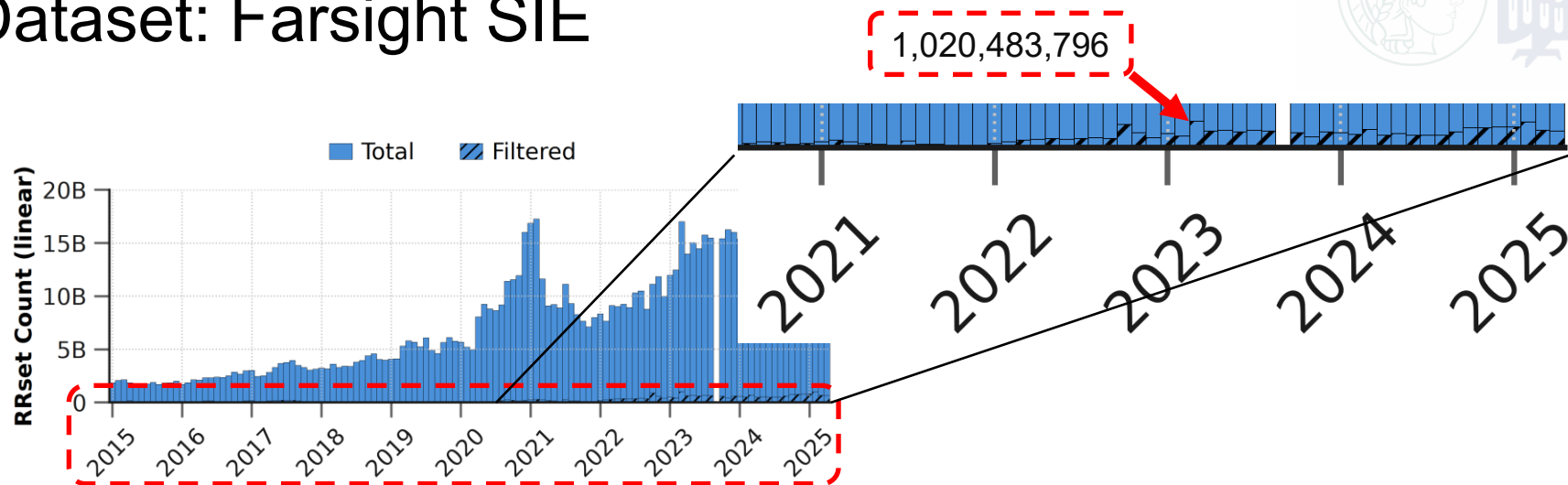
Filtering of RRsets

- Bogon IPv4/IPv6 addresses in rdata
- Invalid TLD
- PTR record structural validation
- Uncommon or non-standard record Types (A6 or TYPE records)

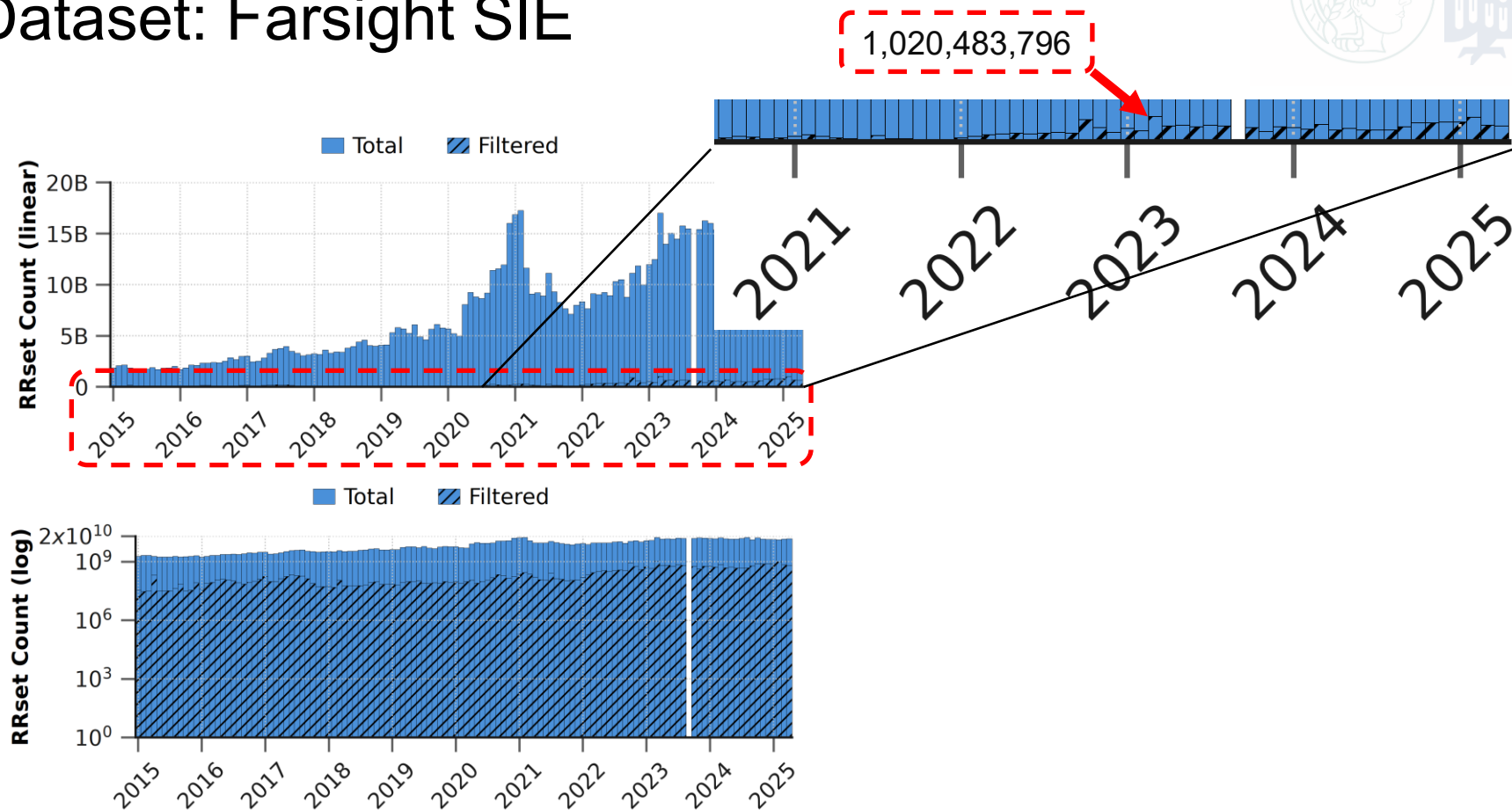
Dataset: Farsight SIE



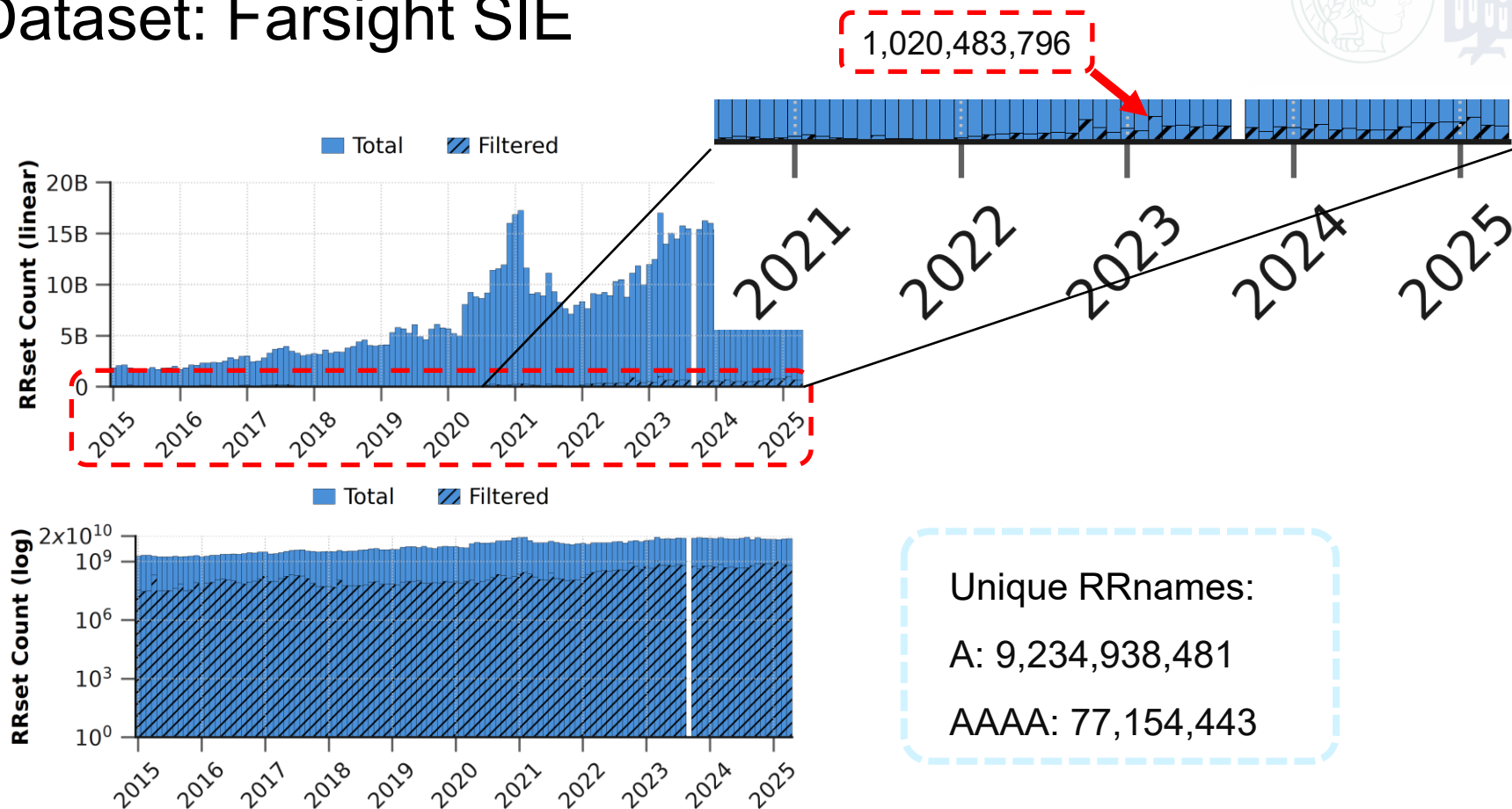
Dataset: Farsight SIE



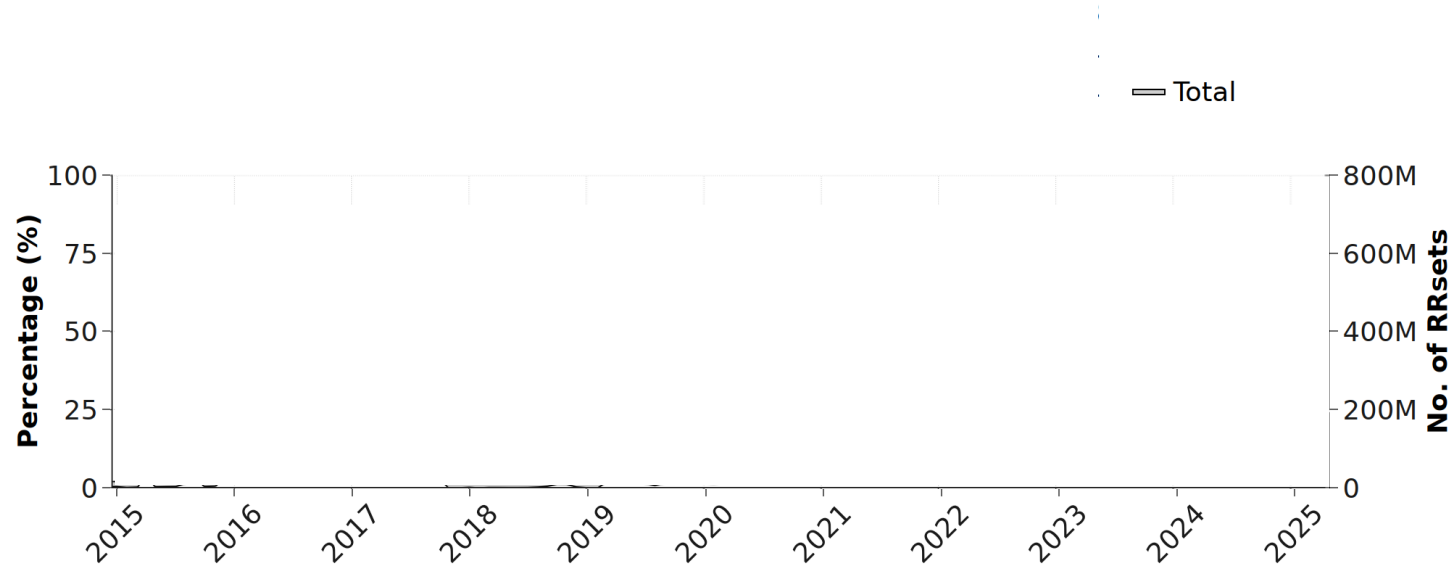
Dataset: Farsight SIE



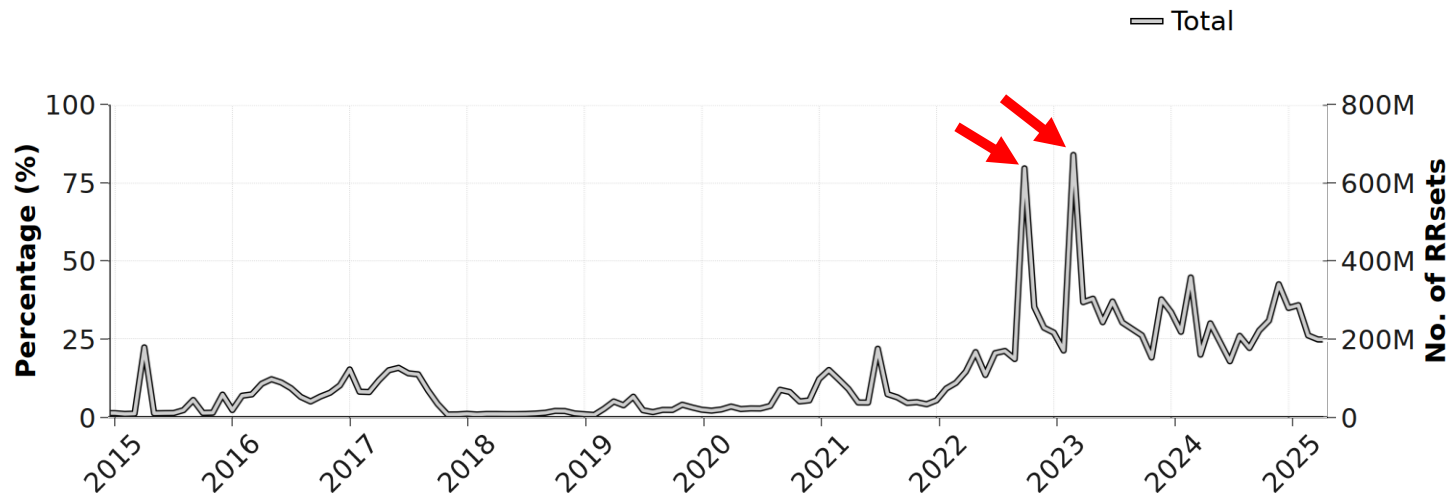
Dataset: Farsight SIE

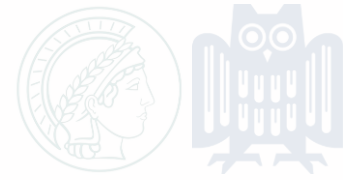


Analysis of “A” Resource Records

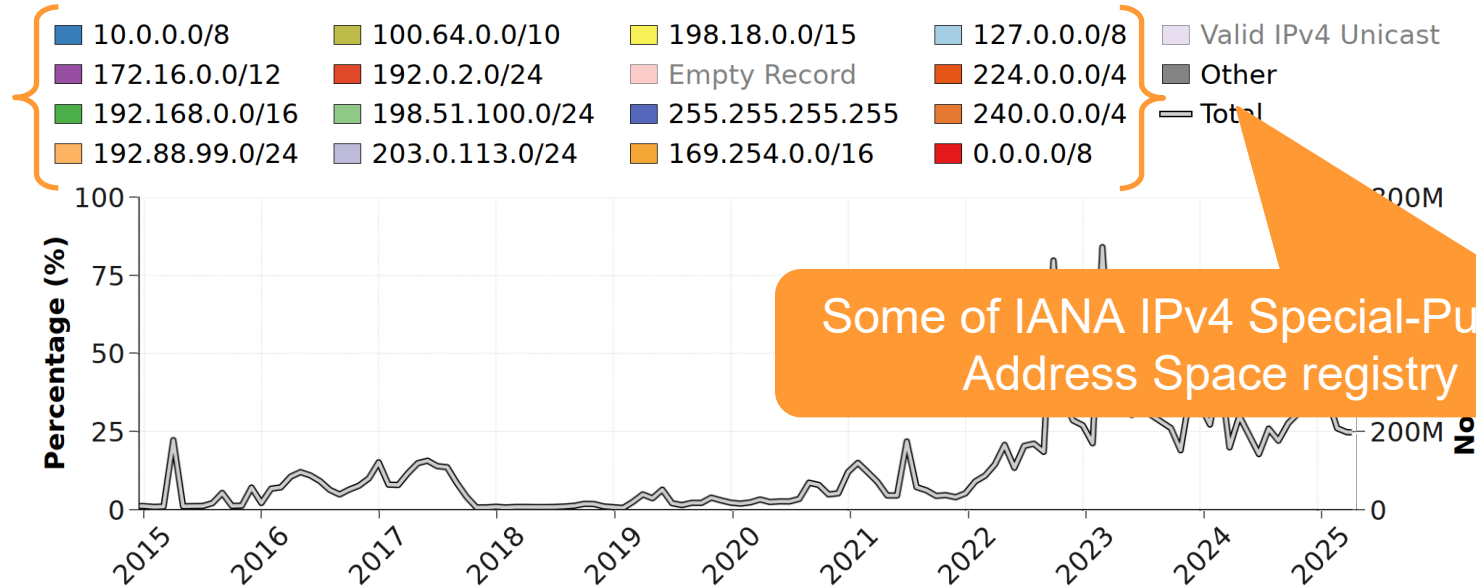


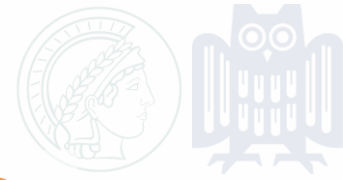
Analysis of “A” Resource Records



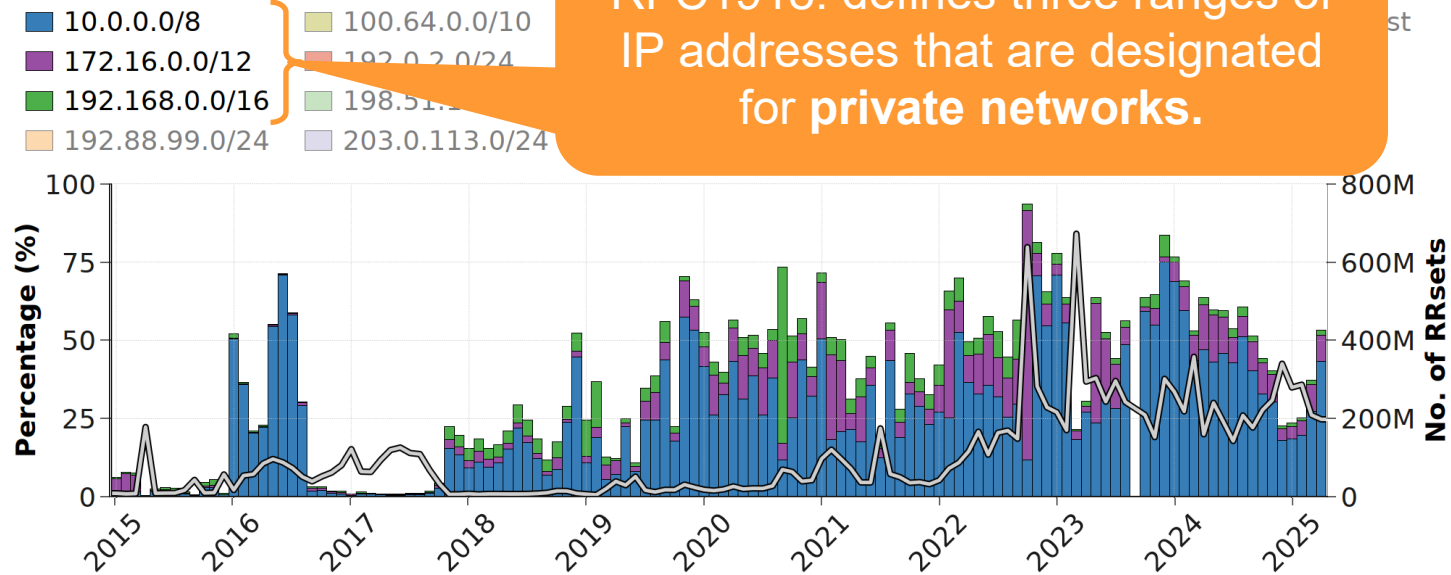


Analysis of “A” Resource Records



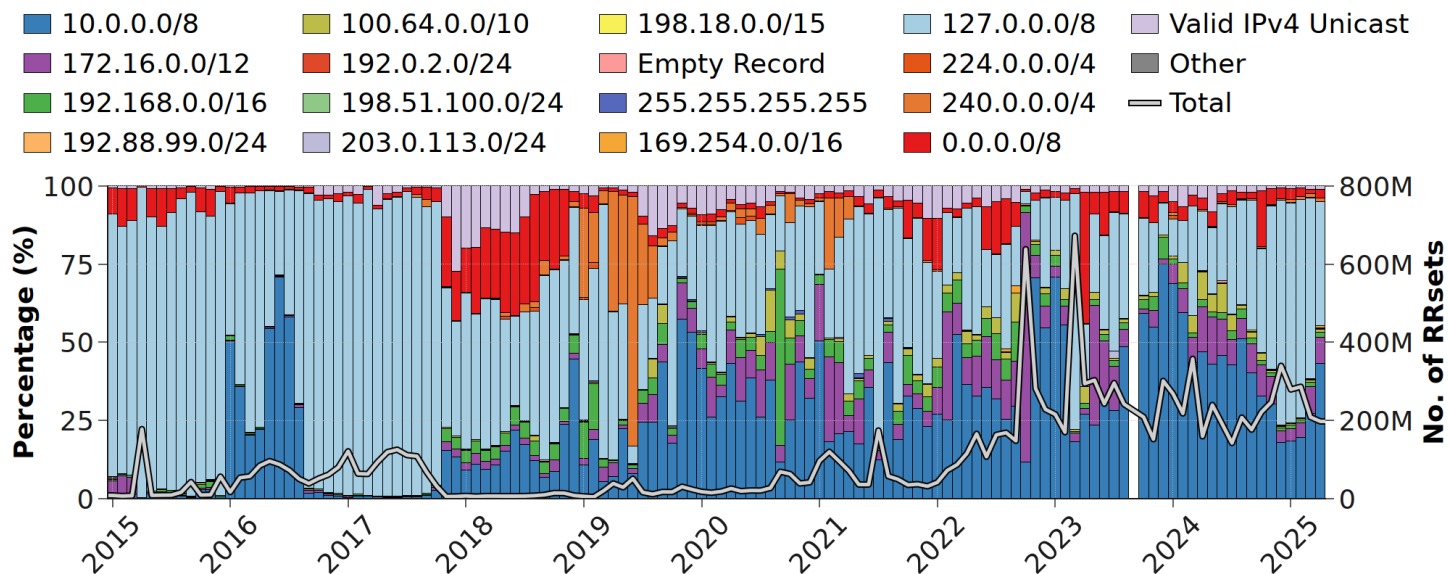


Analysis of “A” Resource Records



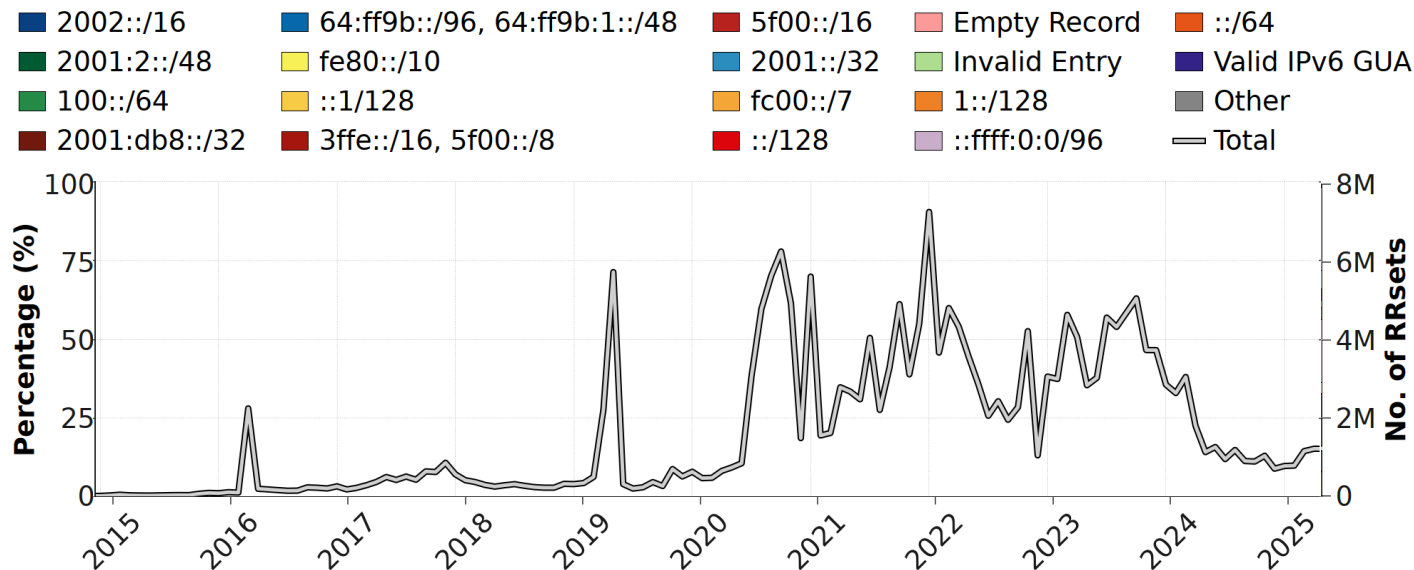


Analysis of “A” Resource Records

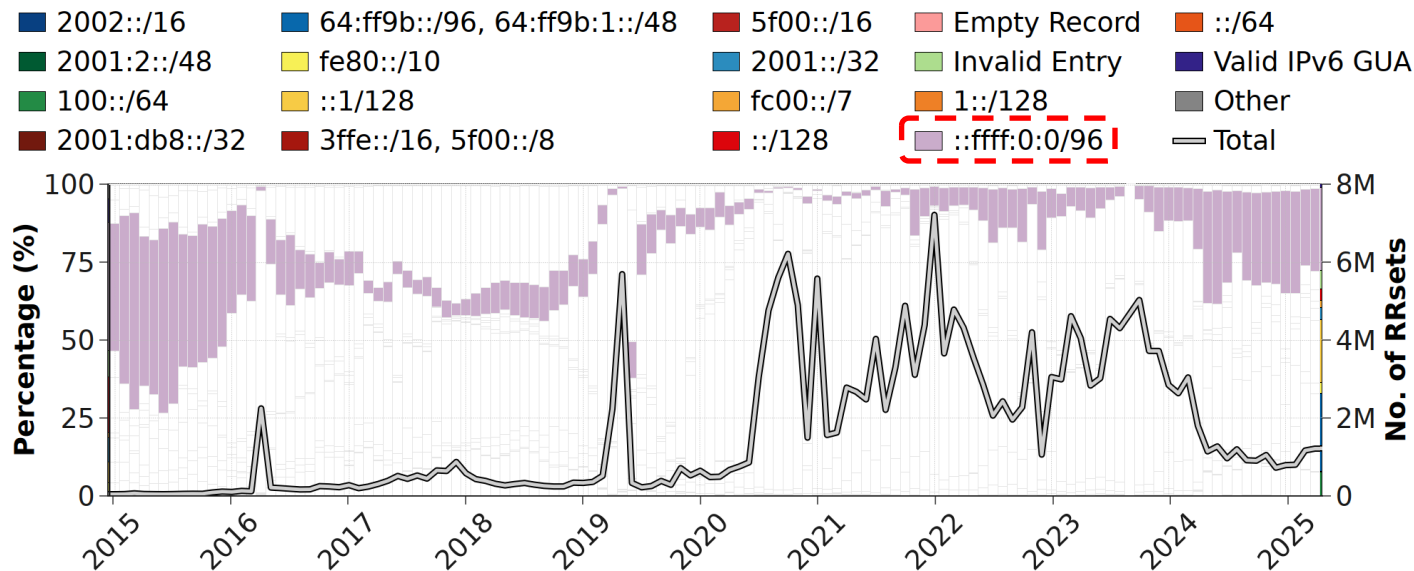


Bogon IP addresses appeared a lot in IPv4 DNS resolutions

Analysis of “AAAA” Resource Records

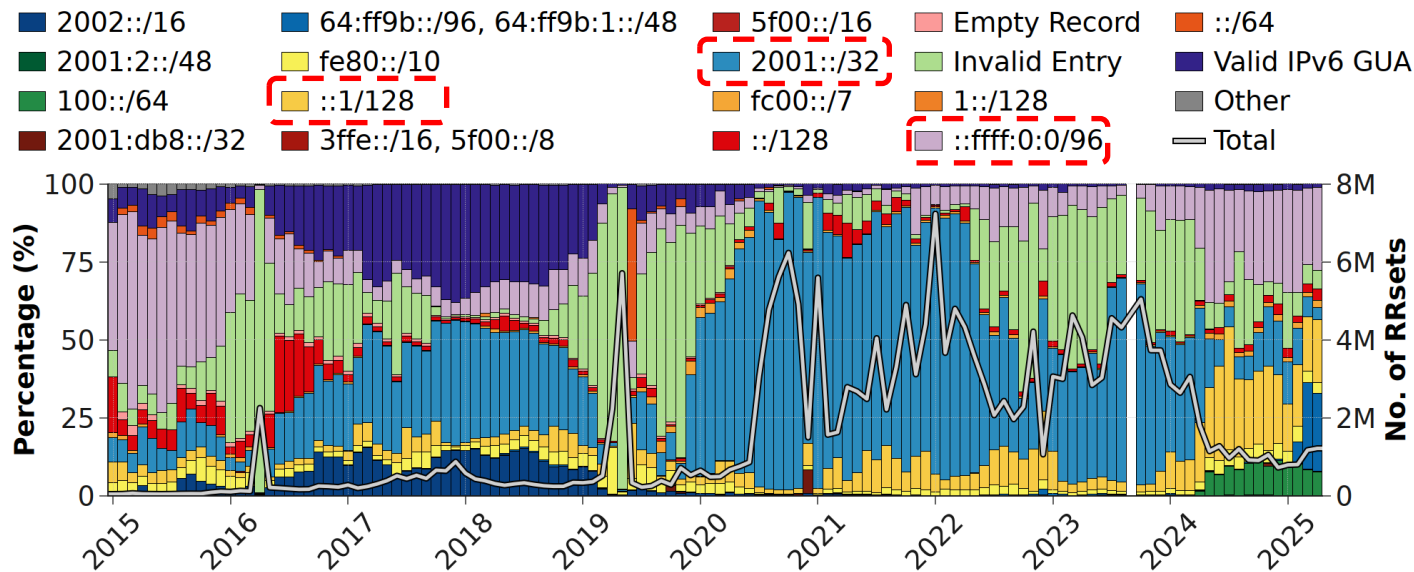


Analysis of “AAAA” Resource Records



IPv4-mapped IPv6 (::ffff:0:0/96) addresses containing mapped public IPv4 addresses.

Analysis of “AAAA” Resource Records

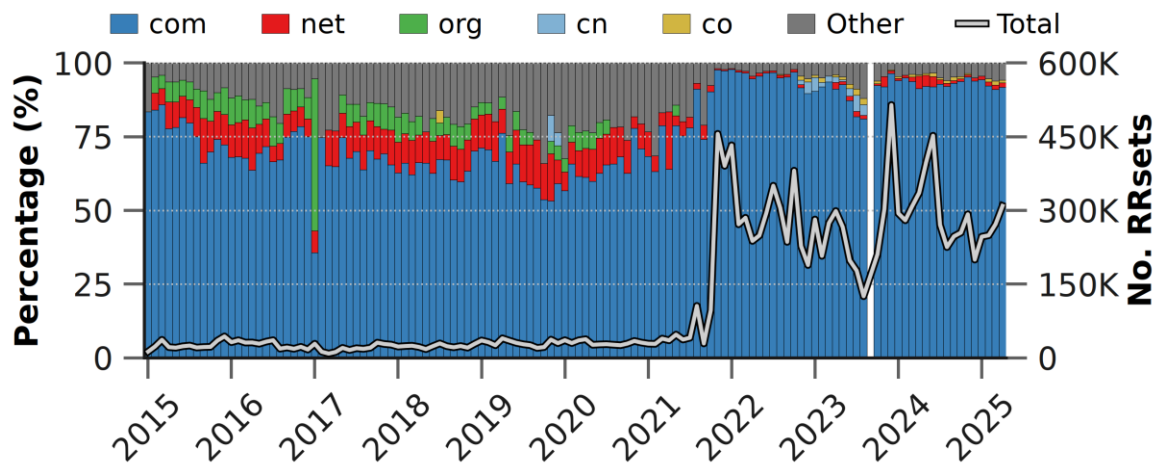


Teredo (2001::/32), IPv4-mapped addresses (::ffff:0:0/96), and ::1/128.



Case-Study: v4-mapped-v6 addresses

- The increase by an order of magnitude from late 2021.
- Related to `opendns.com`, a component of Cisco's umbrella service.





Auto-Generated Subdomains

- Static wildcard: many names resolve to the same IP address

Catch-all records

```
*.example.com.    IN    A    192.168.1.1
```

Any subdomain that is not explicitly defined (e.g., test.example.com, random.example.com) will resolve to 192.168.1.1.



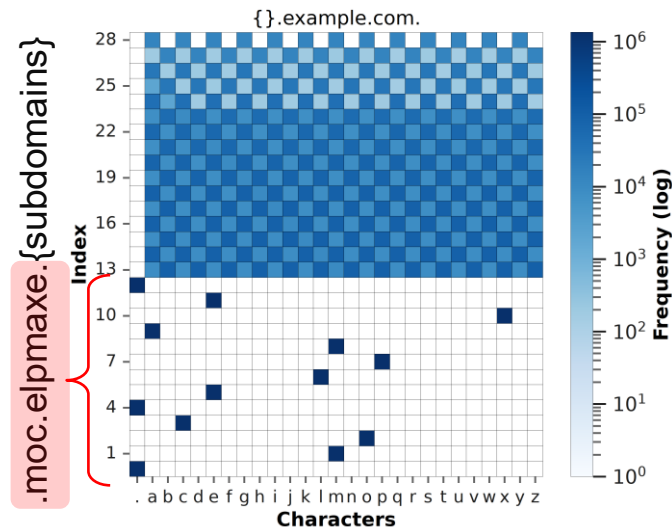
Auto-Generated Subdomains

- Static wildcard: many names resolve to the same IP address
- Auto-generated subdomains
- Chess pattern like subdomains



Auto-Generated Subdomains

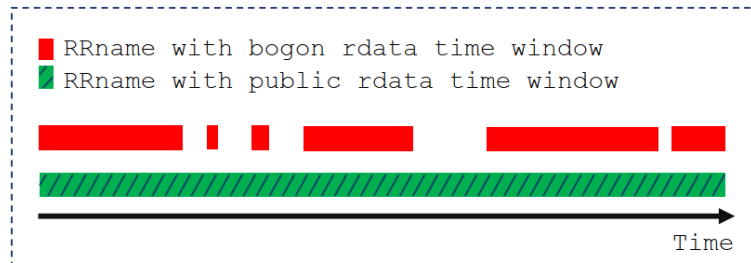
- Static wildcard: many names resolve to the same IP address
- Auto-generated subdomains
- Chess pattern like subdomains





Public and Private IP Addresses Overlap

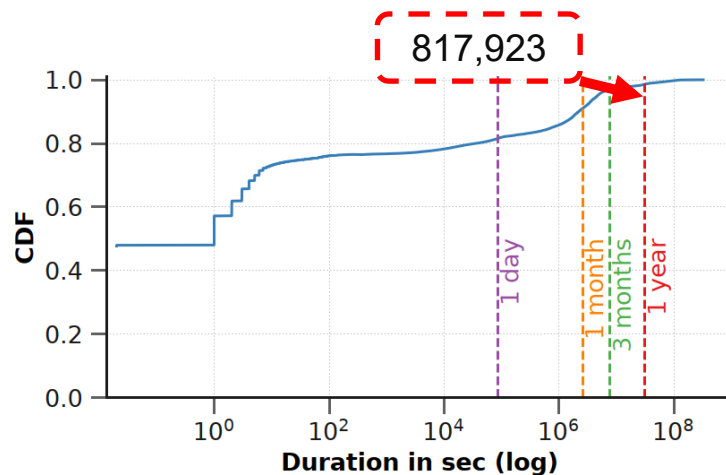
- Overlapping time windows of public and bogon RRsets for the same RRname.





Public and Private IP Addresses Overlap

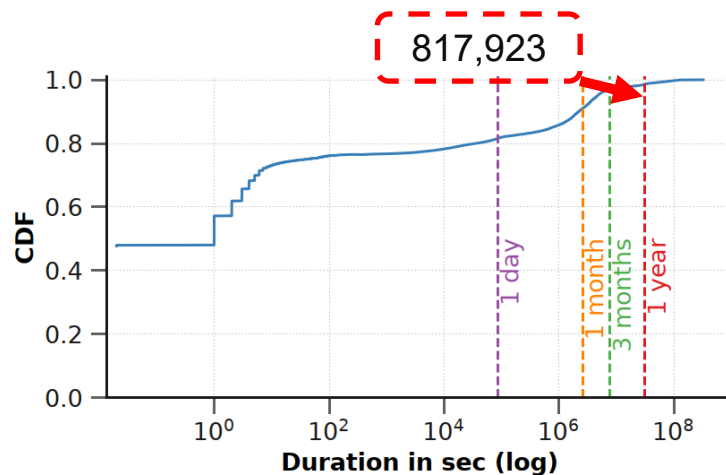
- Overlapping time windows of public and bogon RRsets for the same RRname.





Public and Private IP Addresses Overlap

- Overlapping time windows of public and bogon RRsets for the same RRname.
- Top 5 gTLDs: com, net, info, edu, org
- Top 5 ccTLDs: de, ir, cn, ru, in



Summary

- Bogon IP addresses in the public DNS are quite common.
- “Weird” answers often reflect deliberate choices, automation, leakage, or malicious activity rather than random noise.



fosali@mpi-inf.mpg.de



<https://www.linkedin.com/in/fariba-osali/>