For confidence, click here.

The Impact of Negative Caching and DNS Resolution Failures

Yannis Labrou & Matthew Thomas, Verisign

February 8th, 2024

OARC 42, Charlotte, NC, USA

Understanding the impact

- Observed several incidents of aggressive resolver behavior during DNS outages over the last several years
  - Facebook and .CLUB outages as well as botnet domains

- RFC9520 Negative Caching of DNS Resolution Failures
  - Updates RFC2308 to require negative caching of all DNS resolution failures

- **Goal**: To better quantify the amount of retry queries to authoritative servers during resolution failure scenarios

SERVFAIL/TIMEOUT responses of child zones lead to recursive **consistent, persistent and sizeable** re-querying of TLD authoritatives

Consistent

- ASNs have consistent % of their traffic attributed to re-querying

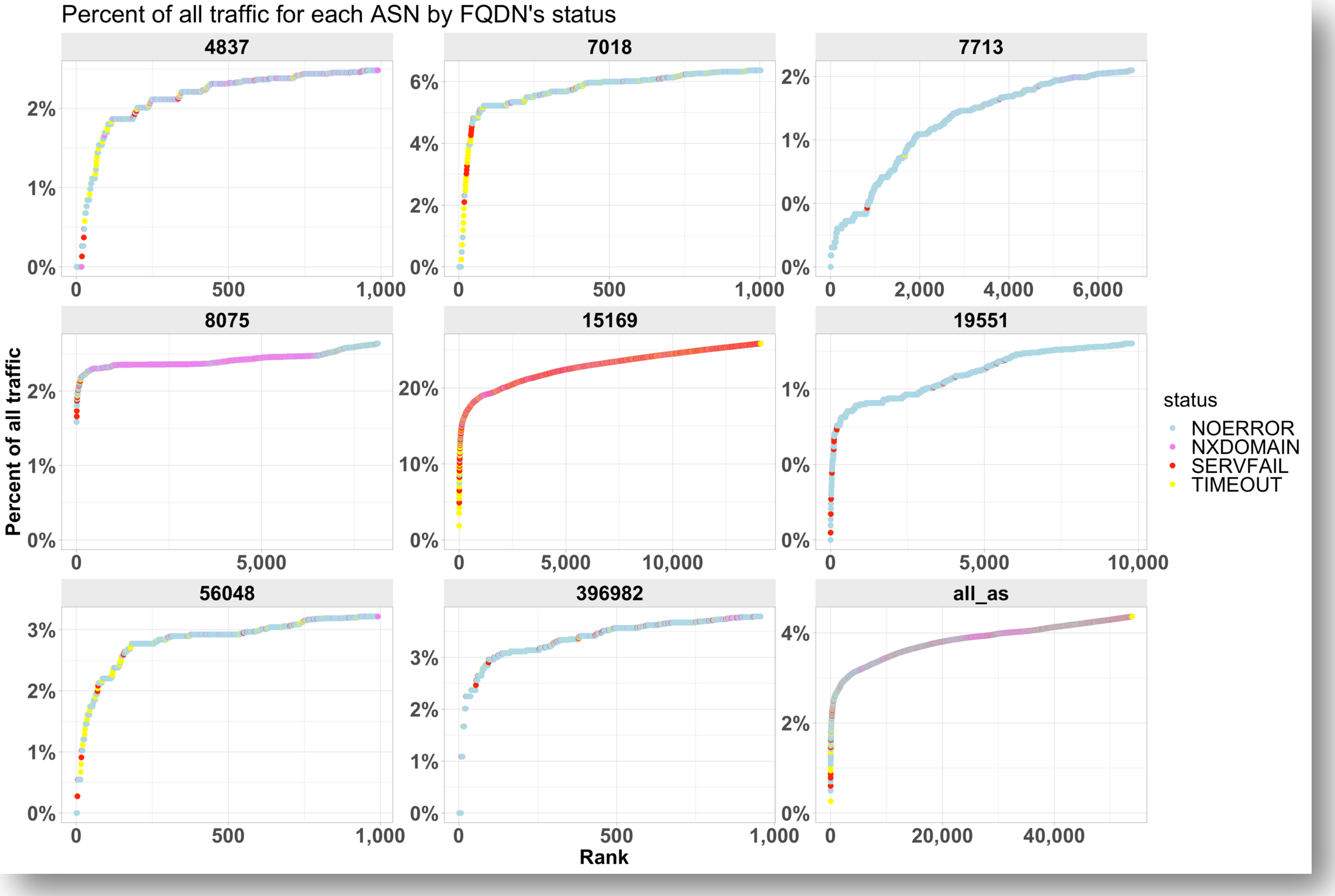
Persistent

- Specific SERVFAIL/TIMEOUT SLD's persist over long periods of time

Sizeable

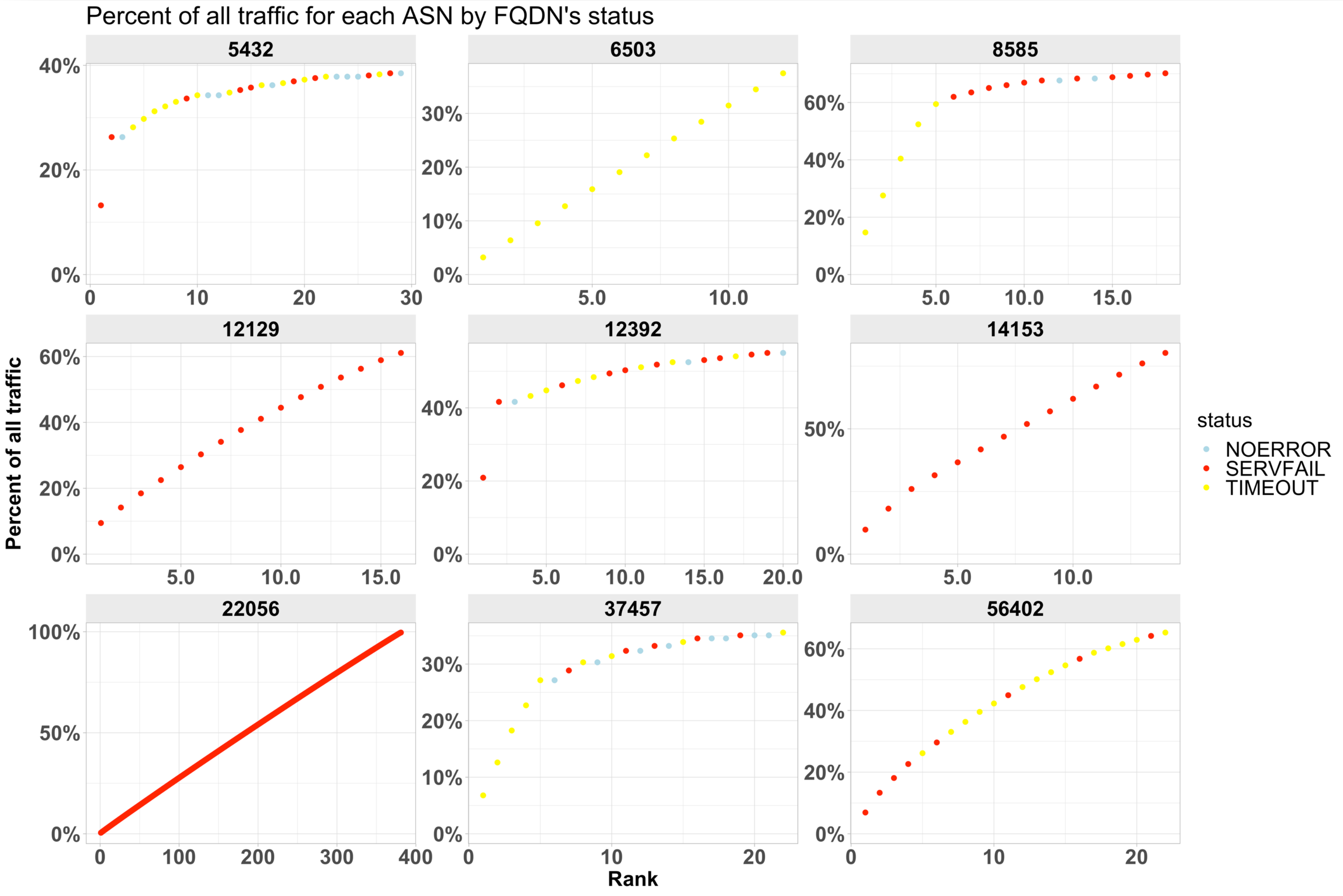
- 2.5% - 5% of traffic to COM/NET authoritatives
- 10% - 25% of traffic to COM/NET authoritatives for a top talker AS

Snapshot: CDF of SERVFAIL/TIMEOUT-attributable traffic as a % of total traffic, per AS by rank for **top talker** ASN's to COM/NET authoritative name servers. Red dots are SERVFAIL FQDN's and Yellow is TIMEOUT



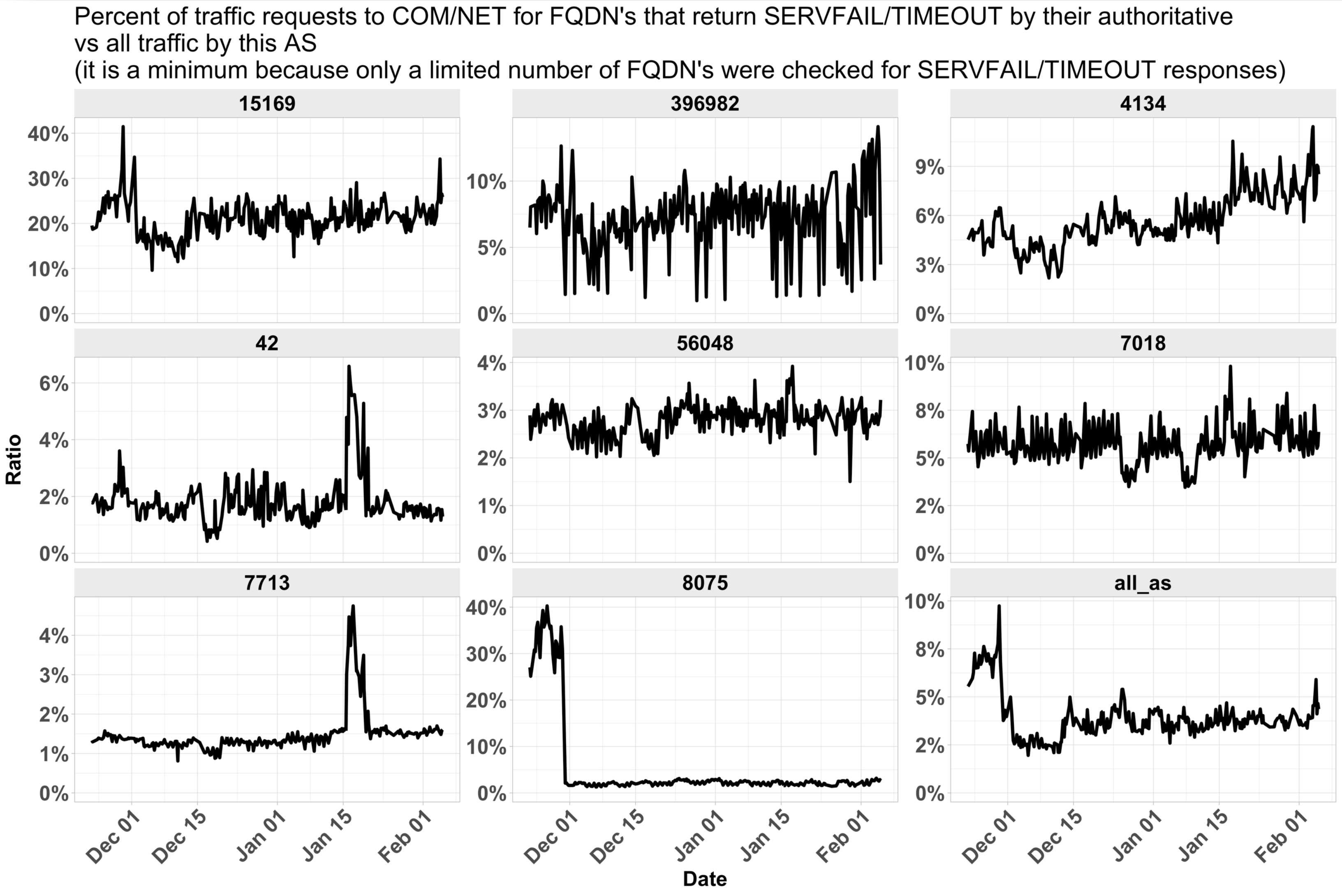
x-axis is FQDN rank

Snapshot: CDF of SERVFAIL/TIMEOUT-attributable traffic as a % of total traffic, per AS by rank for ASN's with **highest ratio** SERVFAIL/TIMEOUT traffic to COM/NET authoritative name servers. Red dots are SERVFAIL and Yellow is TIMEOUT



x-axis is FQDN rank

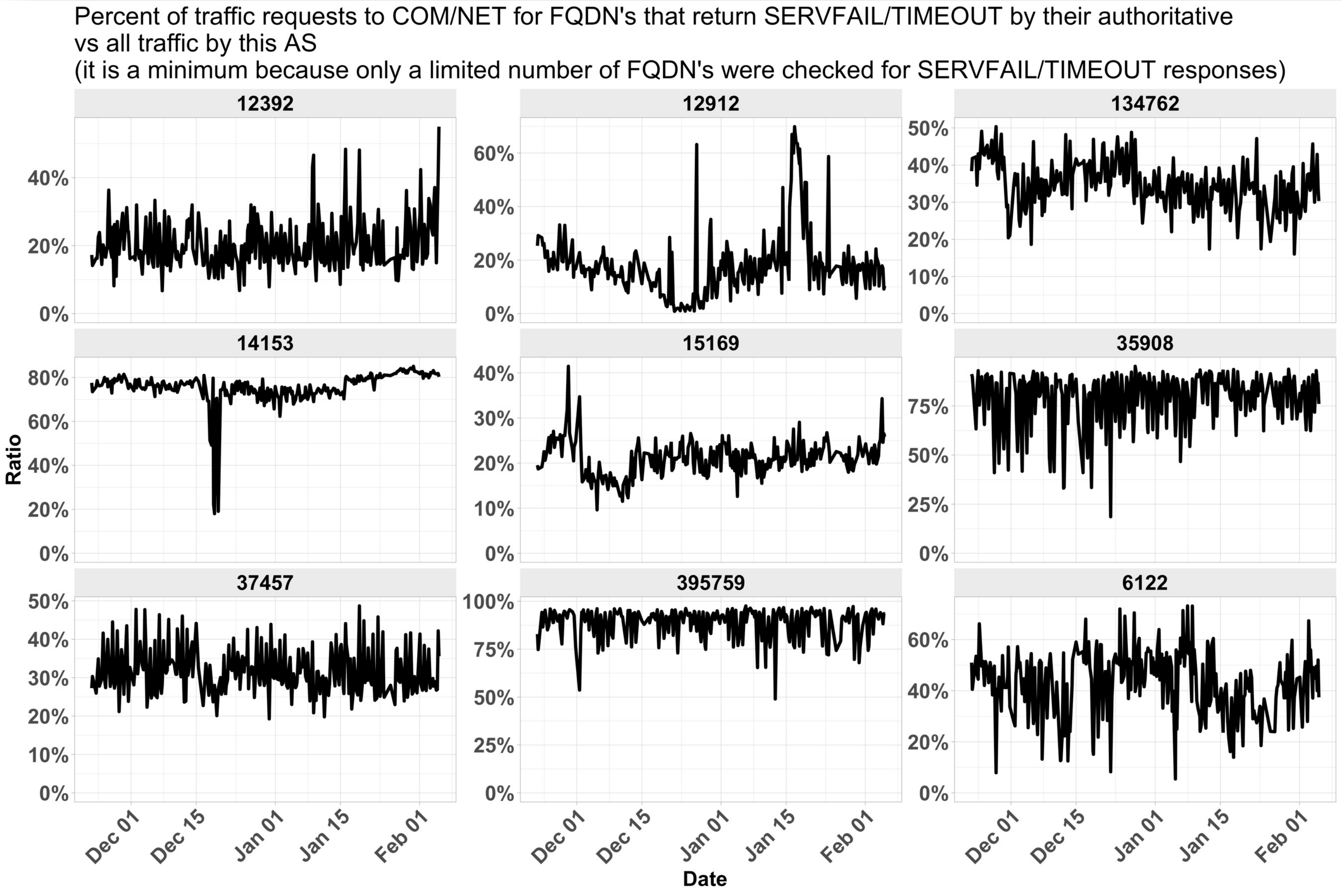
Longitudinal: SERVFAIL/TIMEOUT attributable traffic as % of traffic per AS for top talker AS's



powered by VERISIGN

Data since mid November 2023

Longitudinal: SERVFAIL/TIMEOUT attributable traffic as % of traffic (per AS) for AS's with the highest SERVFAIL ratio



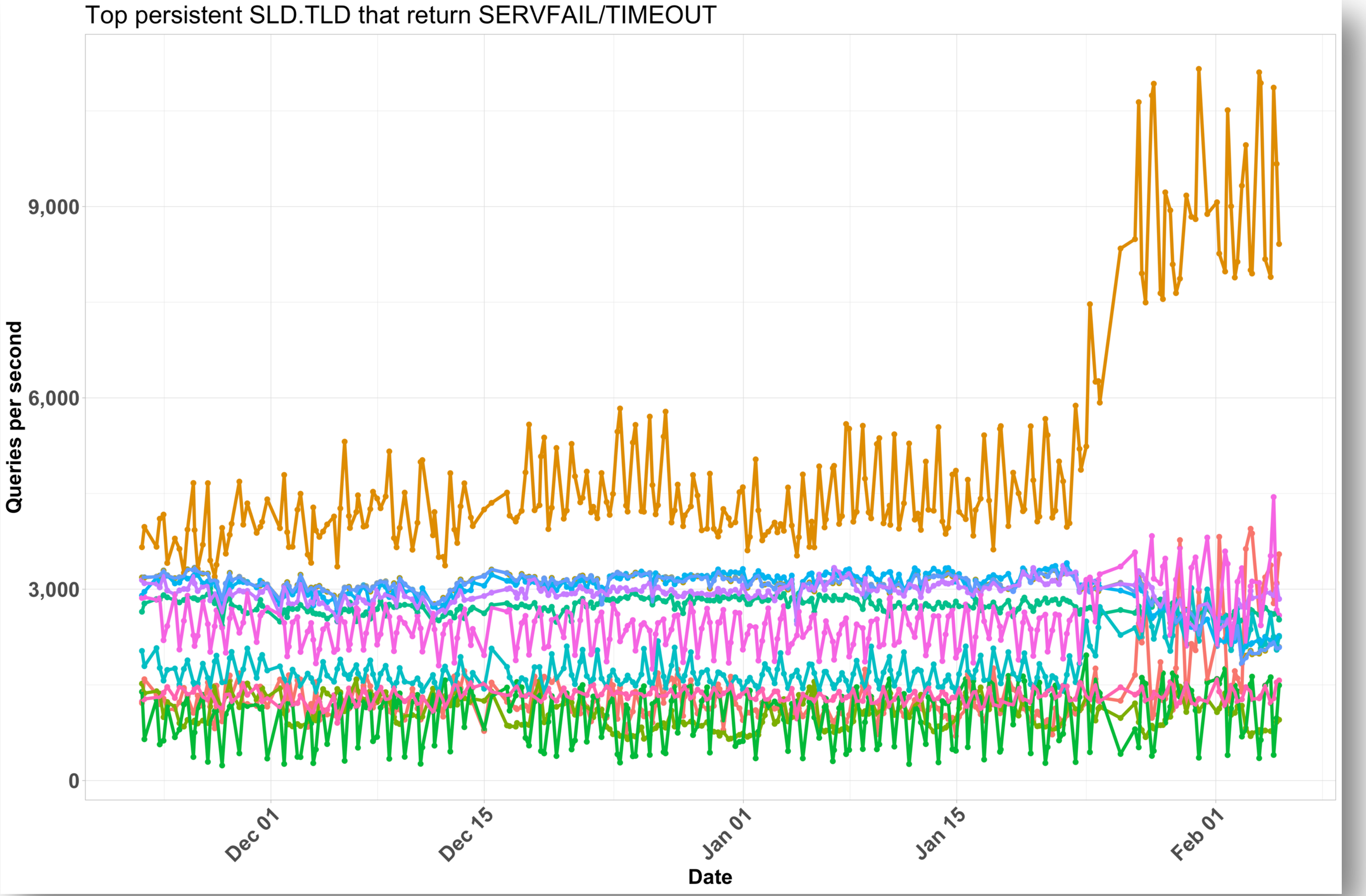
Verisign Public

powered by VERISIGN

Data since mid November 2023

Longitudinal: Persistent SLD.TLD

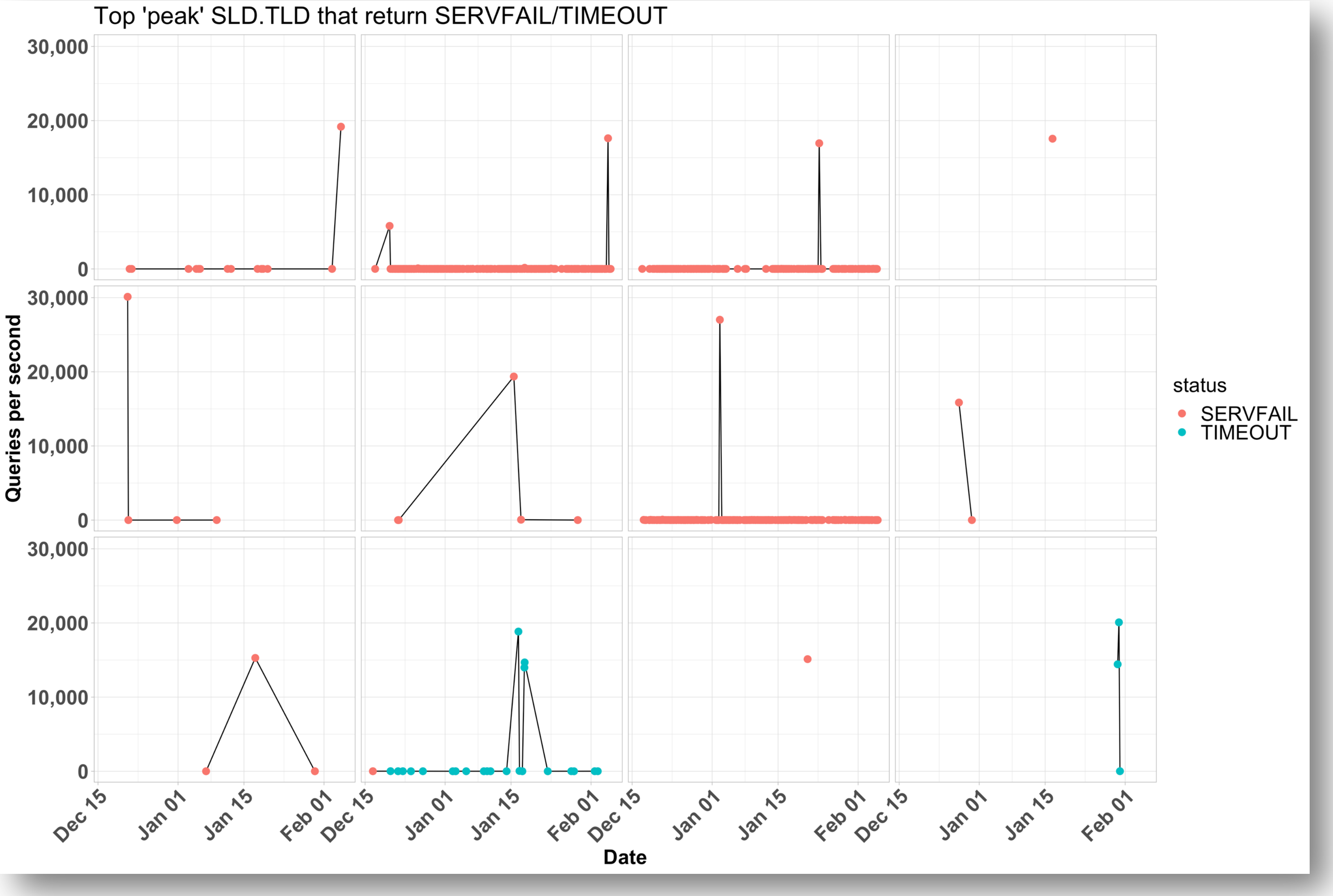
Each time series represents a single SLD.TLD



Data since mid November 2023

Longitudinal: Peaky SLD.TLD

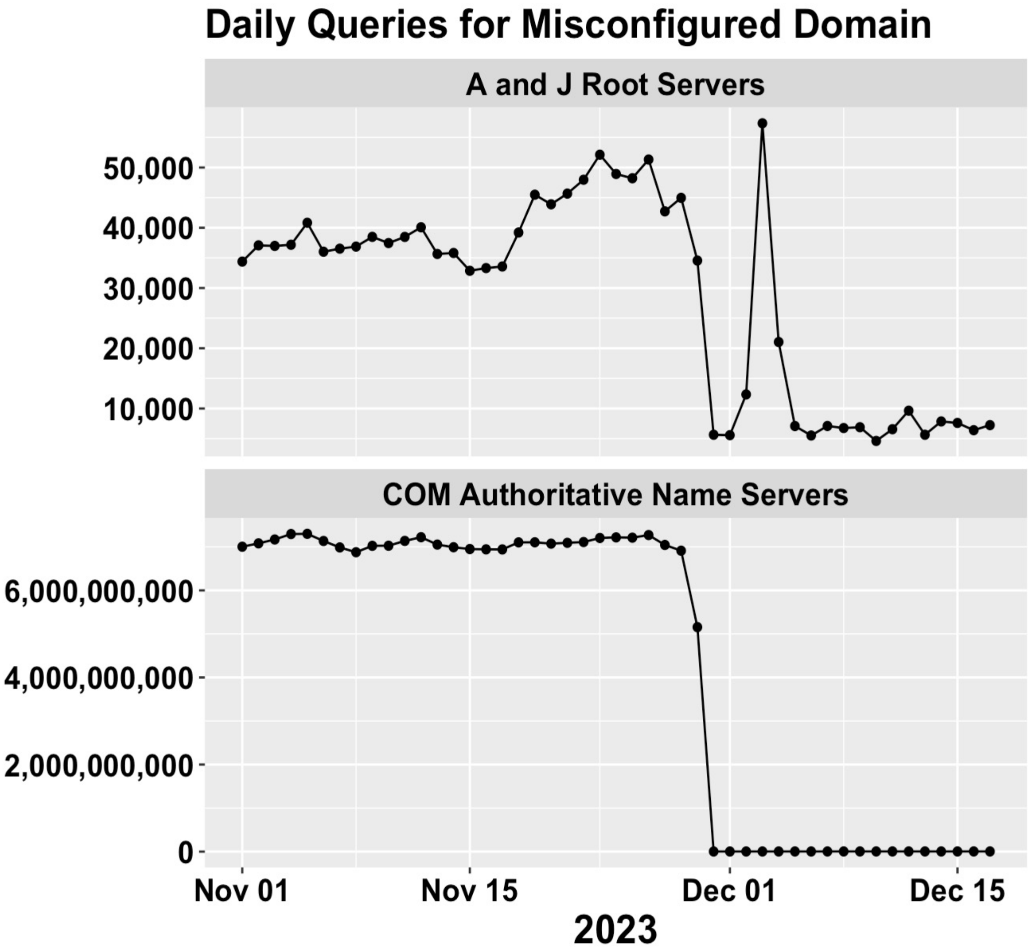
Each “box” is a time series that represents a single SLD.TLD



Reaching out to operators

A **single** domain name that had misconfigured name servers

- Peak
  - 7.2B/day COM
  - 57K/day A & J RSIs
- Post Fix
  - 2.6M/day COM
  - 4.6K/day A & J RSIs



Closing thoughts

- Re-querying is consistent, persistent and sizeable
  - In “normal” times it is inefficient but not impactful
  - During disruptive events (such as the Facebook outage) it could unpredictably impact the resolution ecosystem
- We encourage implementation of negative caching of resolution failures (i.e., the RFC9520 update to RFC2308)
- We are available to collaborate with operators to assess the relation of number of requests to the resolver for a SERVFAIL/TIMEOUT and the resulting rate of re-querying

powered by

VERISIGN™