Verisign's Transition to Elliptic Curve DNSSEC

Duane Wessels, Verisign

ICANN 79 DNSSEC & Security Workshop

March 6, 2024

Preparations

- Old algorithm: RSA/SHA-256
  - Algorithm number 8
  - Also known as “RSA”
- New algorithm: Elliptic Curve Digital Signature Algorithm Curve P-256 with SHA-256
  - Algorithm number 13
  - Also known as “ECDSA”
- Began planning early 2023
- Extensive QA and OTE testing
- Fully hands-off design, with changes scheduled at specific times
- Weekly coordination meetings involving multiple teams and 35+ people

Concern: Scheduling

- Rollovers require strict sequencing of events
- Nearly all DNSSEC rollover incidents are due to scheduling mistakes
  - Signatures without corresponding keys
  - DS records without corresponding signatures
- Solutions:
  - Conservative double-signing
  - Automated scheduling
  - Extensive testing

Concern: Resolution Failures

- Due to larger responses and resolvers unable to query over TCP
- Solutions:
  - Communicate to community
  - Coordinate with large resolver operators
  - Real-time monitoring
  - Outreach if necessary
  - Tweak truncation policy if necessary

Double Signing Algorithm Rollover Schedule

Day	Activity
1	ECDSA keys activated for use
2-5	ECDSA signatures added
6	ECDSA keys published
7-12	Root zone DS record changed
13	RSA keys un-published
14	RSA keys deactivated
15-18	RSA signatures removed

Response Sizes, Truncation, and TCP

Factors Affecting Truncation

- Client's maximum UDP size
- Server's maximum UDP size
- Number of signatures, NS, DS, and glue records
- Glue truncation policy
  - RFC 9471 "DNS Glue Requirements in Referral Responses"
  - Only affects delegations, not NXDomain responses

Response Types and Properties

Type	Response Size	Signature Count	Probability of Truncation Due to Double Signing	Approximate Composition
DO=0	varies	0	none	10%
Secure Referral	small	1	minimal	5%
Insecure Referral	medium	2	small	60%
DS denial-of-existence	medium, but fixed	3	minimal	15%
NXDomain	large	4	high	10%

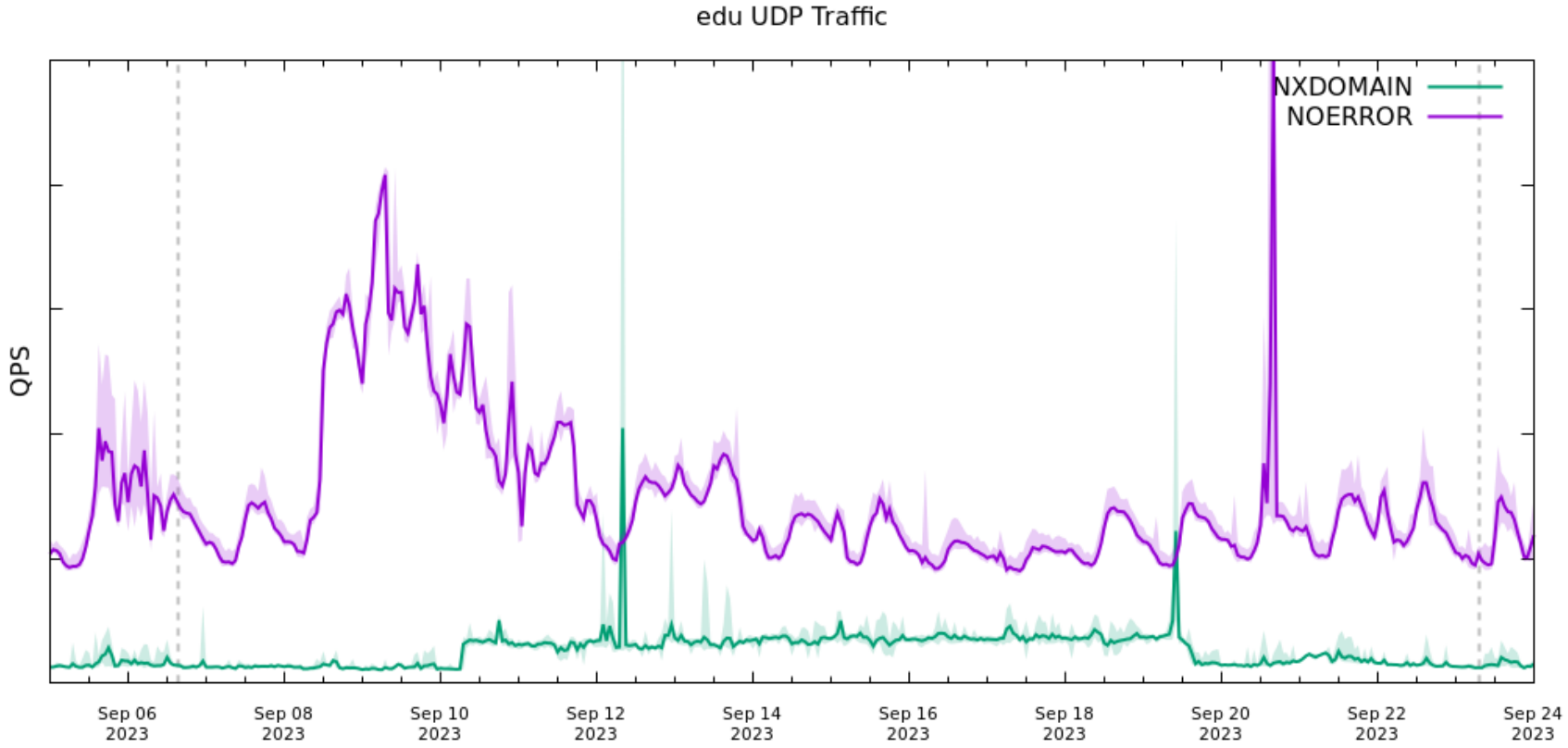
Each new ECDSA signature adds 100 bytes

Rollover Traffic Observations

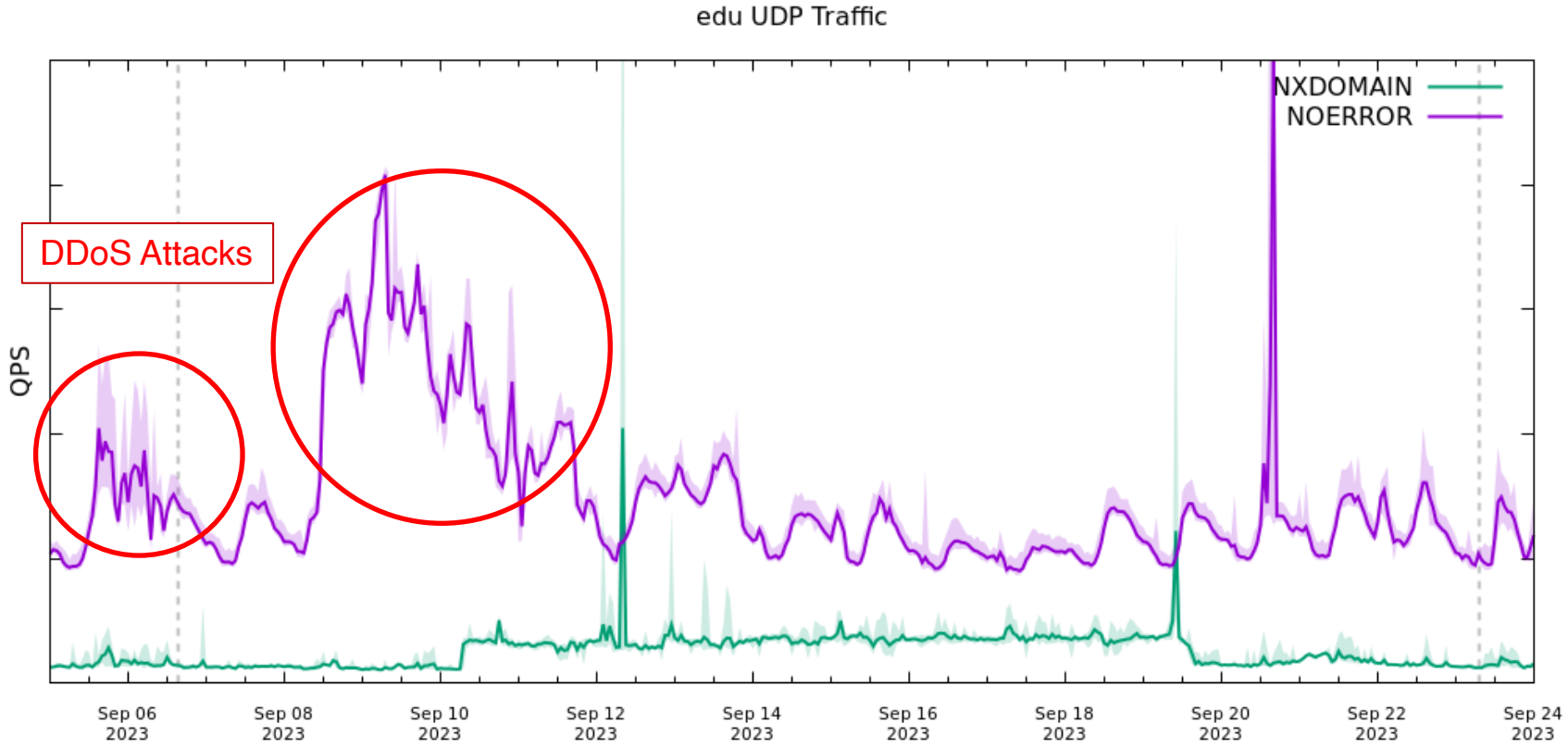
EDU Traffic Observations

- Traffic increases just before and after the start of the rollover were cause for concern
  - Turned out to be DDoS attacks
- More UDP/NXDOMAIN traffic than expected
  - Likely caused by resolvers unable to fall back to TCP

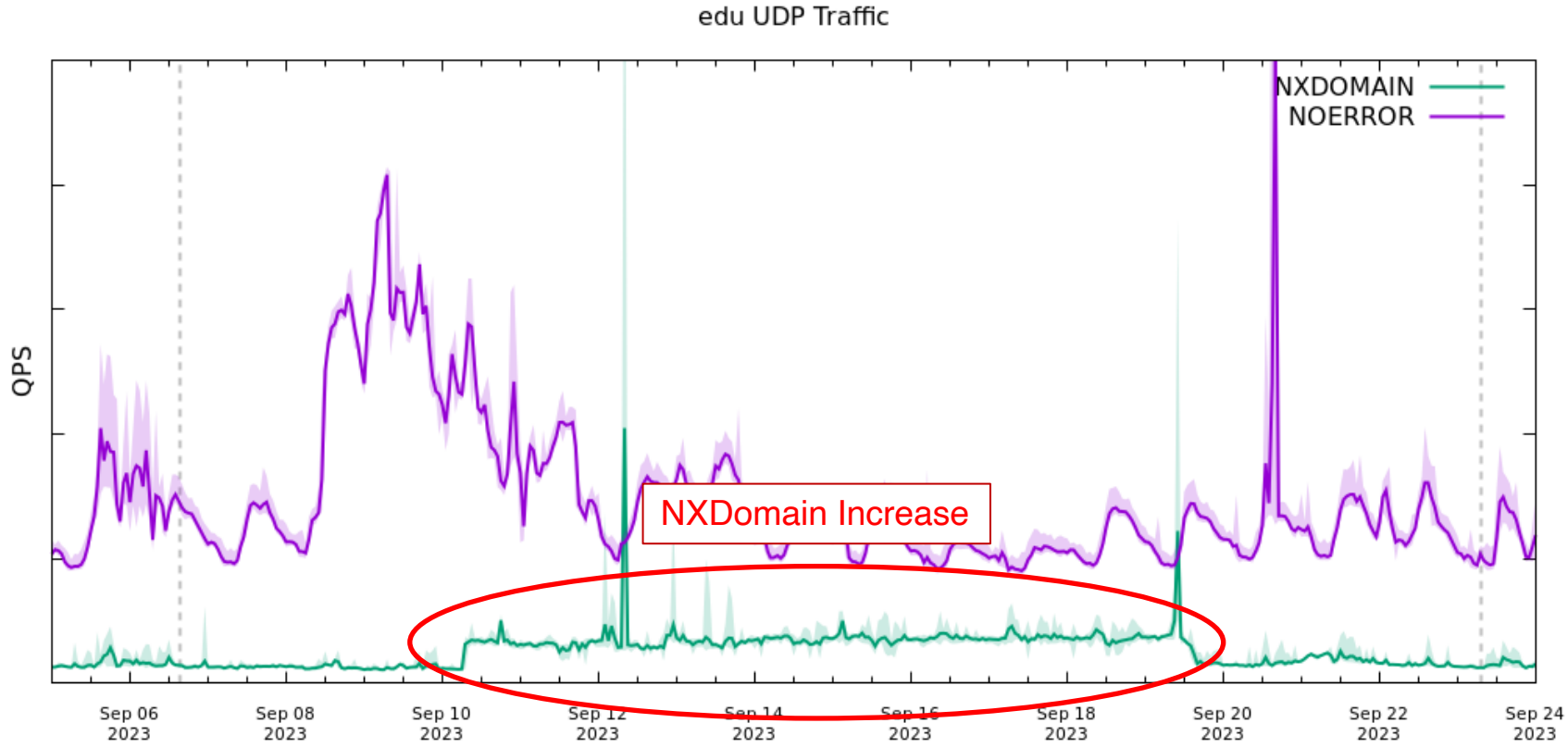
EDU UDP Traffic Levels



EDU UDP Traffic Levels

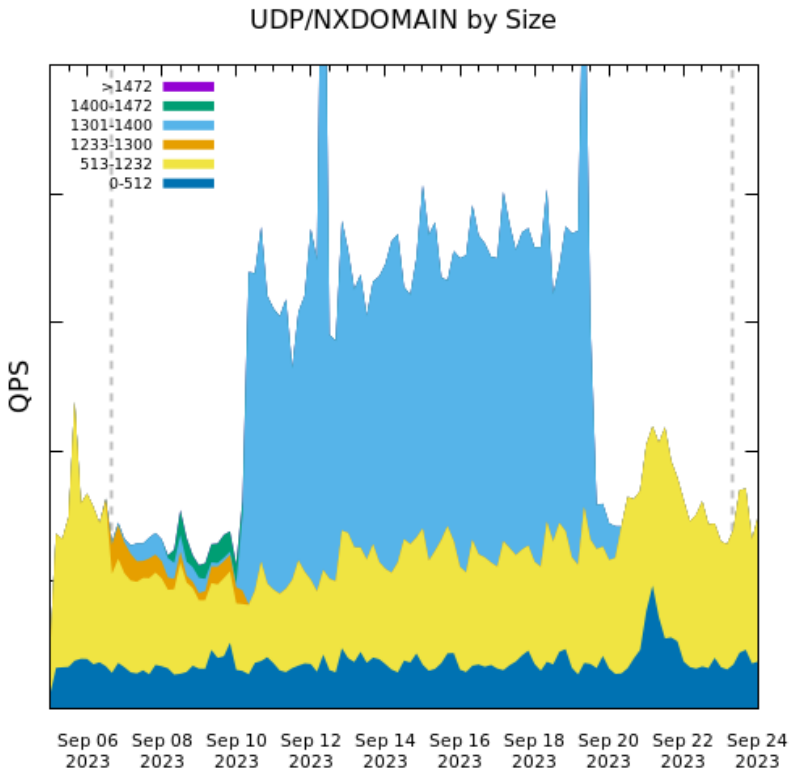


EDU UDP Traffic Levels

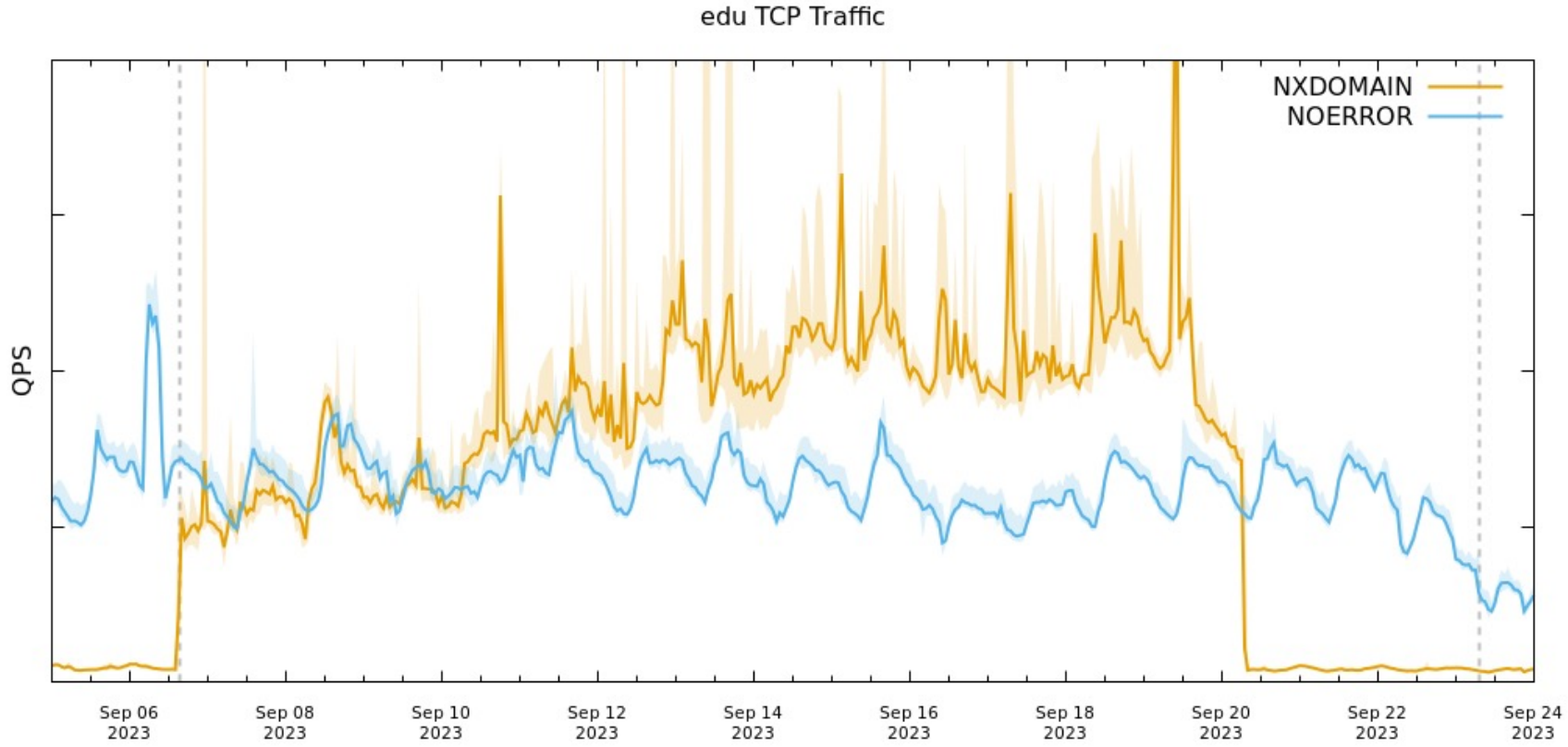


UDP/NXDOMAIN Traffic Increase

- From only a few resolvers
- Querying for a single domain name
- A non-existent variant of a real EDU domain name
- example.edu → example-s.edu



EDU TCP Traffic Levels



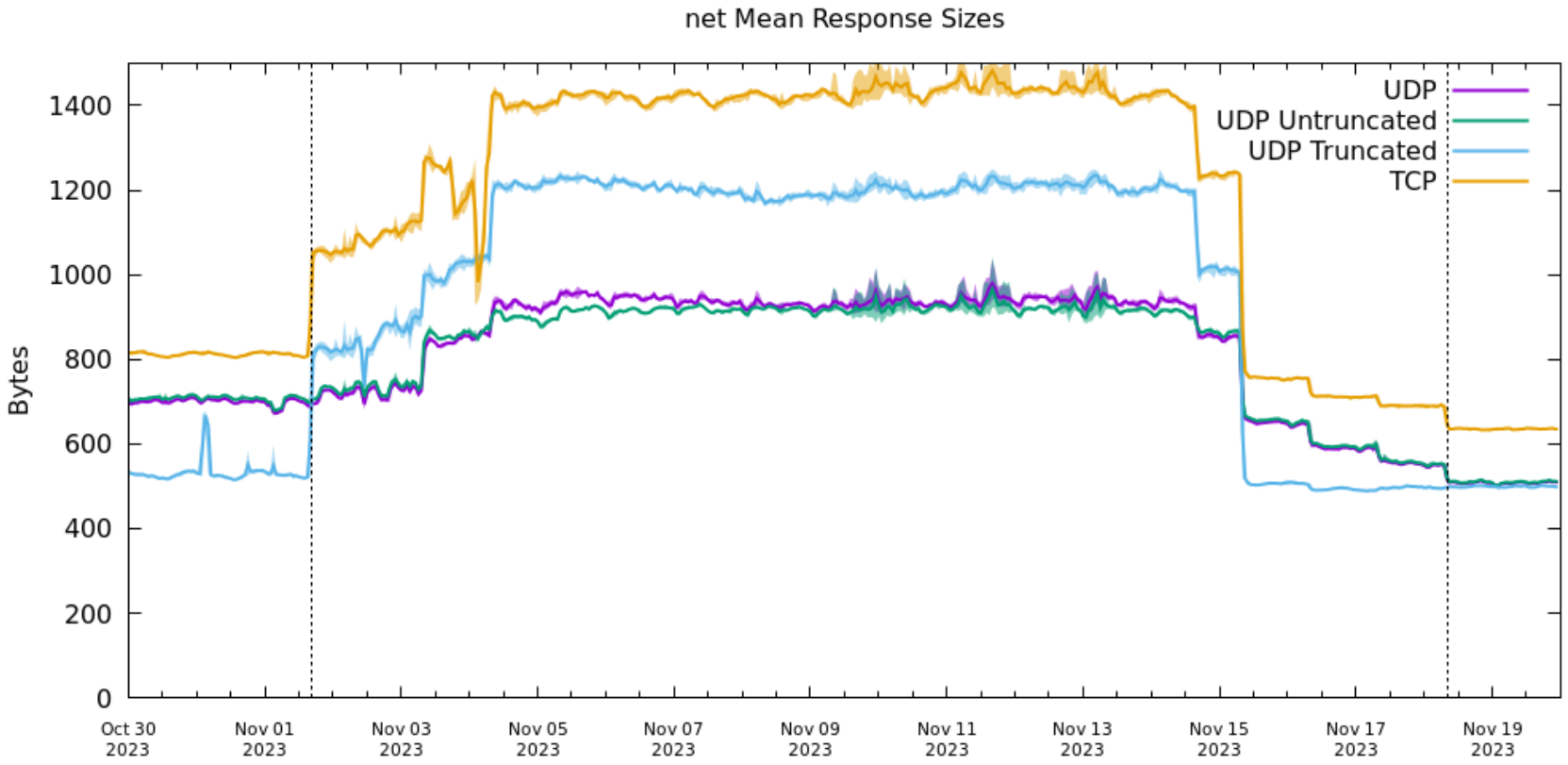
Before the NET Rollover

- Observed high rates of UDP retry traffic from some resolvers for domains operated by Akamai
- Akamai recently made changes to increase IPv6 glue
- We considered changes to our glue truncation policy
- Akamai updated their delegation data to reduce response sizes prior to rollover start
- See DNS-OARC 42 talk “Real world challenges with large responses, truncation, and TCP”

NET Traffic Observations

- Same patterns as EDU, although on a larger scale
- More resolvers exhibiting challenges with UDP truncation
- Paid close attention to root-servers.net

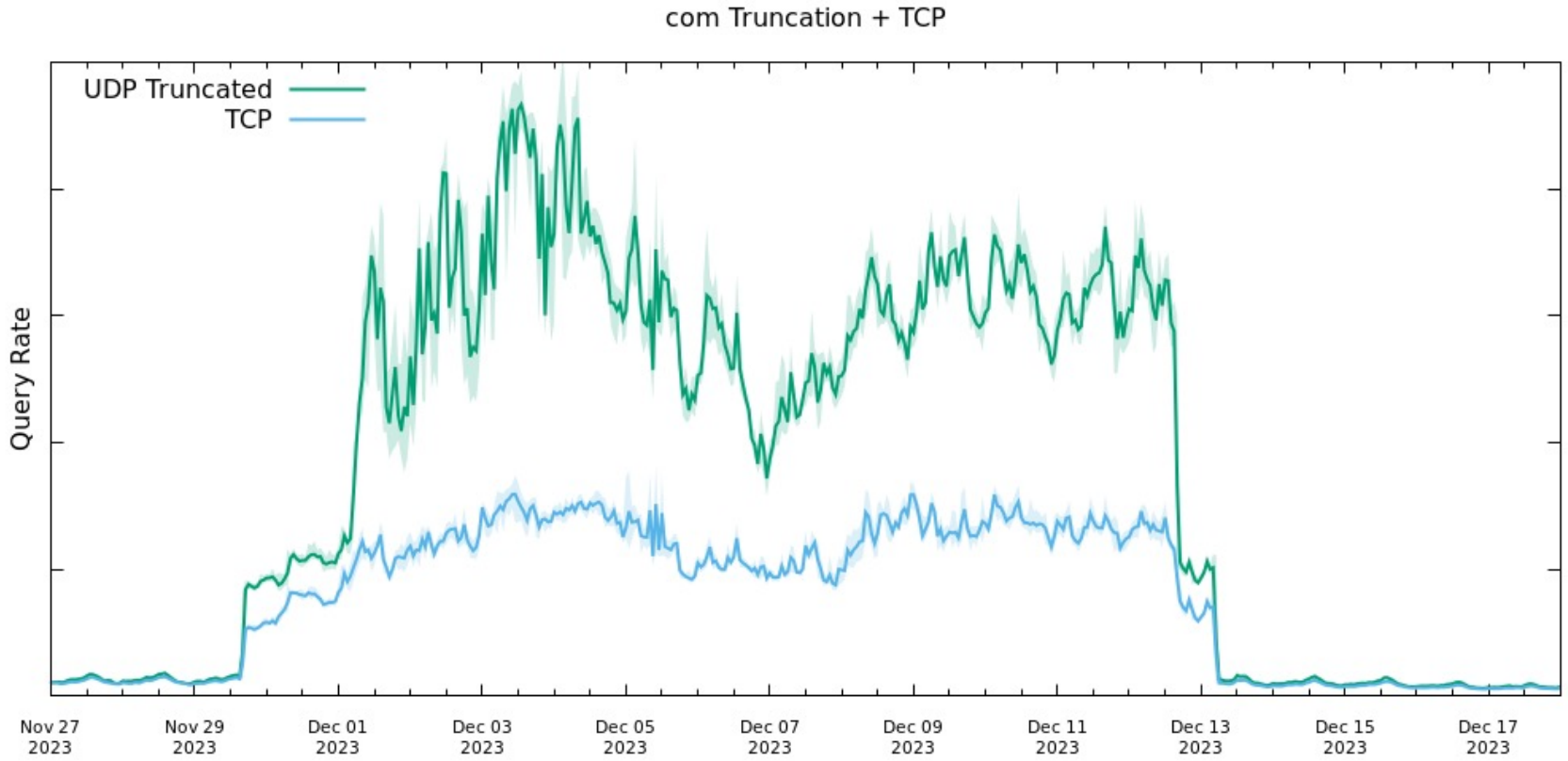
NET Response Sizes Over Time



COM Traffic Observations

- Very similar to EDU and NET
- Larger responses
- All signed UDP/NXDomain responses are truncated
- More UDP truncation than we'd like to see

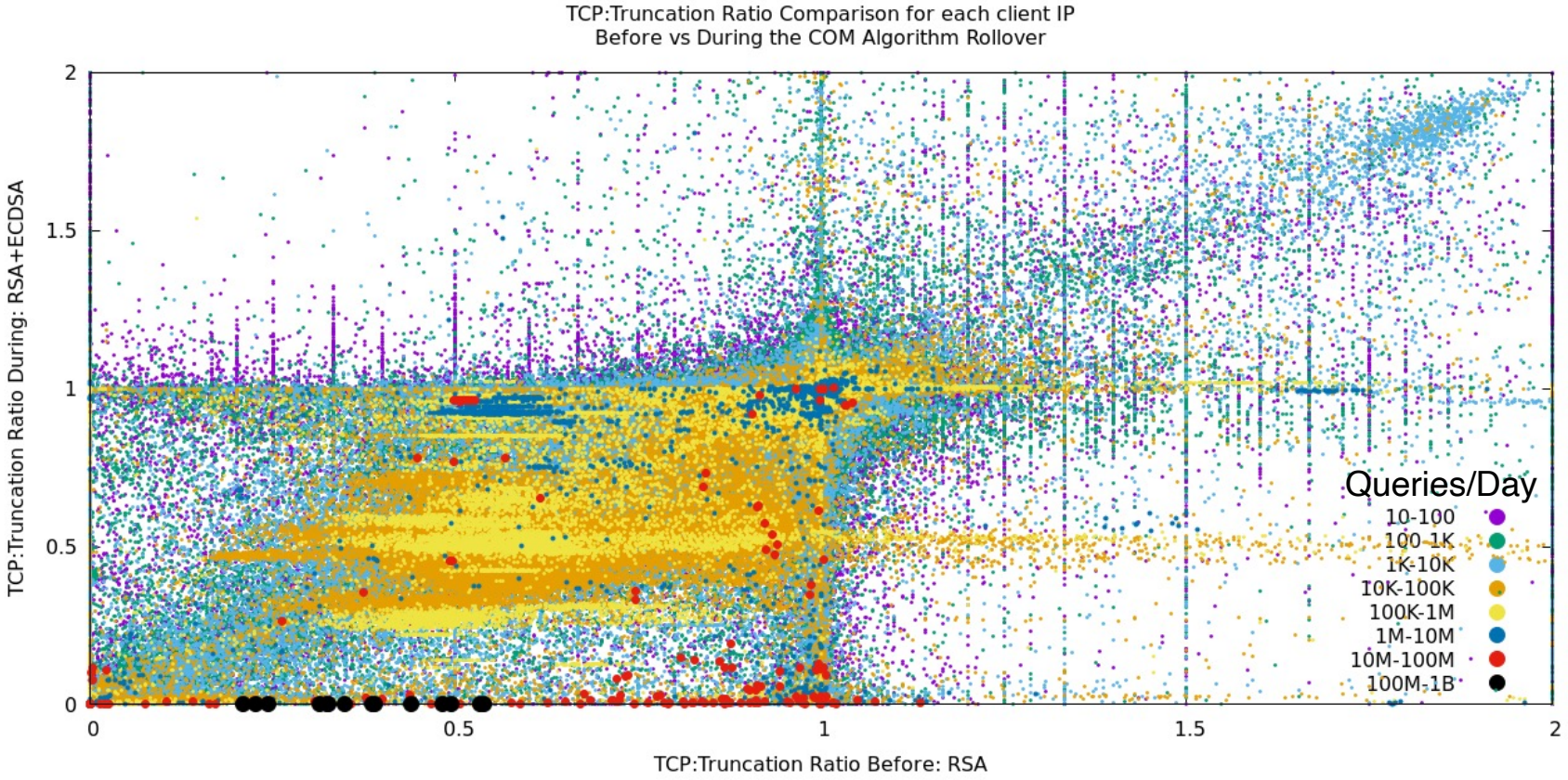
Truncation Levels Higher Than Expected



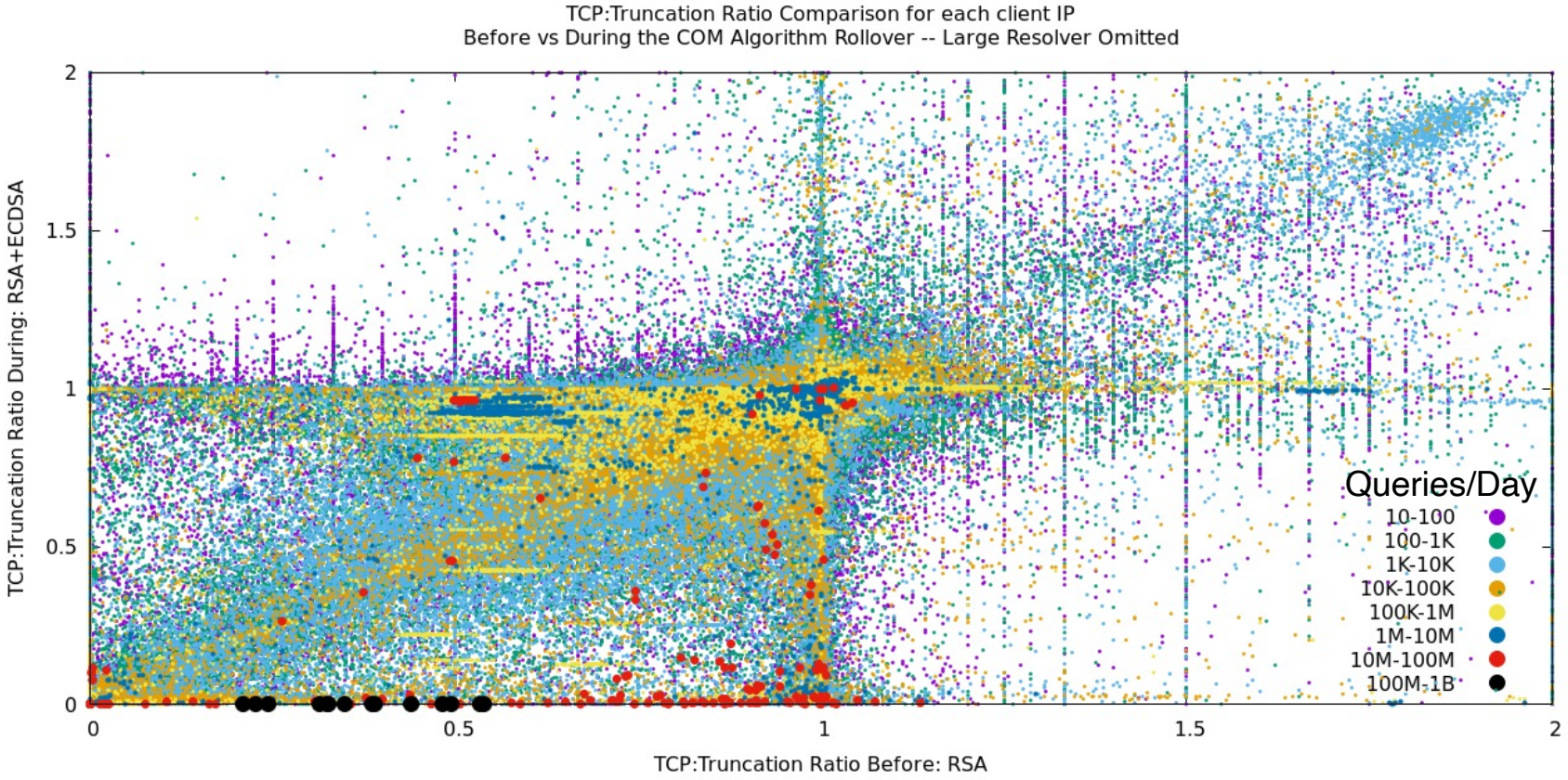
Why So Much Truncation?

- Responses larger during rollover, obviously, but...
- Resolvers unable to query over TCP retry over UDP?
- Possibly from non-resolver clients that don’t need untruncated responses?
- Can we quantify the resolvers that apparently struggle with truncation?

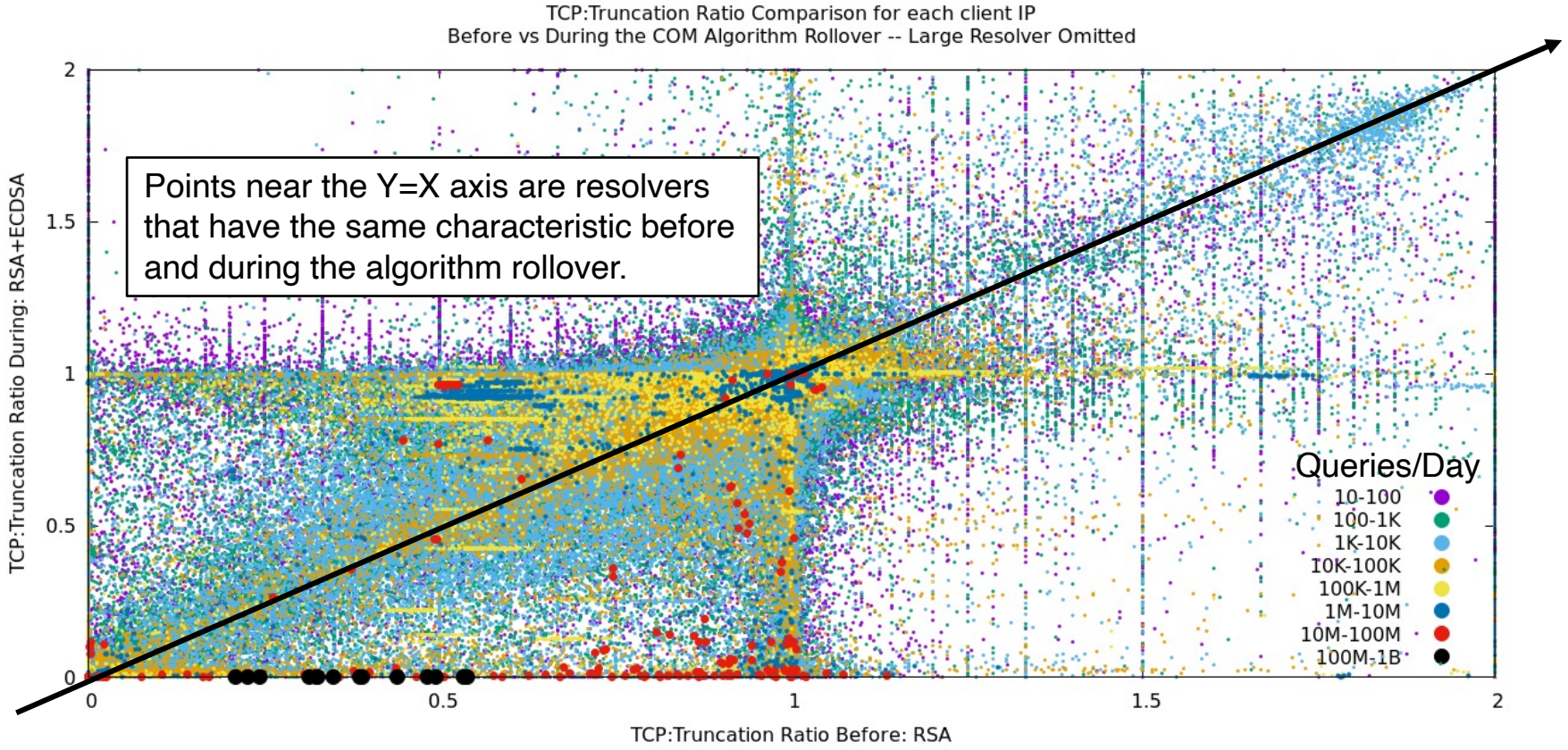
Ratio of TCP to Truncated Responses



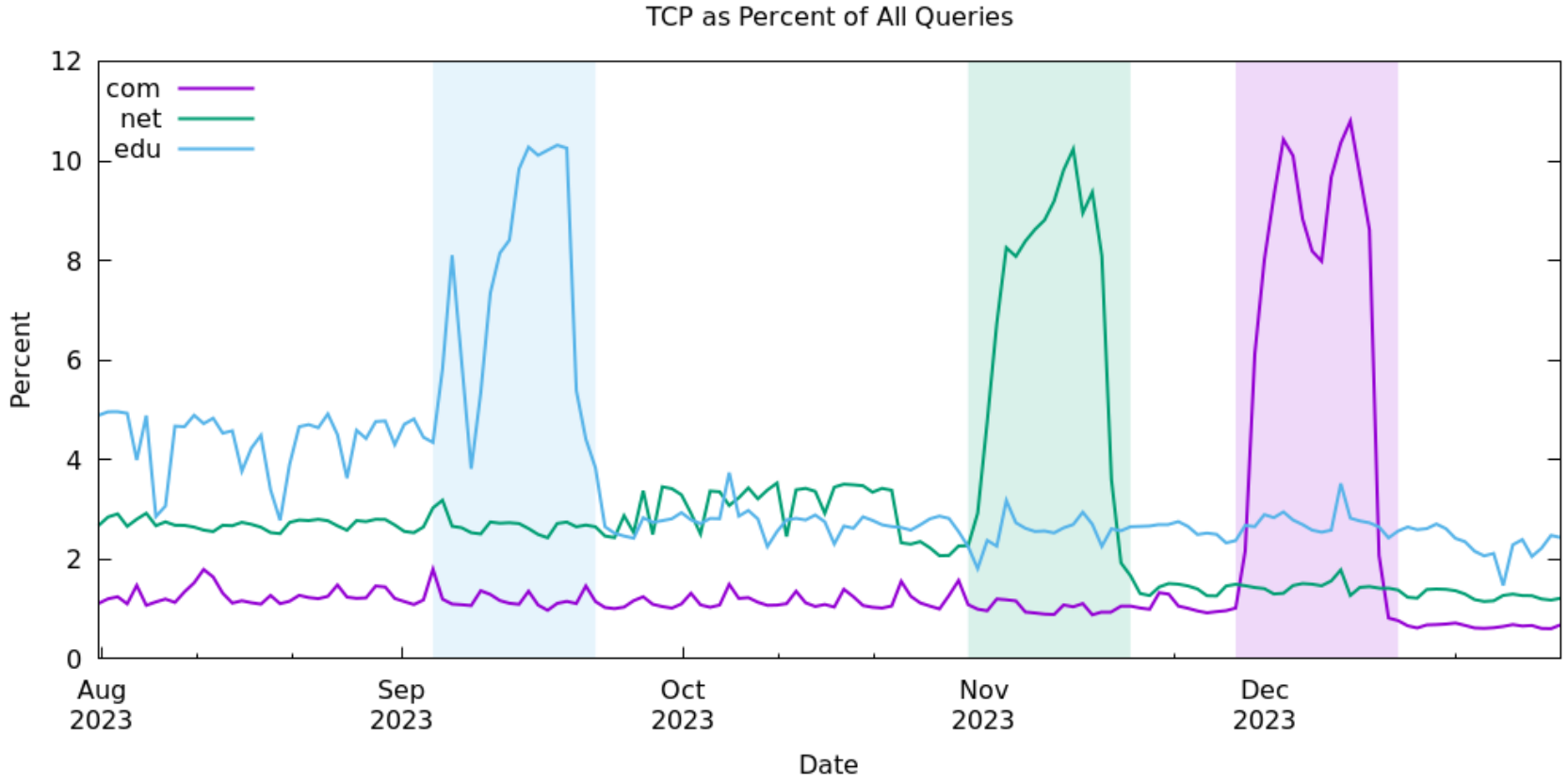
Ratio of TCP to Truncated Responses – No large resolver sources



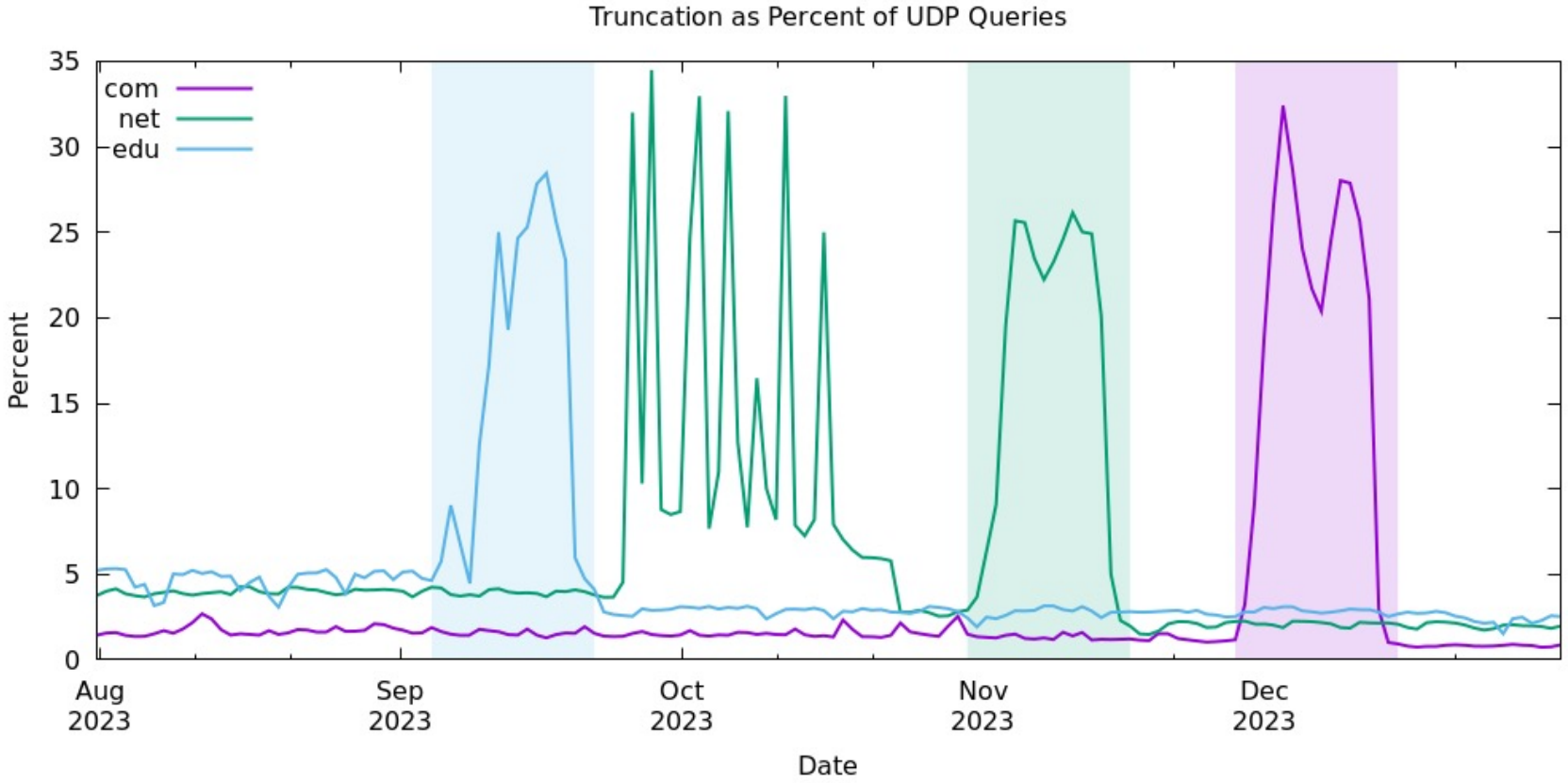
Ratio of TCP to Truncated Responses – No large resolver sources



Summary of Observed TCP Traffic Increases



Summary of Observed UDP Truncation Increases



Executive Summary

- Schedules executed perfectly
- Increase in TCP traffic – as expected
- Increase in UDP Truncation – more than expected
- Evidence that some *resolvers* experienced difficulty with non-existent domain names
- No reports or evidence that *end users* experienced resolution failures

VERISIGN®