RIPE NCC
RIPE NETWORK COORDINATION CENTRE

Debogonising 2a10::/12

Stephen Strowes <sds@ripe.net> | 2020-08-05 | MAT-WG/MAPRG joint interim

Background

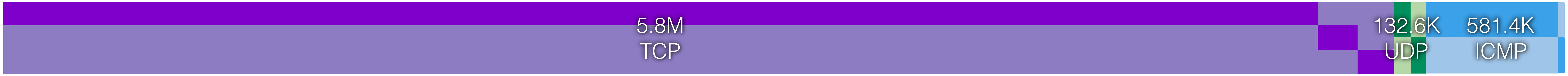
- January 2020
  - Announced 2a10::/12, and four /32s and four /48s drawn from it, for one week
- June 2020
  - Presented paper at TMA
  - https://tma.ifip.org/2020/wp-content/uploads/sites/9/2020/06/tma2020-camera-paper23.pdf
  - https://vimeo.com/425663114
- July 2020
  - Presented short follow-up at ANRW
  - https://dl.acm.org/doi/abs/10.1145/3404868.3406673
  - https://vimeo.com/441420020

Traffic Analysis

https://www.esa.int/Enabling_Support/Operations/Hubble_operations

Traffic Analysis

- We captured 85.2M packets with destinations in 2a10::/12
  - 78.7M of these were generated by RIPE Atlas
- The remaining 6.5M falls into a few main categories



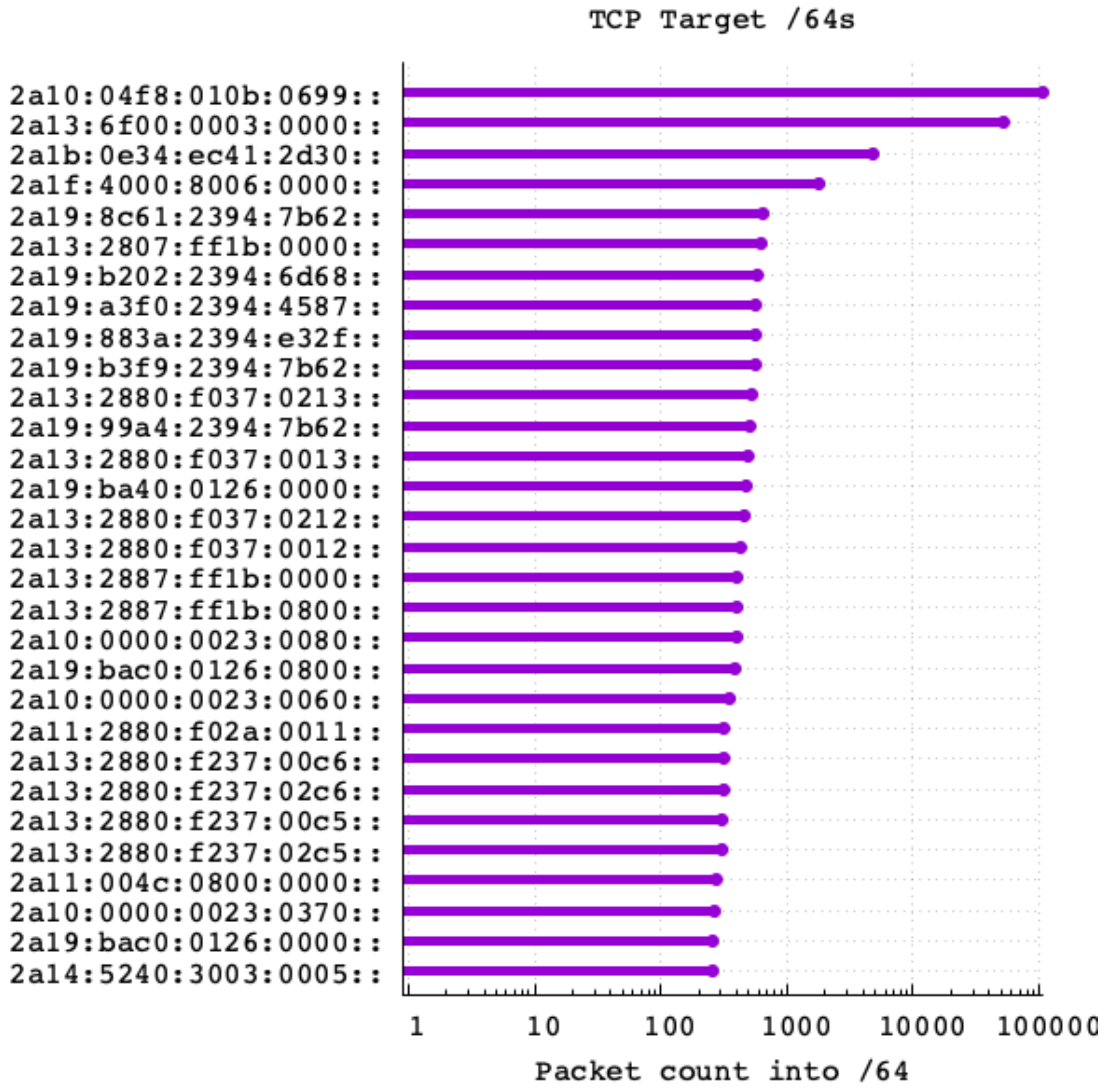
- TCP traceroute; some TCP port scanning
- Some DNS (misconfiguration)
- Echo requests (solicited)

TCP

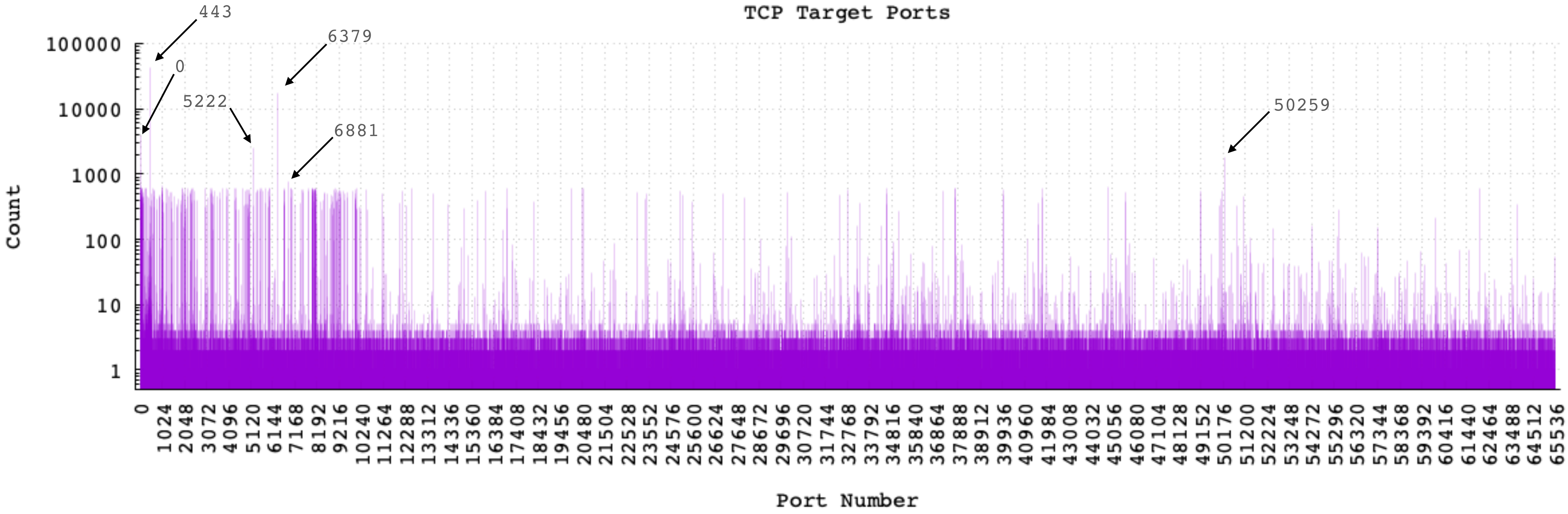
- 5.8M total packets carrying a TCP payload
  - 5.5M in a coordinated TCP traceroute campaign into the space
  - ~164k, port scanning from one origin
  - ~41k, dst port == 443 + ACK flag

TCP: Target addrs

- Traceroute campaign
    - 261k targets in 261k /64s
- Remaining targets broadly distributed
    - 133k targets in 112k /64s
- Sources
    - 118k sources in 110k /64s



TCP: Port numbers

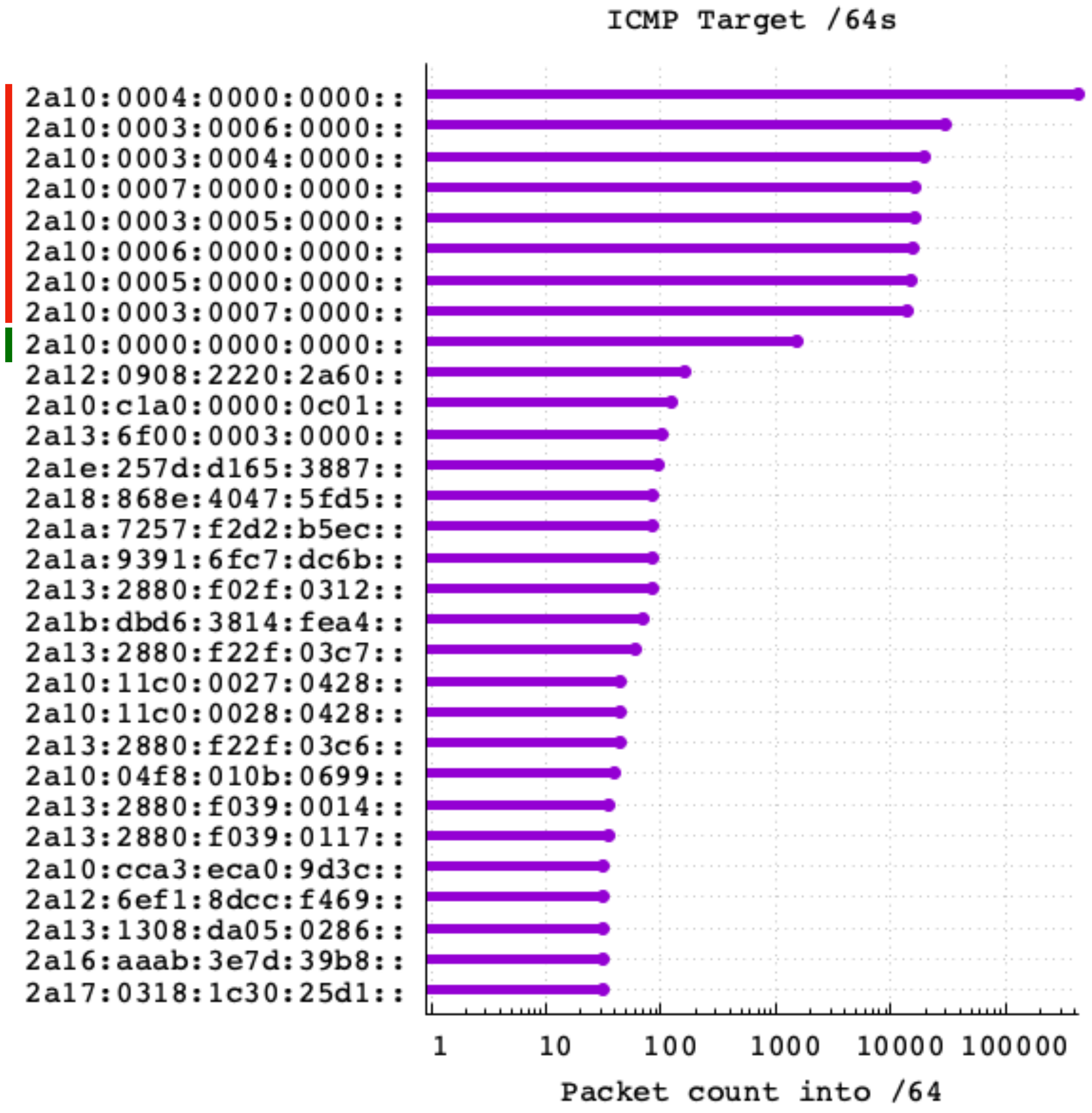


UDP

- ~133k UDP packets
  - 50% of which were DNS
  - misconfiguration: reported and fixed

ICMP: Largely Solicited

- 95% of ICMP went to our targets
- Some went to 2a10::
  - (unresponsive)
- Long-tail of remaining targets
  - 20.1k targets in 19.7k /64s



Routing & Reachability

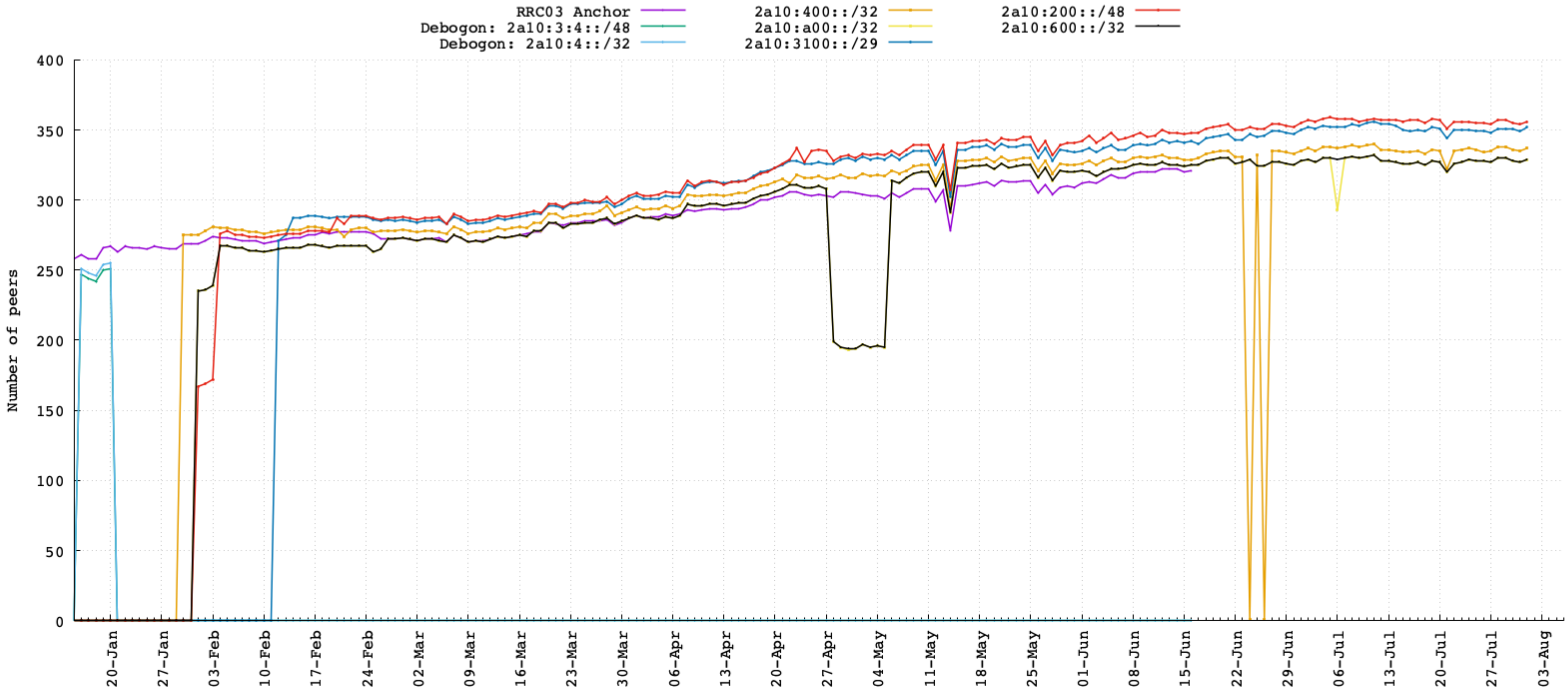
- TMA and ANRW papers cover aspects routing state
- Measurements from RIPE Atlas identified a couple of patterns
  - Reachability to all responsive targets was generally good, ~99%, excepting:
  - No probe in AS8881 could reach any of our targets; some probes in other networks
  - No probe in (or routed via) AS3320 could reach a specific subset of targets
    - specifically prefixes intended to be less reachable

Current Status

Data release

- RIPE Atlas and RIS routing data is public
  - pointers to specifics are in the TMA paper
- Now that some time has passed:
  - we may be able to look again at releasing the captured traffic, or a form of it

2a10::/12 is now in use



2a10::/29 is now out of quarantine

- The space the /32s and /48s were drawn from was quarantined
- This space has now been reissued
  - So it is likely to show up in the wild soon
  - Potential future comparison between this space from a route collector vs. announcements from elsewhere

End Notes

- First “darknet” study on IPv6 traffic since 2013
- No traffic into this space seems problematic
- Routing and reachability appeared good
  - See TMA paper
- Observational “quirks” of observing space announced by the route collector system
  - See ANRW paper
- Address space is live and in use

Questions ?

sds@ripe.net
@sdstrowes