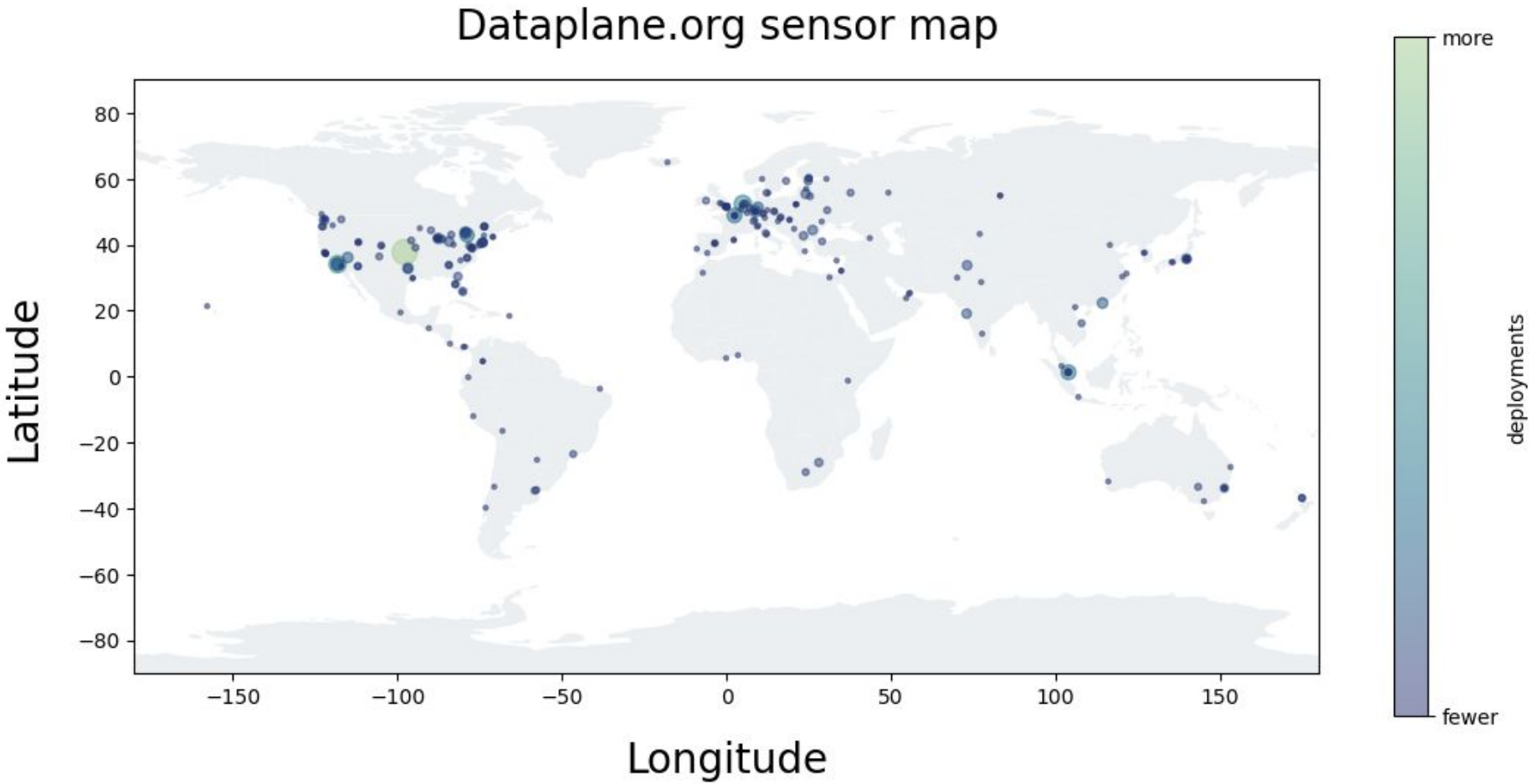
What a Distributed Network Sees:

Internet Observations from All Over

John Kristoff

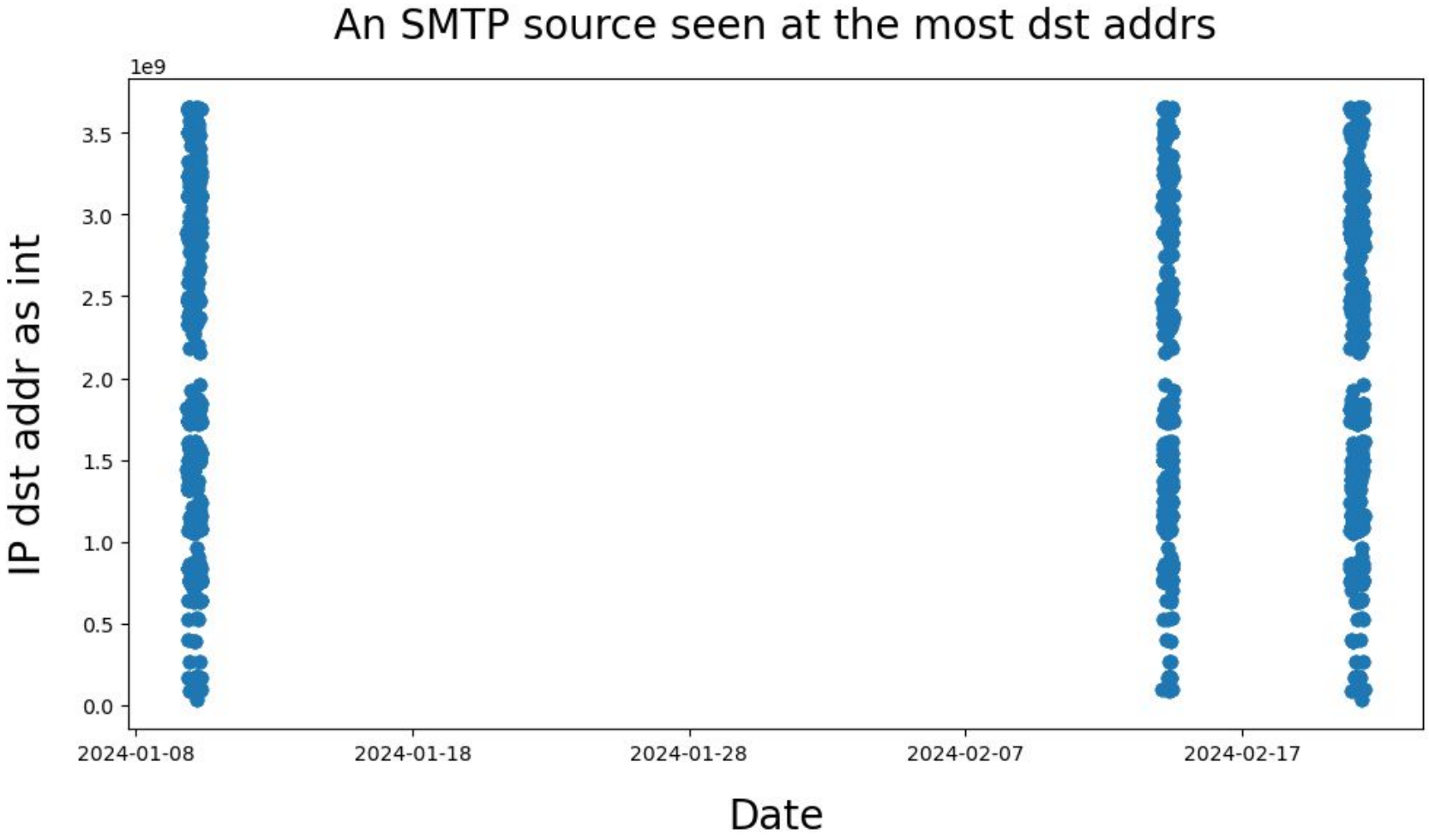
Overview

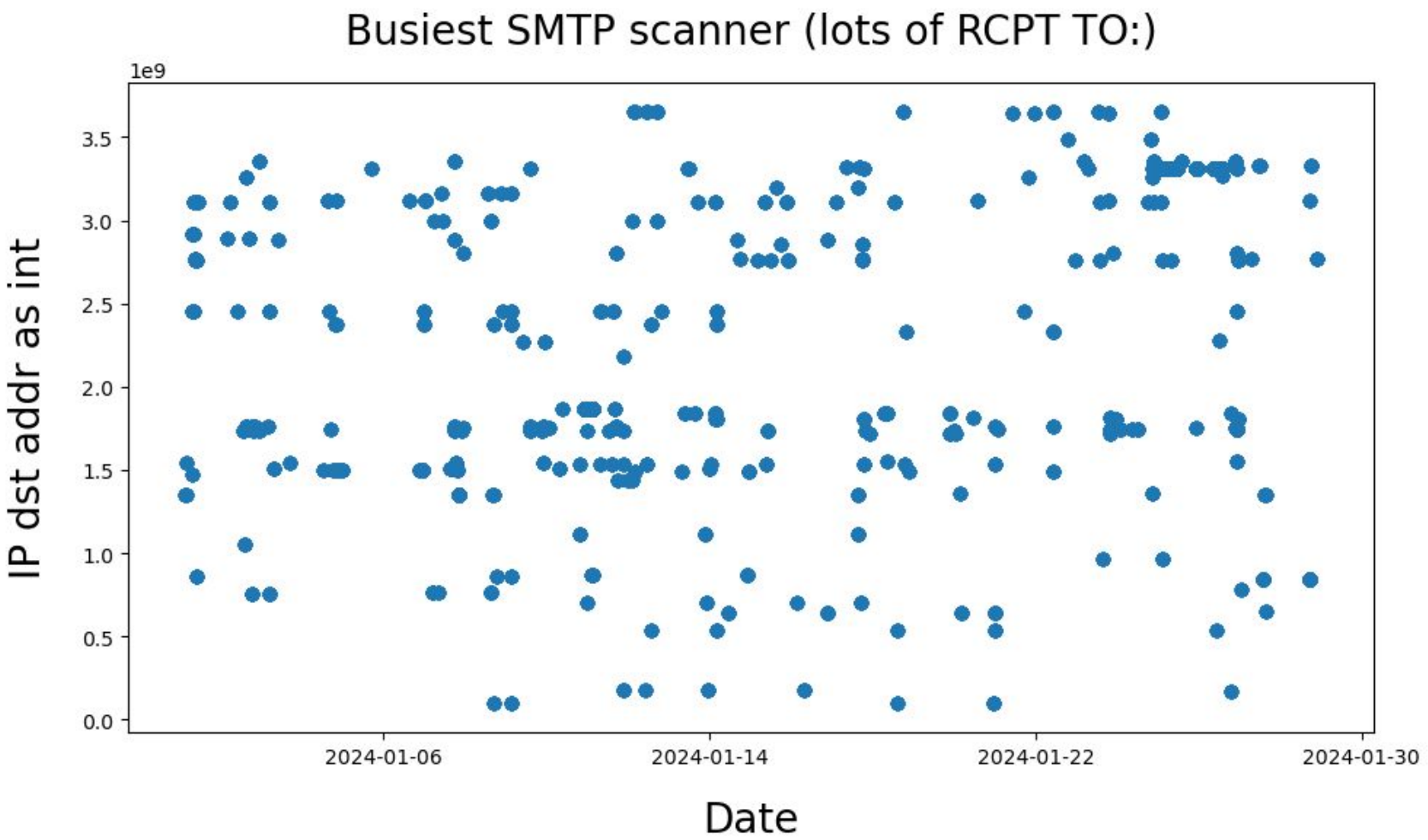
- 500+ leased nodes in ~100 nets
- Unadvertised service (no A/AAAA/MX RRs)
- App sensors
  - Complete handshakes, serve no content
- Net probes
  - Low-frequency measurement packets

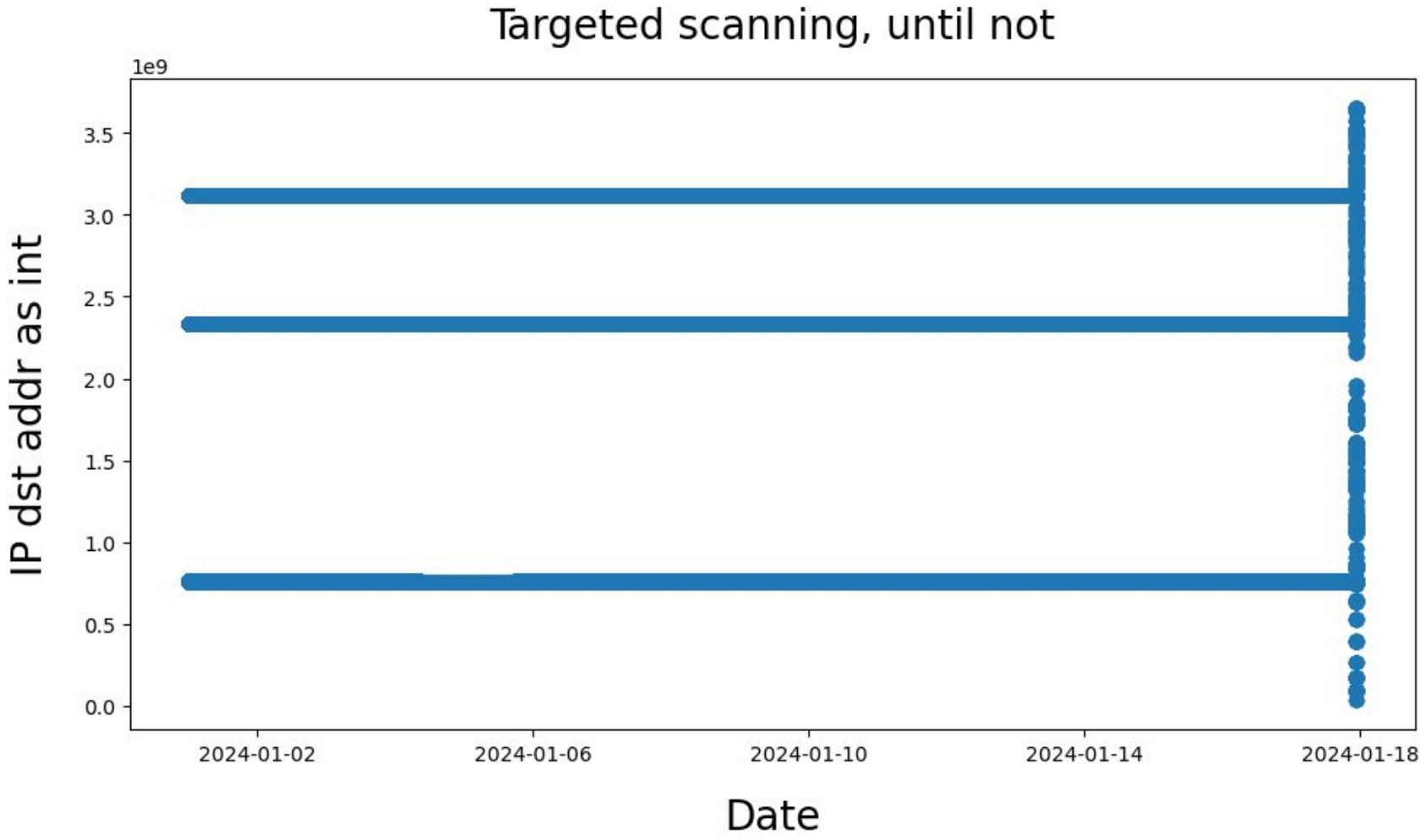

Dataplane.org sensor map
Latitude
Longitude
80
60
40
20
0
−20
−40
−60
−80
−150
−100
−50
0
50
100
150
more
fewer
deployments

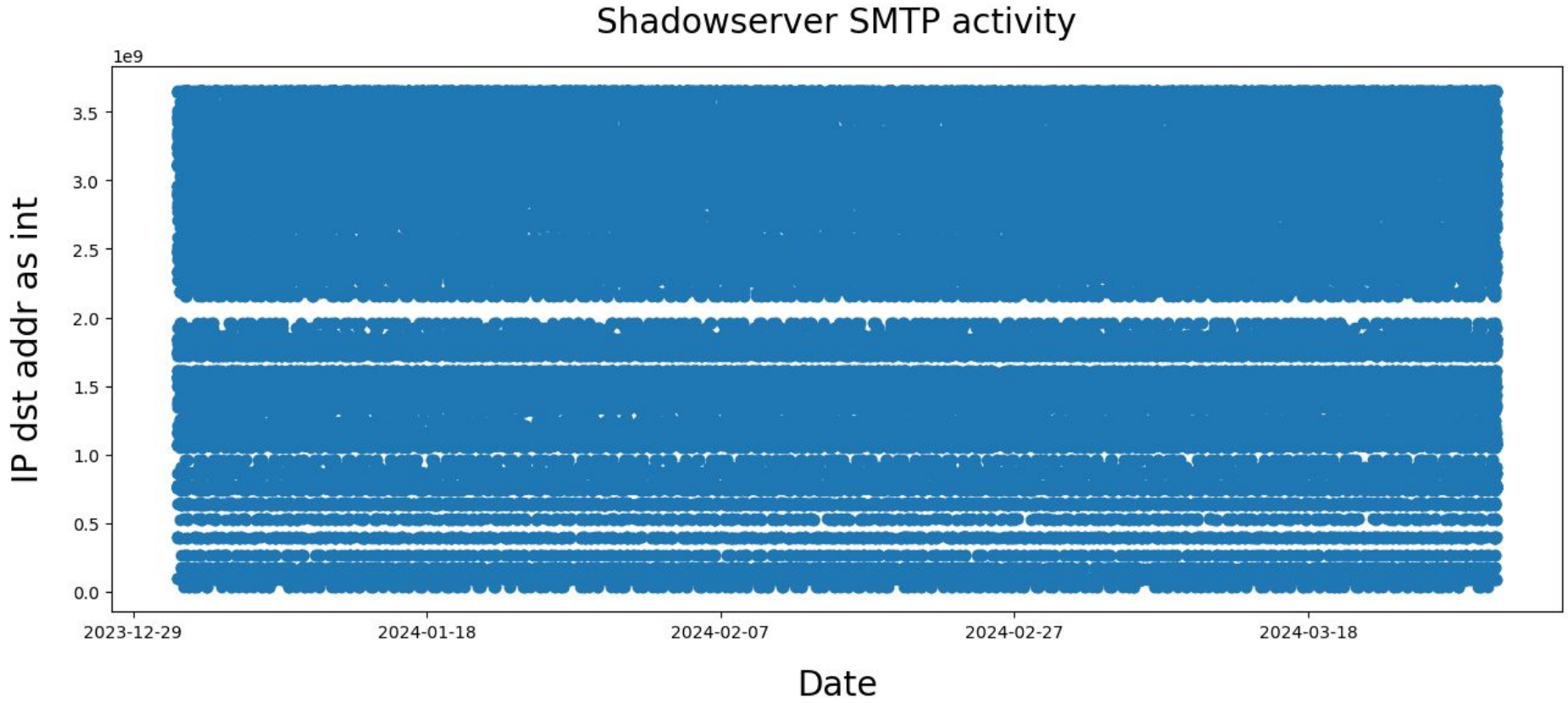
SMTP Activity

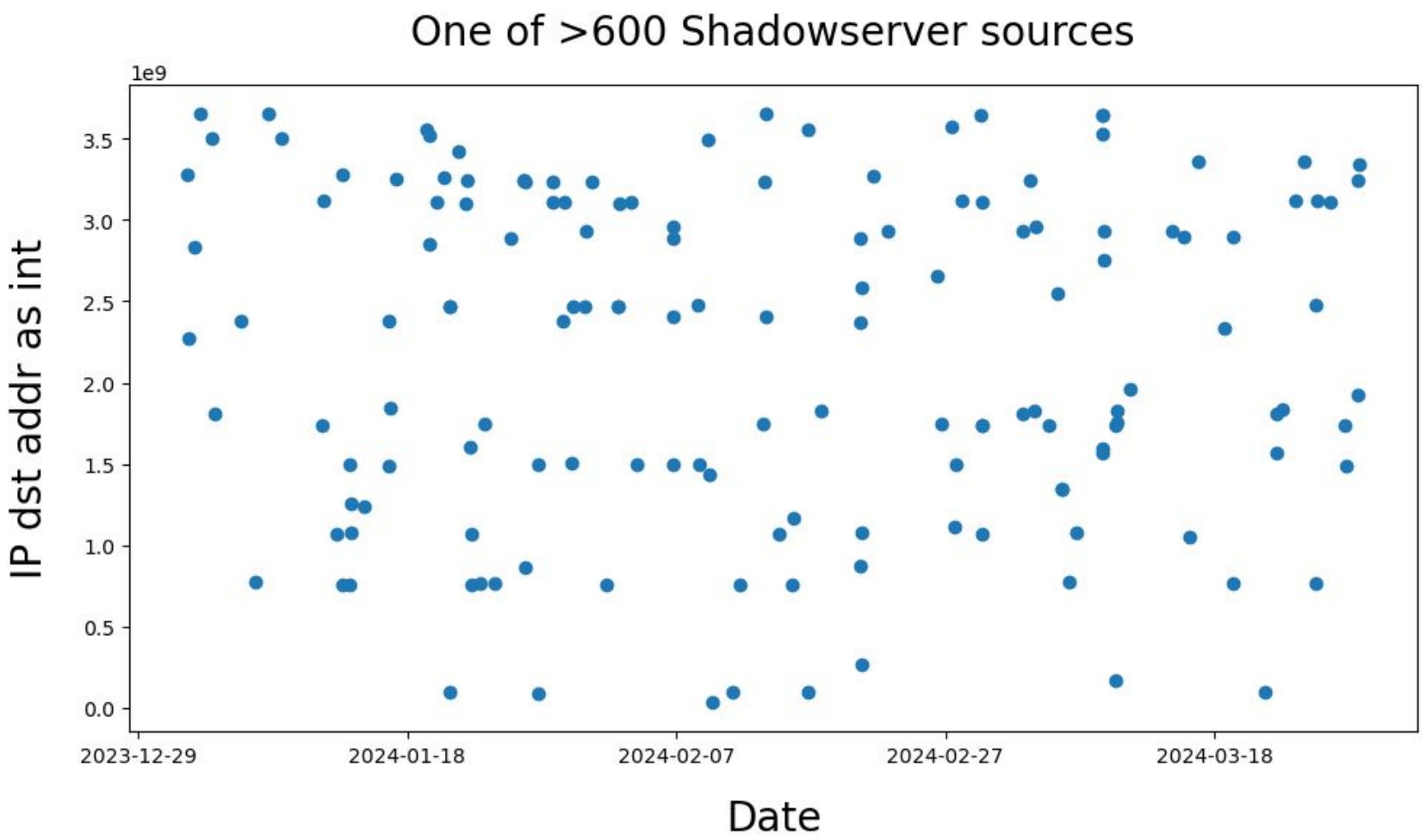
- 2024-Q1
  - 27+ million events
  - connect, helo, ehlo, rcpt to, ...
  - !body

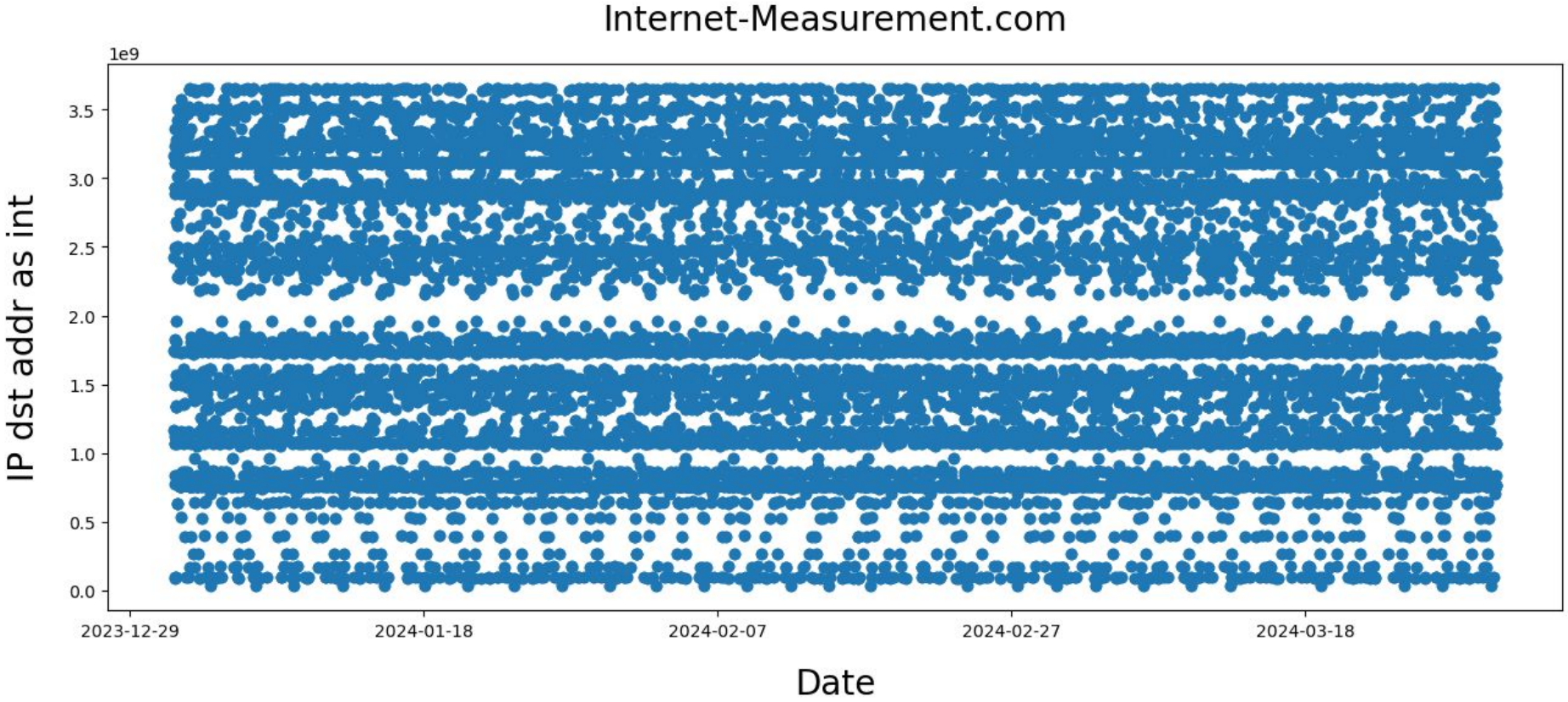

An SMTP source seen at the most dst addrs
1e9
3.5
3.0
2.5
2.0
1.5
1.0
0.5
0.0
IP dst addr as int
2024-01-08
2024-01-18
2024-01-28
2024-02-07
2024-02-17
Date

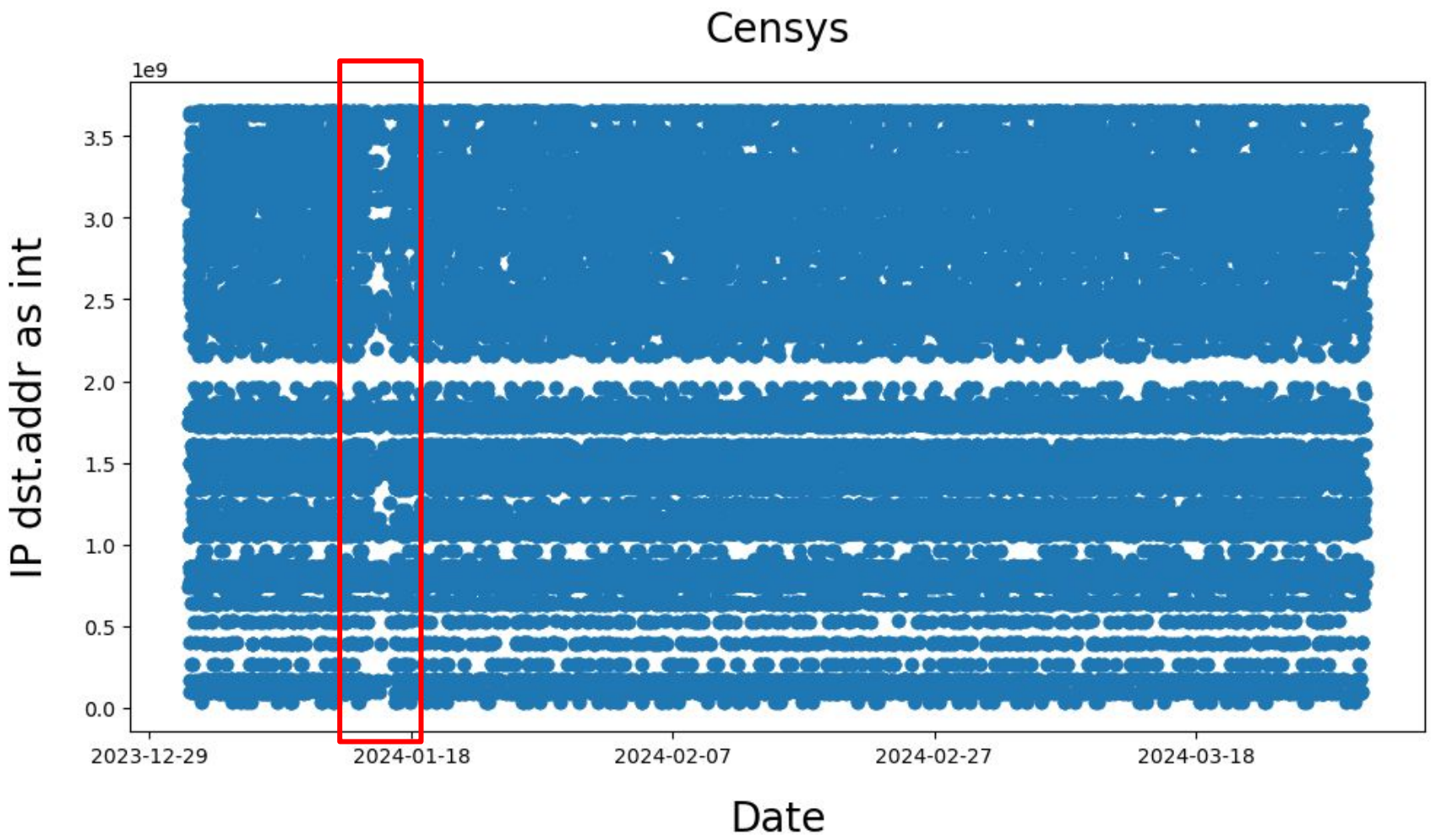

Busiest SMTP scanner (lots of RCPT TO:)
1e9
3.5
3.0
2.5
2.0
1.5
1.0
0.5
0.0
IP dst addr as int
2024-01-06
2024-01-14
2024-01-22
2024-01-30
Date

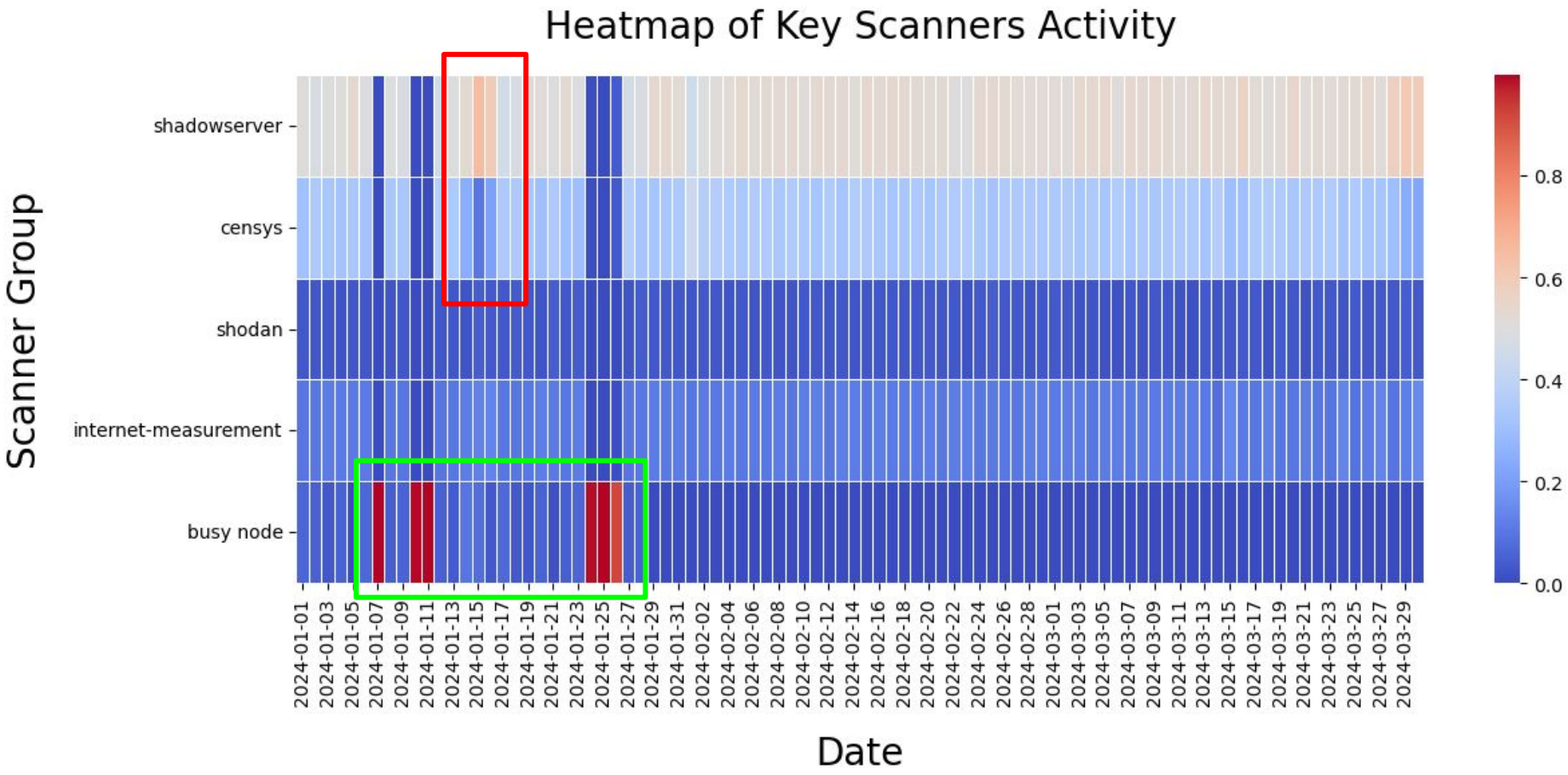

Targeted scanning, until not
1e9
3.5
3.0
2.5
2.0
1.5
1.0
0.5
0.0
IP dst addr as int
2024-01-02
2024-01-06
2024-01-10
2024-01-14
2024-01-18
Date


Shadowserver SMTP activity
1e9
3.5
3.0
2.5
2.0
1.5
1.0
0.5
0.0
IP dst addr as int
2023-12-29
2024-01-18
2024-02-07
2024-02-27
2024-03-18
Date

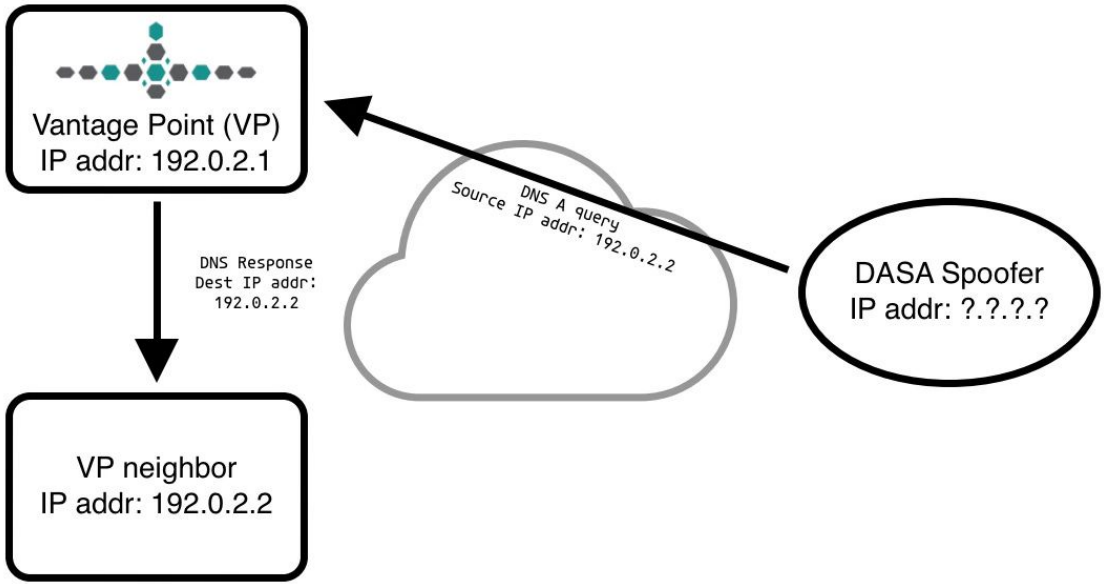

One of >600 Shadowserver sources
1e9
3.5
3.0
2.5
2.0
1.5
1.0
0.5
0.0
IP dst addr as int
2023-12-29
2024-01-18
2024-02-07
2024-02-27
2024-03-18
Date


Internet-Measurement.com
1e9
3.5
3.0
2.5
2.0
1.5
1.0
0.5
0.0
IP dst addr as int
2023-12-29
2024-01-18
2024-02-07
2024-02-27
2024-03-18
Date

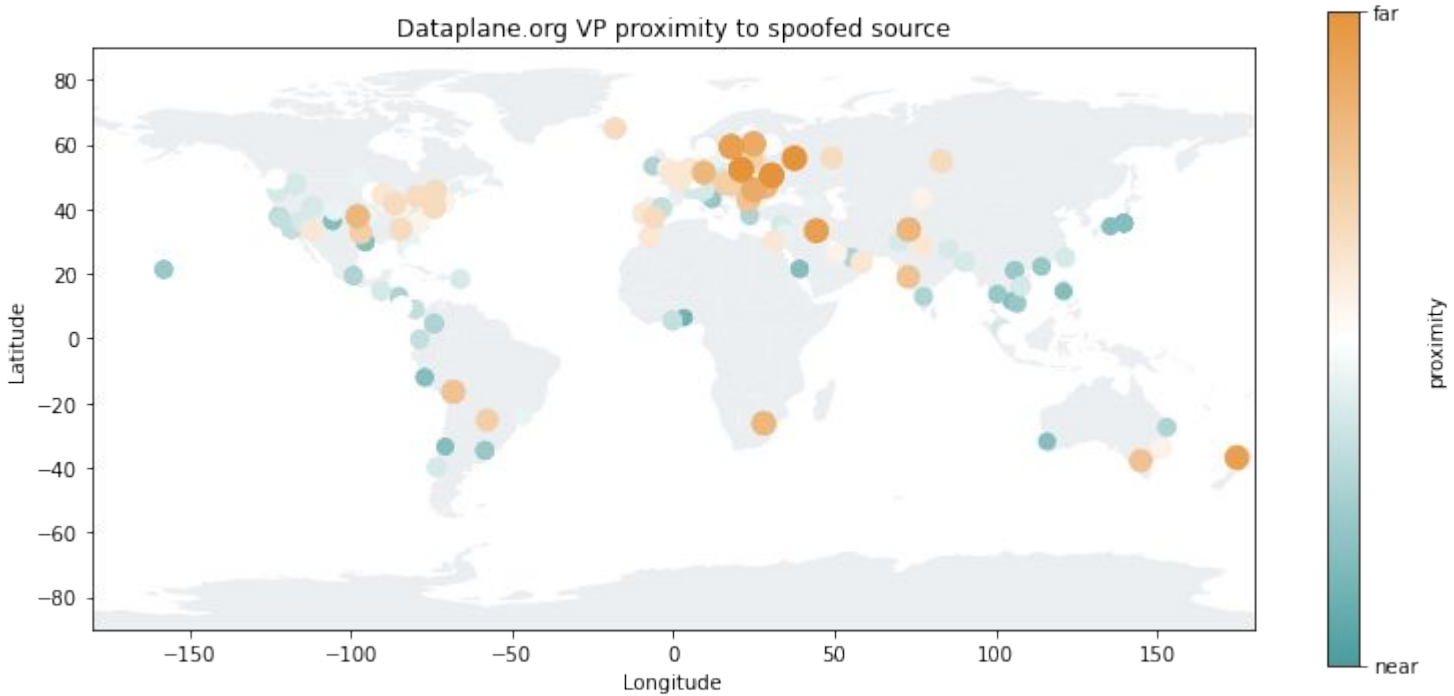

Censys
1e9
3.5
3.0
2.5
2.0
1.5
1.0
0.5
0.0
IP dst.addr as int
2023-12-29
2024-01-18
2024-02-07
2024-02-27
2024-03-18
Date


Heatmap of Key Scanners Activity
Scanner Group
shadowserver
censys
shodan
internet-measurement
busy node
2024-01-01
2024-01-03
2024-01-05
2024-01-07
2024-01-09
2024-01-11
2024-01-13
2024-01-15
2024-01-17
2024-01-19
2024-01-21
2024-01-23
2024-01-25
2024-01-27
2024-01-29
2024-01-31
2024-02-02
2024-02-04
2024-02-06
2024-02-08
2024-02-10
2024-02-12
2024-02-14
2024-02-16
2024-02-18
2024-02-20
2024-02-22
2024-02-24
2024-02-26
2024-02-28
2024-03-01
2024-03-03
2024-03-05
2024-03-07
2024-03-09
2024-03-11
2024-03-13
2024-03-15
2024-03-17
2024-03-19
2024-03-21
2024-03-23
2024-03-25
2024-03-27
2024-03-29
Date
0.8
0.6
0.4
0.2
0.0

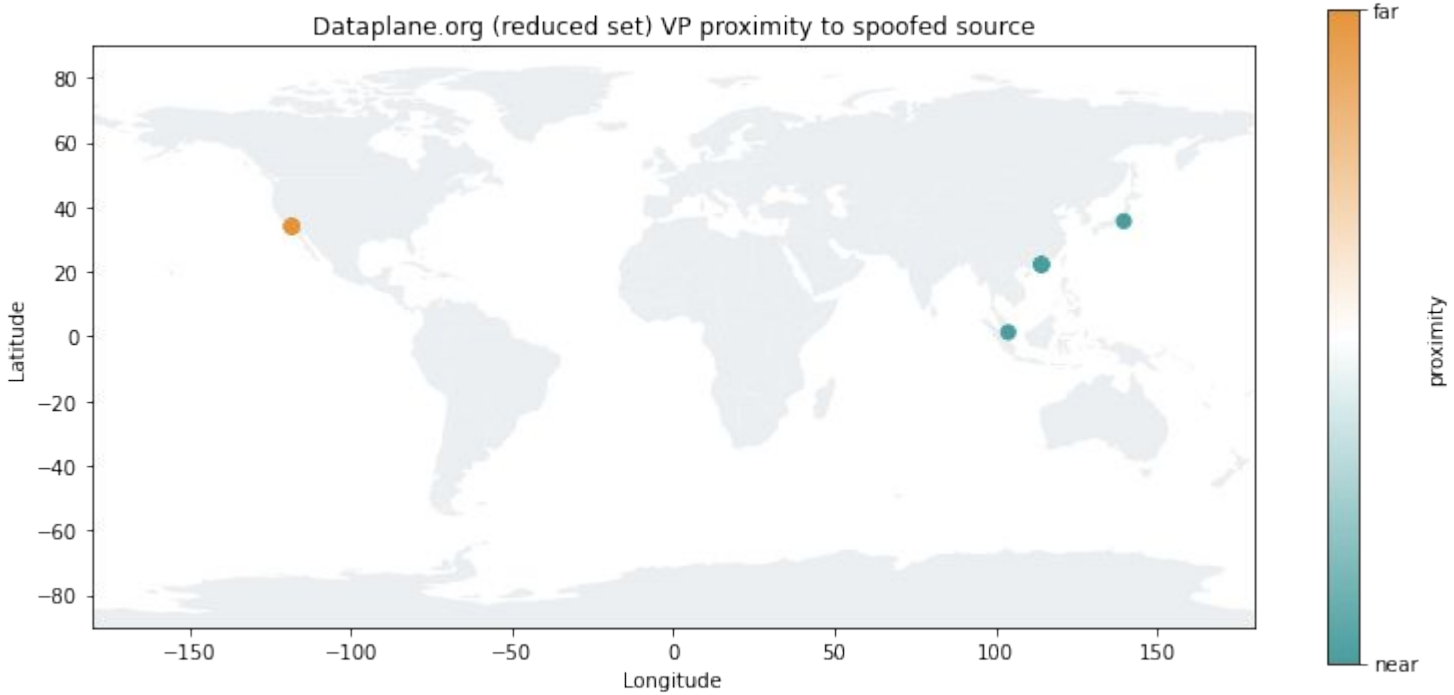
Destination-Adjacent Source Address (DASA) spoofing



IP4 TTL Triangulation



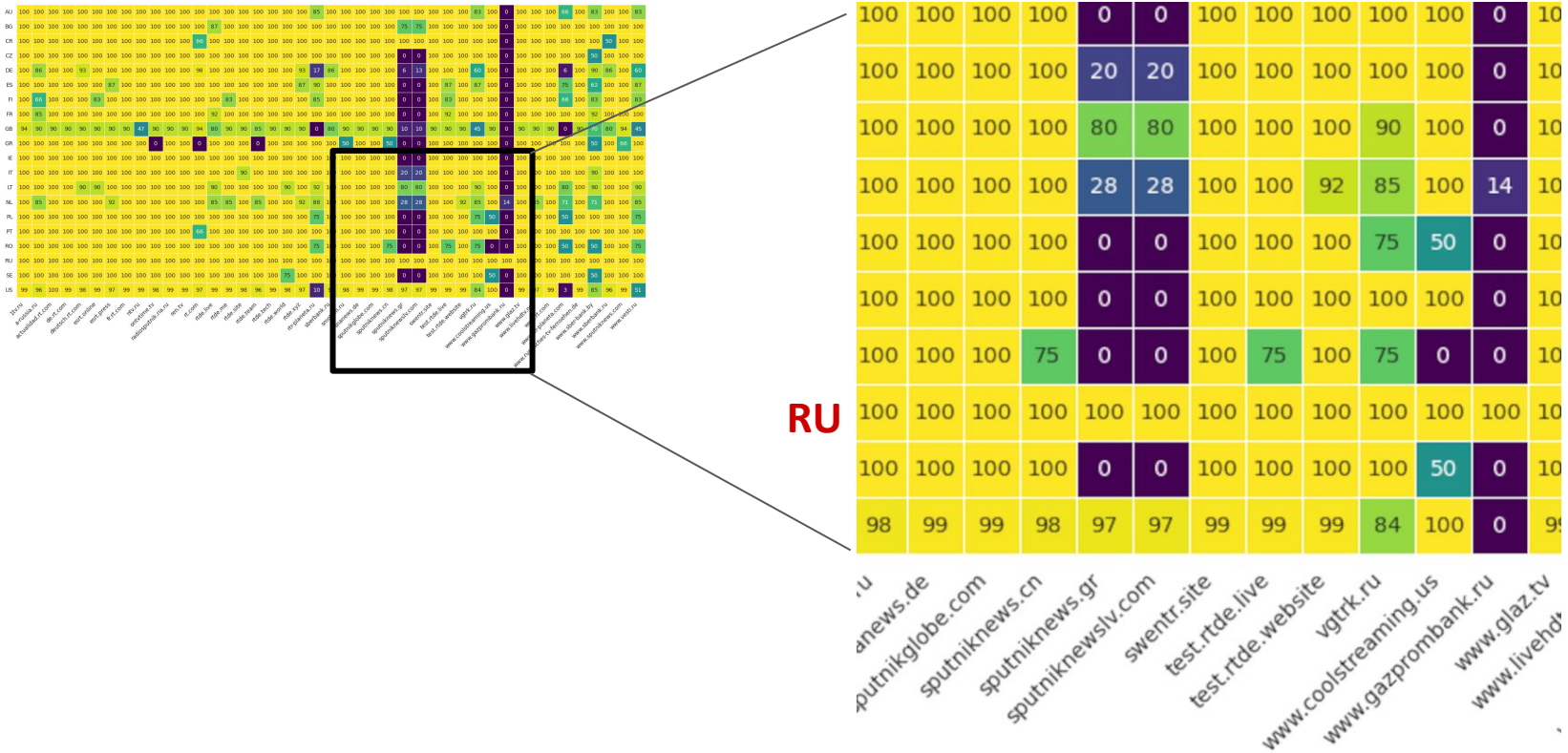
Applying a Low-pass Filter



DASA spoofer, what and why?

- (Likely) CN-based academic research project
- Probably not mapping our infrastructure
  - DASA spoofers in our report, now fixed
- IPv6 DASA spoofers seen too
- Maybe testing external->internal filters
  - Vast majority of sensors saw these queries

Probing for Internet Sanctions on RU



1/5 Evolution of Controlled Tests

- Manually SSH to nodes
- Run tests
- Download results

2/5 Evolution of Controlled Tests

- For each node...
- Background SSH proxy
  - `ssh -D 49152 -f -M -N -S ./${NODE}.sock ${NODE}`
- Loop through targets to test
  - `cat targets | test.sh -p ${NODE} >> output`
- Shut down SSH/proxy
  - `ssh -S ${NODE}.sock -O exit ${NODE}`

3/5 Evolution of Controlled Tests

- Ansible mtr (or other tool) play
  - Install mtr if necessary
  - Upload target list
  - Run test
    - `shell: "nohup mtr … -F targets > output &"`
- Another play to fetch results and clean up

4/5 Evolution of Controlled Tests

- For more complex experiments…
- Ansible-driven, but async poll a control script
  - Fetch node properties (e.g., router L2 address)
  - Prepare node and run test.sh
  - Async poll
  - When tests finish, retrieve output and cleanup

5/5 Evolution of Controlled Tests

- Sorry: no direct SSH access
- Sorry: too complicated/difficult
  - e.g., unusual dependencies, resource constraints
- Sorry: no full-bore zmap from country X

- Future: API?
- Supporting research is time consuming and costly

Bibliography

- John Kristoff, “**Building an Internet Security Feeds Service**”, USENIX ;login;, Fall 2018
- John Kristoff, Mohammad Ghasemisharif, Chris Kanich, Jason Polakis, “**Plight at the End of the Tunnel: Legacy IPv6 Transition Mechanisms in the Wild**”, in Proceedings of the Passive and Active Measurement Conference (PAM), 2021.
- Resing, Max, “**Should network operators hop on the data plane?**”, Bachelor Thesis, University of Twente, 2021.
- John Kristoff, Moritz Müller, Arturo Filastò, Max Resing, Chris Kanich, Niels ten Oever, “**Internet Sanctions on Russian Media: Actions and Effects**”, in Proceedings of Free and Open Communications on the Internet (FOCI), 2024.
- Georgia Tech-led measurement paper, under submission.
- University of Maryland-led measurement paper, in progress.

Thank you, contact information

Contact: John Kristoff

 jtk@dataplane.org

 https://dataplane.org/jtk/

 https://infosec.exchange/@jtk