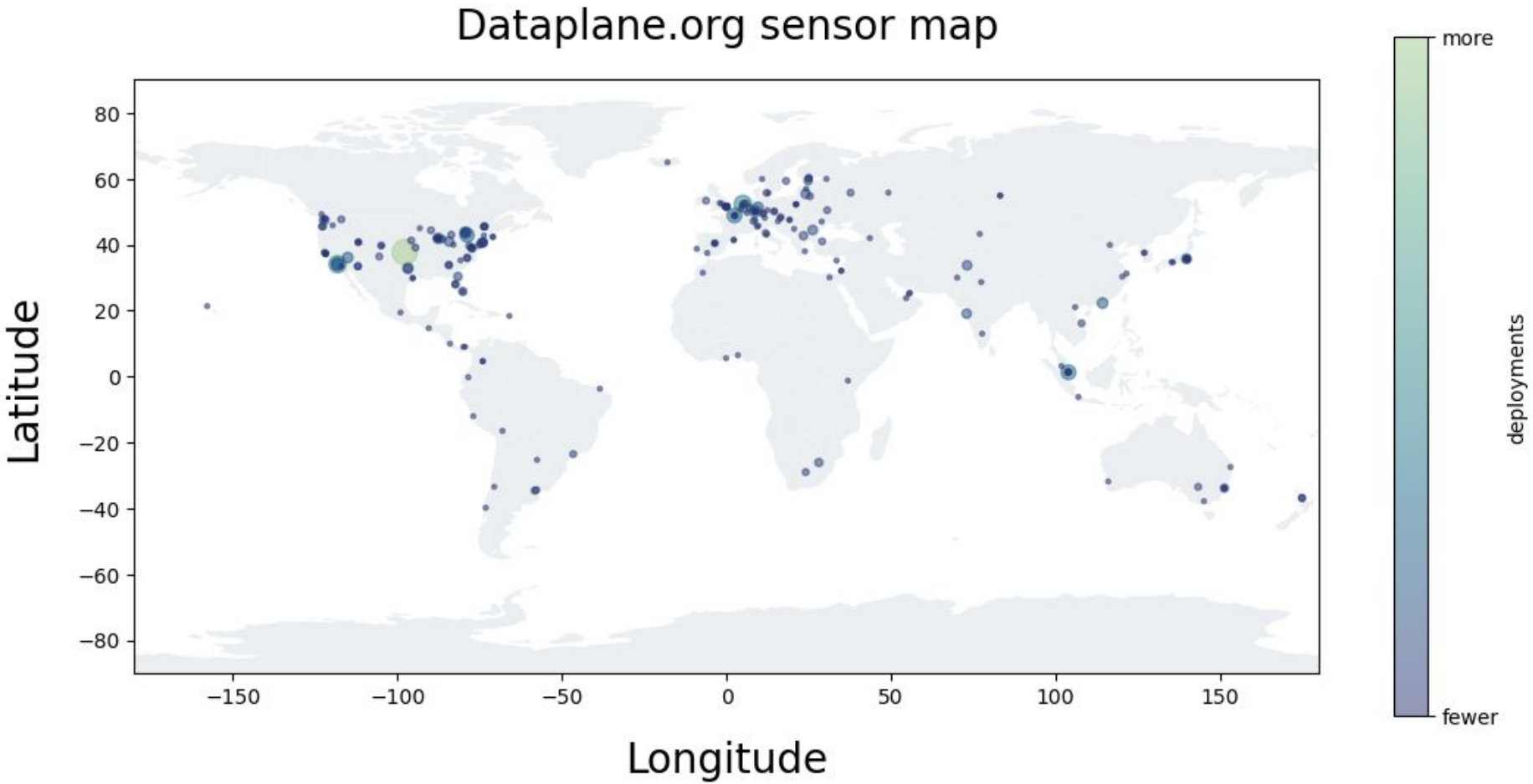
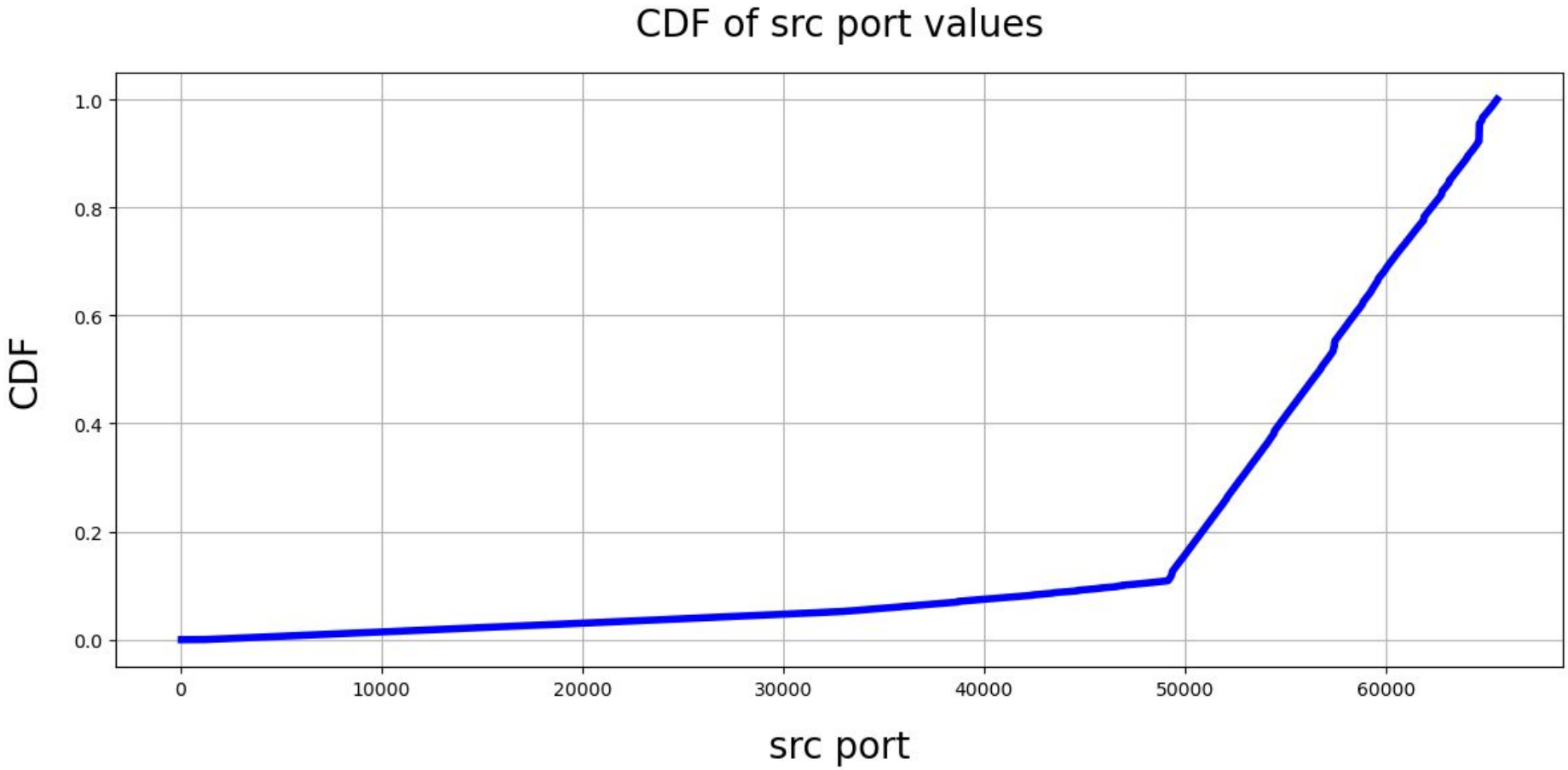
SMTP Distributed Monitoring in-the-wild

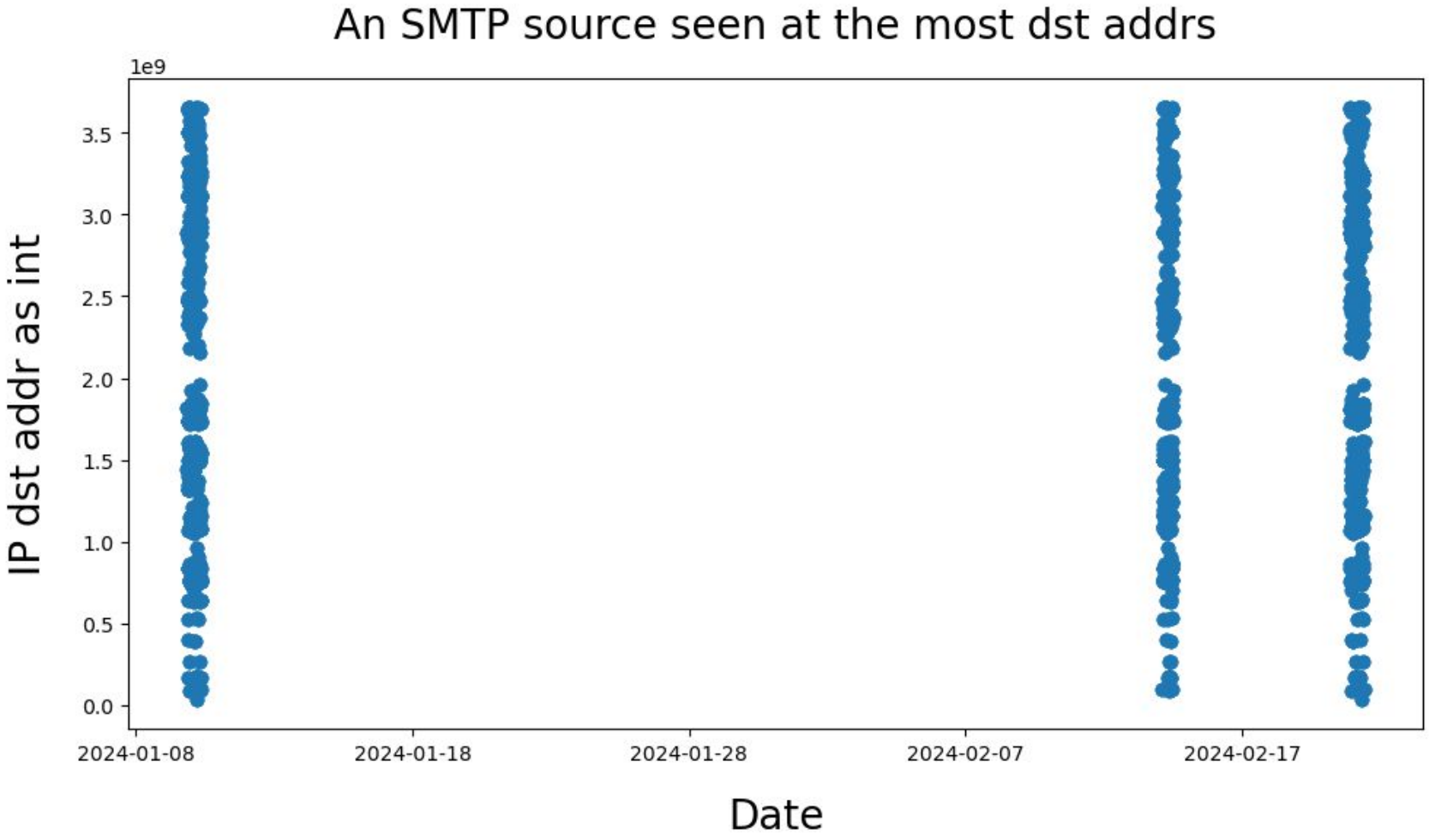
John Kristoff

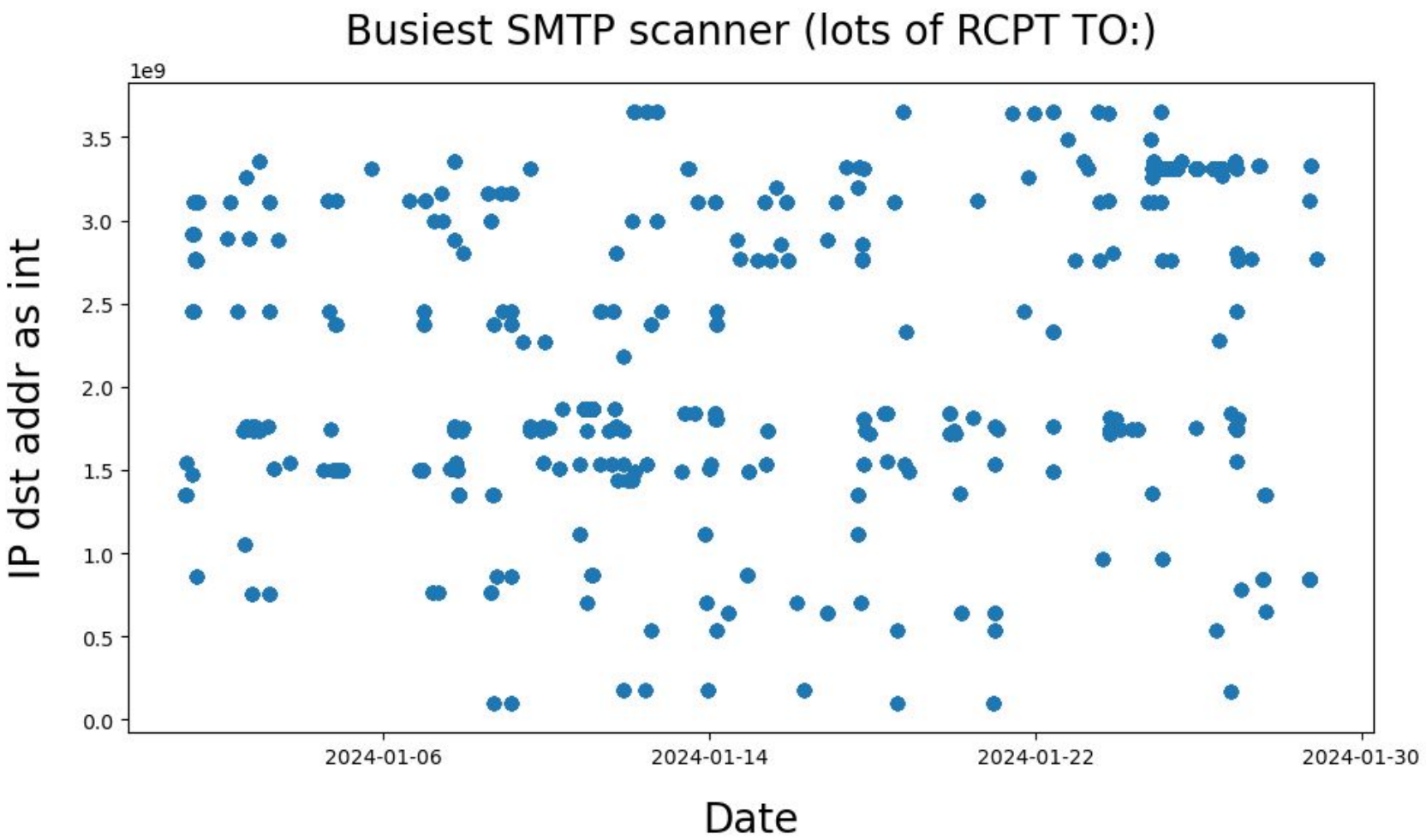
Overview

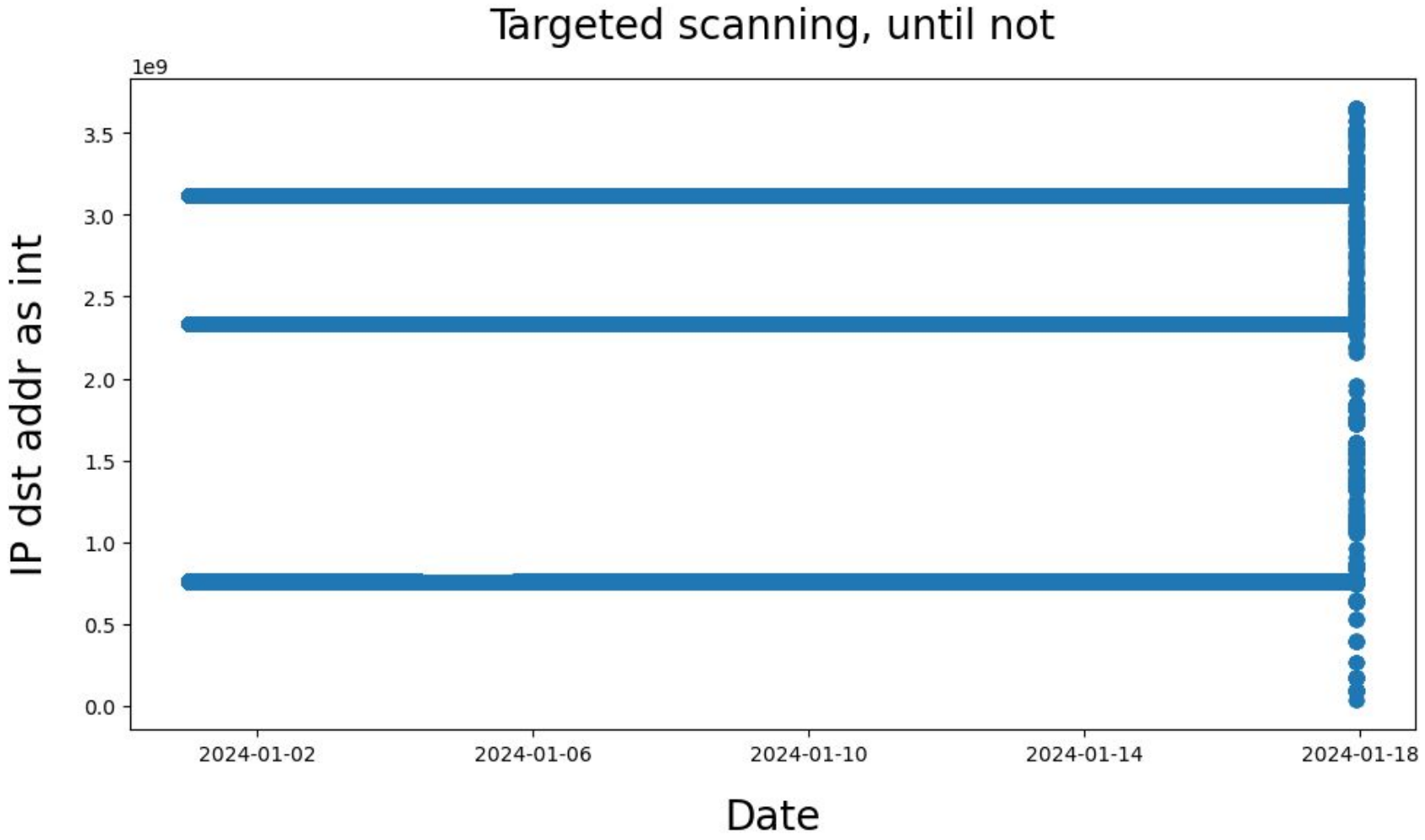
- ~500 sensor nodes in ~100 nets
- Unadvertised service (no A/AAAA/MX RRs)
- Data window: 2024-01-01 to 2024-03-31
- 27+ million events
  - connect, helo, ehlo, rcpt to, ..., !body

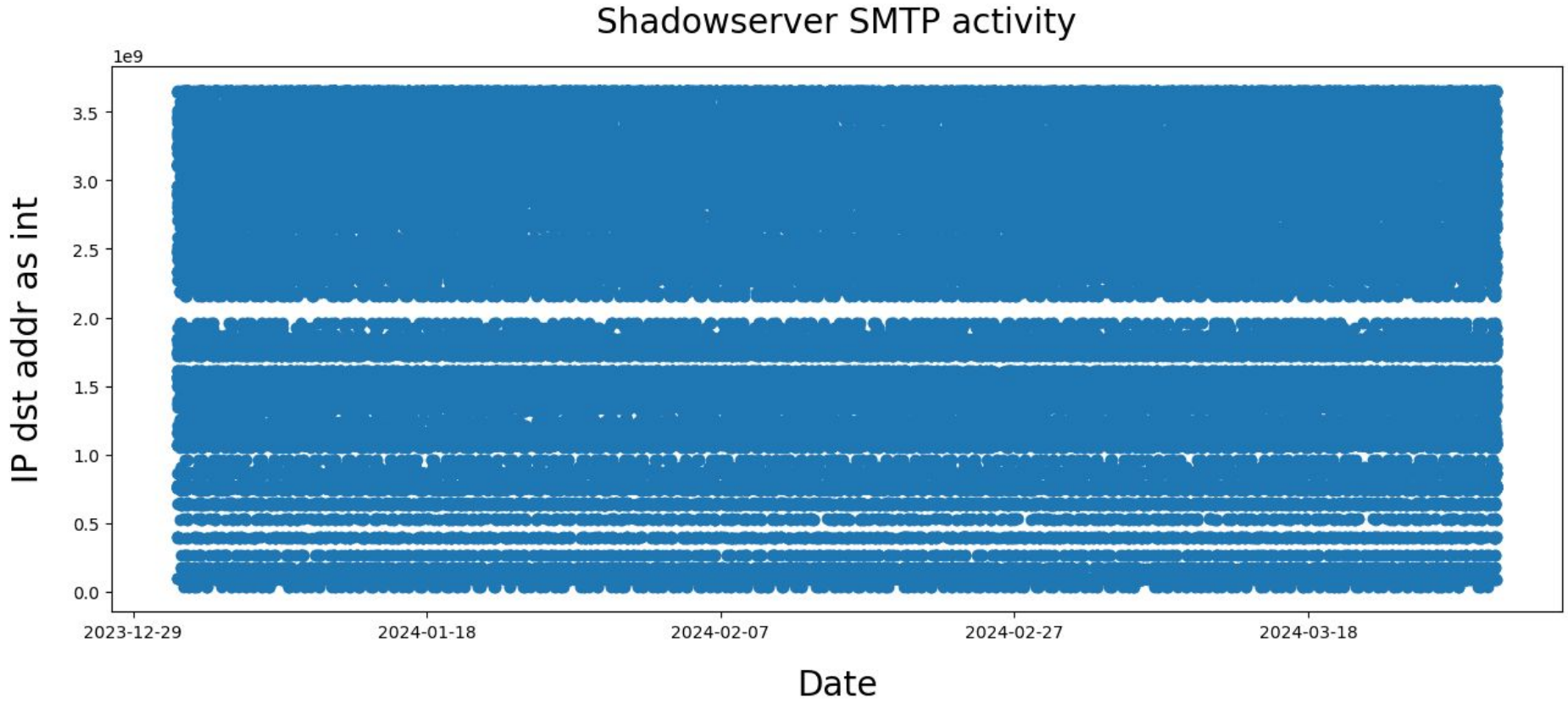

Dataplane.org sensor map
Latitude
Longitude
80
60
40
20
0
−20
−40
−60
−80
−150
−100
−50
0
50
100
150
more
fewer
deployments

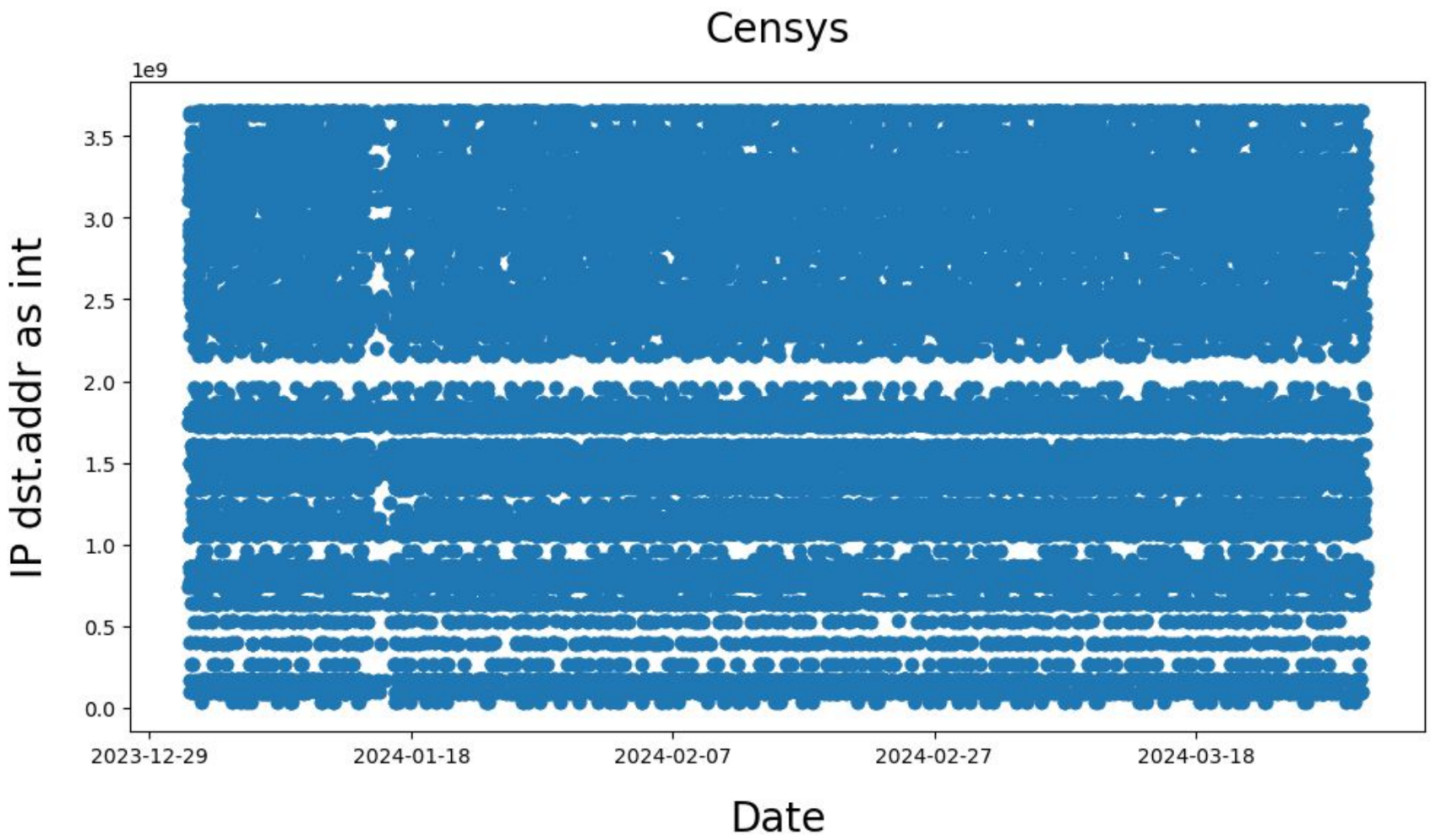

CDF of src port values
CDF
1.0
0.8
0.6
0.4
0.2
0.0
0
10000
20000
30000
40000
50000
60000
src port

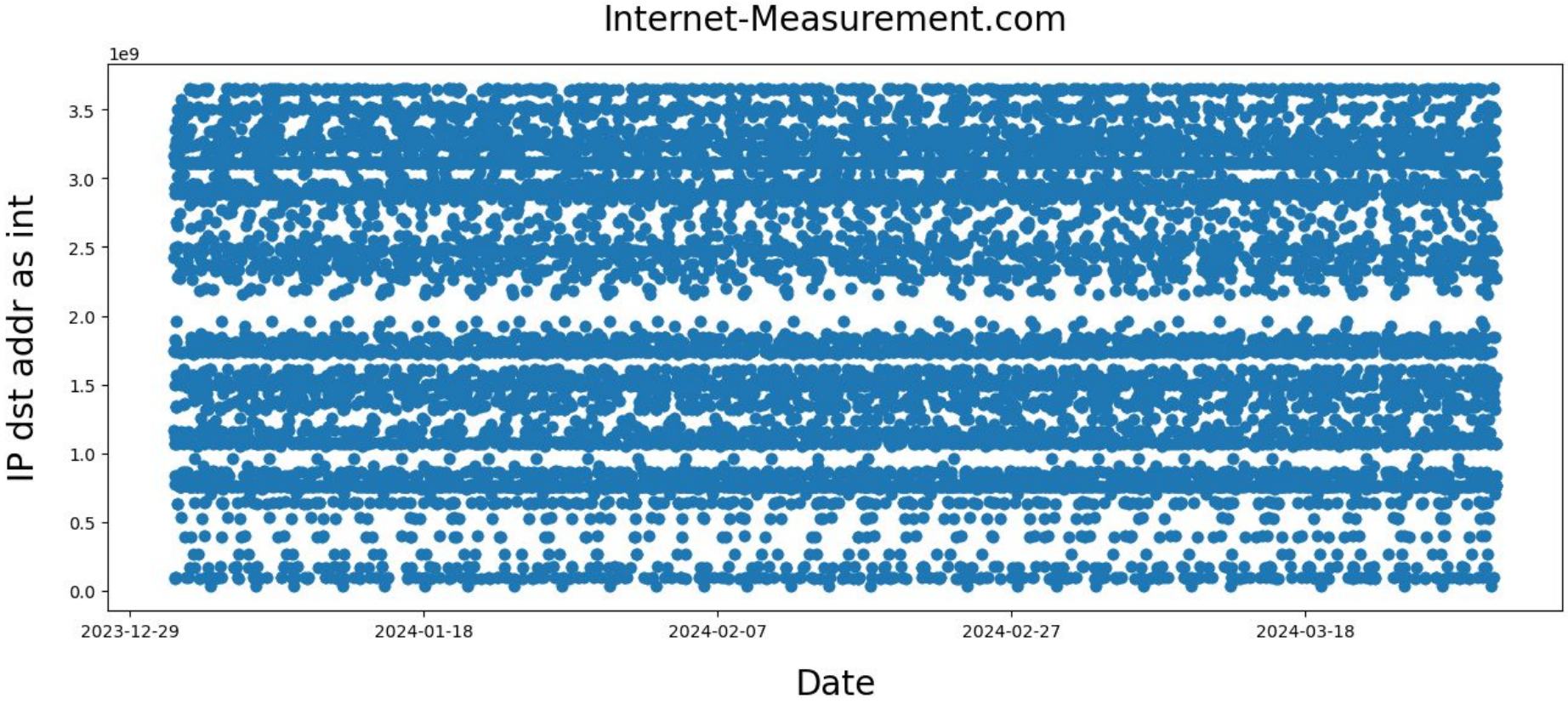

An SMTP source seen at the most dst addrs
1e9
3.5
3.0
2.5
2.0
1.5
1.0
0.5
0.0
IP dst addr as int
2024-01-08
2024-01-18
2024-01-28
2024-02-07
2024-02-17
Date

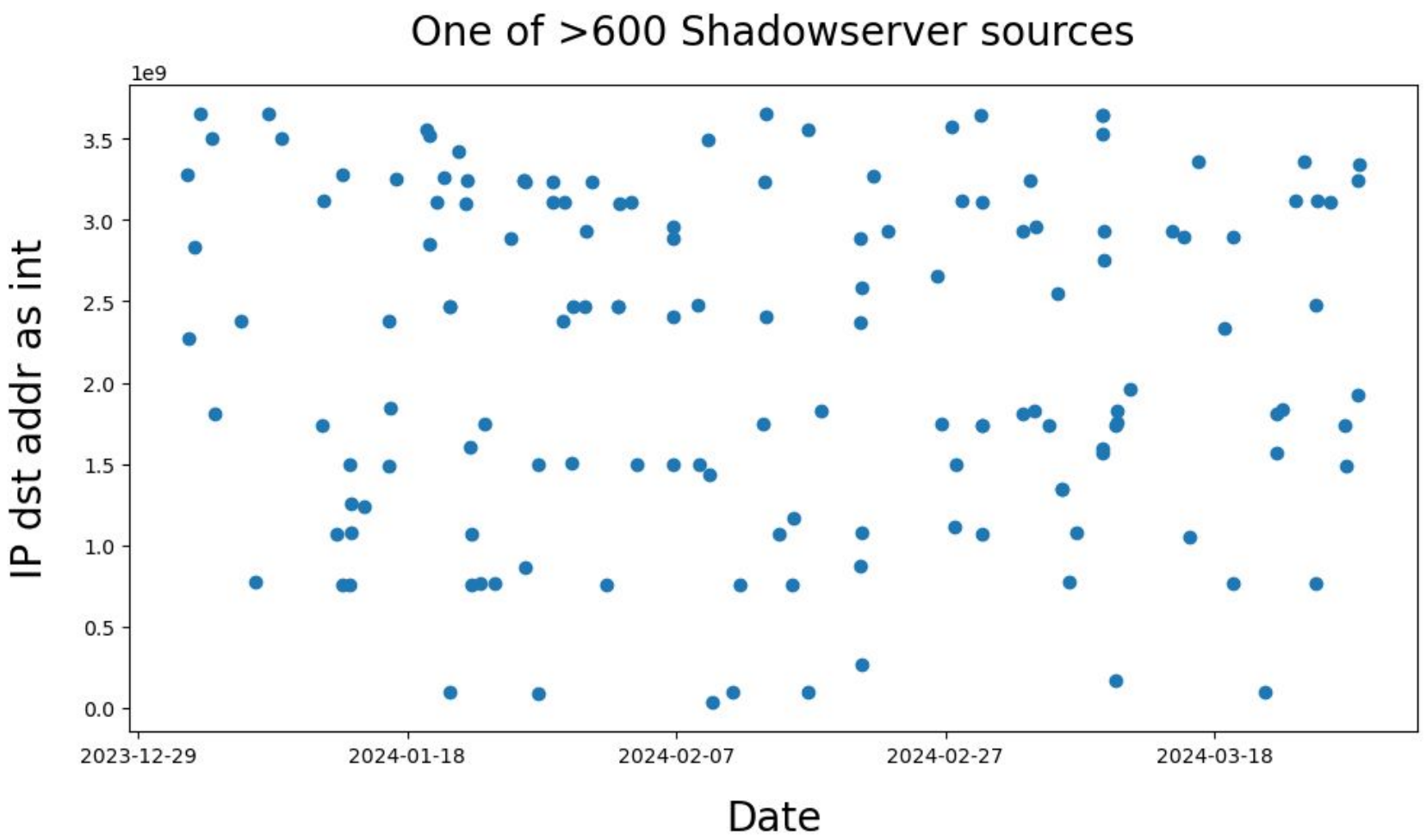

Busiest SMTP scanner (lots of RCPT TO:)
1e9
3.5
3.0
2.5
2.0
1.5
1.0
0.5
0.0
IP dst addr as int
2024-01-06
2024-01-14
2024-01-22
2024-01-30
Date

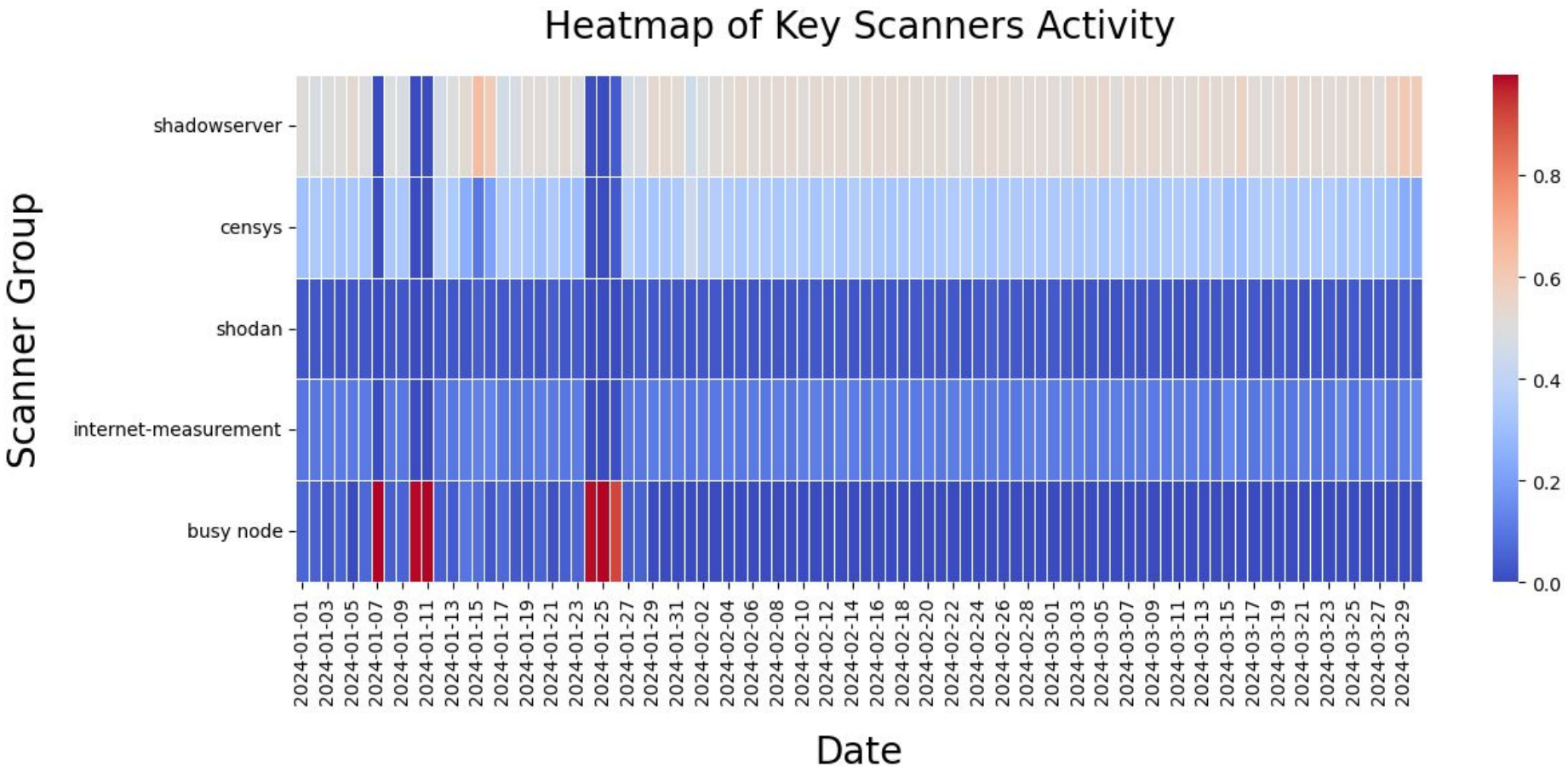

Targeted scanning, until not
1e9
3.5
3.0
2.5
2.0
1.5
1.0
0.5
0.0
IP dst addr as int
2024-01-02
2024-01-06
2024-01-10
2024-01-14
2024-01-18
Date


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


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


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


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


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

Thank you, contact information

Contact: John Kristoff

 jtk@dataplane.org

 https://dataplane.org/jtk/

 https://infosec.exchange/@jtk