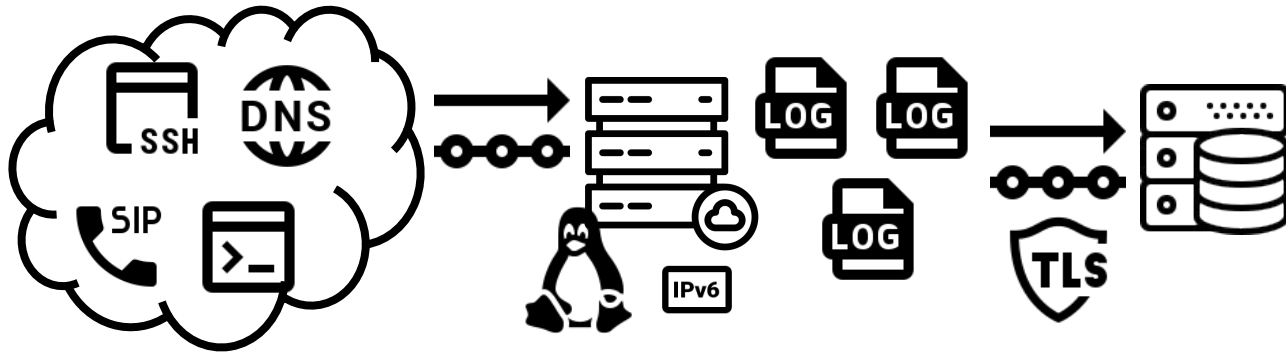# Dataplane.org

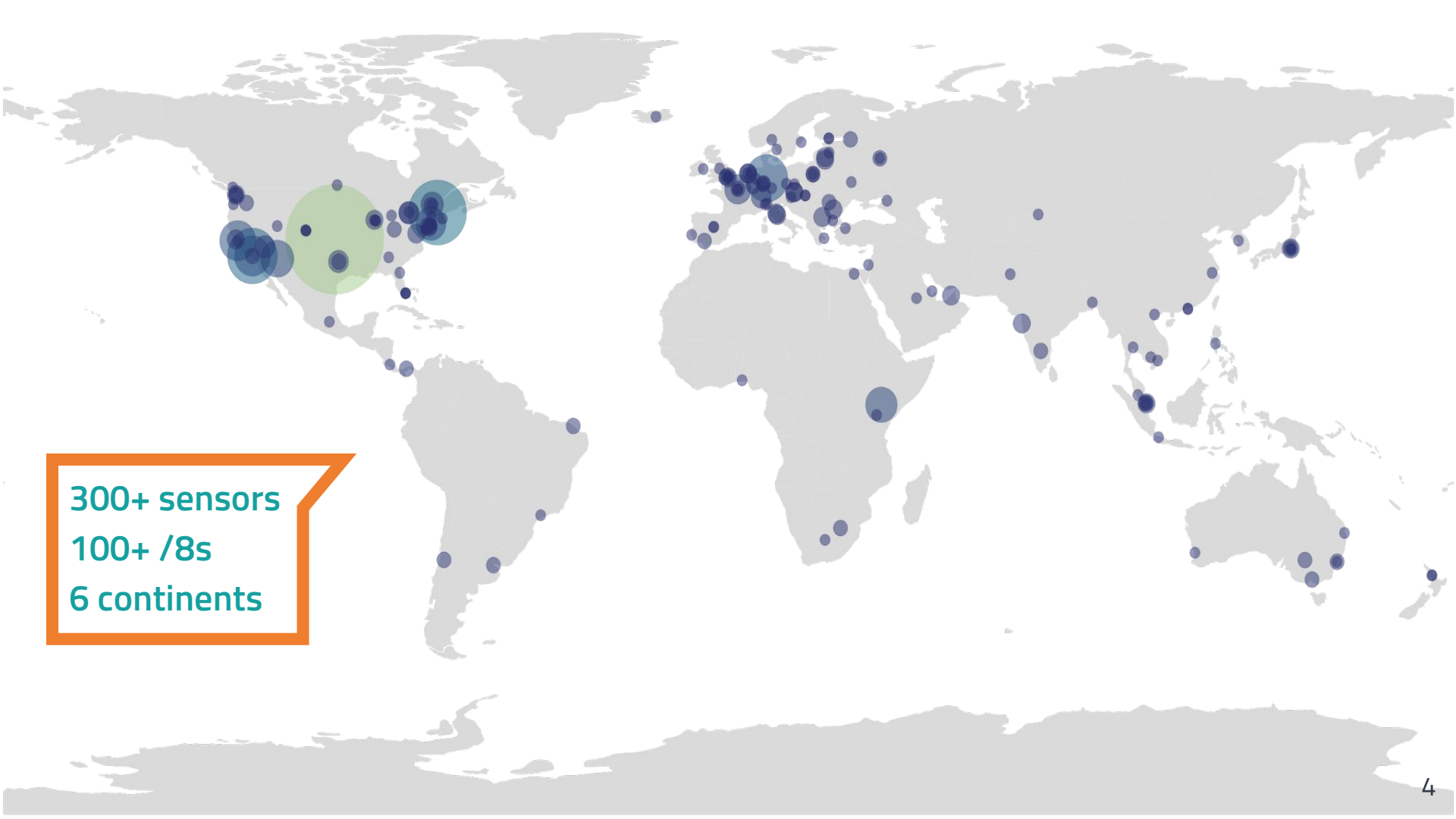The Dataplane.org Sensor Network:
Operation and Analysis

Table of Contents

- What is a sensor?
- Sensor acquisition and setup
- Network infrastructure
- Signals (aka feeds, data, and insight)
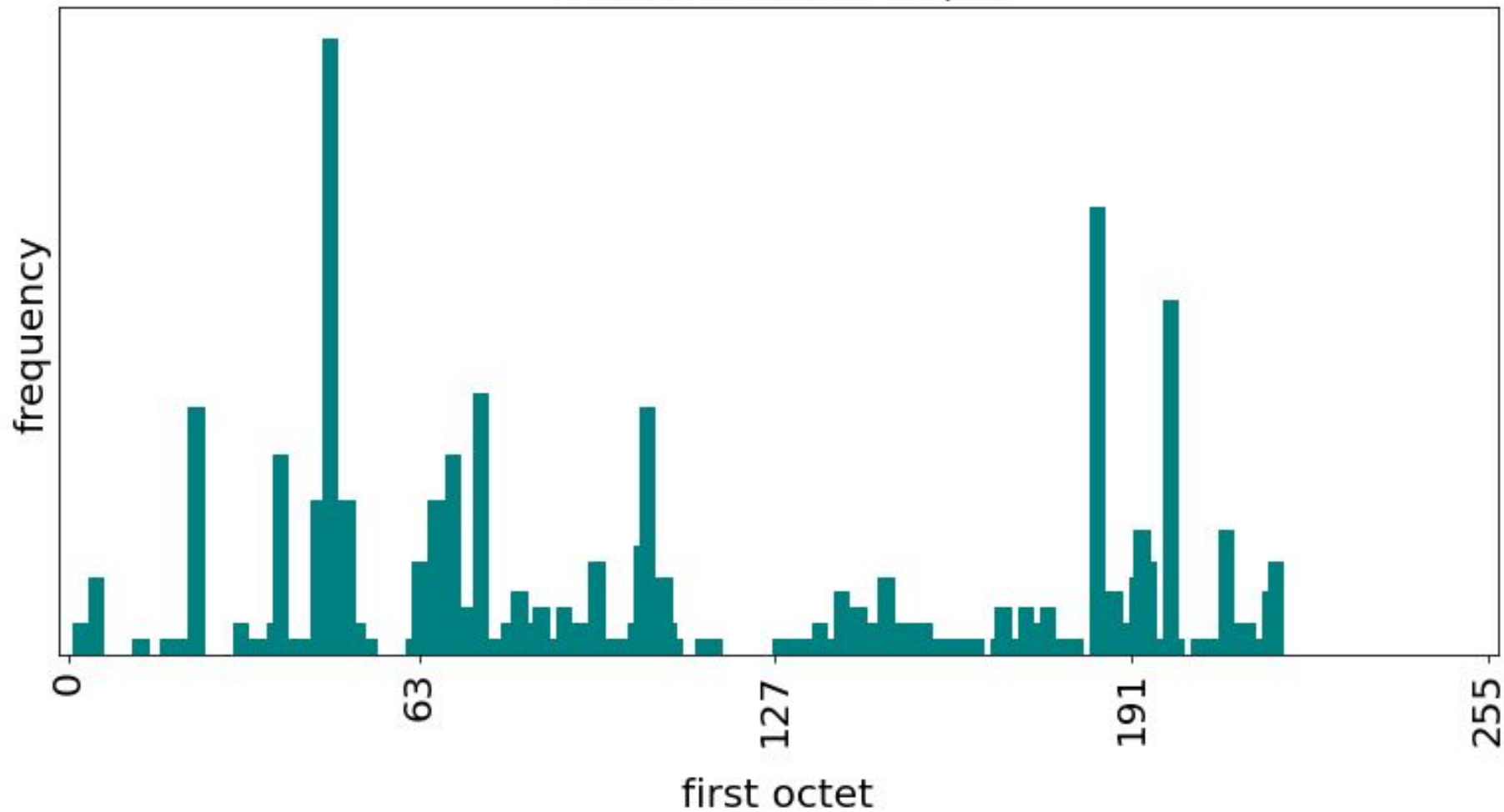- Analysis and use cases
- Future

Vantage Points

- **Sensors - listeners**
- Probes   - senders

300+ sensors
100+ /8s
6 continents

Sensors in the IPv4 /8s

frequency

first octet

0   63   127   191   255

5

Hosting providers

- ○ ~100 different hosting providers
- ○ OpenVZ, KVM, dedicated servers, others
- ○ Lots of logins and payment agreements
- ○ Cost varies from <$10/year to >$20 month
- ○ Stability, support, and practices vary widely

IP re-addressing events in 2022

- 70% – never

- 12% – once

- 15% – twice

- 2% – three times

- <1% but not zero – four times

Host Provider Uncertainty

provider X network migration effect
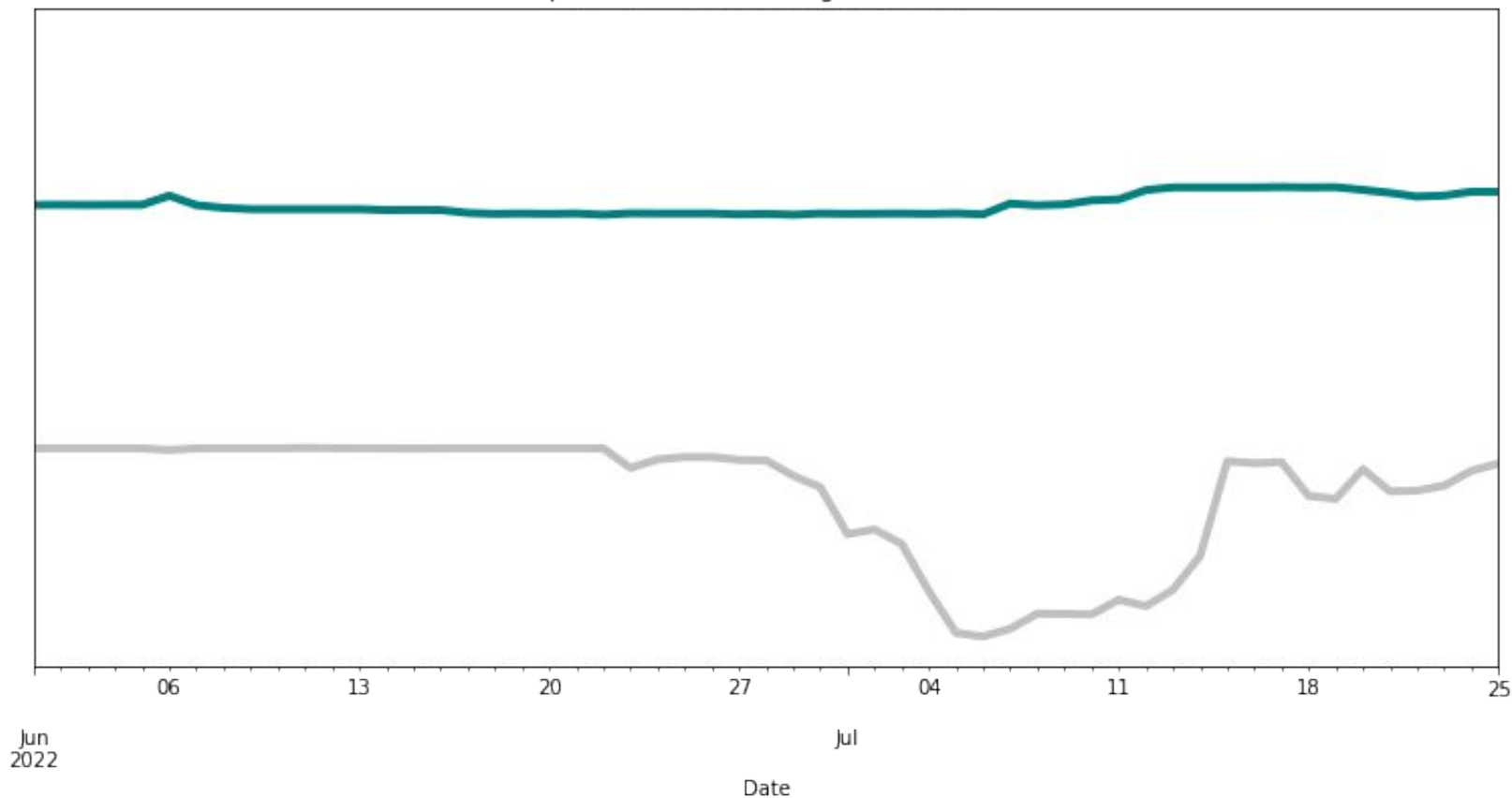
Sensing techniques

- ○ **Passive pcap or firewall log-based**
- ○ **Custom or standard listeners**
- ○ **Local system handling versus tunneled**
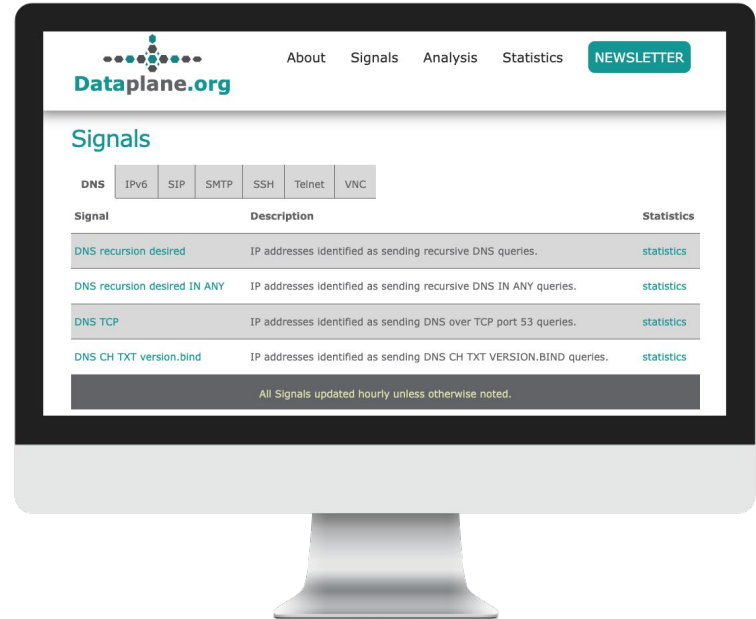
Sensor
Management

Signals

- **Not block lists**
- **Minimal daemons**
- **Logs to syslog**
- **Signals (partial list)**
  - DNS
  - SIP
  - SSH
  - Telnet
  - VNC

SSH Signal

SSH Client Connections

```
# ASN   | ASname       | ipaddr          | lastseen            | category
---------------------------------------------------------------------------
803     | SASKTEL      | 71.17.149.4     | 2022-09-27 05:28:05 | sshclient
88      | PRINCETON-AS | 128.112.138.144 | 2022-09-27 13:48:37 | sshclient
```

SSH Password Authentication

```
# ASN   | ASname       | ipaddr          | lastseen            | category
---------------------------------------------------------------------------
3       | MIT-GATEWAYS | 18.18.245.11    | 2022-09-22 10:58:53 | sshpwauth
1257    | TELE2        | 83.249.223.18   | 2022-09-26 02:06:11 | sshpwauth
```

SSH ID/Password Pairs

```
# category | id     | password
----------------------------------
sshidpw    | admin  | pa$$w0rd15
sshidpw    | centos | qwerty1234
```

DNS Signal

DNS Recursion Desired

# ASN	ASname	ipaddr	lastseen	category
4134	CHINANET-BACKBONE	112.102.204.2	2022-09-25 10:13:24	dnsrd
13036	TMOBILE-CZ T-Mobile Czech Repu	46.13.73.47	2022-09-28 17:19:48	dnsrd

DNS Recursion Desired IN ANY

# ASN	ASname	ipaddr	lastseen	category
18881	TELEFONICA BRASIL S.A	177.16.64.10	2022-09-22 02:53:24	dnsrdany
203451	K-Telecom-Network K-telekom LL	185.15.37.229	2022-09-25 21:09:46	dnsrdany

DNS TCP

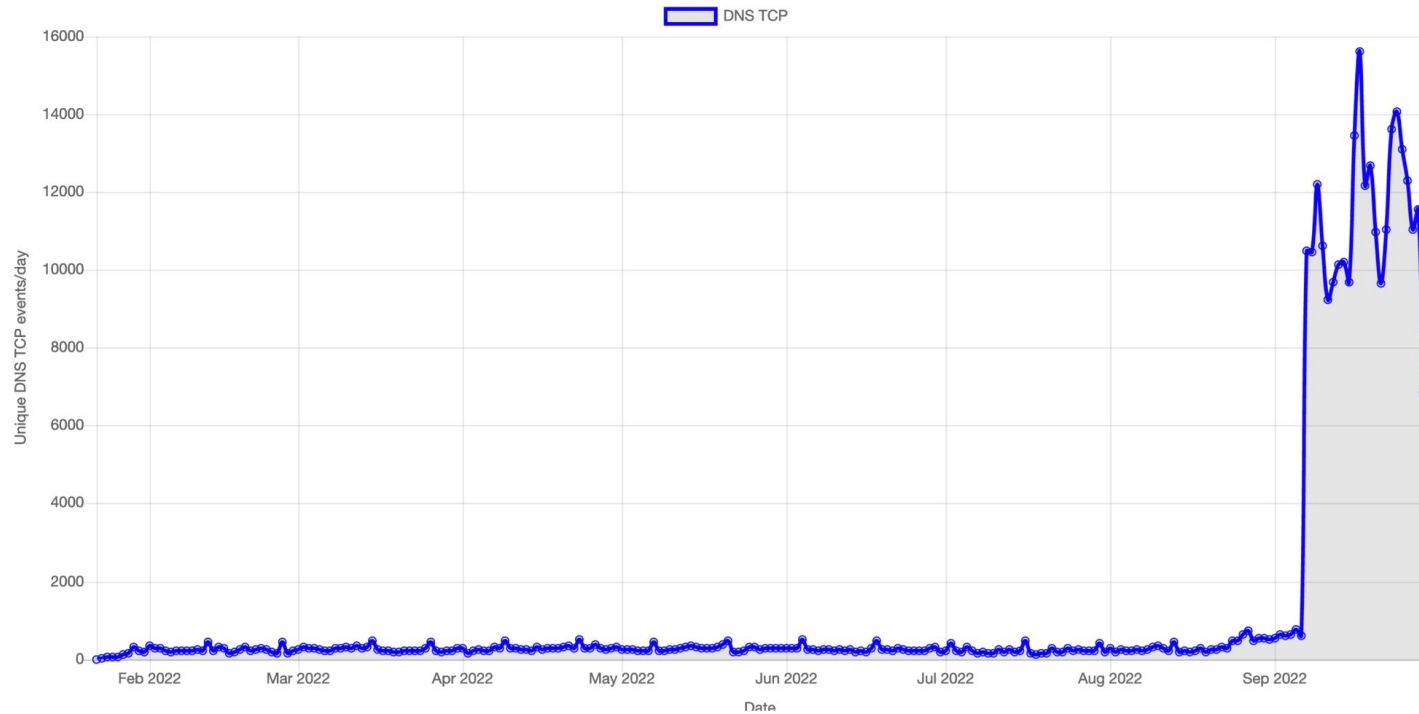| # ASN	ASname	ipaddr	lastseen	category
1103	SURFNET-NL SURF B.V.	145.102.6.125	2022-09-28 15:58:26	dnstcp
3214	XTOM xTom GmbH	62.133.33.33	2022-09-26 08:00:51	dnstcp

DNS CH TXT version.bind

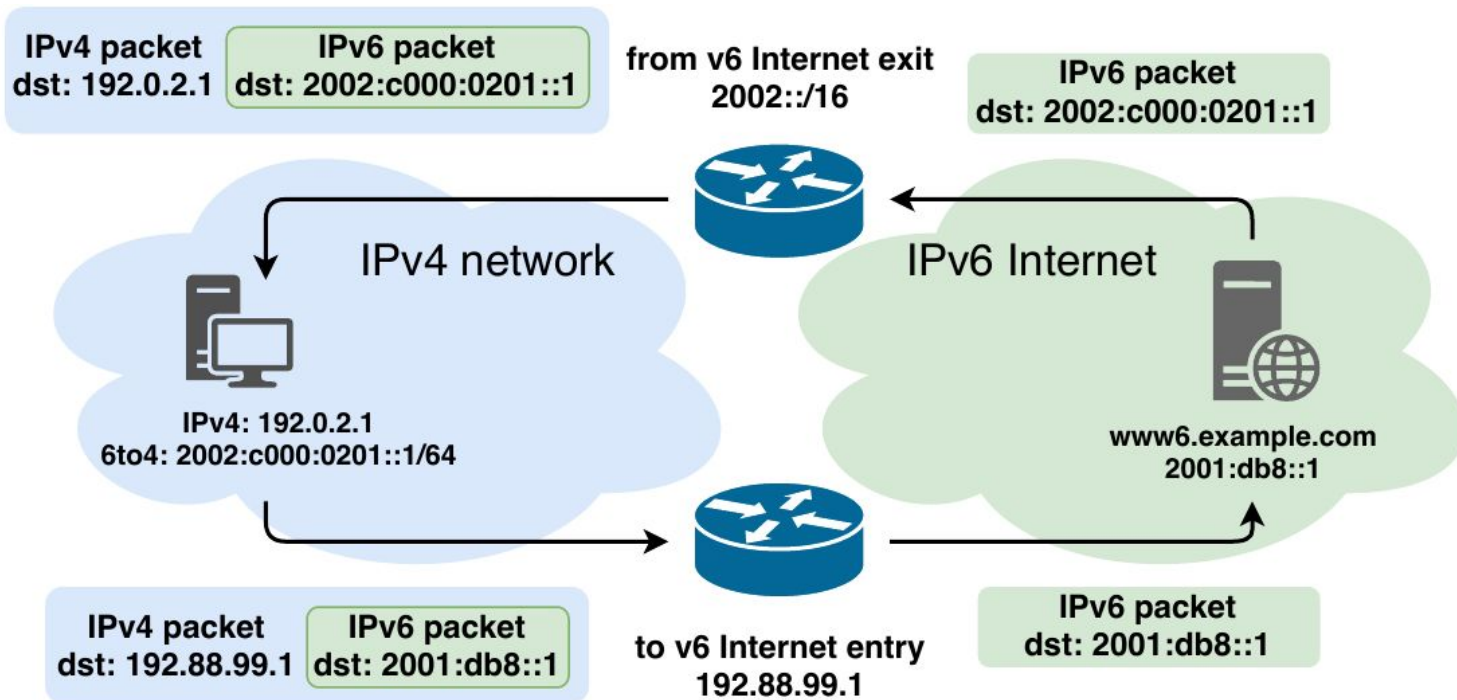| # ASN	ASname	ipaddr	lastseen	category
9808	CHINAMOBILE-CN China Mobile Co	117.187.173.111	2022-09-25 16:23:37	dnsversion
37963	ALIBABA-CN-NET Hangzhou Alibab	8.142.139.58	2022-09-26 14:56:18	dnsversion

DNS TCP

DNS TCP Signal Statistics @ Dataplane.org

This interactive time-series plot is a measure our observed DNS TCP signals data.

IP protocol 41 (proto41)

IPv4 packet
dst: 192.0.2.1

IPv6 packet
dst: 2002:c000:0201::1

from v6 Internet exit
2002::/16

IPv6 packet
dst: 2002:c000:0201::1

IPv4 network

IPv6 Internet

IPv4: 192.0.2.1
6to4: 2002:c000:0201::1/64

www6.example.com
2001:db8::1

IPv4 packet
dst: 192.88.99.1

IPv6 packet
dst: 2001:db8::1

to v6 Internet entry
192.88.99.1

IPv6 packet
dst: 2001:db8::1

IP Protocol 41

IP protocol 41 Signal Statistics @ Dataplane.org

This interactive time-series plot is a measure our observed IP Protocol 41 signals data.
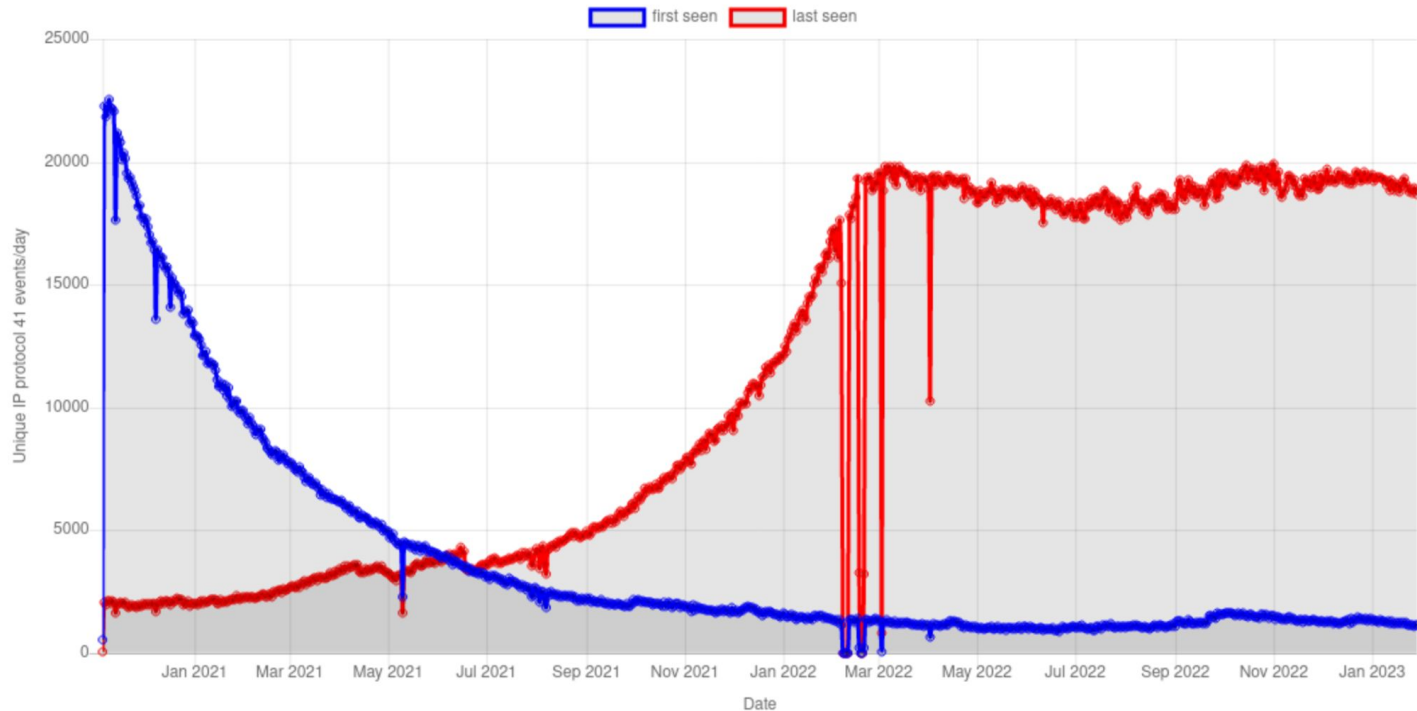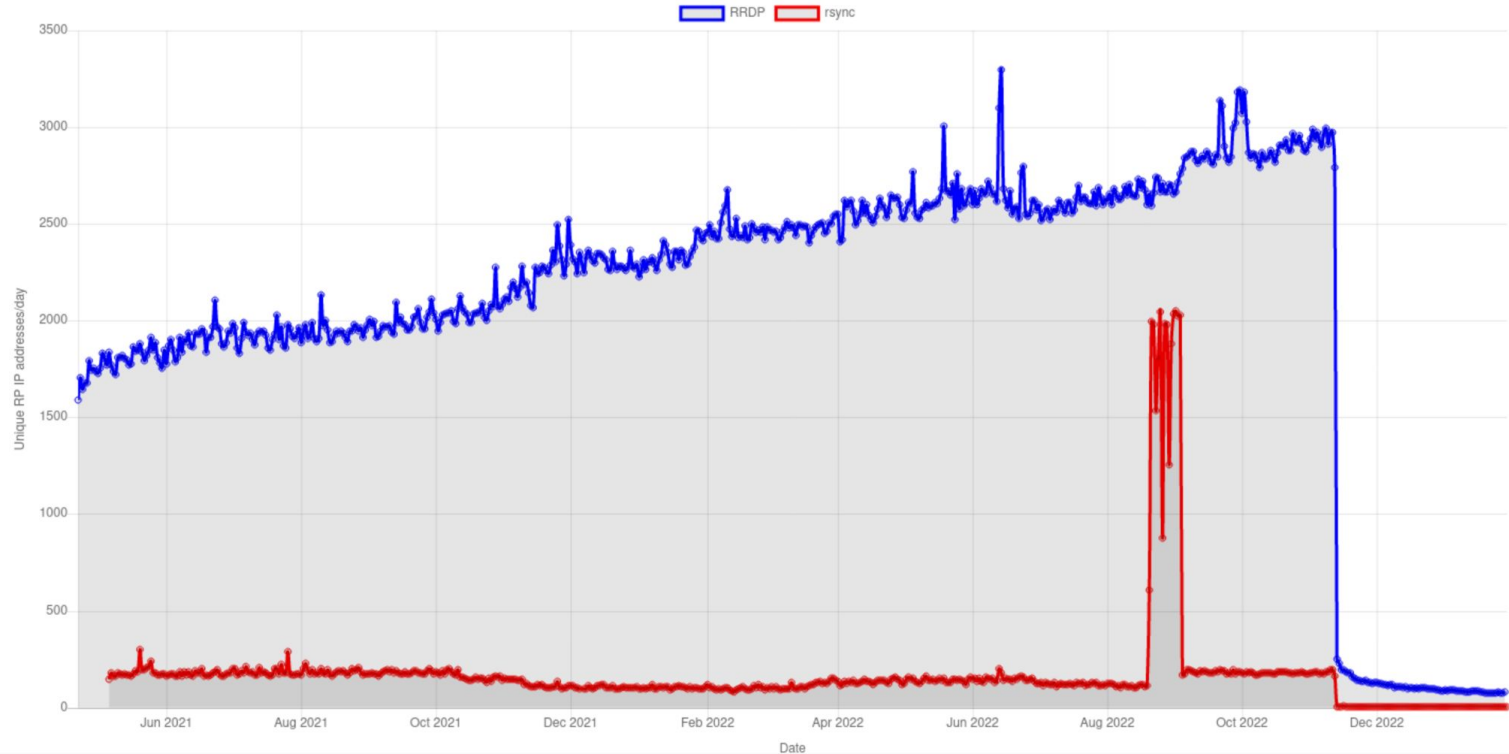
Dataplane.org PP operation

The rpki.dataplane.org system is a publication point (PP) under the ARIN RPKI trust anchor (TA)
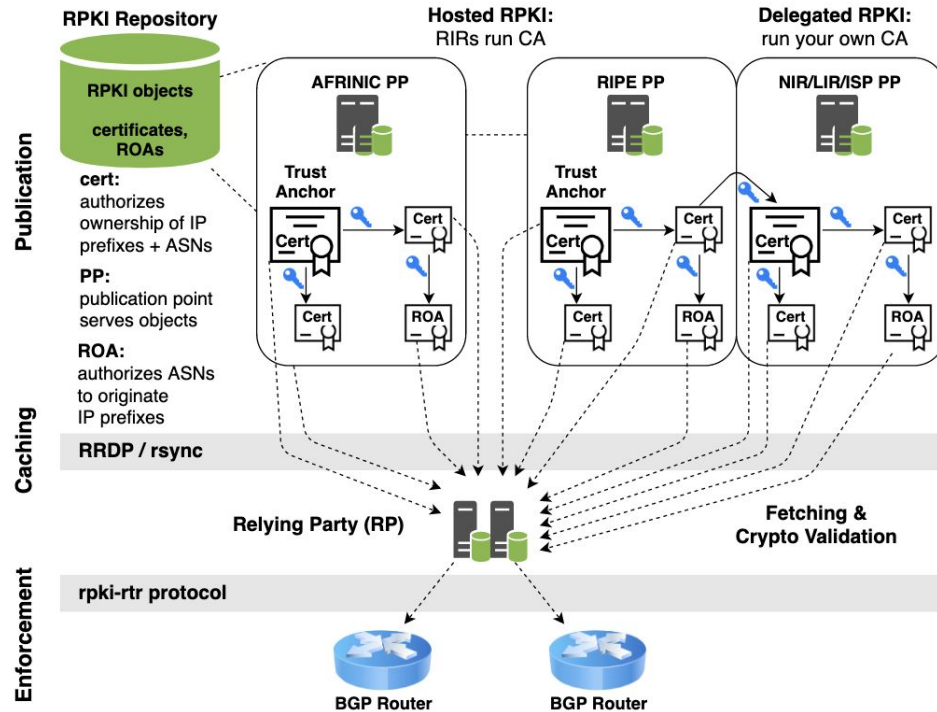
On Measuring RPKI Relying Parties. https://dataplane.org/jtk/publications/kbkmp-mrrp-20.pdf

RPKI Monitor

Number of per day unique IP addresses retrieving RRDP /rrdp/notification.xml file or rsync fetch on the repository
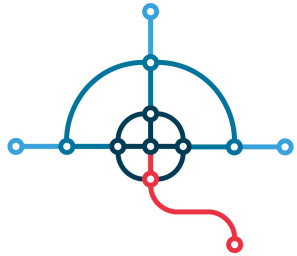
Signal Users

19

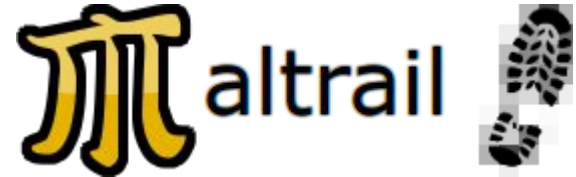# Signal data in 2023

- ○ Full public archive of delayed data
- ○ Custom real-time signal feeds
- ○ Additional applications (e.g., RDP)
- ○ Additional insight (e.g., SSH client software)
- ○ Full flow monitoring
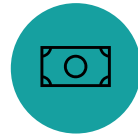- ○ BGP RTBHs (black hole announcements)

Legal

Incorporation
Employer Identification Number
Charitable Status 501(c)(3)

Financial

Banking
Tax Exempt Status
Expenses

Reporting

Accounting
Tax Preparation
Board Meetings

Not For Profit Setup

Matt   **John**   **Bill**

To improve Internet infrastructure operations by facilitating access to raw data collections, measuring Internet activity, analyzing trends, and supporting researchers.

THANK YOU!

🌐 https://dataplane.org

Ⓜ fosstodon.org/@dataplane

dataplane.substack.com

github.com/dataplane

AS 54278