Dataplane.org

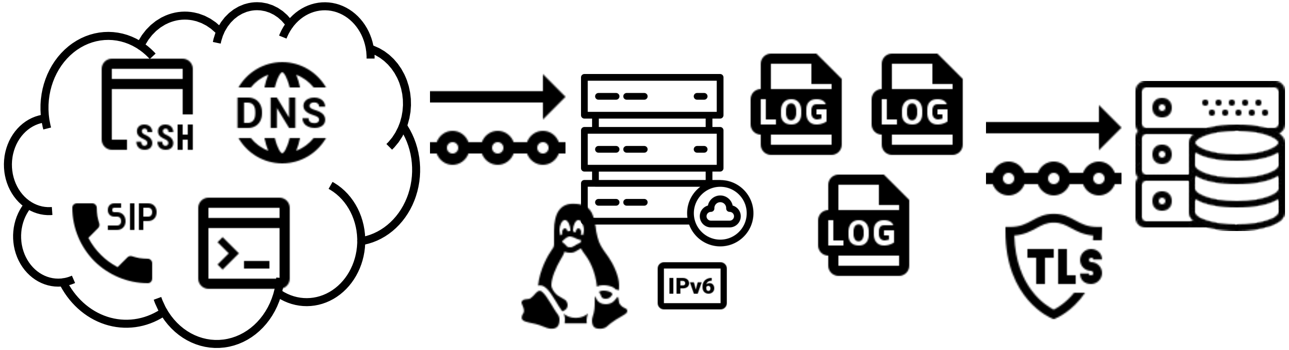
The Dataplane.org Sensor Network: Operation and Analysis

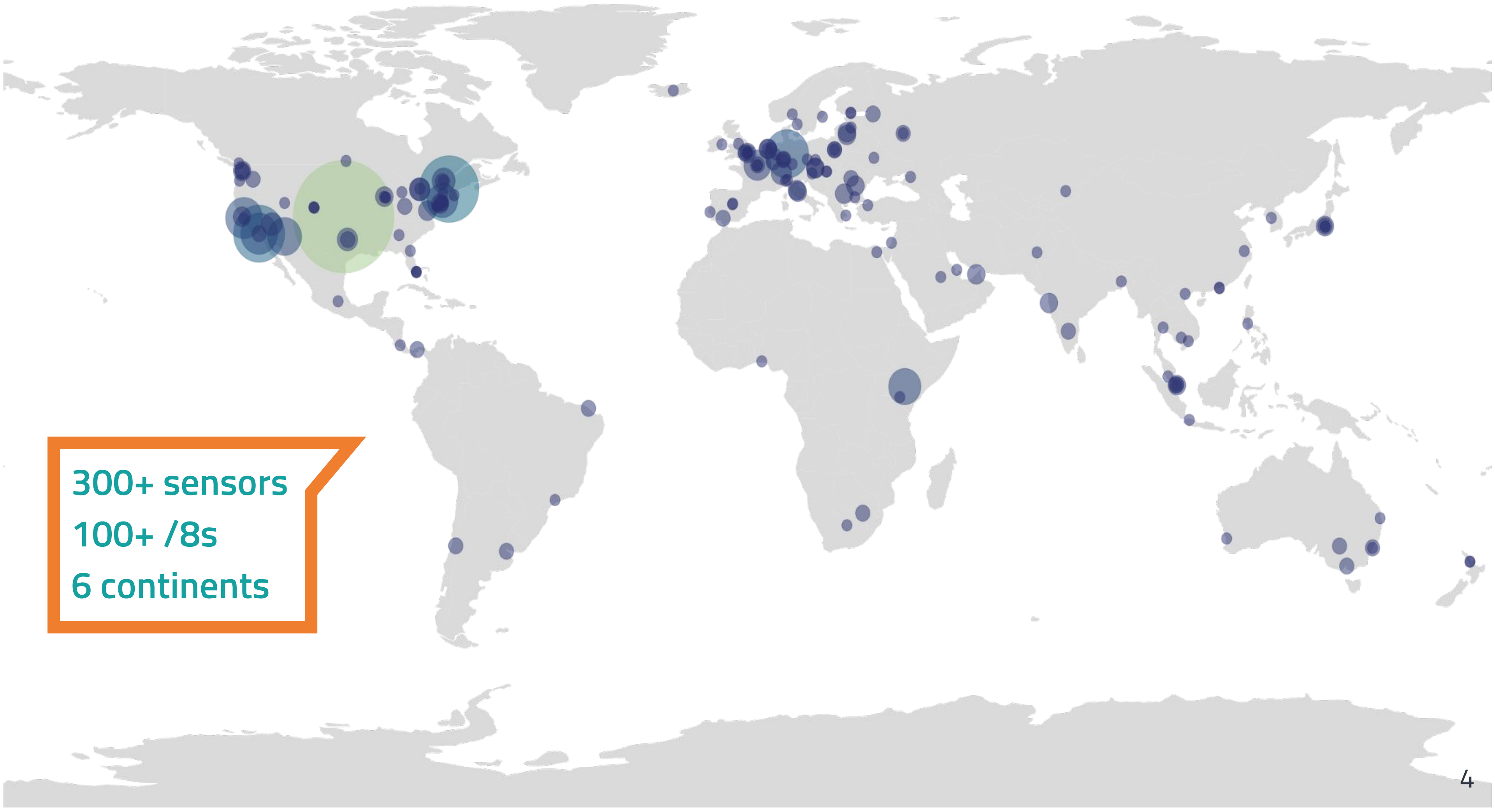
Table of Contents

- 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

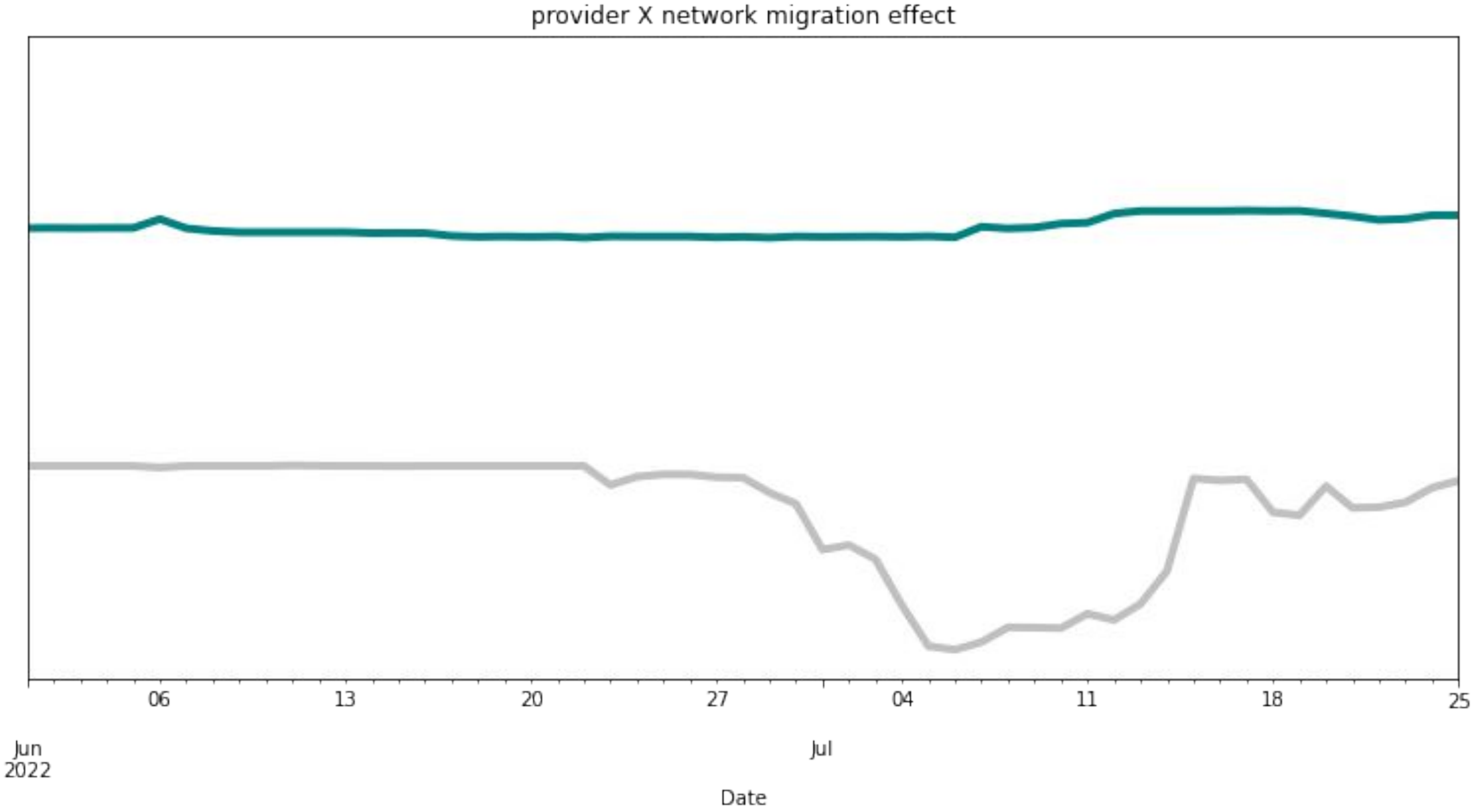
Hosting providers

- ~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 2021

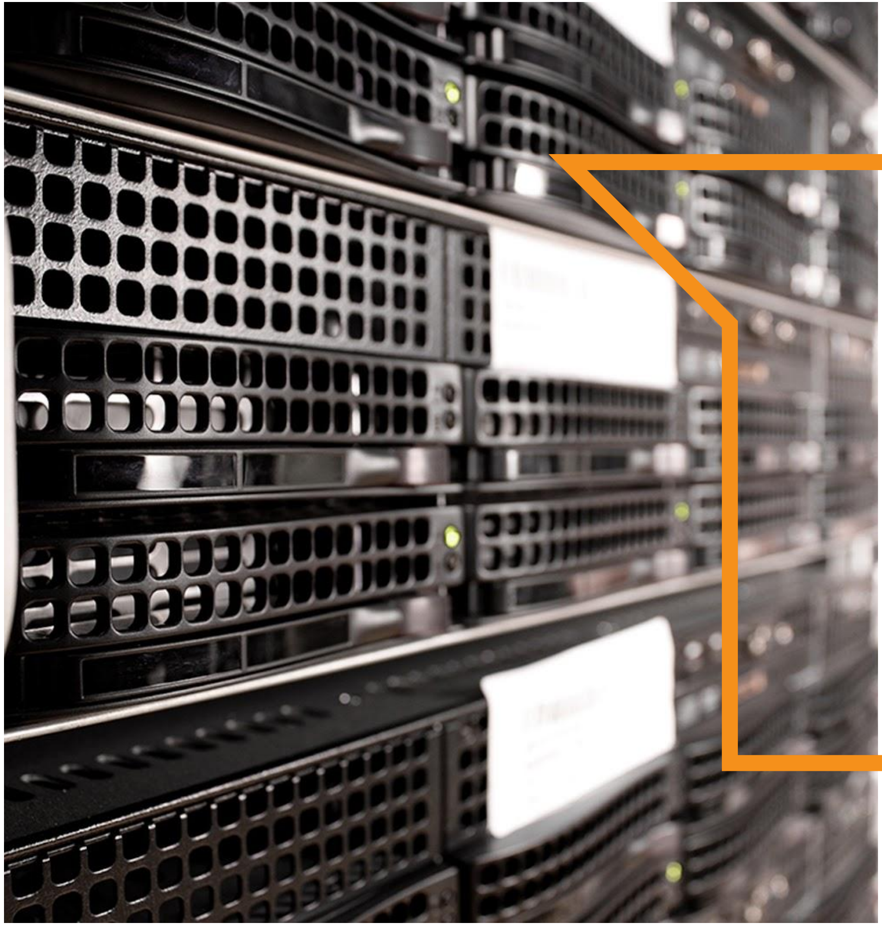
- 70% - never
- 12% - once
- 15% - twice
- 2% - three times
- <1% but not zero - four times

Host Provider Uncertainty



Sensing techniques

- Passive pcap or firewall log-based
- Custom or standard listeners
- Local system handling versus tunneled



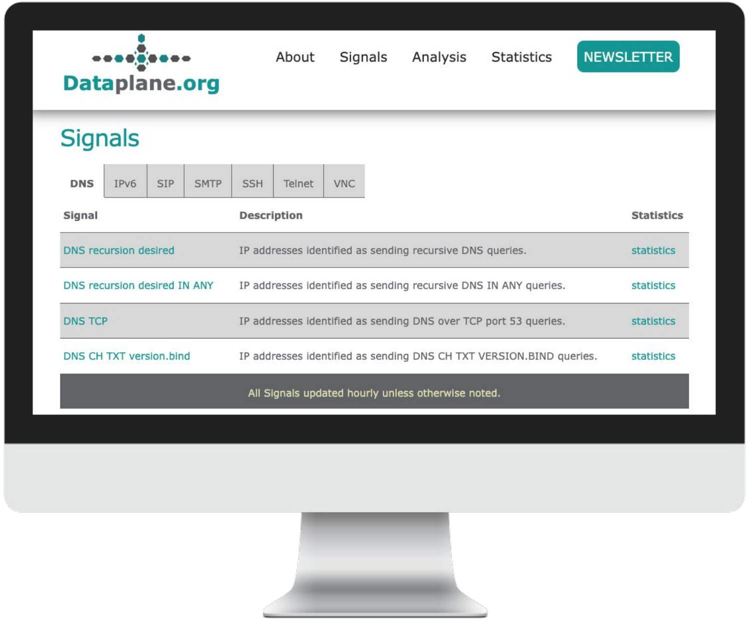
Sensor Management

ANSIBLE

debian

Signals

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



Signals

Signal	Description	Statistics
DNS recursion desired	IP addresses identified as sending recursive DNS queries.	statistics
DNS recursion desired IN ANY	IP addresses identified as sending recursive DNS IN ANY queries.	statistics
DNS TCP	IP addresses identified as sending DNS over TCP port 53 queries.	statistics
DNS CH TXT version.bind	IP addresses identified as sending DNS CH TXT VERSION.BIND queries.	statistics

All Signals updated hourly unless otherwise noted.

Use Cases

SSH Signals

ASN

ASN Name

IP Address

ID/Password

Last Seen - Past 7 days

DNS Signals

ASN

ASN Name

IP Address

Recursion bit set

DNS over TCP (see RFC 9210 / BCP 235)

Last Seen - Past 7 days

RPKI Monitor

Unique IP addresses - RRDP file / rsync

IP version relying party (RP) clients

RP software implementation

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
```

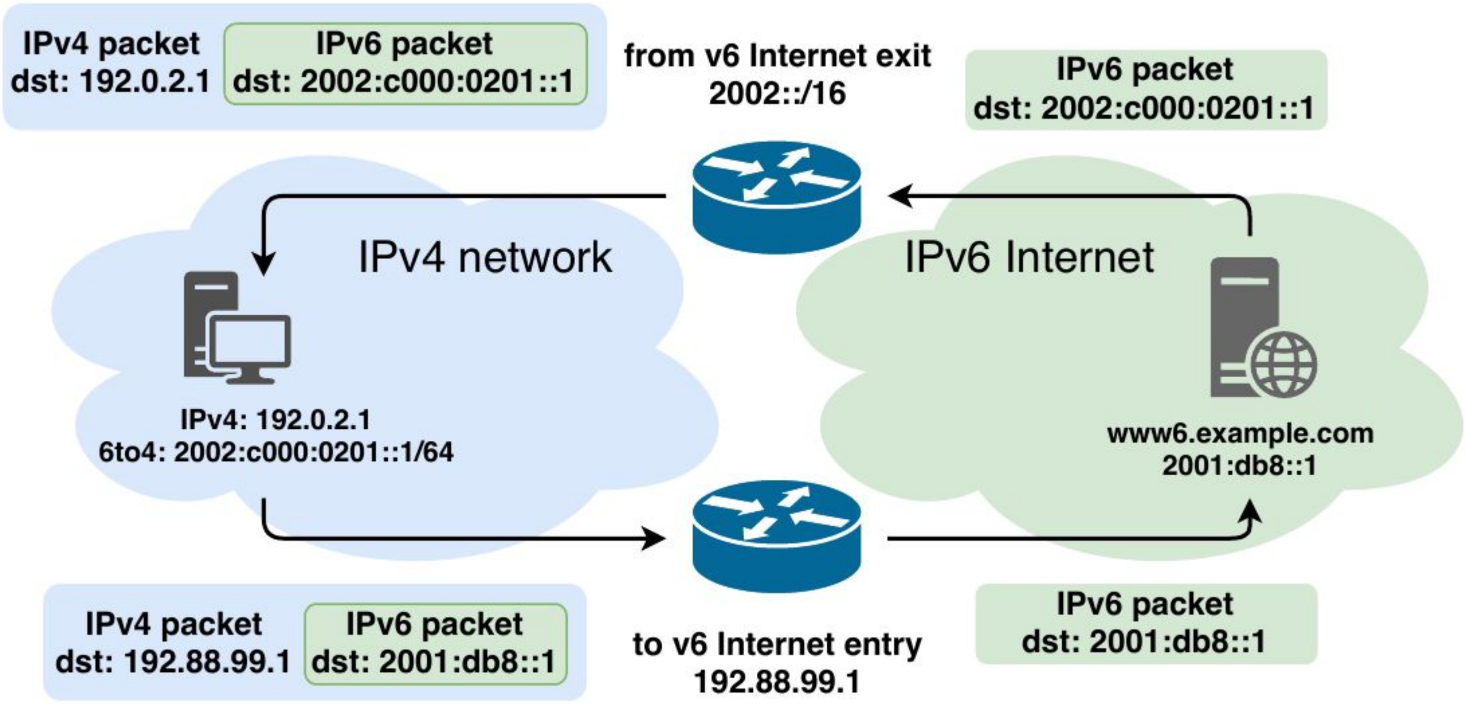
```
SSH Password Authentication
# ASN  |  ASname        |  ipaddr          |  lastseen             |  category
-------------------------------------------------------------------------------
3      |  MIT-GATEWAYS  |  18.18.245.11    |  2022-09-22 10:58:53  |  sshpwauth
1257   |  TELE2         |  83.249.223.18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

```
SSH ID/Password Pairs
# category  |  id     |  password
---------------------------------
sshidpw     |  admin  |  pa$$w0rd15
sshidpw     |  centos |  qwerty1234
```

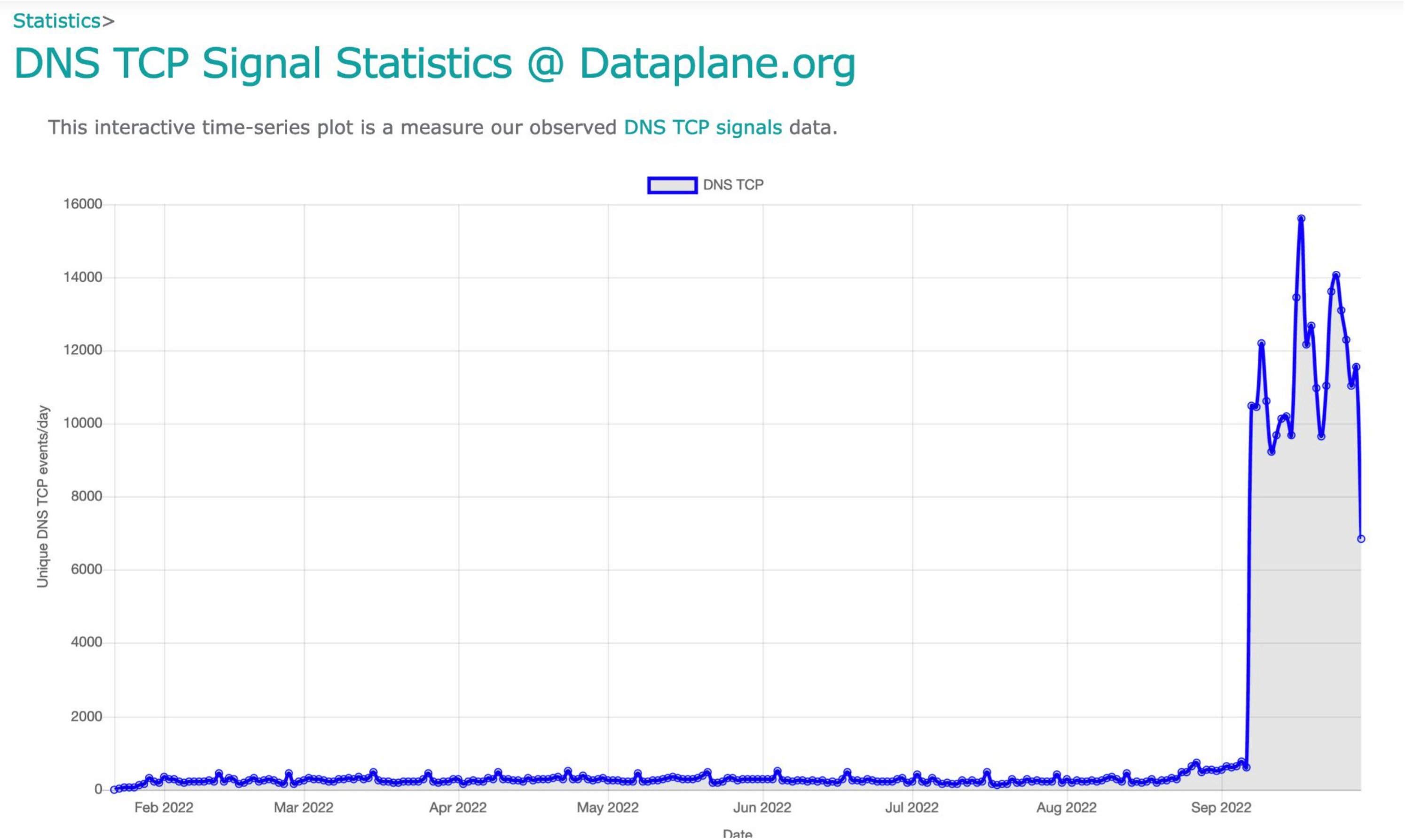
DNS Signal

```
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
```

IP protocol 41 (proto41)



DNS TCP



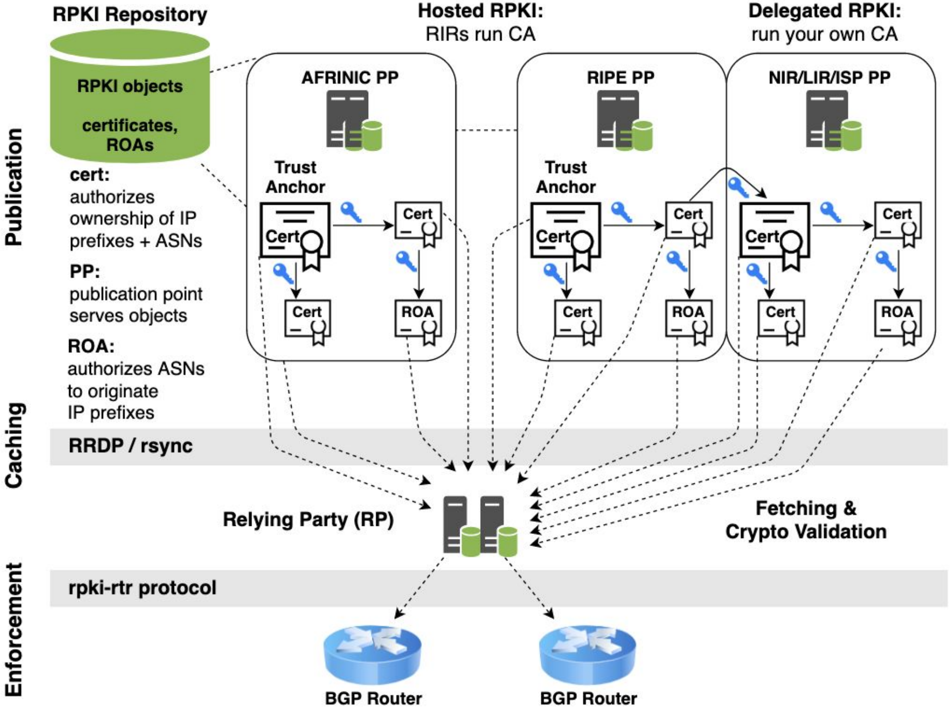
Statistics>

DNS TCP Signal Statistics @ Dataplane.org

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

RPKI Monitor

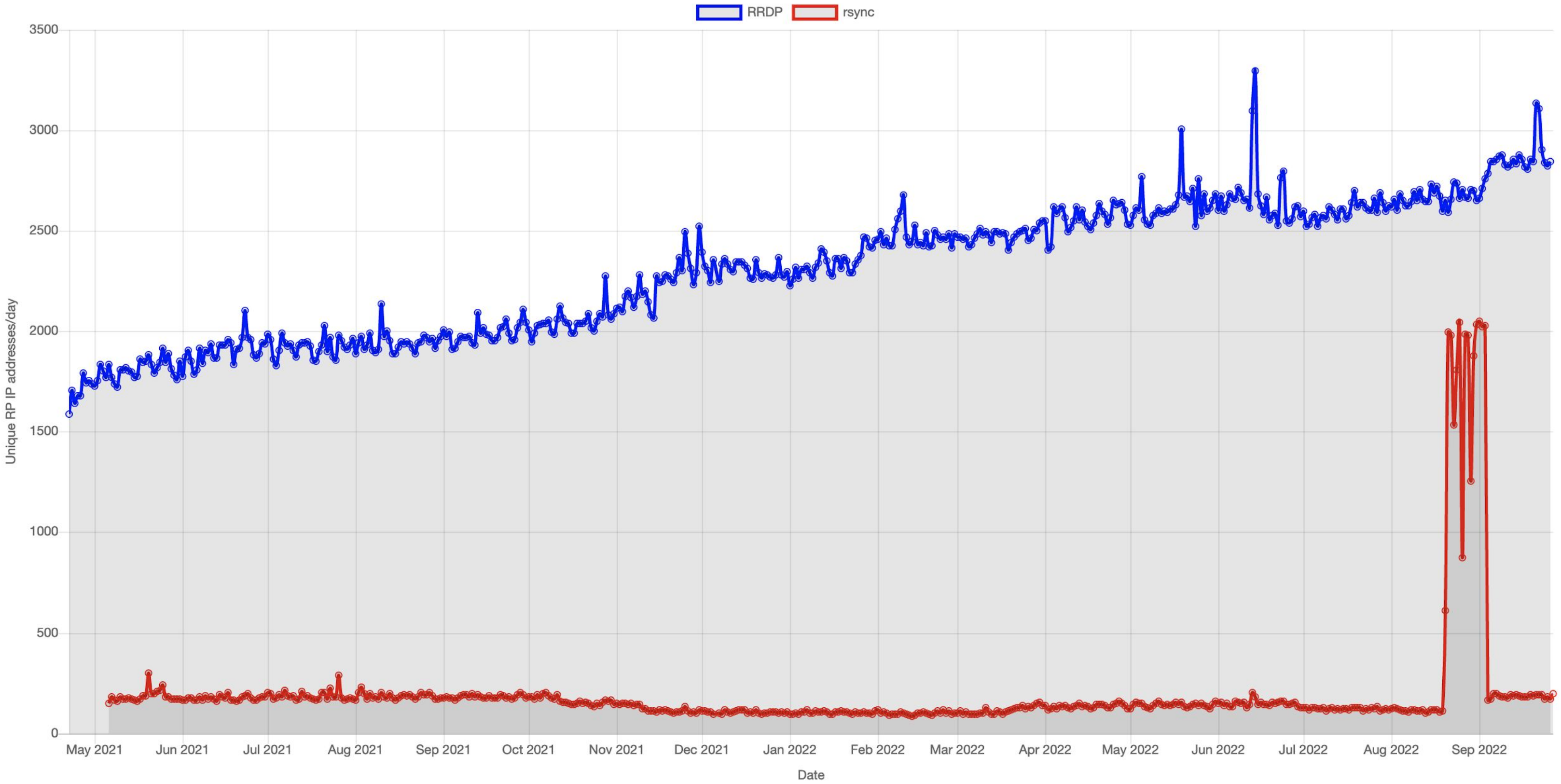
The rpki.dataplane.org system is a publication point (PP) under the ARIN RPKI trust anchor (TA)



On Measuring RPKI Relying Parties. https://dataplane.org/jtk/publications/kbkmp-mrrp-20.pdf

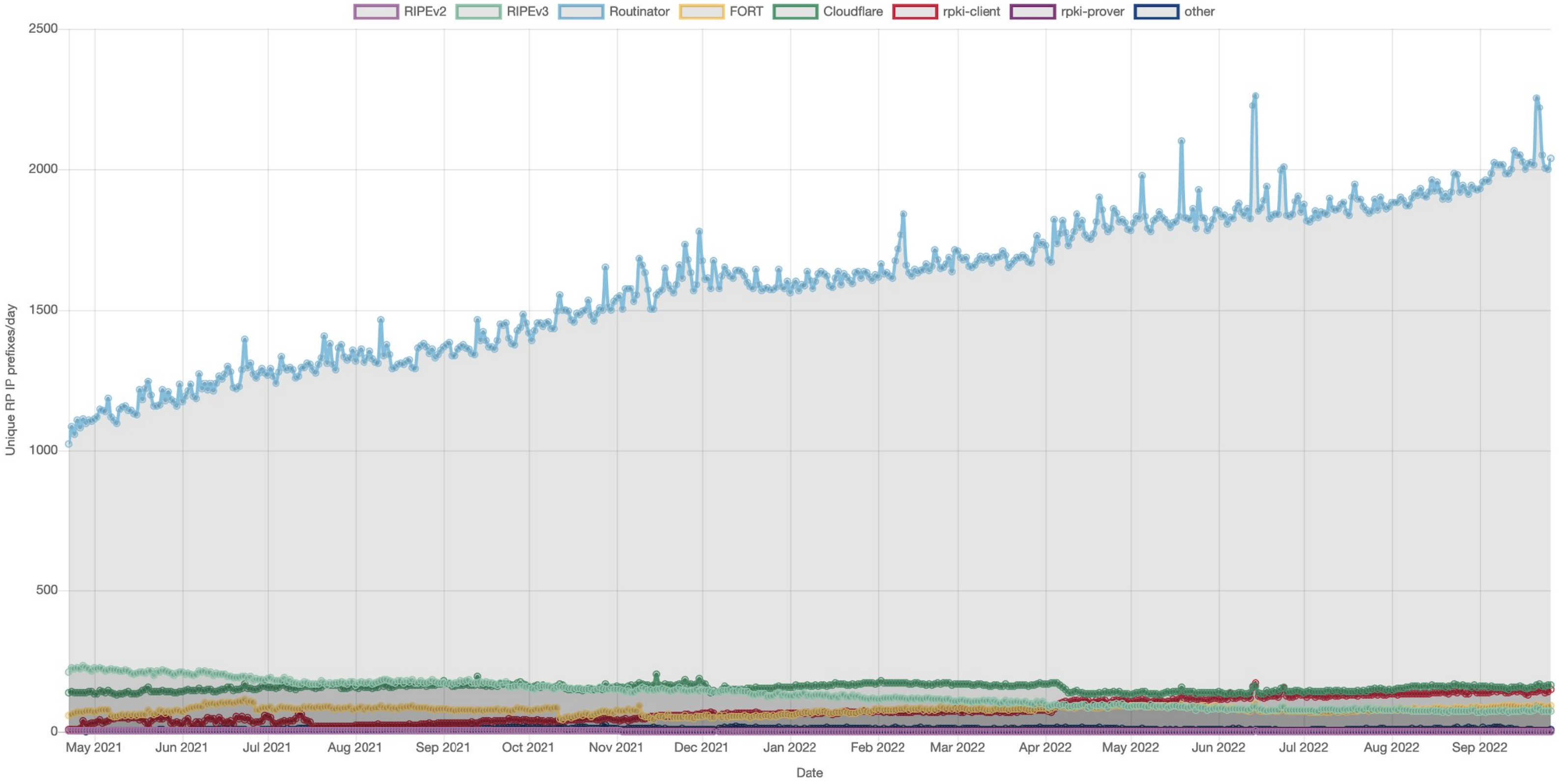
RPKI Monitor

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



RPKI Monitor

RP software implementation by IPv4/24 or IPv6/64 prefix fetching data from _rpki.dataplane.org wit RRDP



Matt

John

Bill

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

Not For Profit Setup

Legal

Incorporation

Employer Identification Number

Charitable Status 501(c)(3)

Financial

Banking

Tax Exempt Status

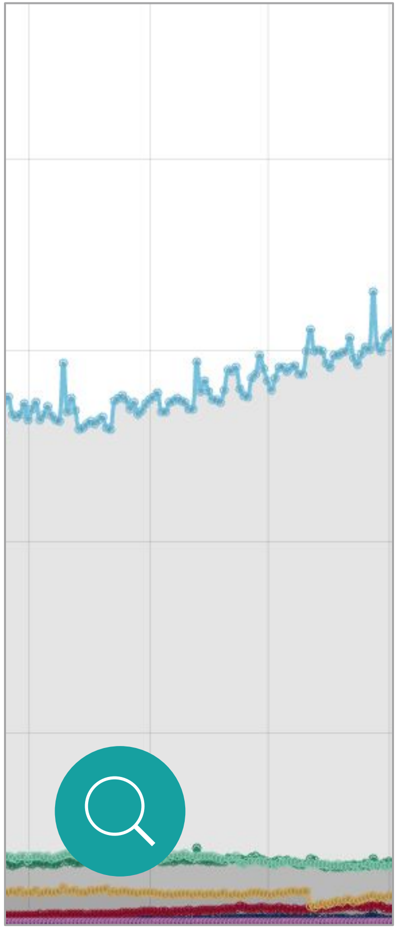
Expenses

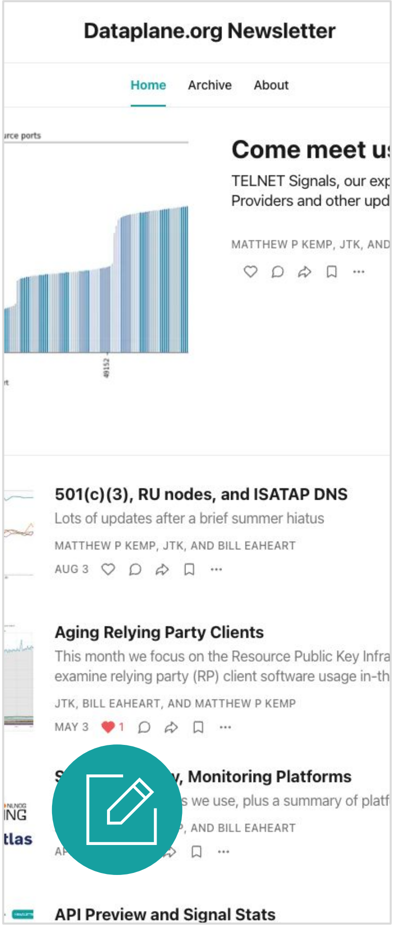
Reporting

Accounting

Tax Preparation

Board Meetings





Dataplane.org Newsletter

Come meet u

TELNET Signals, our exp
Providers and other upd

MATTHEW P KEMP, JTK, AND

501(c)(3), RU nodes, and ISATAP DNS

Lots of updates after a brief summer hiatus

MATTHEW P KEMP, JTK, AND BILL EAHEART

AUG 3

Aging Relying Party Clients

This month we focus on the Resource Public Key Infra
examine relying party (RP) client software usage in-th

JTK, BILL EAHEART, AND MATTHEW P KEMP

MAY 3 1

S , Monitoring Platforms

s we use, plus a summary of platf

, AND BILL EAHEART

API Preview and Signal Stats

api.Dataplane.org

1

allows you to find if an IP address, CIDR notation or
ignal within the past seven (7) days. The feature is
not a substitute for utilizing Signals directly.

te limit as it is a public interface of 10 requests per r

```
equests
```

```
 requests, please try again later."
```

```
lane.org/v1/search/127.0.0.1
```

```
 "127.0.0
: "127.0.
one",
 "None",
022-01-21 1:1
"IP Addresses identified as attempting SSH password auth
["https://dataplane.org/signals/sshpwauth.txt"]
```

- ○ Research
- ○ Newsletter
- ○ Future
  - ○ Listening on all ports
  - ○ Active probing
  - ○ Performance metrics
  - ○ Path analysis
  - ○ Announce our v4 /24
  - ○ DDoS attack signals
  - ○ RDP
  - ○ HTTP

THANK YOU!

https://dataplane.org

fosstodon.org/@dataplane

github.com/dataplane

AS 54278