A Look at New ASNs

John Kristoff

Outline

- Background

- Data

- Analysis

- Discussion

- Future Work

Background

- Border Gateway Protocol (BGP)
- What is an ASN?
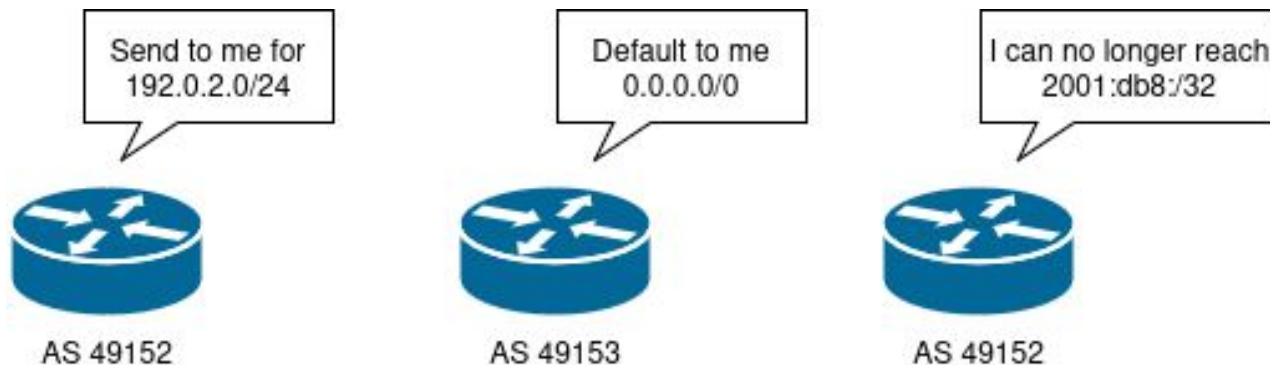- Where do you get an ASN?
- How do you use an ASN?

Before there was BGP...

○ IETF RFC 827 – Exterior Gateway Protocol
Eric C. Rosen, October 1982

"Autonomous systems will be assigned 16-bit identification numbers (in much the same ways as network and protocol numbers are now assigned) [...]"

BGP in a slide

- ○ The exchange of "reachability" information
- ○ Router peers use BGP to communicate
- ○ Each peer is associated with an "AS"

Send to me for
192.0.2.0/24

Default to me
0.0.0.0/0

I can no longer reach
2001:db8:/32

AS 49152

AS 49153

AS 49152

What is an ASN?

- Autonomous System Number

- **A**: Independent, self-managed
- **S**: Hardware, software, protocols
- **N**: Unique identifier

Where do you get an ASN?

- Local Internet Registries (LIRs)
  - e.g., Internet service providers (ISPs)
- Regional Internet Registries (RIRs)
  - AFRINIC, APNIC, ARIN, LACNIC, RIPE
- Internet Assigned Numbers Authority (IANA)

How do you use an ASN? 1/x

```
router bgp 49152
 network 192.0.2.0 mask 255.255.255.0
 neighbor 198.51.100.1 remote-as 49153
 neighbor 198.51.100.1 route-map peer-routes in
 neighbor 198.51.100.1 route-map my-routes out
```

How do you use an ASN? 2/x

```
Neighbor         V       AS    MsgRcvd    MsgSent      TblVer   InQ OutQ Up/Down   State/PfxRcd
4.68.4.46        4     3356    7180841     114377   597286039    0    0  5w1d         973111
12.0.1.63        4     7018    1999185       8811   597286039    0    0  5d13h        973603
37.139.139.17 4     57866   14082611     114807   597286039    0    0  5w1d         976882

[...]

route-views>show ip bgp 8.8.8.8
BGP routing table entry for 8.8.8.0/24, version 590291451
Paths: (17 available, best #5, table default)
  Not advertised to any peer
  Refresh Epoch 1
  7018 15169
    12.0.1.63 from 12.0.1.63 (12.0.1.63)
    Origin IGP, localpref 100, valid, external
    Community: 7018:2500 7018:37232
    path 7F154BD66A10 RPKI State valid
```

Who uses ASNs?

- ○ BGP-speaking routers
- ○ Anyone receiving Internet routes
- ○ Anyone updating Internet routes
- ○ GLOP (IP multicast) block addresses
- ○ Internet surveyors and researchers
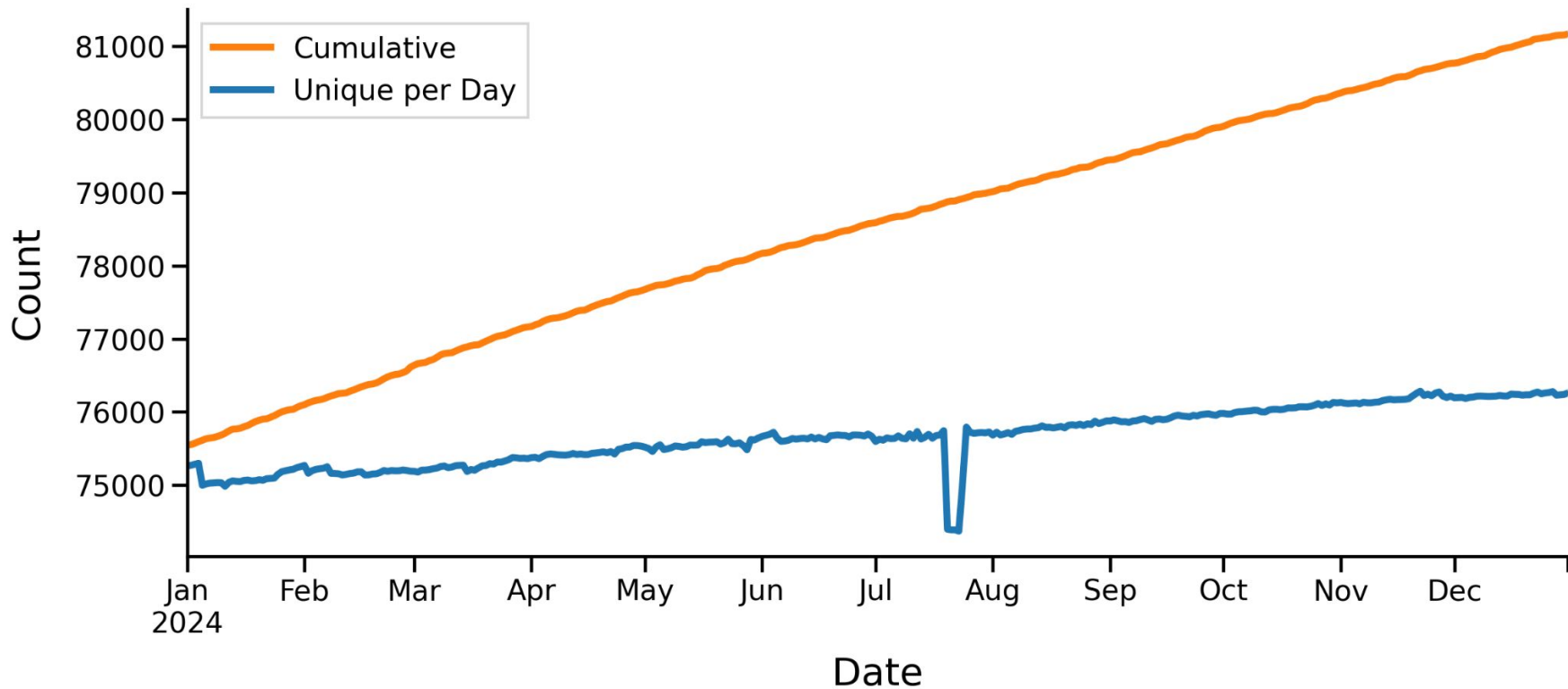- ○ The infosec community

ASN allocation and assignment

- IANA-> [RIRs->] [LIRS->] registrants
- There are private, special, and reserved ASNs
- Costs and assignment policies vary
- Often transferred
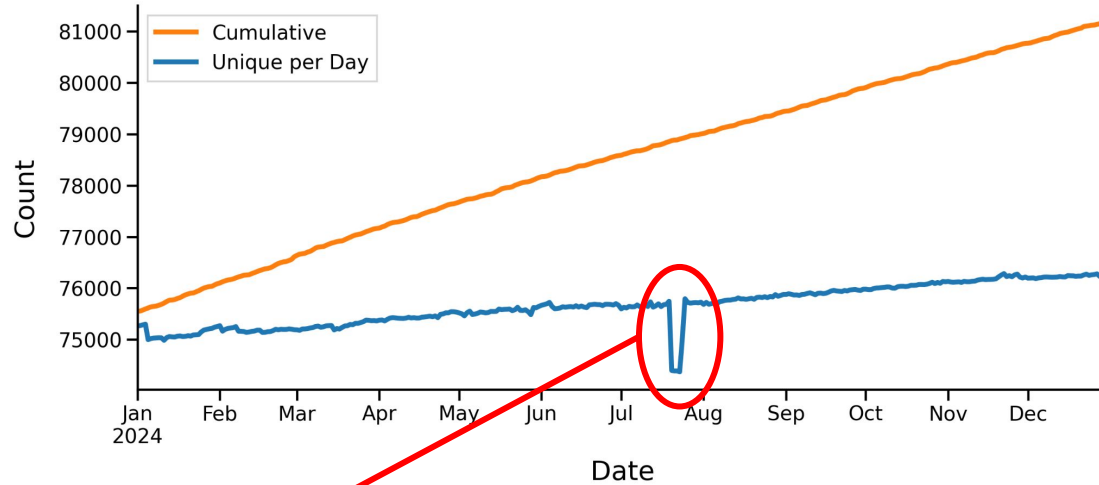- Sometimes revoked or returned
- Relatively easy and cheap to get

Data sources

- ○ Routing history (RIPE RIS / RouteViews)
- ○ RIR databases
- ○ DDoS mitigation provider alerts
- ○ Dataplane.org sensor data
- ○ Spamhaus ASN drop list

Unless otherwise stated, 2024 data assumed
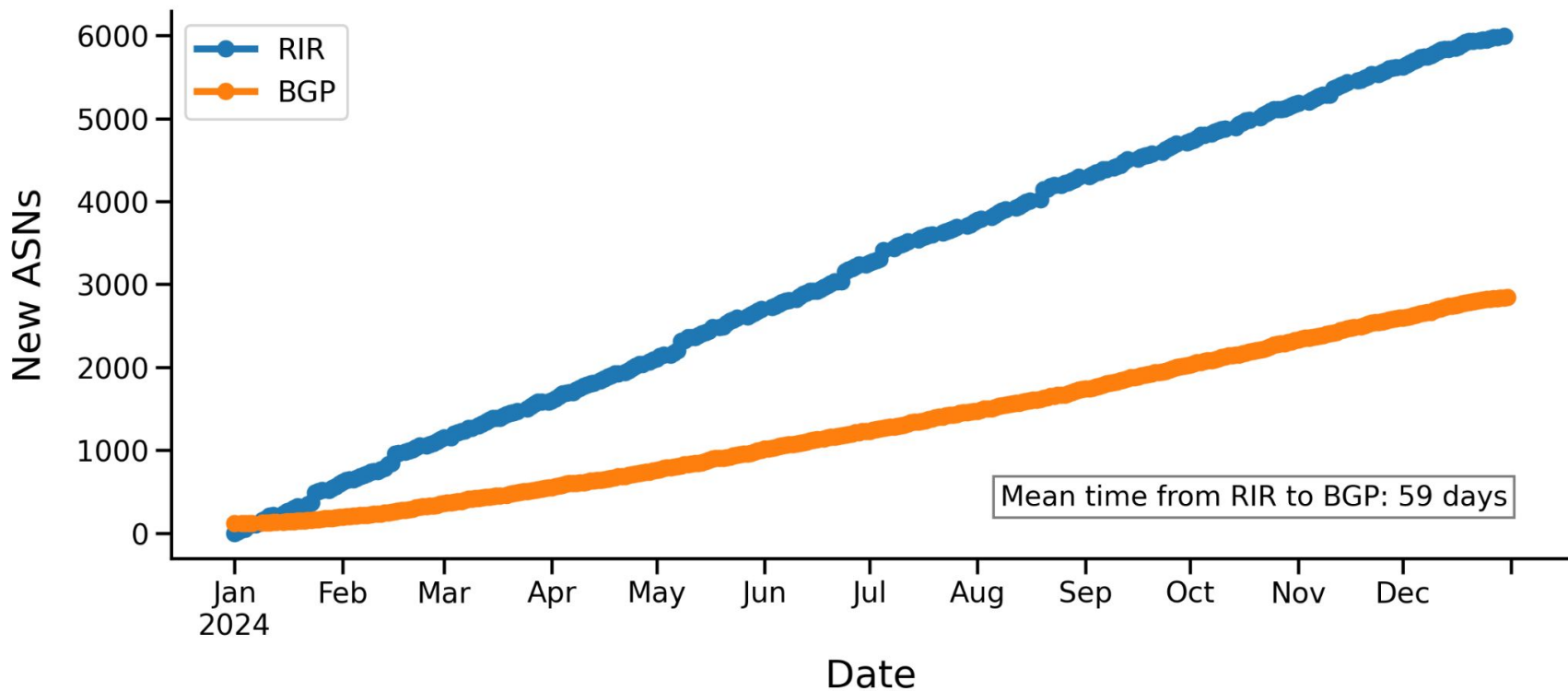
Origin ASNs in BGP

An aside….

Internet shutdown

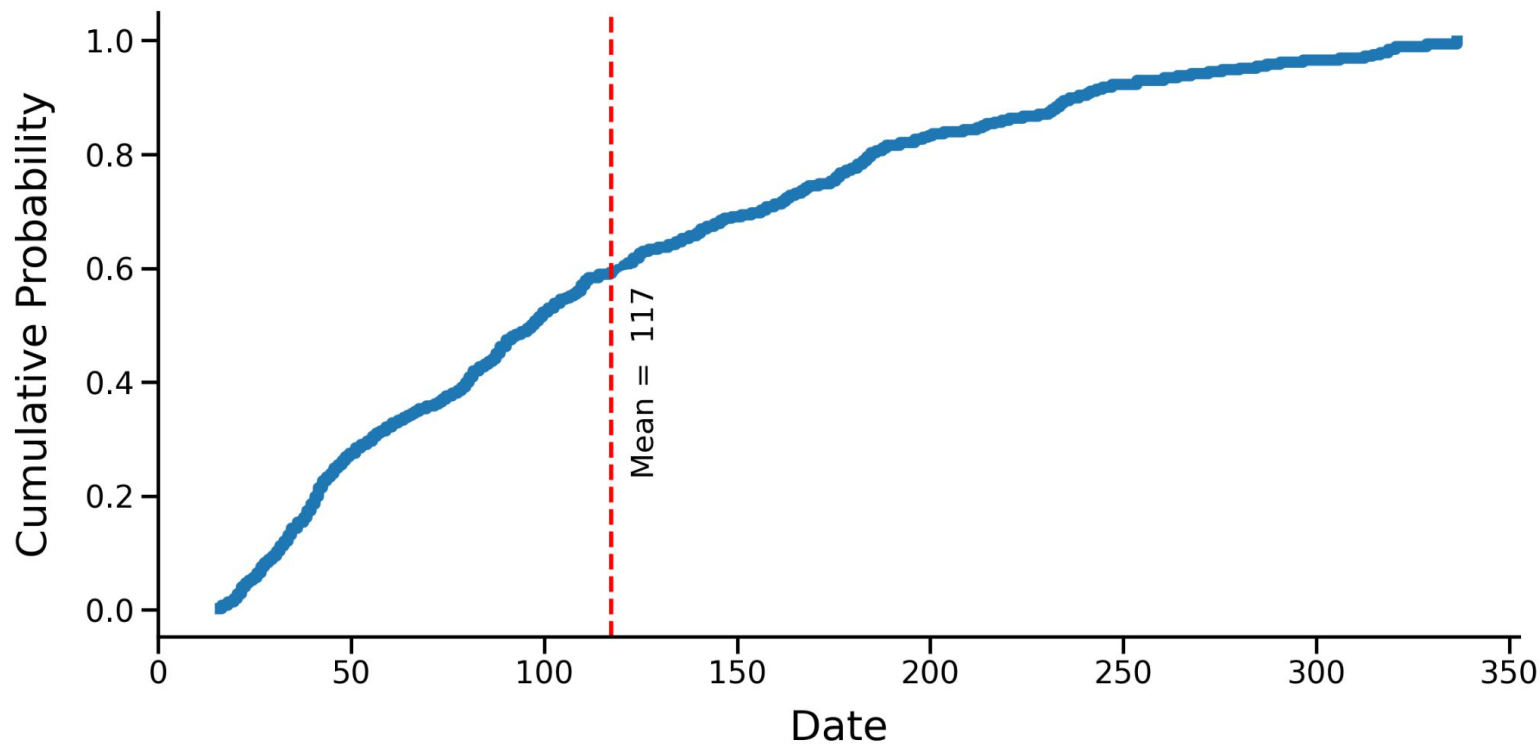https://pulse.internetsociety.org/en/shutdowns/mobile-internet-shut-down-in-bangladesh-amidst-protests/

Assignments vs. announcements

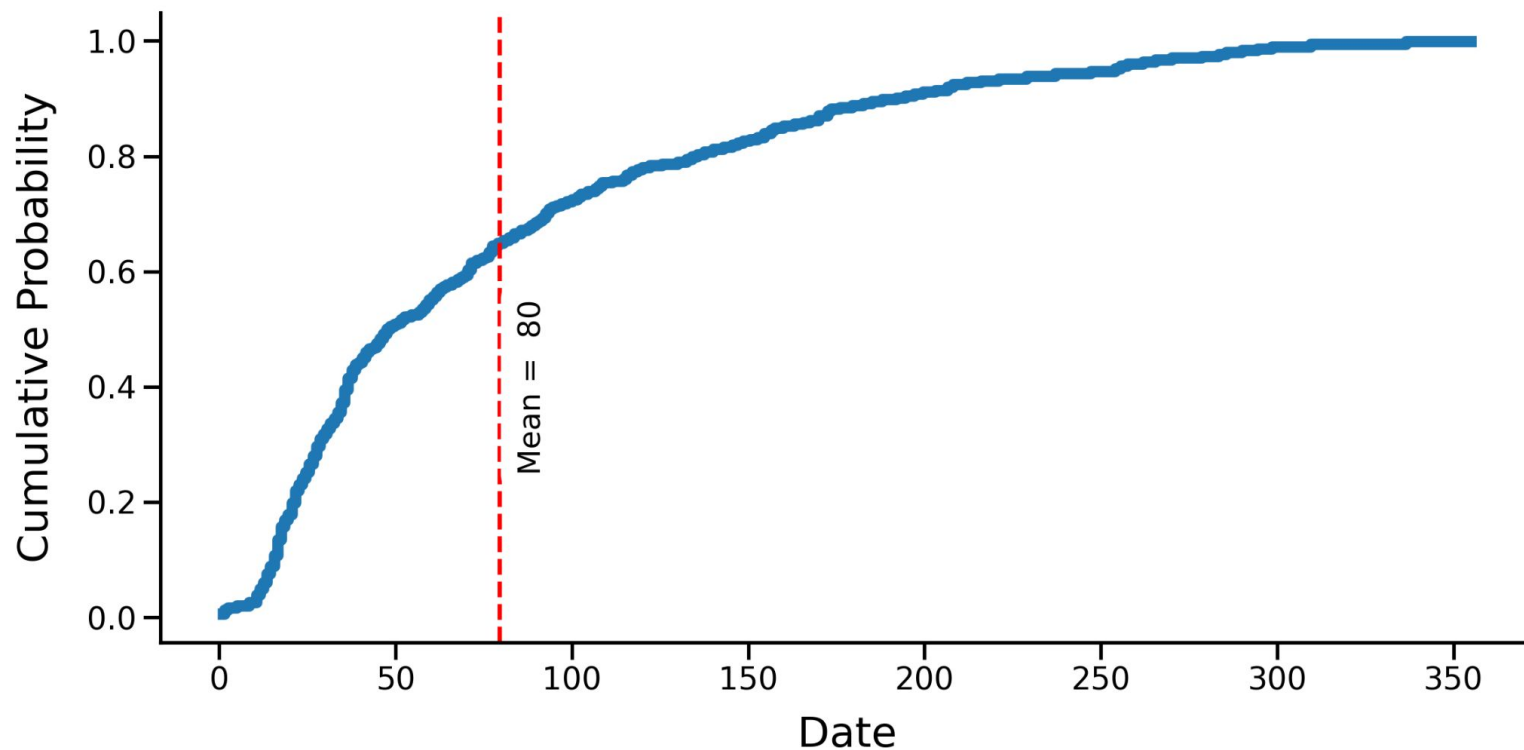

Mean time from RIR to BGP: 59 days

New ASNs and DDoS attacks

Time from assignment to attack

Time from announcement to attack

DDoS mitigation provider observations

- ~300 (10% routed) new ASNs targeted by DDoS
  - Probably the floor
- ~750 (25% routed) new ASNs source DDoS
  - May include sympathetic, some spoofing

New ASNs and sensor networks

# Dataplane.org sensor observations 1/x

○ From prefixes associated with new ASNS

    ○ ~15 million SSH brute force attempts

○ HOWEVER...

    ○ At the time of an event...

    ○ the covering prefix...

    ○ was originated by a different ASN...

    ○ ~33% of the time!

Dataplane.org sensor observations 2/x

- New ASNs often get "dirty" addresses
  - Lots of anecdotal evidence
  - i.e., leased address block effects
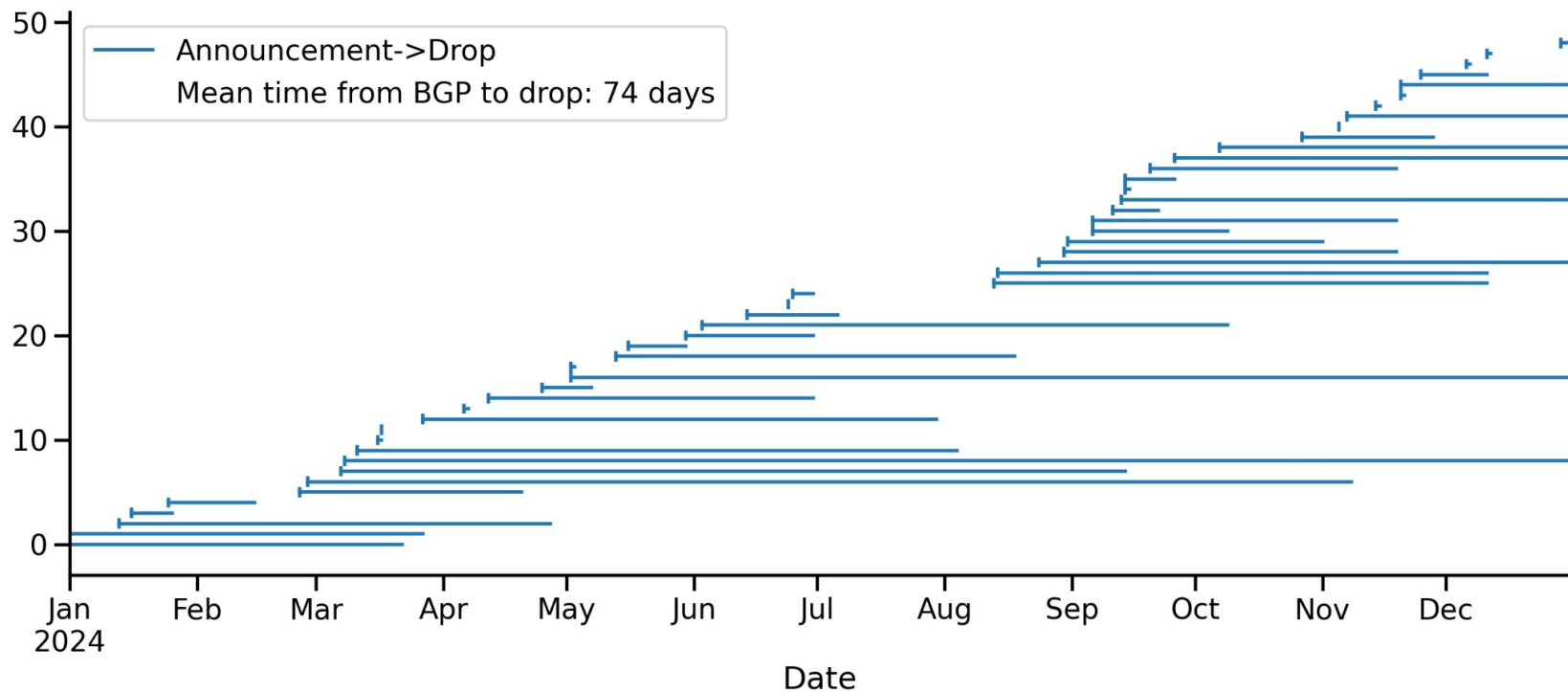- Address-to-ASN mapping time matters

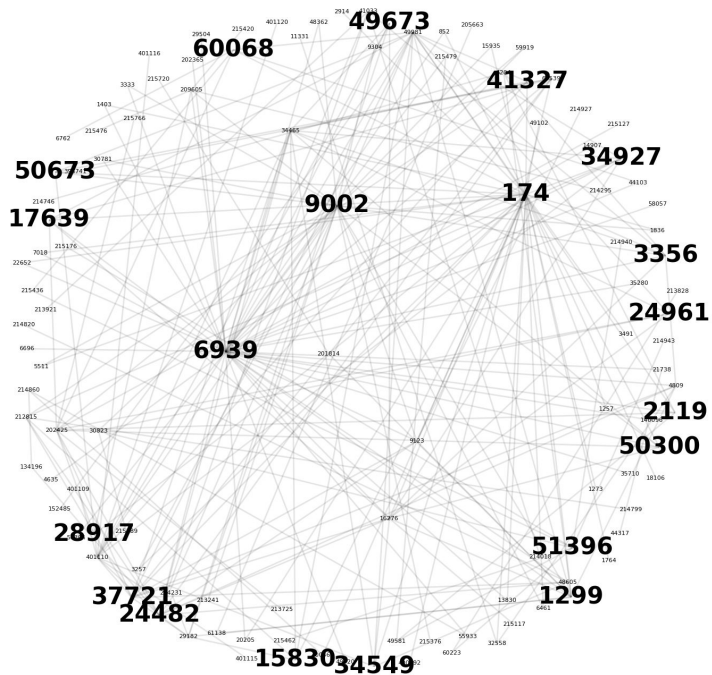# New ASNs and block lists

Assignment to ASN drop latency
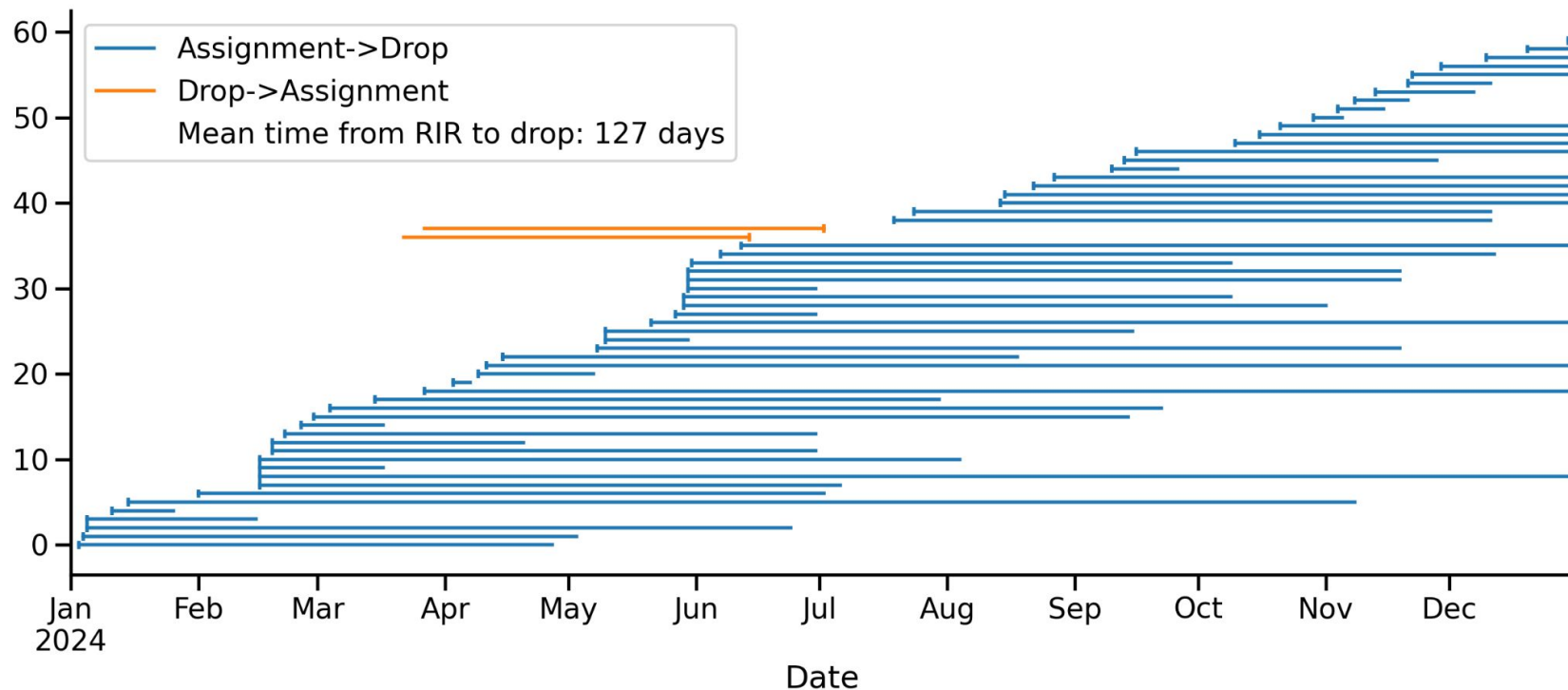
Announcement to ASN drop latency

ASN drop observations

- ○ 60 new ASNs in drop list
- ○ Drop latency varies widely
- ○ Is Spamhaus prescient?
  - ○ Internet resource volatility applies to ASNs too

New ASN Drop Connectivity

Discussion

- New ASNs actionable insight?
- New ASNs policy ideas?
- Additional research directions...

New ASN-related Resources

- https://www.nro.net/about/rirs/statistics/
- RIPE RIS
- RouteViews
- PeeringDB
- bgp.he.net / bgp.tools
- BGP Kit
- www.domaintools.com/resources/blog/finding-new-asns/

Thank you

John Kristoff

✉ **jtk@dataplane.org**

🌐 **https://dataplane.org/jtk/**

https://infosec.exchange/@jtk