

7 April 2025

Routing Security

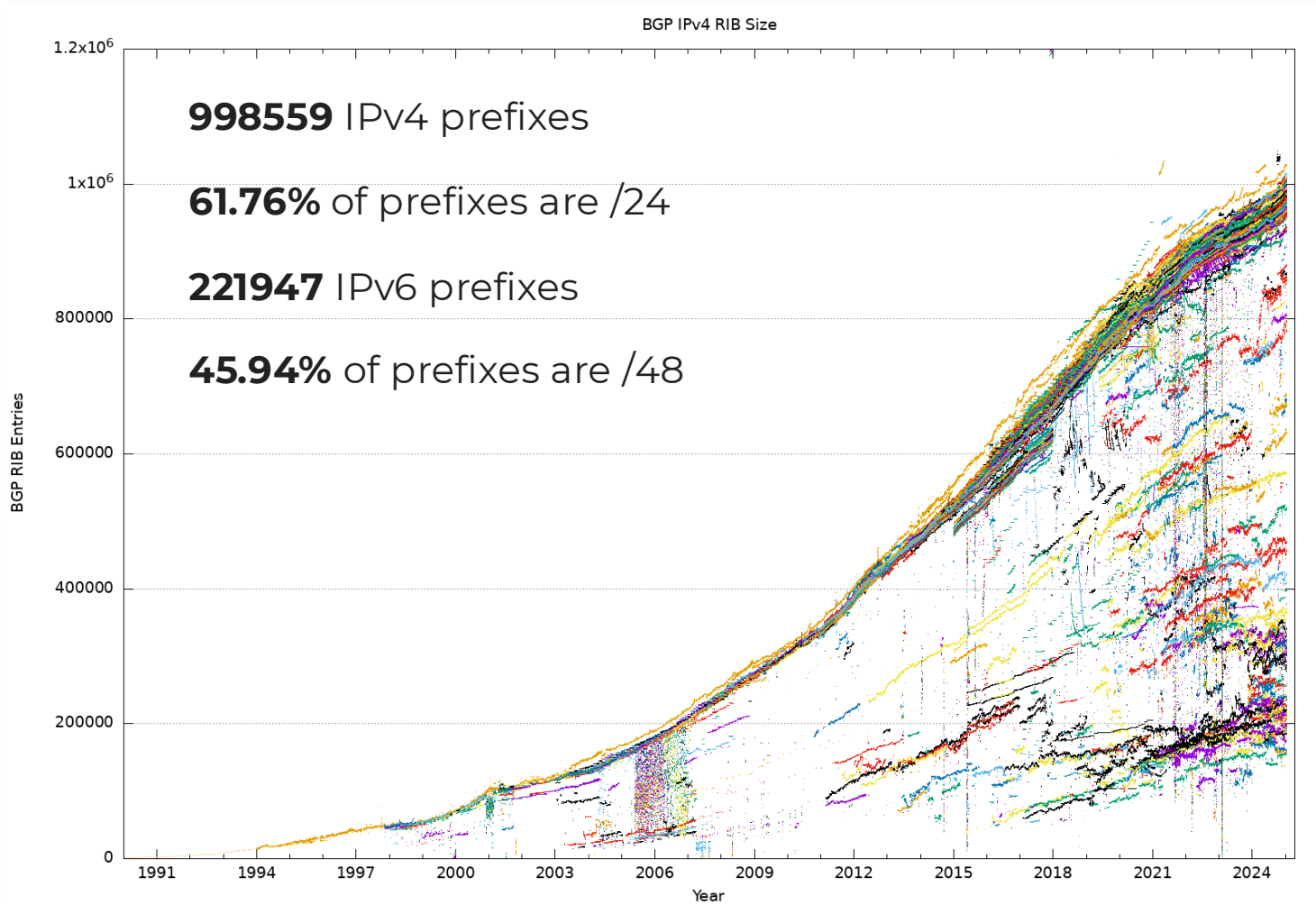
Threats, countermeasures, and data analysis

Flavio Luciani / Namex CTO

The Internet

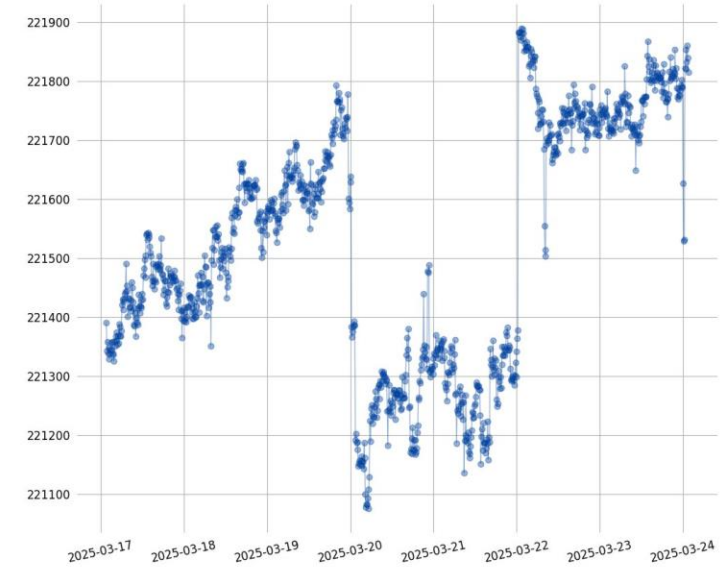
- An Autonomous System (AS) is a collection of IP networks and routers under the control of a single organization that presents a common routing policy to the internet
- As of today, **118,226** ASs have been assigned globally. Of these, **83,467** are active and advertised in the Internet routing system
- Each AS makes its own decisions about how to move Internet traffic using a language called **Border Gateway Protocol (BGP)**
- BGP is a fundamental underpinning of the Internet. It is the routing protocol used to exchange routing information between AS on the Internet

The Internet



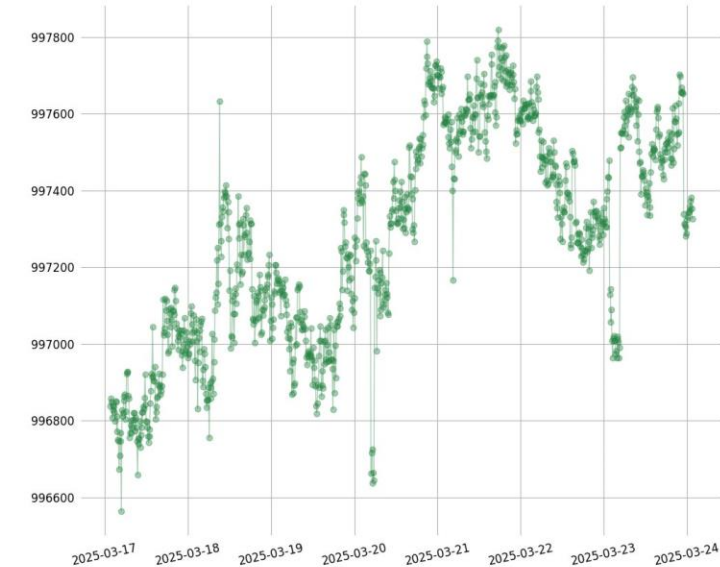
IPv6 table movement for week ending 23-Mar-2025

data by @mellowdrifter | www.mellowd.dev



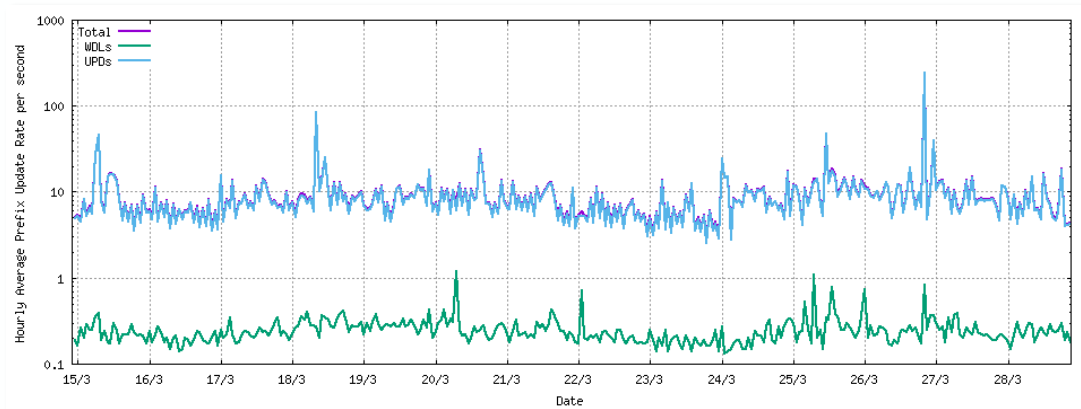
IPv4 table movement for week ending 23-Mar-2025

data by @mellowdrifter | www.mellowd.dev



The problem with BGP

- BGP was created in 1989, before Internet security was a concern
- BGP assumes all networks are trustworthy. Any network can announce it has a path to any other network, even if it does not
- There is no built-in security mechanism to check if traffic is legitimate or not
- BGP is vulnerable to both malicious attacks and human mistakes



Number of BGP Update Messages	25.731.926
Number of Prefix Updates	11.396.246
Number of Prefix Withdrawals	30.1688

14 Day BGP Profile: 15-March-2025 00:00 - 28-March-2025 23:59 (UTC+1000)

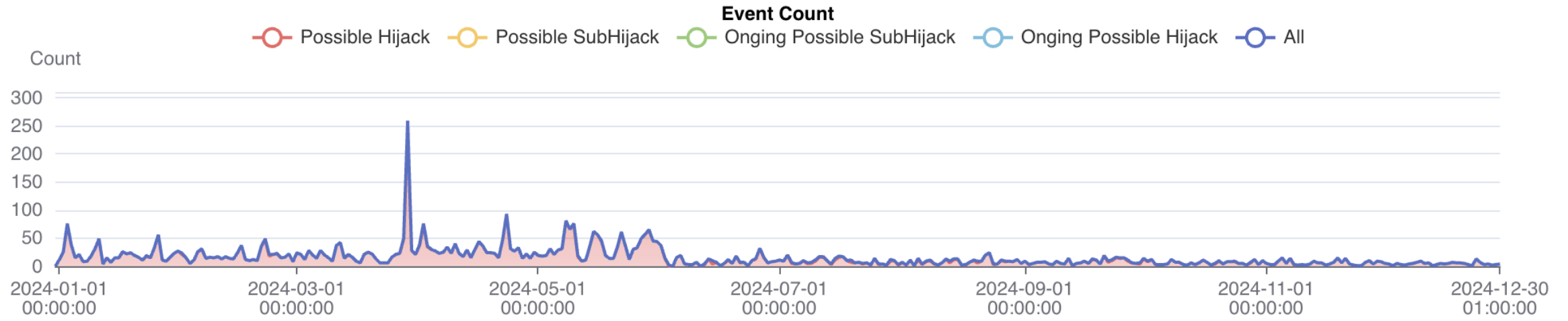
Hourly Average of Per-Second Updated and Withdrawn Prefix Rate

Impact of a BGP incident

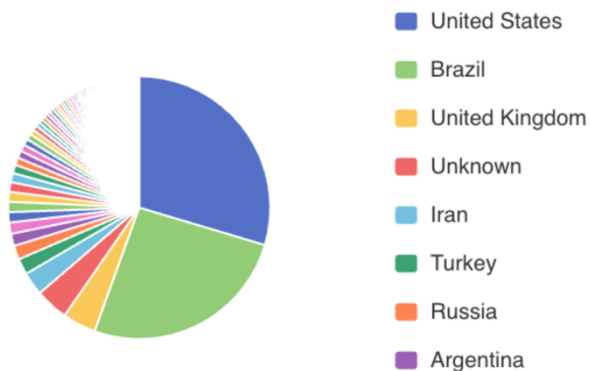
- Disrupt the flow of legitimate internet traffic
- Nation state control on flow of information
- Misdirection of communications
- Security risk from interception or manipulation
- Attacks on cryptocurrency services
- BGP session flaps: affect the stability of the global routing table

BGP incidents

Source: <https://bgpwatch.cgtf.net/#/>



Victim Economy/Region



Level:

4179

Low

1429

Middle

165

High

Impact Range:

1443

<10%

2064

>=10%

2228

>=50%

Data Plane Detection:

4740

Not Done

378

No Result

233

Not Hijack

285

Low Possible

138

High Possible

Status:

5774

Finish

Event Type:

101

SubHijack

5673

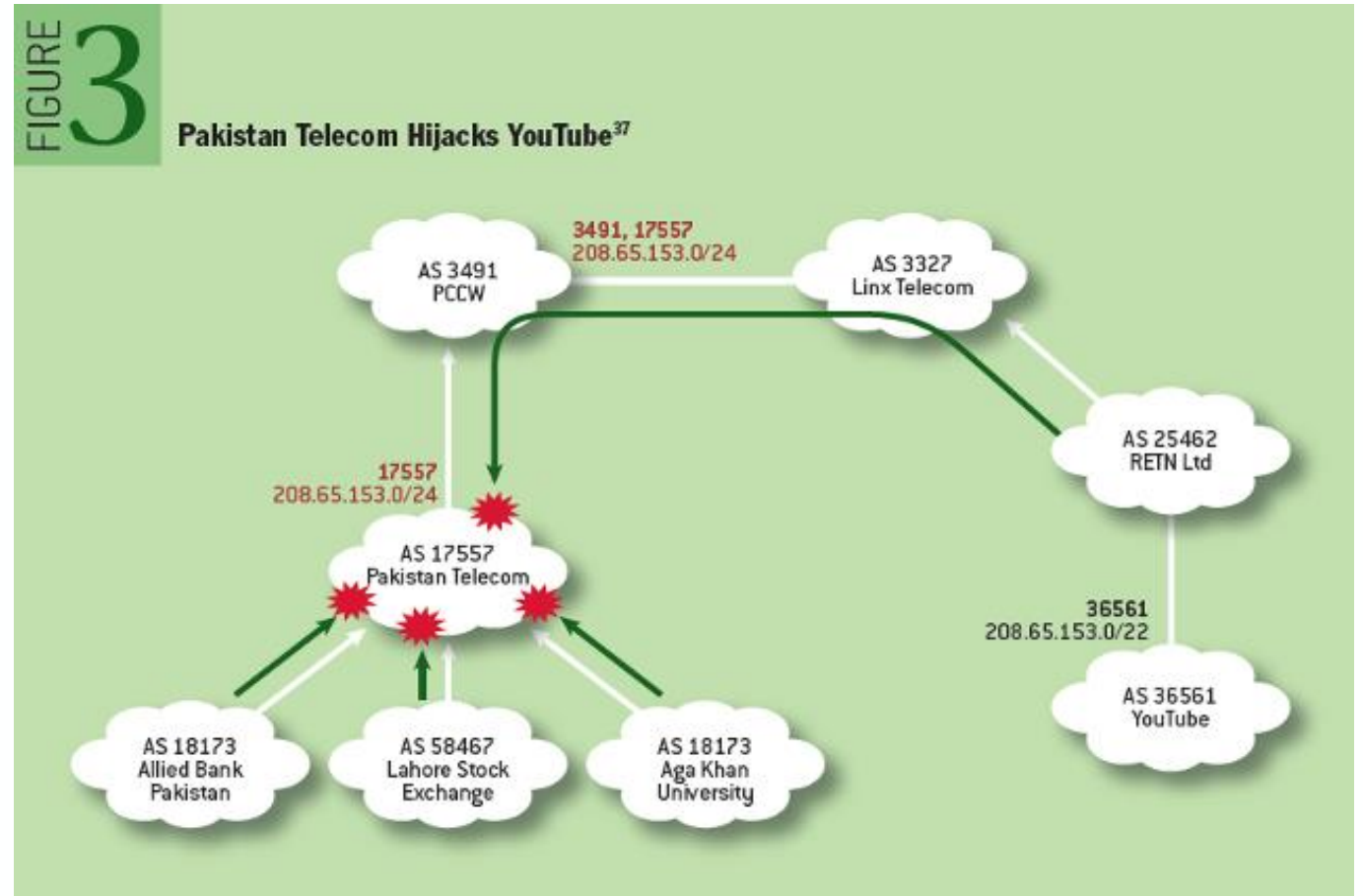
Hijack

BGP incidents definitions

- BGP Hijacks: a network or attacker impersonates another network, pretending that a server or network is their client
- BGP leaks: a network or attacker advertises illegitimate IP prefixes, which propagate across networks and lead to incorrect or suboptimal routing
- AS PATH errors: occurs when an AS inserts itself as an illegitimate intermediary into the forwarding path of traffic bound for a different destination
- IP squatting: occurs when an AS announces IP address ranges that are normally unrouted on the global Internet

Pakistan Telecom Hijack of YouTube (2008)

- Government of Pakistan ordered access to YouTube to be blocked in the country due to a video it deemed antislamic
- Pakistan Telecom intended to blackhole traffic inside their network
- Leaked it to their upstream providers

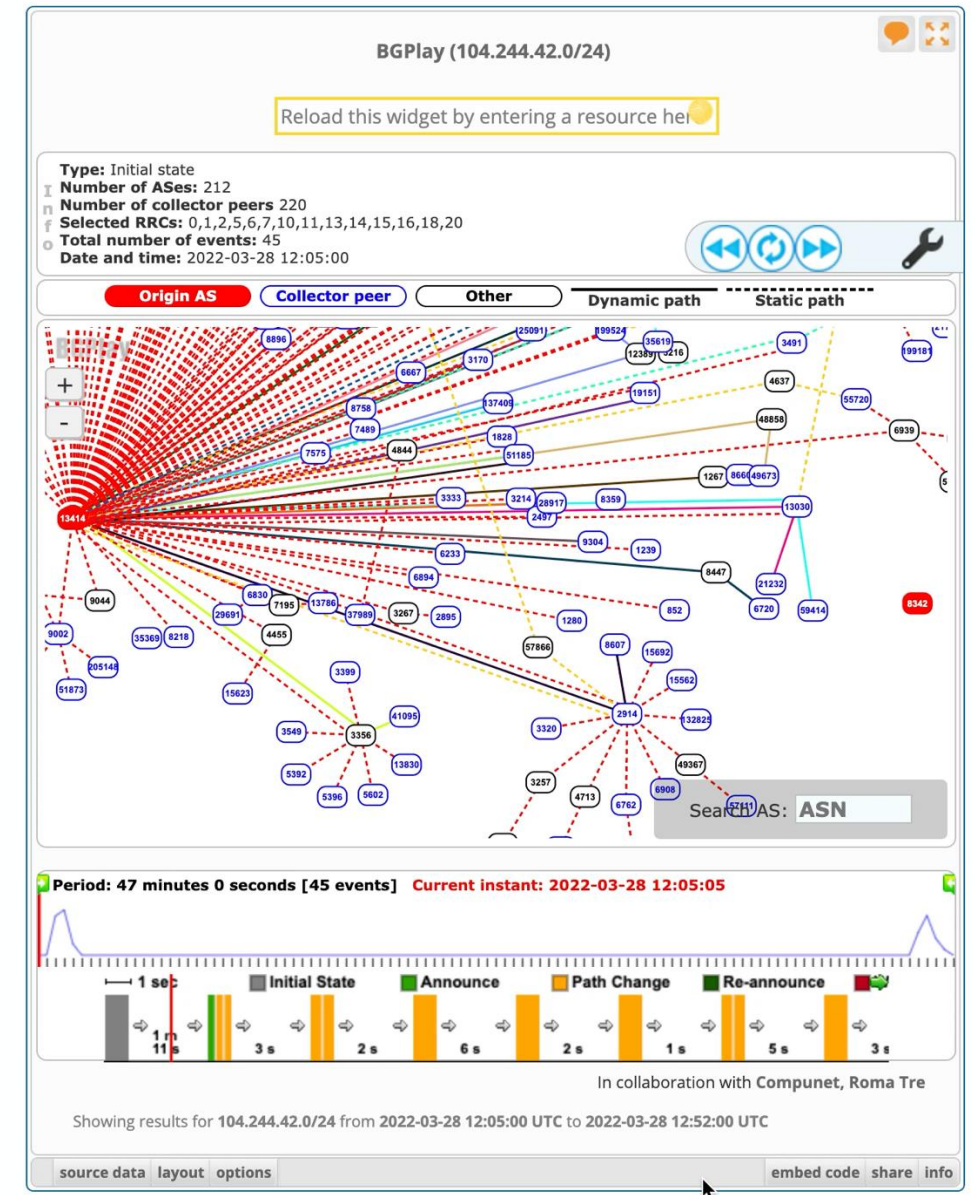


Img source: <https://dl.acm.org/doi/fullHtml/10.1145/2668152.2668966>

Russian Hijack of Twitter (2022)

- Twitter prefix (104.244.42.0/24) announced by Russian Telecom RTComm during the Russian invasion of the Ukraine
- Same prefix was hijacked during the military coup in Myanmar in 2021
- Less propagation this time due to RPKI ROA

at > ogplay



Other BGP incidents

- **April 2017: Rostelecom** (AS12389) hijacked 37 prefixes, including those of **MasterCard** and **Visa**, for about 7 minutes.
- **December 2017: DV-LINK-AS** (AS39523) announced 80 high-traffic prefixes, including those of **Google**, **Apple**, **Facebook**, and others.
- **April 2018: eNet** (ISP in Columbus, Ohio) hijacked about 1,300 IP addresses from **Amazon Route 53**, affecting several peering partners.
- **July 2018: Iran Telecommunication Company** (AS58224) hijacked 10 prefixes of **Telegram Messenger**.
- **November 2018: China Telecom** originated Google addresses in the US.
- **May 2019:** Traffic to a public DNS run by **TWNIC** was rerouted to Brazil (AS268869).
- **June 2019: China Telecom** rerouted European mobile traffic after **SafeHost** (AS21217) leaked over 40,000 routes.
- **February 2021: Cablevision Mexico** (AS28548) leaked 282 prefixes, causing conflicts across 80 countries.
- **April 2021: Vodafone Idea Ltd** (AS55410) hijacked over 30,000 prefixes, causing a spike in inbound traffic.
- **February 2022:** Attackers hijacked BGP prefixes from a South Korean cryptocurrency platform and stole \$1.9 million in cryptocurrency.

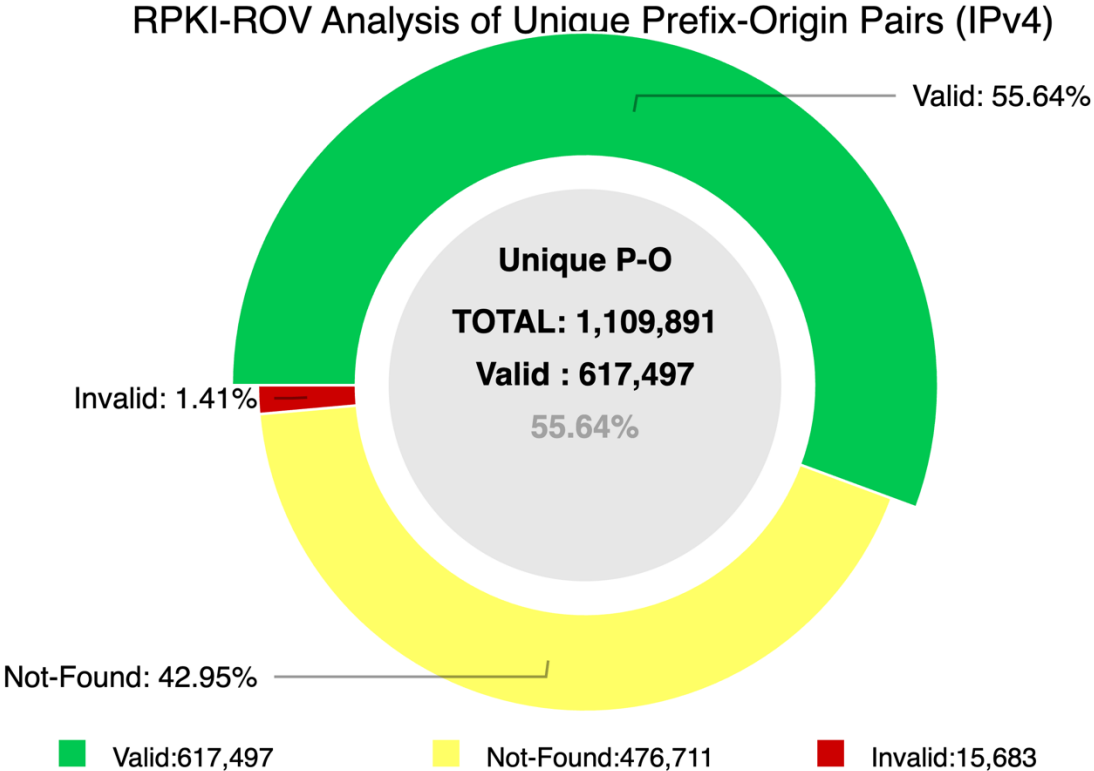
What can operators do

- Watch BGP monitoring solutions to respond quickly
- RPKI ROV by creating ROAs for your prefixes
- Configure your routers to reject RPKI Invalid routes
- Mutually Agreed Norms for Routing Security (MANRS)
- Join IXPs and improve adjacencies with other ASes, using Route Server infrastructures

Internet eXchange Points help

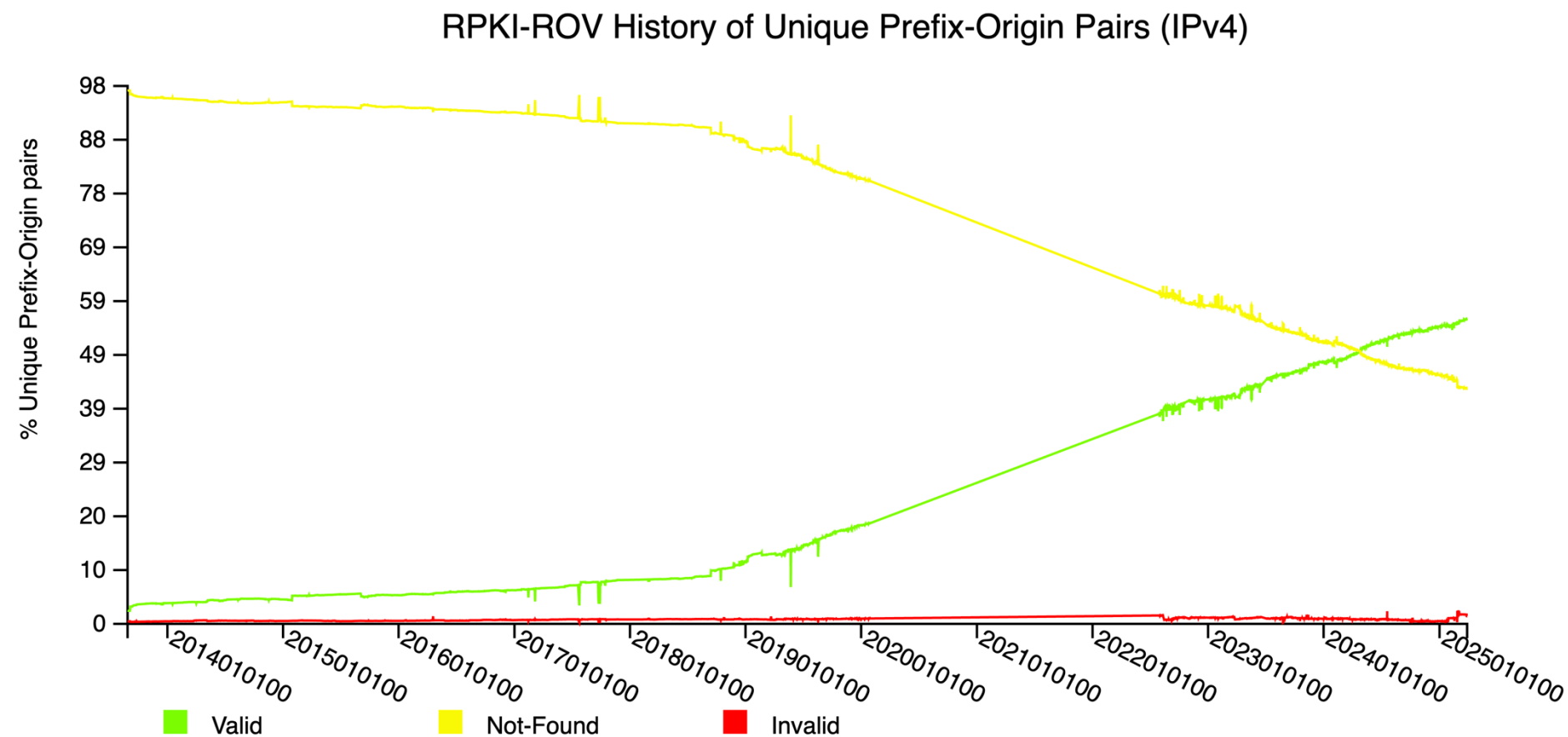
- Route Servers help IXPs peer with major content providers when traffic is too low for direct sessions
- Route Servers have grown in popularity, adding new security features over time
- They filter routes from peers, ensuring reliability and blocking hijacks, bogons, and default routes
- Route Servers apply security policies by validating BGP announcements using IRR and RPKI
- They export only verified prefixes, ensuring a clean and secure routing environment

We are making progress



NIST RPKI Monitor: RPKI-ROV Analysis **Protocol:** IPv4 **RIR:** All **Date:** 2025-03-29 06:00
URL: <https://rpki-monitor.antd.nist.gov/ROV#div1>

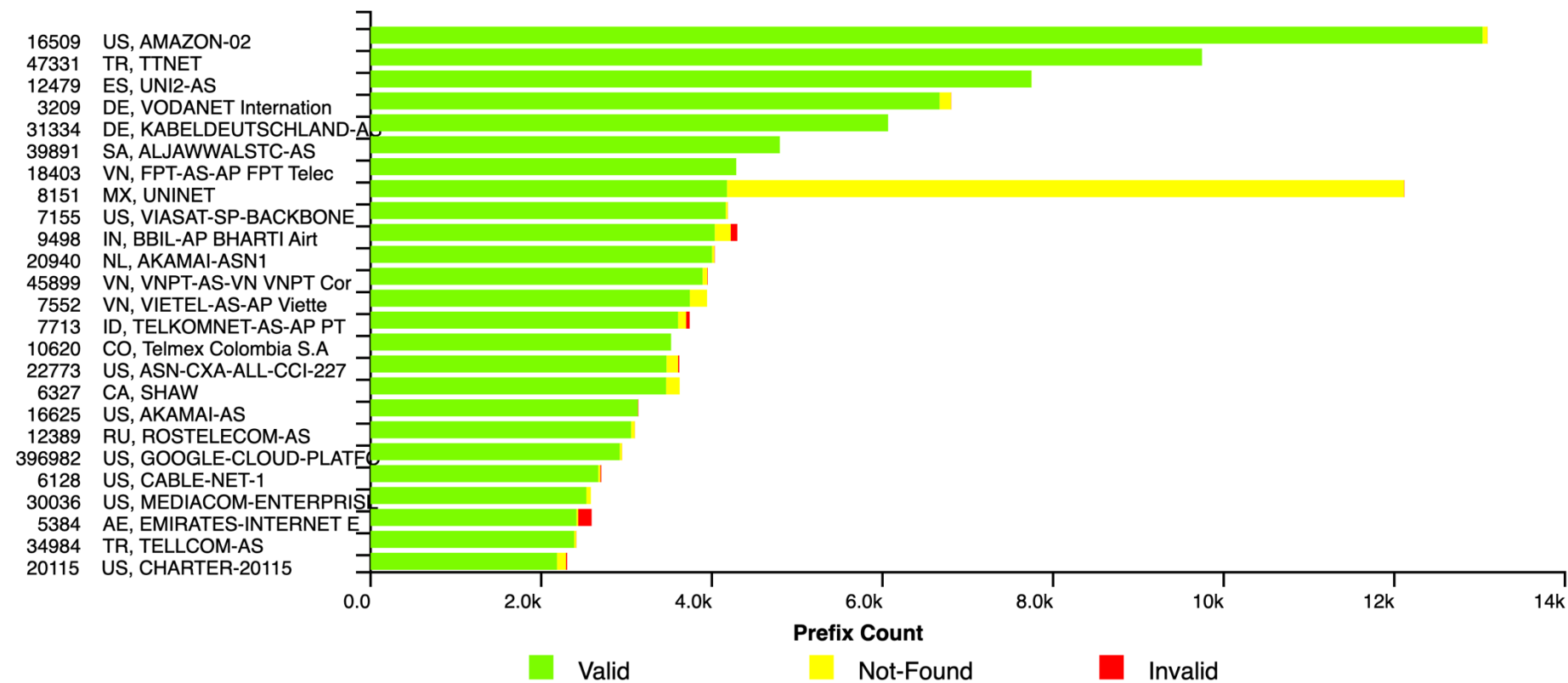
We are making progress



We are making progress

25 Autonomous Systems with the most BGP observed Prefixes VALID by RPKI-ROV (IPv4)

URL: <https://rpki-monitor.antd.nist.gov/ROV#div25>



7 April 2025

THANKS!

Flavio Luciani / Namex CTO