



RIPE NCC

RIPE NETWORK COORDINATION CENTRE

RPKI

Do we really need it?
(Yes, we do)

Alex Semenyaka | 2022.11.16 | CAPIF-1, Almaty

Some history



- Created in 1989 (RFC 1105)
- Current BGP version (BGPv4) was released in 1994
- BGP was never created with the security in mind
 - The first major incident (AS 7007 incident): April 25, 1997

No built-in security in BGP!



- Any AS can announce any prefix
- Anyone can prepend any ASN to the BGP path
- BGP announcements are accepted without validation
- BGP packets are transmitted without any encryption or authentication mechanisms
- No single authoritative source for who should be doing what

(From RPKI RIPE Training Course)

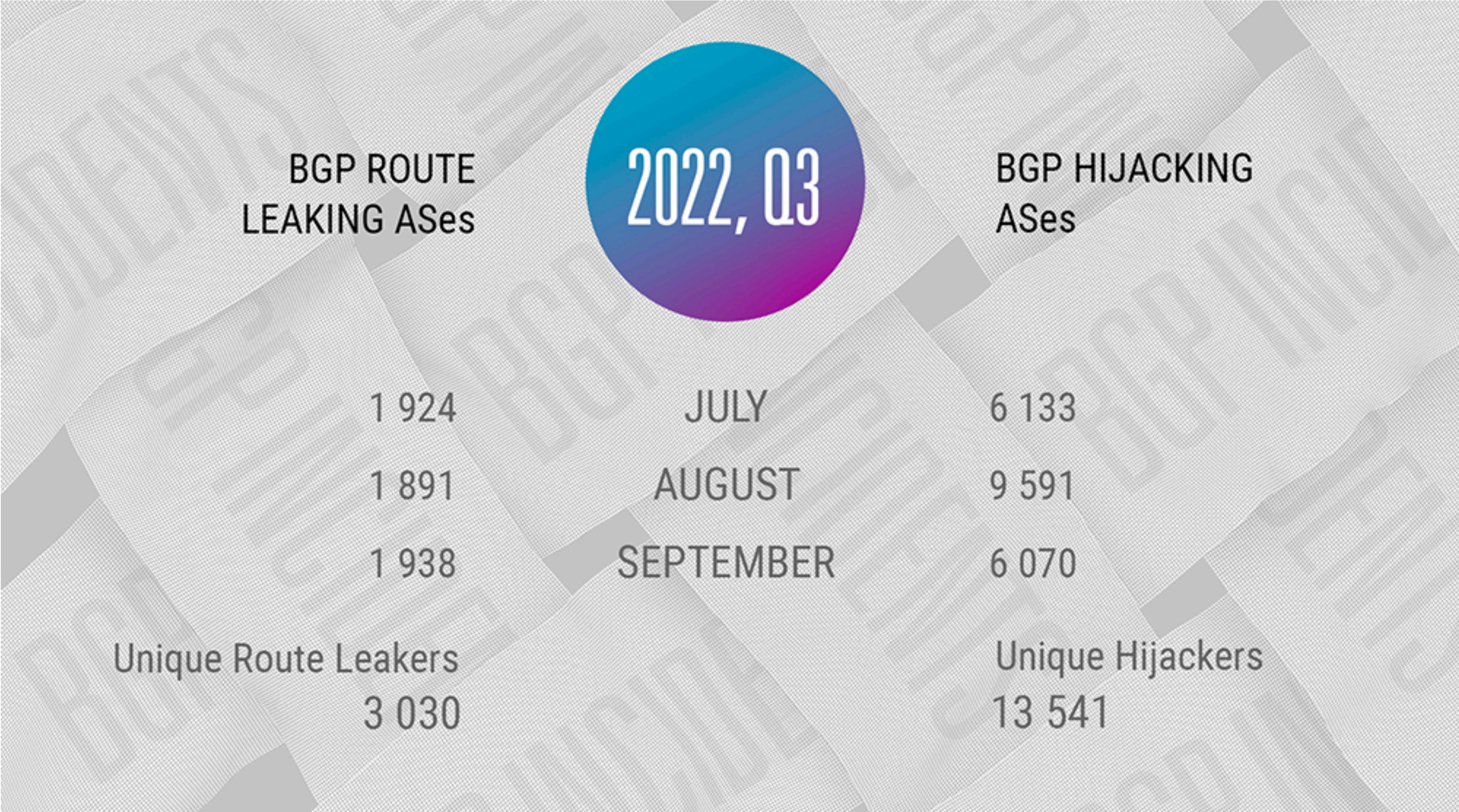
Sometimes it happens accidentally!



- Typing errors
 - Also known as “fat fingers”
 - May cause mis-origination
- Configuration errors
 - Faulty BGP filter configuration
 - AS path prepending mistakes
 - Cause routing policy violations and unintentional route leaks

(From RPKI RIPE Training Course)

Statistics from Qrator Labs



Can IRR help?



Concerns with the IRR system

1

Not globally deployed

Just distributed databases

2

No central authority

Who will verify the accuracy of the data?

3

No verification of holdership

Anyone can input anything

4

Not updated properly

Information is missing, outdated or incorrect

(From RPKI RIPE Training Course)

That's why RPKI was created



- RPKI is...
 - A **resource certification** (X.509 PKI certificates)
 - A security **framework**
- The currently implemented part of the RPKI is ROA
 - ROA = **Route Origin Authorisation**



(From RPKI RIPE Training Course)

How does it work?



Ties IP addresses and ASNs to public keys



Follows the RIR hierarchy



Authorised statements from resource holders

- “ASN X is authorised to announce my prefix Y”
- Signed, holder of Y

(From RPKI RIPE Training Course)

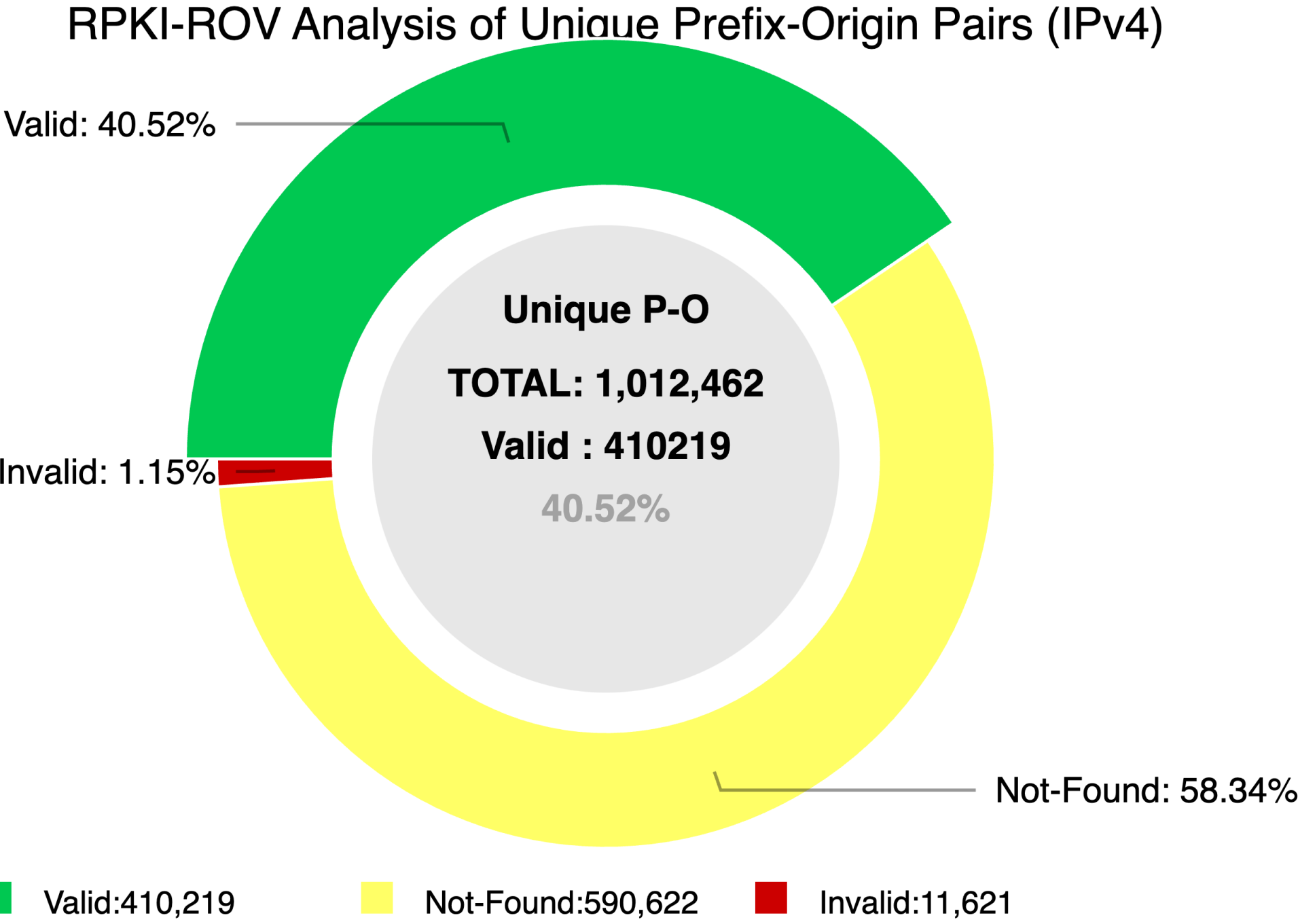
How does RPKI help with routing security?



- Verifies the association between resource holders and their Internet number resources.
 - Proves holdership through a public key and certificate infrastructure
- Used to validate the **origin of BGP announcements**
 - Is the originating ASN authorised to originate a particular prefix?
- Stepping stone to “**Path Validation**”

(From RPKI RIPE Training Course)

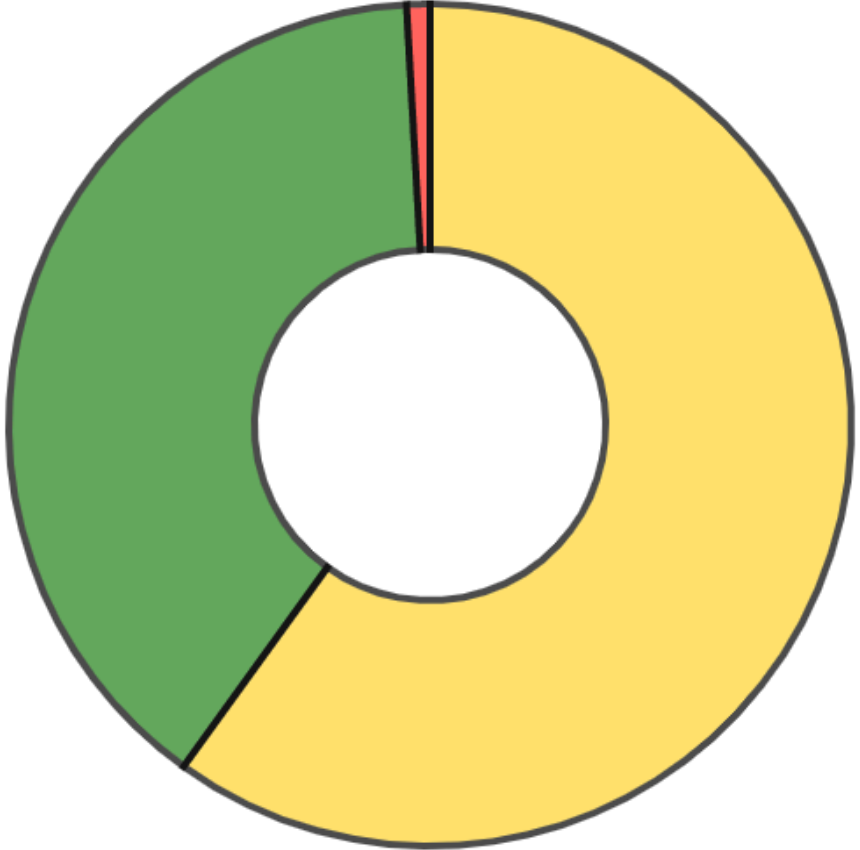
The global overview



NIST RPKI Monitor: RPKI-ROV Analysis Protocol: IPv4 RIR: All Date: 2022-11-15 06:00

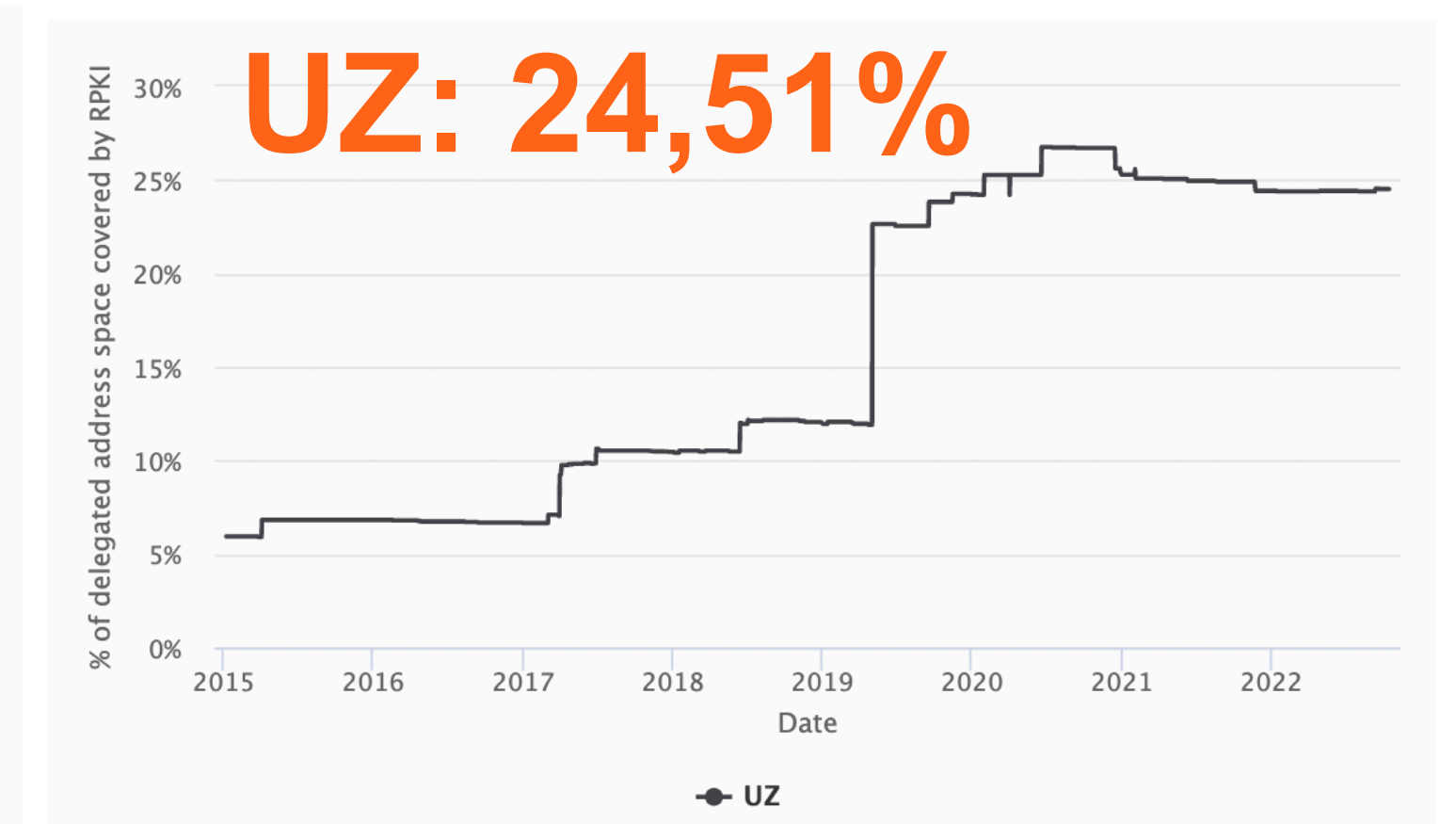
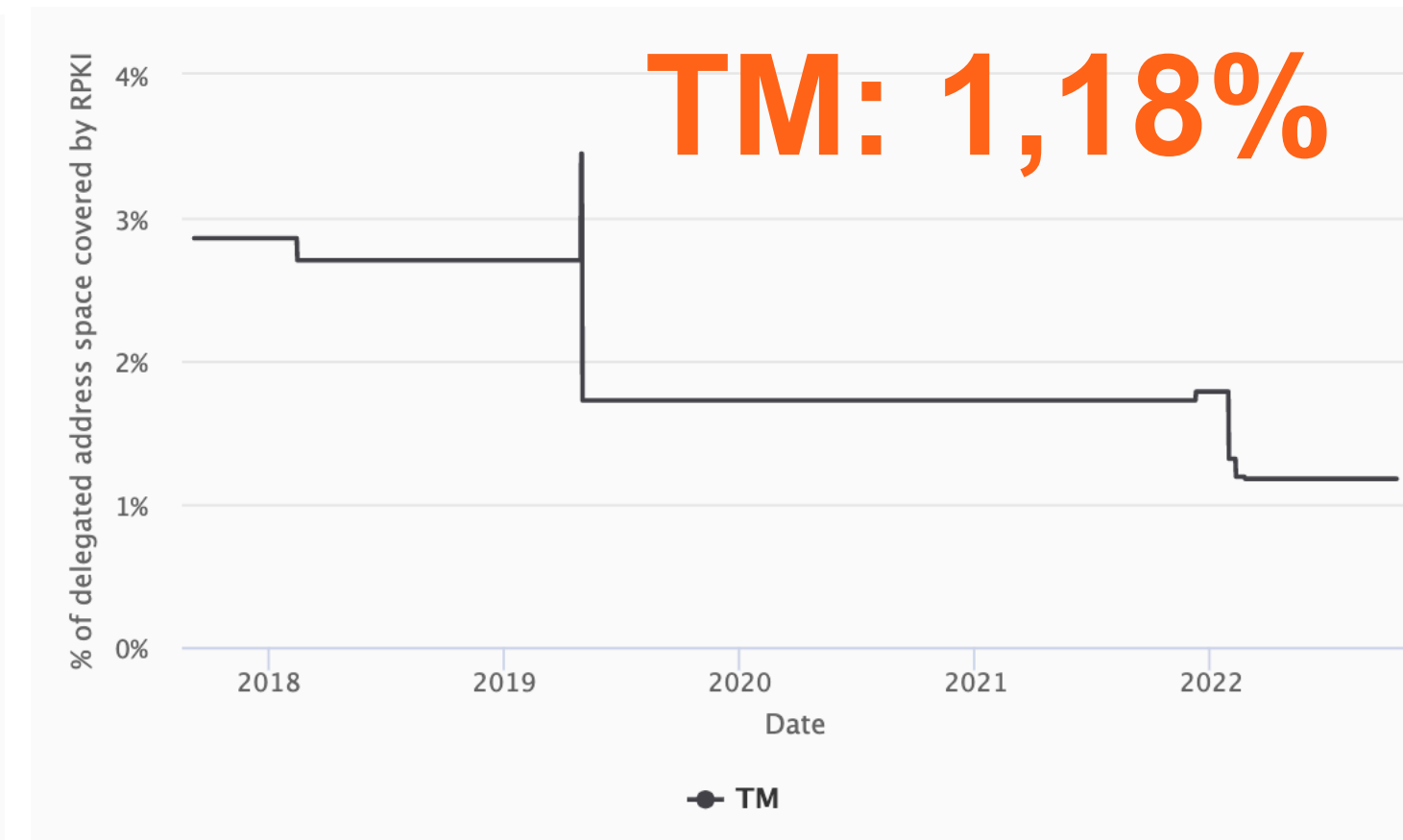
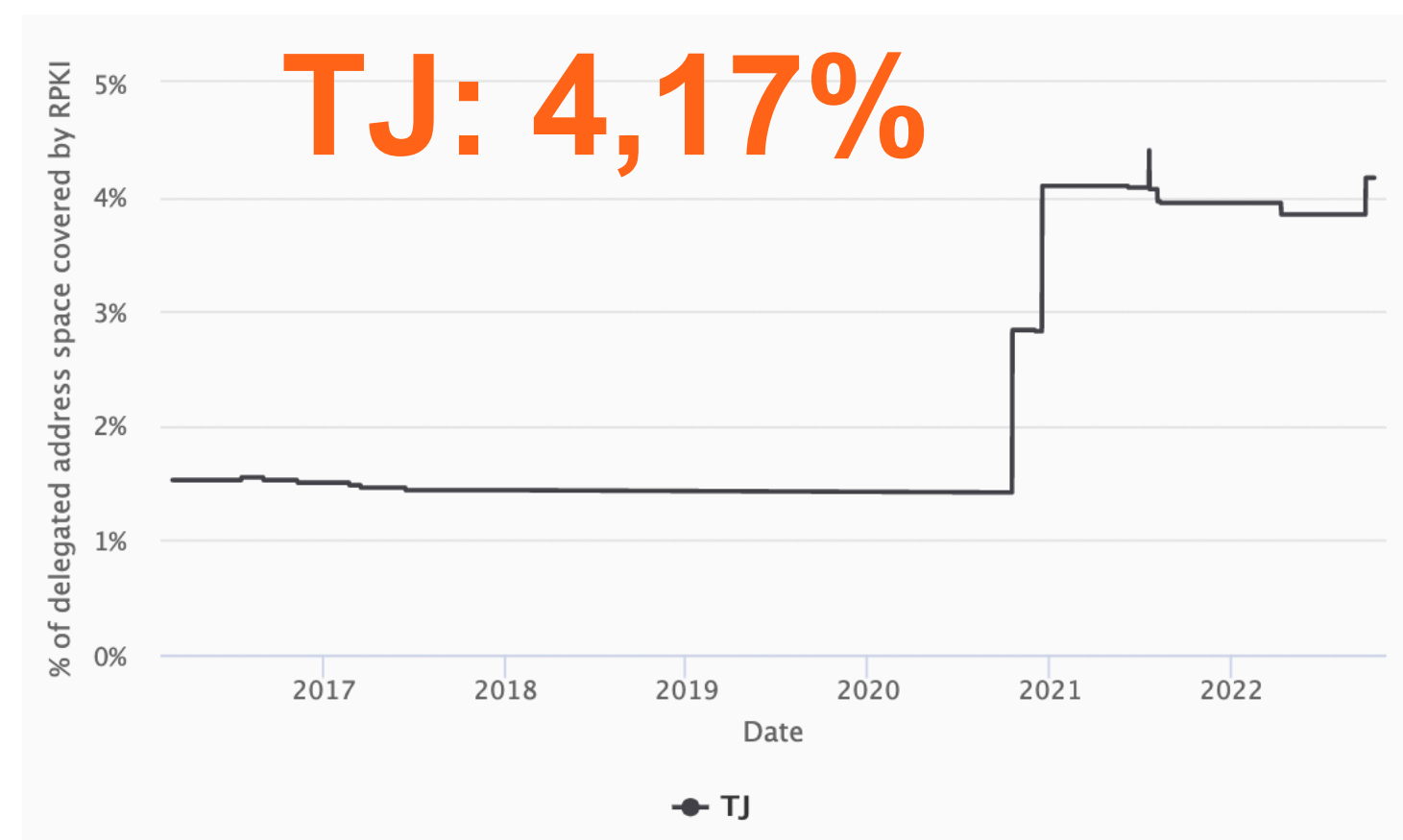
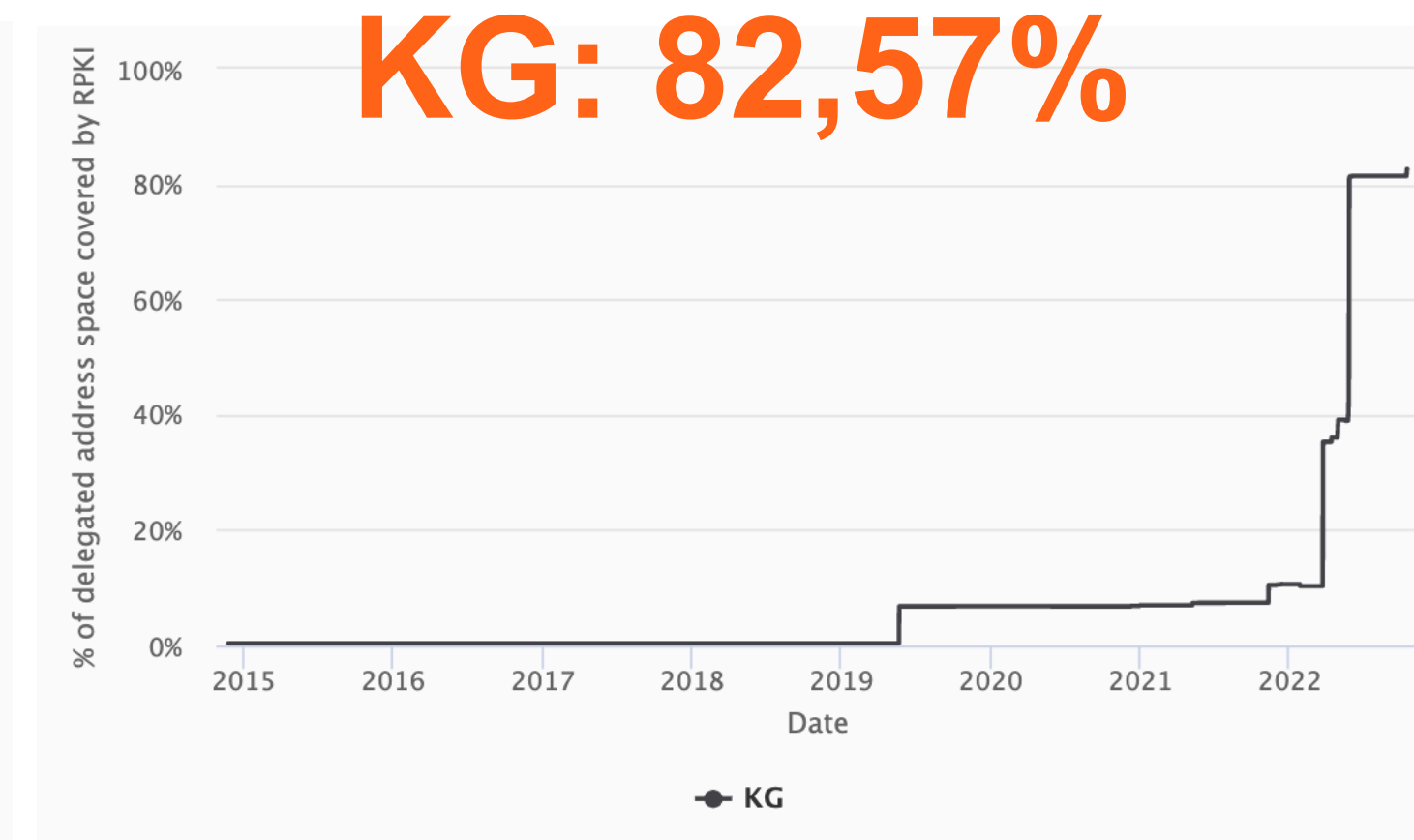
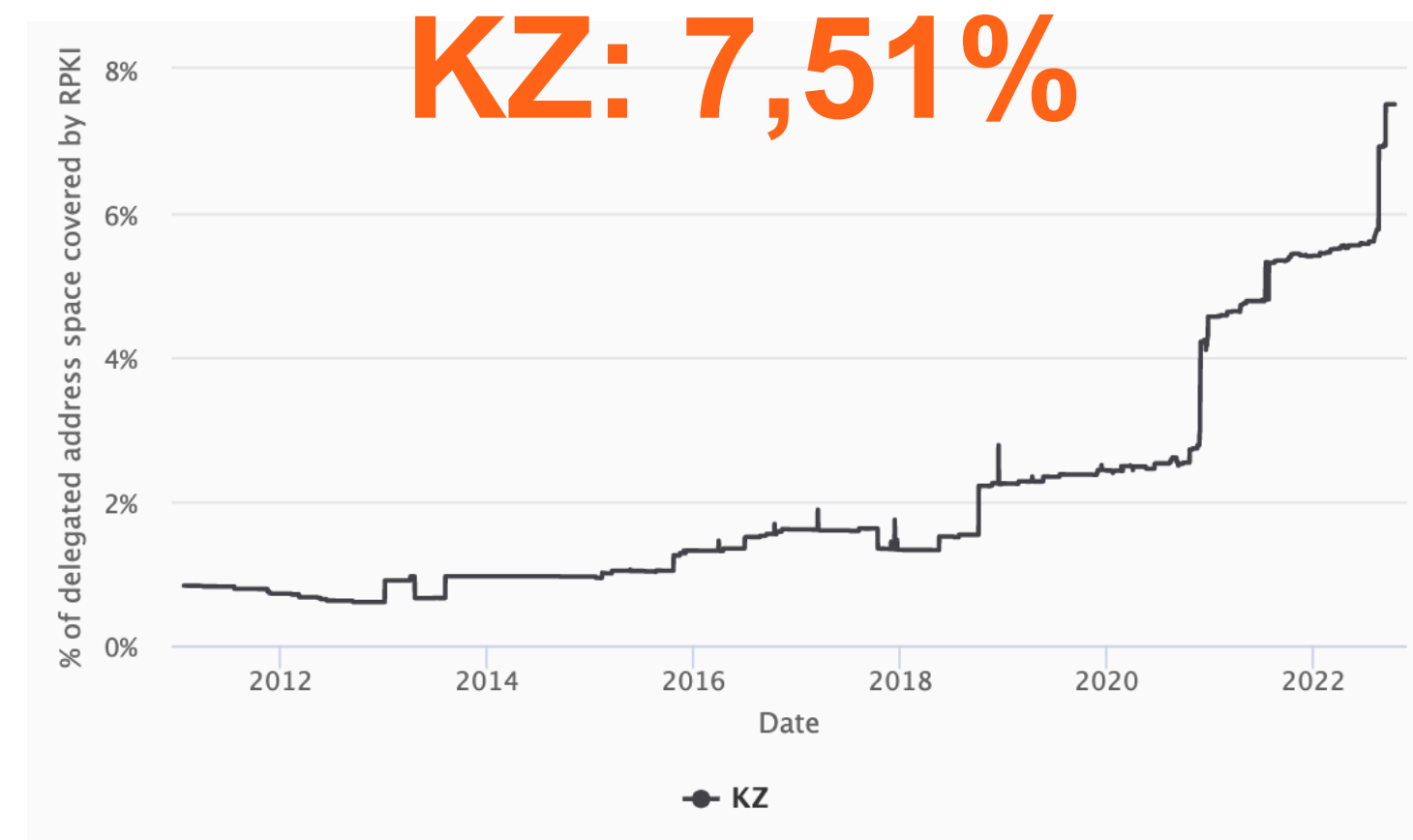
NIST data

IPv4		
Total	924685	
Valid Routes	362165	39.17%
Unknown Routes	554256	59.94%
Invalid Routes	8264	0.89%



MANRS data

RPKI deployment over the region



(By RIPEStat)



Questions



asemenyaka@ripe.net