ROA / ROV Measurements

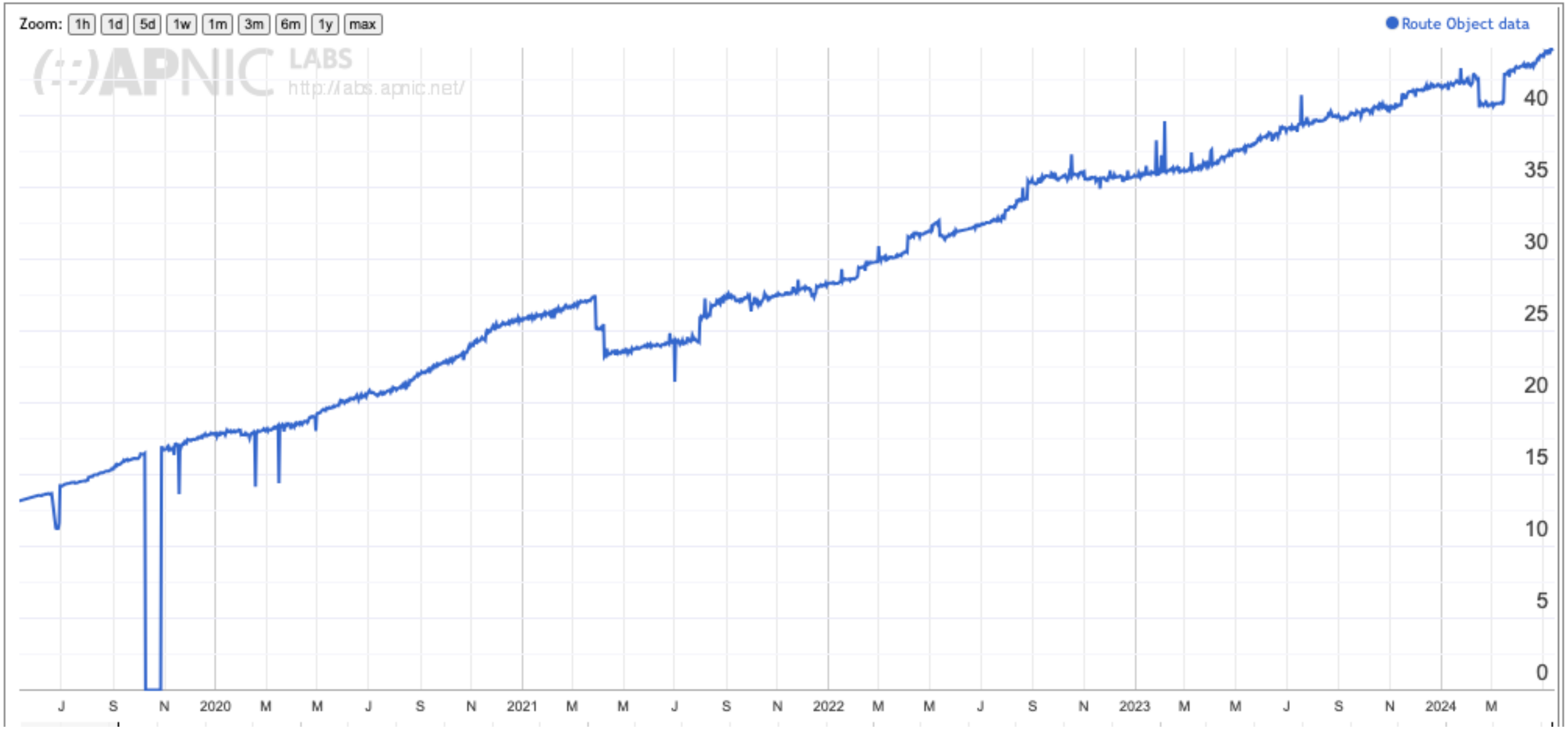
Geoff Huston

APNIC

May 2024

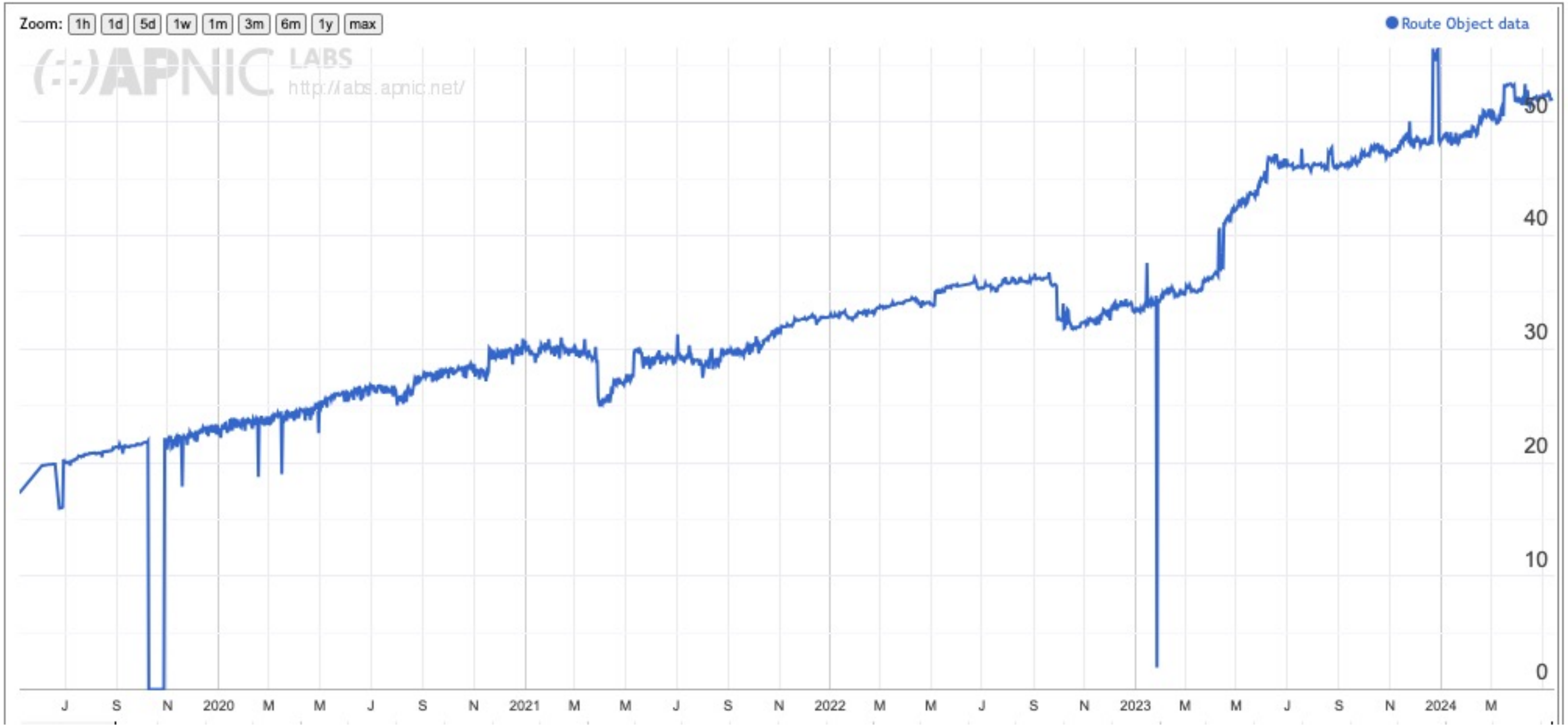
Time Series – IPv4

Proportion of IPv4 route objects that have an associated RPKI ROA

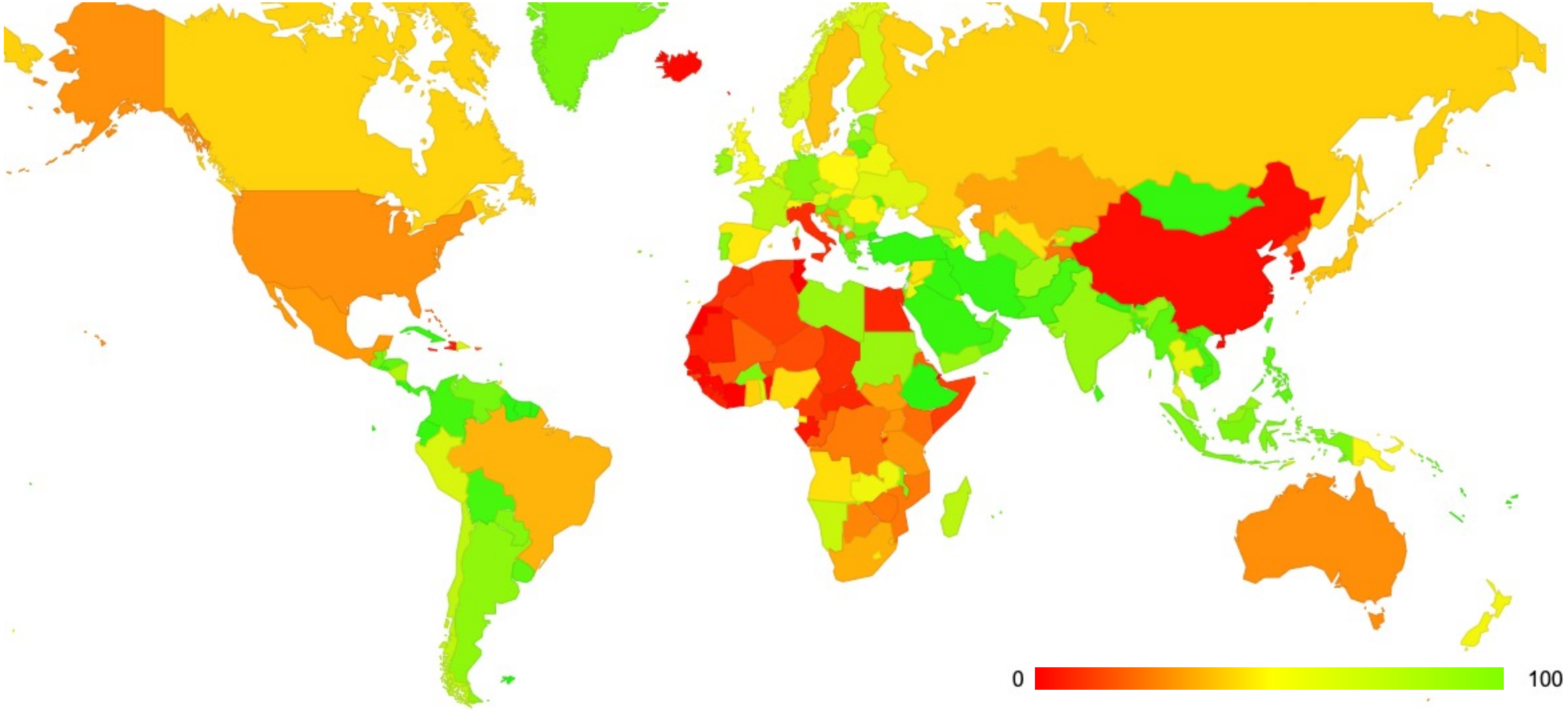


Time Series – IPv6

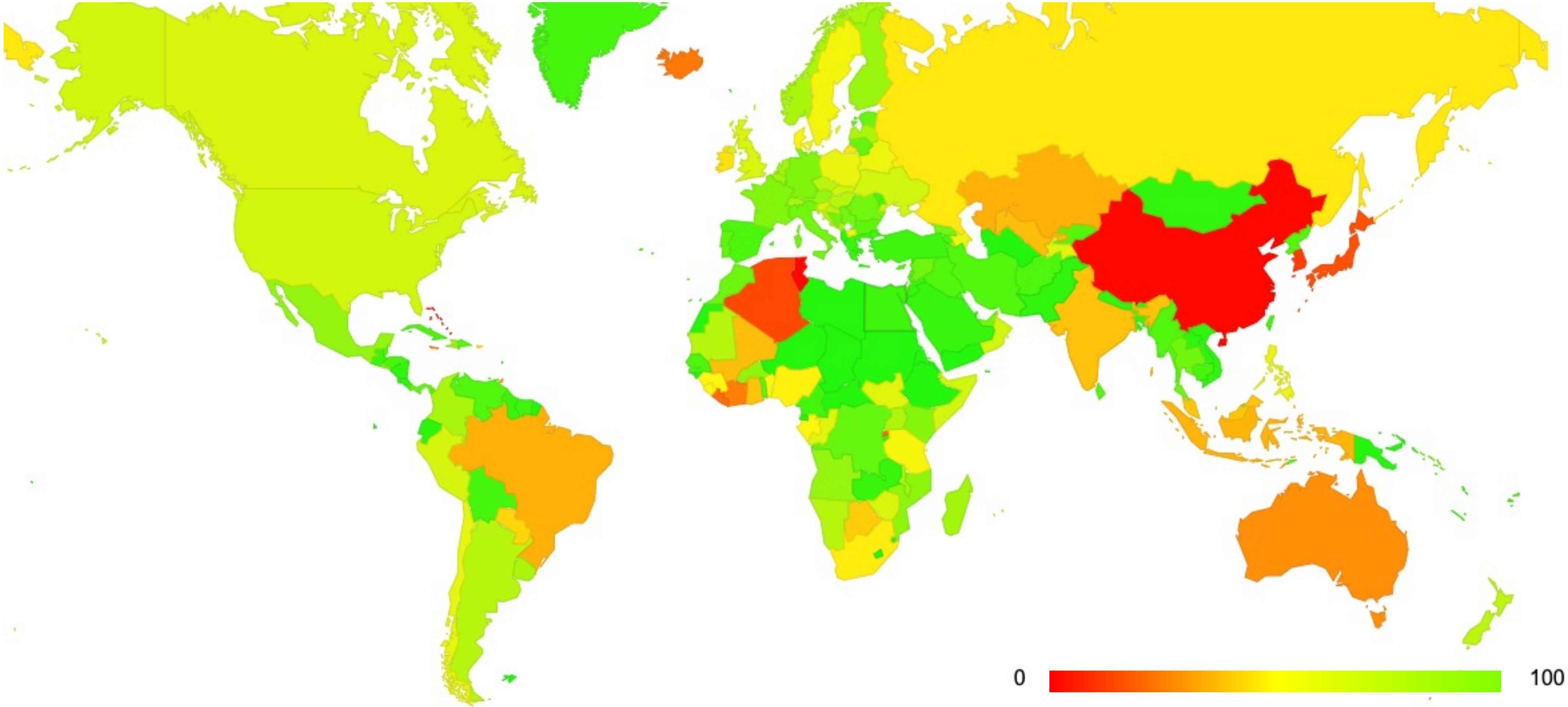
Proportion of IPv6 route objects that have an associated RPKI ROA



Where are ROAs deployed? – IPv4



Where are ROAs deployed? – IPv6

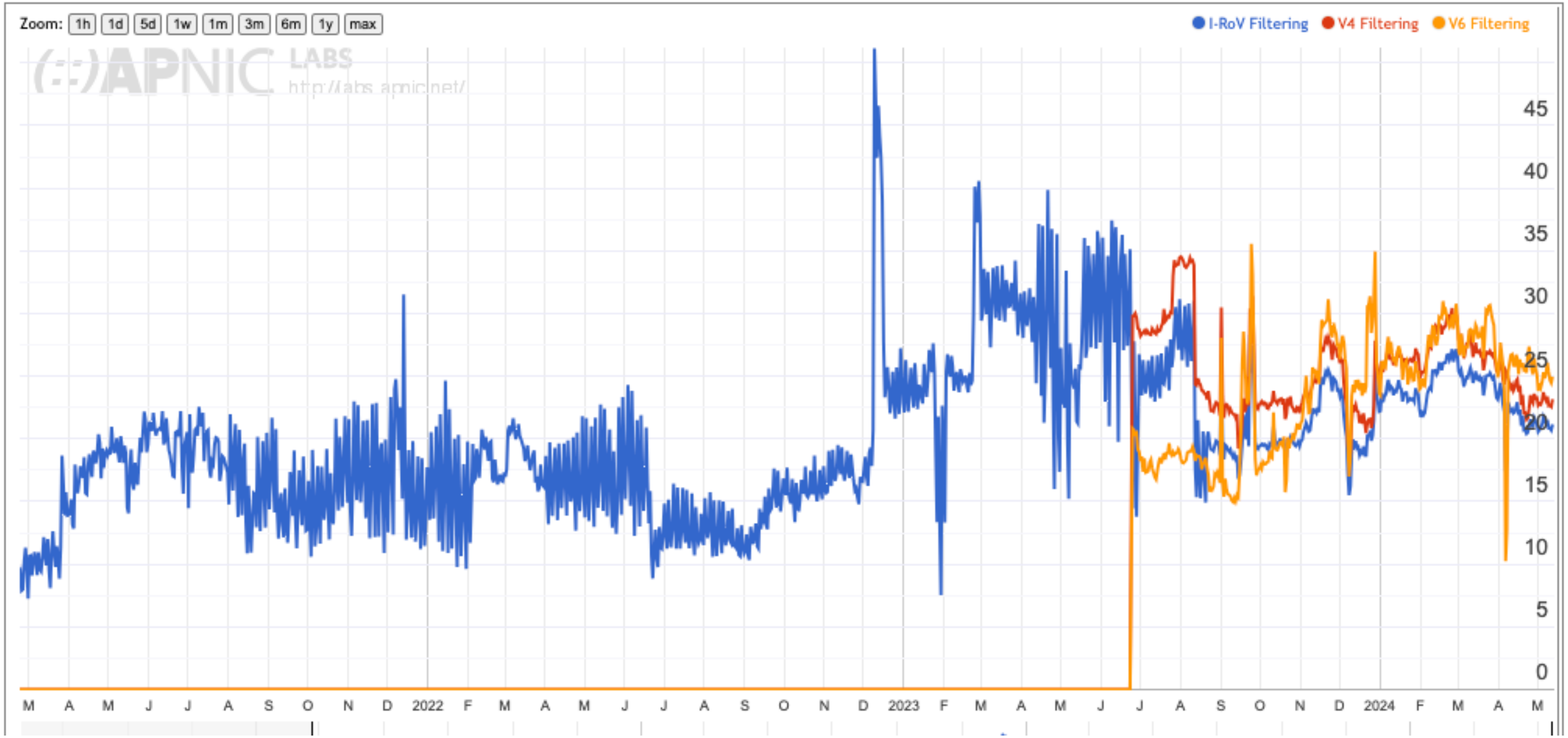


Where are we with ROA publication?

- And the answer is that we appear to be in a surprisingly good place!
- ROAs have been extensively deployed across much of Europe, the Middle East, Asia and South America
- The RPKI publication system appears to be adequately robust, although there is a very high level of reliance on the RPKI publication services operated by the RIRs

Measuring I-ROV Route Drop

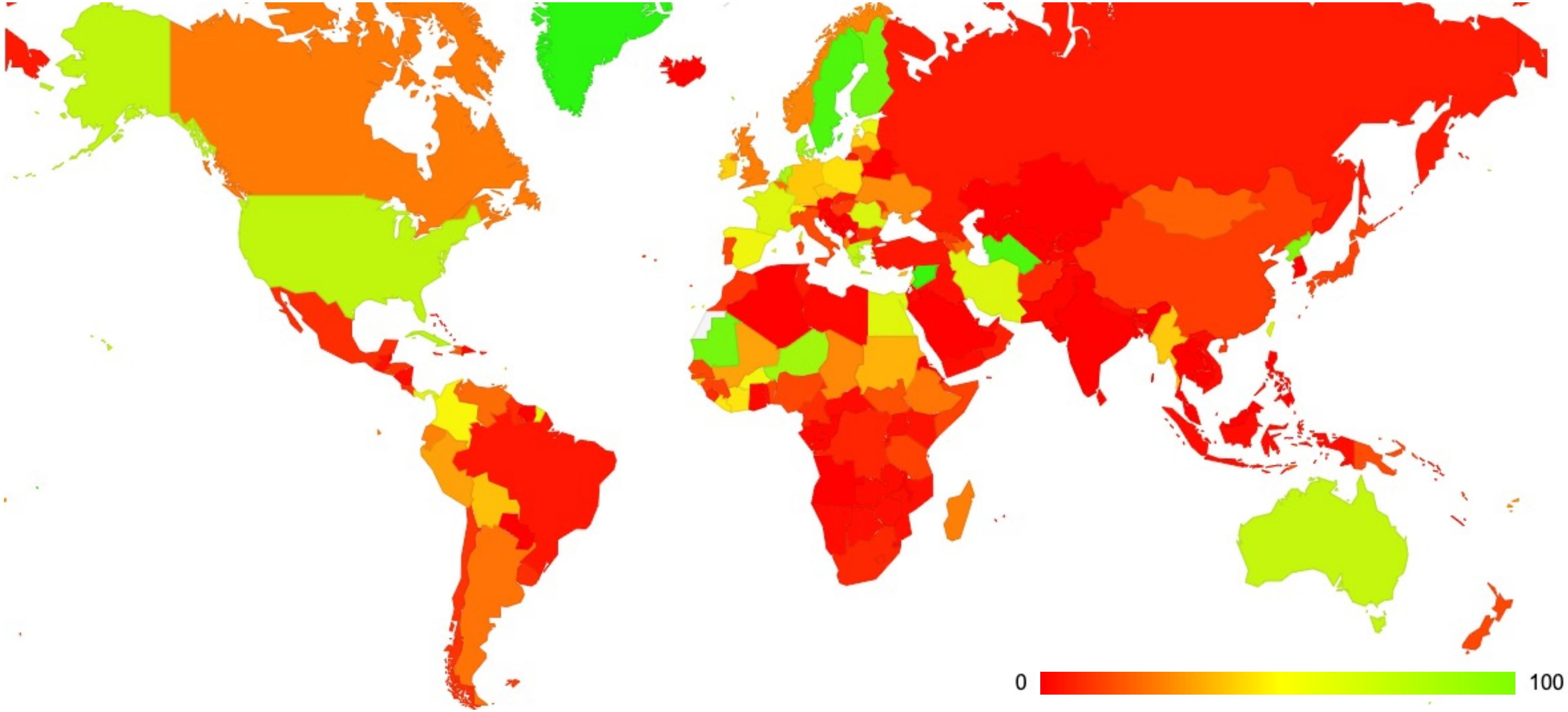
Proportion of end users that CANNOT access an object that lies behind an invalid route



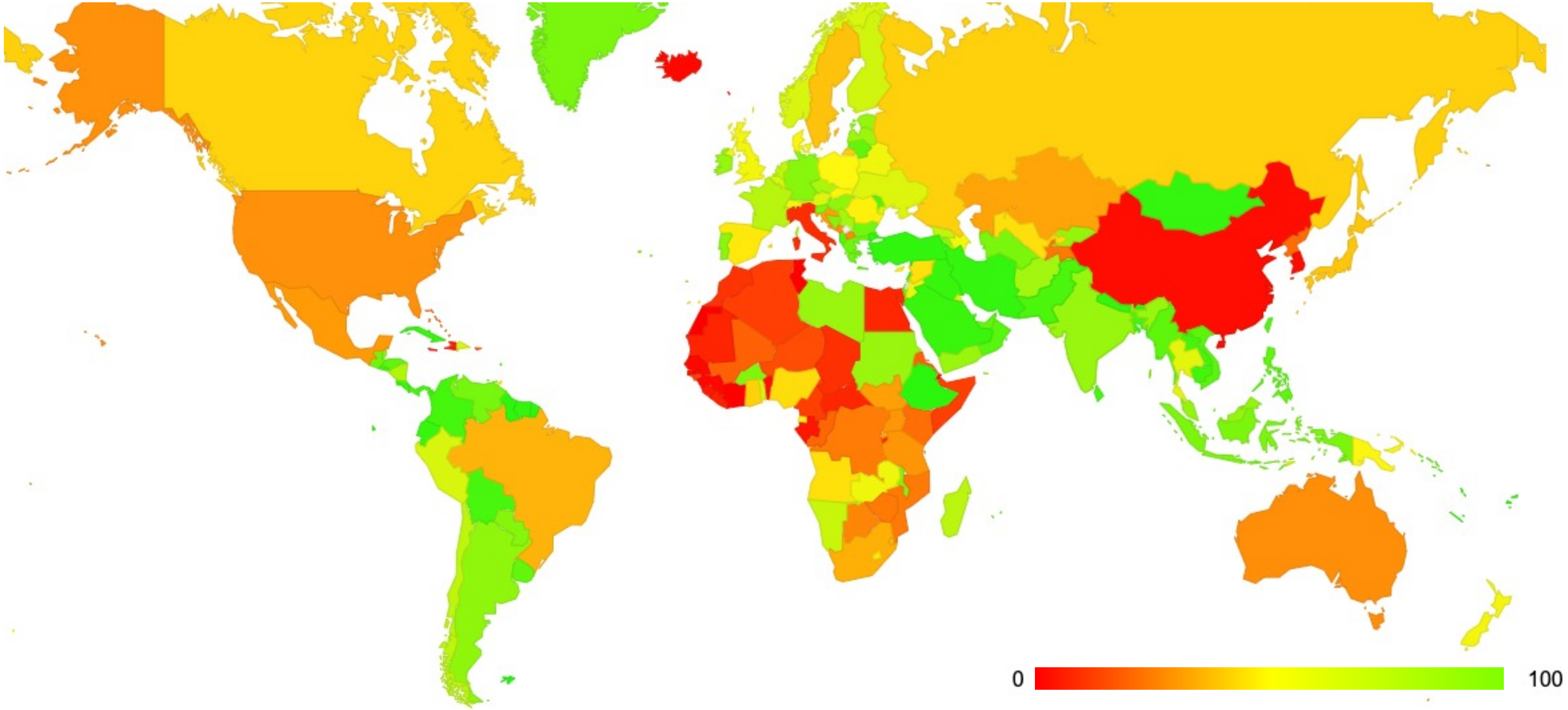
Measuring I-ROV Route Drop

- In this measurement we use an invalid destination advertised by a CDN (Cloudflare)
  - We do this to minimize the effects of transit networks masking the ROV behaviour of stub networks
- We then use an online ad campaign to enroll ~10M endpoints to reach this destination per day
- The measurement is the proportion of endpoints who cannot reach the invalid destination

Where do ISPs drop I-ROV routes?



Where are ROAs deployed? – IPv4

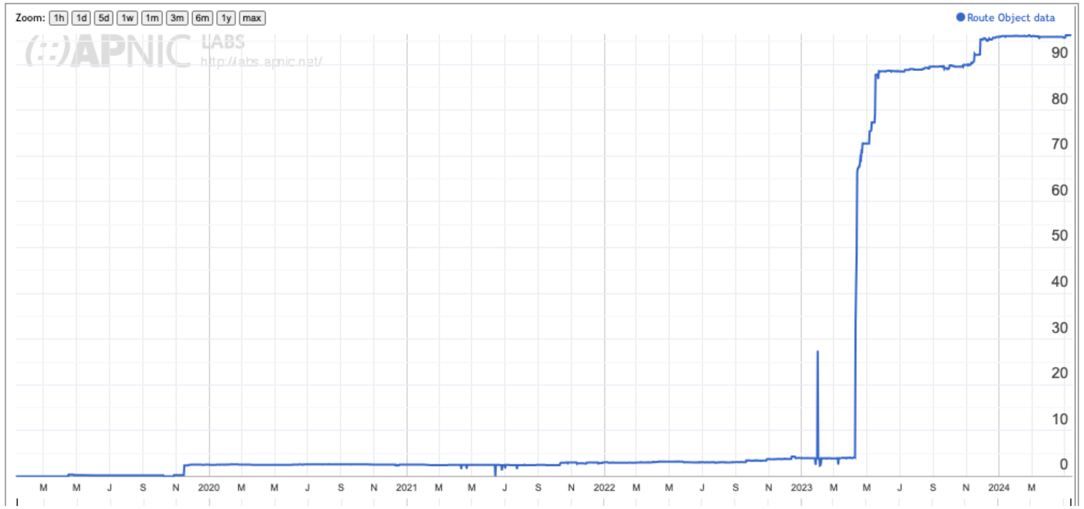


Many networks sign ROAS, but fewer perform I-ROV Filtering

For Example - Saudi Arabia

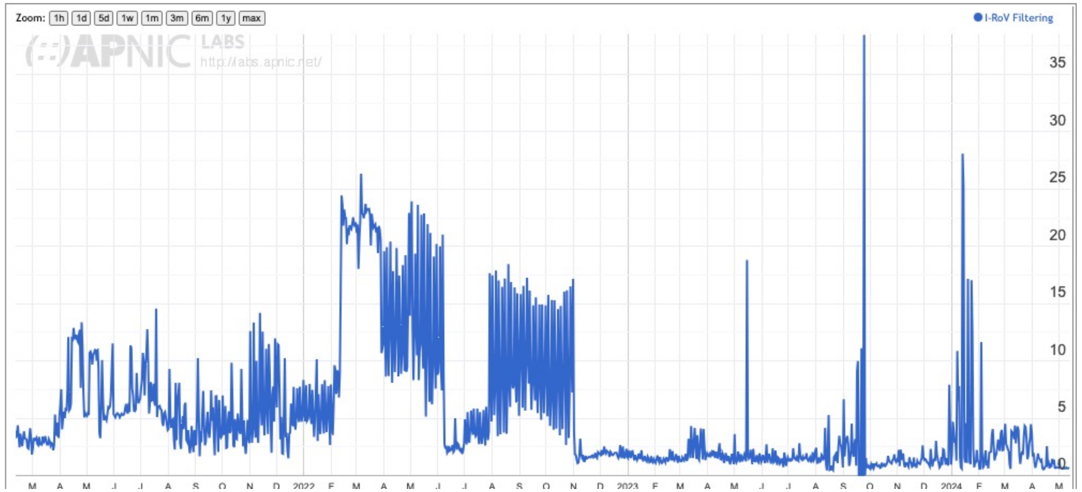
Use of Route Object Validation for Saudi Arabia (SA)

Display: **Addresses** (Advertised ROA-Valid Advertised Addresses), **IPv4**, **Percent** (of Total)



ROA Signing - 90%

Use of RPKI Validation for Saudi Arabia (SA)



I-ROV Filtering - 0%

Unfinished Routing Security Work

- Validated Origination without AS Path protection is ineffectual against determined attack
  - It is useful against inadvertent route leaks, but a determined attacker can forge a AS Path that reflects “correct” origination
- BGPSEC (RFC8205) can protect the AS Path, but the cost of deployment appears to be too high - deployment of BGPSEC has not gathered momentum, and it’s unlikely to ever do so!
- ASPA provides a weaker form of Path protection but there is no sign of operational uptake
  - The draft specification is still in the IETF process after ~7 years

Is all this helping?

- This is a hard question to answer with measurements
  - Preventative technologies are all about the **absence** of behaviours
  - And its always hard to measure what's NOT happening!
- I'm not sure we understand how we can take a fully distributed system such as inter-domain routing and impose an overlay of credentials and constraints that completely prevents all forms of aberrant behaviours
- But we can make it harder to abuse the routing system, either through inadvertent lapses or through deliberate intent
  - And the RPKI / ROV framework is our best effort to improve the security and integrity of the routing system
  - It's not a panacea and routing vulnerabilities still exist in many ways and many forms – but it can help the overall picture of routing resilience

Thanks!