Measuring the Effectiveness of Route Origin Validation Filtering via Drop Invalids from the perspective of the End User using a Technique of Broad Scale Reachability Measurement

Geoff Huston, Joao Damas
APNIC Labs

Measuring RPKI

Geoff Huston, Joao Damas
APNIC

Route Origin Validation Filtering!

Measuring ~~RPKI~~

Geoff Huston, Joao Damas
APNiC

Routing Security

What’s “the objective” of routing security?

Routing Security

What’s “the objective” of routing security?

- □Protect the routing system from all forms of operator mishaps?
- □Protect the routing system from some forms of operator mishaps?
- □Protect the routing system from all hostile attacks?
- □Protect the routing system from some hostile attacks?
- □Prevent the routing of bogus address prefixes?
- □Prevent the use of bogus AS’s in the routing system?
- □Prevent all forms of synthetic routes from being injected into the routing system?
- □Prevent unauthorised route withdrawal?
- □Protect users from being directed along bogus routing paths?

Let's not be too ambitious!

Enforcing rules to ensure that the routes carried in BGP are both protocol-wise accurate and policy-wise accurate is well beyond the capabilities of BGP and viable BGP control mechanisms *

Route Origin Validation is designed to prevent BGP speakers from learning and preferring routes that are not authorised by the prefix holder

The intent of not preferring unauthorised routes is to prevent users’ traffic from being steered along these bogus routes

* BGP is not a deterministic protocol, but more of a negotiation protocol that attempts to find meta-stable ‘solutions to importer / export policy preferences simultaneously. Where the policies are incompatible the BGP “solution” is not necessarily reached deterministically and different outcomes will be seen at different times – see “BGP Wedgies” for an illustration of this form of indeterminism

Routing Security

What’s “the objective” of routing security?

- □ Protect the routing system from all forms of operator mishaps?
- □ Protect the routing system from some forms of operator mishaps?
- □ Protect the routing system from all hostile attacks?
- □ Protect the routing system from some hostile attacks?
- □ Prevent the routing of bogus address prefixes?
- □ Prevent the use of bogus AS’s in the routing system?
- □ Prevent all forms of synthetic routes from being injected into the routing system?
- □ Prevent unauthorised route withdrawal?
- ☑ Protect users from being directed along bogus routing paths!

Our Objective

- To measure the "impact" of invalid route filtering on users

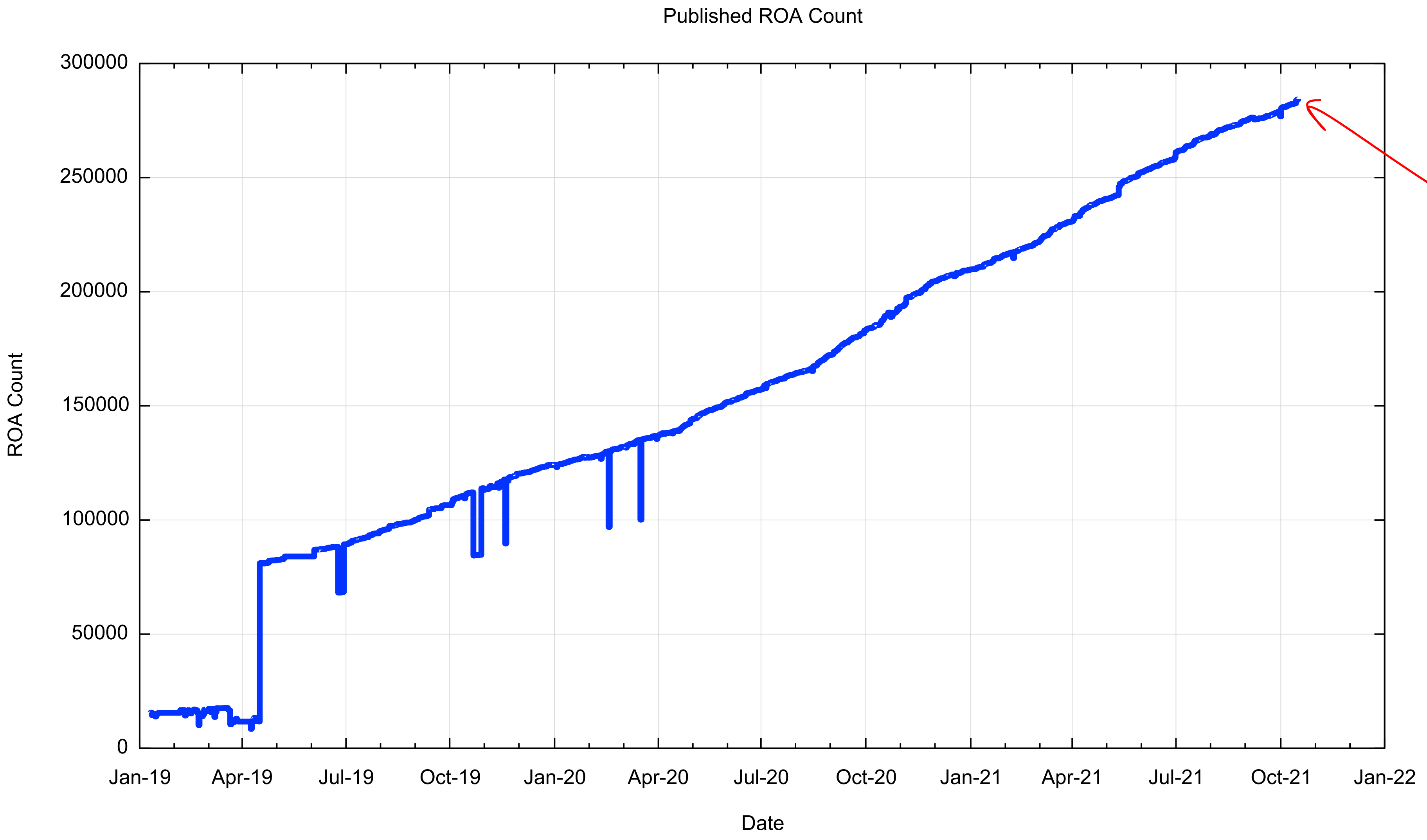
- The question we want to answer here is user-centric:
  - **What proportion of users can't reach a destination when the destination route is invalid according to ROV?**

Production vs Consumption

There are two aspects to this framework:

- Generating ROAs to describe the intended origination of prefixes
- Looking for those networks that will admit and propagate invalid routes
    - i.e.: those networks that are not performing some for of “drop invalid” filtering on BGP advertisements

Populating the RPKI – ROAs

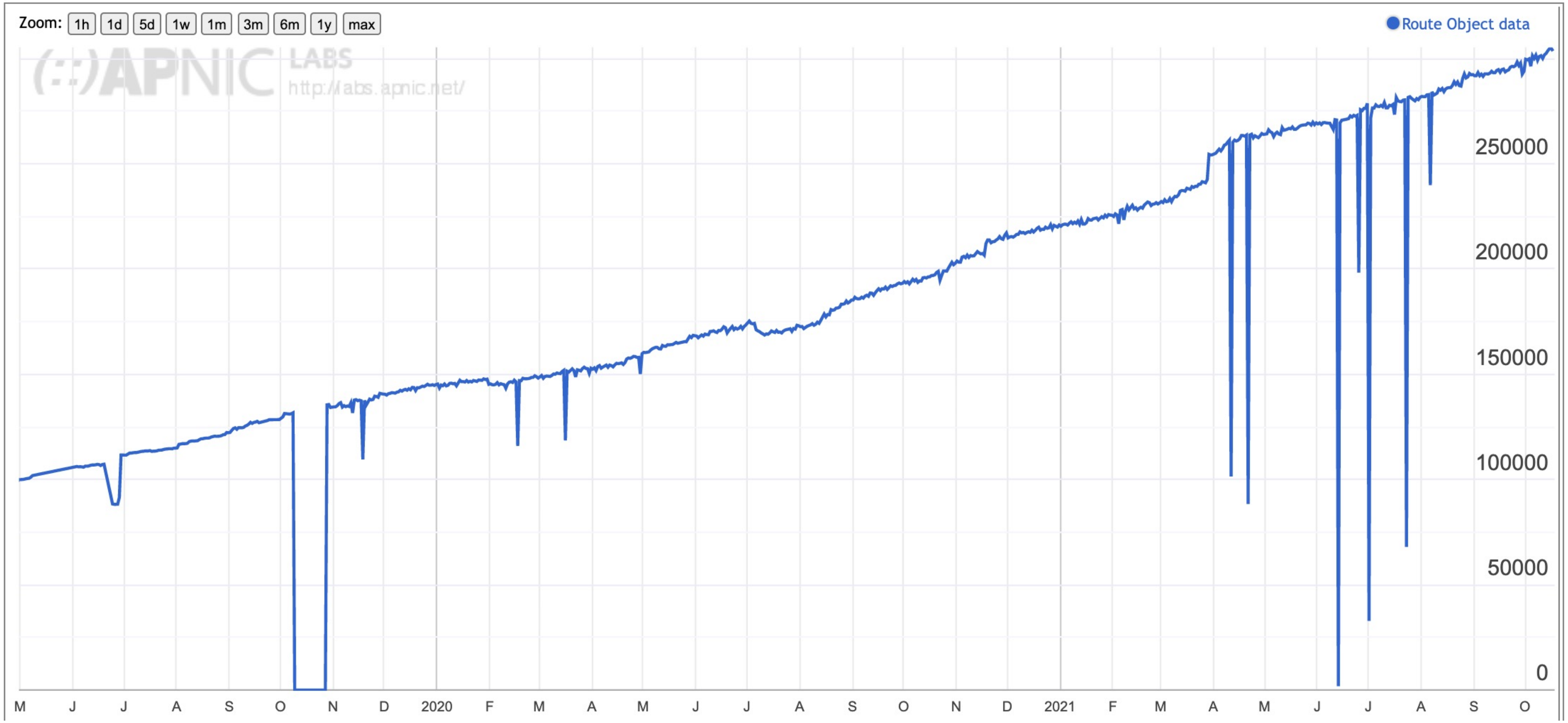


284,000 ROAs are published today

Applying ROAs to Routes

IPv4 Routes that are ”covered” by a ROA

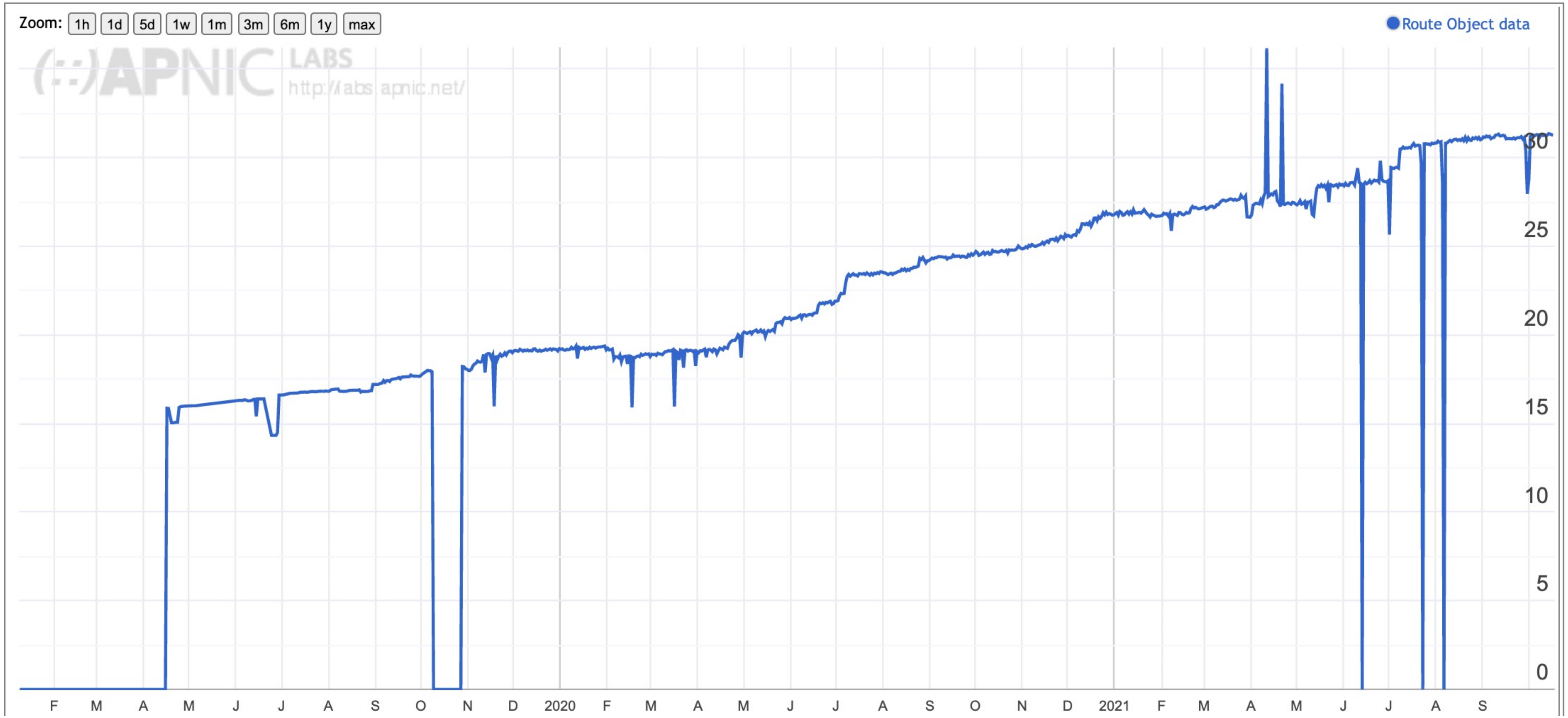
Display: **ROAs** (Advertised ROA-Valid Route Advertisements), **IPv4**, **Count**



Applying ROAs to Routes

IPv4 Addresses that are ”covered” by a ROA

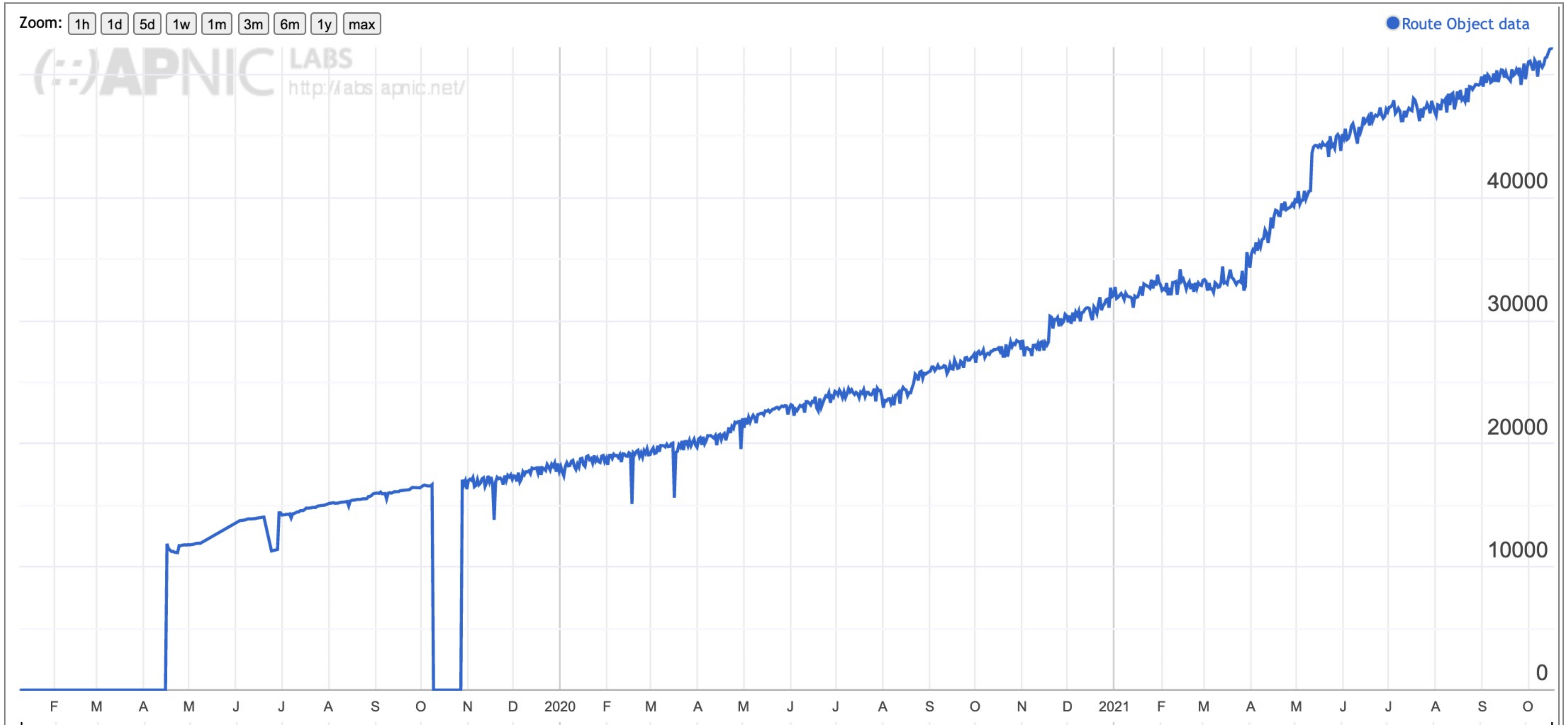
Display: **Addresses** (Advertised ROA-Valid Advertised Addresses), **IPv4**, **Percent** (of Total)



Applying ROAs to Routes

IPv6 Routes that are ”covered” by a ROA

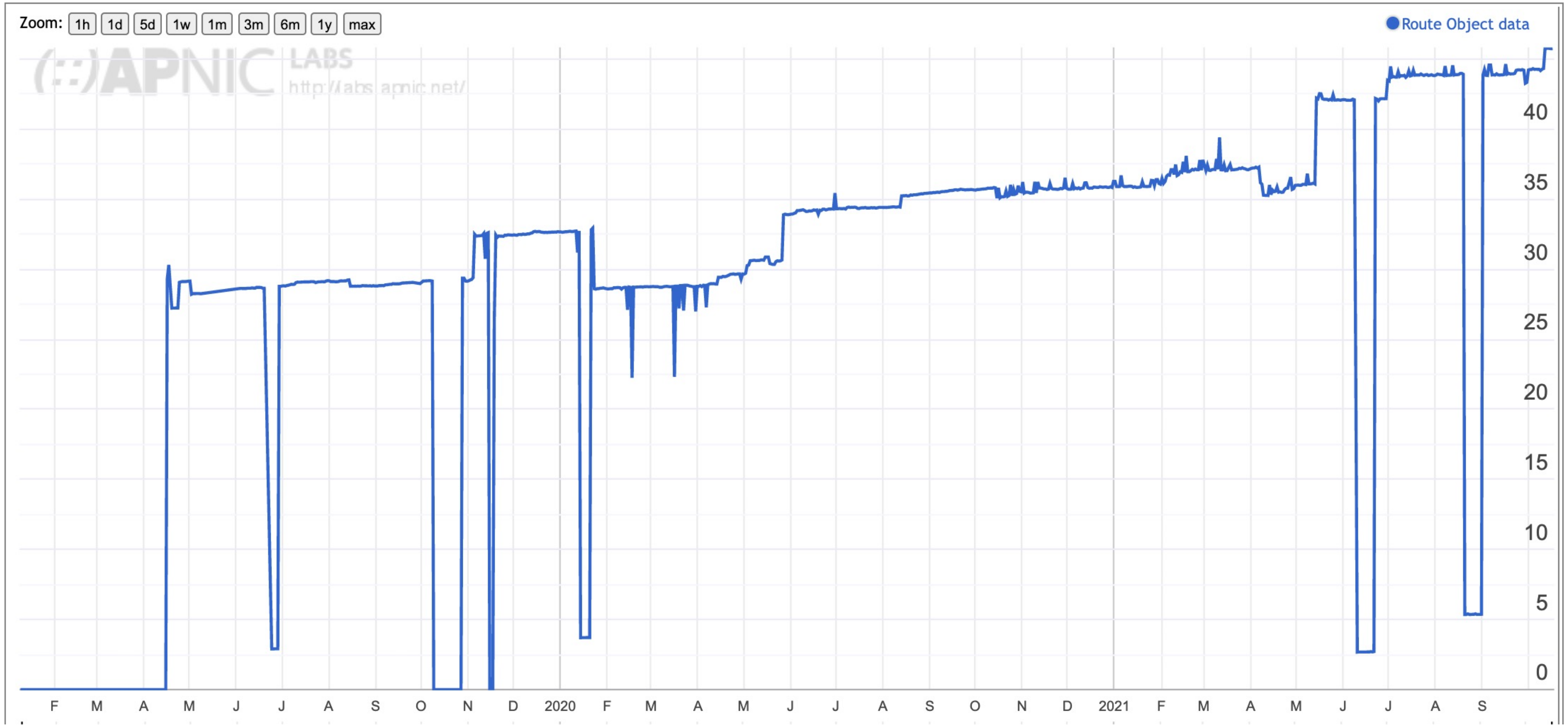
Display: **ROAs** (Advertised ROA-Valid Route Advertisements), **IPv6**, **Count**



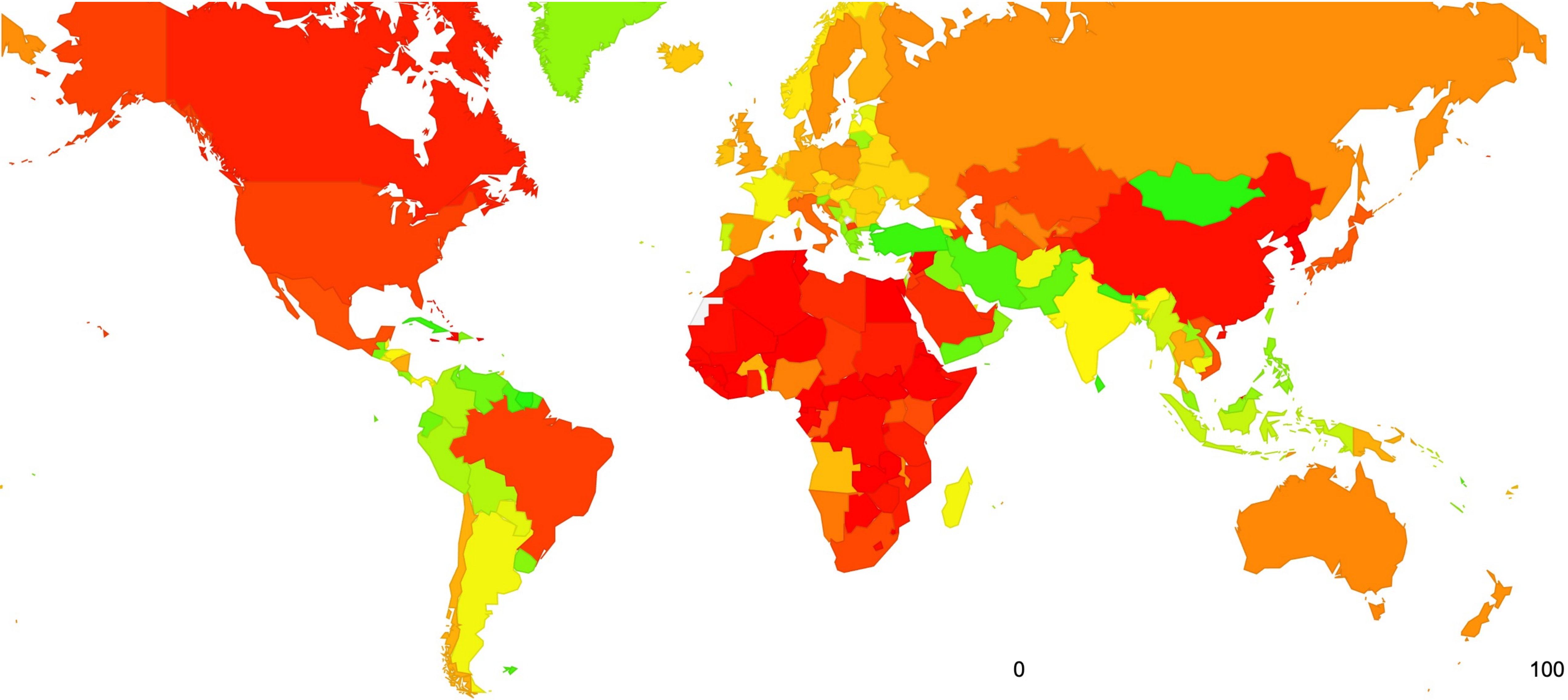
Applying ROAs to Routes

IPv6 Addresses that are ”covered” by a ROA

Display: **Addresses** (Advertised ROA-Valid Advertised Addresses), **IPv6**, **Percent** (of Total)



RoA coverage by Economy

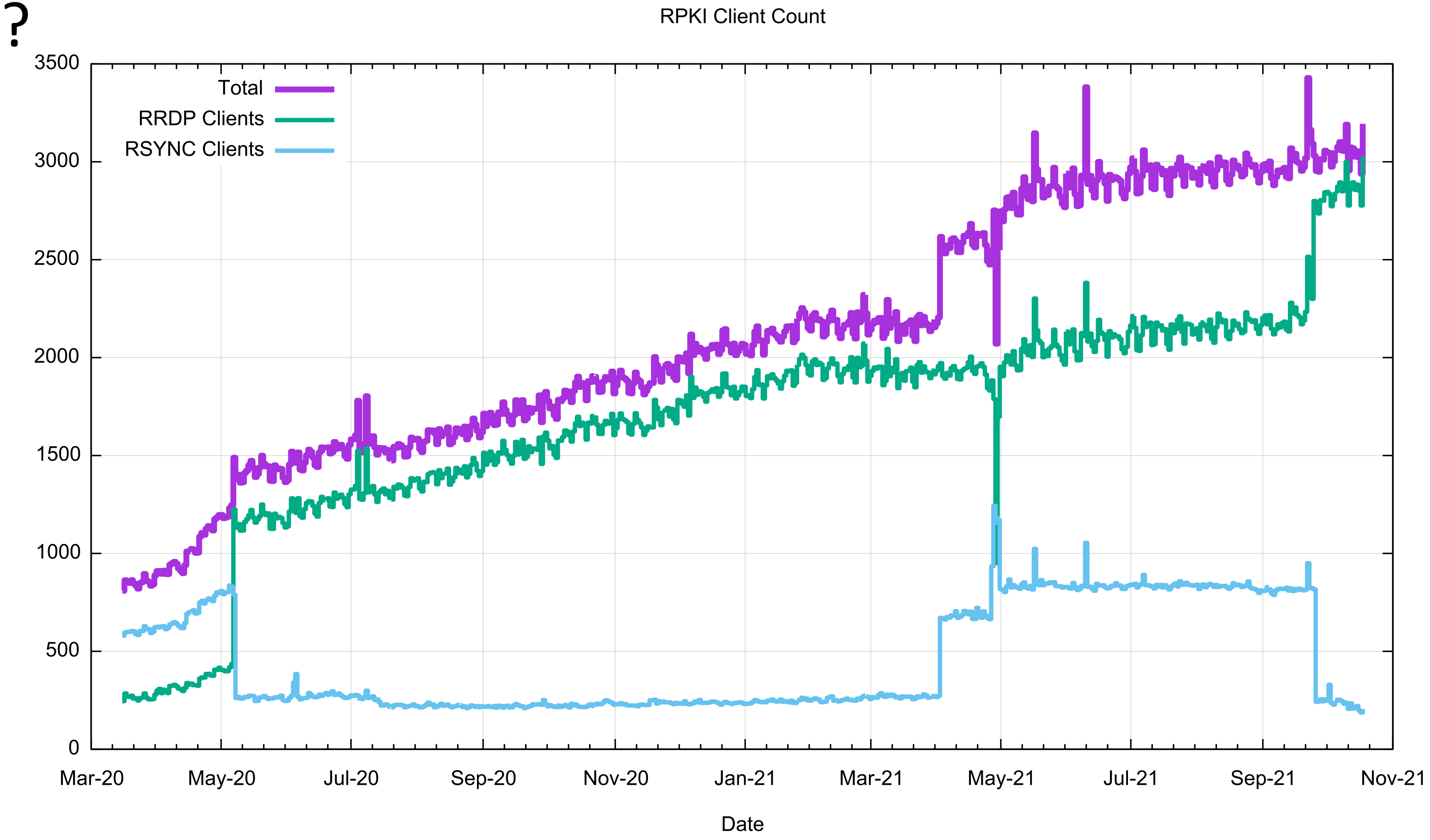


Production vs Consumption

- The next question is: Who is using these ROAs to determine whether to accept routes (or not!)

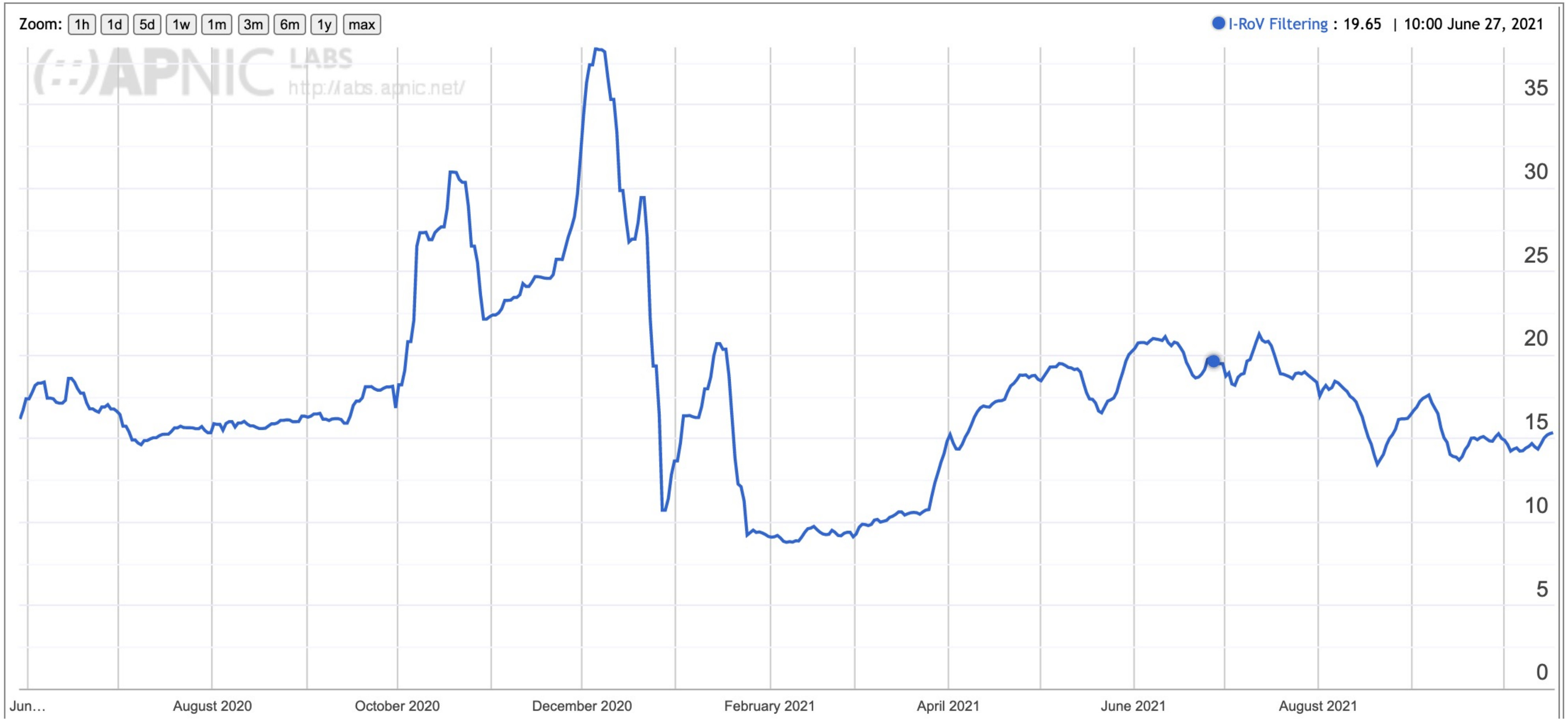
RPKI Clients

- How many clients regularly maintain a local cache of the entire RPKI product set ?

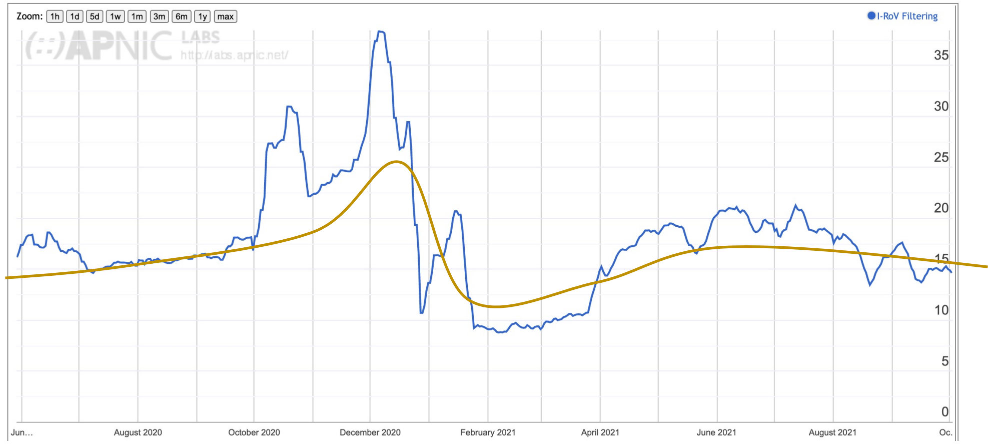


Filtering RoV routes

What proportion of users are behind networks that filter ROV-invalid routes?

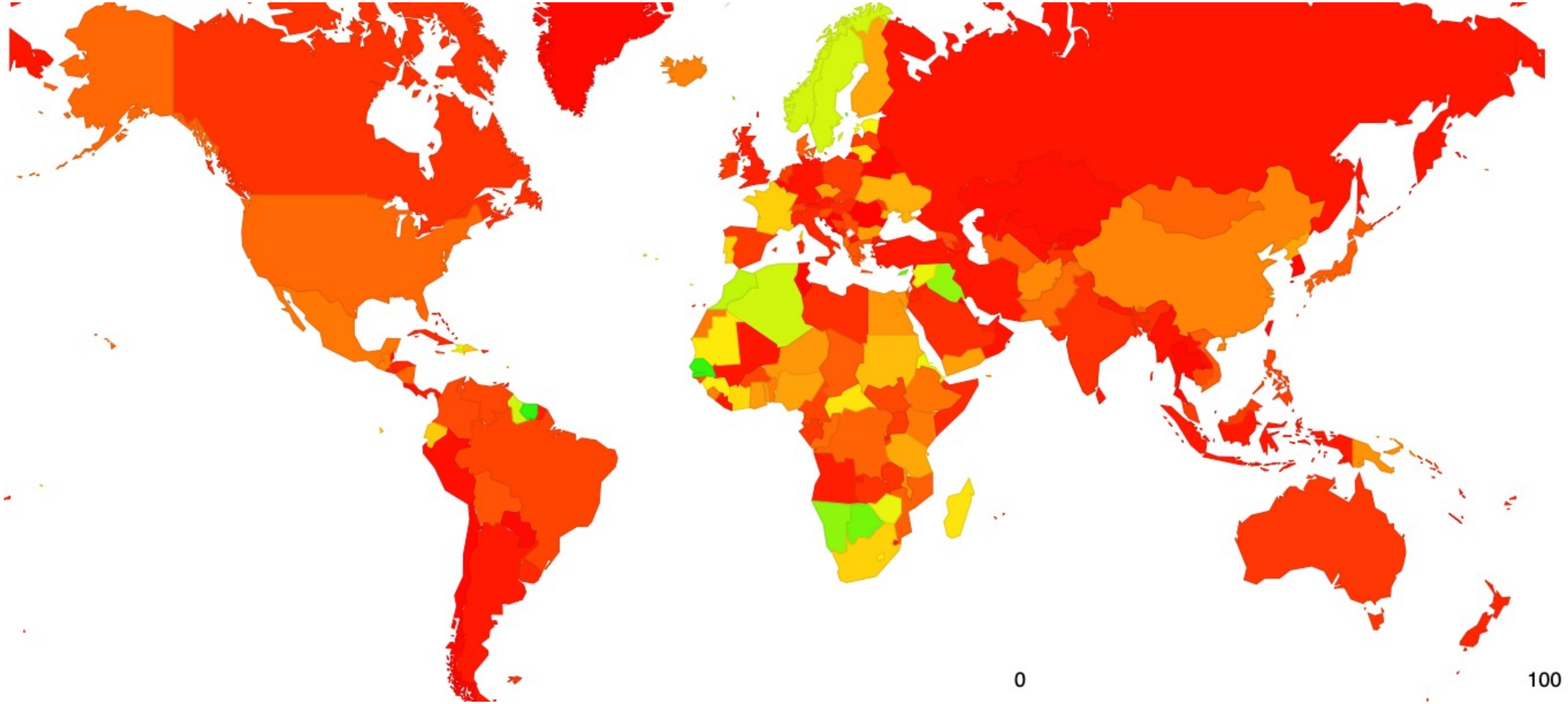


RoV Filtering



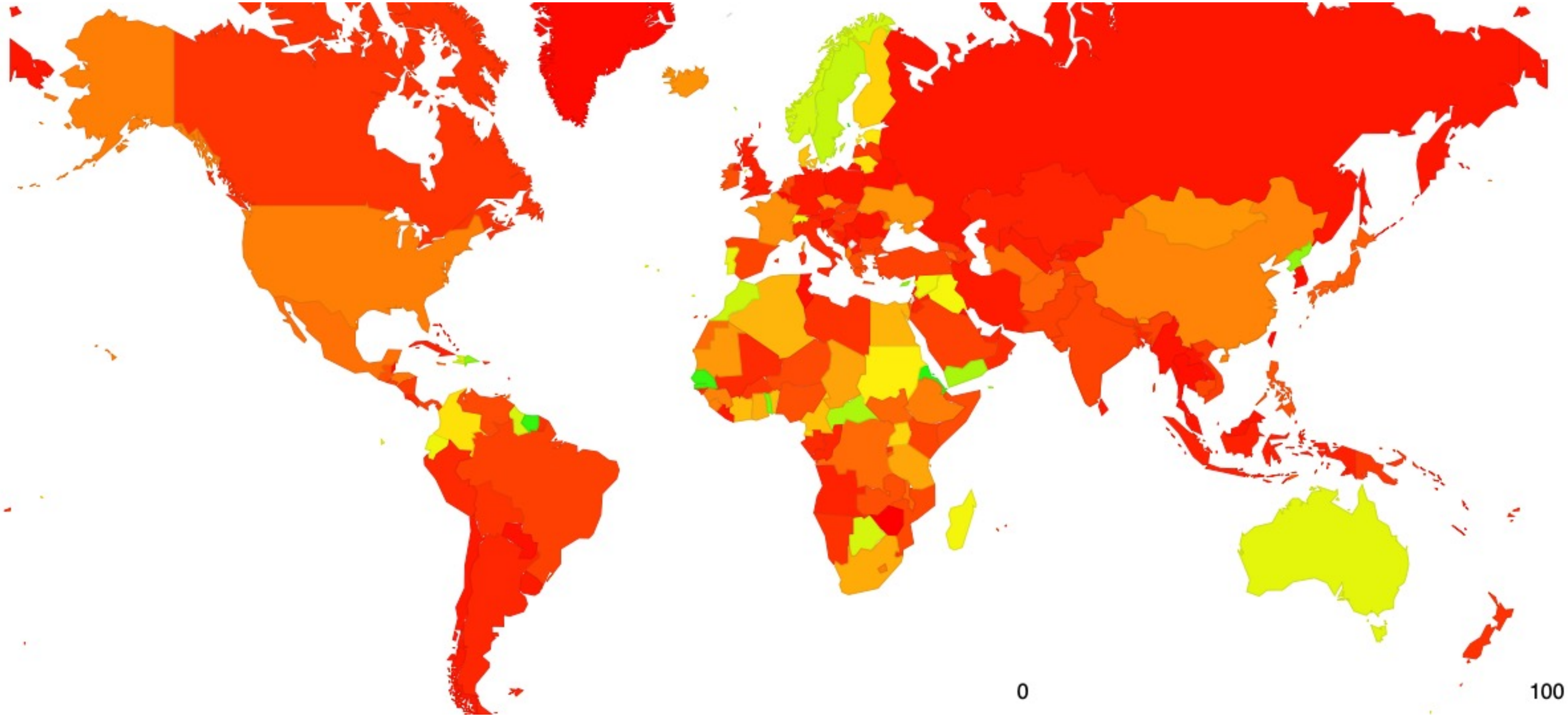
- This is an unexpected result
- Only some 15% of users cannot reach a prefix when it is advertised using a ROV-invalid prefix
- And this has been constant measurement for the past ~12 months
- It seems that few edge networks have been performing ROV dropping
- And similarly few transit networks have taken up ROV-dropping
- And there is sufficient diversity in the inter-AS topology that even if some paths are filtered out, alternate transit paths sill provide access

Results: User Impact of ROV filtering - Jul 2020



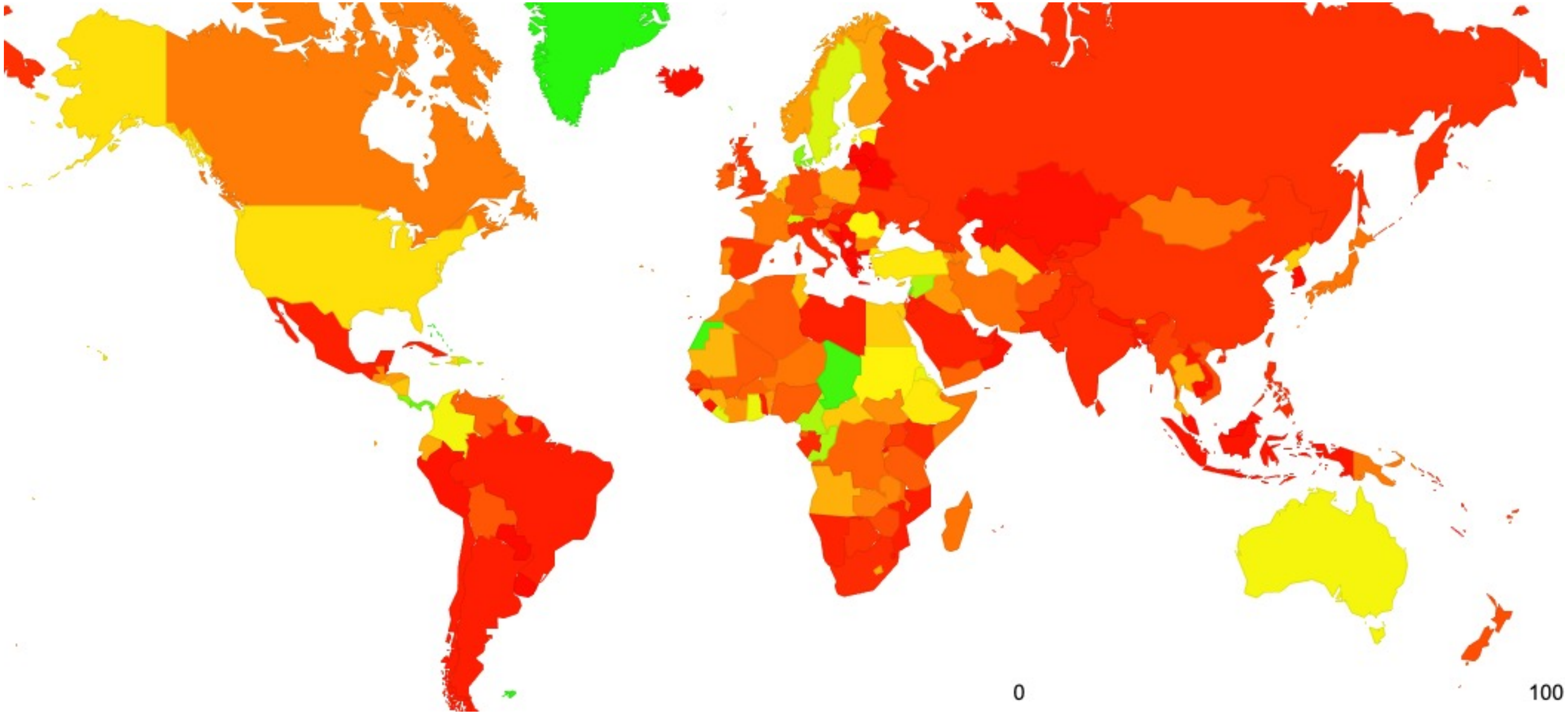
https://stats.labs.apnic.net/rpki

Results: User Impact of ROV filtering - Oct 2020



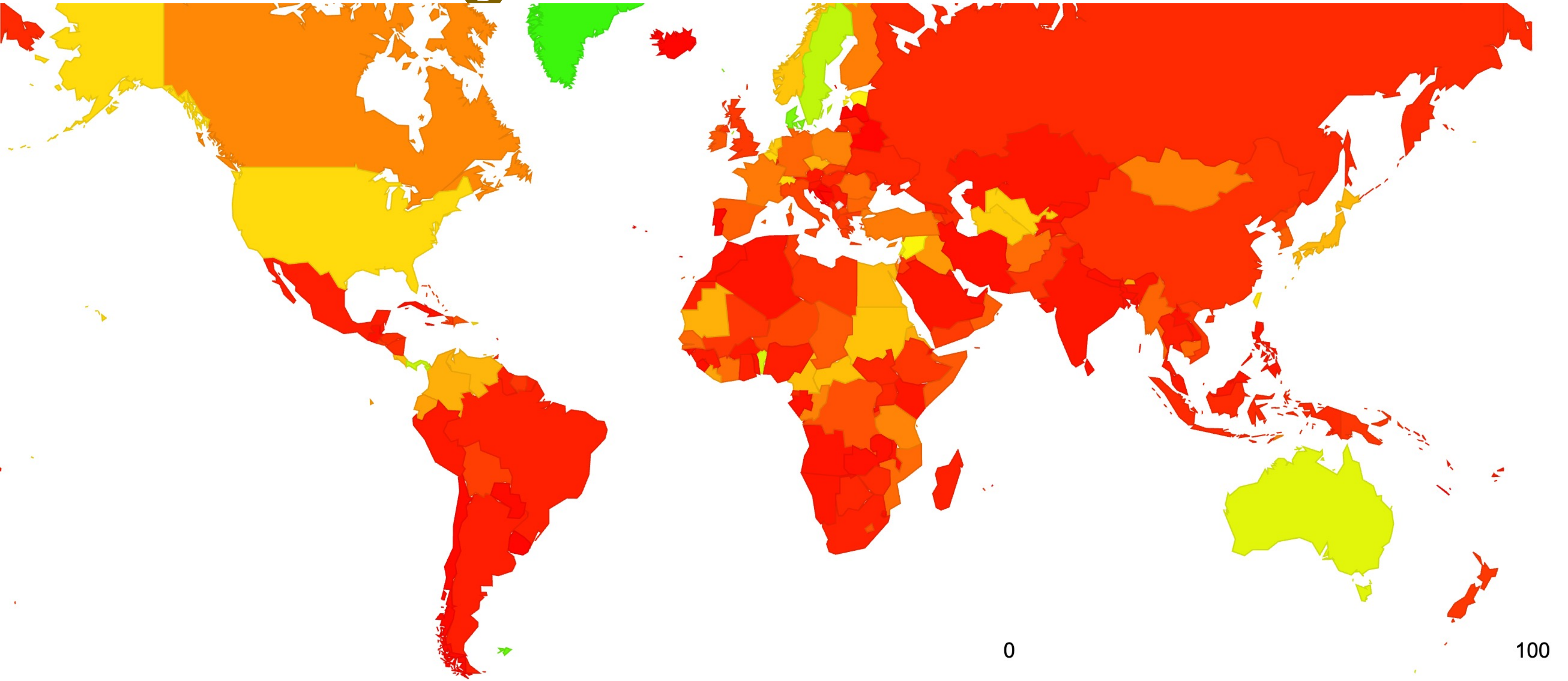
https://stats.labs.apnic.net/rpki

Results: User Impact of ROV filtering - June 2021



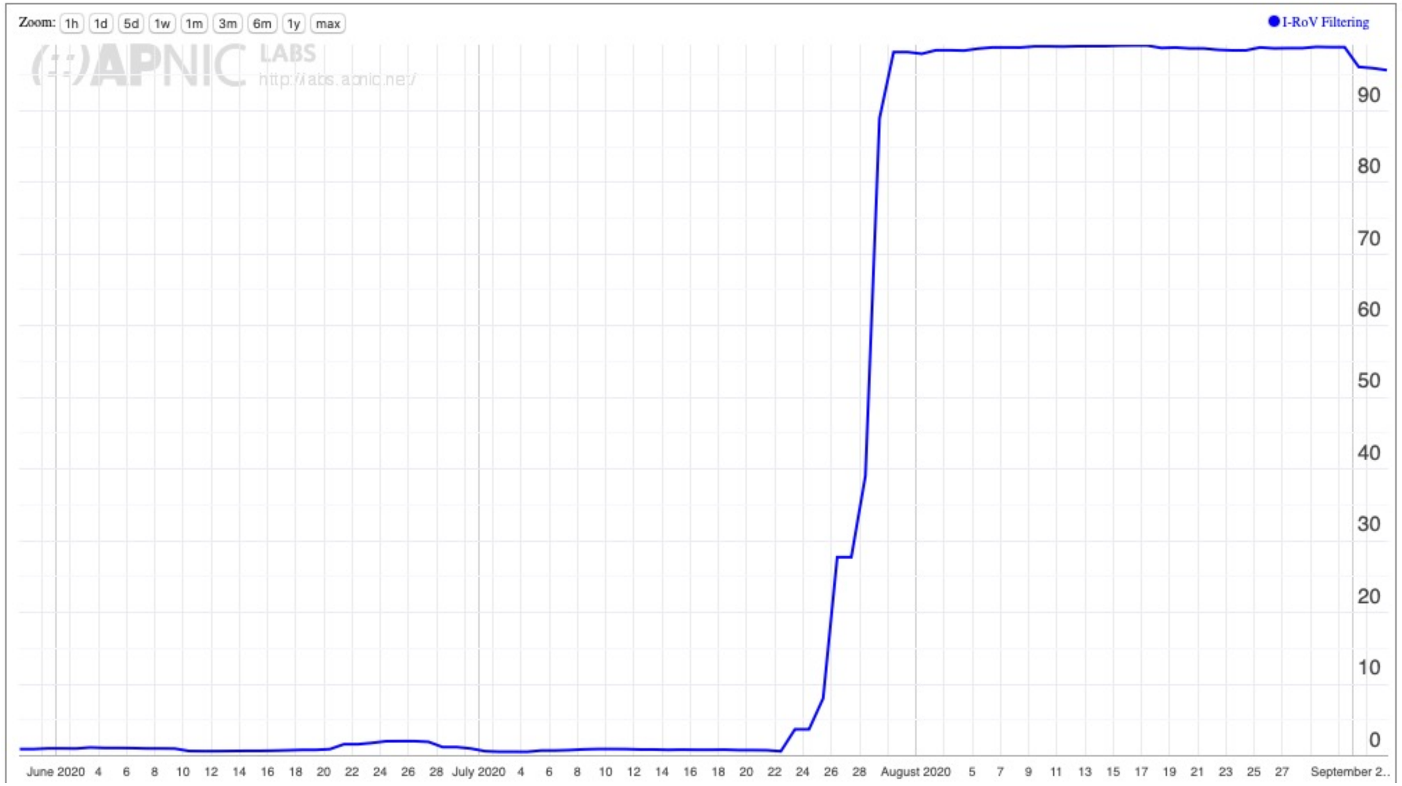
https://stats.labs.apnic.net/rpki

Results: User Impact of ROV filtering - October 2021



Turning on Drop Invalid Filtering

RPKI I-ROV Per-Country filtering for AS1221: ASN-TELSTRA Telstra Corporation Ltd, Australia (AU)

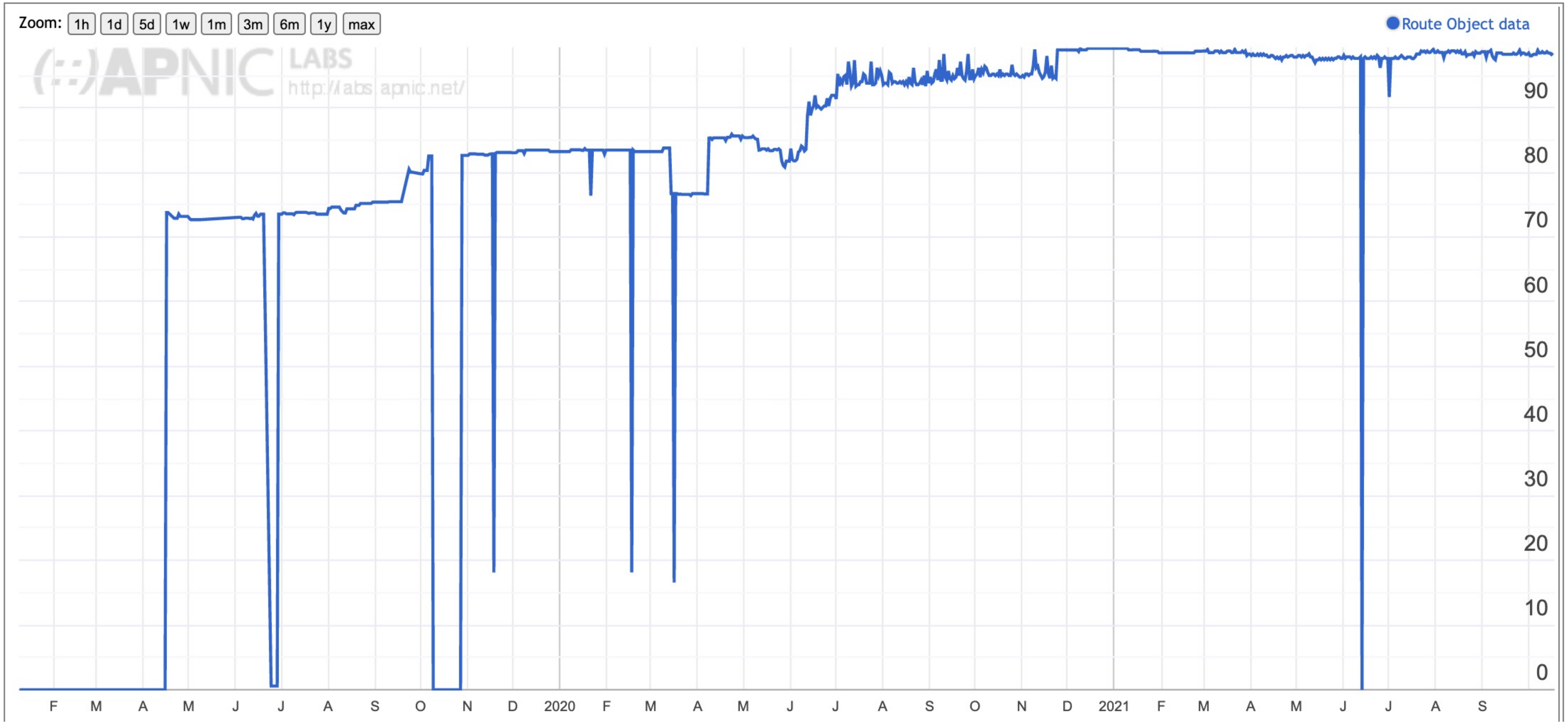


Many operators are reluctant to turn on ROV Filtering

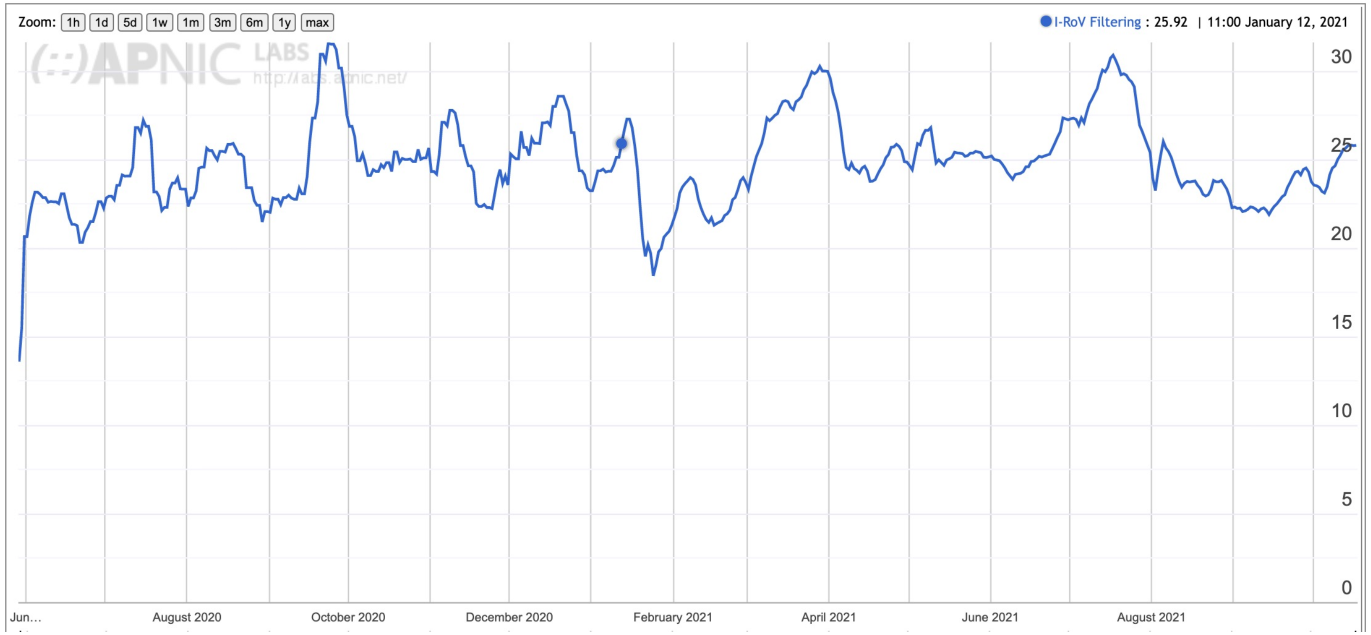
- It appears that generating ROAs for advertised routes has had a good uptake across network operators
- However turning on RoV drop invalid filtering has had had a slower update
- For example, Mongolia has an almost complete set of ROAs for advertised routes, but far less in terms of ROV drop invalid update

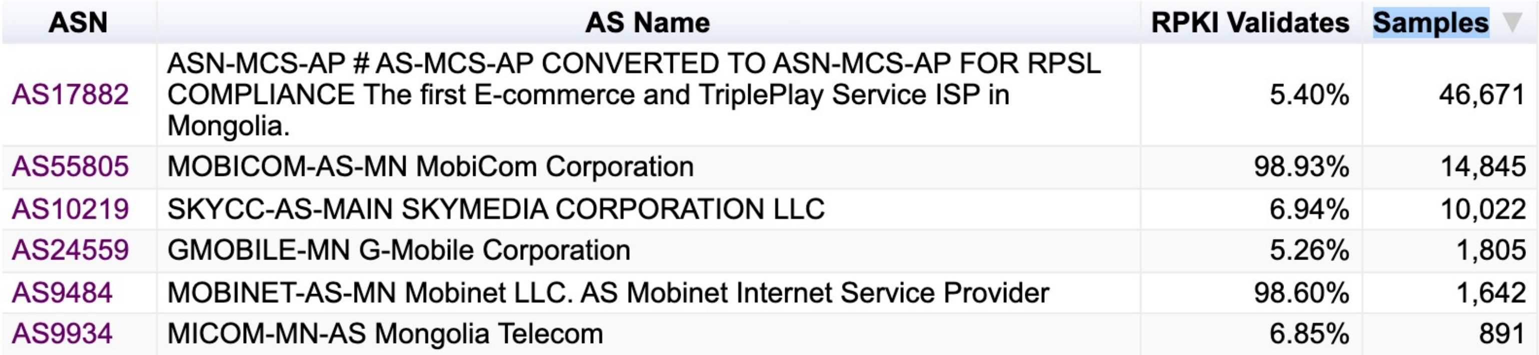
ROAs for networks in Mongolia

Display: **ROAs** (Advertised ROA-Valid Route Advertisements), **IPv4**, **Percent** (of Total)



ROV for networks in Mongolia





ASN	AS Name	RPKI Validates	Samples ▼
AS17882	ASN-MCS-AP # AS-MCS-AP CONVERTED TO ASN-MCS-AP FOR RPSL COMPLIANCE The first E-commerce and TriplePlay Service ISP in Mongolia.	5.40%	46,671
AS55805	MOBICOM-AS-MN MobiCom Corporation	98.93%	14,845
AS10219	SKYCC-AS-MAIN SKYMEDIA CORPORATION LLC	6.94%	10,022
AS24559	GMOBILE-MN G-Mobile Corporation	5.26%	1,805
AS9484	MOBINET-AS-MN Mobinet LLC. AS Mobinet Internet Service Provider	98.60%	1,642
AS9934	MICOM-MN-AS Mongolia Telecom	6.85%	891

Questions we might want to think about

Stub vs Transit

- Is it necessary for every AS to operate RPKI ROV infrastructure and filter invalid routes?
- If not, what’s the minimal set of filtering networks that could provide similar levels of filtering for the Internet as a whole
- What’s the marginal benefit of stub AS performing RPKI ROV filtering?

Questions we might want to think about (2)

Ingress vs Egress

- Should a stub AS RPKI only RoV filter its own announcements?
- Should every AS filter their own announcements?
- What’s more important: Protecting others who DON’T RoV filter from your operational mishaps or protecting yourself from the mishaps of others?
- Does Partial Adoption of ROV filtering change your answer?

Questions we might want to think about (3)

Prefix attestations vs AS attestations

- Should an AS be able to enumerate ALL of its originations in a AS-signed attestation?

Questions we might want to think about (4)

When and how will we protect the AS Path?

- What is going in with the ASPA drafts in the IETF?
- Is anyone experimenting with ASPA yet?

- What is the benefit of Origination protection without AS Path protection?

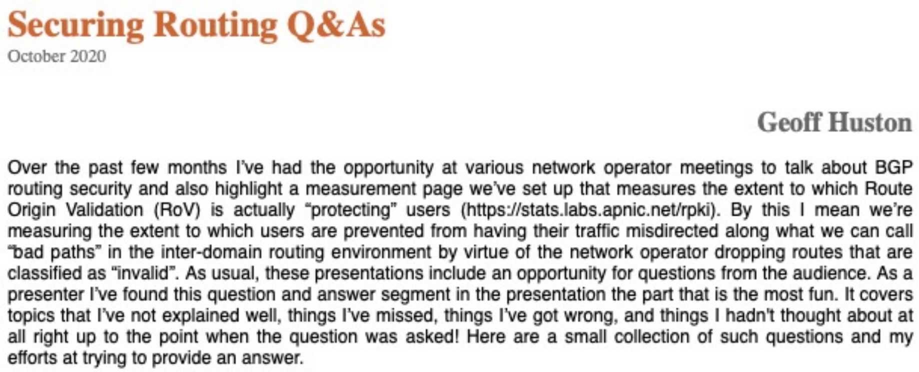
What are we trying to achieve here?

- If this is a routing protection measure then what are you trying to protect? From whom? From what threat?
- If this is guard against operational errors then don’t forget that operational mishaps are endlessly varied, and we can’t foresee all possible causes of routing accidents!
- If this is a user protection measure then the issue of route filtering is an issue for transit providers, not stub networks
  - A stub network should generate ROAs for its routes, but there is far less of an incentive to perform RoV invalid filtering if the stub’s upstreams / IXs are already performing this filtering
  - Is it more important for IXs and Transits to perform drop-invalids than for stubs?

Thanks!

Questions?

See https://www.potaroo.net/ispcol/2020-10/rpkiqa.html



Securing Routing Q&As

October 2020

Geoff Huston

Over the past few months I've had the opportunity at various network operator meetings to talk about BGP routing security and also highlight a measurement page we've set up that measures the extent to which Route Origin Validation (RoV) is actually "protecting" users (https://stats.labs.apnic.net/rpki). By this I mean we're measuring the extent to which users are prevented from having their traffic misdirected along what we can call "bad paths" in the inter-domain routing environment by virtue of the network operator dropping routes that are classified as "invalid". As usual, these presentations include an opportunity for questions from the audience. As a presenter I've found this question and answer segment in the presentation the part that is the most fun. It covers topics that I've not explained well, things I've missed, things I've got wrong, and things I hadn't thought about at all right up to the point when the question was asked! Here are a small collection of such questions and my efforts at trying to provide an answer.