1

RPKI Deployment Status 2022 in review

2

Agenda

- Routing incidents
- RPKI at-a-glance
- ROA and ROV adoption
- Global and APAC stats
- RPKI validators update
- BGP path validation
- RPKI at APNIC

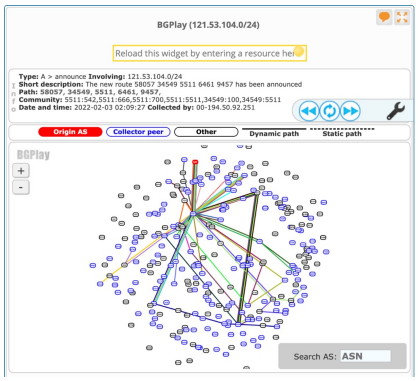
3

Routing Incidents

4

Headlines

- Hackers steal 1.9m worth of crypto currency – **03 Feb 2022**
  - AS38099 (Kakao Corp) hosts KLAYswap on 121.53.104.157
    - AS9457 (Dreamline Co) delegated 121.53.104.0/23 to Kakao Corp
      - It's announced to KINX only
      - **No ROA coverage**
    - Attacker announced **121.53.104.0/24** in global routing table with **AS9457**
      - **AS_PATH:** 40630 6939 **6461 9457**
      - Managed to announce through Zayo
      - Traffic rerouted to hackers' network
      - More detailed analysis: https://www.manrs.org/2022/02/klayswap-another-bgp-hijack-targeting-crypto-wallets/



5

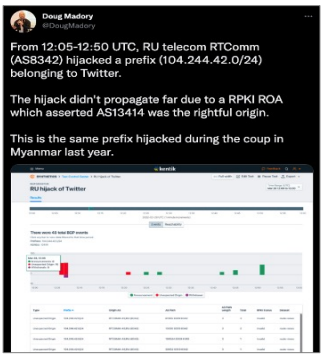
Headlines

- AS8342 attempts to hijack Twitter (AS13414) – **28 Mar 2022**
  - 104.244.42.0/24 advertised to AS12389, AS8920, AS8359, AS25091, AS6939
    - Only AS8359 propagated the announcement, others dropped it
    - Impact was minimized due to Twitter adopting **RPKI ROA**

Covering ROAs:

Trust Anchor	Prefix	Max Length	ASN	Expiration	Match
ARIN	104.244.42.0/24	24	13414	in a year	✓

Validating route **104.244.42.0/24**
from origin **AS8342**
Invalid
1 covering ROA found

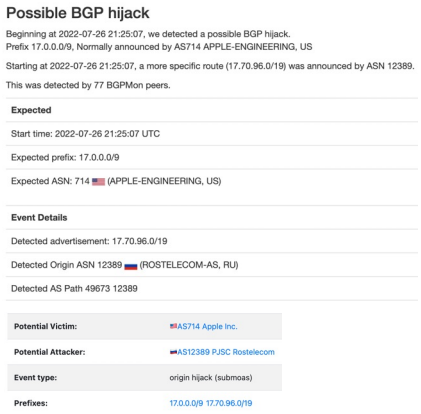


Potential Victim:	AS13414 Twitter Inc.
Potential Attacker:	AS8342 JSC RTComm.RU
Event type:	origin hijack (moas)
Prefixes:	104.244.42.0/24

6

Headlines

- AS12389 hijacks one of the Apple's prefix – **26 Jul 2022**
  - Apple's usual announcement 17.0.0.0/9
    - More specific 17.70.96.0/19 was hijacked
  - Main Upstream leakers
    - AS7473 (Singtel)
    - AS1273 (Vodafone UK)
    - AS4826 (Vocus)
  - Apple announced 17.70.96.0/21 to mitigate
    - Affected for more than 5 hours
    - AS12389 withdrew the announcement after 12+ hours



https://bgpstream.crosswork.cisco.com/event/293915

RPKI at-a-Glance

Route Origin Authorization (ROA)

- Digitally signed object
  - Binds list of prefixes and the nominated ASN
  - *can be verified cryptographically*

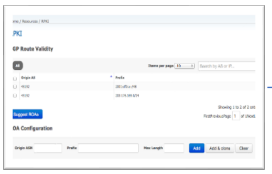
Prefix	2406:6400::/48
Max-length	/48
Origin ASN	**AS17821**

- ** *Multiple ROAs can exist for the same prefix*

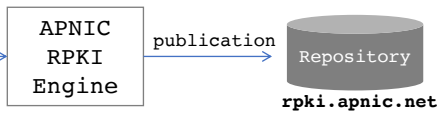
9

RPKI Components

- **Issuing Party** – Internet Registries (*IRs)
  - Certificate Authority (CA) that issues resource certificates to end-holders
  - Publishes the objects (ROAs) signed by the resource certificate holders



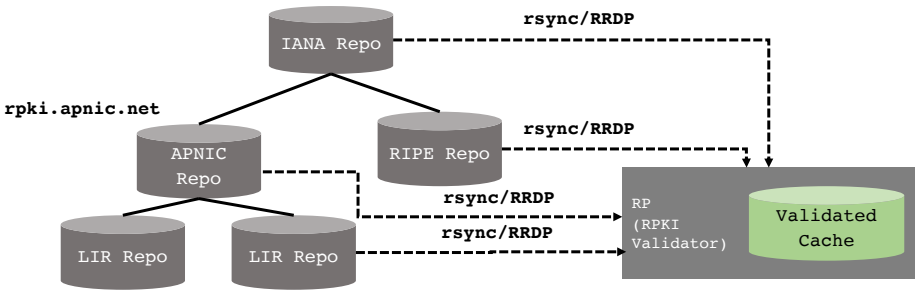
MyAPNIC GUI



10

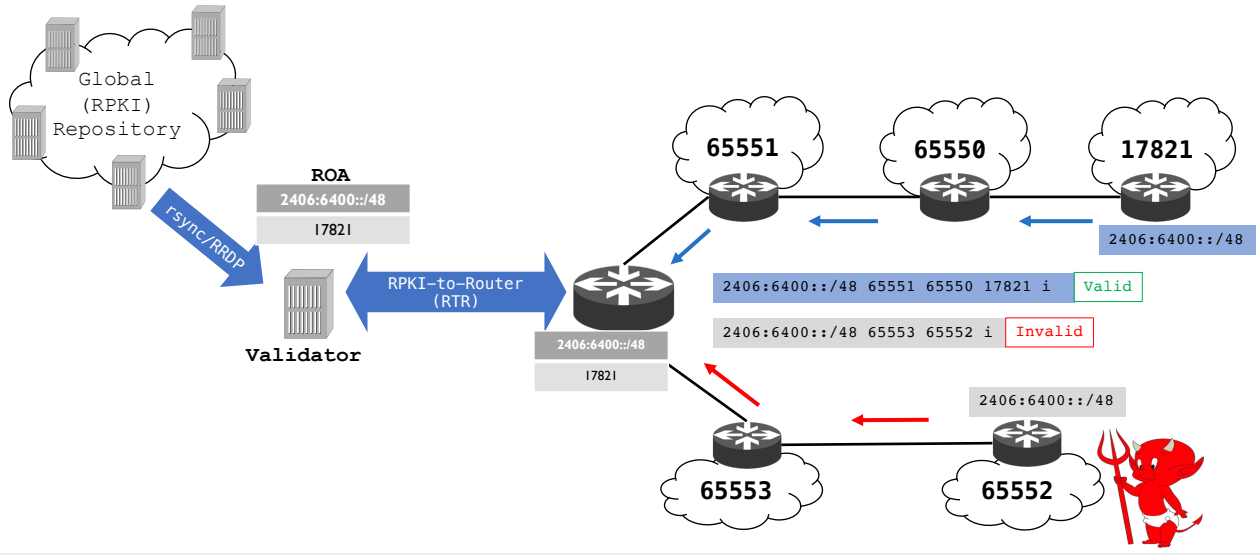
RPKI Components

- **Relying Party (RP)**
  - RPKI Validator that gathers data (ROA) from the distributed RPKI repositories
  - Validates each entry's signature against the TA to build a "*Validated cache*"



11

Route Origin Validation (ROV)



12

RPKI Validation States

ROA

ASN	Prefix	Max Length
65420	10.0.0.0/16	18

BGP Routes

ASN	Prefix	RPKI State
65420	10.0.0.0/16	VALID
65420	10.0.128.0/17	VALID
65421	10.0.0.0/16	INVALID
65420	10.0.10.0/24	INVALID
65430	10.0.0.0/8	NOT FOUND

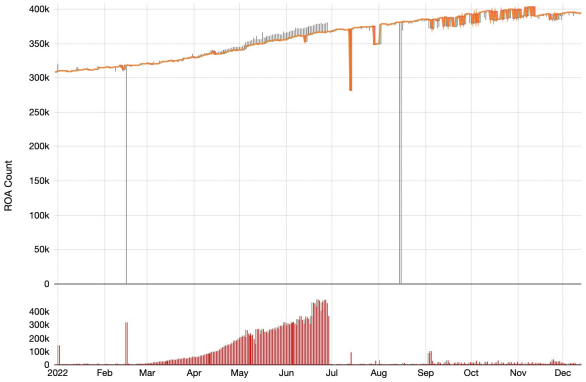
13

RPKI Deployment Status

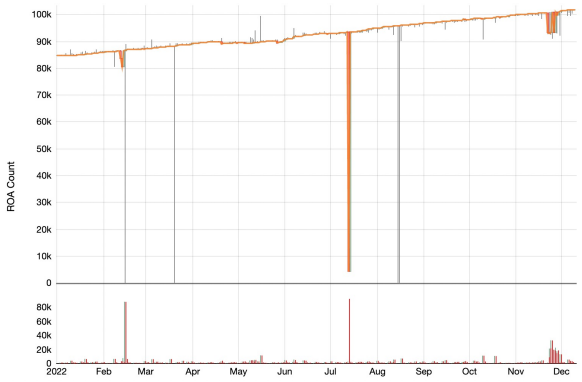
14

RPKI ROA Adoption – Number of ROAs

Global



APAC



https://rpki.cloudflare.com/?view=statistics

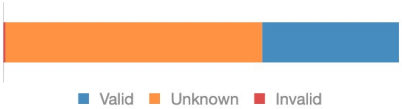
15

RPKI ROA Adoption - Global

Dec 2021

Routing completeness (RPKI)

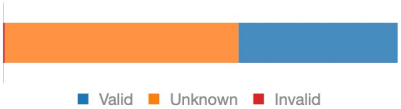
Valid	372,259	34.6%
Unknown	697,573	64.9%
Invalid	4,883	0.5%



Dec 2022

Routing completeness (RPKI)

Valid	455,921	40.3%
Unknown	669,192	59.2%
Invalid	5,822	0.5%



https://observatory.manrs.org/

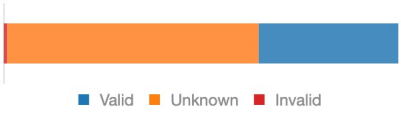
16

RPKI ROA Adoption - APAC

Dec 2021

Routing completeness (RPKI)

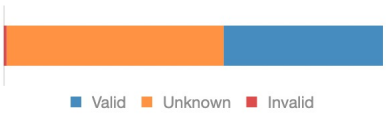
Valid	102,640	35.4%
Unknown	184,517	63.7%
Invalid	2,716	0.9%



Dec 2022

Routing completeness (RPKI)

Valid	129,690	42.0%
Unknown	176,904	57.2%
Invalid	2,510	0.8%

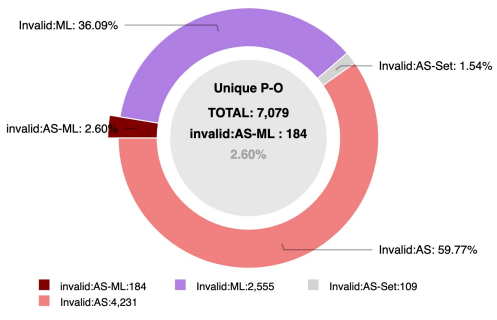


https://observatory.manrs.org/

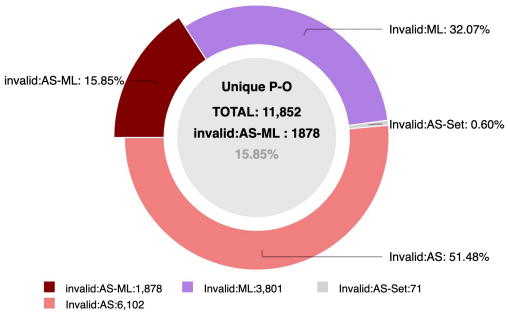
17

RPKI ROA Adoption – Global INVALIDs (IPv4)

Dec 2021



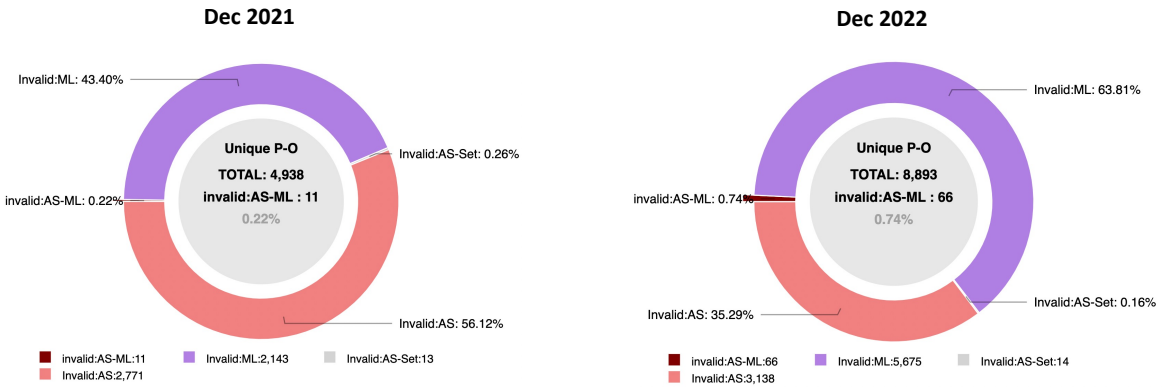
Dec 2022



https://rpki-monitor.antd.nist.gov/Inv

18

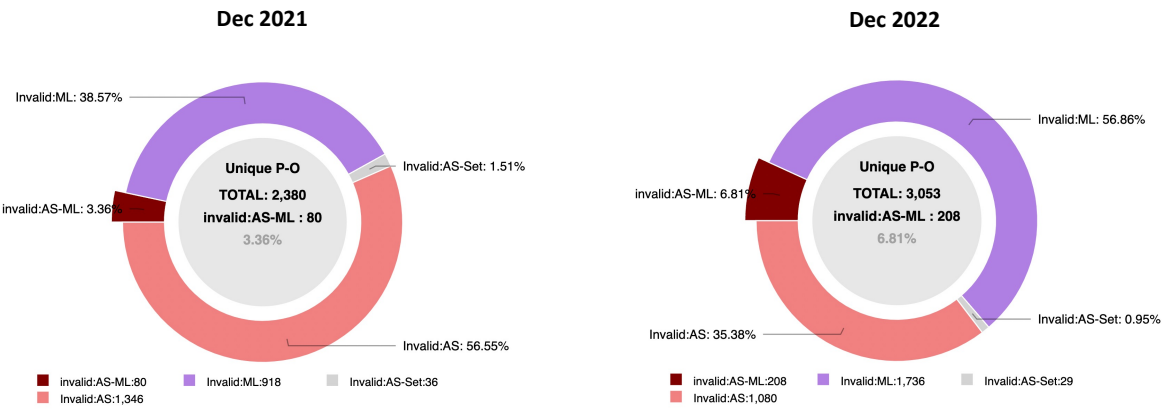
RPKI ROA Adoption – Global INVALIDs (IPv6)



https://rpki-monitor.antd.nist.gov/Inv

19

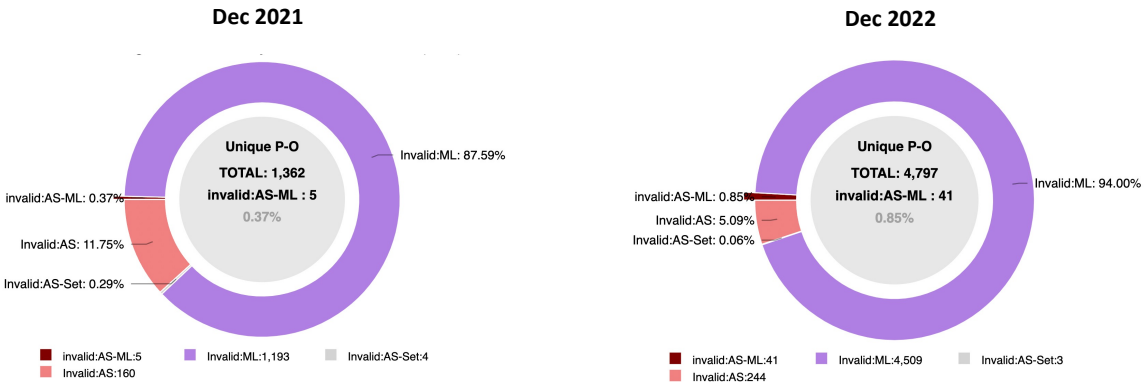
RPKI ROA Adoption – APAC INVALIDs (IPv4)



https://rpki-monitor.antd.nist.gov/Inv

20

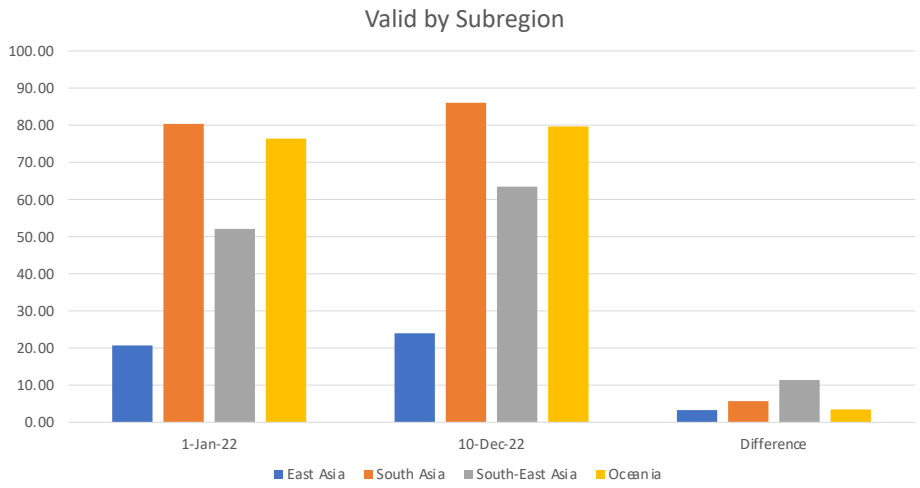
RPKI ROA Adoption – APAC INVALIDs (IPv6)



https://rpki-monitor.antd.nist.gov/Inv

21

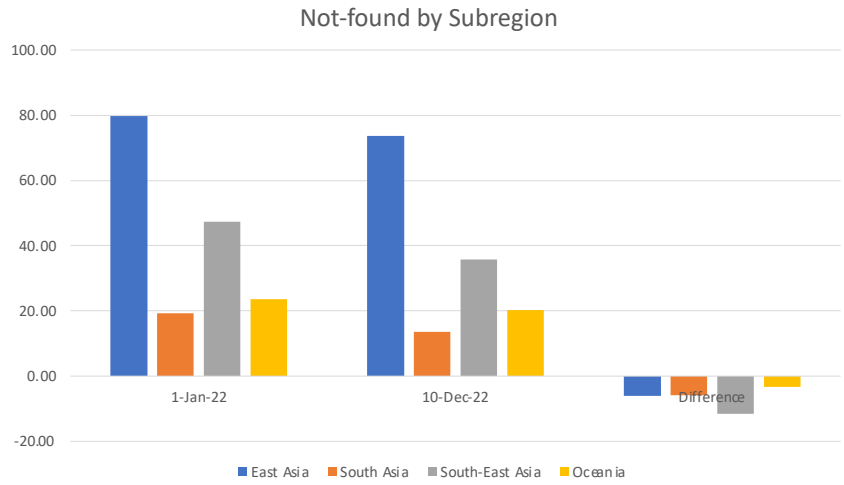
RPKI Valid ROA by Subregions



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

22

RPKI Not-Found ROA by Subregions

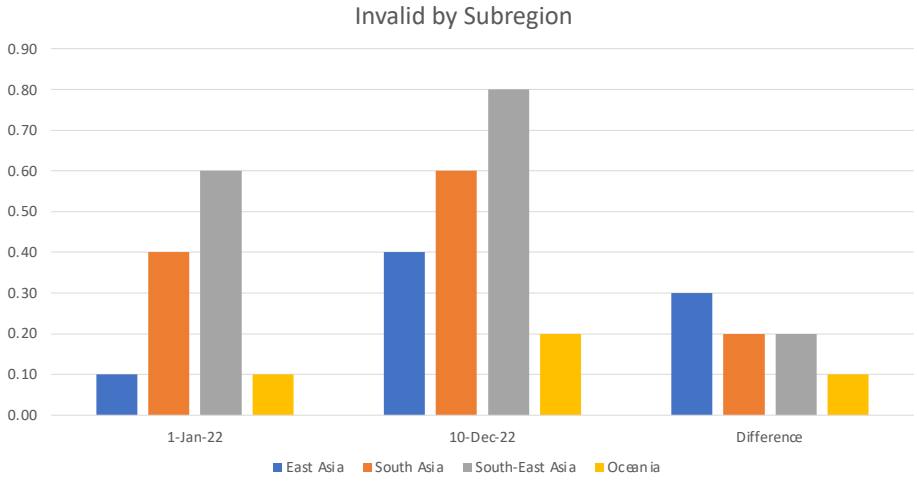


https://stats.labs.apnic.net/roa

APNIC 23

23

RPKI Invalid ROA by Subregions

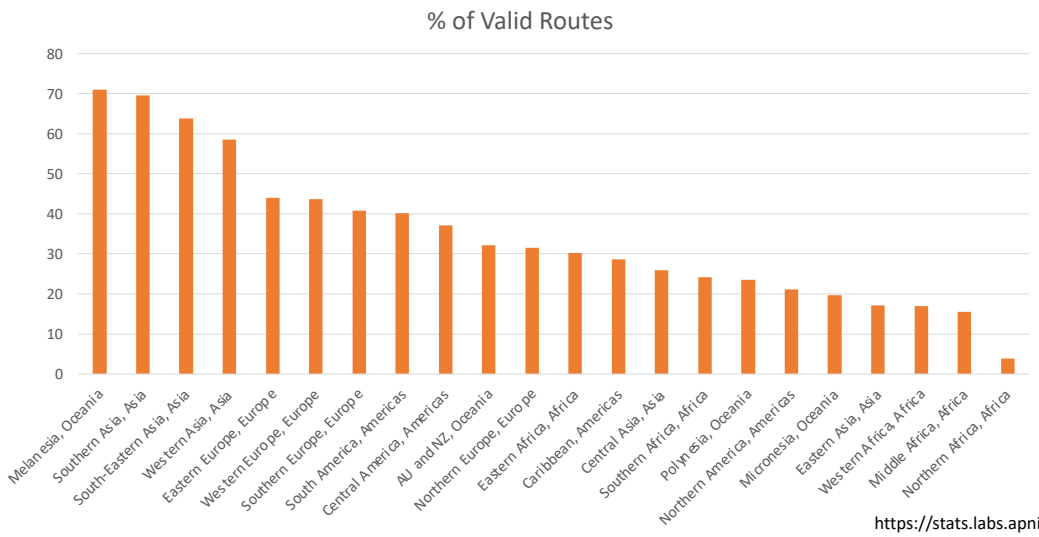


https://stats.labs.apnic.net/roa

APNIC 24

24

RPKI: Global Leaderboard



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

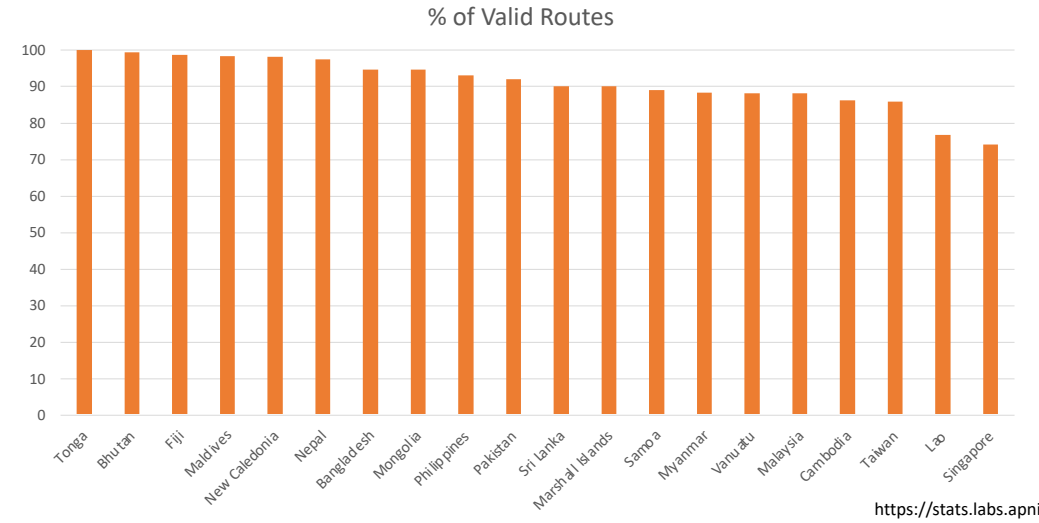
APNIC

25

v1.0

25

RPKI: APAC Top 20



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

APNIC

26

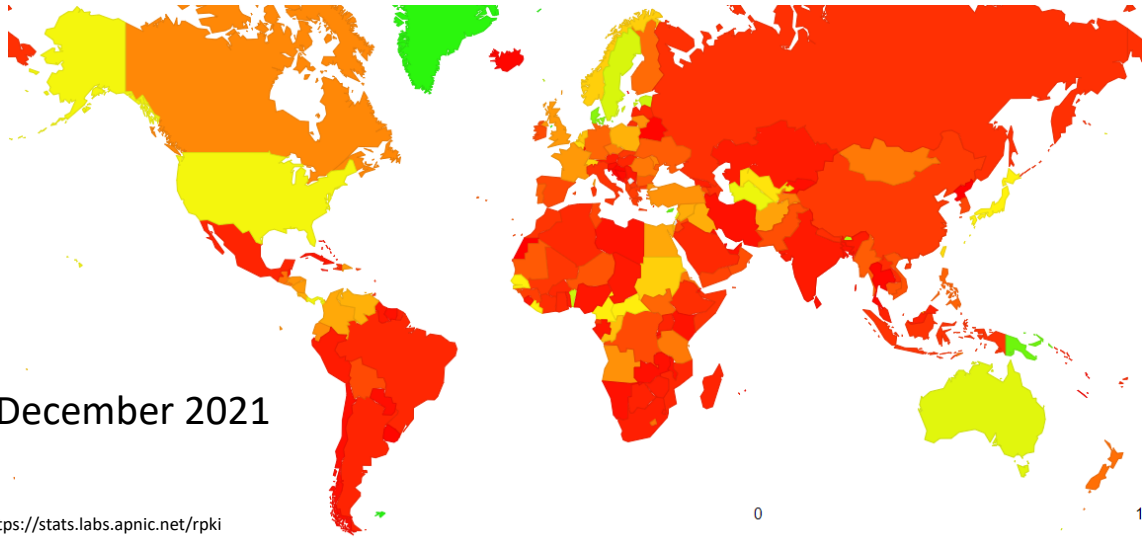
v1.0

26

Route Origin Validation

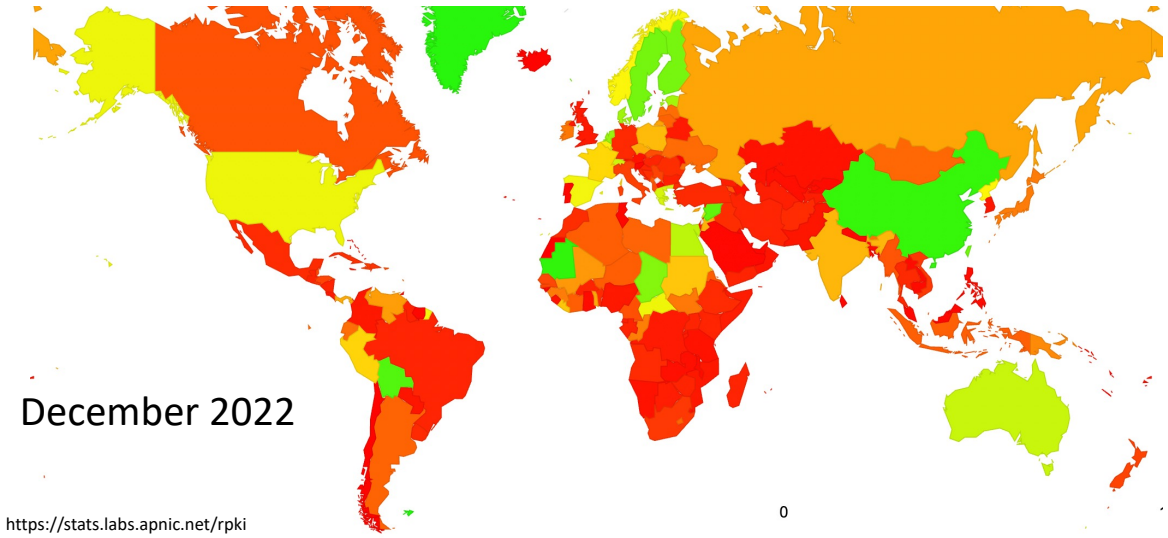
27

Origin Validation



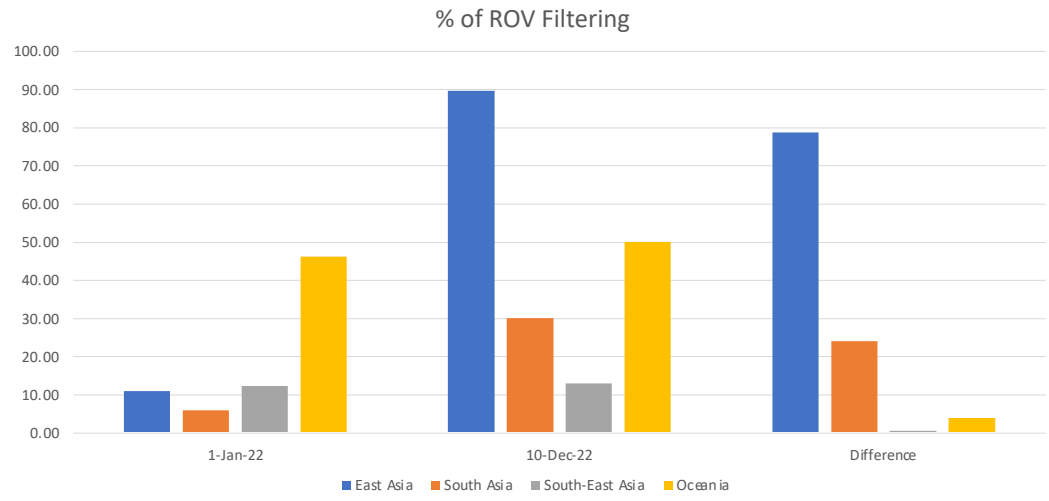
28

Origin Validation



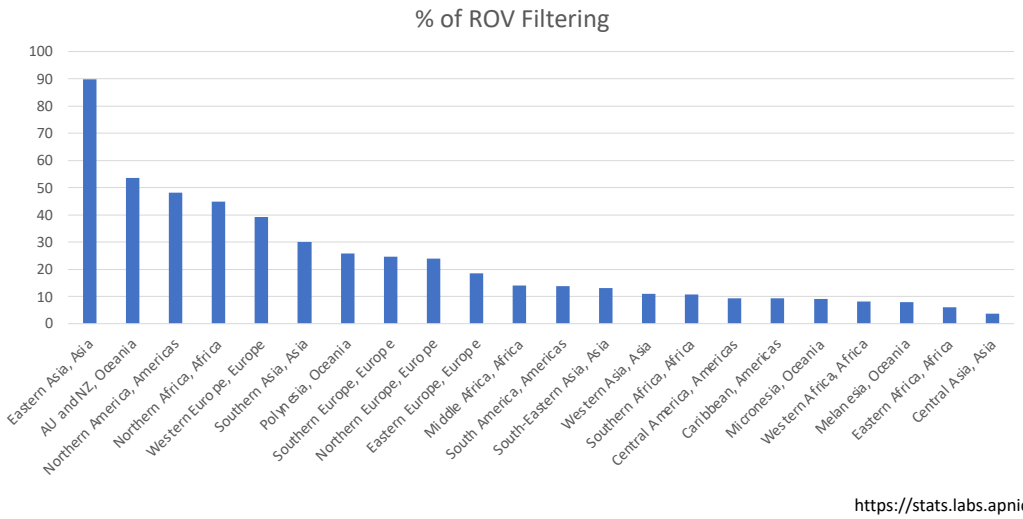
29

Origin Validation by Subregion



30

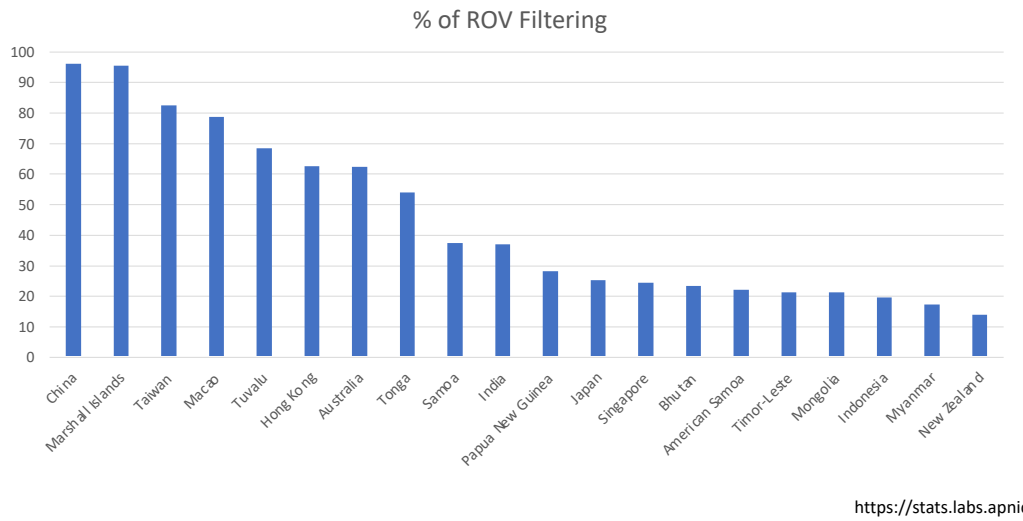
Origin Validation: Global Leaderboard



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

31

Origin Validation: APAC Top 20

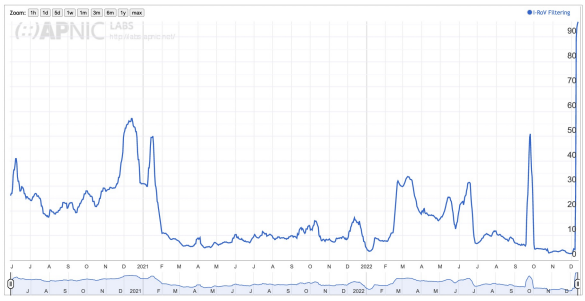


https://stats.labs.apnic.net/rpki

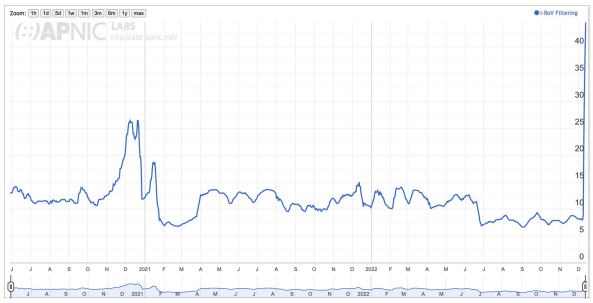
32

Origin Validation: China

Use of RPKI Validation for China (CN)



Use of RPKI Validation for Asia (XD)

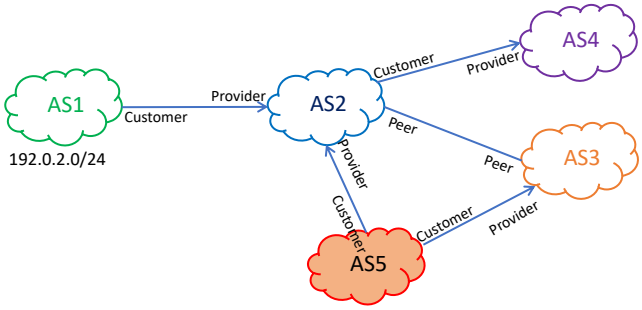


https://stats.labs.apnic.net/rpki

RPKI and Path Validation

AS Path Validation – ASPA

- Each AS creates and signs an **aspa-object** to authorize its provider ASs
  - Similar to a ROA, its an "authority" to propagate a route



AS1 aspa-object: Providers AS2

AS2 aspa-object: Providers AS4

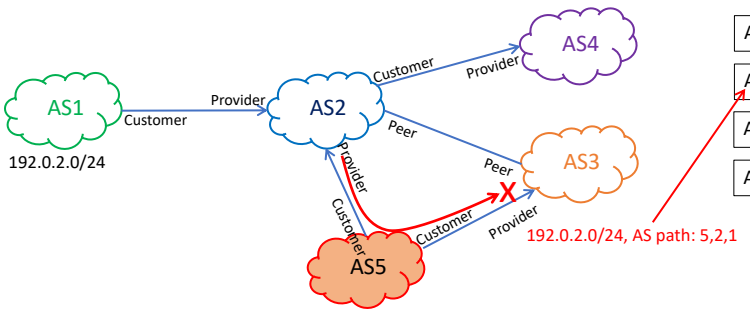
AS3 aspa-object: Providers AS2

AS5 aspa-object: Providers AS2, AS3

35

AS Path Validation – ASPA

- If AS5 leaks a route learned from AS 2 to AS 3, AS3 can detect this leak if it verifies the aspa-object, i.e. the customer and provider relationship



AS1 aspa-object: Providers AS2

AS2 aspa-object: Providers AS4

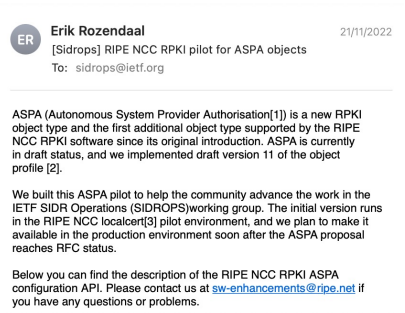
AS3 aspa-object: Providers AS2

AS5 aspa-object: Providers AS2, AS3

36

AS Path Validation – ASPA

- RIPE NCC starts ASPA pilot
  - Follow SIDROPS ML for updates
    - https://www.ietf.org/mailman/listinfo/sidrops
  - aspa-objects on test:
    - AS 970 - https://console.rpki-client.org/rpki-rps.arin.net/repository/8a848adf8143bf6201823bd454752be6/0/AS970.asa.html
    - AS 21957 - https://console.rpki-client.org/rpki-rps.arin.net/repository/8a848adf8143bf6201823bd454752be6/0/AS21957.asa.html
    - AS 15562 - https://console.rpki-client.org/chloe.sobornost.net/rpki/RIPE-nljobsnijders/VCIb3NxttGlL0VzKekHcAGpU9Ls.asa.html



ER **Erik Rozendaal** 21/11/2022

[Sidrops] RIPE NCC RPKI pilot for ASPA objects

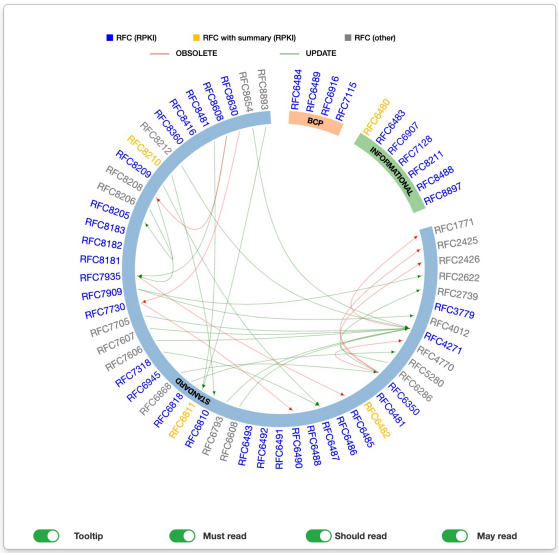
To: sidrops@ietf.org

ASPA (Autonomous System Provider Authorisation[1]) is a new RPKI object type and the first additional object type supported by the RIPE NCC RPKI software since its original introduction. ASPA is currently in draft status, and we implemented draft version 11 of the object profile [2].

We built this ASPA pilot to help the community advance the work in the IETF SIDR Operations (SIDROPS)working group. The initial version runs in the RIPE NCC localcert[3] pilot environment, and we plan to make it available in the production environment soon after the ASPA proposal reaches RFC status.

Below you can find the description of the RIPE NCC RPKI ASPA configuration API. Please contact us at sw-enhancements@ripe.net if you have any questions or problems.

RPKI RFCs



https://rpki-rfc.routingsecurity.net/

RPKI Validators

39

RPKI Validators Update

- Routinator: 0.11 → 0.12
- OctoRPKI: 1.4.3 → 1.4.4
- rpki-client: 7.8 → 8.0
- rpki-prover: 0.3 → 0.5
- Fort: 1.5.3
- RPSTIR2

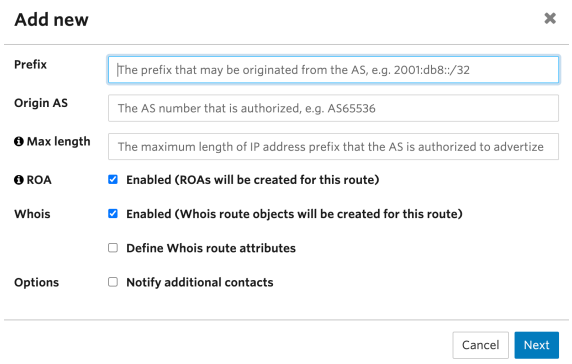
40

RPKI at APNIC

41

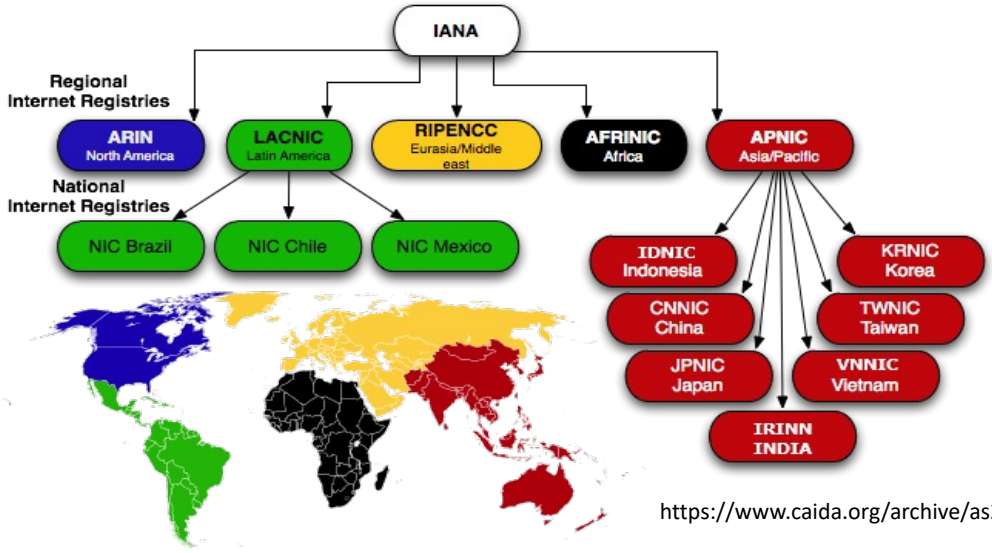
RPKI: APNIC Portal

- New MyAPNIC portal
  - Helpful information added while ROAs to be created



42

RPKI: Chain of Trust



https://www.caida.org/archive/as2org/

43

RPKI: Historic Resources

- APNIC51 (22/02/2021)
  - RPKI available for historic resources
  - No fees if joined by Jan 2023
- Further questions?
  - Contact the helpdesk
  - https://help.apnic.net/s/contactsupport
  - helpdesk@apnic.net

https://blog.apnic.net/2021/03/26/rpki-services-now-available-to-apnic-historical-resource-holders/

44

https://www.apnic.net/community/security/resource-certification/#routing

45

Any questions?

46

47