

Tackling Routing Security

One step at a time

Aftab Siddiqui

siddiqui@isoc.org

@aftabsiddiqui

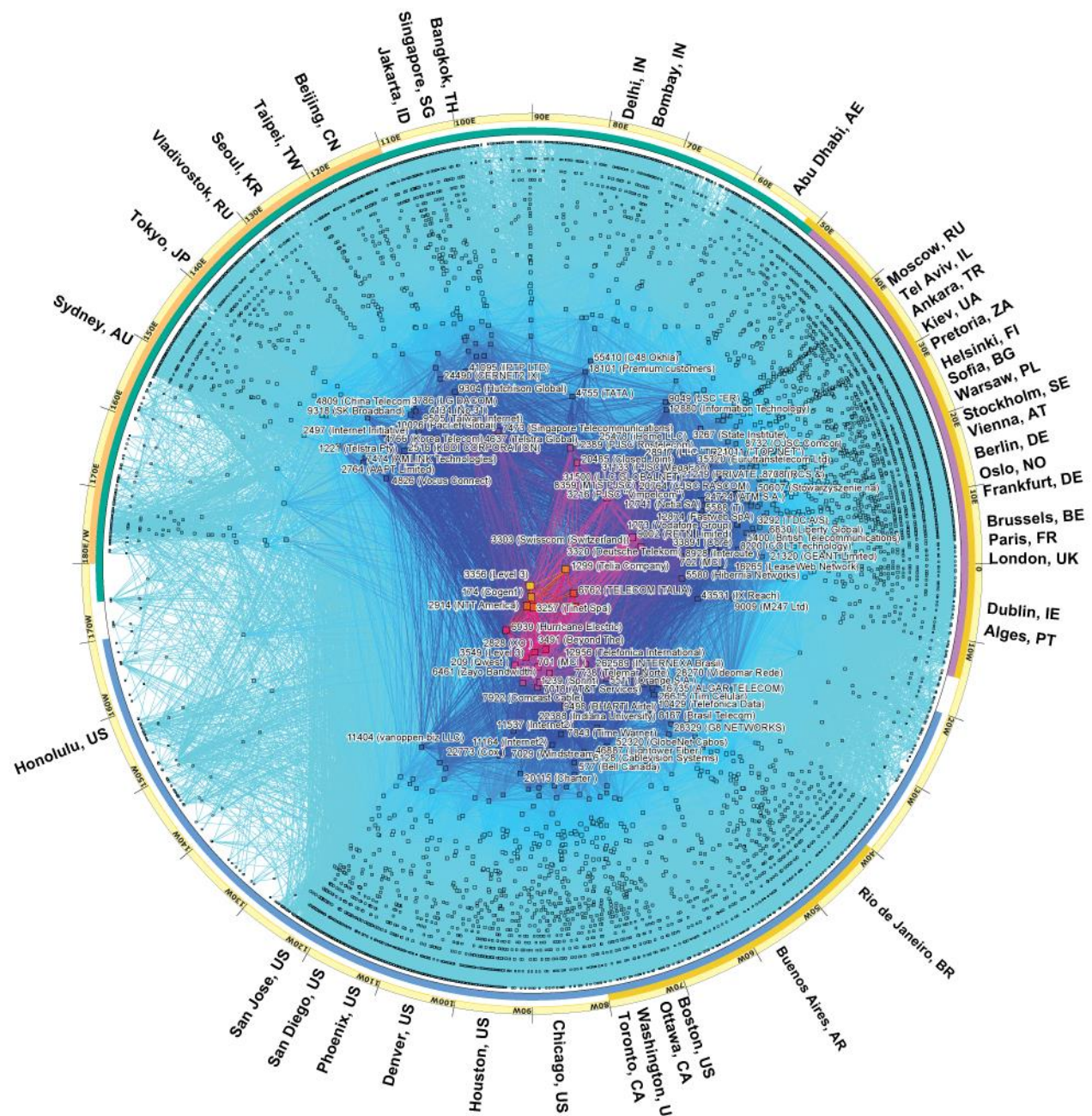


Global Routing System Overview

(as of 25 June 2023)

74,590 networks known as Autonomous Systems are connected to the Internet, each using a unique Autonomous System Number (ASN) for identification.

939,462 (v4) and 180,299 (v6) advertised IP prefixes (routes).



Before You Connect – Routing Etiquette



There are certain formal routing etiquettes which every network operator should follow, for example make sure:

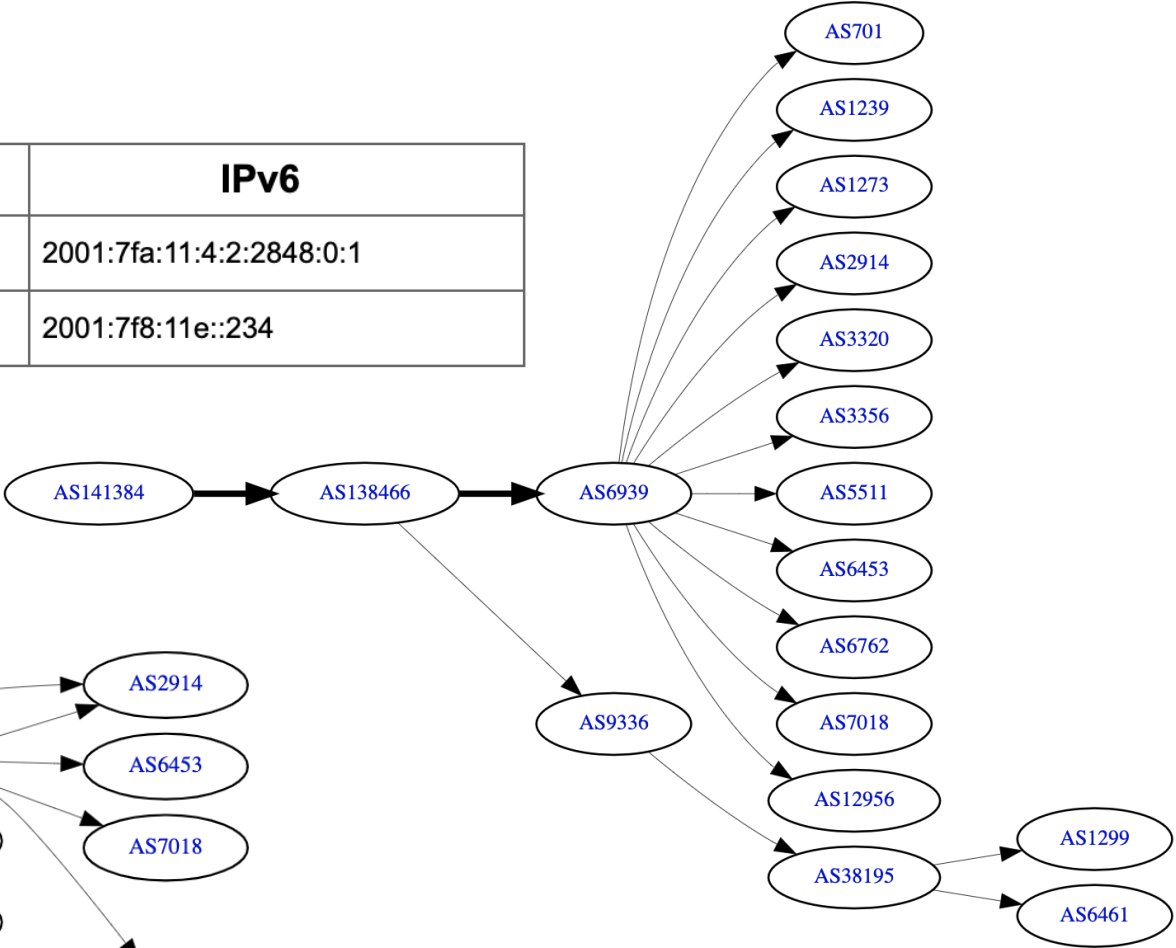
- **All route objects** exist in the **IRR** database of your respective RIR (APNIC). Create AS-SET if required with correct downstream customers.
- Route Origin Authorisation (**ROA**) is created for all the routes you wish to advertise from your network (ASN).
- To check for any stale or old route objects in un-authenticated IRR databases such as RADb, ALTDB etc.
- To add details of your network and peering details in **PeeringDB**.



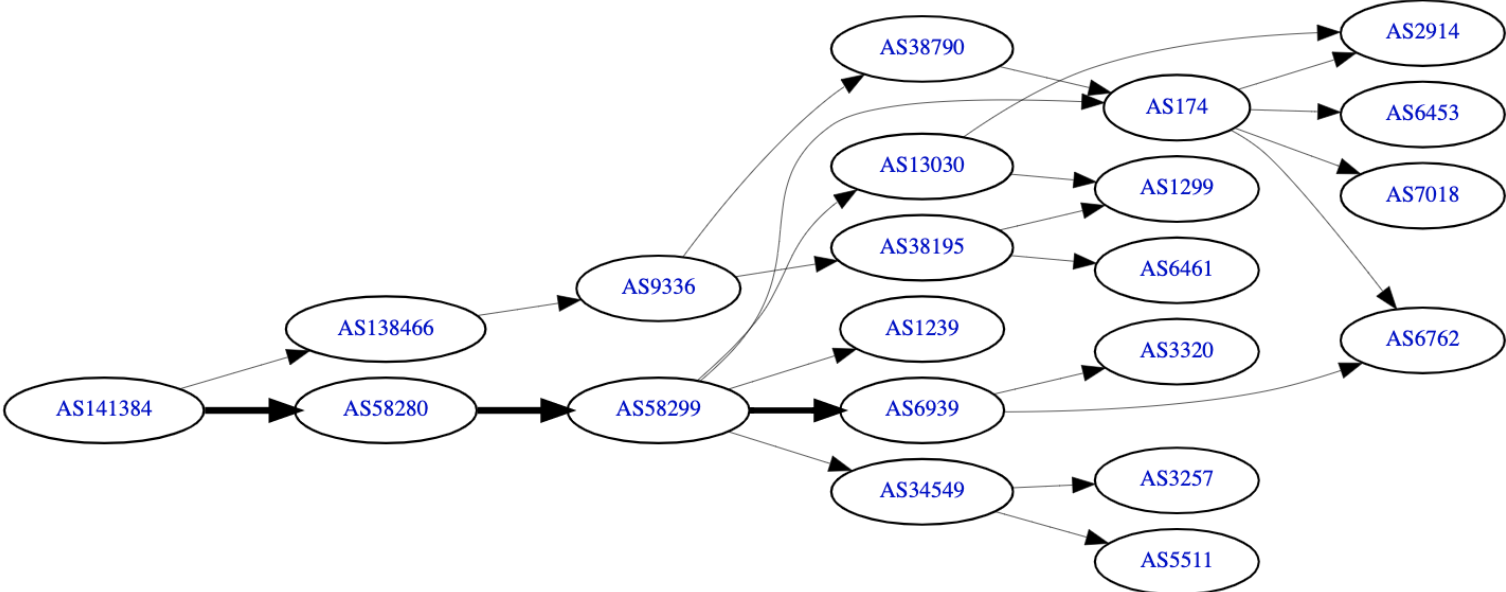
ISOC - Network Connectivity

AS141384 IPv6 Route Propagation

Exchange	CC	City	IPv4	IPv6	
<u>IX Australia NSW</u>		AU	Sydney	218.100.53.78	2001:7fa:11:4:2:2848:0:1
<u>IXP.ge</u>		GE	Tbilisi	185.1.224.234	2001:7f8:11e::234



AS141384 IPv4 Route Propagation



ISOC - Network Resources – Route Objects

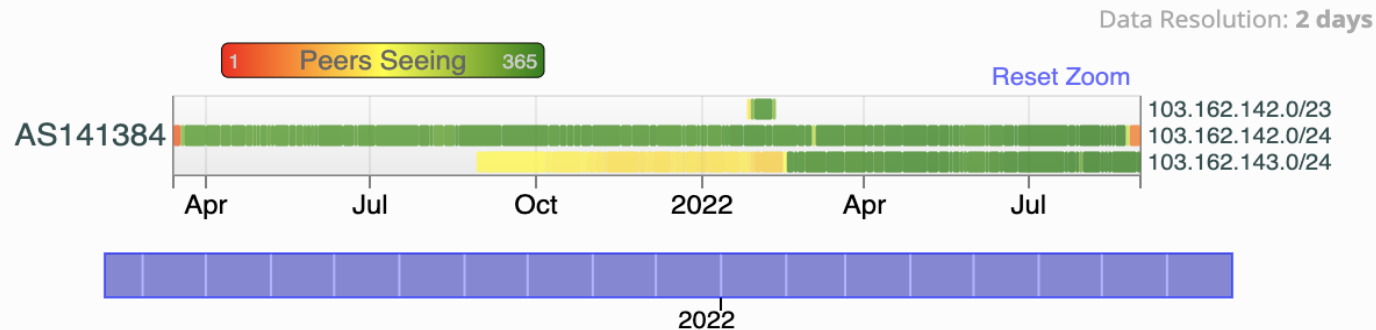
```
inetnum:      103.162.142.0 - 103.162.143.255
netname:      ISAL-SG
descr:        Internet Society Asia Limited
descr:        3 Temasek Avenue Level 21 Centennial Tower
country:      SG
org:          ORG-ISAL1-AP
admin-c:      ISAL1-AP
tech-c:       ISAL1-AP
abuse-c:      AI706-AP
status:       ASSIGNED PORTABLE
remarks:      -----
remarks:      To report network abuse, please contact mnt-irt
remarks:      For troubleshooting, please contact tech-c and admin-c
remarks:      Report invalid contact via www.apnic.net/invalidcontact
remarks:      -----
mnt-by:       APNIC-HM
mnt-routes:   MAINT-ISAL-SG
mnt-irt:      IRT-ISAL-SG
last-modified: 2021-02-05T03:52:16Z
source:       APNIC
```

```
% Information related to '103.162.142.0/24AS141384'

route:        103.162.142.0/24
origin:       AS141384
descr:        Internet Society Asia Limited
              3 Temasek Avenue Level 21 Centennial Tower
mnt-by:       MAINT-ISAL-SG
last-modified: 2022-02-10T02:19:58Z
source:       APNIC
```

```
% Information related to '103.162.143.0/24AS141384'

route:        103.162.143.0/24
origin:       AS141384
descr:        Internet Society Asia Limited
              3 Temasek Avenue Level 21 Centennial Tower
mnt-by:       MAINT-ISAL-SG
last-modified: 2022-01-27T10:06:57Z
source:       APNIC
```



ISOC - Network Resources - ROA

Validating route **103.162.142.0/24**

from origin **AS141384**

✓ **Valid**

2 covering ROAs found

Covering ROAs:

Trust Anchor	Prefix	Max Length	ASN	Expiration	Match
APNIC	103.162.142.0/24	24	141384	in a year	✓
APNIC	103.162.142.0/24	24	139038	in a year	✗

Validating route **103.162.143.0/24**

from origin **AS141384**

✓ **Valid**

1 covering ROA found

Covering ROAs:

Trust Anchor	Prefix	Max Length	ASN	Expiration	Match
APNIC	103.162.143.0/24	24	141384	in a year	✓



PeeringDB

ISOC Research Network

Gold Sponsor

Edit

Organization	Internet Society
Also Known As	
Long Name	
Company Website	http://www.internetsociety.org
Twitter	internetsociety
ASN	141384
IRR as-set/route-set ?	AS141384:AS-ISOC
Route Server URL	
Looking Glass URL	
Network Type	Non-Profit
IPv4 Prefixes ?	3
IPv6 Prefixes ?	3
Traffic Levels	20-100Mbps
Traffic Ratios	Balanced
Geographic Scope	Global
Protocols Supported	<input checked="" type="checkbox"/> Unicast IPv4 <input type="checkbox"/> Multicast <input checked="" type="checkbox"/> IPv6 <input type="checkbox"/> Never via route servers ?

Public Peering Exchange Points

Filter

Exchange ↓ [#] IPv4	ASN IPv6	Speed	RS Peer
IX Australia (Sydney NSW) 218.100.53.78	141384 2001:7fa:11:4:2:2848:0:1	10G	<input checked="" type="checkbox"/>
IXP.ge 185.1.224.234	141384 2001:7f8:11e::234	1G	<input checked="" type="checkbox"/>

Interconnection Facilities

Filter

Facility ↓ [#] ASN	Country City
Equinix SY4 - Sydney 141384	Australia Sydney
NTT Zurich 1 Data Center (ZRH1) 141384	Switzerland Rümlang

The Problem

Network operators must publicly document their intended routing announcements in the appropriate RIR routing registry or create ROAs. This includes ASNs and IP prefixes originating on their own networks, as well as the networks for which they provide transit services.

Let's see how Viet Nam networks perform for RPKI and Route Objects?

Help me, help you!



Reminder – IRR is an Honor System:

The IRR ecosystem is massive, RIRs provide authenticated IRR services whereas outside RIR jurisdiction there are multiple IRR databases such as RADb

- There is no system to validate whether these objects are legitimate
- Lack of reliability of data because of stale objects



Let's Investigate!

We decided to find out who is updating these objects in RADb

- Comparing RIR delegation file with RADb
- Selecting All ASN delegated to VN
- All data is publicly available for further review
 - Types
 - Status 1: Exact → Route object for exact allocation
 - Status 1: More Specific – Route Object for More Specifics
 - Status 3: More Specific - Route Object for Only More Specifics



<http://103.162.143.30/route-check/data/>

APNIC Resource Status

- As per the APNIC delegation file 1.0.4.0/22 was allocated in 20110412.
- In RADb, there are 4 route objects of “Exact” match

apnic | AU | ipv4 | 1.0.4.0 | 1024 | 20110412 | allocated

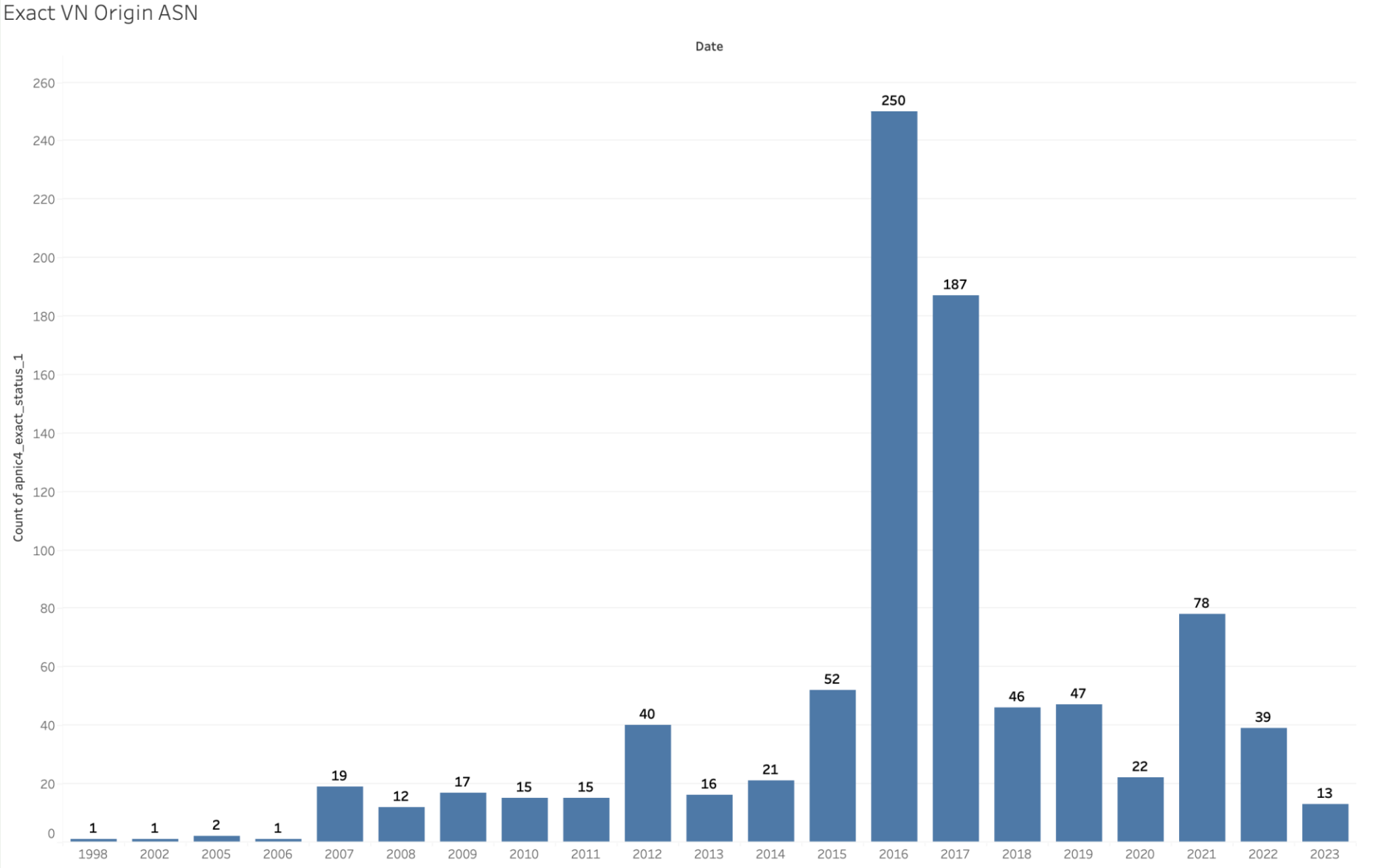
<http://ftp.apnic.net/apnic/stats/apnic/delegated-apnic-latest>



```
[
{
  "descr": "(139763)",
  "origin": "AS56203",
  "mnt": "MAINT-AS2764",
  "last-modified": "nobody@connect.com.au 20120207",
  "source": "RADB",
  "prefix": "1.0.4.0/22"
},
{
  "descr": "Proxy route object registered by AS2764",
  "origin": "AS24130",
  "mnt": "MAINT-AS2764",
  "last-modified": "nobody@aapt.com.au 20130219",
  "source": "RADB",
  "prefix": "1.0.4.0/22"
},
{
  "descr": "Proxy route object registered by AS2764",
  "origin": "AS7545",
  "mnt": "MAINT-AS2764",
  "last-modified": "nobody@aapt.com.au 20130628",
  "source": "RADB",
  "prefix": "1.0.4.0/22"
},
{
  "descr": "Proxy route object registered by AS2764",
  "origin": "AS38803",
  "mnt": "MAINT-AS2764",
  "last-modified": "nobody@aapt.com.au 20210701",
  "source": "RADB",
  "prefix": "1.0.4.0/22"
}
]
```

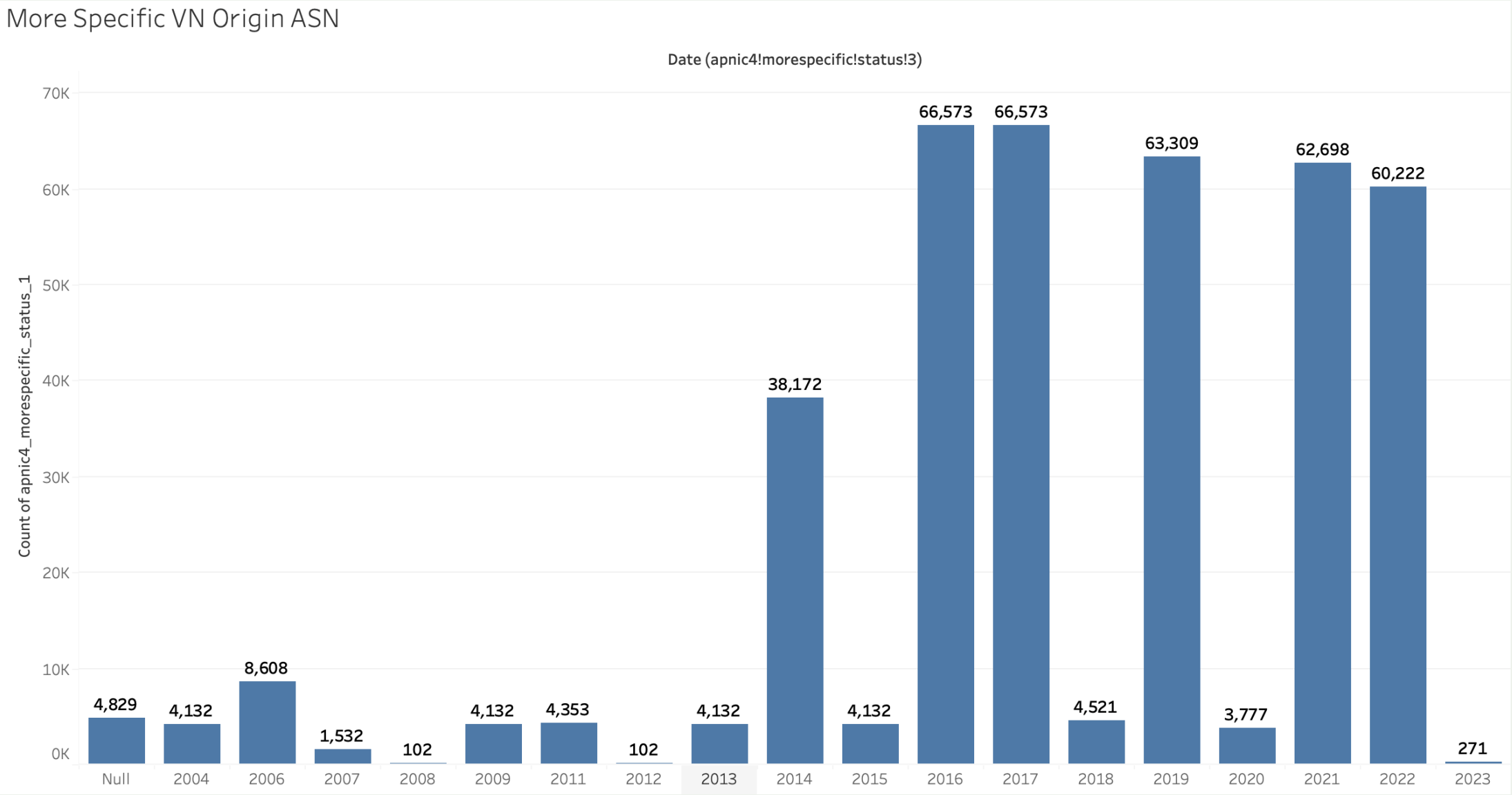
VN IPv4 Resource Status

Status: 1 Type: Exact Match



VN IPv4 Resource Status

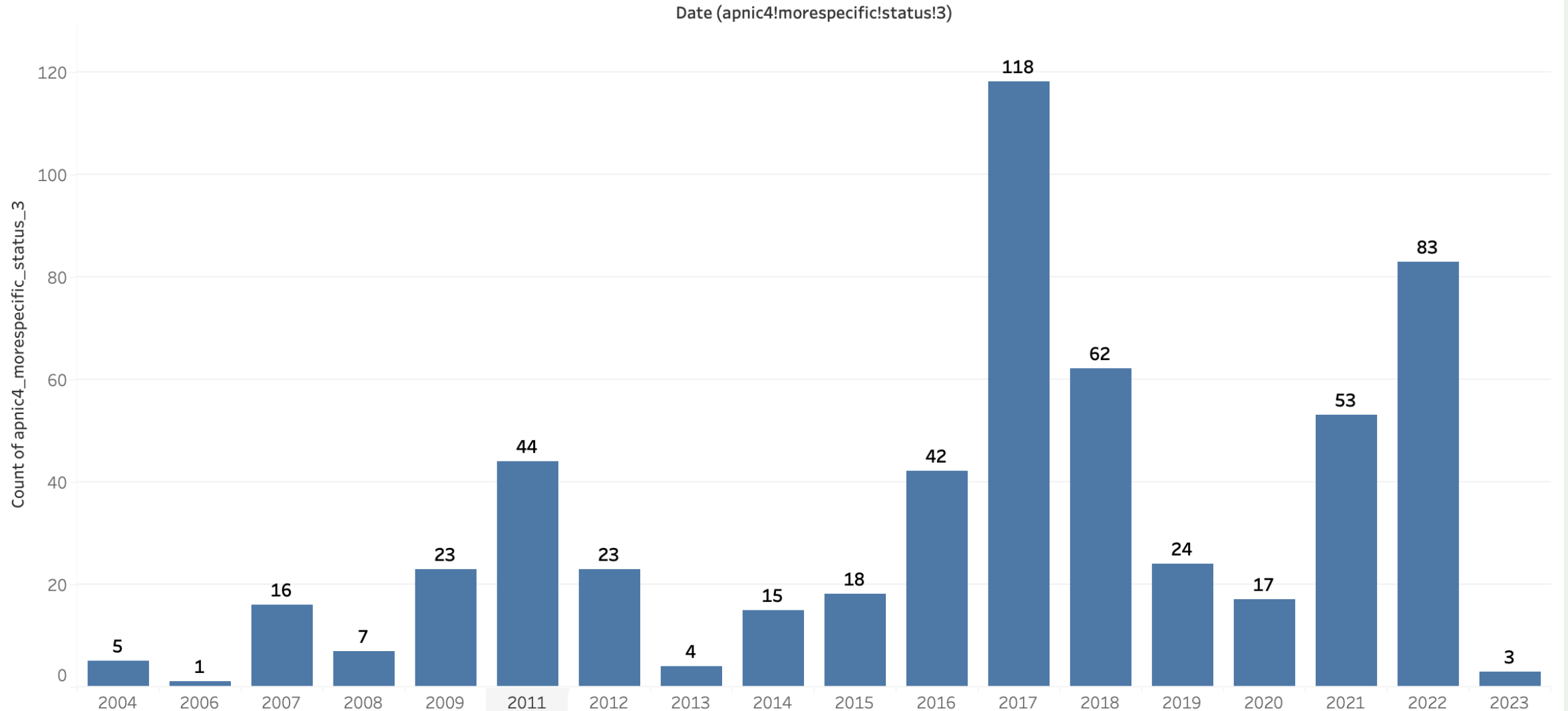
Status: 1 Type: More Specifics



VN IPv4 Resource Status

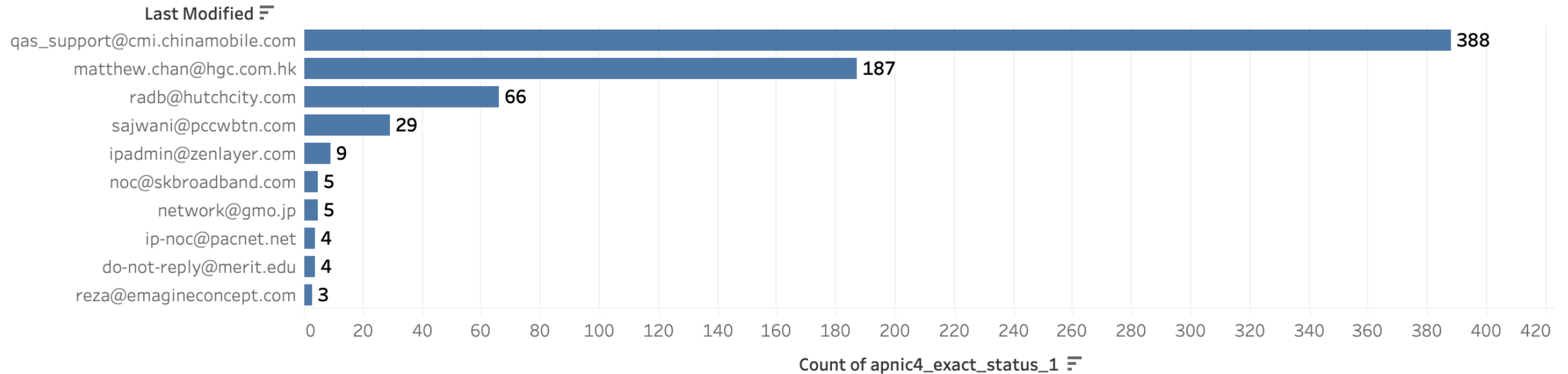
Status: 3 Type: More Specifics

Most Specific Status 3



VN IPv4 Resource Status – Who created them?

Exact-last Modified Status 1



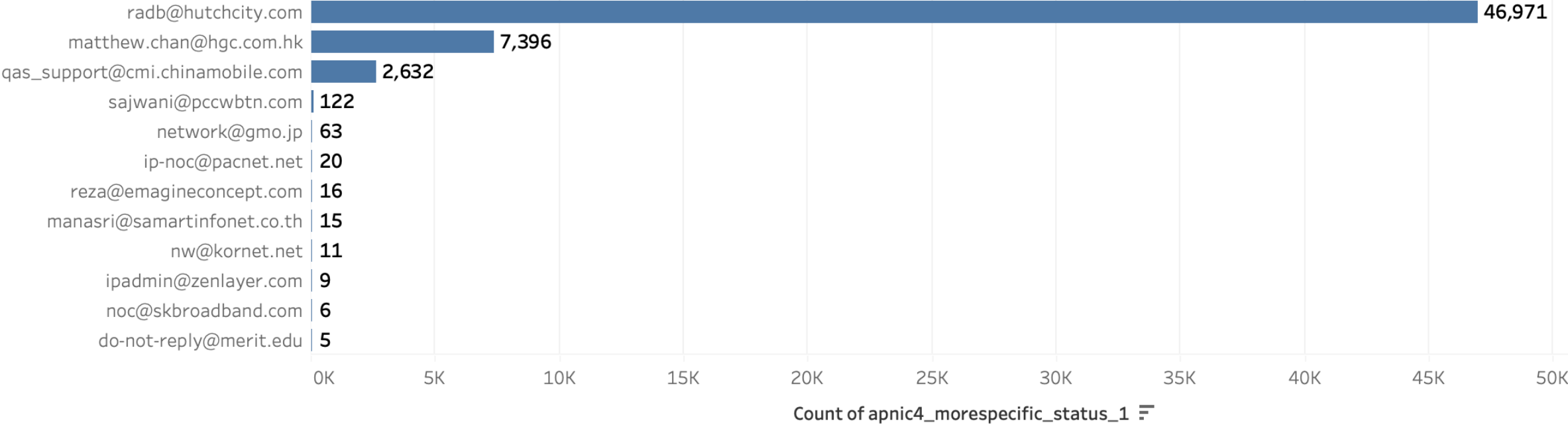
Status: 1 Type: Exact



VN IPv4 Resource Status – Who created them?

More Specific Last Modified Status 1

Last Modified (apnic4!morespecific..)



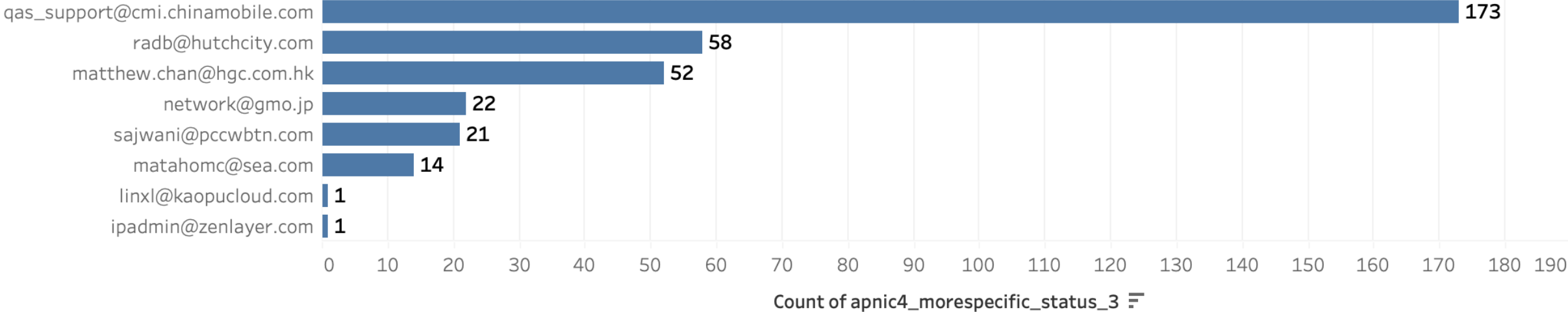
Status: 1 Type: More Specific



VN IPv4 Resource Status – Who created them?

More Specific Last Modified Status 3

Last Modified (apnic4!morespecif.. 🗑

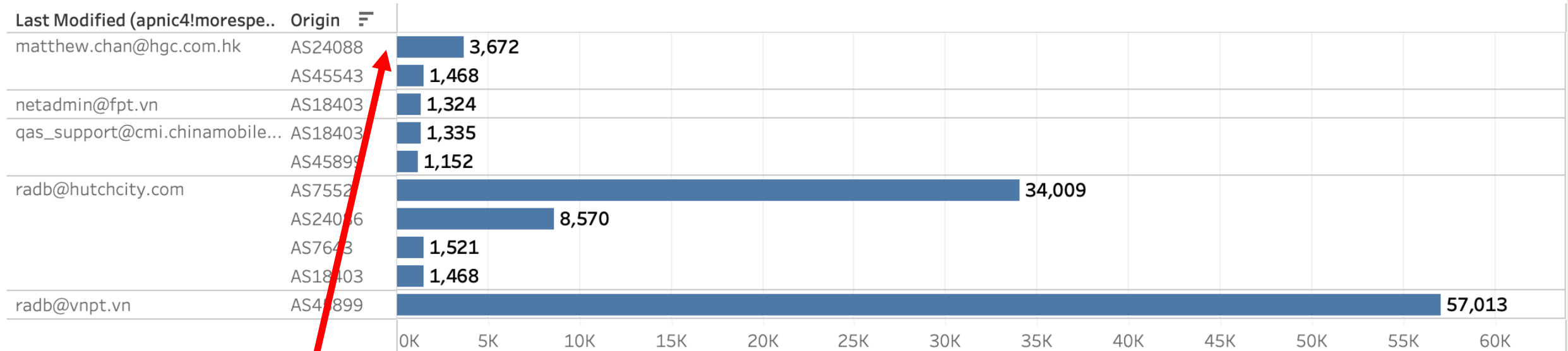


Status: 3 Type: More Specific



VN IPv4 Resource Status – Who created them?

More Specific - Status 1



Routing Status (AS24088)

At 2023-06-29 16:00:00 UTC, AS24088 was visible to 100% of 369 IPv4 and 100% of 378 IPv6 RIS full peers.

First ever seen as origin announcing 203.128.240.0/21, on 2005-11-25 08:00:00 UTC.

Originated IPv4 prefixes: 91
 Originated IPv6 prefixes: 1
 Observed BGP neighbours: 72
 Address space announced (IPv4): 18432 IPs
 Address space announced (IPv6): equiv. to 1 /48s

Status: 1 Type: More Specific

RPKI – No Duct Tape

Step 1: Create ROAs of all your advertised routes

Step 2: Enable ROV

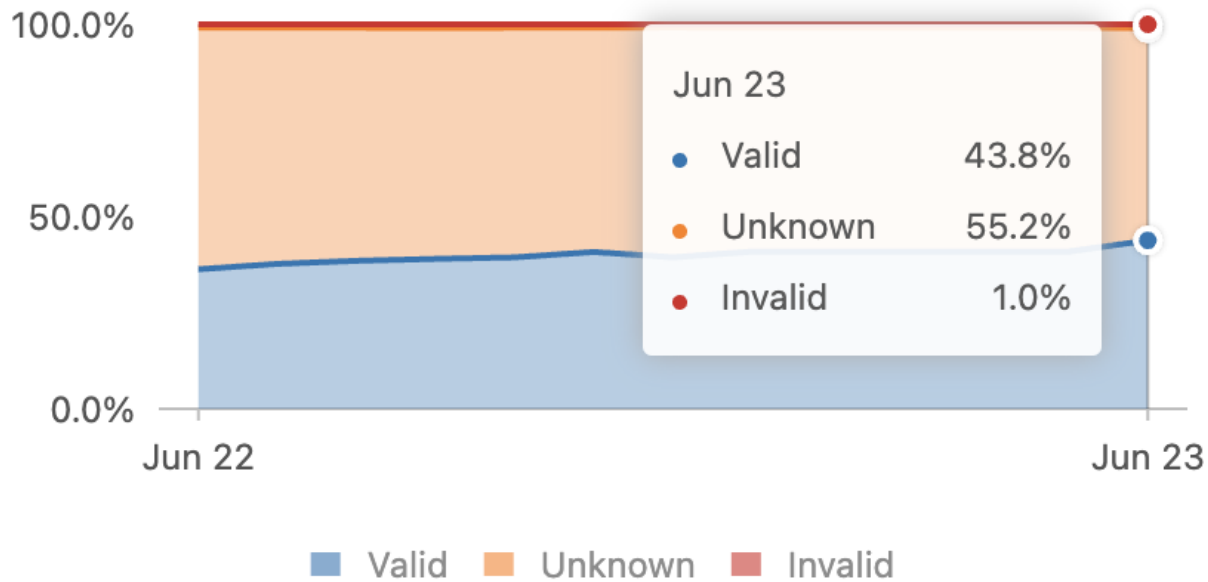


RPKI – No Duct Tape

Step 1: Create ROAs of all your advertised resources

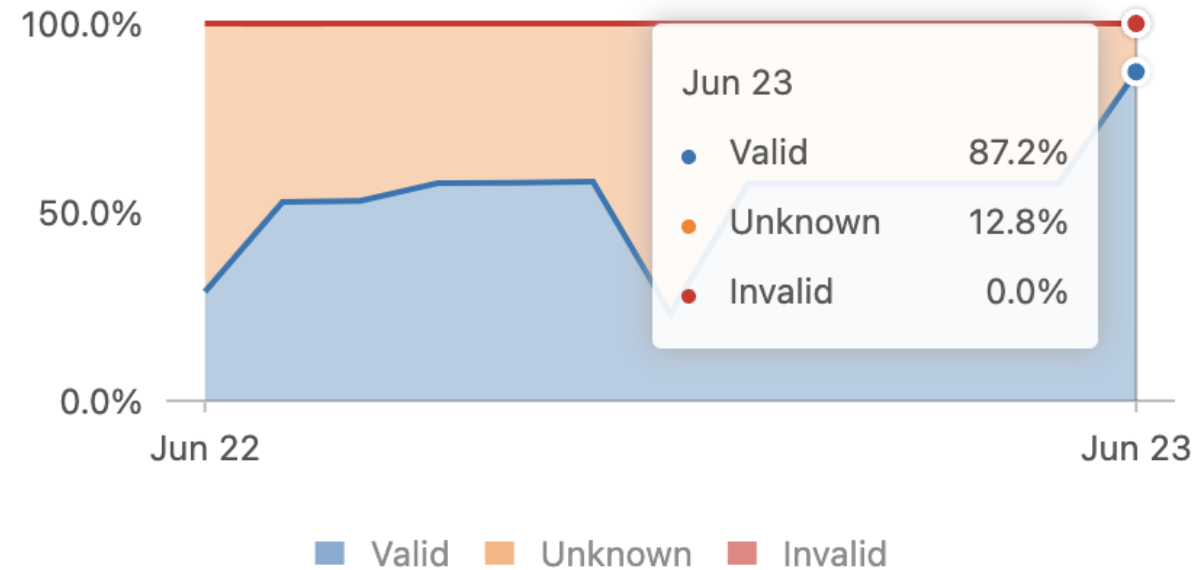
<https://observatory.manrs.org/#/history>

Routing Information (RPKI) i



Global ROA Coverage

Routing Information (RPKI) i



Viet Nam ROA Coverage



rpkf.apnic.net

VN

[AS7552](#)

90

<https://rpkf.today>

RPKI Invalid - VN

The RPKI status of a route in the global BGP table is determined by its associated ROA, specifically the Validated ROA Payload (VRP). As outlined in RFC 6811, if a route prefix is covered by at least one VRP but does not have a matching VRP, the BGP route will be considered RPKI invalid.

Route		
Origin ASN	Prefix	RPKI
AS135987	103.127.196.0/22 INDRA-RELOAD-VN	✗ Invalid
AS59729	78.136.196.0/24	✗ Invalid
AS59729	78.136.203.0/24	✗ Invalid
AS45899	123.30.109.0/24 VNPT-Net	✗ Invalid
AS135905	123.30.134.0/24 VNPT-Net	✗ Invalid
AS209372	109.238.201.0/24	✗ Invalid
AS140788	2407:34c0::/48 Catiedu Online Training Academy Company Limited	✗ Invalid

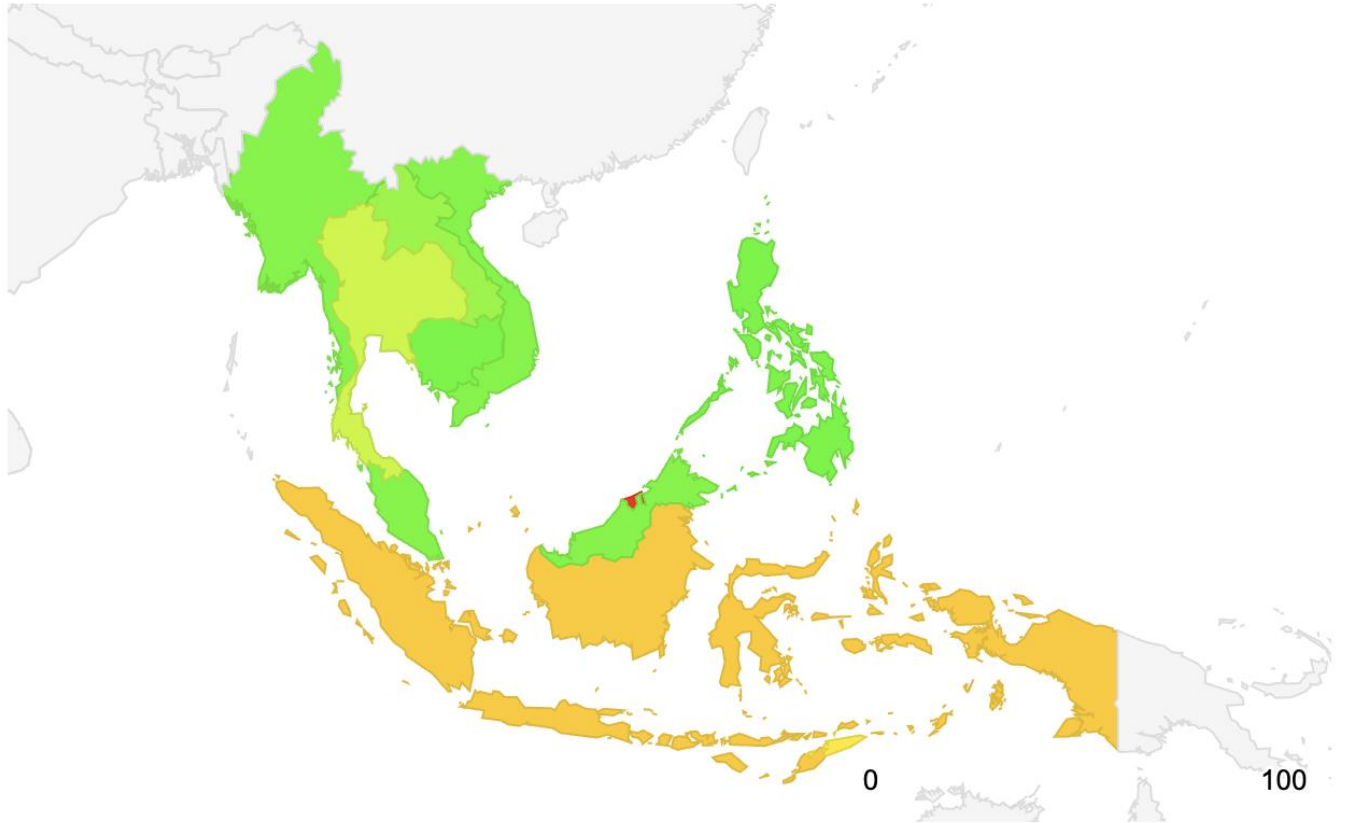


RPKI – No Duct Tape

Step 1: Enable ROA

Viet Nam is doing good in terms of Route Origin Authorisation in the South Eastern Asia region

Region Map for South-Eastern Asia (035)



<https://stats.labs.apnic.net/roa/VN>

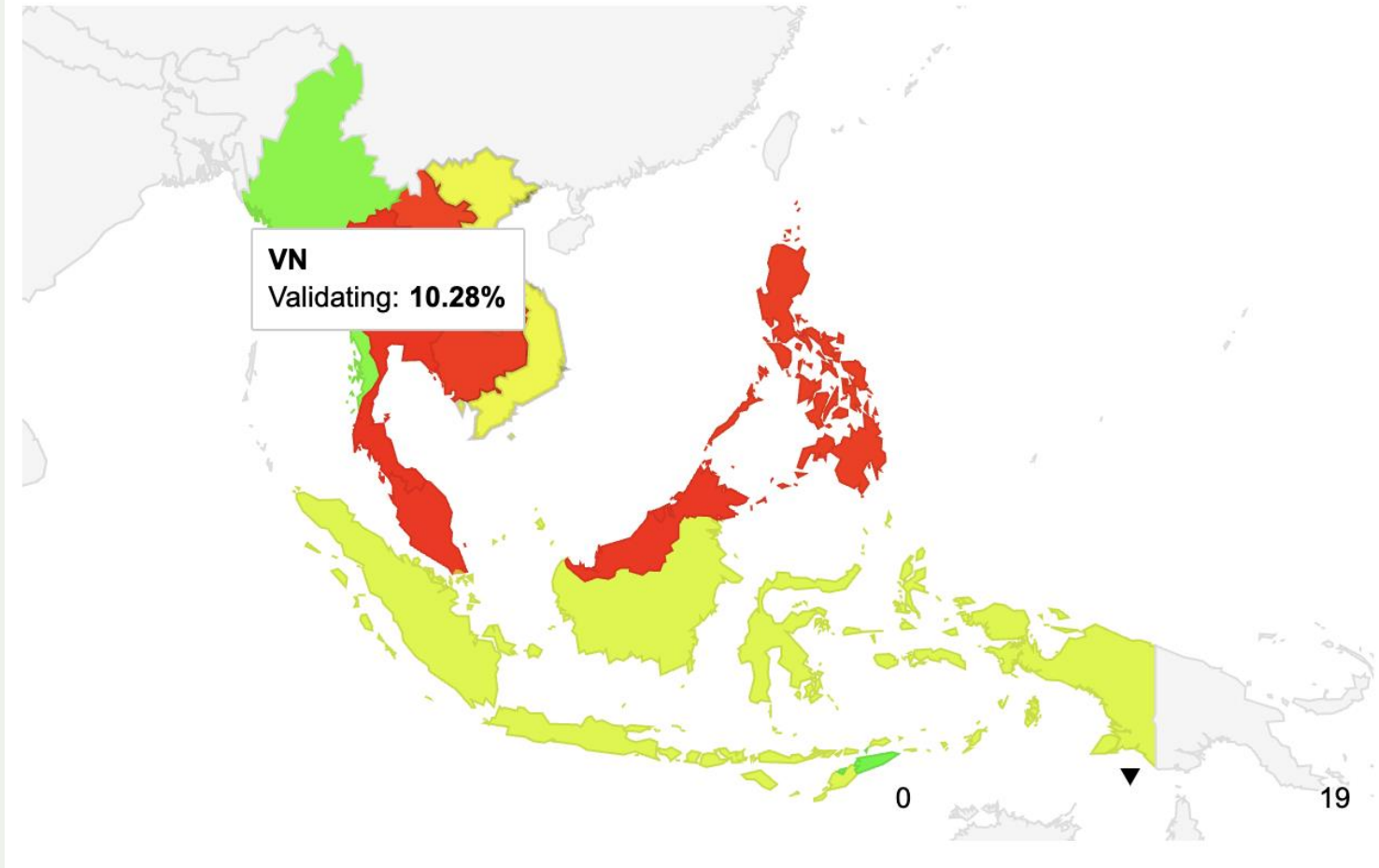


RPKI – No Duct Tape

Step 2: Enable ROV

Viet Nam is "Not" doing good in terms of Route Origin Validation in the South Eastern Asia region

Region Map for South-Eastern Asia (035)



<https://stats.labs.apnic.net/rpki/VN>



RPKI – No Duct Tape

Step 2: Enable ROV

Viet Nam is "Not" doing good in terms of Route Origin Validation in the South Eastern Asia region

ASN	AS Name	RPKI Validates
AS13335	CLOUDFLARENET	99.25%
AS24086	VIETTEL-AS-VN Viettel Corporation	97.40%
AS7602	SPT-AS-VN Sai gon Postel Corporation	97.39%
AS133606	VIETTELTIMORLESTE-AS-AP Viettel Timor Leste	96.36%
AS38247	VIETNAMOBILE-AS-VN Vietnamobile Telecommunications Joint Stock Company	76.54%
AS24088	HTCHCMC-AS-VN Hanoi Telecom Joint Stock Company - HCMC Branch	44.54%
AS7552	VIETEL-AS-AP Viettel Group	35.93%

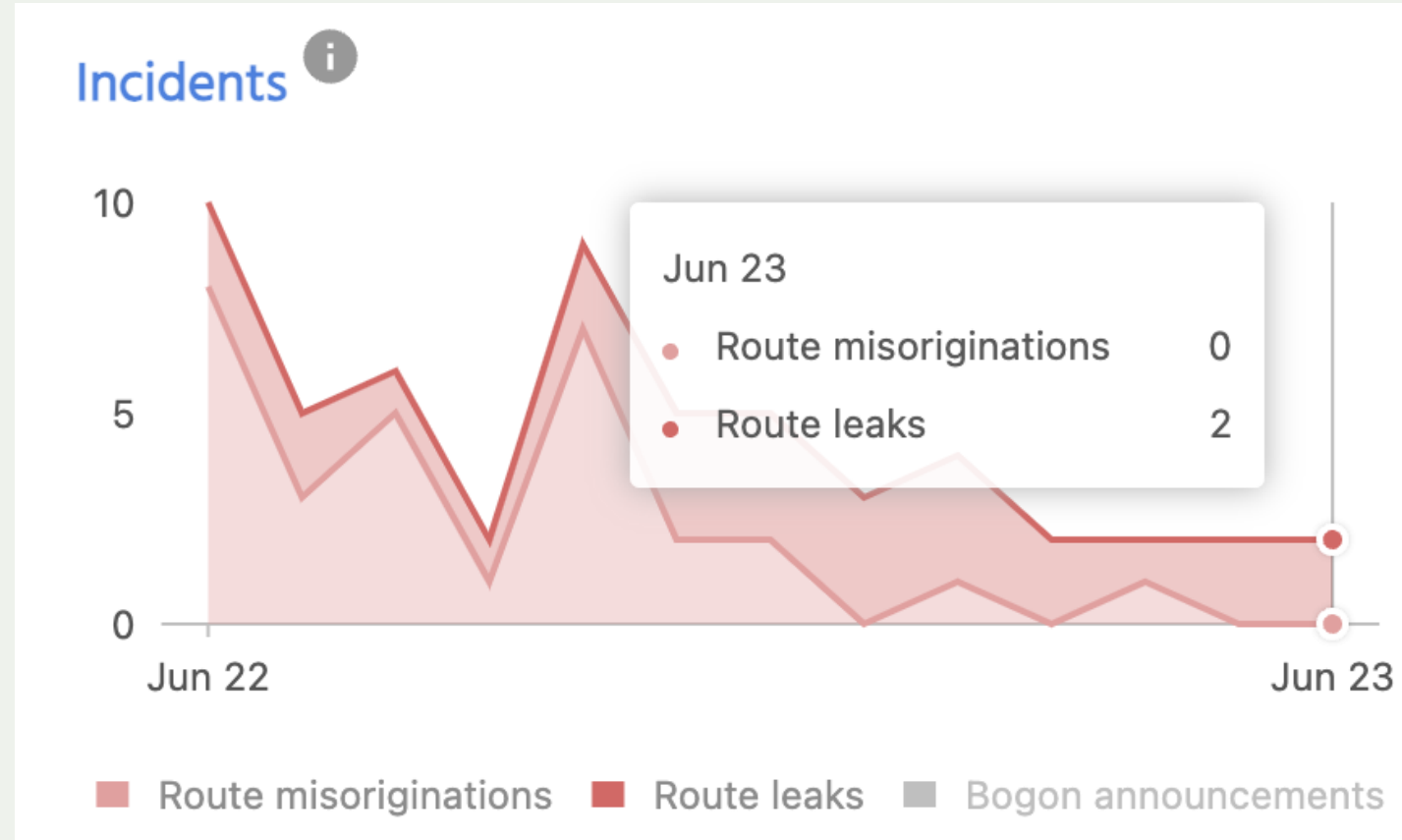
<https://stats.labs.apnic.net/rpki/VN>



BGP – Route Mis-origination or Leaks

Most (not all) of the Route Mis-origination and Route Leak incidents happen because of configuration mistakes which are very easily fixable.

Reach out to check if your network generated any of these incidents



<https://observatory.manrs.org/#/history>

PeeringDB – AS-SET

ASN Description	ASN	AS-SET
Viettel	7552	AS-7552
CMC Telecom	45903	AS-45903
VTC DIGICOM	38726	AS-38726
Hanoi Telecom	24088	AS-HANOITELECOM
VNPT	45899	AS-45899, AS-45899CUST
DUYTAN University	131357	
Online Data Services	45538	
VNIX-HN Route Servers	23899	
VNIX-HCM Route Servers	23962	
VNIX-DN Route Servers	56156	
VNNIC	23902	
VNNIC DN	131415	
VNNIC HCM	24066	
NetNam	24173	
Digital Storage Company	56153	
VTC Online	135945	
CPT Network	63747	
RVC Network	135964	
IPTP Vietnam	135993	
LDCV	131398	AS-131398
EverTheLess	209988	
Netnam Ho Chi Minh City	24176	
VIVU	206439	



So, What is the Solution?

- Don't rely on 3rd party IRR databases such as RADb, ALTDB etc, only use IRR services by RIRs .
- ROA uptake is very good in Viet Nam and can easily replace IRR.
- If someone has created route object for your resources, then contact IRR operator.
- Encourage operators to use RPKI (create ROAs – drop invalids).
- Start implementing Route Origin Validation (ROV).
- **Will you be interested in getting monthly reports of your resources?**
- **Sign up for MANRS (manrs.org)**



Thank you.