Detecting route announcements of unassigned IP address

Kentaro Goto
Waseda univ. Uchida lab
Route Research Expert Team

WASEDA University

JPNIC

Brief summary

- Our purpose

  To better understand the reality of

  “unexpected” route announcements

- Compared IPv4 full route

  with IPv4 address pool in JPNIC

- Found 3 different route announcements

  -- 3 separate /24 networks

Background info – Related works (1/2)

Research about unallocated prefixes from RIRs exists

allocate

NIRs or ISPs EUs

RIR-pooled

= unallocated

Not supposed to appear in any actual routes

Background info – Related works (2/2)

- RIR-allocation progresses
  - FTP sites by APNIC

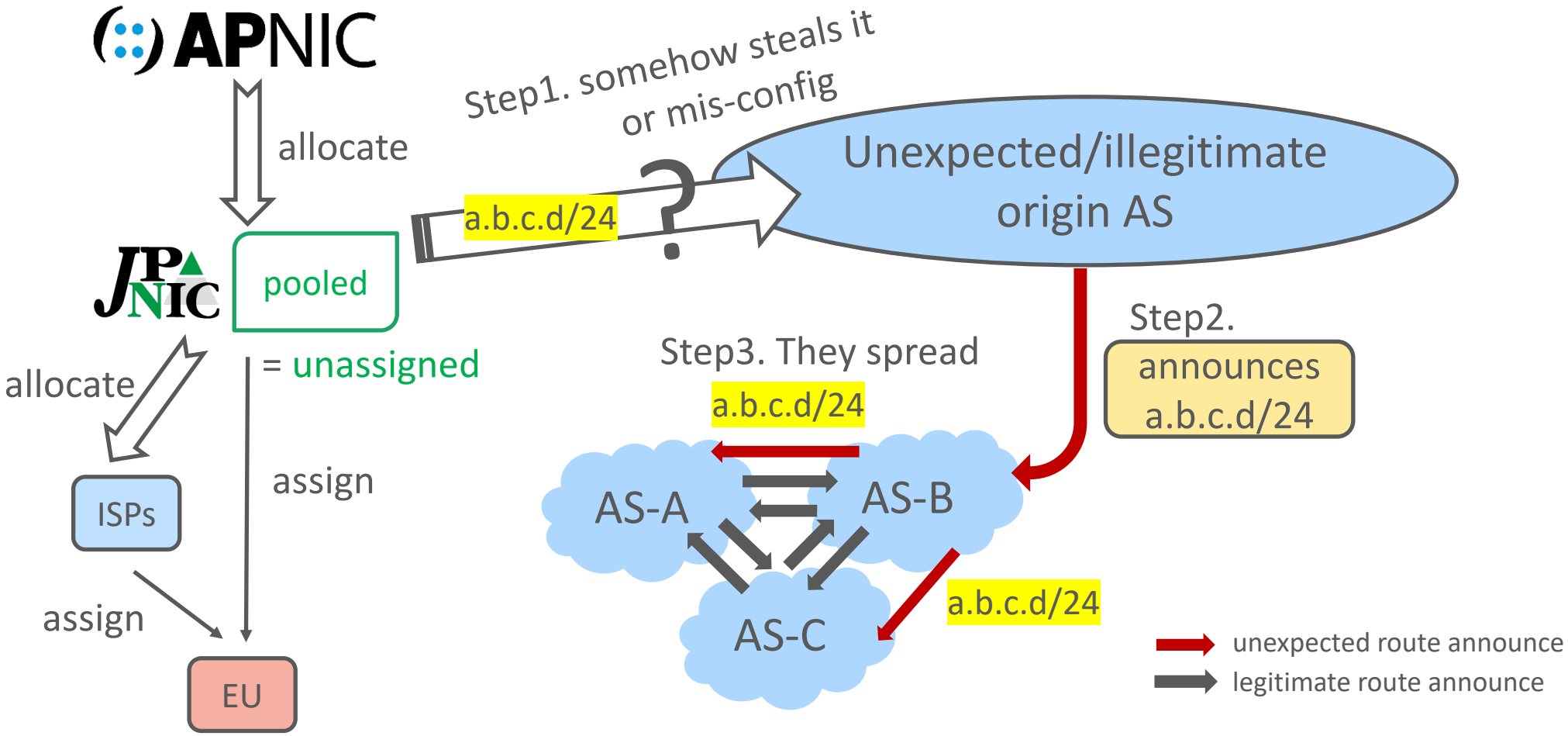
    http://ftp.apnic.net/stats/apnic/
- Mis-announced address space/AS numbers
  - For “bad” address

    http://thyme.apnic.net/current/data-add-IANA
  - For “bad” AS

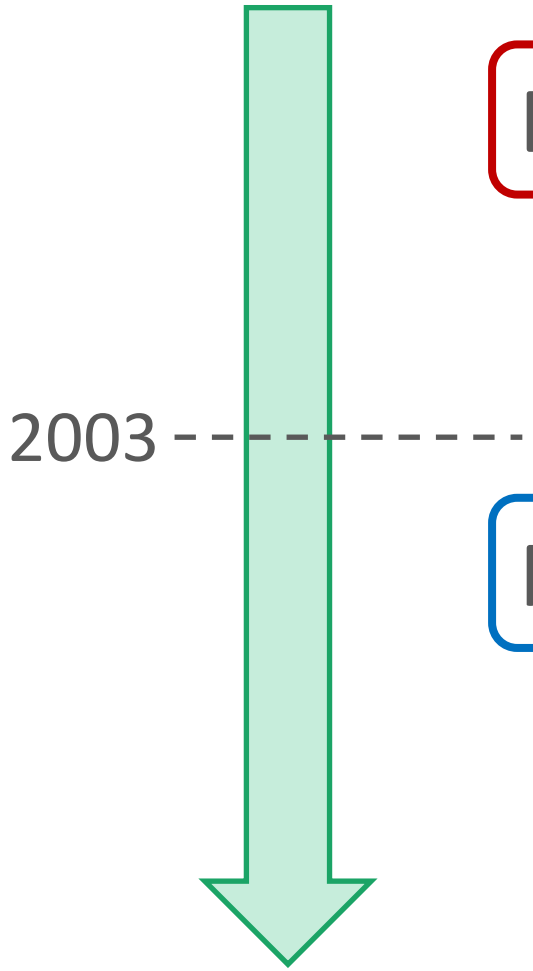
    http://thyme.apnic.net/current/data-badAS

What about NIR-pooled addresses?

Background info - stakeholders



FYI - JPNIC-pooled addresses



2003

Before 2003

Any NIRs were able to hold resources allocations for further allocation to ISPs in their economy

Now

JPNIC forwards each allocation request from local ISPs to APNIC

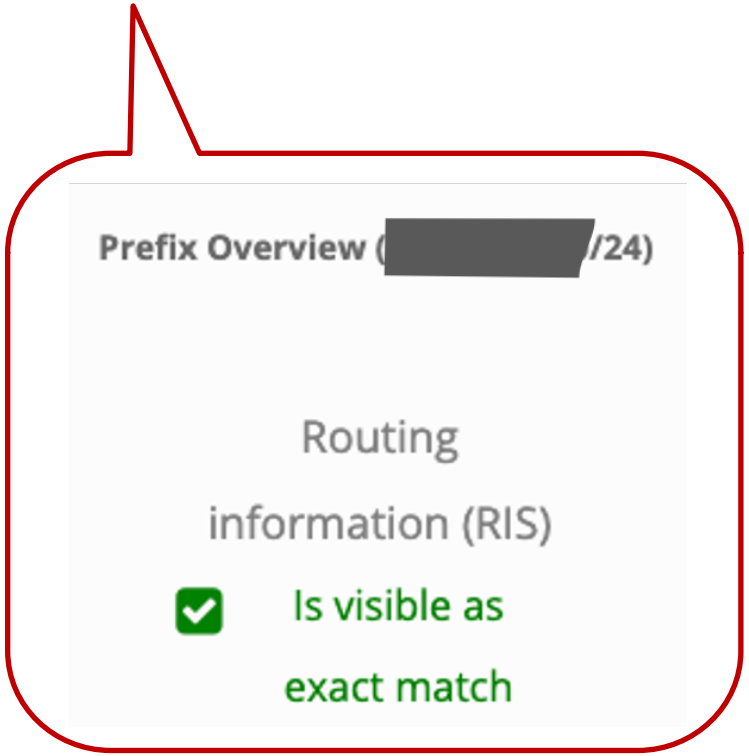
Background info – DB search

Unassigned IP addresses announced

```
No match!!

Reference: WHOIS servers of RIRs
   APNIC WHOIS(whois.apnic.net)
   ARIN WHOIS(whois.arin.net)
   RIPE WHOIS(whois.ripe.net)
   LACNIC WHOIS(whois.lacnic.net)
   AfriNIC WHOIS(whois.afrinic.net)
```

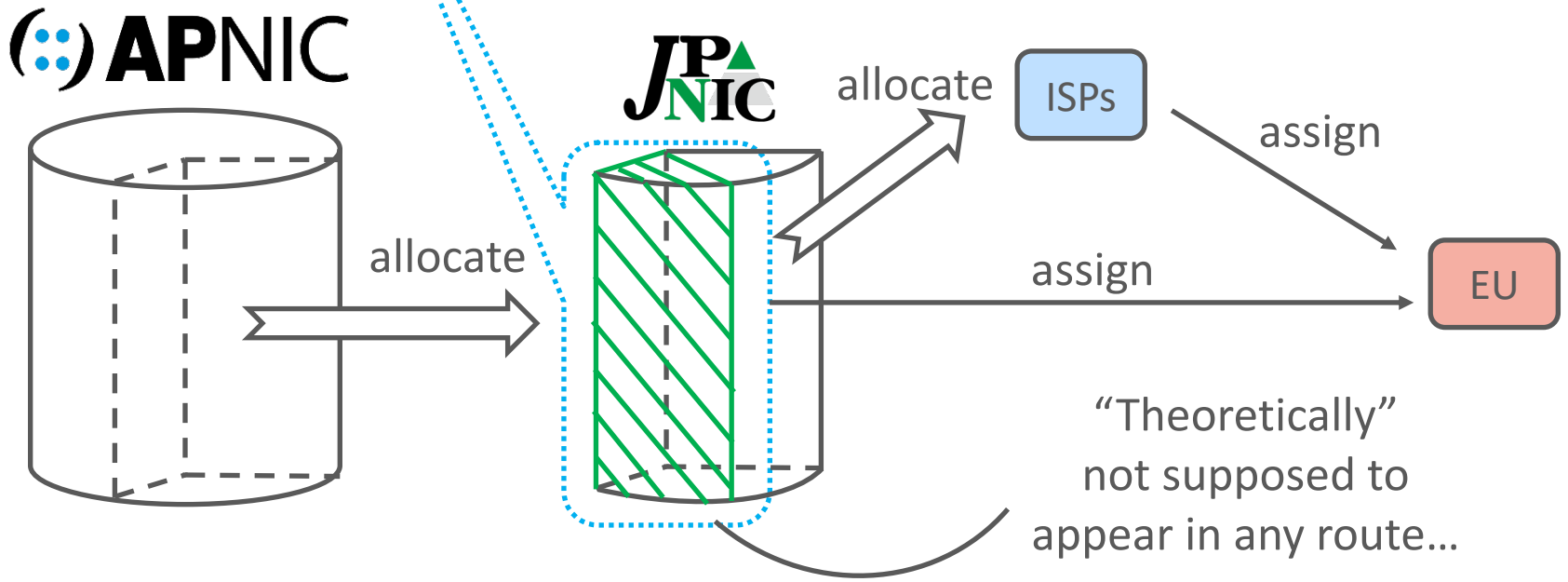
Not found in JPNIC WHOIS



...but visible in RIPEstat

Hypothesis

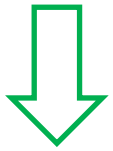
Unassigned IP networks are announced in the Internet



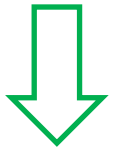
Overview again

Overview

Compare IPv4 full route with IPv4 address pool in JPNIC



Detect unassigned networks announced as routes



Search for details on route monitoring system

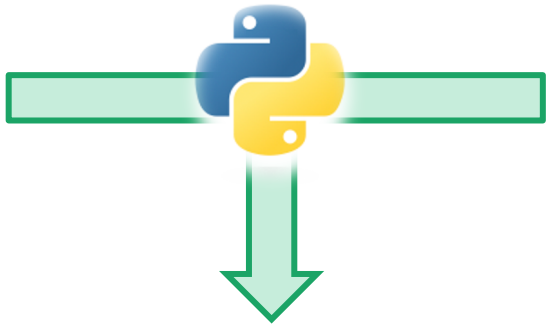
Detecting “Unexpected” by python™

(1) Announced ∩ (2) unassigned

(1) Announced IP prefixes

192.0.2.0/24
aa.bbb.xx.y/16
aa.bbb.ss.t/8
203.0.113.0/24
…

∩ (AND)



(2) Unssigned IP Addresses

aa.bbb.xx.y/21
aa.bbb.ss.t/24
…

Announced ∩ Unassigned

aa.bbb.xx.y/21
aa.bbb.ss.t/24

Data details

(1) Announced IP prefixes

- Downloaded from RIPE RIS*

  *RIS: Routing Information Service
- Around 800,000 announcements
- Size equivalent to around 15,341,353 /24 networks

rcc06.ripe.net
Otemachi, Japan. Collects route updates announced by JPIX members from Aug. 2001

(2) Unassigned IPv4 Addresses

- Calculated from JPNIC database (10th Dec 2019)
- Size equivalent to 14,497 /24 networks
- Needless to say ...
  - NOT open to the public
  - NO IPv6 included

Requirements and links

Reading Route info/JPNIC database csv

pandas

Extracting Announced && Unassigned

netaddr, ipaddress

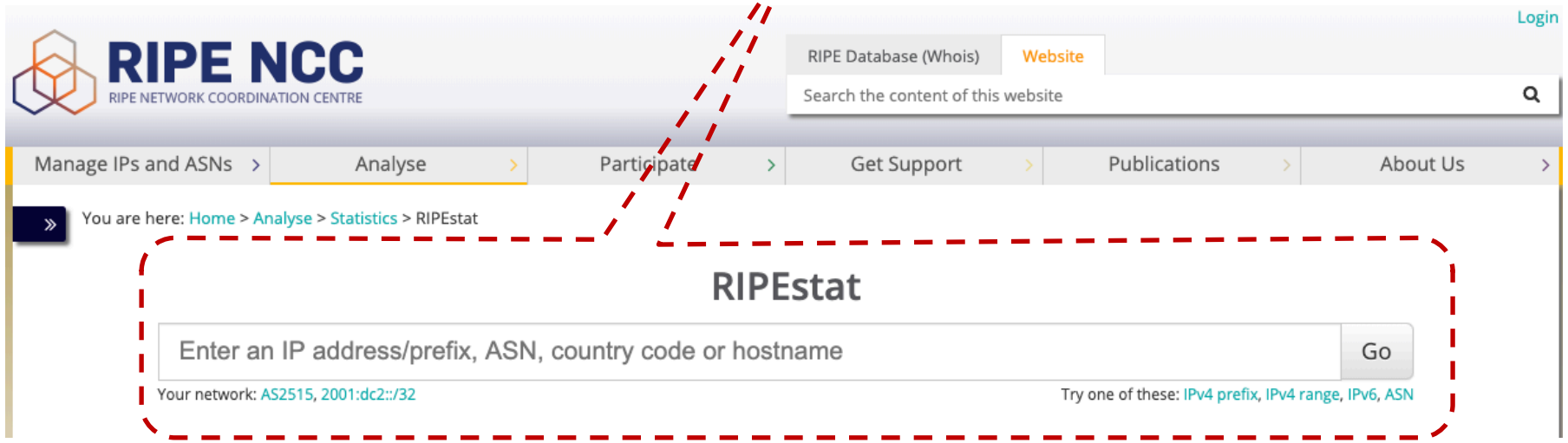
For network addresses manipulation

- netaddr – IPSet()
  https://netaddr.readthedocs.io/en/latest/introduction.html
- ipaddress
  https://docs.python.org/3/library/ipaddress.html

Results verification - flow

Detected 3 unassigned networks announced in route information

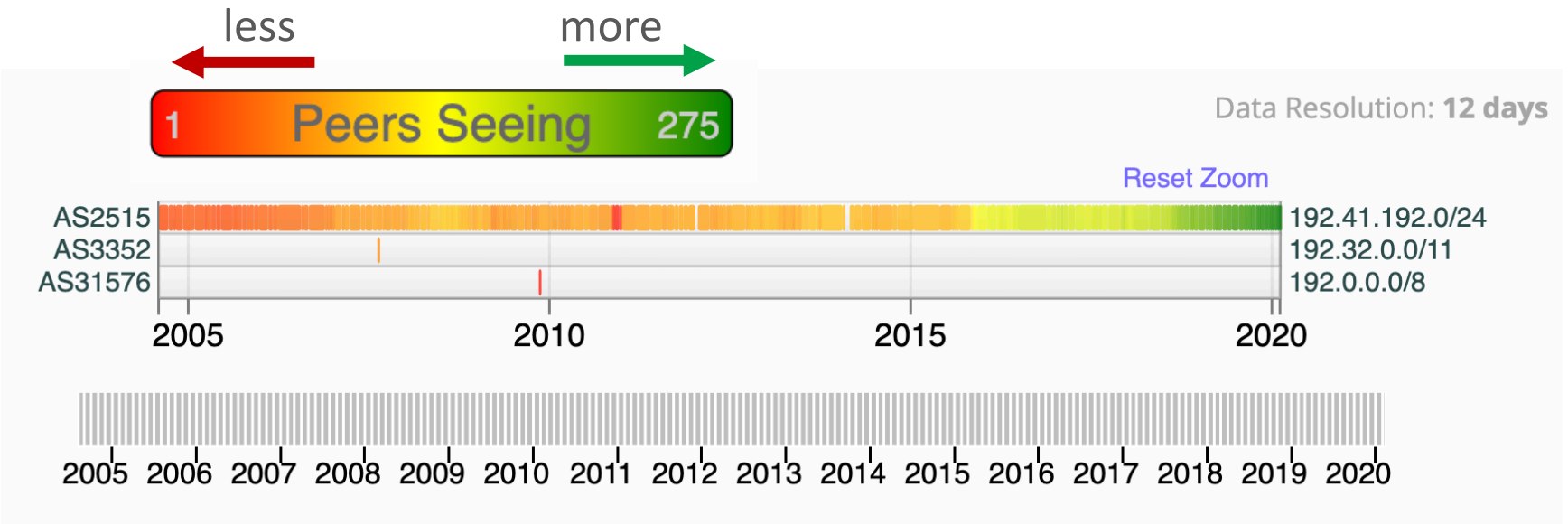
Search them on RIPEstat for details



Results verification - example


```
→  lab (master) ✗ host whois.nic.ad.jp
whois.nic.ad.jp has address 58.84.254.30
whois.nic.ad.jp has address 192.41.192.40
```

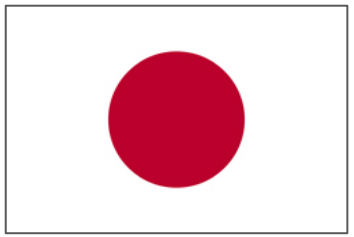
JPNIC office IP prefix 192.41.192.0/24



Heatmap of an announced route https://stat.ripe.net/

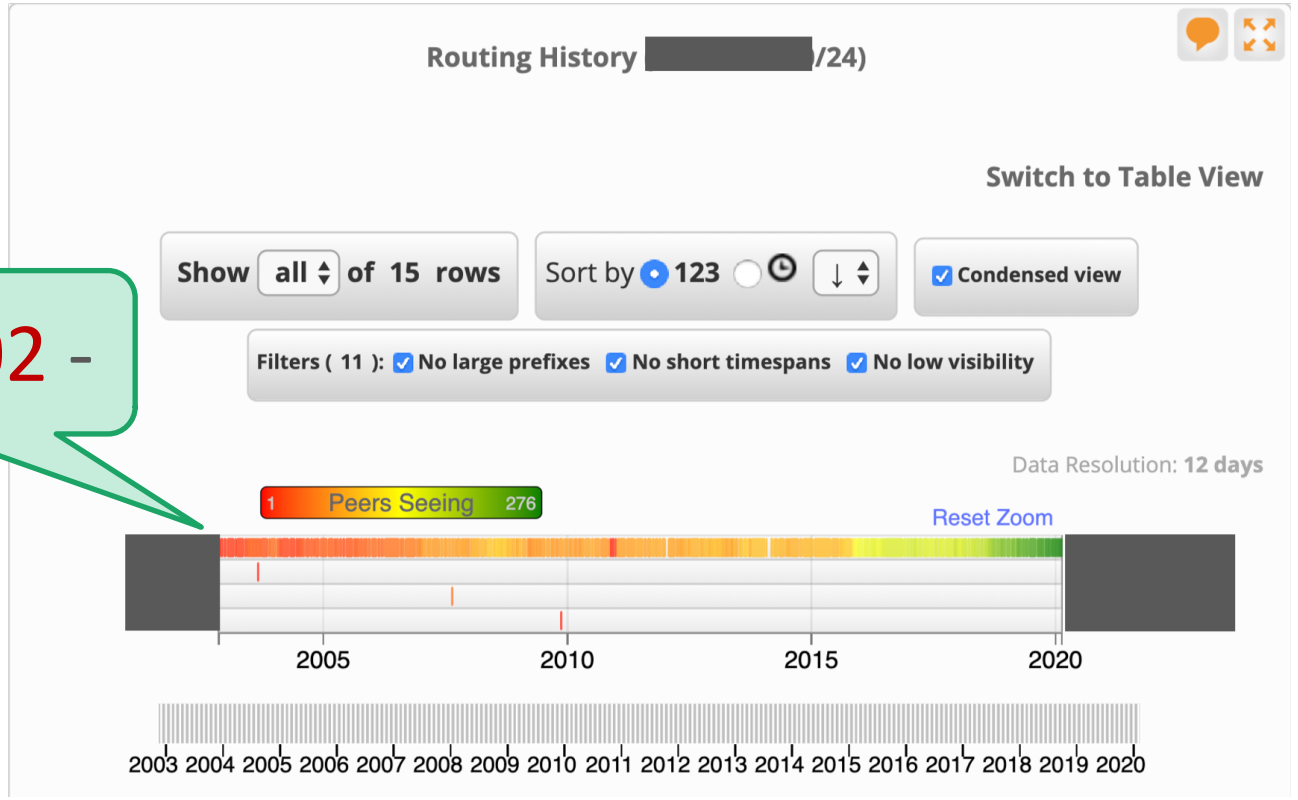
RIPEstat search Results

Results - from an AS in Japan



https://stat.ripe.net/

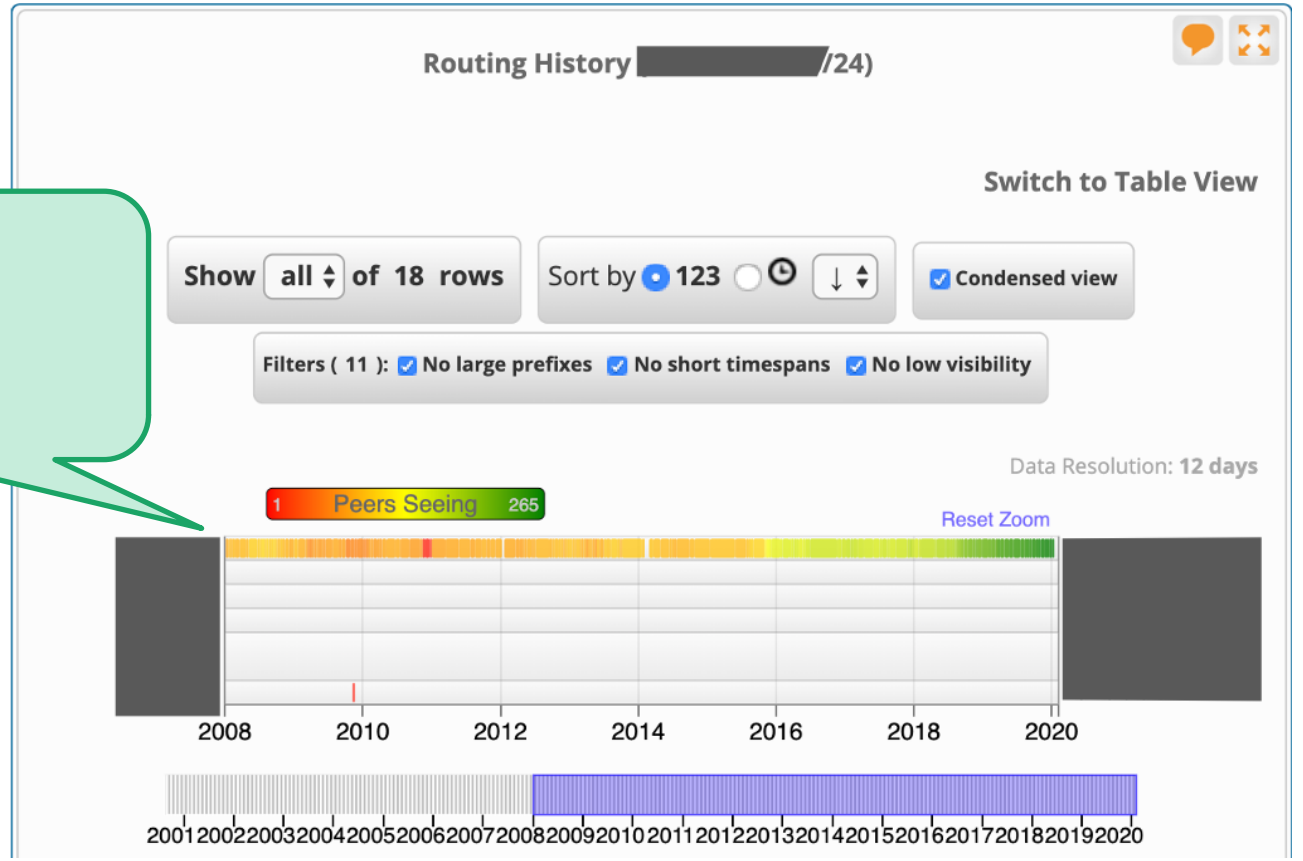
Nov. 2002 -



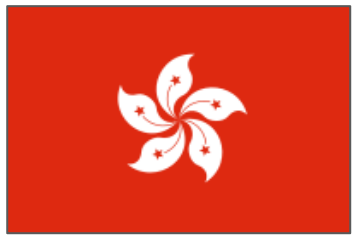
Results - from an AS in S.Korea

https://stat.ripe.net/

Jan. 2008
- Jan. 2020

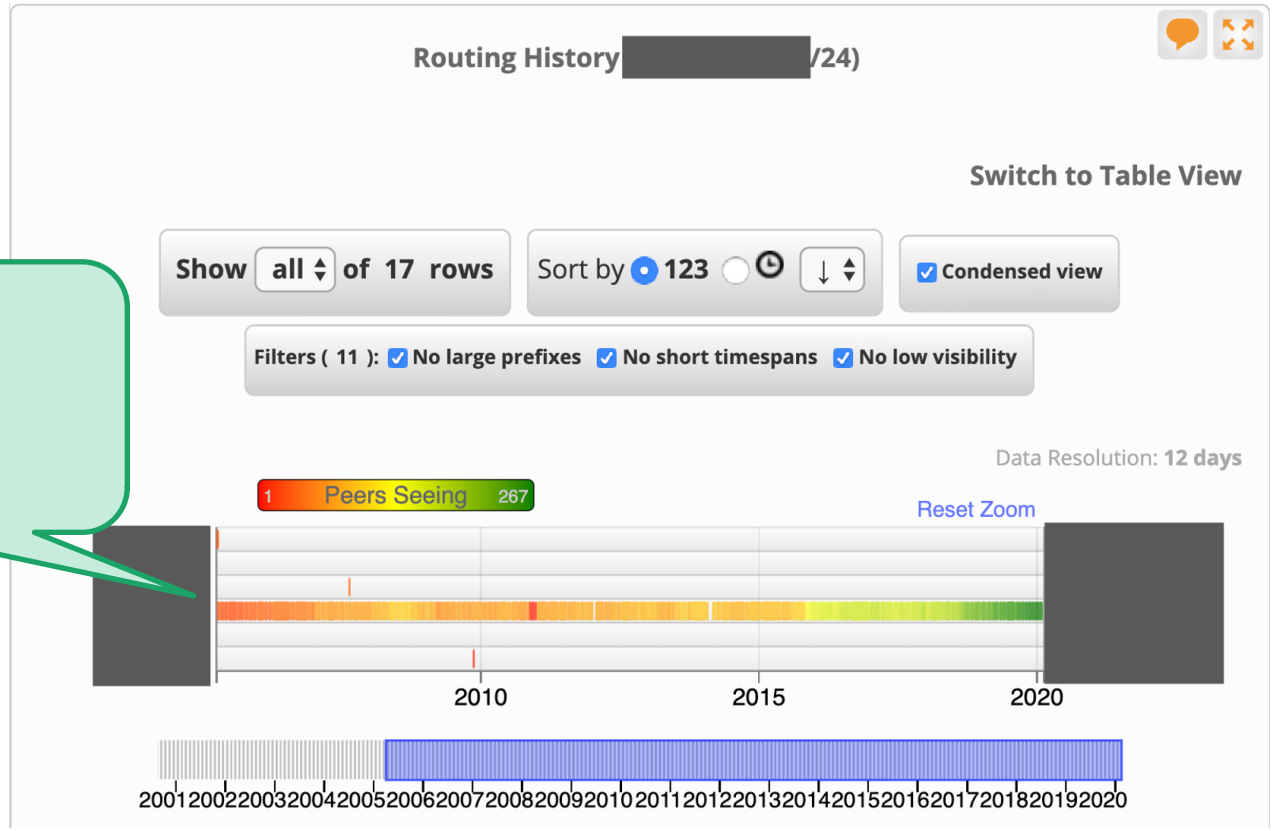


Results - from an AS in Hong Kong

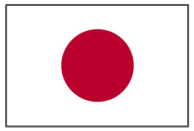


https://stat.ripe.net/

Apr. 2005
– Jan. 2020



Consequences of the detected networks

- from an AS in Japan 
  - Previously was returned to JPNIC

    …but announcement settings has not followed
- from an AS in S.Korea
  - Withdrawn after contact
  - Mis-config
- from an AS in Hong Kong
  - Withdrawn after contact
  - Mis-config

Conclusion

Found 3 unassigned networks announced in route information

Even unused IP addresses are routed in the Internet

… not an organisation dependent problem

Future work

- Active monitoring
  - ping them all
- Investigate open ports on the hosts in the detected IP networks to see their purposes
- IRR search for more info?
- Further research for other regions
- Further research involving malicious domain names
- Anomaly detection by machine learning

Appendix

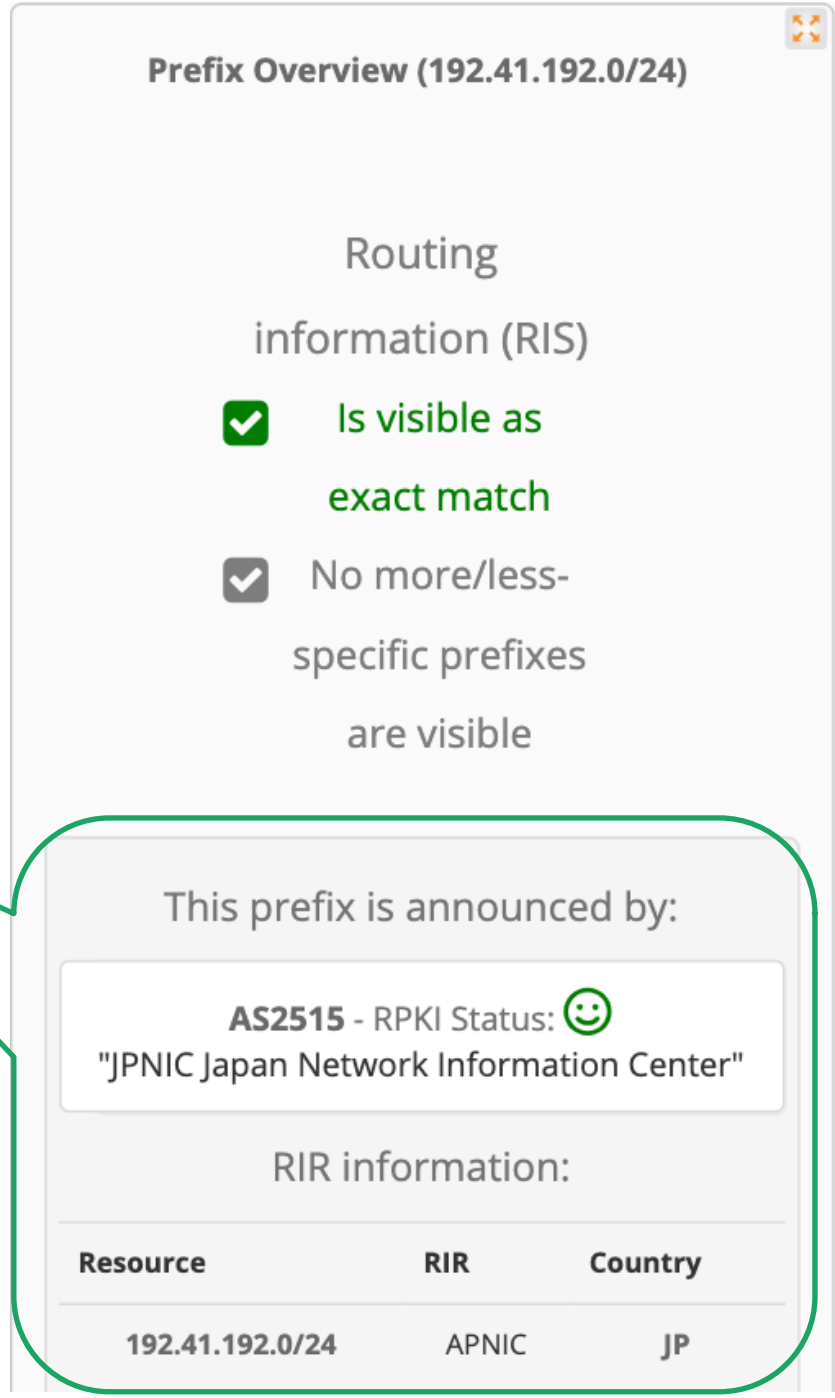
- Public GitHub repository

  https://anonymous.4open.science/r/0d8ee868-194c-48b0-a17d-c58b17837596/

  - A simple python script
- Applicable to arbitrary IP prefixes pool
  - So please give it a try

Thank you

RIPEstat search results for RIR/RPKI info



https://stat.ripe.net/