Suspicious BGP Announcements

Matsuzaki ‘maz’ Yoshinobu

<maz@iij.ad.jp>

On Jan 25, we got a information

- "An AS is hijacking a bunch of IPv4 prefixes, and even worse the AS is an APNIC unassigned AS"
- Yes, AS135091 was originating weird prefixes at that time - mostly big allocations for different economies and also unallocated spaces.
  - 27.146.0.0/16 MY
  - 42.128.0.0/16 CN
  - 49.8.0.0/16 KR
  - 130.21.0.0/16 US
  - 150.25.0.0/16 JP

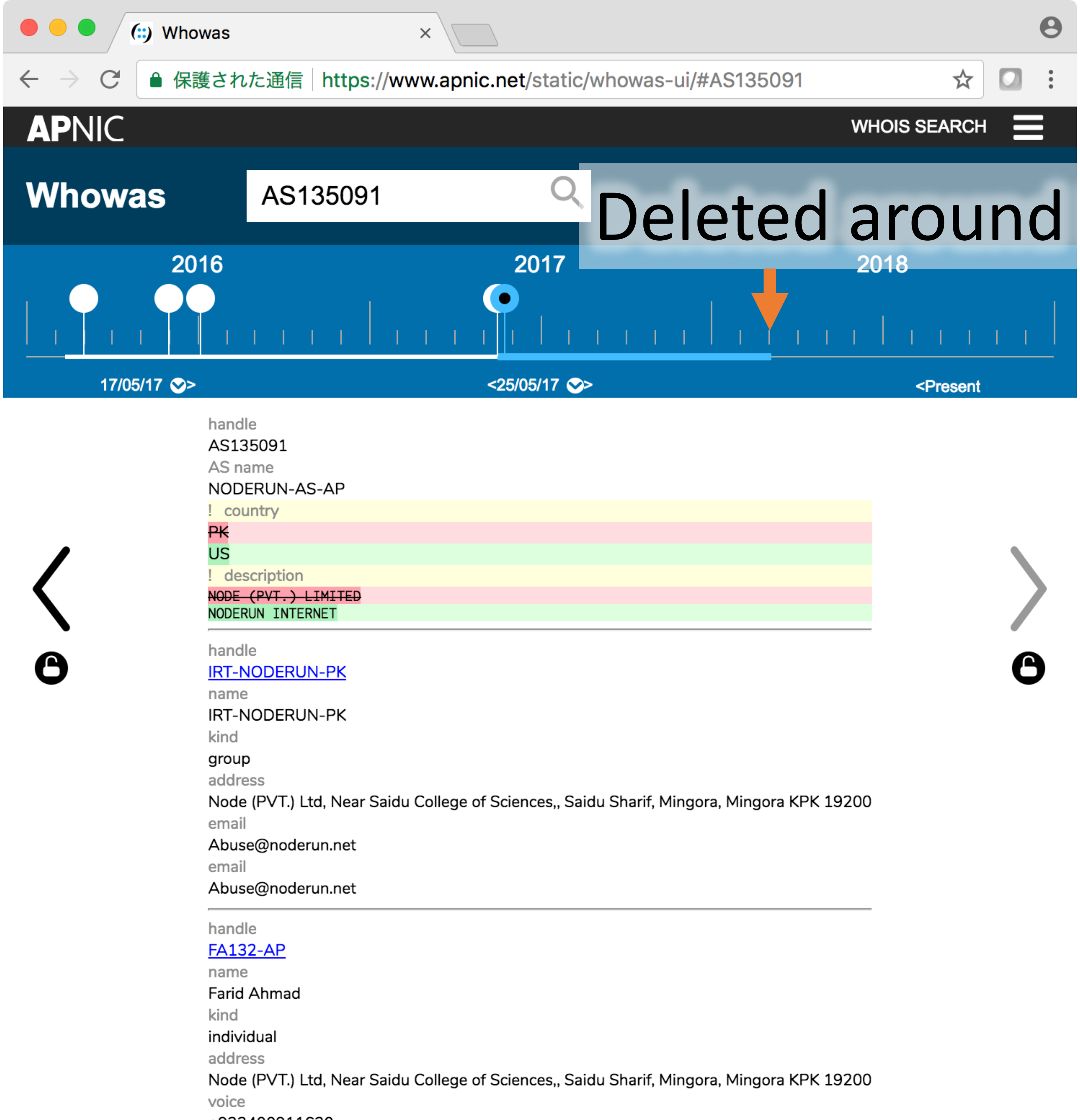
  … and many more

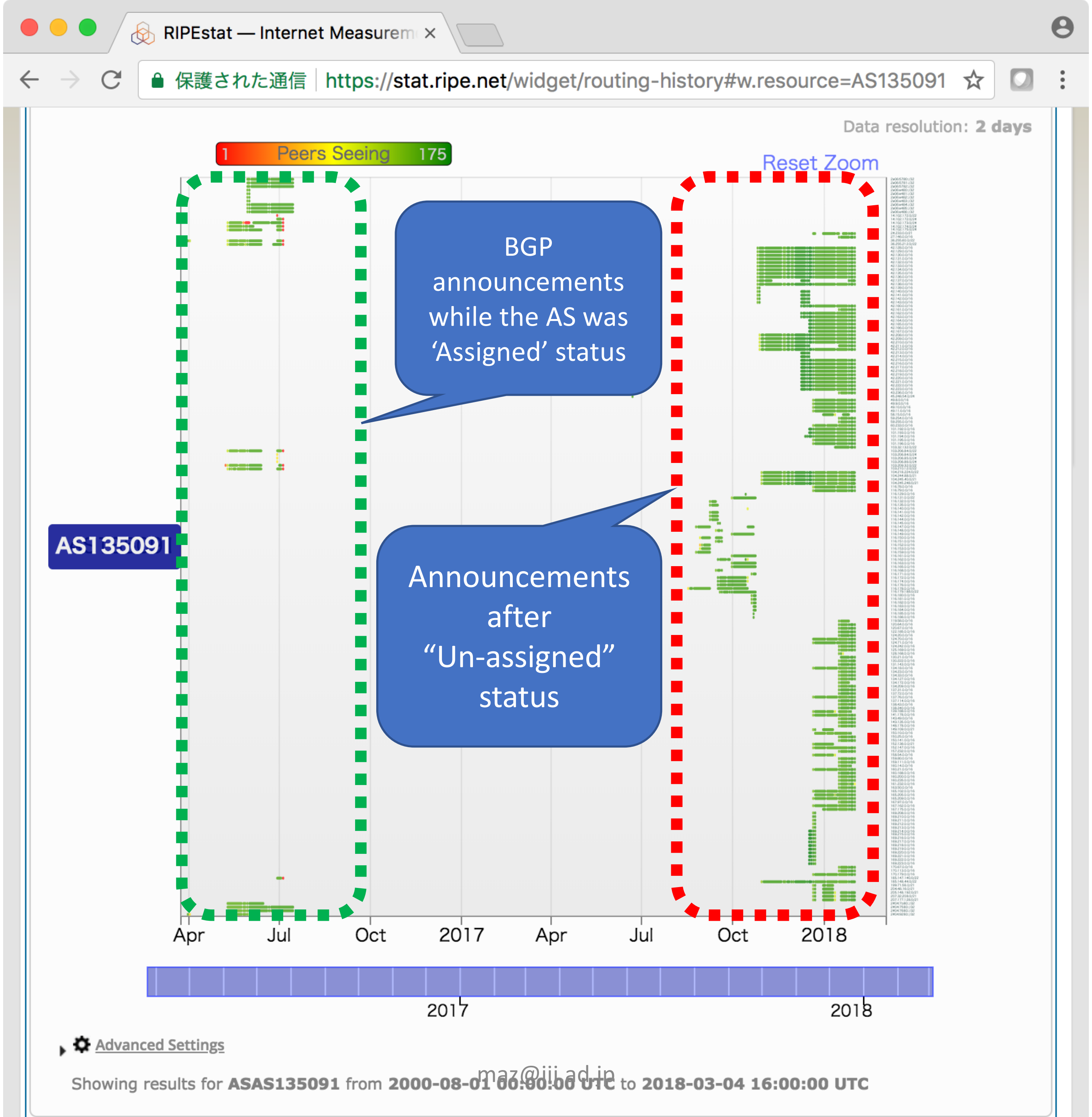
AS135091 status at that time

~ — -bash — 85×24

```
pro2015:~ maz$ whois -h whois.apnic.net AS135091 | grep %
% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html
% Information related to 'AS134557 - AS135580'
% This query was served by the APNIC Whois Service version 1.88.15-43 (WHOIS-US3)
pro2015:~ maz$
```

In case of assigned AS, I should be able to see something like "% Information related to 'AS135091'" there


Whowas
保護された通信
https://www.apnic.net/static/whowas-ui/#AS135091
APNIC
WHOIS SEARCH
Whowas
AS135091
Deleted around here
2016
2017
2018
17/05/17
<25/05/17
<Present
handle
AS135091
AS name
NODERUN-AS-AP
! country
~~PK~~
US
! description
~~NODE (PVT.) LIMITED~~
NODERUN INTERNET
handle
IRT-NODERUN-PK
name
IRT-NODERUN-PK
kind
group
address
Node (PVT.) Ltd, Near Saidu College of Sciences,, Saidu Sharif, Mingora, Mingora KPK 19200
email
Abuse@noderun.net
email
Abuse@noderun.net
handle
FA132-AP
name
Farid Ahmad
kind
individual
address
Node (PVT.) Ltd, Near Saidu College of Sciences,, Saidu Sharif, Mingora, Mingora KPK 19200
voice



RIPEstat — Internet Measurem
保護された通信
https://stat.ripe.net/widget/routing-history#w.resource=AS135091
Data resolution: 2 days
1
Peers Seeing
175
Reset Zoom
BGP announcements while the AS was 'Assigned' status
Announcements after "Un-assigned" status
AS135091
Apr
Jul
Oct
2017
Apr
Jul
Oct
2018
2017
2018
Advanced Settings
Showing results for ASAS135091 from 2000-08-01 00:00:00 UTC to 2018-03-04 16:00:00 UTC

Contacted the upstream AS

- 2018/Jan/25
  - Contacted their NOC
  - Some stopping, re-announcing ....
- 2018/Jan/30
  - Contacted a person in the upstream AS
  - Convinced the person to work together
- 2017/Feb/05
  - The suspicious announcements were stopped

Lesson Learned

- Validate your announcing prefixes
  - Including transiting AS and its prefixes
  - Check with Whois, RPKI
- Make your prefixes visible from the Internet
  - Announce your prefixes once you get allocation
  - Unused resources might be abused
- Let’s fix together!
  - In case you find anything suspicious, contact the AS or its upstream.
  - SANOG and such communities can help. :)