Prelude to a BGP hijack?

Improper uses of AS-sets?

Lasse Jarlskov
Lasse.jarlskov@teliacompany.com

Telia Company

What happened?

- Our upstream IP-transit provider alerted us.
- An AS-SET in the RIPE DB suddenly showed up referencing our AS-number

https://bgp.tools/as/59580

Start here...

View | Edit

Batterflyai Media ltd.

AS Number **59580**

Overview | Prefixes | Connectivity | Whois

Registered on
14 Aug 2012 (12 years old)

Network status
Active, Allocated under RIPE

Network type
Unknown

Prefixes Originated
3 IPv4, 0 IPv6

Upstreams

- AS43350 - NForce Entertainment B.V.
- AS3257 - GTT Communications Inc.

Locations of Operation

- Russian Federation

IRR EXPLORER

AS59580:AS-ALL

Data source status

Report for AS-set AS59580:AS-ALL

Expands to:

Name	Source	Depth	Path	Members
AS59580:AS-ALL	RIPE	1	AS59580:AS-ALL	AS3301 AS59580

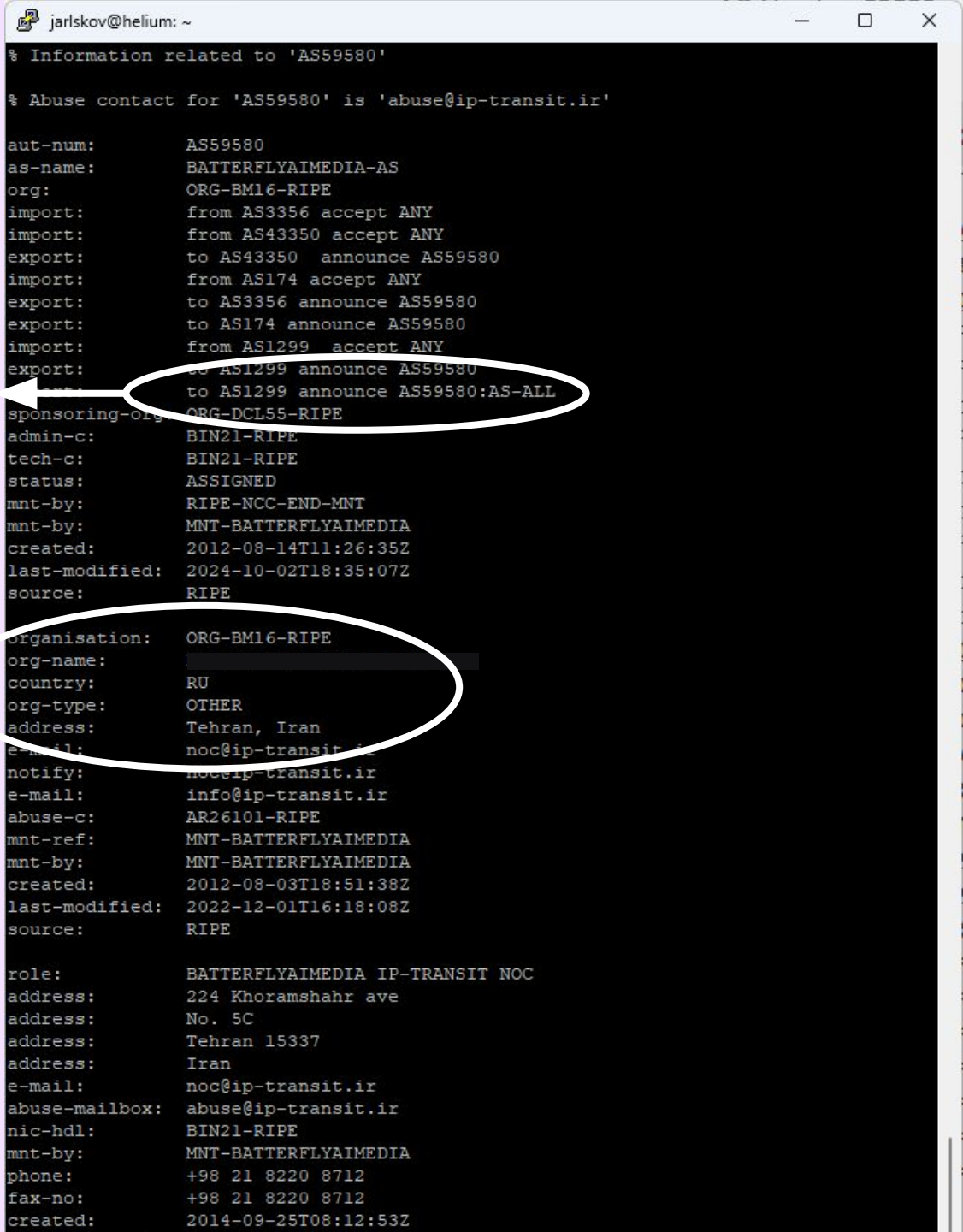
Who dis?

— Clearly presenting the AS-set to their upstream:

```
export:          to AS1299 announce AS59580:AS-ALL
```

— Russia or Tehran, IR?

```
organisation:    ORG-BM16-RIPE
org-name:        E
country:         RU
org-type:        OTHER
address:         Tehran, Iran
e-mail:          @ip-transit.ir
```

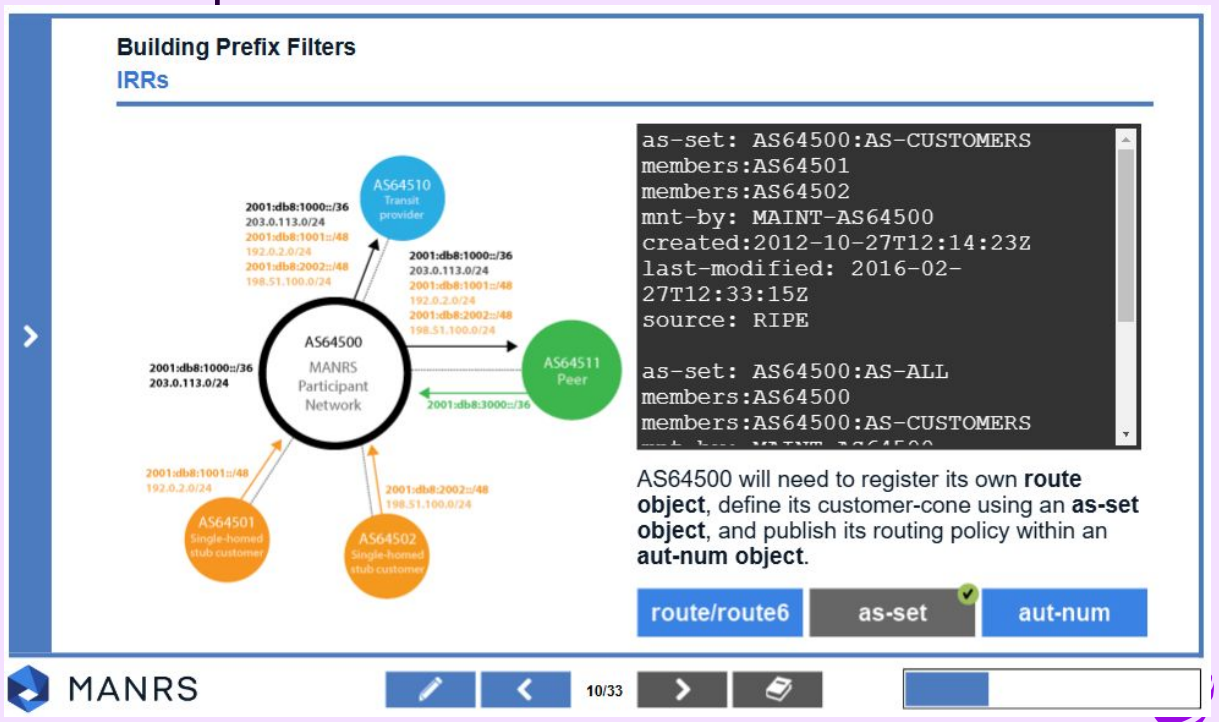


What is an AS-SET anyway?

- Just a list of AS's
- Can be used for anything:
  - AS's present at my IXP.
  - AS's I have a BGP-session with somewhere.
  - AS's whose sales-people bought me a beer at the latest conference.

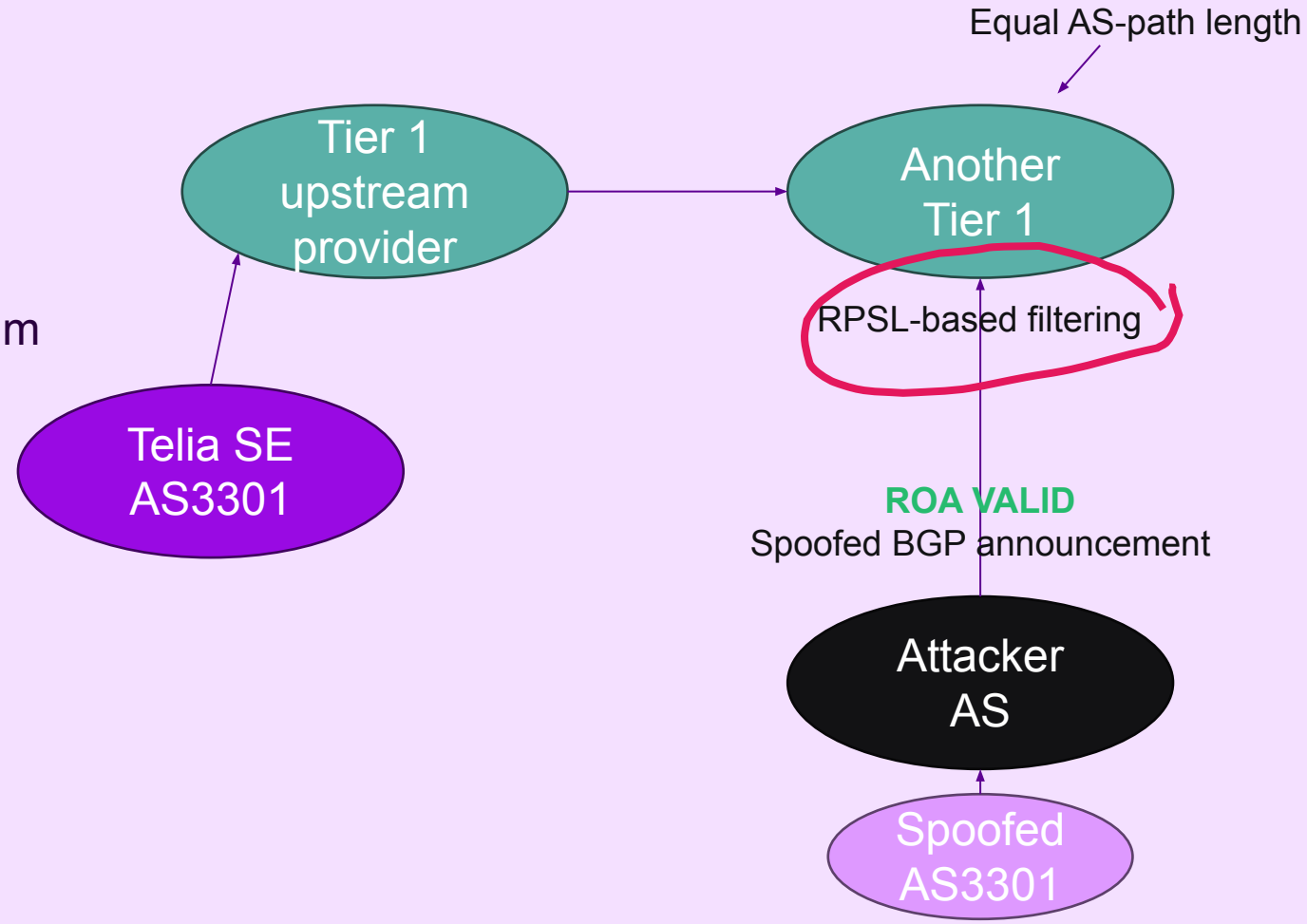
- **Most common recommended usage:**
  - IP-transit providers filtering BGP-announcements from their customers

- Example from MANRS:



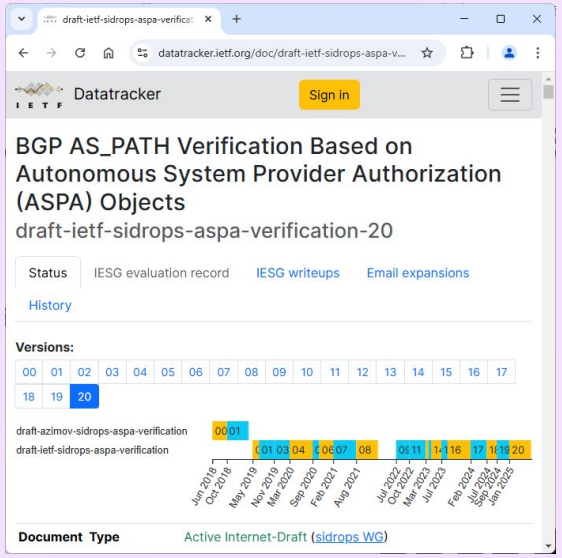
IP Transit filtering

- ROA – Route Origin Authorisation
  - Only validates the originating ASN
  - Easily spoofed
- RPSL-based filtering
  - Based on AS-Set, route(6) and aut-num objects
  - Best practice (MANRS)



What can we do about fraudulent AS-sets?

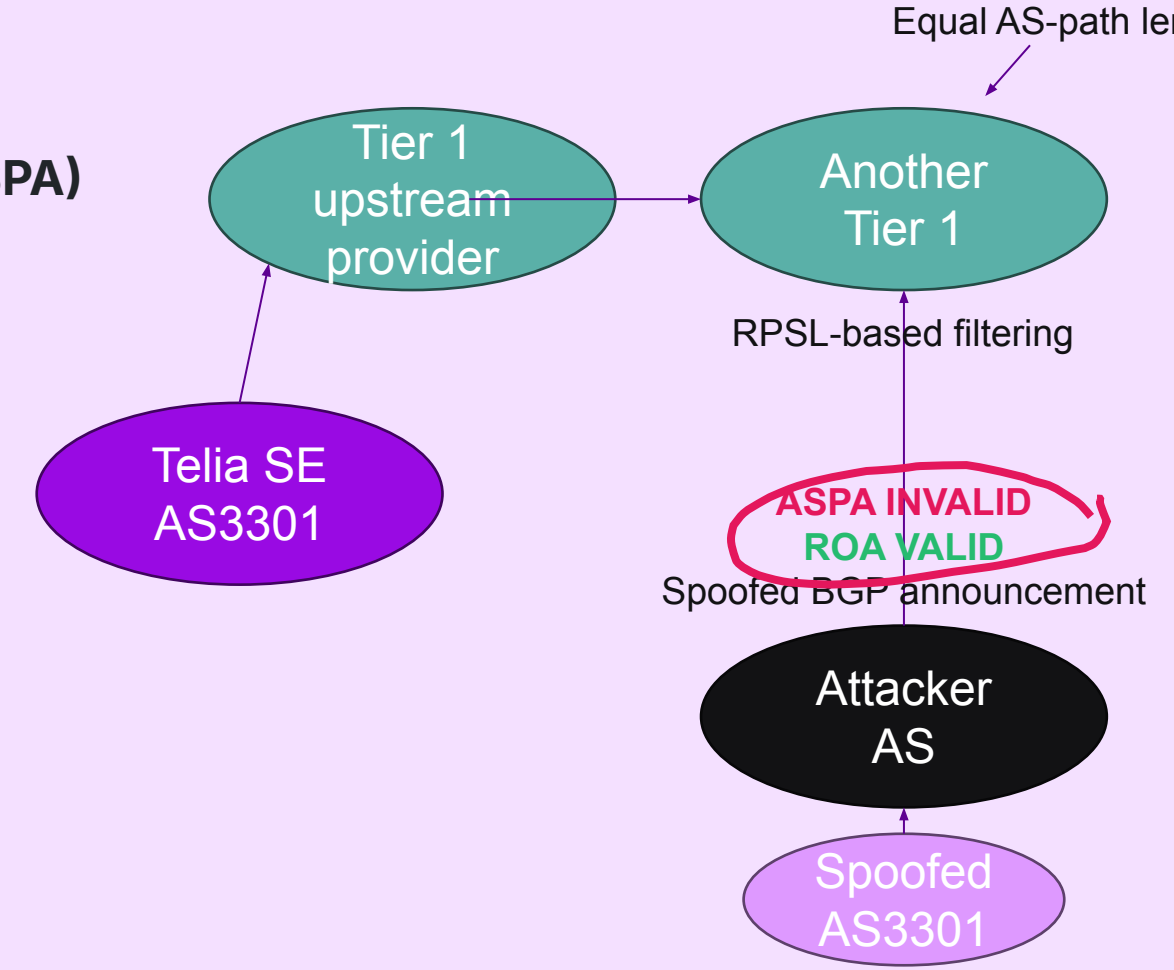
- **ASPA**
  - **Autonomous System Provider Authorization**
  - Currently going through IETF
  - Not ready yet



- **Monitoring IRR's**
  - IRRexplorer
  - BGP.tools
  - Etc.

What to do?
ASPA

- **ASPA** was designed specifically against this
  - **Autonomous System Provider Authorization (ASPA)**
  - In short: “Who are my allowed upstreams?”
  - Still being worked on in IETF – “Real Soon Now[tm]”



Soon: IETF SIDROPS WGLC

- WGLC = Working Group Last Call ("*speak now or silent forever*")
- Operators must be able to test the system *end-to-end*
  a. Publish ASPA in test environment of RIR
  b. Run a validator to fetch it
  c. Feed it via RTR to a router
  d. See on the router which routes are rejected/accepted
  e. Use SLURM to locally override above results

The ASPA drafts are interconnected, they form a 'cluster'

What are the ASPA components?

- draft-ietf-sidrops-aspa-profile
  - (how to encode ASPA objects in DER)
- draft-ietf-sidorps-aspa-verification
  - (how to apply ASPA to BGP)
- draft-ietf-sidrops-aspa-slurm
  - (defining local overrides)
- draft-ietf-sidrops-8210bis
  - (RPKI-To-Router specification)

Already today lots of software!

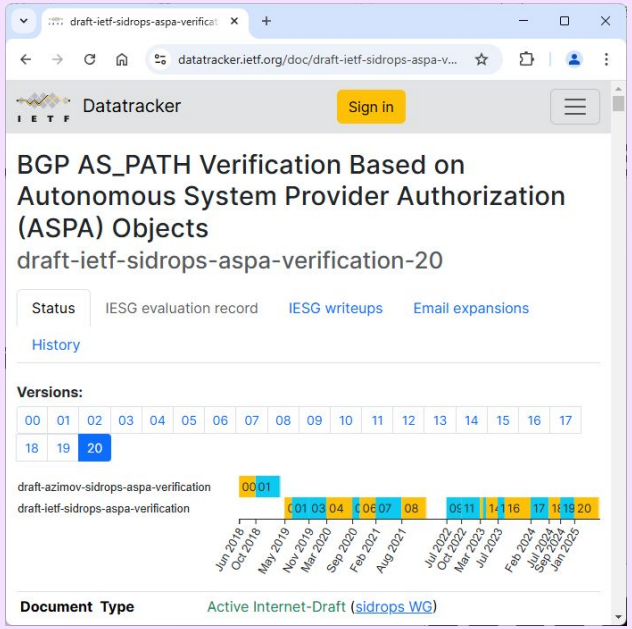
- OpenBGPD
- BIRD
- Rpki-client
- Routinator
- Rtrlib
- StayRTR

- Next year: Cisco? Juniper? Huawei?

ASK YOUR VENDOR!

What can we do about fraudulent AS-sets?

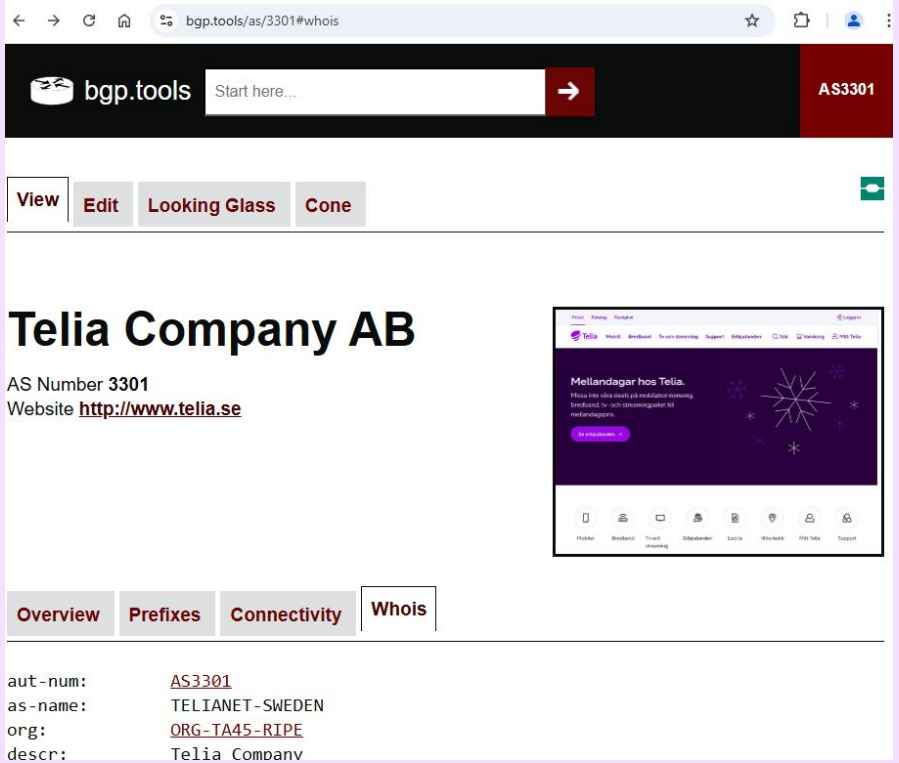
- **ASPA**
  - **Autonomous System Provider Authorization**
  - Currently going through IETF
  - Not ready yet

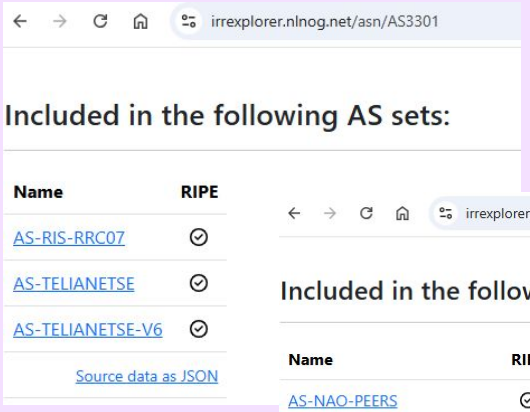


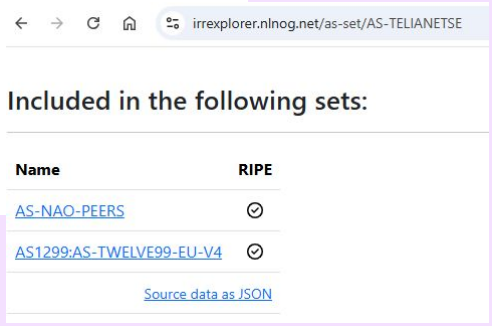
- Monitoring IRR's
  - Why would you need a "Peering" AS-set?
  - Are you sure your "Peering" AS-set actually only contains your peers?

What to do – right now? Monitoring IRRs

- Search for your ASN / AS-Set
  - E.g. bgp.tools, ”Whois” tab
  - irrexplorer.nlnog.net
  - Follow the chain of references
- Some automated monitoring tools, can provide automated alerts for long reference chains







Recursive monitoring

- Many many many AS-sets with questionable semantic meaning
  - E.g. Telia does not peer at DECIX Düsseldorf
- Please sanity check your AS-SET.
- Please document the semantic meaning of your AS-SET.