

Prelude to a BGP hijack?

Improper uses of AS-sets?

Lasse Jarlskov

Lasse.jarlskov@teliacompany.com

What happened?

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



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

Start here... →

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



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
```

```
jarlskov@helium: ~
% Information related to 'AS59580'

% Abuse contact for 'AS59580' is 'abuse@ip-transit.ir'

aut-num:       AS59580
as-name:       BATTERFLYAIMEDIA-AS
org:           ORG-BM16-RIPE
import:        from AS3356 accept ANY
import:        from AS43350 accept ANY
export:        to AS43350 announce AS59580
import:        from AS174 accept ANY
export:        to AS3356 announce AS59580
export:        to AS174 announce AS59580
import:        from AS1299 accept ANY
export:        to AS1299 announce AS59580
export:        to AS1299 announce AS59580:AS-ALL
sponsoring-org: ORG-DCL55-RIPE
admin-c:       BIN21-RIPE
tech-c:        BIN21-RIPE
status:        ASSIGNED
mnt-by:        RIPE-NCC-END-MNT
mnt-by:        MNT-BATTERFLYAIMEDIA
created:       2012-08-14T11:26:35Z
last-modified: 2024-10-02T18:35:07Z
source:        RIPE

organisation:  ORG-BM16-RIPE
org-name:      ██████████
country:       RU
org-type:      OTHER
address:       Tehran, Iran
e-mail:        noc@ip-transit.ir
notify:        noc@ip-transit.ir
e-mail:        info@ip-transit.ir
abuse-c:       AR26101-RIPE
mnt-ref:       MNT-BATTERFLYAIMEDIA
mnt-by:        MNT-BATTERFLYAIMEDIA
created:       2012-08-03T18:51:38Z
last-modified: 2022-12-01T16:18:08Z
source:        RIPE

role:          BATTERFLYAIMEDIA IP-TRANSIT NOC
address:       224 Khoramshahr ave
address:       No. 5C
address:       Tehran 15337
address:       Iran
e-mail:        noc@ip-transit.ir
abuse-mailbox: abuse@ip-transit.ir
nic-hdl:       BIN21-RIPE
mnt-by:        MNT-BATTERFLYAIMEDIA
phone:         +98 21 8220 8712
fax-no:        +98 21 8220 8712
created:       2014-09-25T08:12:53Z
```

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:

Building Prefix Filters
IRRs

```
as-set: AS64500:AS-CUSTOMERS
members:AS64501
members:AS64502
mnt-by: MAINT-AS64500
created:2012-10-27T12:14:23Z
last-modified: 2016-02-27T12:33:15Z
source: RIPE

as-set: AS64500:AS-ALL
members:AS64500
members:AS64500:AS-CUSTOMERS
```

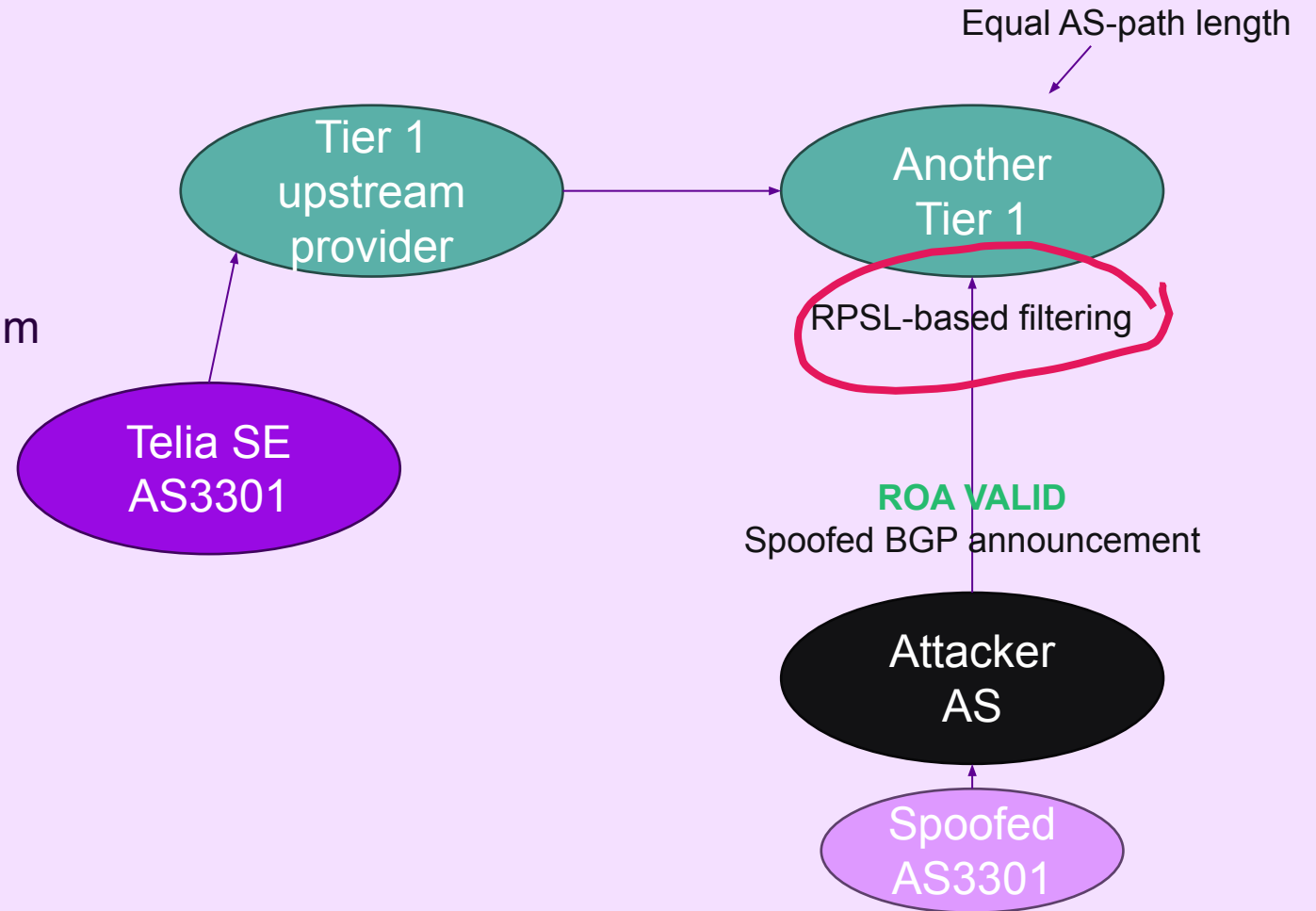
AS64500 will need to register its own **route object**, define its customer-cone using an **as-set object**, and publish its routing policy within an **aut-num object**.

route/route6 as-set aut-num

MANRS 10/33

IP Transit filtering

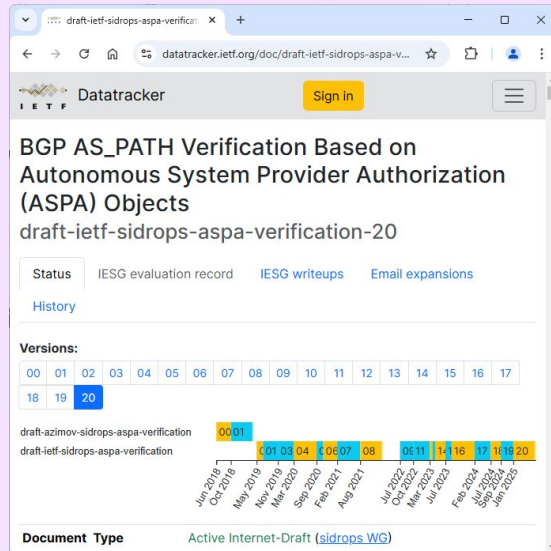
- ROA – Route Origin Authorisation
 - Only validates the originating ASN
 - Easily spoofed
- RPSL-based filtering
 - Based on AS-Set, route(6) and aut-num objects
 - Best practice (MANRS)



What can we do about fraudulent AS-sets?

ASPA

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



Monitoring IRR's

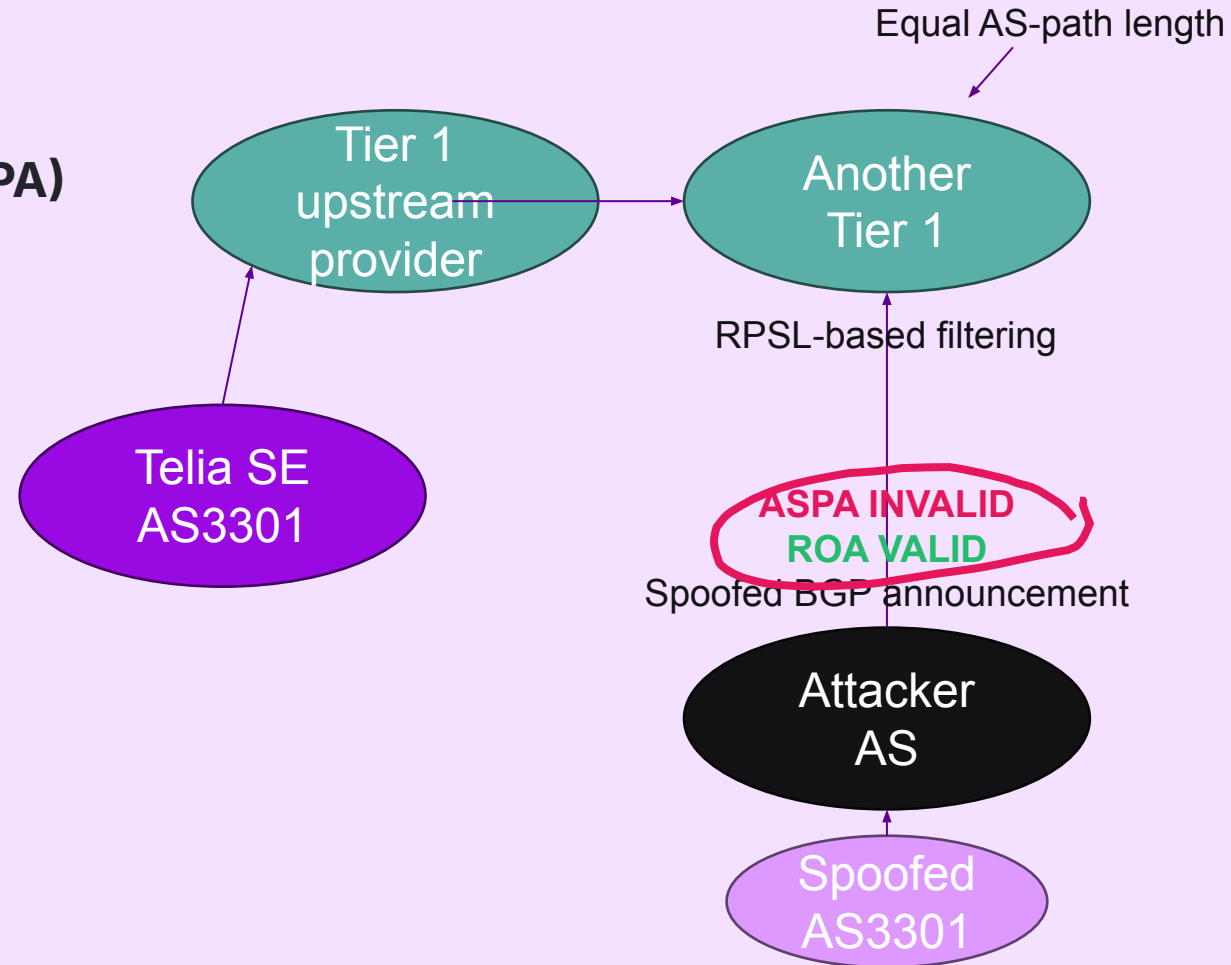
- IRRexplorer
- BGP.tools
- Etc.



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?

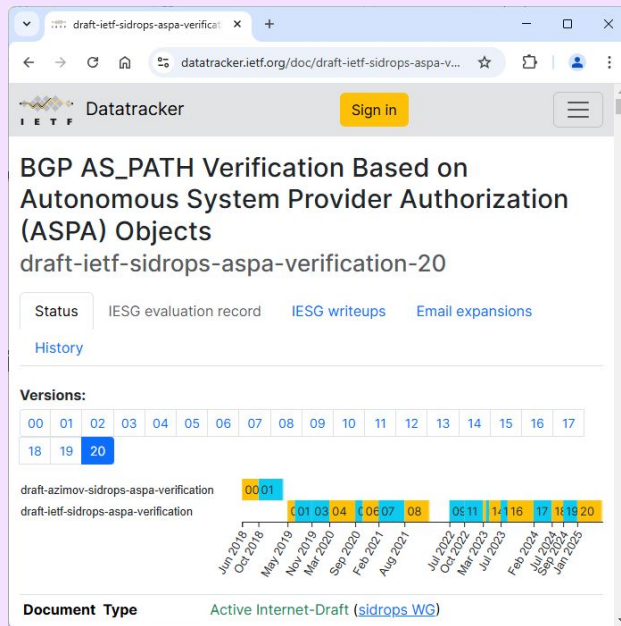
ASK YOUR VENDOR!



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

bgp.tools Start here... AS3301

View Edit Looking Glass Cone

Telia Company AB

AS Number 3301
Website <http://www.telia.se>

Overview Prefixes Connectivity **Whois**

aut-num: AS3301
as-name: TELIANET-SWEDEN
org: ORG-TA45-RIPE
descr: Telia Companv

Member of the following AS-SETs

-	Member	ASN Count
RIPE	as-telianetse-v6	8242
RIPE	as-telianetse	8287
RIPE	as-ris-rrc07	21

irrexplorer.nlnog.net/asn/AS3301

Included in the following AS sets:

Name	RIPE
AS-RIS-RRC07	☑
AS-TELIANETSE	☑
AS-TELIANETSE-V6	☑

[Source data as JSON](#)

irrexplorer.nlnog.net/as-set/AS-TELIANETSE

Included in the following sets:

Name	RIPE
AS-NAO-PEERS	☑
AS1299:AS-TWELVE99-EU-V4	☑

[Source data as JSON](#)



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.

AS3301 now appears in "as56890:as-decix-dus" (RIPE) when recursed.

The screenshot shows the 'View Alert Detail' page on bgp.tools. The browser address bar shows the URL: `bgp.tools/authed/manage-alerts?detail=9ca059ba-086c-41...`. The page header includes the bgp.tools logo, a search bar with 'Start here...' and a right arrow, and a status bar indicating 'Logged in as AS3301'. The navigation menu contains: Home, Contacts, BGP Sessions, Monitoring (active), Settings, Log out. A secondary menu below shows: Settings, Alerts (active), Historical. The main content area is titled 'Alert Detail' and contains the following information:

- Alert For:** AS3301
- Alert Type:** Recursively included in an AS-SET ([More details on this alert type](#))
- Date:** 2025-02-21 16:23:05 +0000 UTC
- IRR Database:** RIPE
- AS-SET Changed:** as56890:as-decix-dus
- AS-SET Recursion Path:** as56890:as-decix-dus -> AS-NETIX-NET -> as-netix-int (RIPE) -> AS-DIGICOMMPS (RIPE) -> as200455:as-peers (RIPE) -> AS-LOCIX (RIPE) -> AS-BALKAN-IX (RIPE) -> AS-DATAIX (RIPE) -> AS-EURASIAPEERING_RS (RIPE) -> AS-TRANSROUTE-2 (RIPE) -> as-piter-ix-msk (RIPE) -> AS-IPTT (RIPE) -> as-piter-ix (RIPE) -> AS-TELIANET (RIPE) -> AS-TELIANETEU (RIPE) -> as1299:as-twelve99-eu-v4 (RIPE) -> AS-TELIANETSE (RIPE)

On the right side of the page, there is a 'Log out' button and a link for '[More details on this](#)'.