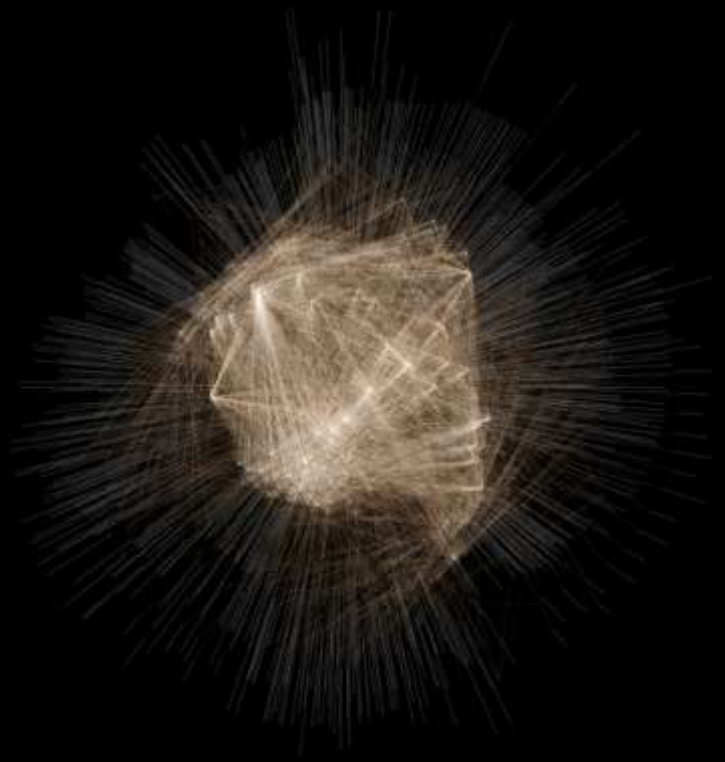


Cloud based BGP hijack and anomaly detection technique

Andis Āriņš, University of Latvia
Cybersecurity conference Cyberchess 2017
2017.10.05

Andis Āriņš

- PhD Student @ Latvian University
- Review expert for EU in future networking research
- LIA board member

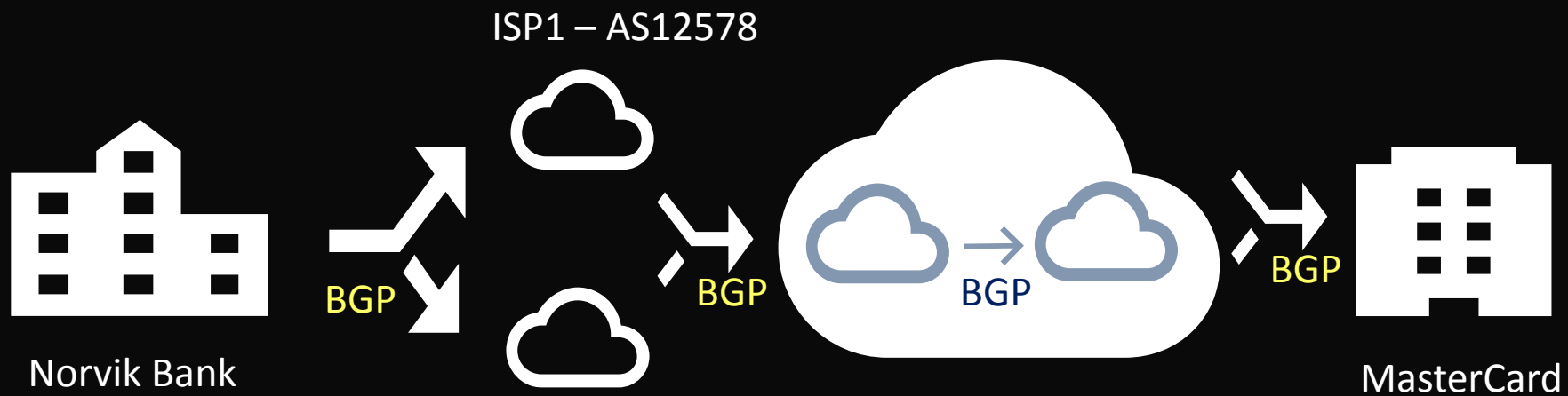
- 15 years in commercial networking
- MikroTik/Microsoft certified tainer
- Cisco CCIP/CCDP/CCNP+voice+security

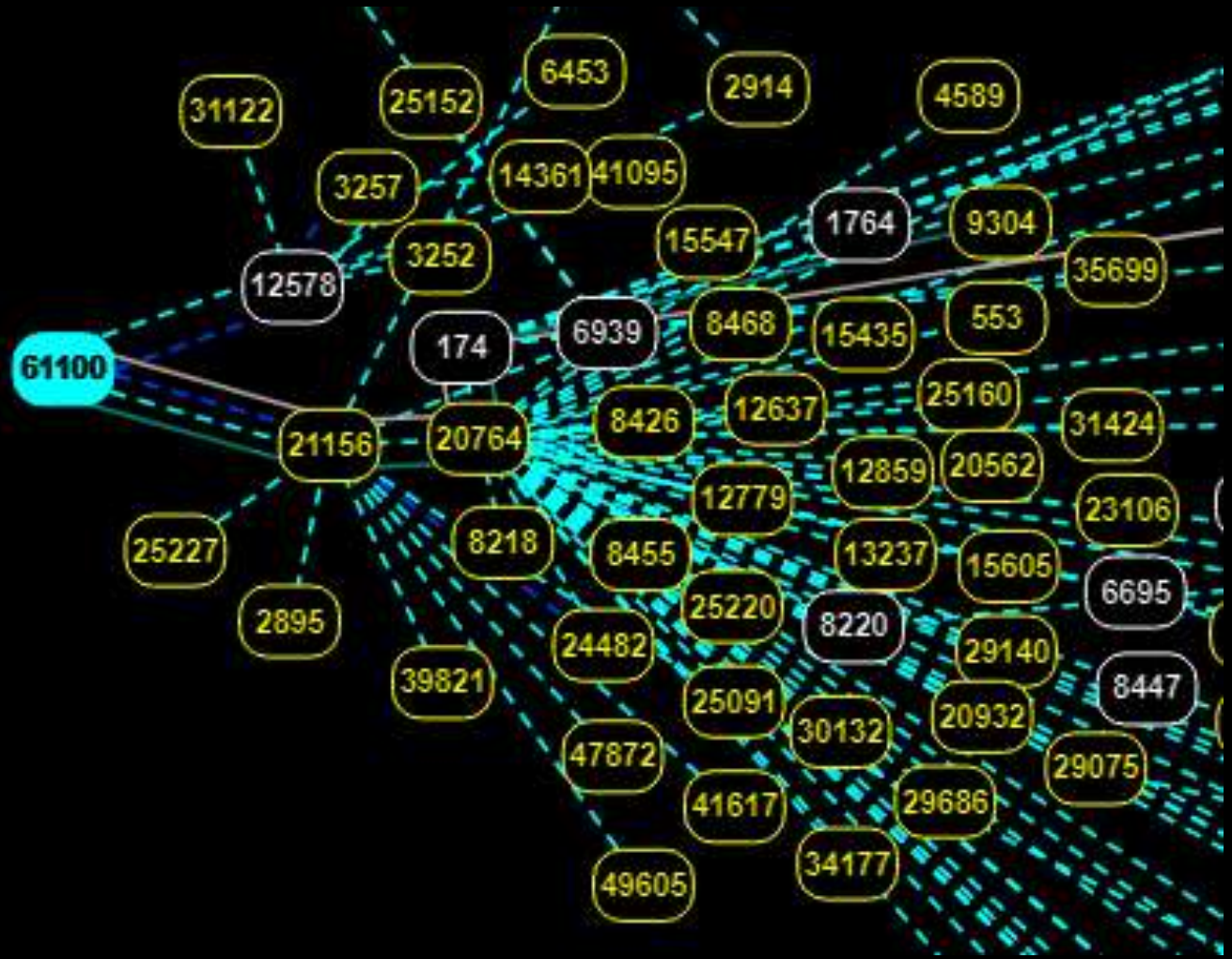
BGP Hijack Case Study

http://www.delfi.lv/bizness/tehnologijas/krievijas-valsts-telekomunikaciju-uznemums-partver-divu-latvijas-banku-datus.d?id=48806779

http://nra.lv/latvija/209001-krievijas-telekomunikaciju-uznemums-partveris-norvik-un-dnb-bankas-datus.htm

How BGP should work normally ?





https://stat.ripe.net/widget/bgplay#w.resource=194.153.135.0/24

traceroute ipv4 216.119.216.1 from AS12578

Thu Oct 5 07:05:17.068 EEST

2914 32787 26380

1 87.110.223.130 0 msec 0 msec
2 83.231.187.189 7 msec 7 msec 7 msec
3 129.250.7.16 [MPLS: Label 457009 Exp 0] 27 msec 27 msec 27 msec
4 129.250.6.207 27 msec 28 msec 27 msec
5 213.198.77.210 27 msec
   212.119.27.234 30 msec 29 msec
6 72.52.48.194 29 msec
   72.52.48.202 26 msec
   72.52.48.192 26 msec
7 72.52.48.197 27 msec 27 msec 28 msec
8 93.191.173.3 114 msec 114 msec
   93.191.173.63 113 msec
9 209.200.146.126 129 msec 130 msec 130 msec
10 * * *

Looking glass from AS12578

2914 32787 26380

```
Router: Riga IC1
Command: show bgp ipv4 unicast 216.119.216.1

Sun Oct  1 22:50:04.555 EEST
BGP routing table entry for 216.119.216.0/24
Last Modified: Feb 16 23:10:41.748 for 32w2d
Paths: (3 available, best #3)
  Advertised to update-groups (with more than one peer):
    0.4 0.10
  Advertised to peers (in unique update groups):
    87.110.223.186  195.13.224.34   195.13.213.242  195.13.173.134
    195.13.173.6
  Path #1: Received by speaker 0
  Not advertised to any peer
  1299 32787 26380 26380 26380
    62.115.144.74 from 1 (80.91.242.1)
      Origin IGP, localpref 100, weight 40, valid, external, group-best
      Received Path ID 0, Local Path ID 0, version 0
      Community: 12578:300
      Origin-AS validity: not-found
  Path #2: Received by speaker 0
  Not advertised to any peer
  3257 2914 32787 26380 26380 26380
    77.67.67.89 from 1 (213.200.87.15)
      Origin IGP, metric 0, localpref 100, weight 40, valid, external, group-best
      Received Path ID 0, Local Path ID 0, version 0
      Community: 12578:100 12578:3257
      Origin-AS validity: not-found
  Path #3: Received by speaker 0
  Advertised to update-groups (with more than one peer):
    0.4 0.10
  Advertised to peers (in unique update groups):
    87.110.223.186  195.13.224.34   195.13.213.242  195.13.173.134
    195.13.173.6
  2914 32787 26380
    87.110.223.15 (metric 2) from 1 (87.110.223.15)
      Origin IGP, metric 8037, localpref 200, weight 40, valid, internal, best, group-best
      Received Path ID 0, Local Path ID 0, version 346063870
      Community: 12578:300
```

36 network prefixes affected

202.138.100.0/24 Reliance Communications Bangalore IN

145.226.109.0/24 Euro-Information-Europeenne FR

193.58.4.0/24 Fortis Bank N.V. Brussels Bruxelles-Capitale BE

217.75.242.0/24 Servicios de Hosting en Internet S.A. ES

194.153.135.0/24 Norvik Banka LV

93.190.87.0/24 Modrium Mdpay Oy Nord-Trøndelag Fylke NO

217.117.65.0/24 NET_217_117_65 UA

195.76.9.0/24 REDSYS SERVICIOS DE PROCESAMIENTO SLU

64.75.29.0/24 Arcot Systems, Inc. Sunnyvale CA US

206.99.153.0/24 Savvis Singapore SG

198.241.161.0/24 VISA INTERNATIONAL CO US

203.112.91.0/24 HSBC banking and financial srv Hong Kong HK

196.38.228.0/24 Internet Solutions Johannesburg Gauteng ZA

216.136.151.0/24 Savvis Arlington VA US

198.161.246.0/24 EMC Corporation Southborough MA US

212.243.129.0/24 UBS Card Center AG Glattbrugg Kanton Zürich CH

203.112.90.0/24 HSBC banking and financial services Hong Kong HK

216.150.144.0/24 Xand Corporation Farmingdale NY US

source: https://bgpstream.com

195.20.110.0/24 Bank Zachodni WBK S.A. PL

193.16.243.0/24 Servicios Para Medios De Pago S.A. ES

202.187.53.0/24 TIME DOTCOM BERHAD Shah Alam Selangor MY

160.92.181.0/24 Worldline France hosting FR

145.226.45.0/24 Euro-Information-Europeenne FR

195.191.110.0/24 card complete Service Bank AG Vienna Wien AT

193.104.123.0/24 PROVUS SERVICE PROVIDER SA București RO

69.58.181.0/24 Verisign, Inc. New York NY US

194.5.120.0/24 DOCAPOST BPO SAS FR

89.106.184.0/24 Worldline SA Frankfurt am Main Hessen DE

217.75.224.0/19 Servicios de Hosting en Internet S.A. Madrid ES

195.114.57.0/24 DNBNORD PLC LV

198.241.170.0/24 VISA INTERNATIONAL CO US

216.119.216.0/24 MasterCard Technologies LLC MO US

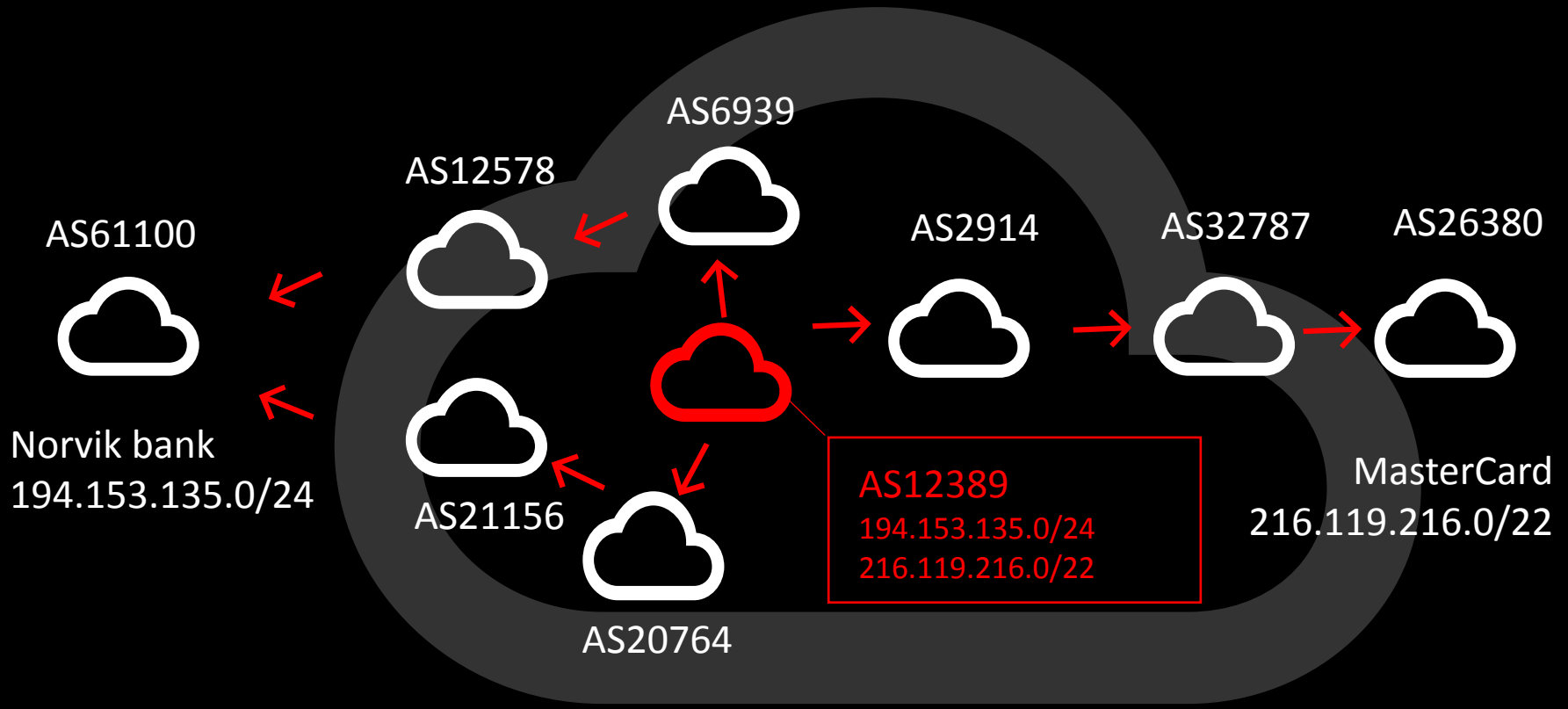
193.203.231.0/24 SIA S.p.A. Milano Lombardia IT

65.205.249.0/24 Symantec Inc Mountain View CA US

194.126.145.0/24 Netcetera AG Zürich Kanton Zürich CH

65.205.248.0/24 Symantec Inc Mountain View CA US

What happened during hijack?

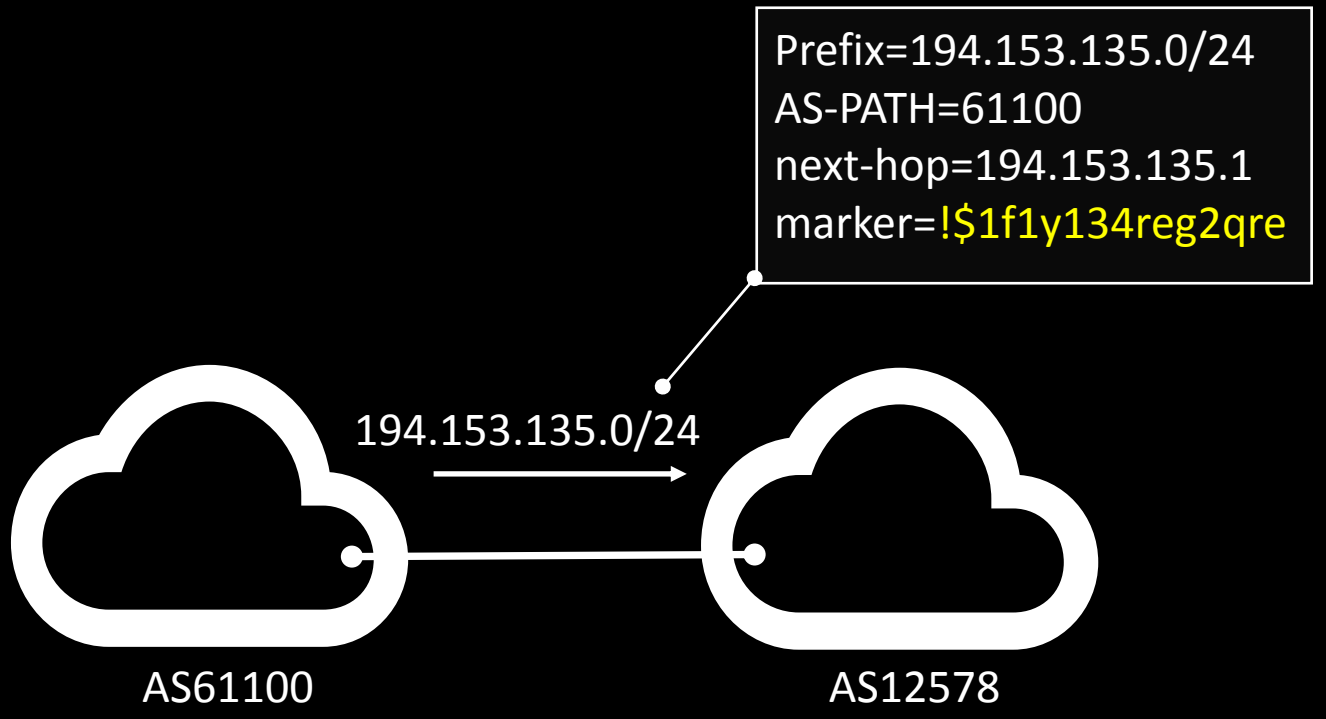


Normal AS-PATH from Norvik to Mastercard: 12578,2914,32787,26380

Hijacked AS-PATH from Norvik to Mastercard : 12578,12389 or 12578,transit-as,12389
If hijacker was more tricky, as-path could be: 12578,12389,26380

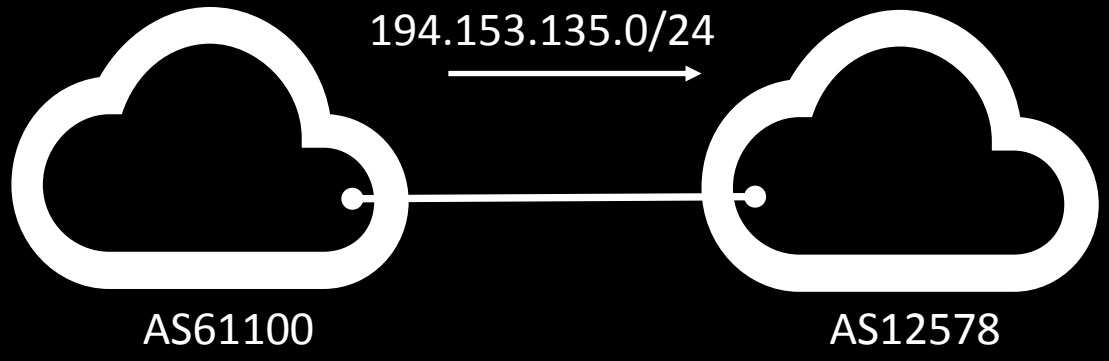
BGP Hijacking Prevention

1. Peering with MD5



BGP Hijacking Prevention

2. IP Prefix Filtering



ip prefix-list as61100in seq 10 permit 194.153.135.0/24

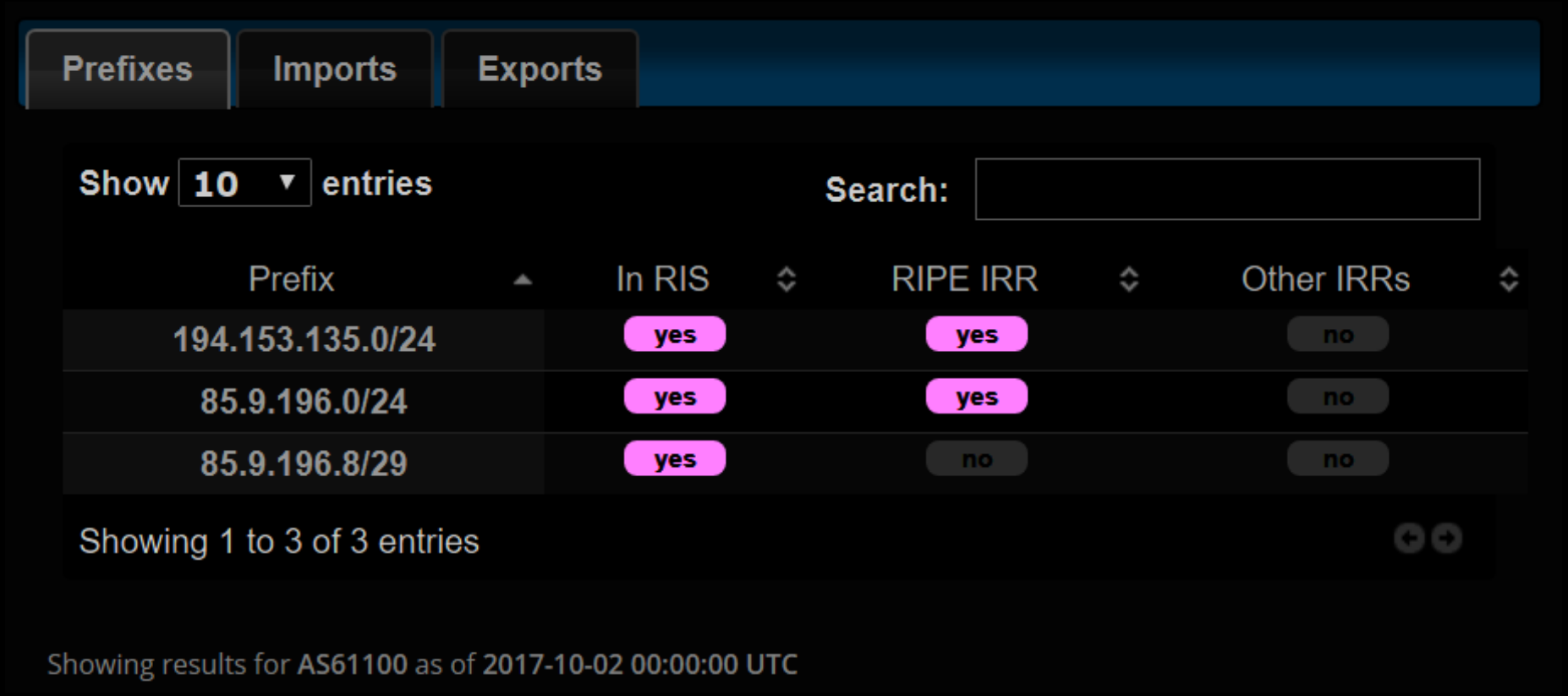
router bgp 12578
neighbor 194.153.135.1 prefix-list as61100in in

BGP Hijacking Prevention

3. IP Prefix Filtering + RIR (or similar) DB

```
aut-num:        AS61100
as-name:        NVKB-AS
org:            ORG-NBA20-RIPE
import:         from AS21156 accept ANY
import:         from AS6747 accept ANY
export:         to AS21156 announce AS61100
export:         to AS6747 announce AS61100
admin-c:        NVKB-RIPE
tech-c:         NVKB-RIPE
remarks:        For information on "status:" attribute
tools/db/faq/faq-status-values-legacy-resources
status:         ASSIGNED
mnt-by:         RIPE-NCC-END-MNT
mnt-by:         NVKB-MNT
created:        2013-02-18T08:37:49Z
last-modified:  2016-04-14T08:57:26Z
source:         RIPE
sponsoring-org: ORG-DA15-RIPE
```

AS Routing Consistency (AS61100)



https://stat.ripe.net/as61100#tabId=database

BGP Hijacking Prevention

4. Resource Public Key Infrastructure (RPKI)

Routing Origin Authorization (ROA) states:

- Announcing AS number
- Address range
- Maximum length

- There can be multiple ROAs for an IP range
- ROAs can overlap

ROA example

194.153.135.0/24
AS 61100

Max Length:

194.153.135.0/24

194.153.134.0/23

194.153.135.0/25

ROA example in LV

Announced By		
Origin AS	**Announcement**	**Description**
AS25107	80.233.138.0/24	MTB-Bank

Less Specific Announcements		
Origin AS	**Announcement**	**Description**
AS5518	80.233.128.0/17	Telia Latvija SIA

https://bgp.he.net/net/80.233.138.0/24

Announced By		
Origin AS	**Announcement**	**Description**
AS41333	80.233.246.0/24	

Less Specific Announcements		
Origin AS	**Announcement**	**Description**
AS5518	80.233.128.0/17	Telia Latvija SIA

https://bgp.he.net/net/80.233.246.0/24

ROA weakness

RPKI only validates if an origin AS is authorized to announce a prefix.

However, RPKI does not check if the entire path is correct. Attacker can bypass it by adding the origin AS at the end of AS_PATH in a BGP update message

61100,12578,12389,26380

BGP Hijacking Prevention

5. BGPSec

https://tools.ietf.org/html/rfc8205
September 2017

BGPSec confirms that the entire path from the source AS to the destination is valid. Each router on the path injects not only its own AS along with prefix but also the AS number of neighbor to whom it is going to send an BGP update message.

BGPsec to work, there must be an unbroken path of BGPsec-capable routers between where a BGP update is originated and where it’s validated. When a BGPsec-capable router talks to a regular BGP router, it converts the BGPsec_Path to a regular AS_PATH, stripping off all security information in the process

Proposed method: digitally signed announcement

Prefix=194.153.135.0/24
AS-PATH=61100
next-hop=194.153.135.1
AS61100-signature=signed with PKI private key

Reciever validates digital signature in received prefix path attributes using reverse-DNS against network address of prefix.

0.135.153.194.in-addr.arpa.

BGP = PKI public-key

Thank you, that’s it!