RIPE NCC

RIPE NETWORK COORDINATION CENTRE

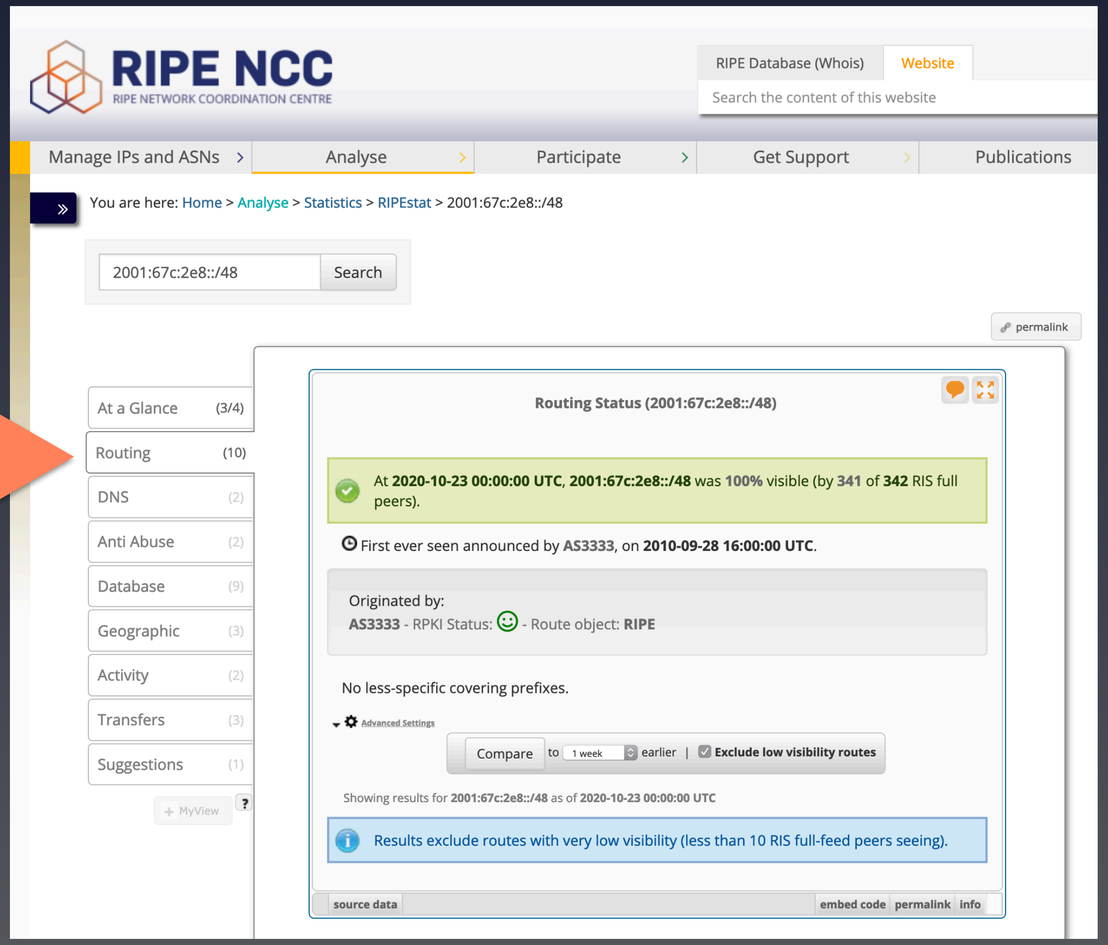
Troubleshooting BGP Issues with RIS and RIPEstat

Oleg Muravskiy | ENOG 17 | 9 November 2020

Contents

- Overview of Routing Widgets
- Looking Glass
- RIS Live
- BGPlay
- RPKI
- Raw Data / bgpdump
- New UI

RIPEstat Routing Widgets



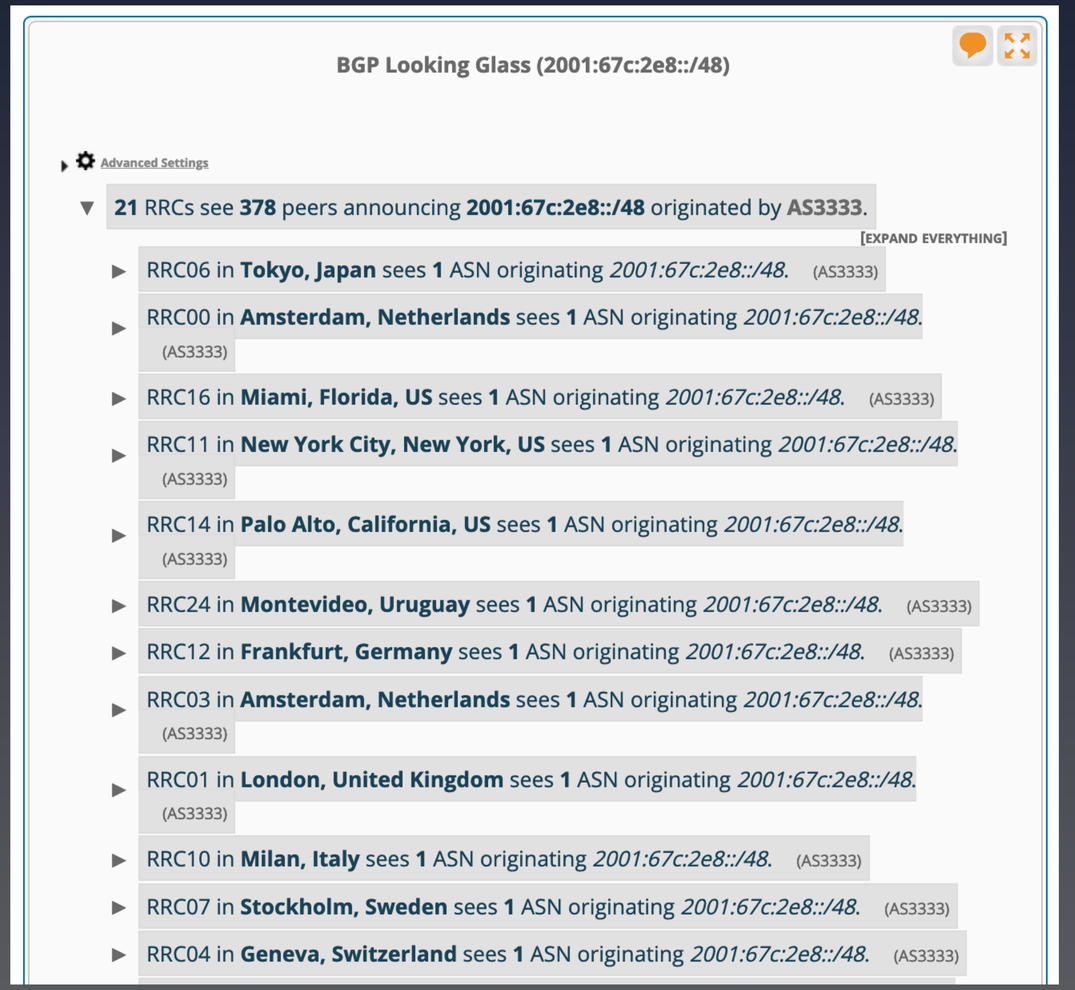
- Routing Status
- BGPlay
- BGP Update Activity
- Routing History
- Looking Glass
- Visibility
- Related Prefixes
- Prefix Routing Consistency
- Upstream Visibility

Full widget list:
stat.ripe.net/widget/list

RIS Looking Glass

How are my prefixes seen right now?

- Simultaneous view of a prefix from all peers
- The most up-to-date RIPEstat widget



RIS Live

Is anybody hijacking my space?

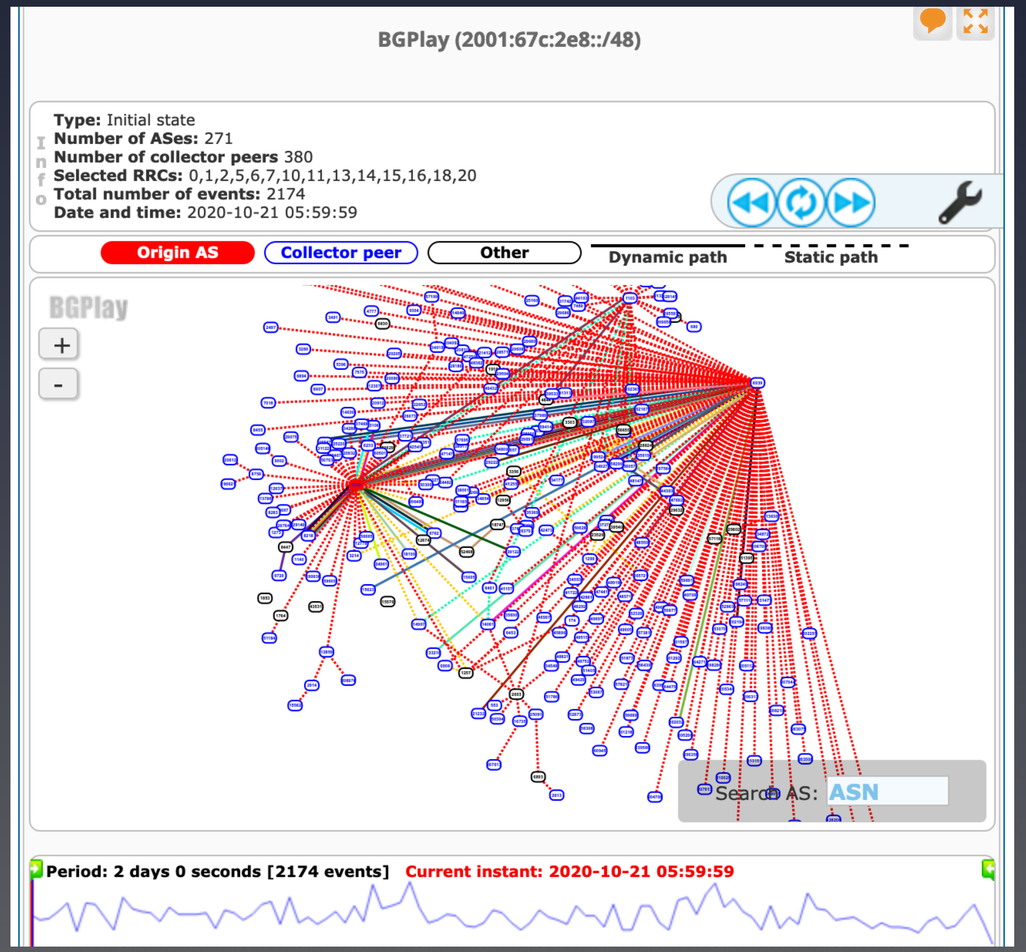
- https://ris-live.ripe.net/
- Feed of BGP messages in real time through web-sockets

- BGPalerter
- https://github.com/jaredmauch/rislive
- https://github.com/morrowc/rislive

BGPlay

How neighbour ASes interact on updates?

- https://stat.ripe.net/widget/bgplay
- RIPE Labs: BGPlay Integrated in RIPEstat



Example Case: RIS Beacons

- RIS Beacons
  - Announce at 00:00, 04:00, …
  - Withdrawal at 02:00, 06:00, …
  - BGPlay replay
- RIS “anycast simulation” beacons
  - Continuous announce from RRC14
  - Announce/withdrawal from RRC03 every 2 hours
  - BGPlay replay

How exactly did THAT happen?

Digging through raw data

- Download files from data.ris.ripe.net
  - Files are in MRT format (RFC 6396)
  - RIB dumps (bview.*.gz) every 8 hours
  - BGP updates (updates.*.gz) grouped per 5 min
- You need tools to parse them:
  - bgpdump
  - bgpscanner
  - mrtparse
  - go-mrt

bgpdump

- use `-v` flag (log to STDERR)
- use `-m` or `-M` for single-line output

oleg@ommbp:~

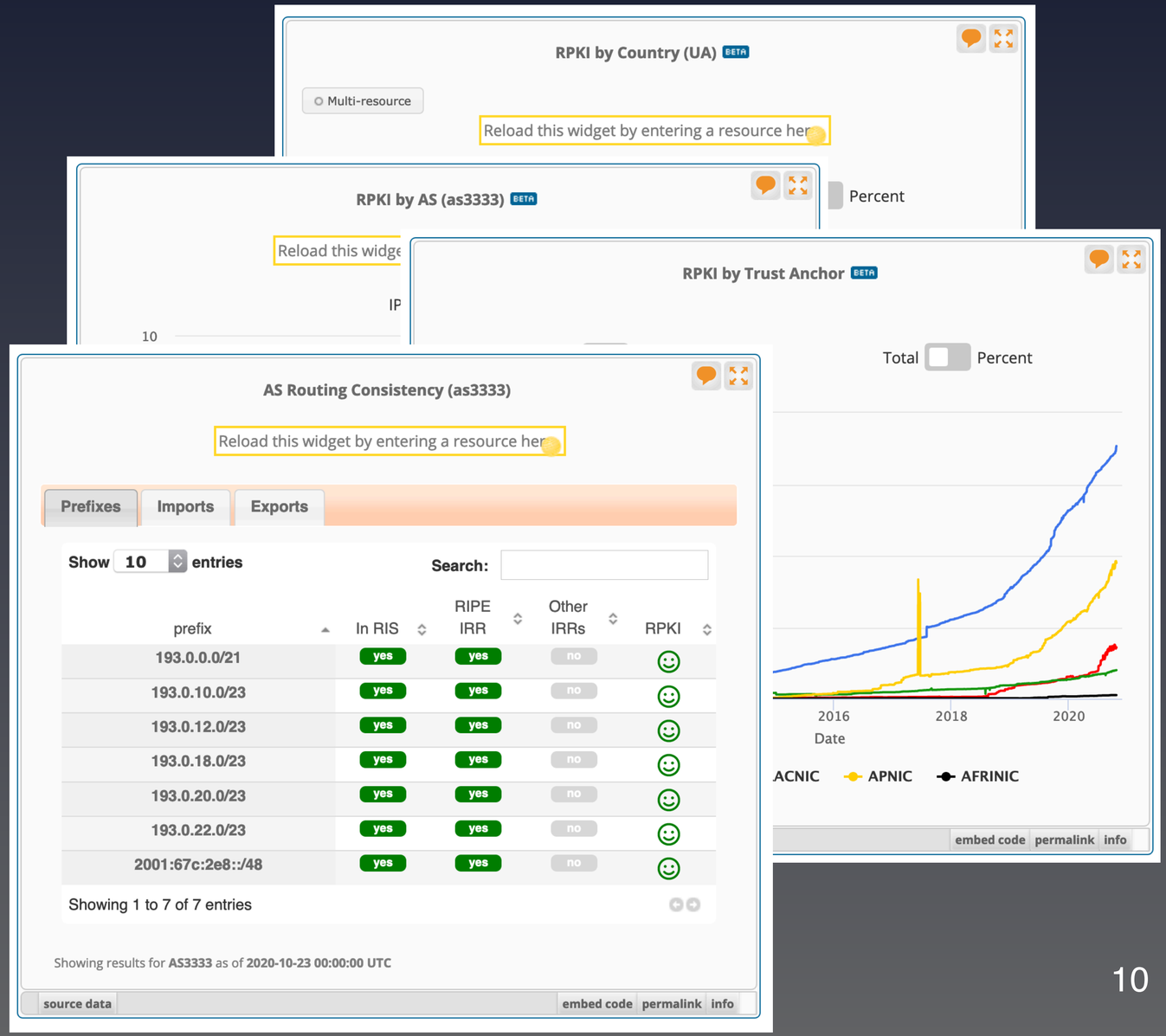
```
$ bgpdump -v updates.20201107.2000.gz | head -20
TIME: 11/07/20 20:00:01
TYPE: BGP4MP/MESSAGE/Keepalive
FROM: 2001:7f8:2a::2:1:2:940 AS20940
TO: 2001:7f8:2a::1:1:1:2654 AS12654

TIME: 11/07/20 20:00:04
TYPE: BGP4MP/MESSAGE/Update
FROM: 193.242.98.98 AS60082
TO: 193.242.98.118 AS12654
WITHDRAW
  185.137.56.0/22

TIME: 11/07/20 20:00:04
TYPE: BGP4MP/MESSAGE/Keepalive
FROM: 193.242.98.133 AS24592
TO: 193.242.98.118 AS12654

TIME: 11/07/20 20:00:05
TYPE: BGP4MP/MESSAGE/Keepalive
FROM: 193.242.98.38 AS13041
```

oleg@ommbp:~

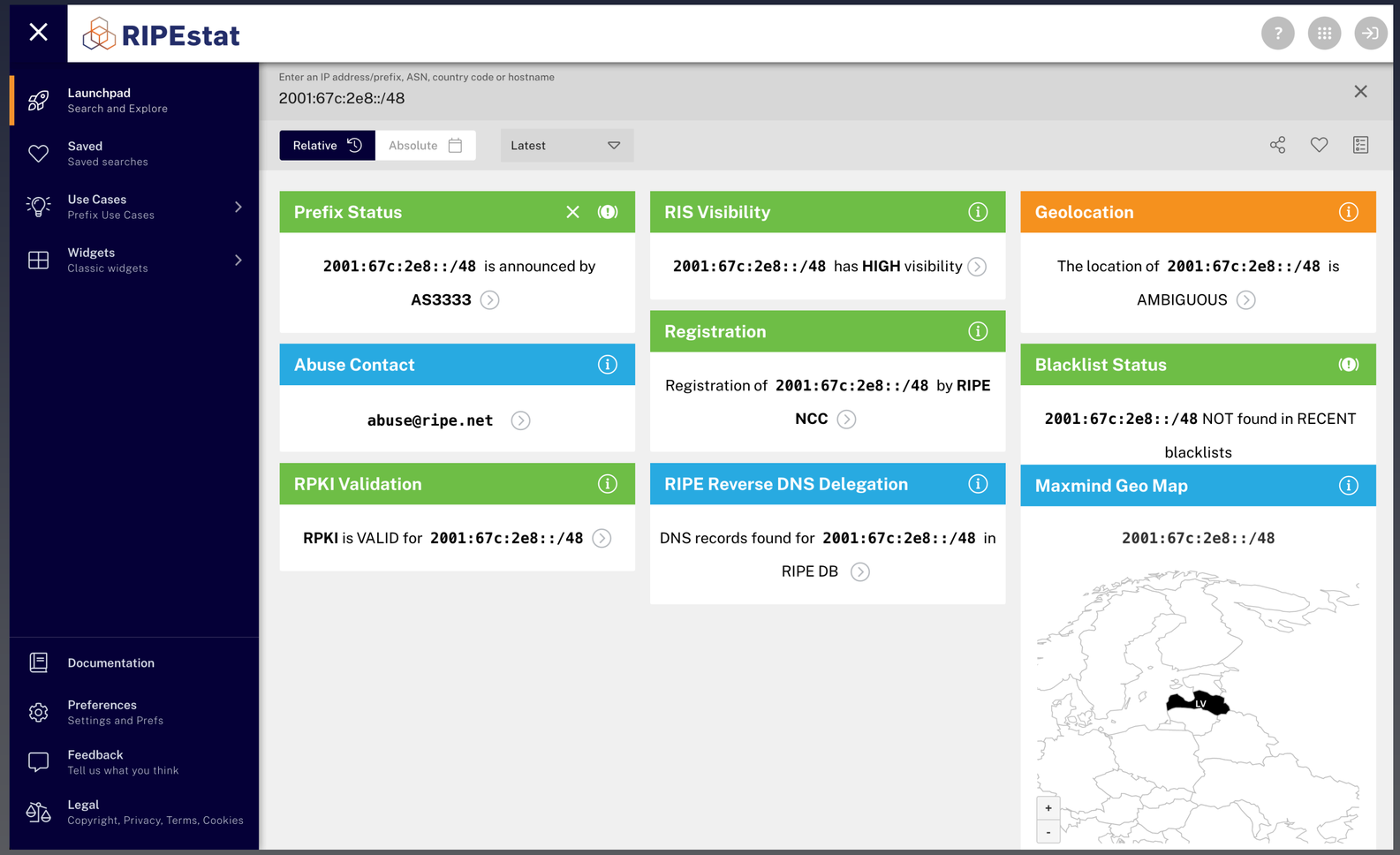
```
$ bgpdump -vm updates.20201107.2000.gz | head -20
BGP4MP|1604779204|W|193.242.98.98|60082|185.137.56.0/22
BGP4MP|1604779212|A|193.242.98.98|60082|185.137.56.0/22|29119|IGP|193.242.98.136|0|0|29119:2 29119:29119 64512:11 64512:21
BGP4MP|1604779212|W|193.242.98.98|60082|185.137.56.0/22
BGP4MP|1604779212|A|193.242.98.141|29680|103.78.152.0/24|29680 8220 6453 4755 17439 17439 17439 132571|IGP|193.242.98.141|
BGP4MP|1604779212|W|193.242.98.141|29680|185.235.214.0/24
BGP4MP|1604779212|A|193.242.98.141|29680|5.252.112.0/22|29680 3257 855|IGP|193.242.98.141|0|0|3257:4000 3257:8076 3257:500
BGP4MP|1604779212|A|193.242.98.141|29680|93.175.149.0/24|29680 8218 12654|IGP|193.242.98.141|0|0|8218:101|NAG|64888 10.9.2
BGP4MP|1604779212|A|193.242.98.141|29680|84.205.71.0/24|29680 9002 12654|IGP|193.242.98.141|0|0||NAG|65011 10.9.2.64|
BGP4MP|1604779212|A|193.242.98.141|29680|84.205.68.0/24|29680 8220 12654|IGP|193.242.98.141|0|0|8220:65000 8220:65120 8220
BGP4MP|1604779212|A|193.242.98.141|29680|84.205.69.0/24|29680 8218 12654|IGP|193.242.98.141|0|0|8218:101|NAG|64872 10.9.2.
BGP4MP|1604779212|A|193.242.98.141|29680|84.205.75.0/24|29680 9002 12654|IGP|193.242.98.141|0|0||NAG|65256 10.9.2.64|
BGP4MP|1604779212|A|193.242.98.141|29680|84.205.77.0/24|29680 9002 12654|IGP|193.242.98.141|0|0||NAG|65365 10.9.2.64|
BGP4MP|1604779212|A|193.242.98.141|29680|84.205.74.0/24|29680 8220 12654|IGP|193.242.98.141|0|0|8220:65000 8220:65060 8220
BGP4MP|1604779212|A|193.242.98.141|29680|93.175.151.0/24|29680 8220 12654|IGP|193.242.98.141|0|0|8220:65002 8220:65302 822
BGP4MP|1604779212|A|193.242.98.141|29680|84.205.70.0/24|29680 3257 2497 12654|IGP|193.242.98.141|0|0|3257:8157 3257:30213
BGP4MP|1604779212|A|193.242.98.141|29680|84.205.82.0/24|29680 3257 37271 12654|IGP|193.242.98.141|0|0|3257:4000 3257:8801
64|
BGP4MP|1604779212|A|193.242.98.141|29680|84.205.67.0/24|29680 8218 12654|IGP|193.242.98.141|0|0|8218:101|NAG|64744 10.9.2.
BGP4MP|1604779212|A|193.242.98.141|29680|84.205.72.0/24|29680 8218 12654|IGP|193.242.98.141|0|0|8218:101|NAG|64744 10.9.2.
BGP4MP|1604779212|A|193.242.98.141|29680|84.205.76.0/24|29680 8218 12654|IGP|193.242.98.141|0|0|8218:101|NAG|65320 10.9.2.
BGP4MP|1604779212|A|193.242.98.141|29680|84.205.65.0/24|29680 8218 12654|IGP|193.242.98.141|0|0|8218:101|NAG|64616 10.9.2.
```

What About Route Origin Validation?

- RPKI by AS
- RPKI by Trust Anchor
- RPKI by Country
- AS Routing Consistency



New RIPEstat UI



Questions

oleg@ripe.net
stat.ripe.net
ris.ripe.net

BGP Hijack, DNS Impersonation, Cryptocurrency Theft

- On 24 April 2018, between 11:05-12:55 (UTC), AS10297 announced five prefixes used by Amazon for Route53 authoritative DNS service
- Fake DNS servers were activated
- DNS queries for myetherwallet.com returned 46.161.42.42 with long TTLs, all other domains – SERVFAIL
- Hijacked route leaked through HE to some clients, including Google's and CloudFlare's free DNS resolvers
- 1.1.1.1 and 8.8.8.8 started to return forged answers for myetherwallet.com

BGP Hijack, DNS Impersonation, Cryptocurrency Theft

- 205.251.199.0/24 on 24 April 2018, 11:00-13:00 (UTC)
  - BGPlay replay / Routing history

- 46.161.42.42 on 24 April 2018, 11:00-13:00 (UTC)
  - BGP replay
  - BGP/DNS Hijacks Target Payment Systems