

Troubleshooting BGP Issues with RIS and RIPEstat

Contents



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

RIPEstat Routing Widgets



The screenshot shows the RIPE NCC website interface. The top navigation bar includes links for 'Manage IPs and ASNs', 'Analyse', 'Participate', 'Get Support', and 'Publications'. The 'Analyse' tab is active. Below the navigation bar, a breadcrumb trail indicates the current location: 'You are here: Home > Analyse > Statistics > RIPEstat > 2001:67c:2e8::/48'. A search bar contains the prefix '2001:67c:2e8::/48'. On the left sidebar, a list of widgets is shown: 'At a Glance (3/4)', 'Routing (10)', 'DNS (2)', 'Anti Abuse (2)', 'Database (9)', 'Geographic (3)', 'Activity (2)', 'Transfers (3)', and 'Suggestions (1)'. An orange arrow points to the 'Routing' widget. The main content area displays the 'Routing Status (2001:67c:2e8::/48)' widget. It shows a green checkmark indicating that the prefix was 100% visible at 2020-10-23 00:00:00 UTC. It also shows the first announcement by AS3333 on 2010-09-28 16:00:00 UTC. The widget includes a section for 'Originated by' showing AS3333 and the route object RIPE. It also has a section for 'Advanced Settings' with a 'Compare' button and a checkbox for 'Exclude low visibility routes'. At the bottom, it shows the results for the prefix as of 2020-10-23 00:00:00 UTC, noting that results exclude routes with very low visibility.

- 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

The screenshot shows the BGP Looking Glass interface for the prefix 2001:67c:2e8::/48. The title bar reads "BGP Looking Glass (2001:67c:2e8::/48)". Below the title bar, there is a section for "Advanced Settings" and a summary line: "21 RRCs see 378 peers announcing 2001:67c:2e8::/48 originated by AS3333." with an "[EXPAND EVERYTHING]" link. The main content area lists 21 RRCs (Regional Route Collectors) and their associated locations, each showing the number of ASNs originating the prefix and the specific ASN (AS3333) in parentheses.

RRC	Location	ASNs	ASN
RRC06	Tokyo, Japan	1	AS3333
RRC00	Amsterdam, Netherlands	1	AS3333
RRC16	Miami, Florida, US	1	AS3333
RRC11	New York City, New York, US	1	AS3333
RRC14	Palo Alto, California, US	1	AS3333
RRC24	Montevideo, Uruguay	1	AS3333
RRC12	Frankfurt, Germany	1	AS3333
RRC03	Amsterdam, Netherlands	1	AS3333
RRC01	London, United Kingdom	1	AS3333
RRC10	Milan, Italy	1	AS3333
RRC07	Stockholm, Sweden	1	AS3333
RRC04	Geneva, Switzerland	1	AS3333

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/jaredmauch/rislive>
- <https://github.com/morrowc/rislive>



Live RIS BGP messages



Connected

741 matching messages ~625 kbit/s ⓘ

```
// Received at 11:07:56 (2.25 second delay)
{
  "timestamp": 1603444074,
  "peer": "37.49.236.71",
  "peer_asn": "34019",
  "id": "21-37-49-236-71-26462295",
  "raw":
  "FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF005202000000374001010040021A0206000084E300000CE7000
  01A6A0000F1310000F0EE0004210D4003042531EC47C0080C84E30CE784E3FFFFFFFFE84E2116B1C8E4",
  "host": "rrc21",
  "type": "UPDATE",
  "path": [34019, 3303, 6762, 61745, 61678, 270605],
  "community": [[34019, 3303], [34019, 65535], [65512, 20001]],
  "origin": "igp",
  "announcements": [
    {
      "next_hop": "37.49.236.71",
      "prefixes": [
        "177.200.228.0/22"
      ]
    }
  ]
}
```

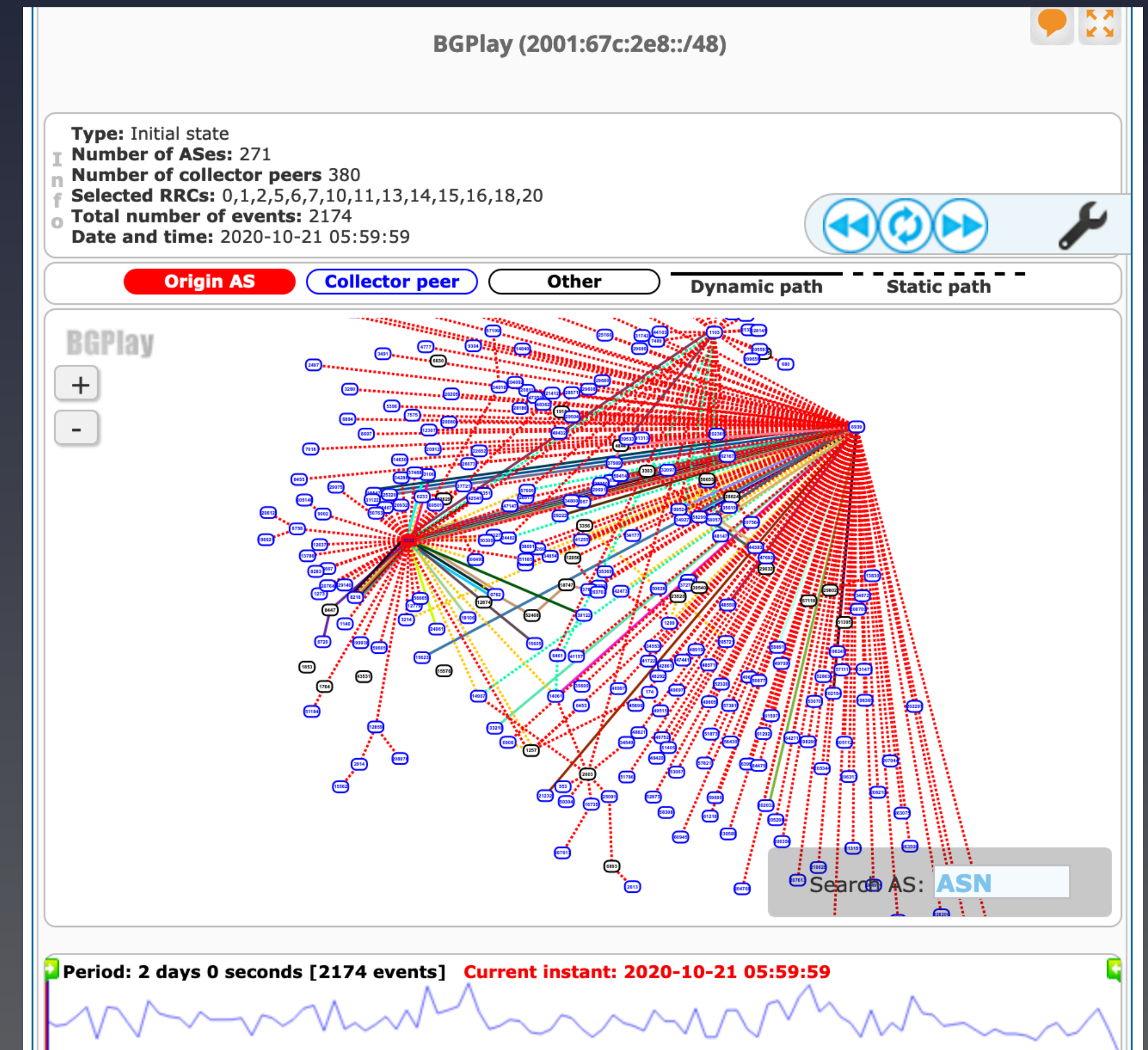
```
// Received at 11:07:56 (2.24 second delay)
{
  "timestamp": 1603444074.01,
  "peer": "37.49.236.71"
```

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](https://tools.ietf.org/html/rfc6396))
 - 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

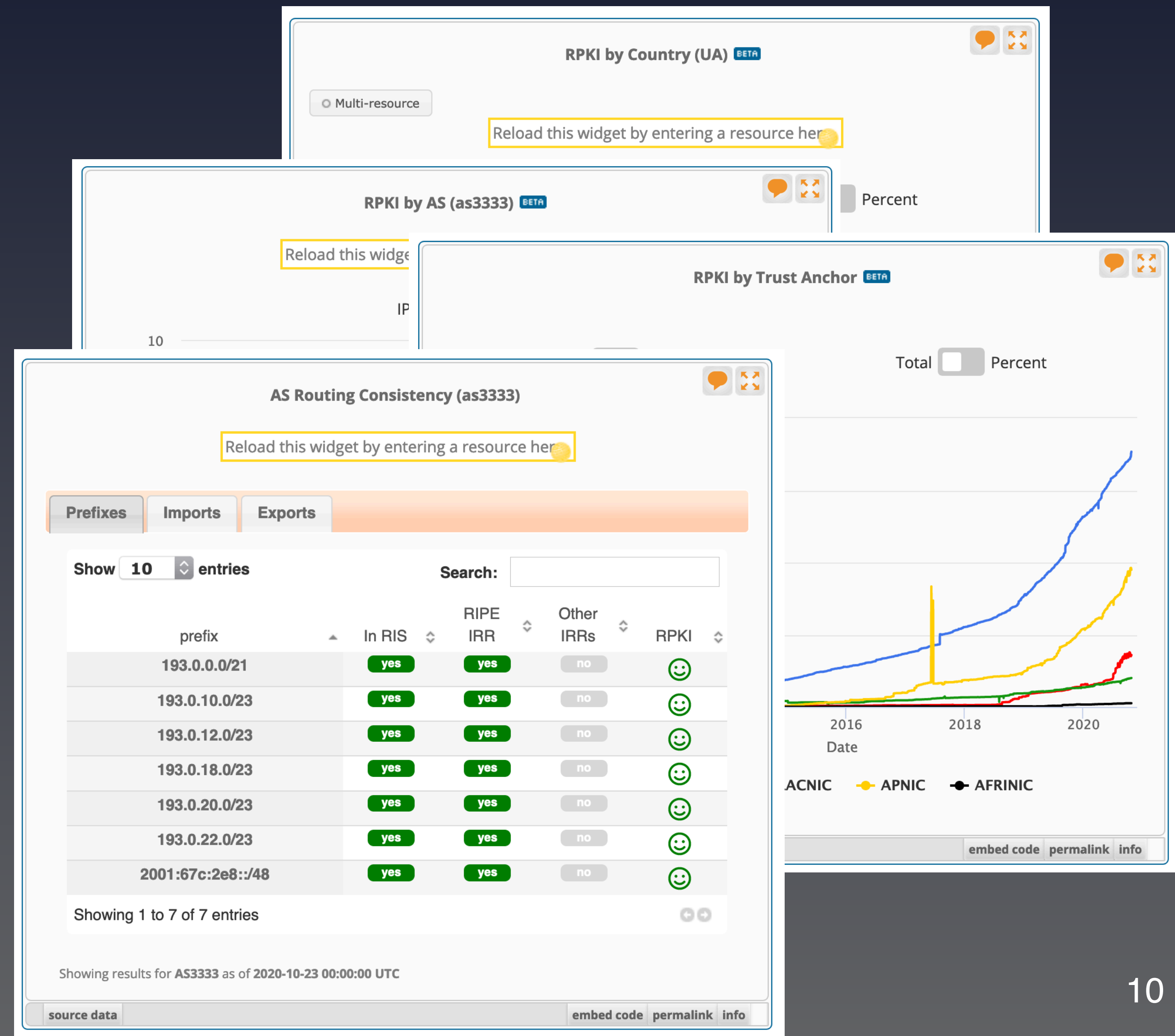
```
oleg@ommbp:~  
$ bgpdump -v updates.20201107.2000.gz | head -20  
TIME: 11/07/20 20:00:01  
TYPE: BGP4MP/MESSAGE/Keepalive  
FROM: 2001:7f8:2a::2:1:2:940 AS20940  
TO: 2001:7f8:2a::1:1:1:2654 AS12654  
  
TIME: 11/07/20 20:00:04  
TYPE: BGP4MP/MESSAGE/Update  
FROM: 193.242.98.98 AS60082  
TO: 193.242.98.118 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



Launchpad
Search and Explore

Saved
Saved searches

Use Cases
Prefix Use Cases

Widgets
Classic widgets

Documentation

Preferences
Settings and Prefs

Feedback
Tell us what you think

Legal
Copyright, Privacy, Terms, Cookies

Enter an IP address/prefix, ASN, country code or hostname

2001:67c:2e8::/48

Relative

Absolute

Latest

Prefix Status

2001:67c:2e8::/48 is announced by
AS3333

Abuse Contact

abuse@ripe.net

RPKI Validation

RPKI is VALID for 2001:67c:2e8::/48

RIS Visibility

2001:67c:2e8::/48 has HIGH visibility

Registration

Registration of 2001:67c:2e8::/48 by RIPE
NCC

RIPE Reverse DNS Delegation

DNS records found for 2001:67c:2e8::/48 in
RIPE DB

Geolocation

The location of 2001:67c:2e8::/48 is
AMBIGUOUS

Blacklist Status

2001:67c:2e8::/48 NOT found in RECENT
blacklists

Maxmind Geo Map

2001:67c:2e8::/48

Oleg Muravskiy | ENOG 17 | 9 November 2020

11



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