Bogons Observatory

Lefteris Manassakis | COO, Code BGP

lefteris@codebgp.com

RIPE 86
Rotterdam, Netherlands
22 - 26 May 2023

Bogon Prefixes - Definition

- **Martians** are private and reserved addresses defined by RFCs
- **Traditional bogons** include martians and prefixes that have not been allocated to a regional internet registry (RIR) by the Internet Assigned Numbers Authority (IANA)
- **Fullbogons** contain the traditional bogon prefixes, but also include the IP space allocated to the RIRs, but not yet assigned by them to Local Internet Registries (LIRs), **for both IPv4 and IPv6** [1]

IPv4 Martians

- **0.0.0.0/8** # RFC 791 & 1122 "This network"
- **10.0.0.0/8** # RFC 1918 Private-Use
- **100.64.0.0/10** # RFC 6598 Shared Address Space
- **127.0.0.0/8** # RFC 1122 Loopback
- **169.254.0.0/16** # RFC 3927 Link Local
- **172.16.0.0/12** # RFC 1918 Private-Use
- **192.0.2.0/24** # RFC 5737 Documentation (TEST-NET-1)
- **192.88.99.0/24** # RFC 7526 Deprecated (6to4 Relay Anycast)
- **192.168.0.0/16** # RFC 1918 Private-Use
- **198.18.0.0/16** # RFC 2544 Benchmarking
- **198.51.100.0/24** # RFC 5737 Documentation (TEST-NET-2)
- **203.0.113.0/24** # RFC 5737 Documentation (TEST-NET-3)
- **240.0.0.0/4** # RFC 1112 Reserved

Sources: https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml
https://bgpfilterguide.nlnog.net/

IPv6 Martians

- **::/8** # RFC 3513 and RFC 4291 IPv4-compatible, loopback, et al
- **0100::/64** # RFC 6666 Discard-Only
- **2001:2::/48** # RFC 5180 BMWG
- **2001:10::/28** # RFC 4843 ORCHID
- **2001:db8::/32** # RFC 3849 documentation
- **2002::/16** # RFC 7526 6to4 anycast relay
- **ffe::/16** # RFC 3701 old 6bone
- **fc00::/7** # RFC 4193 unique local unicast
- **fe80::/10** # RFC 4291 link local unicast
- **fec0::/10** # RFC 3879 old site local unicast
- **ff00::/8** # RFC 4291 multicast

Sources: https://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xhtml
https://bgpfilterguide.nlnog.net/

Bogon ASNs - Definition

- Similarly to prefixes, an ASN should be termed as Bogon **if any of the following conditions is true** [3]
  - It is reserved for special use by an RFC
  - It is not part of the block assigned to a RIR by IANA
  - It is not assigned to a LIR by any RIR

Reserved and Unallocated ASNs

- **0** # RFC 7607
- **23456** # RFC 6793 AS_TRANS
- **64496 - 64511** # RFC 5398 and documentation/example ASNs
- **64512 - 65534** # RFC 6996 Private ASNs
- **65535** # RFC 7300 Last 16 bit ASN
- **65536 - 65551** # RFC 5398 and documentation/example ASNs
- **65552 - 131071** # IANA reserved ASNs
- **151866 - 196607** # Unallocated
- **213404 - 262143** # Unallocated
- **273821 - 327679** # Unallocated
- **329728 - 393215** # Unallocated
- **401309 - 4199999999** # Unallocated
- **4200000000 - 4294967294** # RFC 6996 Private ASNs
- **4294967295** # RFC 7300 Last 32 bit ASN

Source: https://www.iana.org/assignments/as-numbers/as-numbers.xhtml

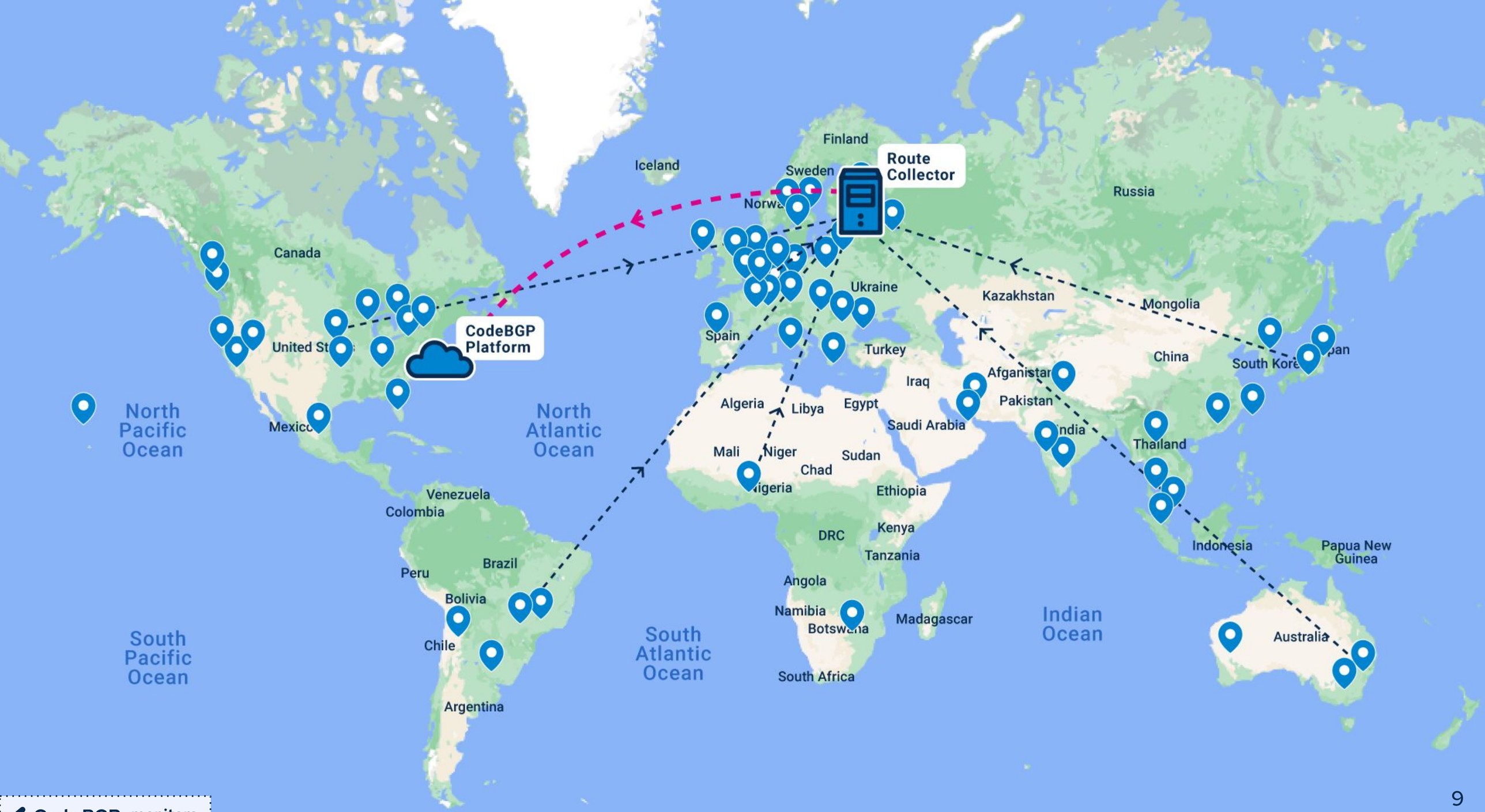
Why we care about Bogons?

- They are usually the result of configuration mistakes
- However, they are also commonly found as the source for various types of misconduct
  - source addresses of DDoS attacks
  - BGP security events, such as hijacks and route leaks
  - other types of nefarious Internet activity

Code BGP Monitor

BGP Monitoring Service developed by Code BGP

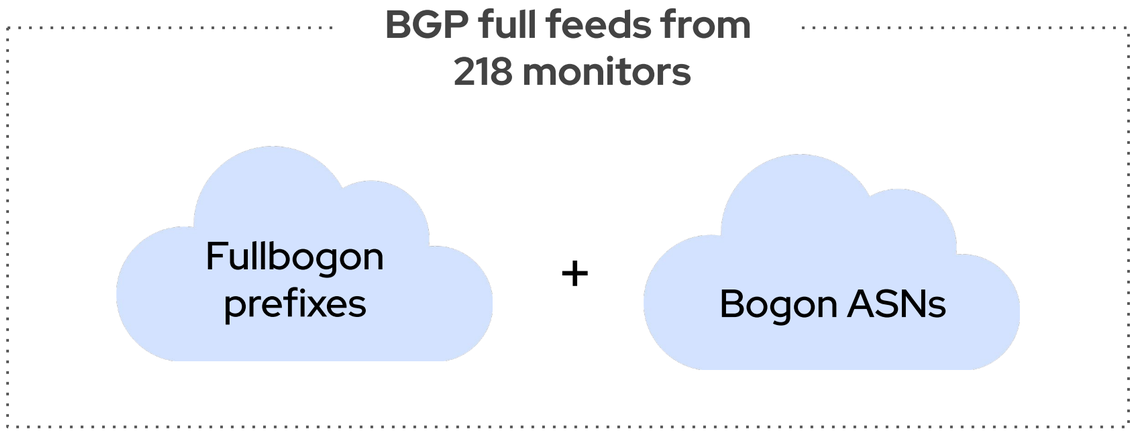
- Routing daemon: Bird 2
- Route Reflection (RFC 4456)
- BGP Add-Path (RFC 7911)
- 218 full feed peerings (v4 & v6)
- 72 cities, 44 countries, 23 upstreams



Code BGP monitors

The Code BGP Platform is configured to monitor

- Fullbogon prefixes (IPv4 and IPv6)
- Bogon ASNs present in AS Paths



Methodology

- RIPE NCC publishes daily a CSV file (~683k lines) which contains the prefixes and ASNs that have been assigned to LIRs, based on data gathered from all five RIRs (**creds to Max Stucci** for the info)
- A script checks every hour and downloads this file, identifies all the entries that are either “available” or “reserved”, and creates two lists
  - Bogon prefixes
  - Bogon ASNs
- These two lists are used to update the Bird BGP filters of the Code BGP Monitor Route Collectors
- The Bogon ASNs and prefixes are forwarded to the Code BGP Platform via BGP

CSV: https://ftp.ripe.net/pub/stats/ripencc/nro-stats/latest/nro-delegated-stats

```
ripencc|DE|asn|2777|1|19930823|assigned|5b92e74d-908f-4643-b09c-91164f9454dd|e-stats
ripencc|DE|asn|2778|1|19930823|assigned|5b92e74d-908f-4643-b09c-91164f9454dd|e-stats
ripencc|ZZ|asn|2779|1|20230411|reserved|ripencc|e-stats
ripencc|DE|asn|2780|1|19930823|assigned|5b92e74d-908f-4643-b09c-91164f9454dd|e-stats
ripencc|ZZ|asn|2781|1|20230411|reserved|ripencc|e-stats
ripencc|DE|asn|2782|1|19930823|assigned|5b92e74d-908f-4643-b09c-91164f9454dd|e-stats
ripencc|ZZ|asn|2783|1|20230411|reserved|ripencc|e-stats
ripencc|ZZ|asn|2784|1|20230411|reserved|ripencc|e-stats
ripencc|ZZ|asn|2785|1|20230411|reserved|ripencc|e-stats
ripencc|ZZ|asn|2786|1|20230411|reserved|ripencc|e-stats
ripencc|ZZ|asn|2787|1|20230411|reserved|ripencc|e-stats
ripencc|ZZ|asn|2788|1|20230411|reserved|ripencc|e-stats
ripencc|ZZ|asn|2789|1|20230411|reserved|ripencc|e-stats
ripencc|ZZ|asn|2790|1|20230411|reserved|ripencc|e-stats
ripencc|ZZ|asn|2791|1|20230411|reserved|ripencc|e-stats
ripencc|DE|asn|2792|1|19930823|assigned|5b92e74d-908f-4643-b09c-91164f9454dd|e-stats
ripencc|ZZ|asn|2793|1|20230411|available|ripencc|e-stats
ripencc|ZZ|asn|2794|1|20230411|available|ripencc|e-stats
ripencc|ZZ|asn|2795|1|20230411|available|ripencc|e-stats
```

Example of reserved and available ASNs

```
290779 arin|US|ipv4|198.17.238.0|256|19930125|assigned|1e7e8b26a7f57161a42d988f6c1ab824|e-stats
290780 arin|US|ipv4|198.17.239.0|256|19930125|assigned|29c22955e3ec738701505c5cac58369e|e-stats
290781 apnic|ZZ|ipv4|198.17.240.0|512|20230411|available|apnic|e-stats
290782 arin|US|ipv4|198.17.242.0|256|19930125|assigned|bb474b75b6f23182ffa56daf1cf9ec23|e-stats
290783 arin|US|ipv4|198.17.243.0|256|19960104|assigned|9f14454567a6c23e60bfd4fec24d1438|e-stats
290784 arin|US|ipv4|198.17.244.0|256|19960104|assigned|9f14454567a6c23e60bfd4fec24d1438|e-stats
290785 arin|US|ipv4|198.17.245.0|256|19930125|assigned|d6380a7662f572e9240353794c0b1f5e|e-stats
290786 arin|US|ipv4|198.17.246.0|256|19930125|assigned|8639bcc29508777c05bd241673461908|e-stats
290787 arin|US|ipv4|198.17.247.0|256|19930125|assigned|f1a97bc35f0ea9127934dc1c93c6ccc5|e-stats
290788 arin|US|ipv4|198.17.248.0|256|20130429|assigned|532539e84cbb18c691a50390db186131|e-stats
290789 arin|US|ipv4|198.17.249.0|256|19930125|assigned|9f14454567a6c23e60bfd4fec24d1438|e-stats
290790 arin|US|ipv4|198.17.250.0|256|19930125|assigned|cdc65c90124b367ce35ae08fc39316b4|e-stats
290791 arin|US|ipv4|198.17.251.0|256|20130422|assigned|96c6fb5ec0231b378d577be3538aa01f|e-stats
290792 arin|US|ipv4|198.17.252.0|256|19930125|assigned|a6ee0552fa98e1f95d685204654a5a8c|e-stats
290793 arin|US|ipv4|198.17.253.0|256|19930125|assigned|1f99771bc3e23e6097509a331544ab65|e-stats
290794 arin|US|ipv4|198.17.254.0|256|19930125|assigned|1f99771bc3e23e6097509a331544ab65|e-stats
290795 arin|US|ipv4|198.17.255.0|256|20130422|assigned|d542f963d47c7774cd04044e7a9978d8|e-stats
290796 iana|ZZ|ipv4|198.18.0.0|131072|19990301|reserved|ietf|iana
290797 arin|US|ipv4|198.20.0.0|2048|20120914|assigned|d2fc8fbc818f19b5b4e50576735f87e4|e-stats
290798 arin|CA|ipv4|198.20.8.0|2048|19921125|assigned|983f7167e66bbee5762aad527e385e27|e-stats
```

Example of reserved and available prefixes

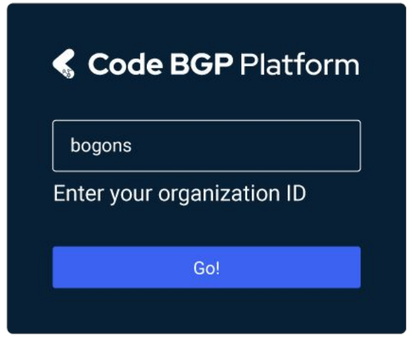
Do it yourself

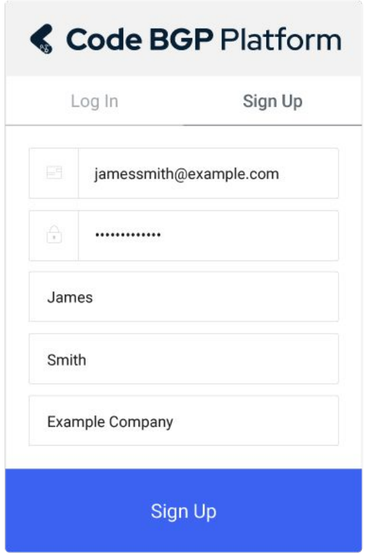
- Open source repo which contains:
  - Shell script implementing the methodology
  - Bird template configuration
  - Python script which extracts Bogons from RIPE RIS or RouteViews MRT dumps
  - README with detailed steps

URL: https://github.com/codebgp/bogons

Or get access to our Platform

- Go to https://cloud.codebgp.com/
  and in the Organisation ID type “bogons”
- Sign up
- Docs: https://docs.codebgp.com/





1 Go to cloud.codebgp.com
Enter ID: **bogons**

2 Sign up

By using the bogons instance we can:

- Make sure we don’t announce or propagate bogon prefixes
- Make sure we don’t use or propagate bogon ASNs
- Figure out who does it and let them know so they fix their announcements and/or filters

Code BGP Platform

Lefteris Manassakis
editor | bogons
LE

- Overview
- Setup
- Looking Glass
- API
- Integrations

Looking Glass Info

Prefixes | Autonomous Systems | Peerings | **Routes** | RPKI ROAs

	Prefix	Origin AS	Neighbor AS	AS						
>	190.123.9.0/24	278014	270814	34						
>	190.123.8.0/24	278014	270814	34						
>	190.123.8.0/23	278014	270814	34						
>	2a07:e340::/32	65042	9009	57						
>	190.123.9.0/24	278014	270814	88						
>	190.123.8.0/24	278014	270814	88						
>	190.123.8.0/23	278014	270814	88						
>	2001:c10:ff02::/48	64588	397942	56						
>	2a0c:3800:300::/48	204378	4200140000	20						
>	95.180.251.0/24	65535	25467	34927	6762	5603	25467	65535	NotFound	Apr 12, 2023, 14:03:39

FILTERS RESET

Prefix

Origin AS

Neighbor AS

AS Path

Communities

RPKI Status
All

First Detected
min max

Last Update
min max

Apply Filters

Find ASNs

Code BGP Platform

Lefteris Manassakis
editor | bogons

- Overview
- Setup
- Looking Glass
- API
- Integrations

Looking Glass Info

Prefixes | Autonomous Systems | Peerings | **Routes** | RPKI ROAs

AS 65651

Name	Not found.
Country	Not found.
Abuse contact	Not found.
More Info	RIPEstat IRR Explorer Not found. Cloudflare Radar

Prefix	Origin AS	Neighbor AS	AS Path		Update
217.16.6.0/24	65651	65601	57695 48024 137409 6		4, 2023, 15:12:00
217.16.12.0/24	65651	65601	57695 48024 137409		2023, 15:12:00
217.16.13.0/24	65651	65601	57695 48024 137409 6		4, 2023, 15:12:00
217.16.8.0/24	65651	65601	57695 137409 6461 8218		24, 2023, 15:11:51
217.16.9.0/24	65651	65601	57695 137409 6461 8218 204		Apr 24, 2023, 15:11:51
217.16.15.0/24	65651	65601	57695 56630 20485 6762 6461 8218 204818 65601 65651		Apr 24, 2023, 15:11:46
217.16.7.0/24	65651	65601	57695 137409 6461 8218 204818 65601 65651		Apr 24, 2023, 15:11:54
217.16.2.0/24	65651	65601	57695 137409 6461 8218 204818 65601 65651	Invalid	Apr 24, 2023, 15:11:50
217.16.13.0/24	65651	65601	57695 137409 6461 8218 204818 65601 65651	Invalid	Apr 24, 2023, 15:11:50
217.16.6.0/24	65651	65601	57695 137409 6461 8218 204818 65601 65651	Invalid	Apr 24, 2023, 15:11:50
5.228.146.0/24	262773	263523	20473 17819 1221 4637 6461 52320 53087 263523 (2) 262773		Apr 24, 2023, 15:11:33
17.16.4.0/24	65651	65601	57695 56630 20485 6762 6461 8218 204818 65601 65651		Apr 24, 2023, 15:11:46

Why bogon?

RIPEstat

Launchpad
Search and Explore

Saved
Saved Searches

Use Cases
ASN Use Cases

Atlas Check

Historical WHOIS

Geo Check

Registration Check

Reverse DNS Consistency

Routing Check

Routing Consistency

RPKI Check

Enter an IP address/prefix, ASN, country code or FQDN
65651

Relative | Absolute | Latest

Abuse Contact

Unknown to RIPE NCC

Allocation History

Records were found in **IANA**

Announced Prefixes

AS65651 has **0** prefixes

AS Name

AS65651

--MISSING--

AS Neighbours

Unique ASNs: **0**

IPv4: **0** left **0** right **0** uncertain

IPv6: **0** left **0** right **0** uncertain

AS Path Length

AS65651 has a median average path length of **0**

IANA

AS65552-AS131071 is reserved

AS Prefix Count

AS65651 has **0** IPv4 Prefixes and **0** IPv6 Prefixes

BGP Update Activity

No data available.

RIPE Atlas Probes

Found 0 records for **AS65651**

Maxmind Geo Map

MaxMind can find NO LOCATION for **65651**

RIPE Atlas Probe Deployment

Query only available for larger timeframes

RIR Stats Country

The location of **AS65651** is UNKNOWN

RIPE Atlas Targets

Found 0 records for **AS65651**

RIR Registration

Why bogon?

Code BGP Platform

Lefteris Manassakis
editor | bogons
LE

- Overview
- Setup
- Looking Glass
- API
- Integrations

Looking Glass Info

Prefixes | Autonomous Systems | Peerings | Routes | RPKI ROAs

FILTERS RESET

Network

Origin AS

IP Version
All

Mask Length

Data Sources (#)
min max

Data Sources (%)
min max

Apply Filters

Network	Origin AS		
2805:f10:f12::/48	262182		
2803:6606:4000::/48	28075		
2620:a0:e0::/48	11278		
2805:f10:f13::/48	262182		
2800:5e00:ffff::/48	28007		
2c0f:f590::/32	36974		
2801:1f:d800::/48	254455		
2801:c4:38::/48	18734	93	100%
2803:6606:4000::/34	28075	93	100%
115.42.0/23	132839	93	100%

Find Prefixes

Next steps

- Conduct a measurement study for the bogon phaenomenon that could result in a publication
  - Try to correlate bogon data with DDoS attacks, BGP hijacks and other security related events

- Seek funding to develop a methodology and automation that will periodically inform people about their misconfigured BGP filters

- Goal: Internet with less bogons

References

[1] Team Cymru "The Bogon Reference" https://www.team-cymru.com/bogon-networks

[2] NLNOG "BGP Filter Guide" https://bgpfilterguide.nlnog.net/

[3] Aftab Siddiqui "Routing Security Terms: Bogons, Vogons, and Martians"

https://www.manrs.org/2021/01/routing-security-terms-bogons-vogons-and-martians/

[4] IANA "IPv4 Special-Purpose Address Registry"
https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml

[5] IANA "Internet Protocol Version 6 Address Space"
https://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xhtml

[6] IANA "Autonomous System (AS) Numbers"
https://www.iana.org/assignments/as-numbers/as-numbers.xhtml

Questions

lefteris@codebgp.com

codebgp.com