

Bogons Observatory

Lefteris Manassakis
COO, Code BGP

✉ lfteris@codebgp.com



About me



Lfteris Manassakis

COO & co-founder
Code BGP



lfteris@codebgp.com



<https://manassakis.net/>

Martians & Traditional Bogons

- 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 - Definition

- **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** [[TEAMCYMRU](#)]

IPv4 Martians

- **0.0.0.0/8** # RFC 791 & RFC 1122
- **10.0.0.0/8** # RFC 1918 Private-Use
- **100.64.0.0/10** # RFC 6598 Shared Ad. 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 (TEST-NET-1)

IPv4 Martians

- **192.88.99.0/24** # RFC 7526
- **192.168.0.0/16** # RFC 1918 Private-Use
- **198.18.0.0/15** # RFC 2544 Benchmarking
- **198.51.100.0/24** # RFC 5737 (TEST-NET-2)
- **203.0.113.0/24** # RFC 5737 (TEST-NET-3)
- **240.0.0.0/4** # RFC 1112 Reserved

References: [[NLNOG](#), [IANA_v4](#)]

IPv6 Martians

- **::/8** # RFC 3513 and RFC 4291
- **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

IPv6 Martians

- **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

References: [[NLNOG](#), [IANA_v6](#)]

Bogon ASNs - Definition

- Similarly to prefixes, an ASN should be termed as Bogon **if any of the following conditions is true** [[MANRS](#)]
 - 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 & Unallocated ASNs

- **0** # RFC 7607
- **23456** # RFC 6793 AS_TRANS
- **64496 - 65551** # RFCs 6996, 7300 & 5398
- **65552 - 131071** # IANA reserved ASNs
- **213404 - 262143** # Unallocated
- **273821 - 327679** # Unallocated

Reserved & Unallocated ASNs

- **329728 - 393215** #Unallocated
- **151866 - 196607** #Unallocated
- **401309 - 4199999999** #Unallocated
- **4200000000 - 4294967294** # RFC 6996
- **4294967295** # RFC 7300 Last 32 bit ASN

Reference: [[IANA_ASNs](#)]

Why we care about Bogons?

- They are usually the result of configuration mistakes
- However, they are also found as the source for various types of misconduct

Misconduct related to Bogons

- Source addresses of DDoS attacks
- BGP security events, such as hijacks and route leaks
- Other types of nefarious Internet activity

Bogon projects

- [CIDR report](#)
- [Team Cymru](#)
- [Hurricane Electric](#)

Our bogons project

- provides real time data
 - from multiple worldwide distributed locations
 - via multiple BGP feeds
 - for all possible bogons
 - fullbogon prefixes
 - bogon ASes anywhere in the AS Path

Code BGP Monitor

BGP Monitoring Service developed by Code BGP

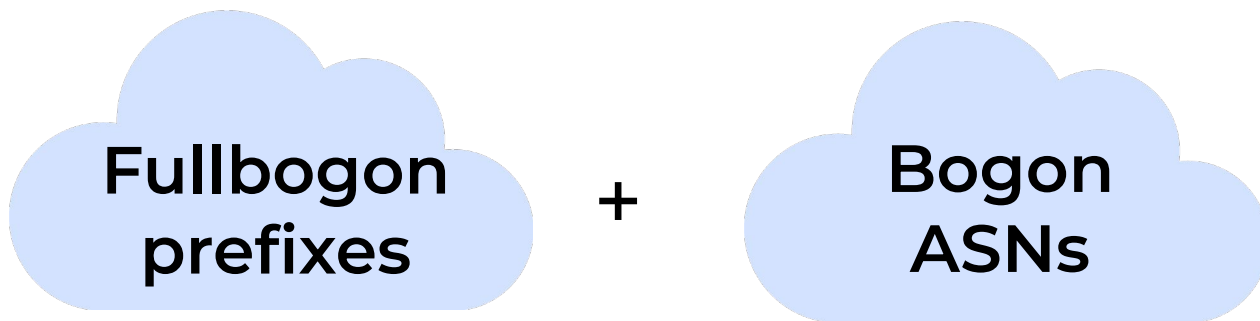
- Routing daemon: Bird 2
- Route Reflection ([RFC 4456](#))
- BGP Add-Path ([RFC 7911](#))
- 220 full feed peers (IPv4 & IPv6)
- 72 cities, 44 countries, 23 upstreams



Configured to monitor

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

BGP full feeds from 220 monitors



Data

- 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)

Methodology - Step 1

- 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

Methodology - Step 2

- These two lists are used to update the Bird BGP filters of the Code BGP Monitor Route Collectors

Methodology - Step 3

- The Bogon ASNs and prefixes are forwarded to the Code BGP Platform via BGP

Data

- CSV:

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

- RIPE NCC documentation:

<https://github.com/RIPE-NCC/nro-delegated-stats/blob/main/Reports.md>

2234	ripenc	DE	asn	2777	1	19930823	assigned	5b92e74d-908f-4643-b09c-91164f9454dd	e-stats
2235	ripenc	DE	asn	2778	1	19930823	assigned	5b92e74d-908f-4643-b09c-91164f9454dd	e-stats
2236	ripenc	ZZ	asn	2779	1	20230411	reserved	ripenc	e-stats
2237	ripenc	DE	asn	2780	1	19930823	assigned	5b92e74d-908f-4643-b09c-91164f9454dd	e-stats
2238	ripenc	ZZ	asn	2781	1	20230411	reserved	ripenc	e-stats
2239	ripenc	DE	asn	2782	1	19930823	assigned	5b92e74d-908f-4643-b09c-91164f9454dd	e-stats
2240	ripenc	ZZ	asn	2783	1	20230411	reserved	ripenc	e-stats
2241	ripenc	ZZ	asn	2784	1	20230411	reserved	ripenc	e-stats
2242	ripenc	ZZ	asn	2785	1	20230411	reserved	ripenc	e-stats
2243	ripenc	ZZ	asn	2786	1	20230411	reserved	ripenc	e-stats
2244	ripenc	ZZ	asn	2787	1	20230411	reserved	ripenc	e-stats
2245	ripenc	ZZ	asn	2788	1	20230411	reserved	ripenc	e-stats
2246	ripenc	ZZ	asn	2789	1	20230411	reserved	ripenc	e-stats
2247	ripenc	ZZ	asn	2790	1	20230411	reserved	ripenc	e-stats
2248	ripenc	ZZ	asn	2791	1	20230411	reserved	ripenc	e-stats
2249	ripenc	DE	asn	2792	1	19930823	assigned	5b92e74d-908f-4643-b09c-91164f9454dd	e-stats
2250	ripenc	ZZ	asn	2793	1	20230411	available	ripenc	e-stats
2251	ripenc	ZZ	asn	2794	1	20230411	available	ripenc	e-stats
2252	ripenc	ZZ	asn	2795	1	20230411	available	ripenc	e-stats

Example of reserved & 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	983f7167e66bbe5762aad527e385e27	e-stats

Example of reserved & available prefixes

```

56 # Bogons (tenant31) filters
57
58 define BOGON_ASNS = [0, 23456, 64496..131071, 151866..196607,
213404..262143, 273821..327679, 329728..393215,
401309..4199999999, 4200000000..4294967295];
59
60 function accept_any_bogon_asns()
61 int set bogon_asns;
62 {
63     bogon_asns = BOGON_ASNS;
64
65     if ( bgp_path ~ [= * bogon_asns * =] ) then {
66         accept;
67     }
68 }
69
70 define BOGON_PREFIXES_V4 = [0.0.0.0/8{8,32}, 10.0.0.0/8{8,32},
100.64.0.0/10{10,32}, 127.0.0.0/8{8,32}, 169.254.0.0/16{16,32},
172.16.0.0/12{12,32}, 192.0.2.0/24{24,32}, 192.168.0.0/16{16,32},
192.88.99.0/24{24,32}, 198.18.0.0/15{15,32},198.51.100.0/24{24,32},
203.0.113.0/24{24,32}, 224.0.0.0/4{4,32}, 240.0.0.0/4{4,32}];
71
72 function accept_bogon_prefixes_v4()
73 prefix set bogon_prefixes_v4;
74 {
75     bogon_prefixes_v4 = BOGON_PREFIXES_V4;
76
77     if (net ~ bogon_prefixes_v4) then {
78         accept;
79     }
80 }
81

```

```

82 define BOGON_PREFIXES_V6 = [::/8{8,128}, 0100::/64{64,128},
2001:2::/48{64,128}, 2001:10::/28{28,128}, 2001:db8::/32{32,128},
2002::/16{16,128}, ffe::/16{16,128}, fc00::/7{7,128},
fe80::/10{10,128}, fec0::/10{10,128}, ff00::/8{8,128}];
83
84 function accept_bogon_prefixes_v6()
85 prefix set bogon_prefixes_v6;
86 {
87     bogon_prefixes_v6 = BOGON_PREFIXES_V6;
88
89     if (net ~ bogon_prefixes_v6) then {
90         accept;
91     }
92 }
93
94 filter bogon_any_v4 {
95     accept_any_bogon_asns();
96     accept_bogon_prefixes_v4();
97 }
98
99 filter bogon_any_v6 {
100     accept_any_bogon_asns();
101     accept_bogon_prefixes_v6();
102 }

```

Example of a Bird filter in a Route Collector

Data comparison between projects - April 18

Project	# of active bogons (v4)	# of active bogons (v6)
CIDR report	690	-
Hurricane Electric	1220	101
Code BGP	2954	3137

Data comparison between projects - April 18

Project	# of bogon prefixes (v4)	# of bogon prefixes (v6)
Team Cymru	981	137556
Code BGP	7927	275250

RPKI Invalids vs Valid - April 18

RCs Setup	# of RPKI Invalid Routes	# of RPKI Valid Routes
Bogon ASNs & Prefixes	6072	9727

- RPKI valid routes are bogons due to the presence of bogon ASNs in the AS path


Do it yourself

- Open source repo which contains:
 - Shell script implementing the methodology
 - Bird template configuration
 - Python script for MRT dumps
 - README with detailed steps

<https://github.com/codebgp/bogons>


Moreover, you can use our service

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



Code BGP Platform

Enter your organization ID



Code BGP Platform

Log In Sign Up

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



Overview

Setup

Looking Glass

API

Welcome, Letteris | Overview

BGP update rates Current (#/min) **632** Daily Avg. (#/min) **890**

Autonomous Systems (#)
0
[View](#)

IPv4 Prefixes (#)
6026
[View](#)

IPv6 Prefixes (#)
4093
[View](#)

Peerings (#)
0
[View](#)

Routes (#)
142436
[View](#)

RPKI ROAs (#)
0
[View](#)

Alert Rules (#)
0
[View](#)

NetOps Queries (#)
5
[View](#)

Data Services

RIS Live: **0**

RPKI: **0**

My Routers: **0**

Code BGP Monitor: **220**

Overview



Overview



Setup



Looking Glass



API



Docs

Looking Glass [Info](#)

Prefixes

Autonomous Systems

Peerings

Routes

RPKI ROAs



	Prefix	Origin AS	Neighbor AS	AS Path	RPKI Status	Last Update
>	41.159.48.0/24	37169	16058	35661 25369 174 6713 16058 37169	NotFound	Jun 1, 2023, 09:33:55
>	41.72.240.0/24	37169	16058	57695 137409 174 6713 16058 37169	NotFound	Jun 1, 2023, 09:33:51
>	41.159.48.0/24	37169	16058	198644 34779 174 6713 16058 37169	NotFound	Jun 1, 2023, 09:33:51
>	41.159.47.0/24	37169	16058	42473 8529 6453 174 6713 16058 37169	NotFound	Jun 1, 2023, 09:33:50
∨	103.52.228.0/22	134105	131322	44684 2914 133385 (2) 1333385 133385 131322 134105 (2)	Valid	Jun 1, 2023, 09:33:47

Data Sources of Route 103.52.228.0/22 - 44684 2914 133385 (2) 1333385 133385 131322 134105 (2)



Data Service	Peer IP	ASN	City	Country	Continent	Last Update
Code BGP Monitor	46.235.224.6	44684	Cambridge	United Kingdom	Europe	Jun 1, 2023, 09:33:47

Rows per page: 10

1-1 of 1



Routes

Rows per page: 10

21-30 of 142456

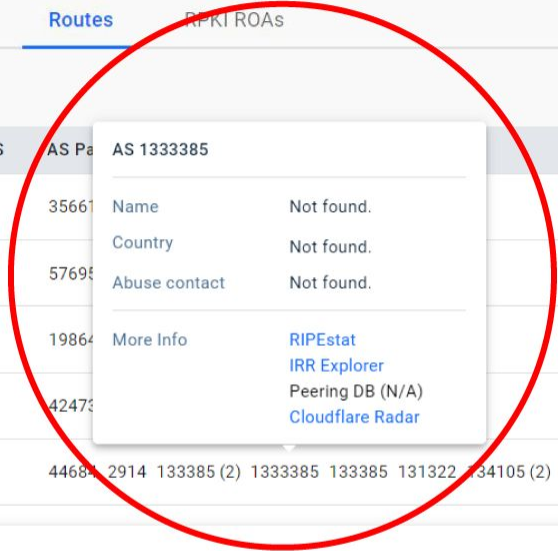


- Overview
- Setup
- Looking Glass
- API
- Docs

Looking Glass Info

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

Prefix	Origin AS	Neighbor AS	AS Path	AS 1333385	RPKI Status	Last Update
> 41.159.48.0/24	37169	16058	35661	Name Not found.	NotFound	Jun 1, 2023, 09:33:55
> 41.72.240.0/24	37169	16058	57695	Country Not found.	NotFound	Jun 1, 2023, 09:33:51
> 41.159.48.0/24	37169	16058	19864	Abuse contact Not found.	NotFound	Jun 1, 2023, 09:33:51
> 41.159.47.0/24	37169	16058	42473	More Info RIPEstat IRR Explorer Peering DB (N/A) Cloudflare Radar	NotFound	Jun 1, 2023, 09:33:50
103.52.228.0/22	134105	131322	44684 2914 1333385 (2) 1333385 133385 131322 134105 (2)		Valid	Jun 1, 2023, 09:33:47



Data Sources of Route 103.52.228.0/22 - 44684 2914 1333385 (2) 1333385 133385 131322 134105 (2)

Data Service	Peer IP	ASN	City	Country	Continent	Last Update
Code BGP Monitor	46.235.224.6	44684	Cambridge	United Kingdom	Europe	Jun 1, 2023, 09:33:47

Rows per page: 10 1-1 of 1

Rows per page: 10 21-30 of 142456

Why bogon?

Search bar: Enter an IP address/prefix, ASN, country code or FQDN. Input: 1333385

Filters: Relative, Absolute, Latest, Refresh icon, Share, Heart, List icons

Abuse Contact ⓘ
Unknown to RIPE NCC

Allocation History ⓘ ↑↓
Records were found in IANA

Announced Prefixes ⓘ
AS1333385 has 0 prefixes

AS Name ⓘ
AS1333385
NO NAME FOUND

AS Neighbours ⓘ
Unique ASNs: 0
IPv4: 0 left 0 right 0 uncertain
IPv6: 0 left 0 right 0 uncertain

AS Path Length ⓘ
AS1333385 has a median average path length of 0

AS Prefix Count ⓘ
AS1333385 has 0 IPv4 Prefixes and 0 IPv6 Prefixes

BGP Update Activity ⓘ
No data available.

IANA ⓘ ↑↓
AS401309-AS4199999999 is unallocated

Maxmind Geo Map ⓘ
MaxMind can find NO LOCATION for 1333385

RIPE Atlas Probe Deployment ⓘ
Query only available for larger timeframes

RIPE Atlas Probes ⓘ
Found 0 records for AS1333385

RIR Registration ⓘ

RIR Stats Country ⓘ
The location of AS1333385 is UNKNOWN

Why bogon?

- Overview
- Setup
- Looking Glass
- API

Prefix ↑	Origin AS	Data Sources (#)	Data Sources (%)
0.0.0.0/0	4200039027, 4200129030, 4200140105, 4288000489, 56655, 61102, 64915	7	6.4%

Data Sources of Prefix 0.0.0.0/0



Data Service	Peer IP	ASN	City	Country	Continent
Code BGP Monitor	185.37.148.232	61102	Tel Aviv	Israel 🇮🇱	Asia
Code BGP Monitor	139.180.161.246	20473	Sydney	Australia 🇦🇺	Oceania
Code BGP Monitor	155.138.194.31	20473	Atlanta	United States 🇺🇸	North America
Code BGP Monitor	45.134.89.1	34927	Sandefjord	Norway 🇳🇴	Europe
Code BGP Monitor	67.219.106.198	20473	Melbourne	Australia 🇦🇺	Oceania
Code BGP Monitor	192.248.158.39	20473	London	United Kingdom 🇬🇧	Europe
Code BGP Monitor	45.76.235.85	20473	Dallas	United States 🇺🇸	North America

Rows per page: 10 1-7 of 7

1.7.203.0/24	65000	1	0.9%
0/24	3507	107	98%

Rows per page: 10 1-10 of 10130

Prefixes

- Overview
- Setup
- Looking Glass
- API

Looking Glass Info

- Prefixes
- Autonomous Systems
- Peerings
- Routes
- RPKI ROAs

Prefix ↑	Origin AS
> 0.0.0.0/0	4200039027, 4200129030, 4200129031, 4288000489, 56655, 61102, 6497
> 1.7.203.0/24	65000
> 2.57.241.0/24	3507
> 2.58.141.0/24	209171
> 2.58.232.0/22	207461
> 2.58.232.0/24	207461
> 2.58.233.0/24	207461
> 2.58.234.0/24	207461

FILTERS RESET

Prefix

IP Version
 All

Data Sources (#)
 min min

Apply Filters

Find Prefixes

2	1.82%
3	2.8%
1	0.9%

Next steps - research

- Collab with **John Kristoff** and conduct a measurement study for the bogon phenomenon that could result in a publication
 - Try to correlate bogon data with DDoS attacks, BGP hijacks and other security related events

Next steps - goal

- Seek funding to develop a methodology and automation that will periodically inform people about their misconfigured BGP filters
- Goal: Internet with less bogons

Questions

✉ leftieris@codebgp.com

