BGP Zombies

Ghost routes as seen by BGP monitoring platforms

Lefteris Manassakis
COO, Code BGP

lefteris@codebgp.com

About me

Lefteris Manassakis

COO & co-founder
Code BGP

lefteris@codebgp.com

https://manassakis.net/

BGP Zombies

- They are **active RIB entries for withdrawn prefixes**
- Also known as **stuck routes** or **ghost routes**
- Term used in previous studies

Reasons BGP Zombies exist

For the same reasons a BGP update message can get lost. A non extensive list includes:

- flapping interfaces
- router reboots and CPU spikes
- prefix withdrawals generate nearly 4 times more traffic [5]
- name here what can go wrong...

Why we care about Zombies wrt BGP Monitoring?

- **During a prefix announcement**, even if some BGP monitoring peers do not receive the update messages, they are received by the vast majority of them
- **The impact** of some peers not receiving updates can be considered minor

Why we care about Zombies wrt BGP Monitoring?

- However**, during prefix withdrawals,** if some monitoring peers do not receive the BGP withdrawal messages, they will incorrectly report the prefix as active
- They **report an erroneous network state**

BGP Zombies Impact

- Routing **Loops** & Routing **Detours** [1]
- Inaccurate **BGP Monitoring** information

Previous studies

- Previous studies [1, 2] have shown:
  - the pervasiveness of BGP zombies
  - that long AS paths, ASes announcing a large number of prefixes and noisy prefixes, like BGP beacons, are more prone to zombies

Extend previous work

- However, these studies were based on data only from RIPE RIS
- We aim to extend previous work by answering these additional questions:

Questions

- If we look for BGP zombies using a BGP monitoring platform other than RIPE RIS, and compare the data with RIS Live, will we have comparable results?
- If we announce a limited number of new prefixes, originated from a new AS not announcing other prefixes, will we still have BGP zombies?

RIPE RIS

- RIPE (Réseaux IP Européens) is the **Regional Internet Registry** for Europe, the Middle East and parts of Central Asia
- RIS (Routing Information Service) **is a routing data collection platform**

RIPE RIS

Provides **real-time routing information**, such as:

- What is currently being announced
- Which prefixes are seen by which peers
- Which ones are not seen

RIS Live

Provides **real-time BGP messages** via a fully filterable interactive WebSocket JSON API, and a full stream (“firehose”) containing all of the messages generated by RIS.
https://ris-live.ripe.net/

23 active RIS Collectors

Name	Location	Scope
RRC00	Amsterdam, NL	global
RRC01	London, GB	LINX, LONAP
RRC03	Amsterdam, NL	AMS-IX, NL-IX

RRC list:
https://ris.ripe.net/docs/10_routecollectors.html

1448 RIS Peers

BGP full feeds:

- IPv4: **366**
- IPv6: **401**

Peer list:
https://www.ris.ripe.net/peerlist/all.shtml

Tools using RIS

- Code BGP Platform
- ARTEMIS
- RIPEstat
- BGPalerter
- Internet Health Report
- IODA
- bgp.he.net

Code BGP Monitor

BGP Monitoring Service developed by Code BGP, and used by the Code BGP Platform

- BGP Route Reflection (RFC 4456)
- BGP Add-Path (RFC 7911)

180 Code BGP Monitor Peers

AS 50414

- All peers provide BGP full feeds
- 60 cities
- 36 countries
- 20 upstreams

Code BGP Monitor locations

Routing beacons

- **A Routing Beacon** is a BGP speaker that announces and withdraws a particular prefix at predetermined time intervals. RIS Route Collectors originate a small number of routing beacons.

Beacon prefixes

- These prefixes are announced and withdrawn according to a set schedule
- For this study **we selected** five v4 and five v6 beacon prefixes, originated by **geographically distributed** RIS RRCs

Selected Prefixes

IPv4	IPv6	Location
84.205.64.0/24	2001:7FB:FE00::/48	RRC00 - AMS, NL
84.205.70.0/24	2001:7FB:FE06::/48	RRC06 - Tokyo, JP

Selected Prefixes

IPv4	IPv6	Location
84.205.75.0/24	2001:7FB:FE0B::/48	RRC11 - NY, US
84.205.79.0/24	2001:7FB:FE0F::/48	RRC15 - SP, BR
84.205.82.0/24	2001:7FB:FE13::/48	RRC19 - JB, ZA

Methodology

- Measurement period: Jan 2-31, 2023
- **Configure these prefixes** to be monitored by the Code BGP Platform, which utilizes both RIS Live and Code BGP Monitor as data sources
- 1:45 hours after the withdrawals check how many peers **still see these prefixes**
- **Compare** the two monitoring sources wrt zombies

Overview
Setup
AS Filters
Prefix Filters
Alert Rules
Data Services
State
API

State Info

Prefixes | Autonomous Systems | Peerings | Routes | RPKI ROAs

Origin AS: 12654

Network	Origin AS	Data Sources (#)	Data Sources (%)
84.205.64.0/24	12654	485	89%
84.205.70.0/24	12654	467	85%
84.205.75.0/24	12654	461	84%
84.205.79.0/24	12654	479	87%
84.205.82.0/24	12654	479	87%
2001:7fb:fe00::/48	12654	487	93%
2001:7fb:fe06::/48	12654	468	89%
2001:7fb:fe0b::/48	12654	487	93%
2001:7fb:fe0f::/48	12654	477	91%
2001:7fb:fe13::/48	12654	475	91%

Rows per page: 10 1-10 of 10

Prefixes

Overview
Setup
AS Filters
Prefix Filters
Alert Rules
Data Services
State
API

State

Info

Prefixes | Autonomous Systems | Peerings | Routes | RPKI ROAs

Origin AS: 12654

Prefix	Origin AS	Neighbor AS	AS Path	RPKI Status	First Detected	Last Update
2001:7fb:fe06::/48	12654	2497	49673 48858 20485 2497 12654	Valid	Jan 6, 2023, 11:03:59	Jan 6, 2023, 11:03:55
2001:7fb:fe13::/48	12654	37271	49673 48858 37271 12654	Valid	Jan 6, 2023, 11:03:59	Jan 6, 2023, 11:03:55
2001:7fb:fe0f::/48	12654	35280	49673 48858 35280 12654	Valid	Jan 6, 2023, 11:03:59	Jan 6, 2023, 11:03:55
2001:7fb:fe06::/48	12654	2497	34927 3356 2497 12654	Valid	Jan 6, 2023, 11:03:03	Jan 6, 2023, 11:03:03
2001:7fb:fe00::/48	12654	58057	6762 174 58057 12654	Valid	Jan 6, 2023, 10:59:54	Jan 6, 2023, 10:59:51
2001:7fb:fe13::/48	12654	37271	6762 174 37271 12654	Valid	Jan 6, 2023, 10:59:28	Jan 6, 2023, 10:59:25
2001:7fb:fe0b::/48	12654	9002	48147 29632 9002 12654	Valid	Jan 6, 2023, 10:44:18	Jan 6, 2023, 10:44:13
2001:7fb:fe0b::/48	12654	9002	142289 29632 9002 12654	Valid	Jan 6, 2023, 10:43:57	Jan 6, 2023, 10:43:54
84.205.79.0/24	12654	35280	28910 31133 35280 12654	Valid	Jan 6, 2023, 10:42:00	Jan 6, 2023, 10:41:56
001:7fb:fe0b::/48	12654	13030	34019 13030 12654	Valid	Jan 6, 2023, 10:38:55	Jan 6, 2023, 10:38:53

Rows per page: 10 1-10 of 4064

Routes

Beacon prefixes results

# of RIS peers	# of Code BGP peers	RIS Zombie %	Code BGP Zombie %
389	89	1.64%	1.25%

New prefixes

- We repeat the experiments, but this time with **3 not previously announced v6 prefixes**
- Announce and withdraw these prefixes **from 5 routers located in 5 continents**
- New origin AS 50907, each location with a different upstream
- Will we still have BGP zombies?

New Prefixes

IPv6	ASN	Owned by
2a12:bc0:3::/48	50907	Code BGP
2a12:bc0:4::/48	50907	Code BGP
2a12:bc0:5::/48	50907	Code BGP

Locations and Upstreams

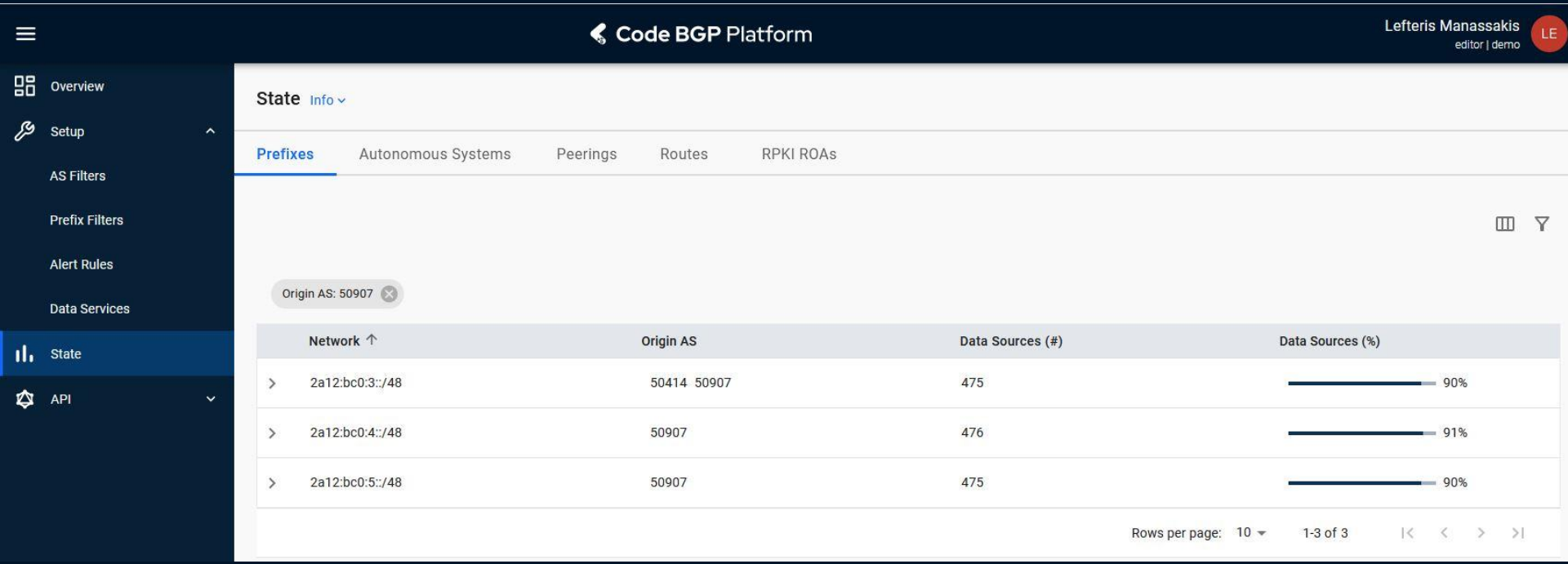
City	Continent	Upstream AS
Paris, FR	Europe	35661
Singapore, SG	Asia	8849
San Jose, US	North America	57695

Locations and Upstreams

City	Continent	Upstream AS
Lagos, NG	Africa	35487
Sydney, AU	Oceania	20473

Methodology

- Measurement period: Jan 2-16, 2023
- **Configure these prefixes** to be monitored by the Code BGP Platform
- Announce them from one location at a time
- After an hour withdraw these prefixes
- 1:45 hours later check how many peers of each monitoring source **still see these prefixes**


Code BGP Platform
Lefteris Manassakis
editor | demo
LE
Overview
Setup
AS Filters
Prefix Filters
Alert Rules
Data Services
State
API
State
Info
Prefixes
Autonomous Systems
Peerings
Routes
RPKI ROAs
Origin AS: 50907
Network
Origin AS
Data Sources (#)
Data Sources (%)
2a12:bc0:3::/48
50414 50907
475
90%
2a12:bc0:4::/48
50907
476
91%
2a12:bc0:5::/48
50907
475
90%
Rows per page: 10
1-3 of 3

Prefixes

Overview
Setup
AS Filters
Prefix Filters
Alert Rules
Data Services
State
API

State

Info

Prefixes | Autonomous Systems | Peerings | Routes | RPKI ROAs

Origin AS: 50907

Prefix	Origin AS	Neighbor AS	AS Path	RPKI Status	First Detected	Last Update
2a12:bc0:3::/48	50907	35661	49673 48858 35661 50907	Valid	Jan 6, 2023, 11:03:59	Jan 6, 2023, 11:03:55
2a12:bc0:4::/48	50907	35661	49673 48858 35661 50907	Valid	Jan 6, 2023, 11:03:58	Jan 6, 2023, 11:03:55
2a12:bc0:5::/48	50907	35661	49673 48858 35661 50907	Valid	Jan 6, 2023, 11:03:58	Jan 6, 2023, 11:03:55
2a12:bc0:4::/48	50907	35661	42473 6762 5511 35661 50907	Valid	Jan 6, 2023, 10:51:56	Jan 6, 2023, 10:51:56
2a12:bc0:5::/48	50907	35661	42473 6762 5511 35661 50907	Valid	Jan 6, 2023, 10:51:55	Jan 6, 2023, 10:51:56
2a12:bc0:3::/48	50907	35661	51088 3257 174 35661 50907	Valid	Jan 6, 2023, 10:26:22	Jan 6, 2023, 10:26:19
2a12:bc0:4::/48	50907	35661	51088 3257 174 35661 50907	Valid	Jan 6, 2023, 10:26:22	Jan 6, 2023, 10:26:19
2a12:bc0:5::/48	50907	35661	51088 3257 174 35661 50907	Valid	Jan 6, 2023, 10:26:22	Jan 6, 2023, 10:26:19
2a12:bc0:5::/48	50907	35661	20912 6939 35661 50907	Valid	Jan 6, 2023, 10:25:18	Jan 6, 2023, 10:25:14
a12:bc0:3::/48	50907	35661	20912 6939 35661 50907	Valid	Jan 6, 2023, 10:25:18	Jan 6, 2023, 10:25:14

Routes

New prefixes results

# of RIS peers	# of Code BGP peers	RIS Zombie %	Code BGP Zombie %
384	88	0.61%	0.49%

Takeaways

- We need to learn to live with **BGP Zombies**
- We **should be aware** of their prevalence and potential impact
- Monitoring infrastructures and platforms should develop ways to:
  - mark routes as zombies
  - inform users of their presence **so their impact is limited**

References

[1] Ongkanchana, P., et al. "Hunting BGP zombies in the wild." ANRW 2021

[2] Fontugne, R., et al. "BGP zombies: An analysis of beacons stuck routes." PAM, 2019

[3] Emile Aben. “Zombie Routes.” RIPE77, 2018

[4] Fontugne, R. et al. “BGP Zombies.” RIPE Labs, 2019

[5] Asturiano, V. “The Shape of a BGP Update.”, RIPE Labs, 2011

Questions