RIPE NCC
RIPE NETWORK COORDINATION CENTRE

Zombie Routes

BGP Routes Getting Stuck

emile.aben@ripe.net / romain@iij.ad.jp | 2018-10 | RIPE77

Zombie Routes?

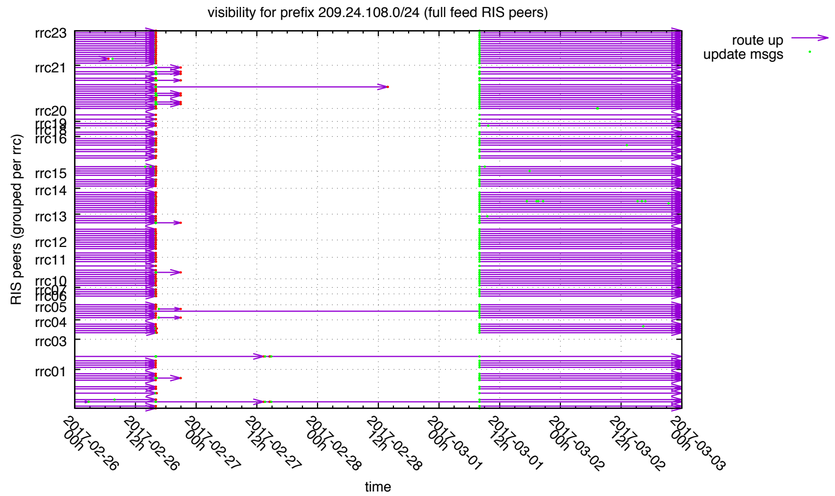
- aka. “stuck route”
- Origin withdrew prefix but route still visible
  - Even after path hunting
- The good: this doesn’t happen too often
  - or does it?
- The bad: it does happen
- The ugly: hard to debug

Even BGP-Nyancat was affected!

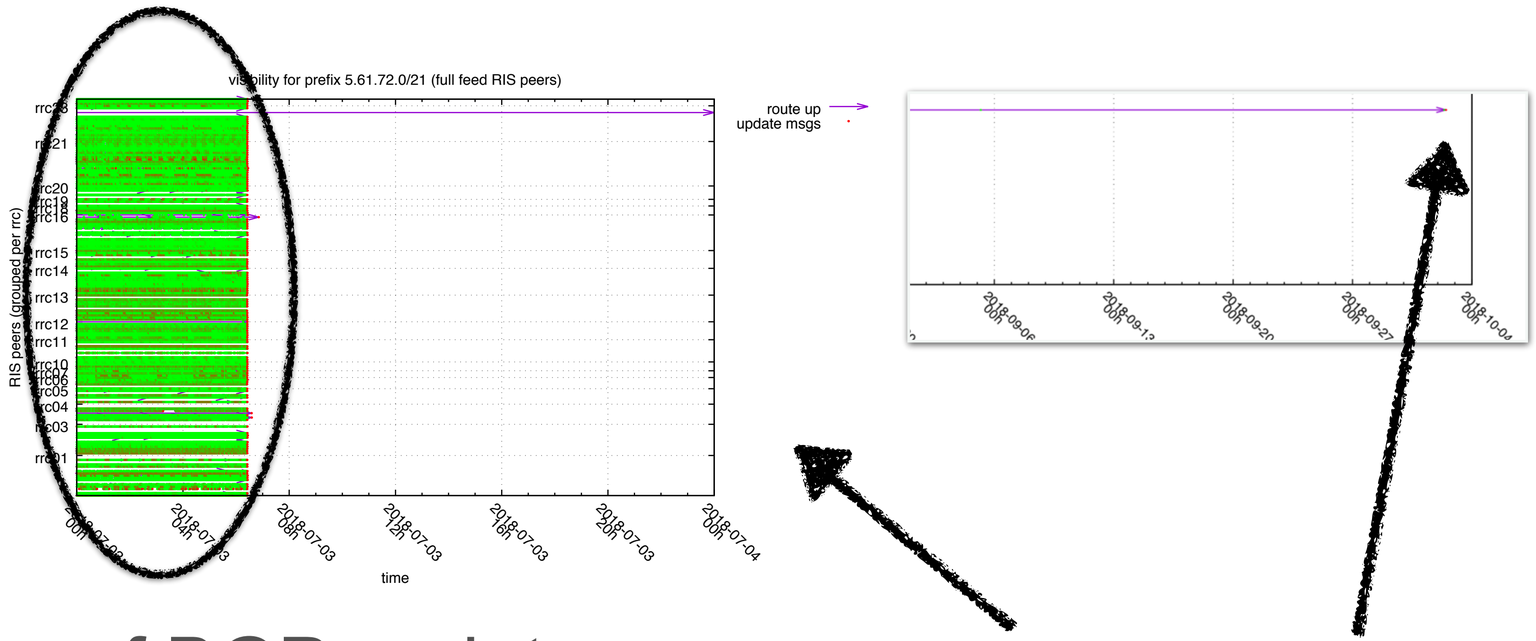
- https://labs.ripe.net/Members/cteusche/bgp-meets-cat

Even BGP-Nyancat was affected!

- https://labs.ripe.net/Members/cteusche/bgp-meets-cat



Example: Long Lived Zombie



Tons of BGP updates

3 Months!

Route totally withdrawn only after manual intervention

Confusing if you want to know: Is this routed publicly?

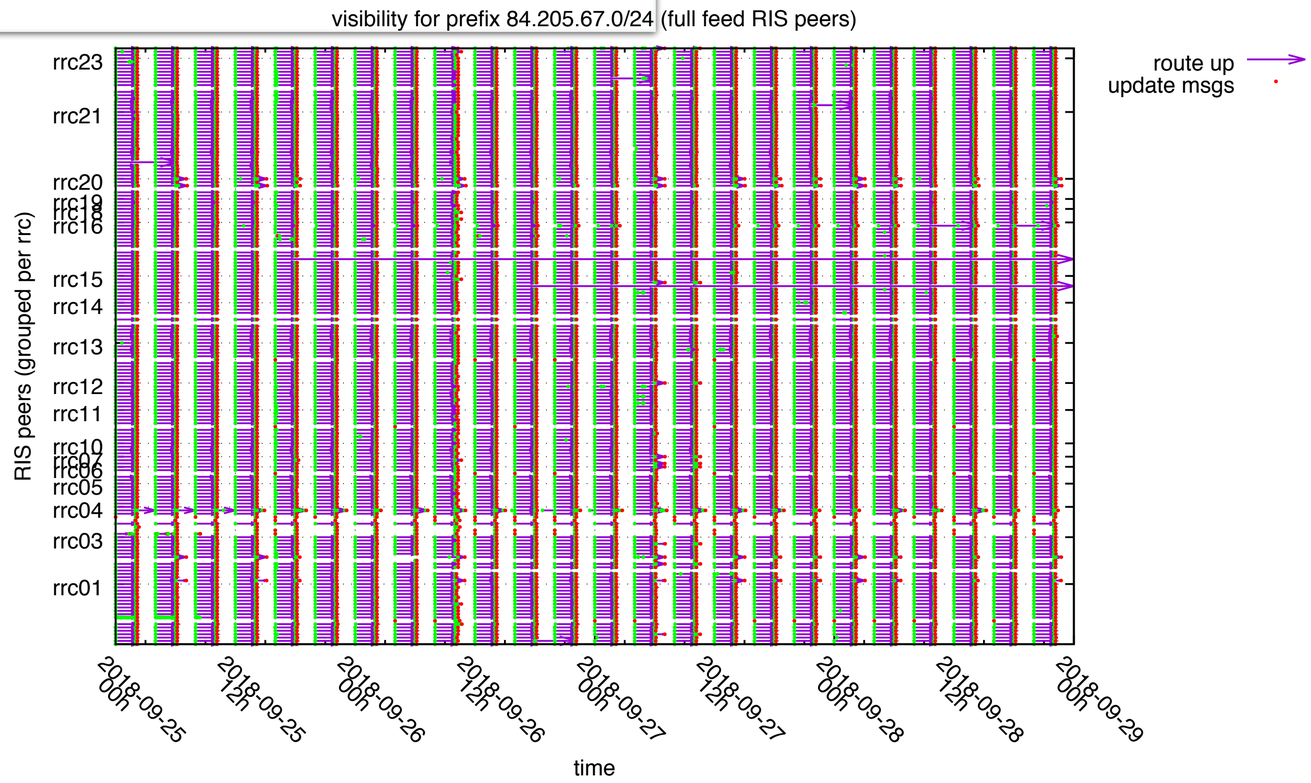
First Step: BGP Beacons

Current RIS Routing Beacons

Note: IPv6 beacons and anchors are now being announced from the RRCs. See below for details.

All RRCs:

- Announcements at 00:00, 04:00, 08:00, 12:00, 16:00, 20:00 (UTC)
- Withdrawals at 02:00, 06:00, 10:00, 14:00, 18:00, 22:00 (UTC)



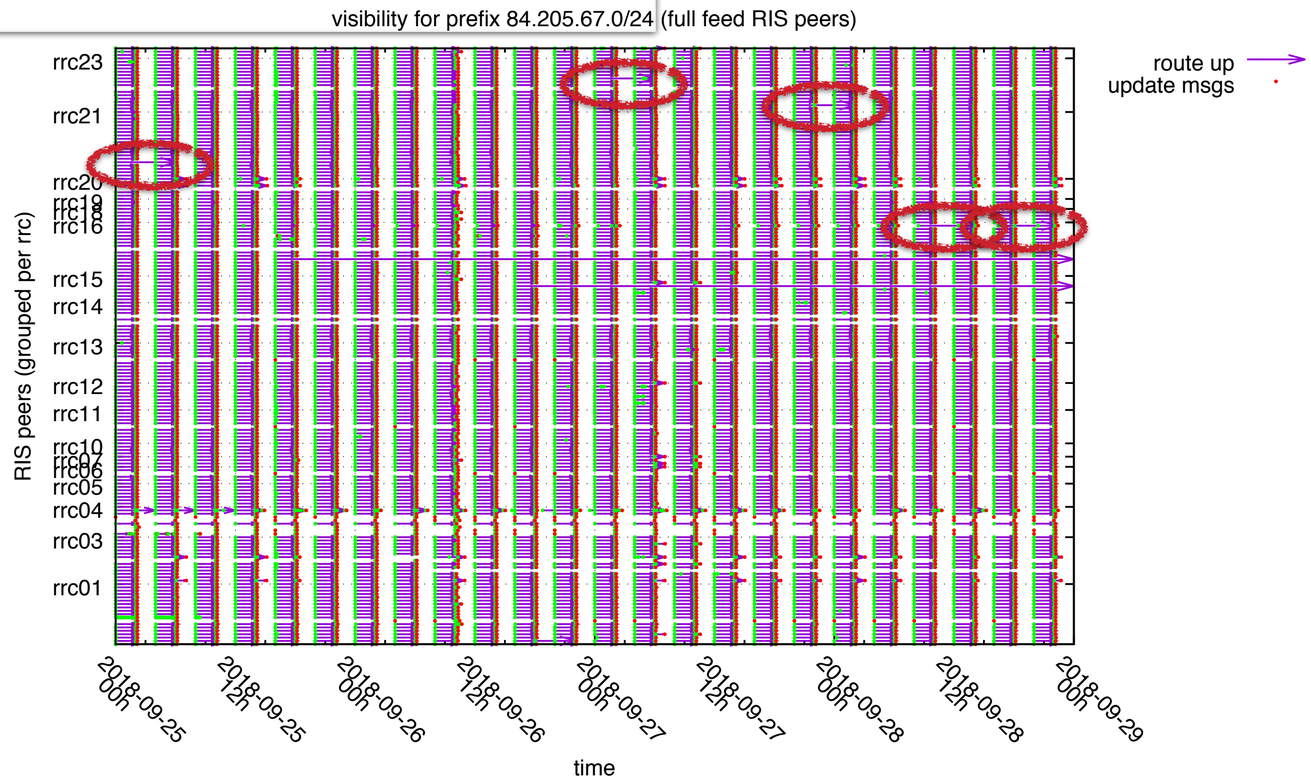
First Step: BGP Beacons

Current RIS Routing Beacons

Note: IPv6 beacons and anchors are now being announced from the RRCs. See below for details.

All RRCs:

- Announcements at 00:00, 04:00, 08:00, 12:00, 16:00, 20:00 (UTC)
- Withdrawals at 02:00, 06:00, 10:00, 14:00, 18:00, 22:00 (UTC)



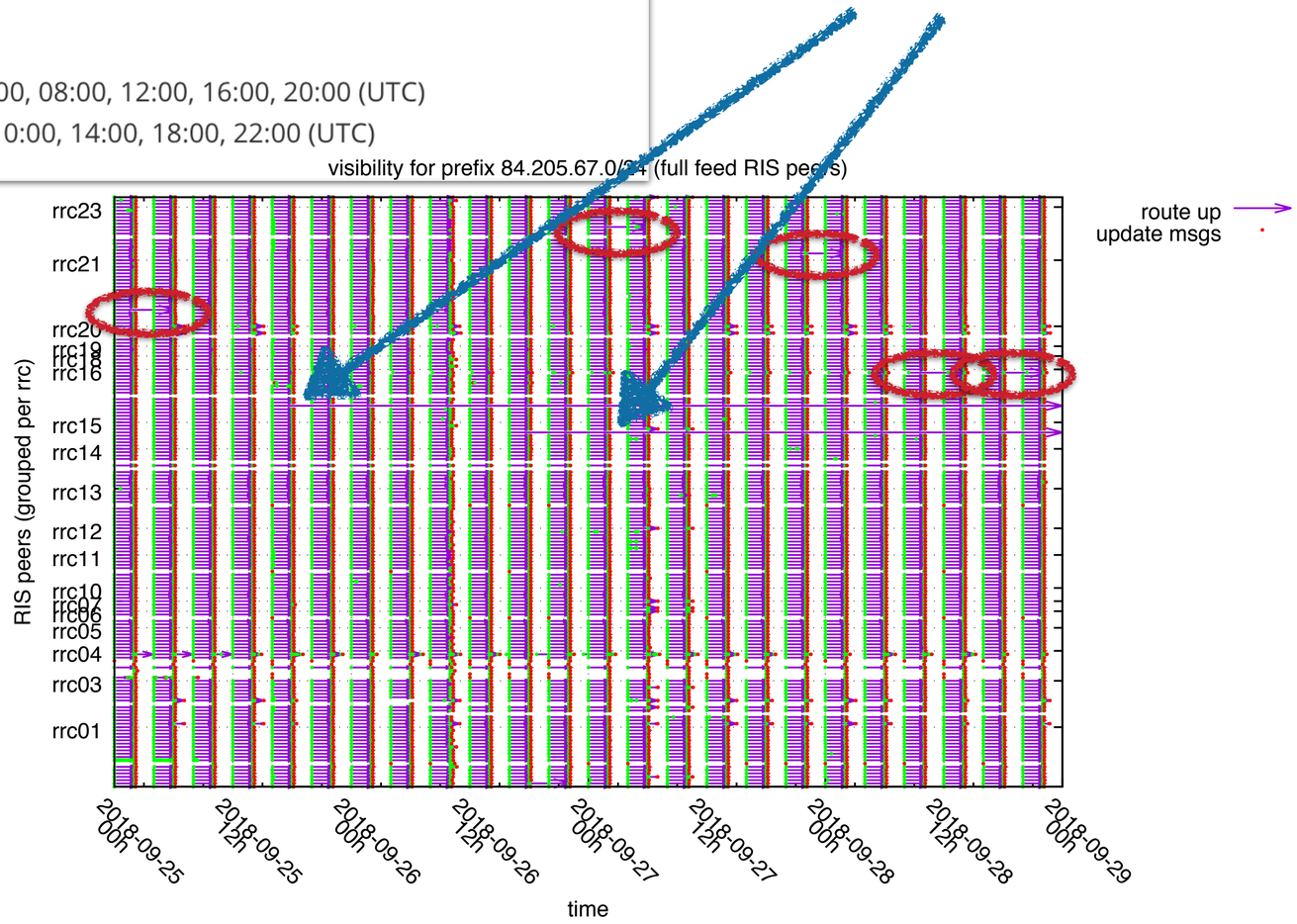
First Step: BGP Beacons

Current RIS Routing Beacons

Note: IPv6 beacons and anchors are now being announced from the RRCs. See below for details.

All RRCs:

- Announcements at 00:00, 04:00, 08:00, 12:00, 16:00, 20:00 (UTC)
- Withdrawals at 02:00, 06:00, 10:00, 14:00, 18:00, 22:00 (UTC)



Beacon Zombies

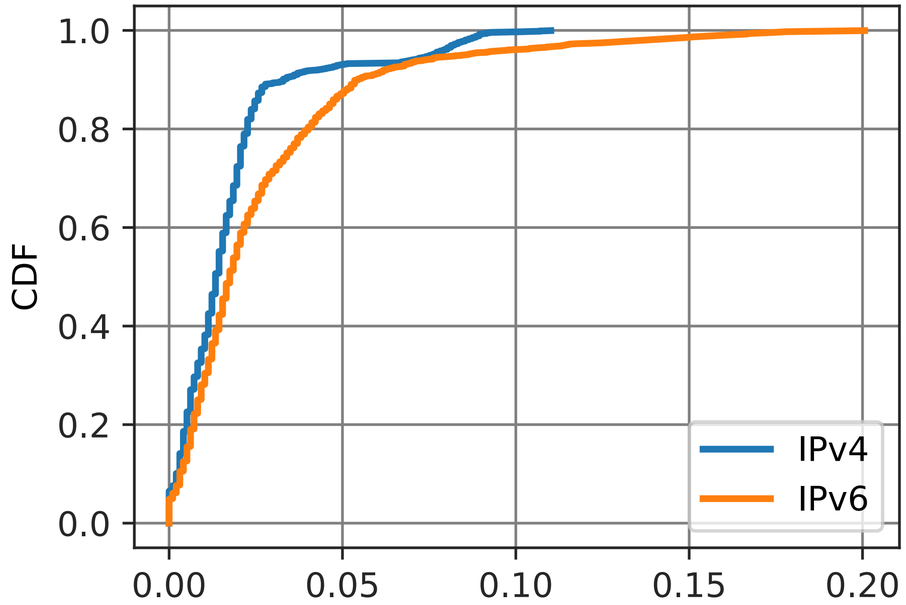
Likelihood for a RIS peer to see a beacon zombie route?

?

Beacon Zombies

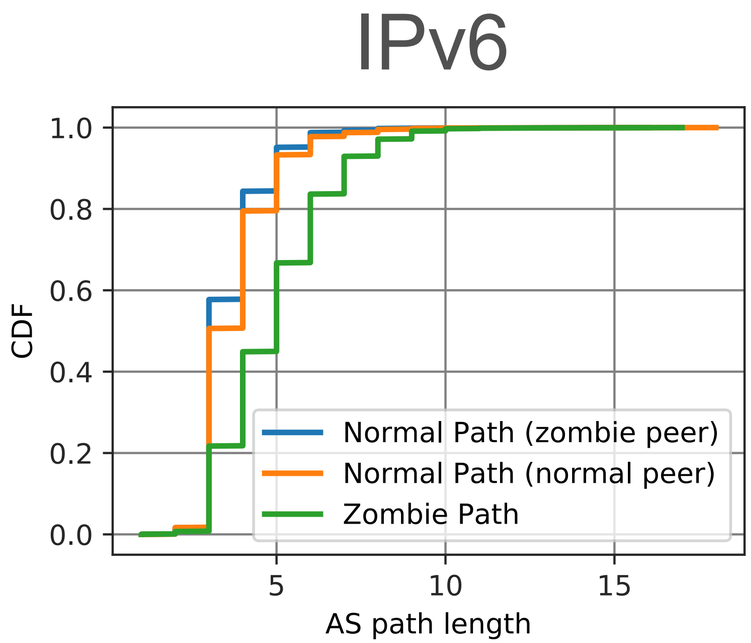
Likelihood for a RIS peer to see a beacon zombie route?

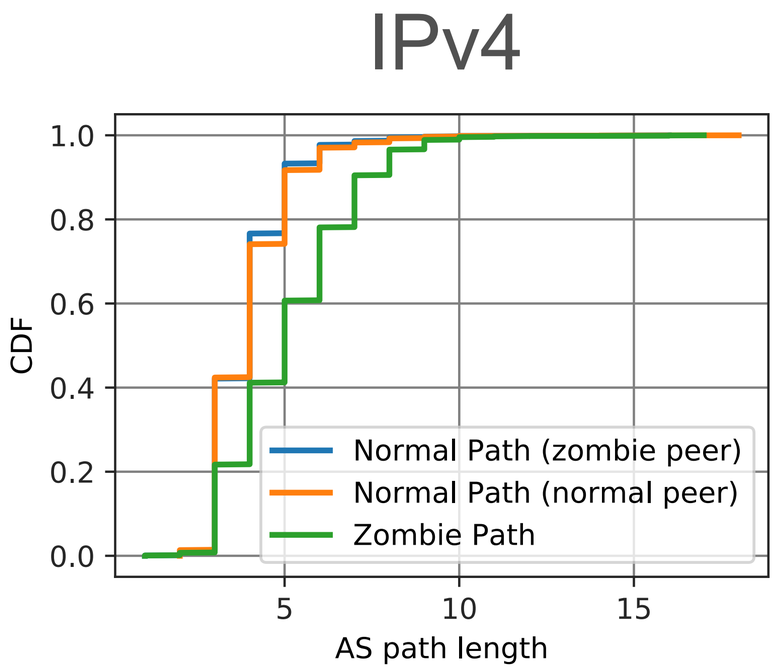
- IPv6: 2.8%
- IPv4: 1.8%



ratio zombie peers/all withdraws

Zombie paths are longer





- Zombie paths (green) are longer than best path
- Mitigate by reannounce/withdraw?

Zombie Apocalypse?

- Is this a canary in the coal-mine?
- Sign of things getting worse?
  - didn’t increase over time (until now) at least
- What if:
  - More prefixes?
  - More updates?

What causes this?

- Software bugs
  - Routers
  - BGP optimisers?
  - Route reflector setups?
  - Route collector systems?
- Is this correlated to update rates?
  - another sign update rates are a problem?

Next Steps

- Zombie-aware BGPlay?
  - Needs us to be able to find zombies in the wild
- Alerting?
  - Do you want to know about these in your network?
  - Does it increase your table size?
- Create awareness
  - Researchers typically not aware this exist
- Operator Feedback!
  - Do you know how much trouble (tickets) this causes?

Questions

emile.aben@ripe.net
romain@iij.ad.jp
not a typo
twitter: @meileaben
mastodon: @meileaben@vis.social
not a typo