RIPE NCC
RIPE NETWORK COORDINATION CENTRE

Zombie Routes

How leaky is BGP?

Name | Date | Event

Zombie Routes?

- aka. “stuck route”
- Origin withdrew the route but it’s 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

Example: DECIX peering LAN

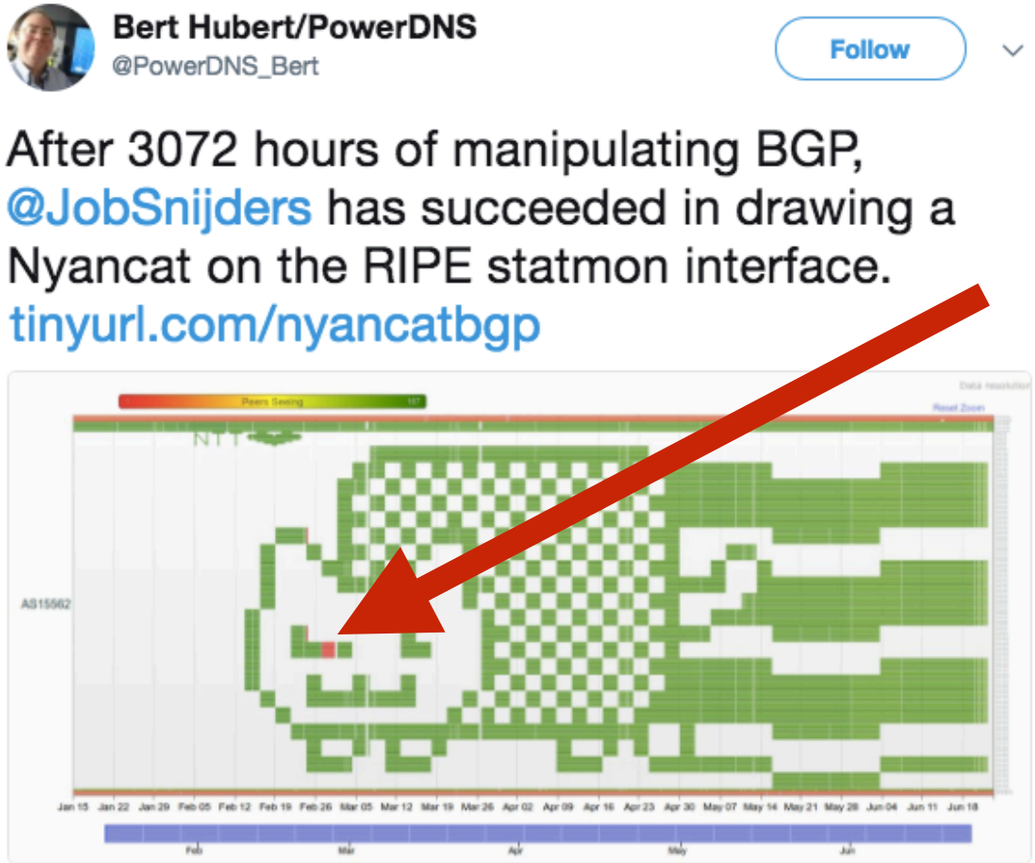
- Took XX tickets over XX days and XX parties to get resolved! (and this is the case of very competent people!)
- @@pic of BGPlay

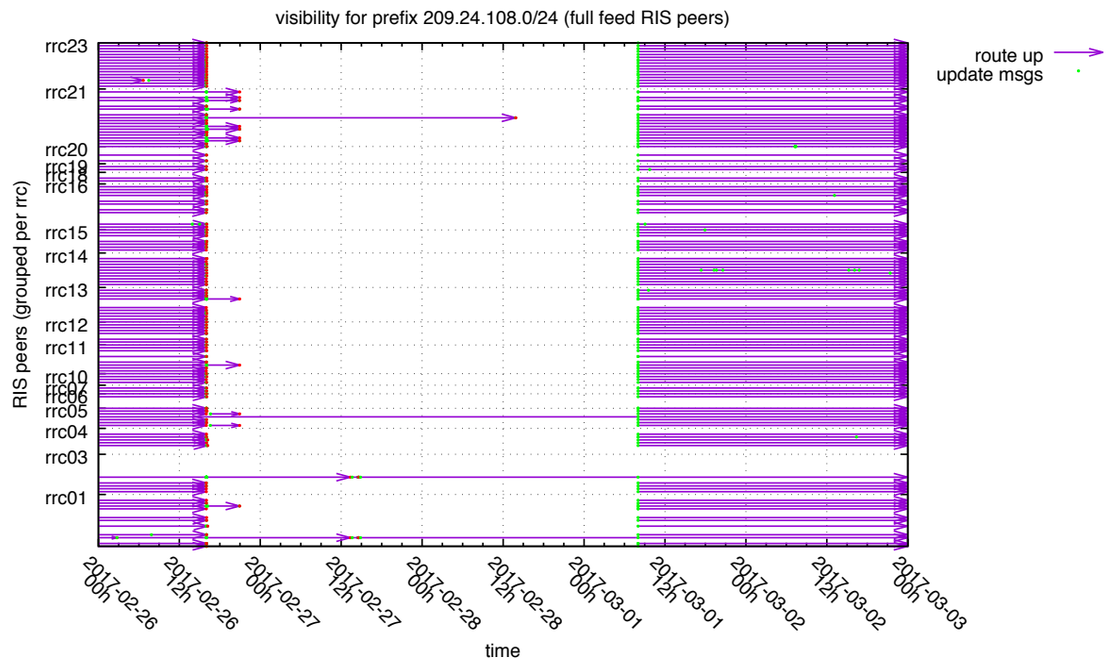
Is address space still “in use”?

- People use RIPEstat / BGPlay for this

Even BGP-Nyancat was affected!

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





Example: Bitcanal still routed?

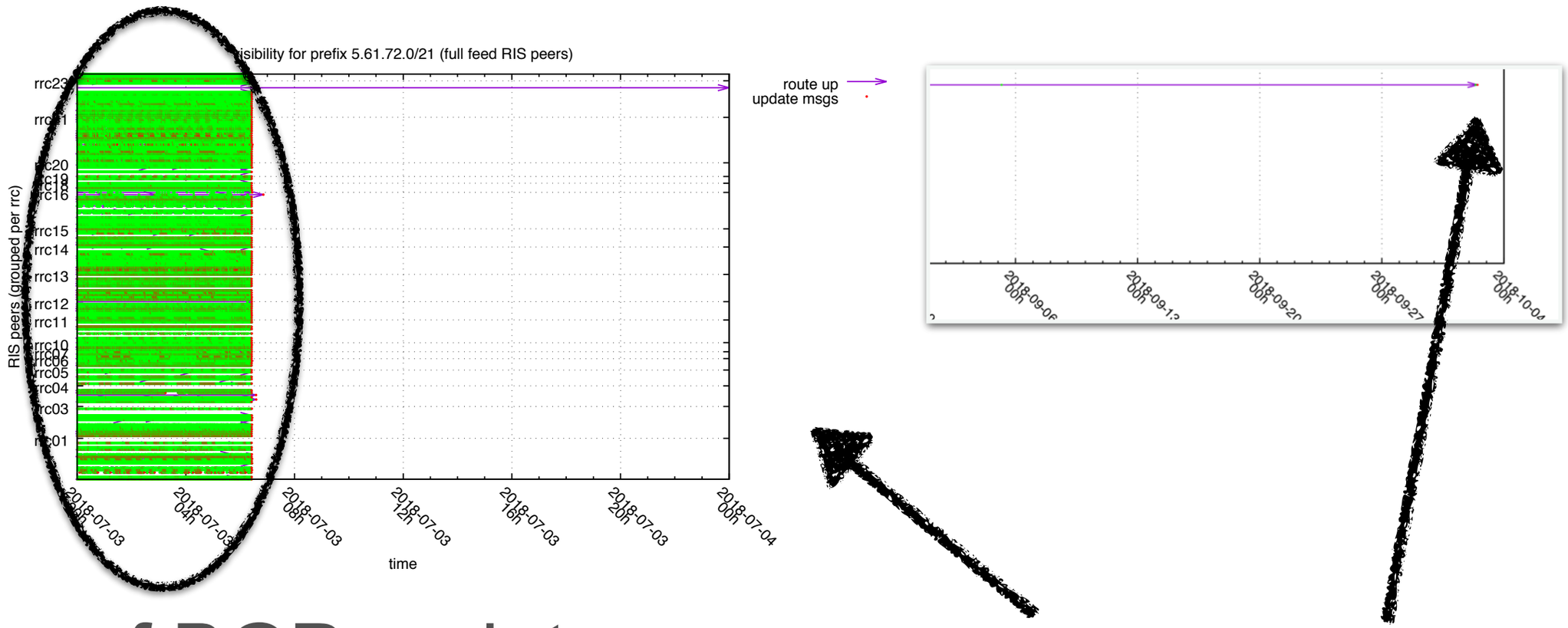
- https://seclists.org/nanog/2018/Jul/381

Re: AS205869, AS57166: Featured Hijacker of the Month, July, 2018

From: Jérôme Nicolle <jerome () ceriz fr>
Date: Wed, 25 Jul 2018 12:58:46 +0200

```
Hi Ronald,

| From your initial list, I can still see some prefixes with the NLnog ring :

http://lg.ring.nlnog.net/prefix_detail/lg01/ipv4?q=206.41.128.0
http://lg.ring.nlnog.net/prefix_detail/lg01/ipv4?q=52.128.192.0
http://lg.ring.nlnog.net/prefix_bgpmap/lg01/ipv4?q=206.222.128.0

Also http://lg.ring.nlnog.net/prefix_bgpmap/lg01/ipv4?q=94.130.90.152

Best regards,
```

Example: Long Lived Zombie



Tons of BGP updates

3 Months!

Route totally withdrawn only after manual intervention

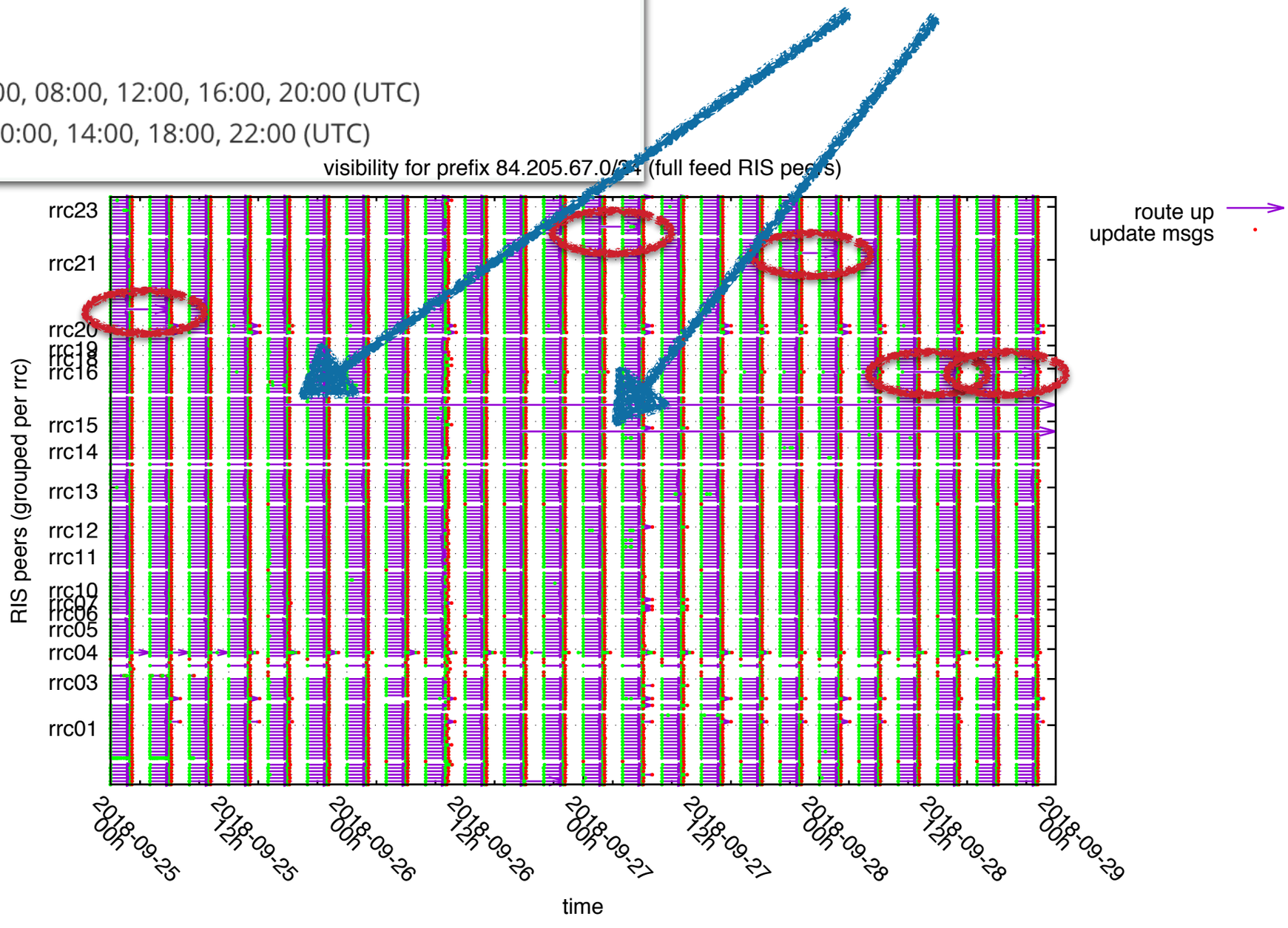
First Step: BGP Beacons

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)



Some RIS peers See More Zombies

- @@we’re still working on this!

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?
-