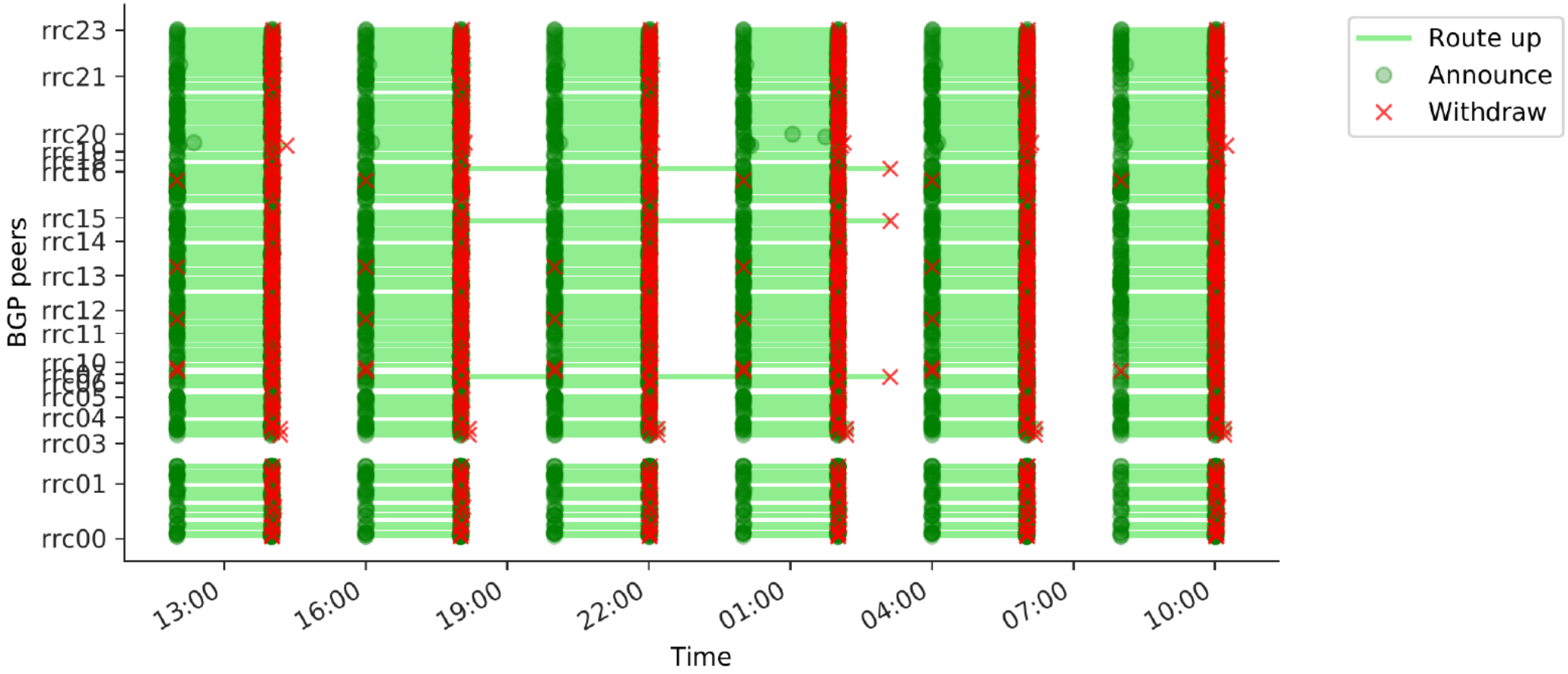
Hunting BGP Zombies in the Wild

Porapat Ongkanchana (U.Tokyo), **Romain Fontugne** (IIJ),
Hiroshi Esaki (U.Tokyo), Job Snijders (Fastly), Emile Aben (RIPE NCC)

BGP zombie?

- **Withdrawn prefix still active in some routing tables**
- **Example with a RIS BGP beacon [PAM19]**



Motivations

Background

- Past study solely on BGP beacons [PAM'19]
- Considered to be due to bugs in routers

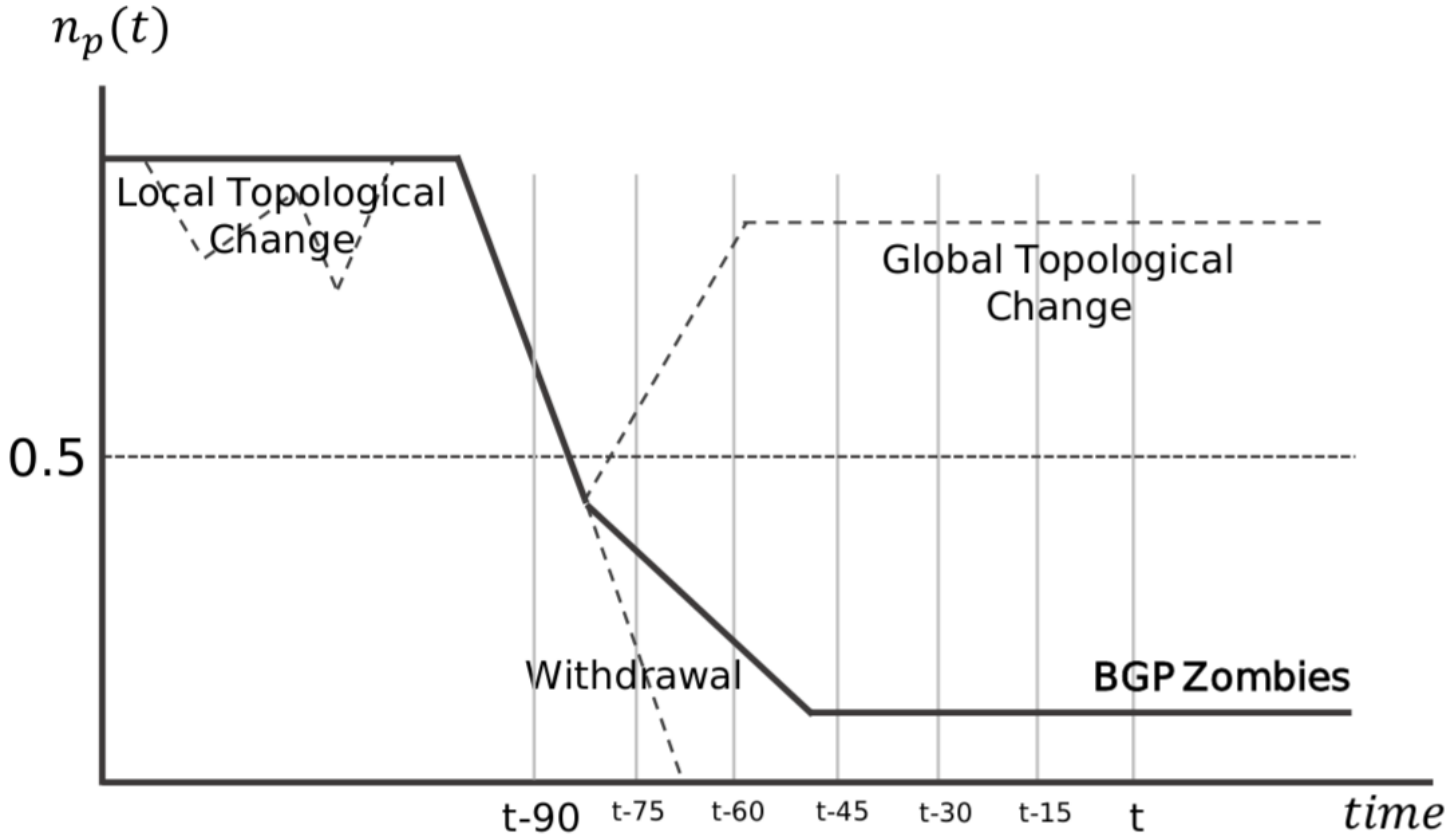
What about 'regular prefixes' used on the Internet?

- Does it happen at the same rate for 'regular prefixes'?
- How bad is zombie propagation in the wild?

Hunting zombies

Finding zombies for beacons is easy, how we do that for regular prefixes?

$n_p(t)$, the number of active routers for a prefix p:

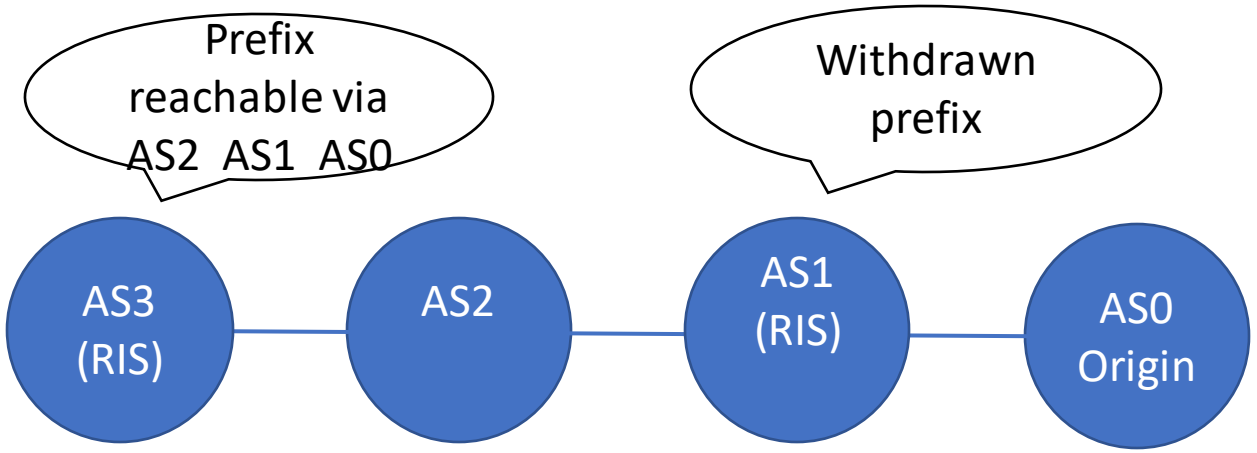


Results

- Run this detector on 6 years of RIS data and found 6.5M BGP zombies
- Sanity checks:
  - State coherence between RIS peers
  - Beacons and noisy prefixes
- Zombies in the wild:
  - Zombies for popular content networks
  - BGP Zombie side effects

State coherence between RIS peers

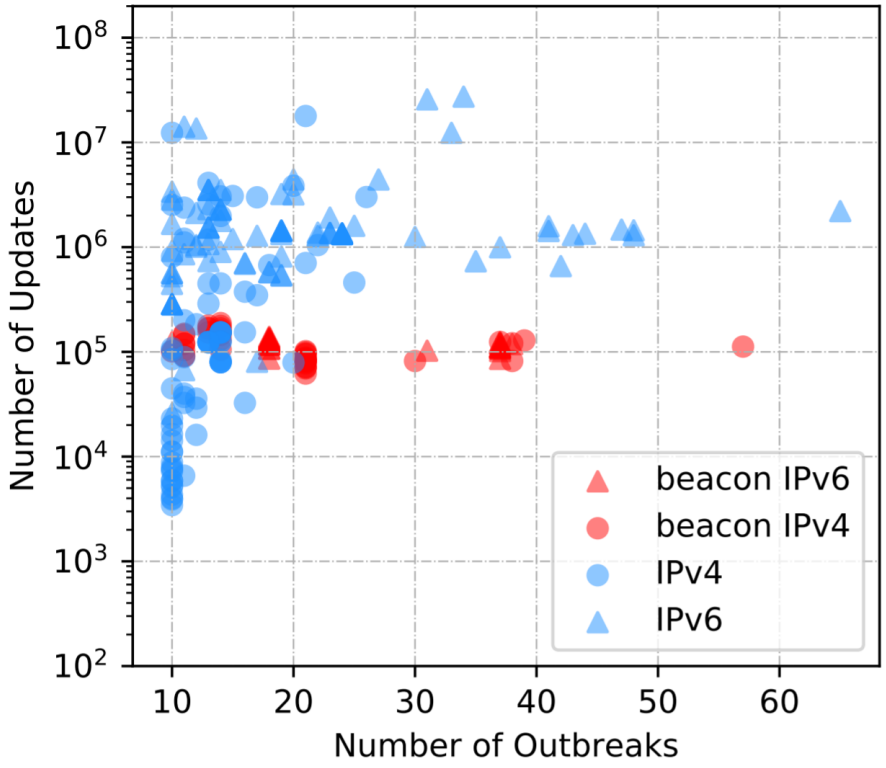
- Zombie with incoherent states:



- Paths with at least two RIS peers (68% of zombie paths)
  - 94.7% of these paths are incoherent
  - the rest are inconclusive

Beacons and noisy prefixes

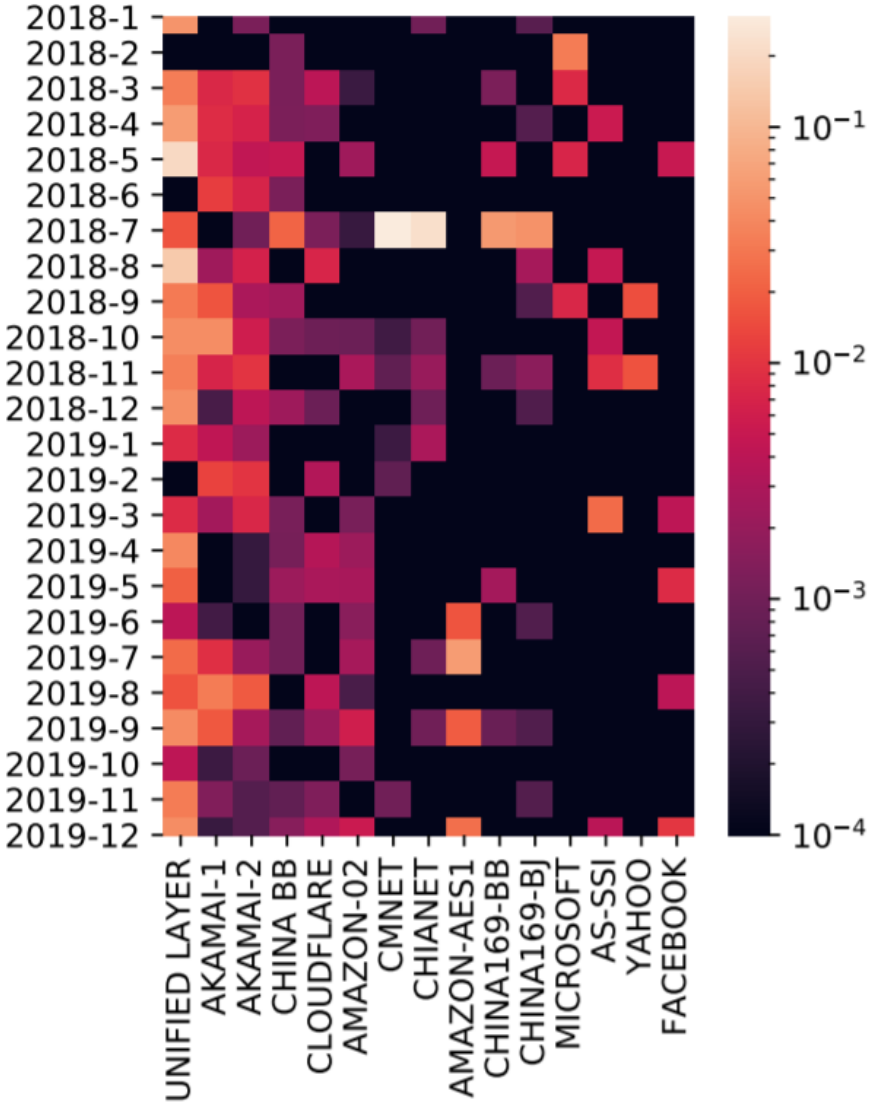
- 3.22% of detected zombies are for the 27 RIS beacon prefixes
- Noisier prefixes are prone to zombification?



→ Beacons are not really representative of what we observe for (IPv4) regular prefixes

Zombies for popular content networks

- Results for ASNs commonly found in top 15 Alexa/Umbrella/Majestic



Zombies for popular content networks

Table 1: Ranking of popular content networks according to prevalence of zombie outbreaks

AS	zombie rank	prefix rank	path rank
46606 Unified Layer	1	13	3
16625 Akamai	2	3	1
20940 Akamai	3	2	7
4134 China BB	4	7	15
13335 Cloudflare	5	6	12

BGP Zombie side effects

- 77k zombies creating detours (e.g. directing traffic to a backup link)
- 51k zombies have an origin AS different from the covering prefix
- 468 potential routing loops

See also: Pawel Malachowski, "Zombie routes", PLNOG 2020
https://www.slideshare.net/atendesoftware/bgp-zombie-routes

Conclusions

- We looked at BGP zombies for regular prefixes
- BGP zombies are widely spread
- But not as bad as what beacon study suggested
- Side effects: detours, routing loops

- Future:
  - Need more work on root cause analysis

- Code:
  - https://github.com/pora49494/zombie-hunter