A First Look into Long-lived BGP Zombies

Iliana Xygkou*+, Antonis Chariton*, Xenofontas Dimitropoulos*, Alberto Dainotti+
*Cisco ThousandEyes, +Georgia Institute of Technology

IMC 2025, Madison, U.S.A.

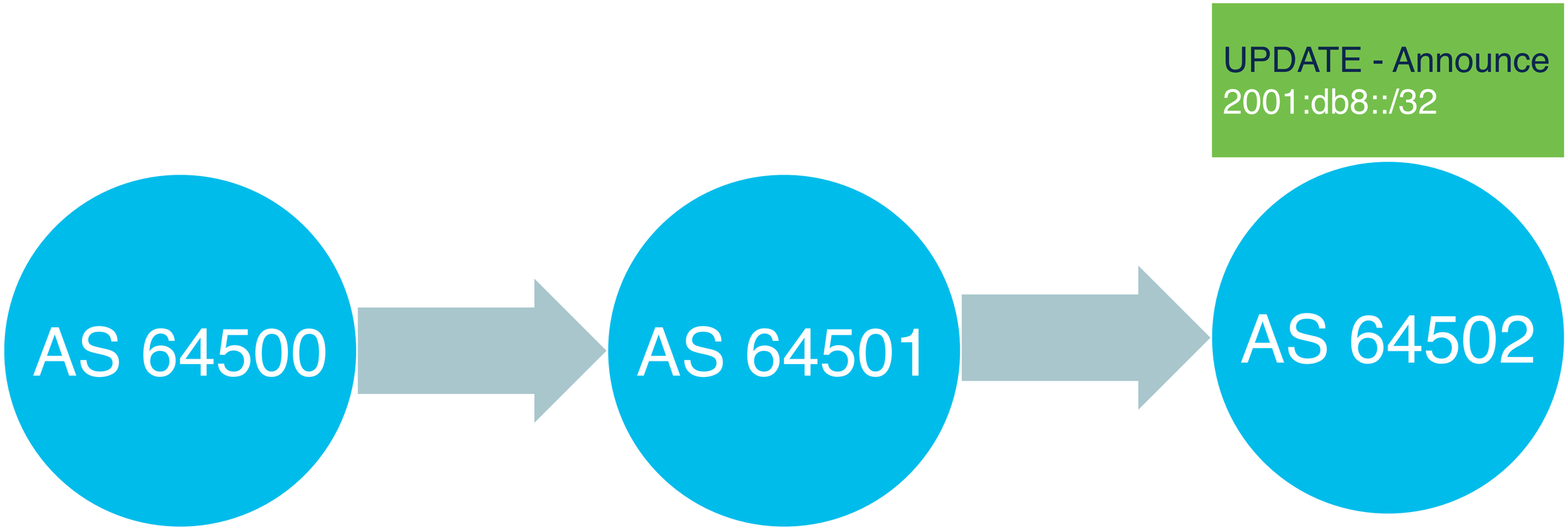
What are BGP Zombies?

What are BGP Zombies?

UPDATE - Announce
2001:db8::/32

What are BGP Zombies?

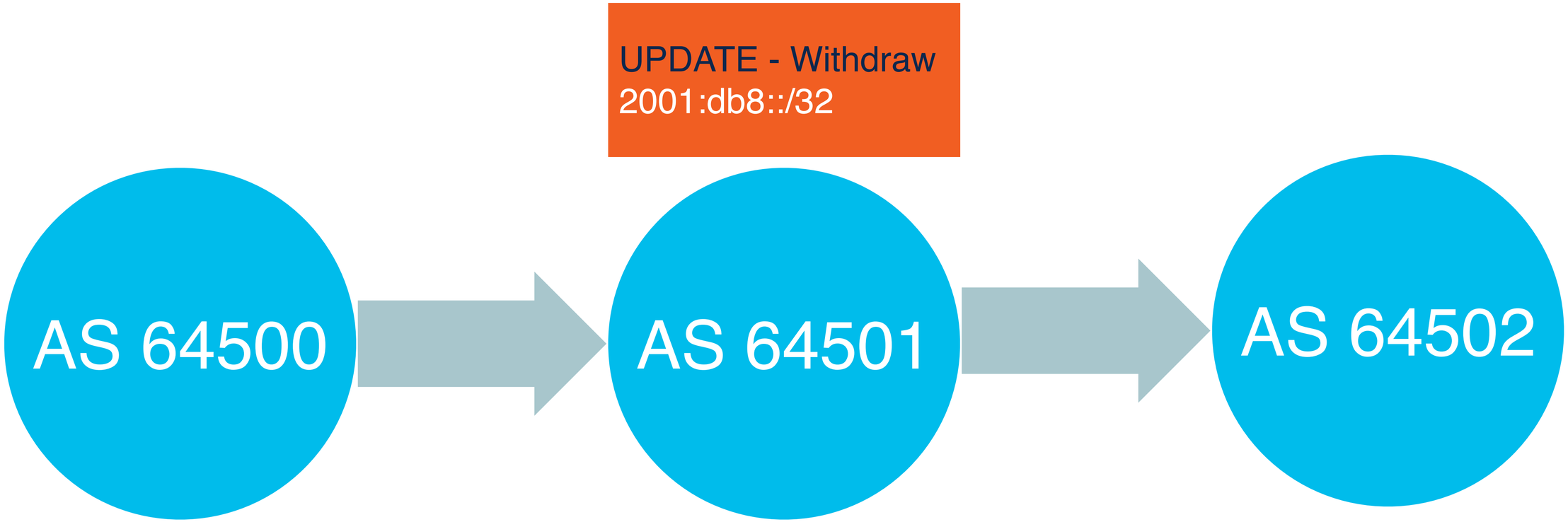
What are BGP Zombies?



What are BGP Zombies?

UPDATE - Withdraw
2001:db8::/32

What are BGP Zombies?



What are BGP Zombies?

What are BGP Zombies?

?

AS 64500

AS 64501

AS 64502

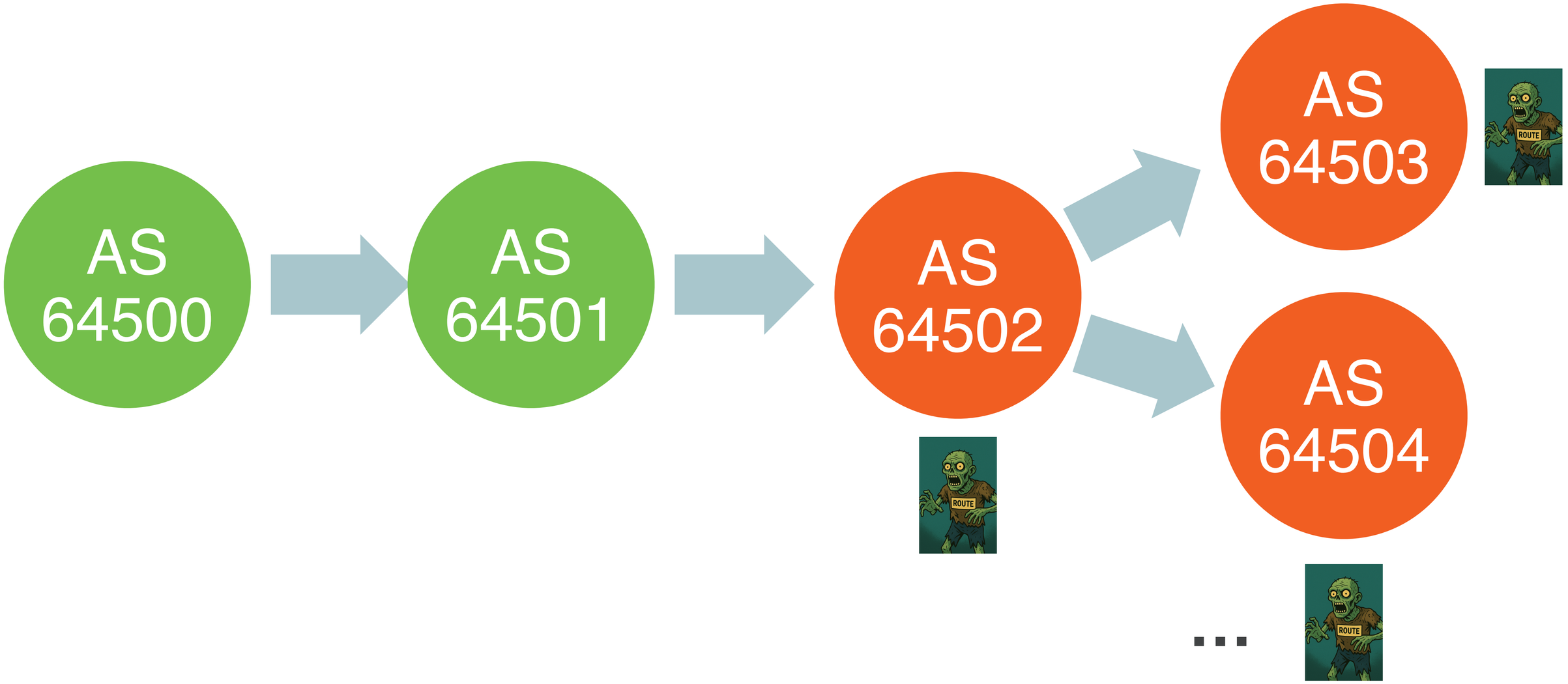
Routing Table
2001:db8::/32
Not found

Routing Table
2001:db8::/32
Not found

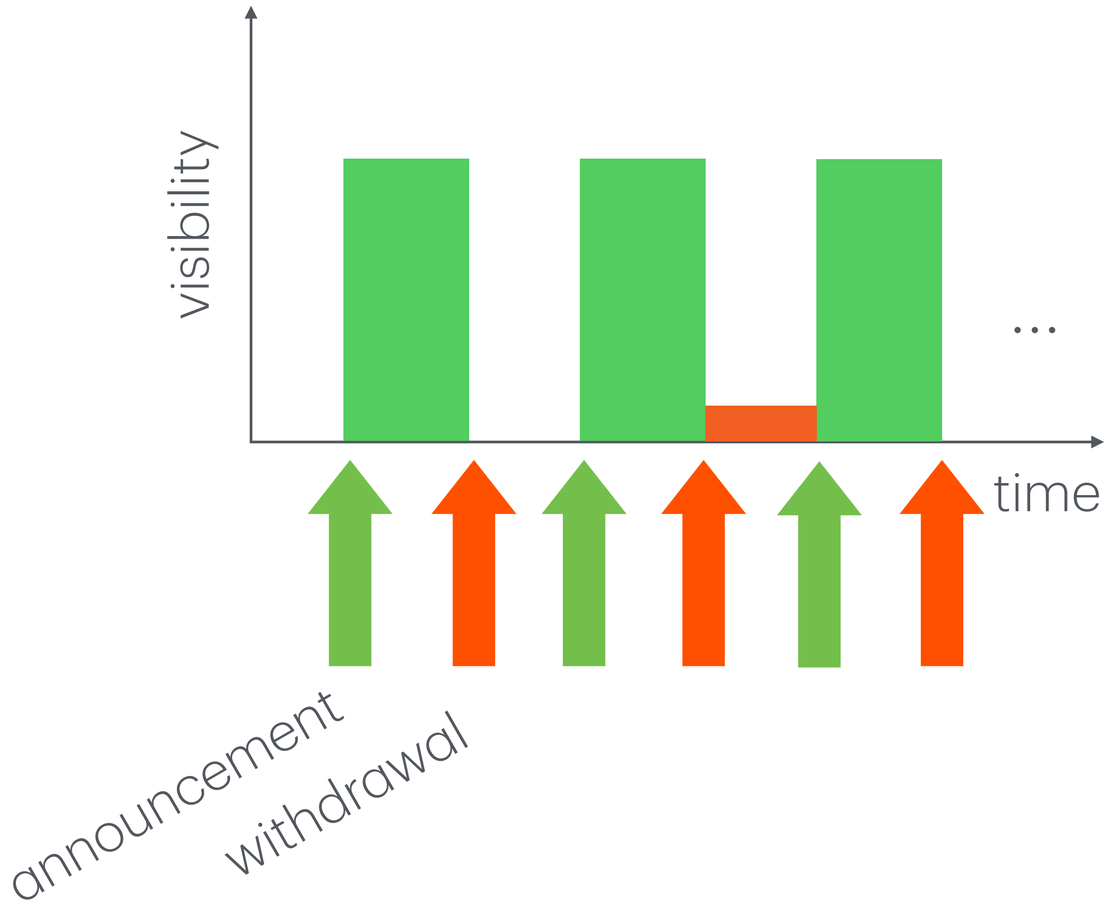
Routing Table
2001:db8::/32
via AS64501

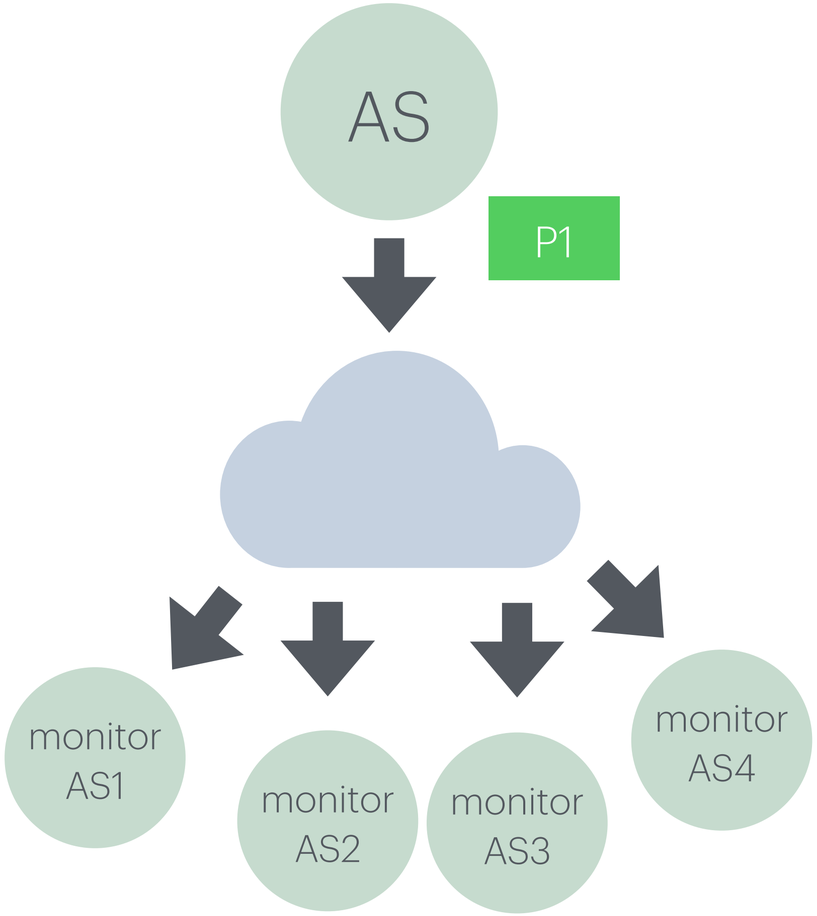
zombie route

What are BGP Zombies?



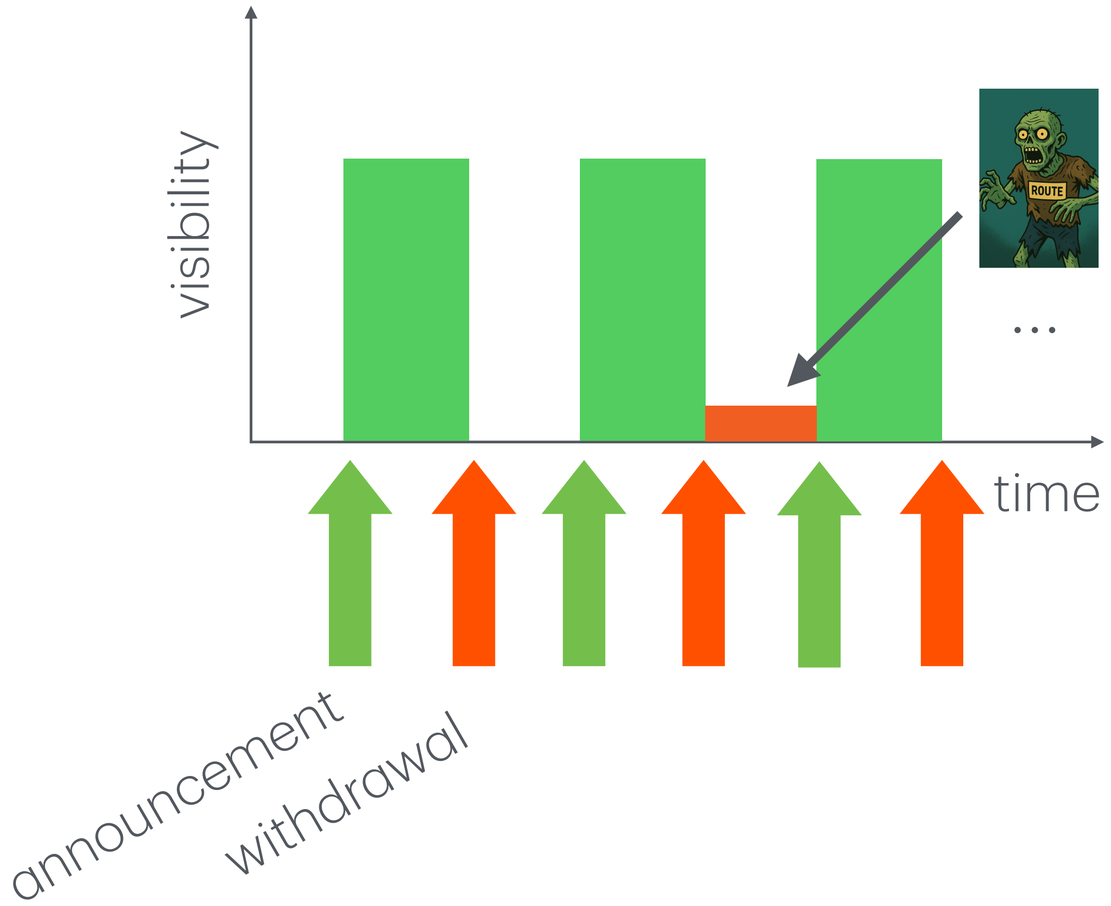
Observing zombies through controlled experiments

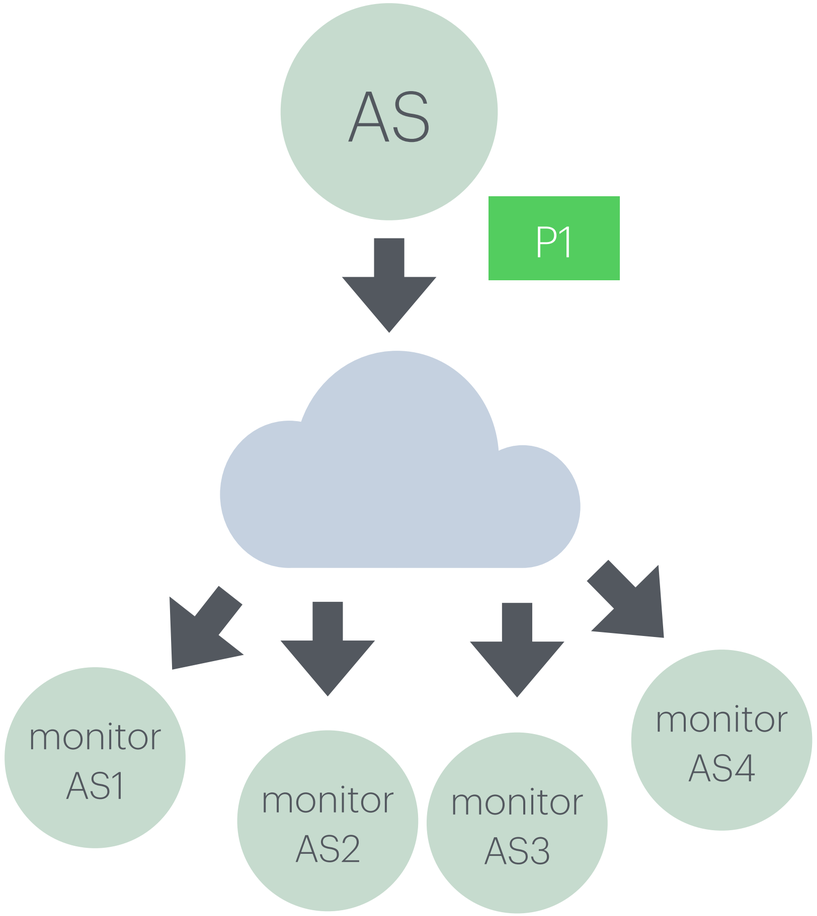




[1] “BGP Zombies: An Analysis of Beacons Stuck Routes.” by Fontugne *et al.* (PAM’19)

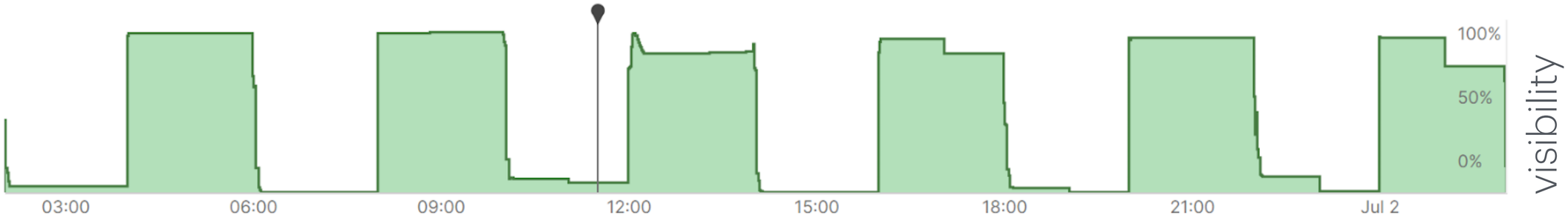
Observing zombies through controlled experiments



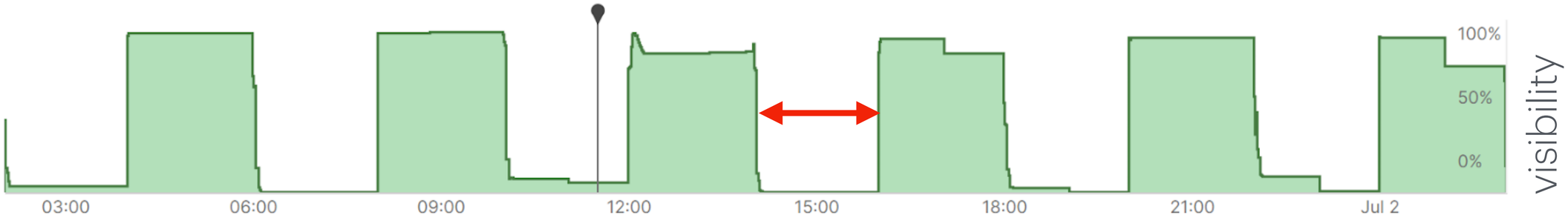


[1] “BGP Zombies: An Analysis of Beacons Stuck Routes.” by Fontugne *et al.* (PAM’19)

RIPE RIS Beacons: announce every 4 hrs, withdraw 2 hrs later

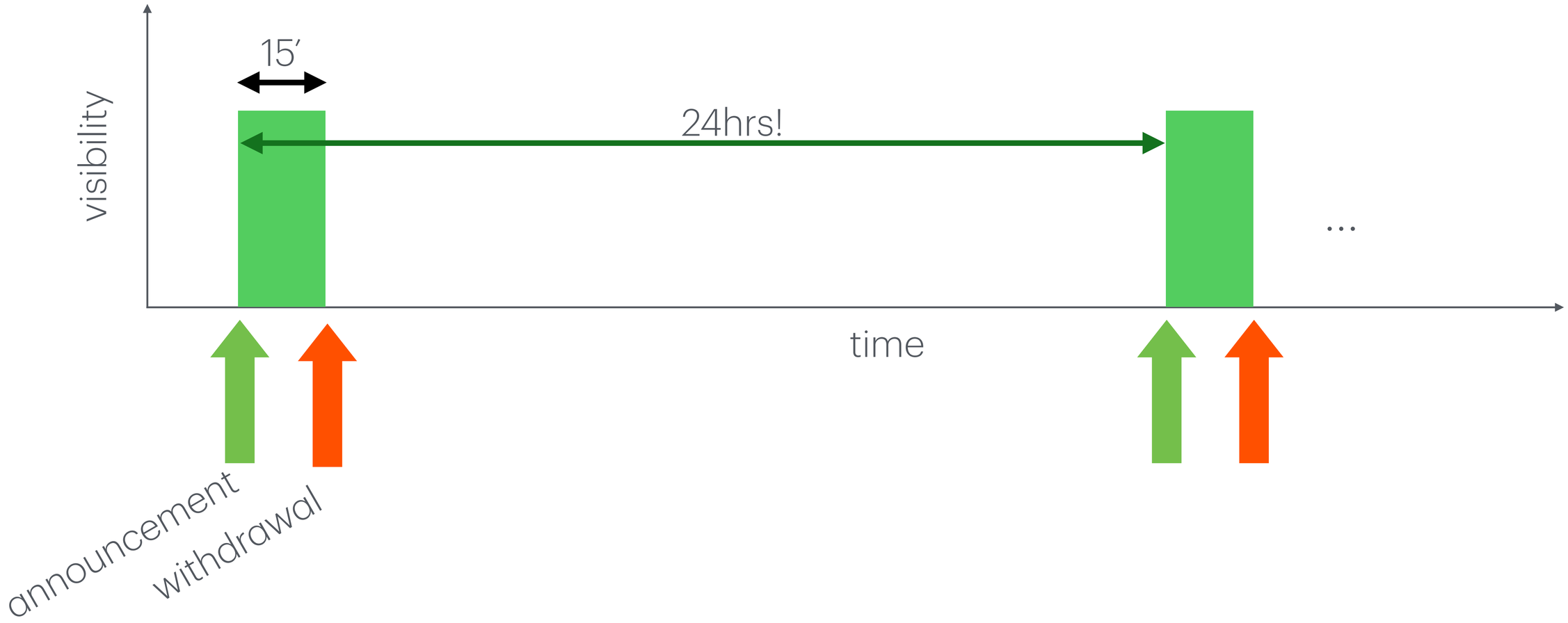


RIPE RIS Beacons: announce every 4 hrs, withdraw 2 hrs later

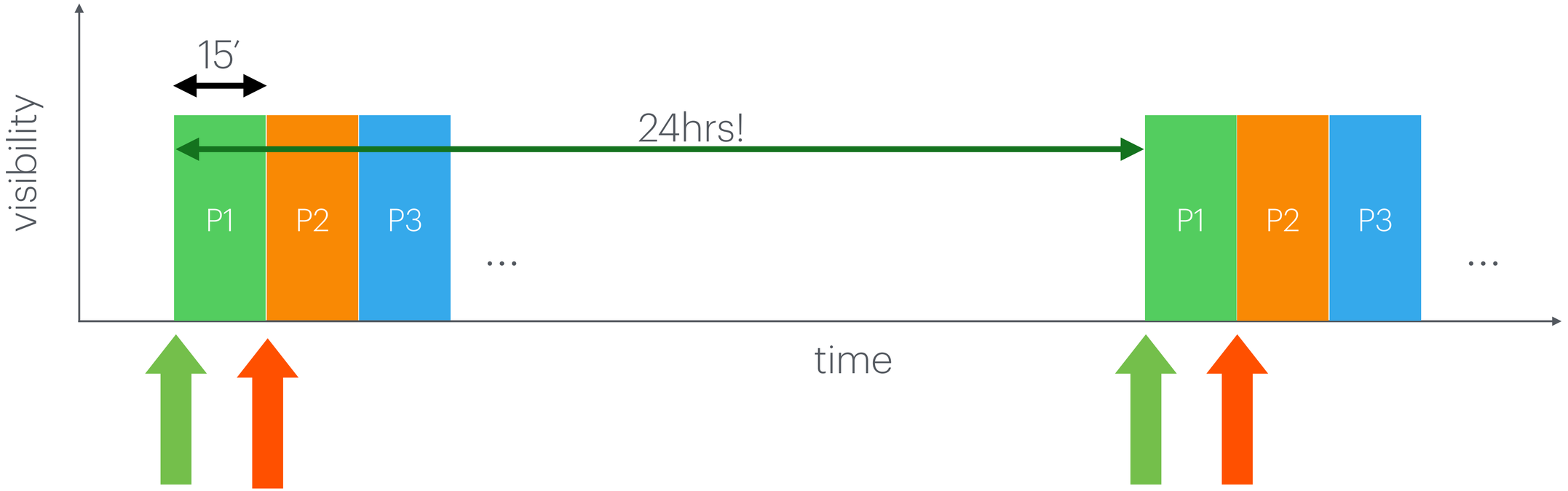


RIPE RIS beacons can remain zombies up to 2 hrs before getting re-announced → not much flexibility to study persistent zombies (**x**)

Our BGP beacons methodology



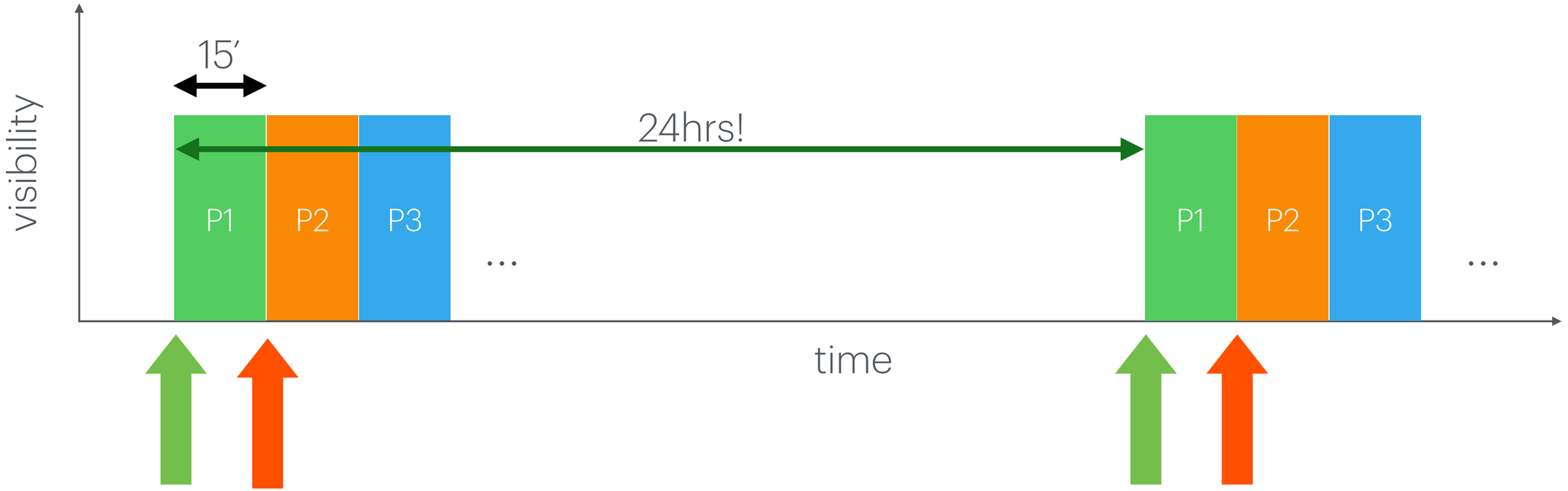
Our BGP beacons methodology



Our BGP beacons methodology

96 prefixes

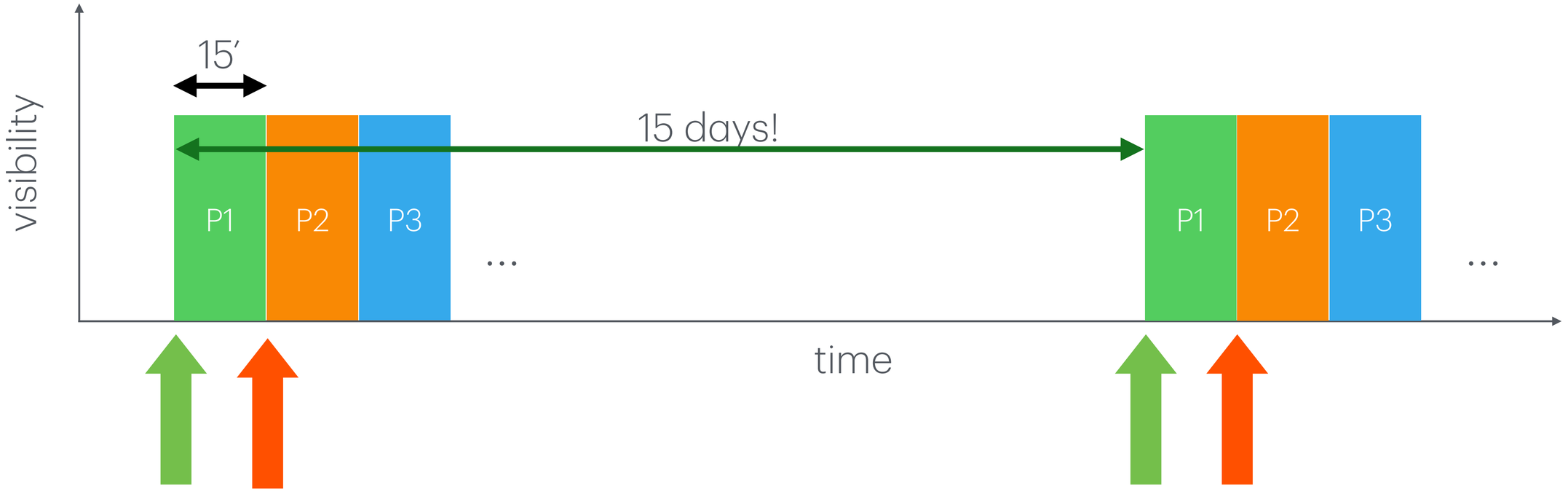
Our BGP beacons methodology



96 prefixes

beacon format: 2a0d:3dc1:HHMM::/48

Our BGP beacons methodology



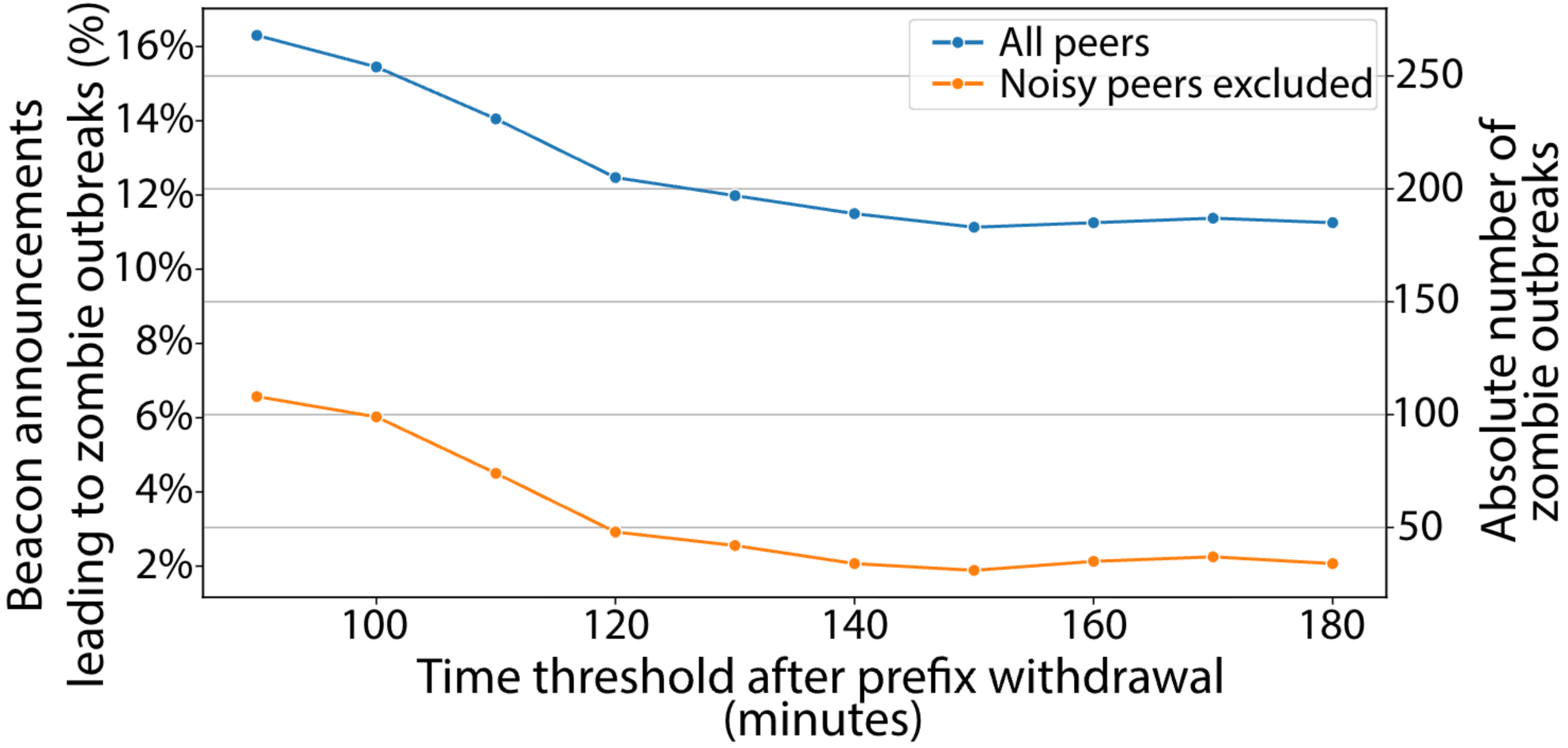
1,440 prefixes

beacon format: 2a0d:3dc1:(HH)(MM+dd%15)::/48

Long-lived Zombies!

- *We run the beacons for 2024/06/04–2024/06/10 (1), and 2024/06/10—2024/06/22 (2)*
- *3 outlier noisy peers with ~7% rate of zombies…*

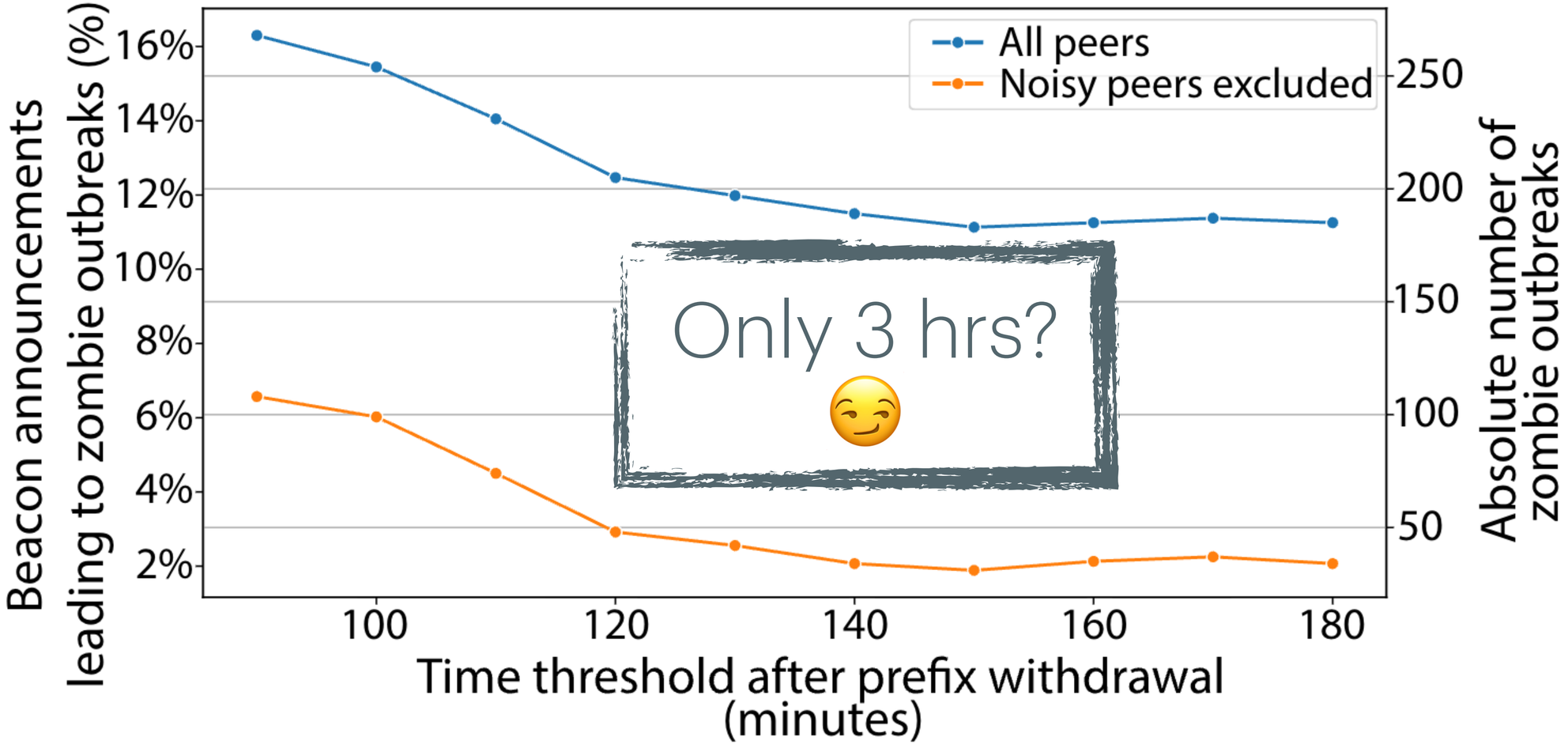
  Zombies indeed persist even after 3 hrs after the withdrawal!



Long-lived Zombies!

- *We run the beacons for 2024/06/04–2024/06/10 (1), and 2024/06/10—2024/06/22 (2)*
- *3 outlier noisy peers with ~7% rate of zombies…*

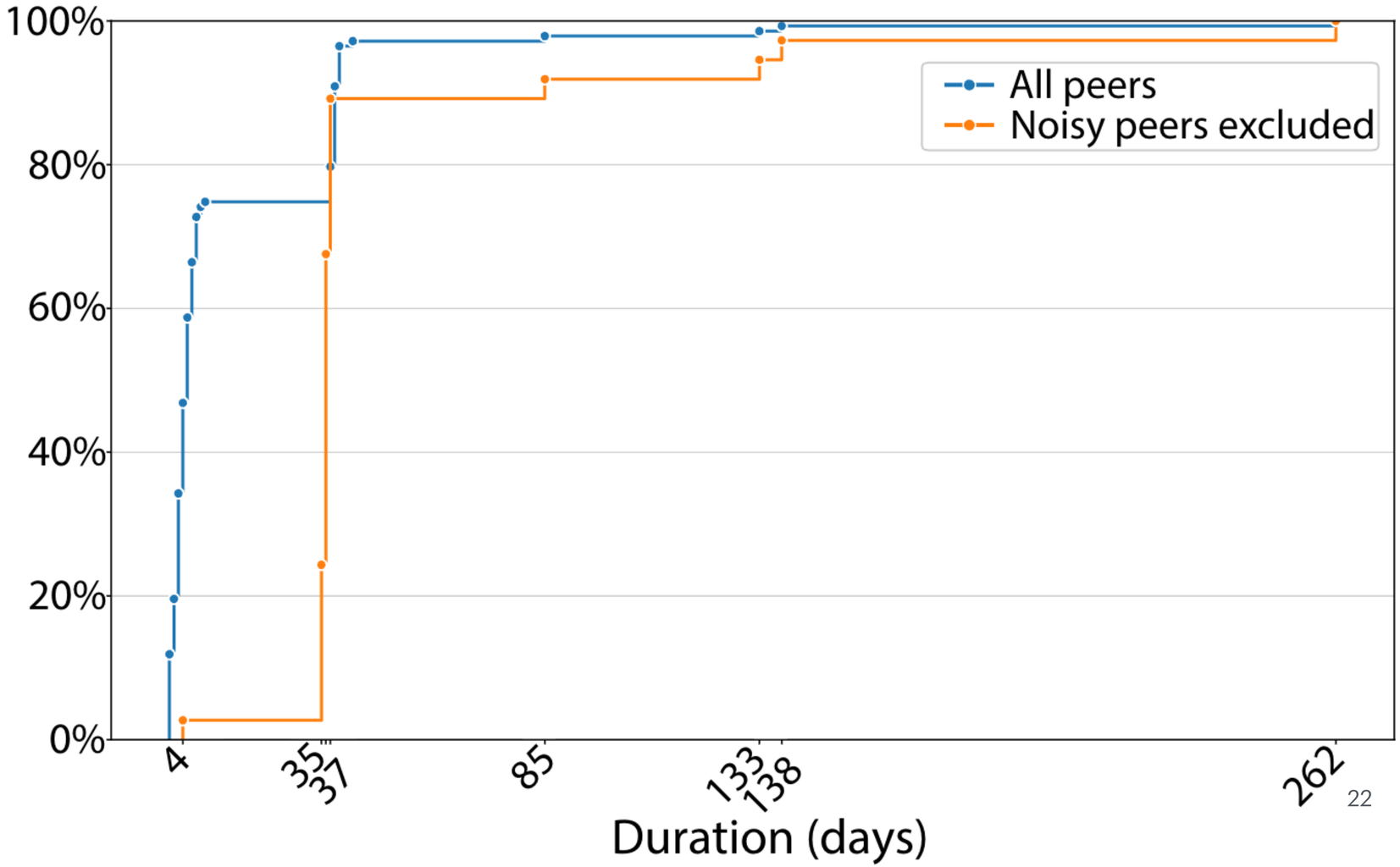
  Zombies indeed persist even after 3 hrs after the withdrawal!



Long-lived Zombies!

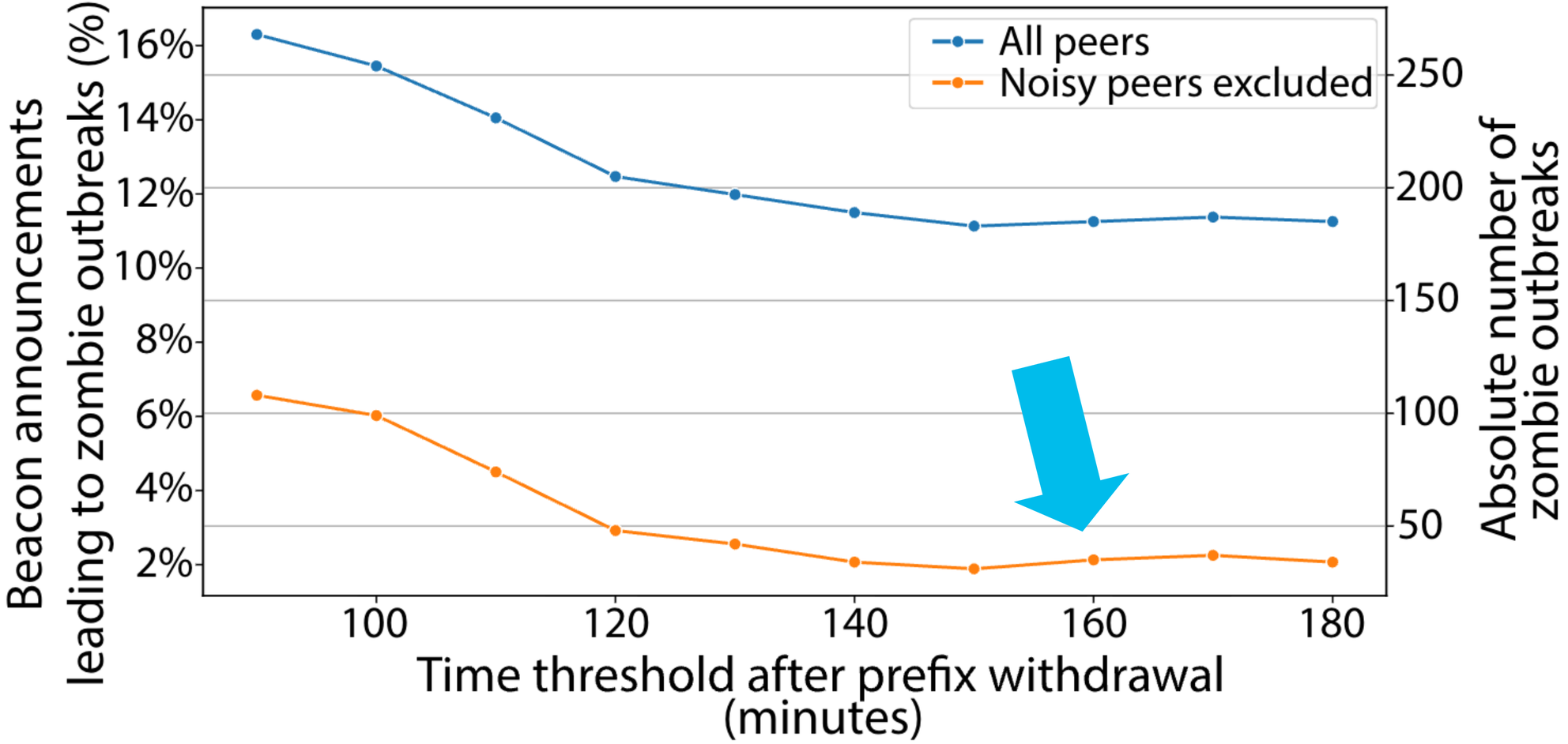
- *Experiments stopped at 2024/06/22*
- *Use RIPE RIS RIB dumps to ..make things faster.. and look even further into time*

- *Zombies can survive even for ~8.5 months!*



Resurrected Zombies!!

Did you notice that? Zombies number can increase over time!

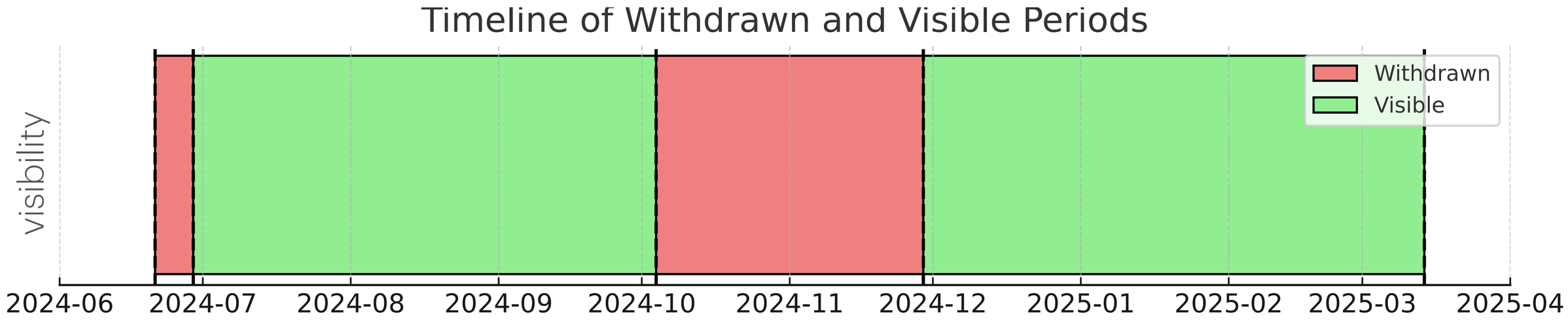


Resurrected Zombies!!

Did you notice that? Zombies number can increase over time!

For example, 2a0d:3dc1:1851::/48 was visible by RIPE RIS peers on and off — it was stuck in some router in the Internet.

Router bugs, BGP session resets or even normal filter changes can make infected routers re-propagate zombie routes to the rest!

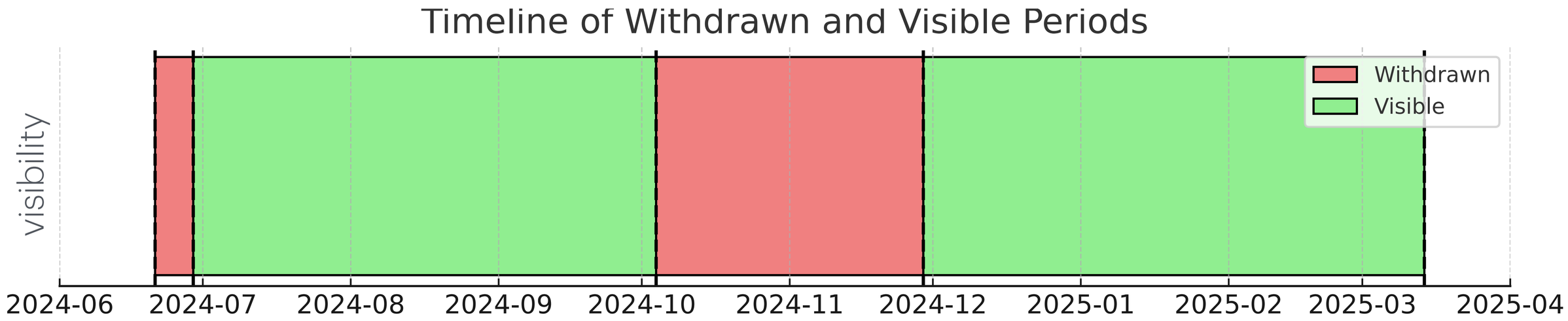


Resurrected Zombies!!

Did you notice that? Zombies number can increase over time!

For example, 2a0d:3dc1:1851::/48 was visible by RIPE RIS peers on and off — it was stuck in some router in the Internet.

Router bugs, BGP session resets or even normal filter changes can make infected routers re-propagate zombie routes to the rest!



Summary & Next Steps

- ✓ Our BGP beacons methodology that allows to study:
  - ✓ Long-lived BGP zombies (even month-long)
  - ✓ Resurrected zombies

Summary & Next Steps

- ✓ Our BGP beacons methodology that allows to study:
  - ✓ Long-lived BGP zombies (even month-long)
  - ✓ Resurrected zombies
- Study different dimensions of BGP zombies
  - IPv6 vs IPv4 ()
  - Root-cause detection + characterization of infected ASes
- Request by network operators for a long-term service of our beacons to detect and mediate stuck routes in real time

Thank you!

Check out the
Stuck Routes Observatory!