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- Withdrawn prefix still active in some routing tables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 $p$: 

![Graph showing $n_p(t)$ over time]
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

Diagram:
- AS3 (RIS) -> AS2 -> AS1 (RIS) -> AS0 Origin
  - Prefix reachable via AS2 AS1 AS0
  - Withdrawn prefix
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

<table>
<thead>
<tr>
<th>AS</th>
<th>zombie rank</th>
<th>prefix rank</th>
<th>path rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>46606 Unified Layer</td>
<td>1</td>
<td>13</td>
<td>3</td>
</tr>
<tr>
<td>16625 Akamai</td>
<td>2</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>20940 Akamai</td>
<td>3</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td>4134 China BB</td>
<td>4</td>
<td>7</td>
<td>15</td>
</tr>
<tr>
<td>13335 Cloudflare</td>
<td>5</td>
<td>6</td>
<td>12</td>
</tr>
</tbody>
</table>
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