Weaponizing BGP
Using Communities

Florian Streibelt, Franziska Lichtblau, Robert Beverly, Cristel Pelsser, Georgios Smaragdakis, Randy Bush, Anja Feldmann
Ill-Defined Semantics

We have a syntax, \texttt{AS:<blarg>}

But there are no formal semantics, just convention and BCPs

We’re putting semantics in comments

\texttt{i = 0; /* i = 42 */}
Flavors, We Think

• Active
  • Path prepending
  • Modify local preference
  • Remote triggered blackholing
  • Selective announcements

• Passive
  • Location Tagging
  • RTT Tagging

And then anything a thousand kiddies have invented
Propagation

• RFC 1997: Communities are a transitive optional attribute
• RFC 7454: Scrub own, forward foreign communities
• So many people do not expect them to propagate that widely
• I, for one, did not
Only 14% of Transit ASs propagate communities

(2.2k of 15.5k)
Surprise!

• 14% seems small, but AS graph is highly connected
• More than 50% of communities traverse more than four ASes
• 10% of communities have a hop count of more than six ASes
• Longest community propagation observed: through 11 ASes
On/Off Path

1 -> 2

2 -> 3

2 -> 4
On/Off Path

Diagram:

1 → 2 → 3 (with probability p)
1 → 2 → 4
On/Off Path

1 → 2

2 → 3
2 → 4
On/Off Path

1 → 2 → 3

1 → 2 → 4
On/Off Path

1 -> 2: 3:666

2 -> 3: p
2 -> 4: p
On/Off Path

1 —> 2: 3:666
2 —> 3 and 4: p
3 —> 4: 3:666
2 and 3 are On Path
On/Off Path

2 and 3 are On Path
On/Off Path

2 and 3 are On Path
4 is Off Path
So Let's Break Things!
Method to our Madness

• All experiments first tested in Lab
• Impacts were estimated
• Validated on the Internet, with operators' consent, e.g. for hijacks
Remote Triggered Black Hole

Safeguards:
• Provider should check customer prefix before accepting RTBH
• Customer may only blackhole own prefixes
• Different policies for Customers/Peers
• On receiving RTBH, add no-export

AS1 sends p, tagged 2:666
AS2 continues announcing p
Traffic to p is dropped at AS2
What Can Happen

AS1 announces p
AS2 hijacks p, with AS3:666
Traffic to p is dropped at AS3
It Works Well

- Works multi-hop and is hard to spot
- Triggering RTBH is possible for attackers because, e.g.,
  - BH prefix is more specific, thus accepted via exception
  - Providers check BH community before prefix filters (bug in NANOG recipe)
- No validation for origin of community is possible
Traffic Steering
Traffic Steering

![Diagram of traffic steering network](image_url)
Traffic Steering
Traffic Steering

![Diagram of traffic steering with nodes labeled p1, p2, p3, p4, p5, and p6, and arrows indicating traffic flow between nodes. The diagram shows the flow from p1 to p2 to p3 to p4 to p5 to p6 to p7.]
Traffic Steering
Traffic Steering
Traffic Steering

Diagram showing traffic steering routes.
Traffic Steering

![Diagram of traffic steering](image-url)
Traffic Steering

Diagram of traffic steering with nodes labeled 1, 2, 3, 4, 5, 6, 7 and arrows indicating traffic flow.
Traffic Steering

Diagram showing traffic steering through nodes labeled 1, 2, 3, 4, 5, 6, and 7. Arrows indicate the flow of traffic with labels such as 'p321' and '6:3'.
That's Not Realistic
Oh Yeah?

https://dyn.com/blog/bgp-dns-hijacks-target-payment-systems/

“BGP hijacks made use of BGP communities to shape route propagation. Although they also changed origins, which was the giveaway.”
It’s the Cloud, Man

- ASN value ambiguous: who is “sender”, “recipient”
- No defined semantics, values can mean anything
- Used both for signaling and triggering of actions
- No cryptographic protection
- Attribution is impossible
- It is hard to apply filters or understand what is going on
Communities can be modified, added, removed by every AS

No attribution is possible

No cryptographic protection

Yet operators bet on their ‘correctness’

Large communities partially improve the situation
Don’t Propagate Without Thinking Very Deeply

• On Input – Drop anything not addressed to you, unless special agreement
• On Output – Drop everything except signals from you to the direct peer
• And Beware Cisco ‘mis-feature’ re well known communities

draft-ietf-grow-wkc-behavior-00
ONLY YOU CAN PREVENT WILDFIRES