Weaponizing BGP Using Communities

Florian Streibelt, Franziska Lichtblau, Robert Beverly, Cristel Pelsser, Georgios Smaragdakis, Randy Bush, Anja Feldmann
BGP Was Not Complex Enough

Operators Wanted Signaling on Top of Signaling
Add BGP Communities

Sprint
AS 1239

Verizon
AS 701

147.28.0.0/16
701:42

147.28.0.0/16
1239:77

IIJ
AS 2497

147.28.0.0/16
Syntax

AS#:number
But

AS#

May really be Anything
And

: number

May really Mean

Anything
Undefined Semantics

We have a syntax, AS:<blarg>

But there are no formal semantics, just convention and common practice

We’re putting semantics in comments

\[ i = 0; /* i = 42 */ \]
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 the 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

Diagram:

1 → 2 → 3
1 → 2 → 4
On/Off Path

1 → 2

p

2 → 3, 4
On/Off Path
On/Off Path

\[
\begin{align*}
1 & \rightarrow 2 \\
2 & \rightarrow 3 \\
2 & \rightarrow 4
\end{align*}
\]
On/Off Path

Diagram:

1 → 2 → 3 → 4

- Arrow from 1 to 2 labeled "p" and "3:666"
- Arrows from 2 to 3 and 4 labeled "p"
On/Off Path

Diagram:

- Node 1 to Node 2 with probability p and cost 3.666
- Node 2 to Node 3 with probability p and cost 3.666
- Node 2 to Node 4 with probability p
- Node 3
- Node 4
On/Off Path

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
Observed Communities

% communities observed

off-path

on-path

Remember this one

Creative Commons: Attribution & Share Alike
And We Have No Idea
What Almost All of Them Mean
The Internet is an Experimental Hack
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
RTBH

One of the Very Few Defined Communities
RTBH
Remotely Triggered Black Hole Community

“TargetAS:666”
Attached to a Prefix
A DoS Defense

Signaling that Traffic to a Prefix be Dropped
DDoS Attack

- AS 1 (1.2.3.4)
- AS 2
- X
- Y
Ask AS 2 to Black Hole

AS 2

AS 1 1.2.3.4

x

y
Traffic Dropped

AS 1
1.2.3.4

AS 2
1.2.3.4

X
2:666

y

2020.04.07 IDR Weaponizing BGP
Creative Commons: Attribution & Share Alike
Safeguards, in Theory

- Provider should check customer prefix before accepting RTBH
- Customer may only blackhole own prefixes
- Different policies for Customers/Peers
- On receiving RTBH, do not propagate
Which Looks Very Cool

Except it is an Attack Vector
The Attack

Attacker

AS 2

AS Z

1.2.3.4
2:666

Victim

AS 1

AS Z announces 1.2.3.4 to AS 2
With Black Hole Community
Good Traffic to AS 1 is Dropped
The Attack

AS Z announces 1.2.3.4 to AS 2
With Black Hole Community
Good Traffic to AS 1 is Dropped
The Attack Works Well

- Works from a distance 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
Off-Path Attacks

Remember this?

off-path

1 65000 666 100 0 3000 2 1000 9498 200

on-path

1000 100 1 200 2000 10 2 3000 0 500
Traffic Steering
Traffic Steering

Diagram:

- Node 1 connected to Node 2 with probability p1
- Node 2 connected to Node 3 with probability p2
- Node 3 connected to Node 4 with probability p3
- Node 4 connected to Node 5 with probability p4
- Node 5 connected to Node 6 with probability p5
- Node 6 connected to Node 7 with probability p6
- Node 7 connected to Node 1 with probability p6

Probabilities:
- p1
- p2
- p3
- p4
- p5
- p6
Traffic Steering

Diagram:

- Node 1 connected to Node 2 with label p1.
- Node 2 connected to Node 3 with label p21.
- Node 3 connected to Node 4 with label p321.
- Node 4 connected to Node 5 with label p4321.
- Node 5 connected to Node 7 with label p54321.
- Node 6 connected to Node 7 with label p6321.
- Node 6 connected to Node 3 with label p321.
Traffic Steering
Traffic Steering
Traffic Steering
Traffic Steering
Traffic Steering

Diagram showing network traffic routing with nodes labeled 1, 2, 3, 4, 5, 6, 7, and edges marked with p3, p2, and p1.
Traffic Steering

The diagram shows a network with nodes labeled 1 to 7. The edges between the nodes are marked with different types of traffic, indicated by the numbers 2, 3, 4, 5, 6, and 7.
Traffic Steering
But Is That Realistic?
Yes, In The Wild!

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
I Read it on the Internet

- 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
- RFC 8642 - Policy Behavior for Well-Known BGP Communities
Design on a Napkin
Die by Napkin
ONLY YOU CAN PREVENT WILDFIRES