“Deep Dive into BGP Communities”

Georgios Smaragdakis

Joint work with Emile Aben, Arthur Berger, Robert Beverly, Randy Bush, Chris Dietzel, Anja Feldmann, Vasileios Giotsas, Franziska Lichtblau, Cristel Pelsser, Philipp Richter, Florian Streibelt, and many other colleagues!
The Internet is the Digital Backbone of our Civilization
Cyberattacks and Outages are Serious Threats

Our objective: Understand the **State** and **Health** of the Internet’s Routing System
The New Internet

source: “Internet Interdomain Traffic”, Labovicz et al. SIGCOMM 2010
IXPs around the Globe

>300 active IXPs, ~125 Tbps Traffic, ~2 Million peerings
IXP is more than a Big Switch, it is an Ecosystem

LINX (London Internet Exchange) in Telehouse Colocation Facility (Telehouse North at Docklands)

1000s of cross-connects established in the datacenters
Peering Infrastructures are Critical Infrastructures

DHS and ENISA have characterized peering infrastructures as critical infrastructures – in the same category as nuclear reactors and power powerhouses. [An Annex to the National Infrastructure Protection Plan, 2010, 2015; Critical Infrastructures and Services, Internet Infrastructure: Internet Interconnections, 2010]

Internet Exchange Points: Typical SLA 99.99% (~52 min. downtime/year)¹

Colocation facilities: Typical SLA 99.999% (~5 min. downtime/year)²

¹ [https://ams-ix.net/services-pricing/service-level-agreement](https://ams-ix.net/services-pricing/service-level-agreement) ² [http://www.telehouse.net/london-colocation/](http://www.telehouse.net/london-colocation/)
Current practice: “Is anyone else having issues?”

- ASes try to crowd-source the detection and localization of outages.
- Inadequate transparency/responsiveness from infrastructure operators.
The AMS-IX outage

Outage in AMS-IX, Amsterdam, The Netherlands on May 14, 2015
The AMS-IX outage

Outage in AMS-IX, Amsterdam, The Netherlands on May 14, 2015

DE-CIX in Frankfurt

Graph showing data rate in Gbps over time (UTC).
Challenges in detecting infrastructure outages

Before outage

Observed paths

Actual incident
Challenges in detecting infrastructure outages

Before outage

During outage

Actual incident

Observed paths
Challenges in detecting infrastructure outages

1. Capturing the **infrastructure-level hops** between ASes

Before outage

During outage

AS path does not change!
Challenges in detecting infrastructure outages

1. Capturing the infrastructure-level hops between ASes
Challenges in detecting infrastructure outages

1. Capturing the infrastructure-level hops between ASes
2. Correlating the paths from multiple vantage points
Challenges in detecting infrastructure outages

1. Capturing the infrastructure-level hops between ASes
2. Correlating the paths from multiple vantage points
3. Continuous monitoring of the routing system
Challenges in detecting infrastructure outages

1. Capturing the infrastructure-level hops between ASes
2. Correlating the paths from multiple vantage points
3. Continuous monitoring of the routing system

Can we combine BGP continuous passive measurements with fine-grained topology discovery?
Deciphering location metadata in BGP

Is BGP an information hiding protocol?

PREFIX: 1.0.0.0/24
ASPATH: 2 1 0
COMMUNITY: 2:200
Deciphering location metadata in BGP

BGP Communities:
- Optional attribute
- 32-bit numerical values
- Encodes arbitrary metadata
Deciphering location metadata in BGP

Prefix: 1.0.0.0/24
ASPATH: 2 1 0
COMMUNITY: 21200

Top 16 bits:
ASN that sets the community.

Bottom 16 bits:
Numerical value that encodes the actual meaning.
Deciphering location metadata in BGP

The BGP Community 2:200 is used to tag routes received at Facility 2 i.e, Location Information!!
Deciphering location metadata in BGP

The BGP Community 4:400 is used to tag routes received at Facility 4 and at the IXP.
Deciphering location metadata in BGP

PREFIX: 3.3.3.3/24
ASPATH: 4 3
COMMUNITY: 4:8714 4:400

PREFIX: 2.2.2.2/24
ASPATH: 4 2
COMMUNITY: 4:8714 4:400

PREFIX: 1.0.0.0/24
ASPATH: 2 1 0
COMMUNITY: 2:200
Deciphering location metadata in BGP

When a route changes ingress point, the community values will be update to reflect the change.
Building a BGP Communities Dictionary

- Community values not standardized
- Natural Language Tools
- Documentation in public data sources: Internet Routing Registries (IRRs), NOCs websites
Building a BGP Communities Dictionary

3,049 communities for **locations** used by 468 Ases
Topological coverage

- ~50% of IPv4 and ~30% of IPv6 paths annotated with at least one Community in our dictionary.
- 24% of the facilities in PeeringDB, 98% of the facilities with at least 20 members.
Passive outage detection: **Initialization**

For each vantage point (VP) collect all the **stable** BGP routes tagged with the communities of the target facility (Facility 2)
Passive outage detection: **Initialization**

For each vantage point (VP) collect all the **stable** BGP routes tagged with the communities of the target facility (Facility 2)
Passive outage detection: **Monitoring**

Track the BGP updates of the stable paths for changes in the communities values that indicate ingress point change.
Passive outage detection: Monitoring

We ignore about single router-level/AS-level path changes if the ingress-tagging communities remain the same.
Passive outage detection: Outage signal

Crowdsourcing mechanism: Concurrent changes of communities values for multiple networks for the same facility is an indication of outage.
Passive outage detection: Outage signal

Crowdsourcing mechanism: Concurrent changes of communities values for multiple networks for the same facility is an indication of outage.
Passive outage detection: **Outage tracking**

End of outage inferred when the majority of paths return to the original facility.
De-noising BGP routing activity

The aggregated activity of BGP messages (announcements, withdrawals, states) provides no outage indication.
De-noising BGP routing activity

The aggregated activity of BGP messages (announcements, withdrawals, states) provides no outage indication.

The BGP activity filtered using communities provides strong outage signal.
Providing Hard Evidence: DE-CIX? Outage

Interxion Frankfurt Outage (2018/04/09)
Changes in BGP paths annotated with communities that tag the location of inter-domain connections
Observed outages

- **159** outages in 5 years of BGP data
  - 76% of the outages not reported in popular mailing lists/websites
- Validation through status reports, direct feedback, social media
  - 90% accuracy, 93% precision (for trackable PoPs)
Effect of outages on Service Level Agreements

~70% of failed facilities worse than 99.999% uptime
~50% of failed IXPs worse than 99.99% uptime
5% of failed infrastructures worse than 99.9% uptime!
Measuring the performance impact of outages

Median RTT rises by > 100 ms for rerouted paths during AMS-IX outage.
Cyberattacks and Outages are Serious Threats
Networks under Attack

AS1

AS2

AS3

AS4

172.18.192.1

Attack Target Server

ATTACK

TARGET
BGP Blackholing in the Internet

172.18.192.1/32
Community = AS3:666

RFC1997, RFC6535, RFC7999

AS1

AS2

AS3

AS4

172.18.192.1

Attack Target Server
BGP Blackholing in the Internet

AS1 → AS2 → AS3 → AS4

RFC1997, RFC6535, RFC7999

172.18.192.1

Attack Target Server
The Rise of BGP Blackholing

Active blackholed prefixes

2014-12-01 2015-03-01 2015-06-01 2015-09-01 2015-12-01 2016-03-01 2016-06-01 2016-09-01 2016-12-01 2017-03-01

(B) (C)(D) (E) (F)

6x
The Rise of BGP Blackholing

Active blackholed prefixes

2014-12-01 2015-03-01 2015-06-01 2015-09-01 2015-12-01 2016-03-01 2016-06-01 2016-09-01 2016-12-01 2017-03-01

Mirai
BGP Blackholing Efficacy: Active Measurements

Reduction by 3 AS hops (on average)
Cyberattacks and Outages are Serious Threats

Can BGP Communities be Abused?
BGP Communities Usage is on the Rise

Communities is the Swiss Knife of operators:
- 75% of the BGP announcement have >1 community

Usage:
- location
- blackholing
- Traffic Engineering: path prepending, local preference, selective announcements
- RTT delays
Teaser Example of BGP Communities Attacks

prefix P originated by AS1

prefix P

prefix P

prefix P

prefix P
Teaser Example of BGP Communities Attacks

prefix P originated by AS1
prefix P
prefix P
prefix P
prefix P
prefix P
prefix P
Teaser Example of BGP Communities Attacks

- Prefix P originated by AS1
- Prefix P|AS3:x3
- X3 AS prepending using the community of AS3
- Community Target

AS1 → AS2 → AS4 → AS3 → AS5 → AS6

Attacker

Attackee

Attackee
Teaser Example of BGP Communities Attacks

- Prefix P originated by AS1
- Prefix PI of AS3
- Prefix PI of AS3
- Prefix PI of AS3
- Prefix PI of AS3
- Prefix PI of AS3
- Prefix PI of AS3

AS1 → AS2 → AS4

AS5

AS6

AS3

Community Target
BGP communities is an optional and transitive attribute:
14% of transit provider (2.2K out of 15.5K) propagate communities
AS path prepending Attack without Hijack even if route is authenticated (on-path)

Similar attacks can take place for local pref and other traffic steering techniques
AS path prepending Attack with Hijack (off-path)
AS path prepending Attack with Hijack (off-path)
Experimentation

Traffic Steering
- Does not propagate communities by default

Blackholing
- Propagates Communities by default
- Order of rules in configuration plays an important role!

Route Manipulation
- Order of rules in configuration plays an important role!

With Ethical Considerations!
- AS relationship plays a role, IRR is checked (difficult)

- Accepted independent of AS relationship, high evaluation order (easy)

- May have to modify IRR (involved)
Discussion

● Have we gone too far with BGP communities? Propagate **only** communities to the peer, o.w. there is a risk of a global effect

● Need for BGP communities **authentication**

● Be aware of **standardized** BGP communities

● Need for proper BGP communities **documentation**

● **Monitor** the hygiene and propagation of BGP communities usage
Conclusion

● BGP communities is on the rise and provide a unique, yet unexplored source of information about the State and Health of the Internet

● BGP communities are increasingly popular to cope with complex operational tasks

● We showcase:

  - How to use BGP communities to detect peering infrastructure outages and assess their impact

  - How to use BGP communities as a proxy to infer attacks and mitigation strategies

  - Assess vulnerabilities due to the abuse of BGP communities abuse
Thank you!

Published papers supported by ERC StG ResolutioNet:

“Detecting Peering Infrastructure Outages in the Wild”, ACM SIGCOMM 2017

“Inferring BGP Blackholing Activity in the Internet”, ACM IMC 2017

“BGP Communities: Even More Worms in the Routing Can”, ACM IMC 2018