BGP Blackjack Attacks

Cristel Pelsser

RESSI, December 2020

University of Strasbourg

Related publications

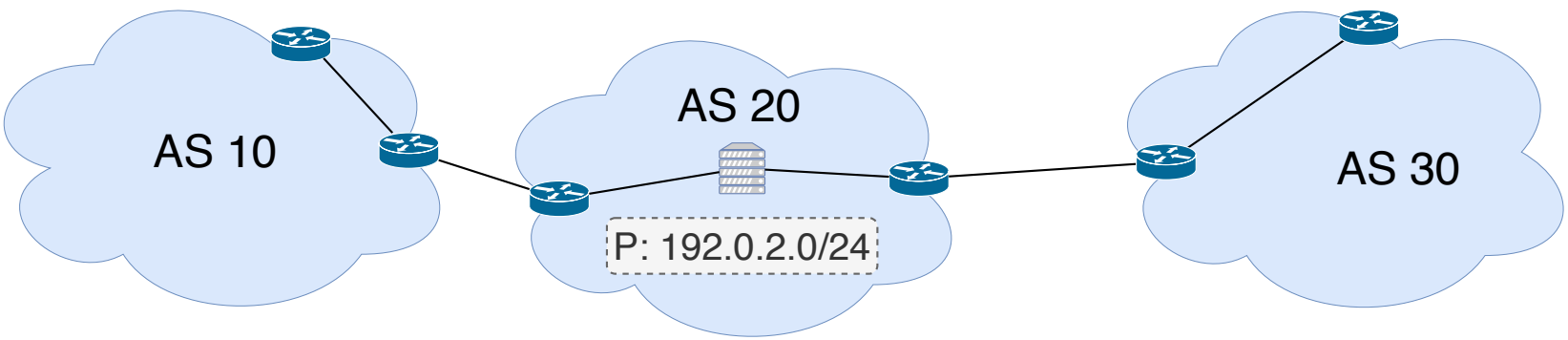
Taxonomy of Attacks using BGP Blackholing.
Loic Miller (U. Strasbourg), Cristel Pelsser (U. Strasbourg).
ESORICS 2019.

BGP Communities: Even more Worms in the Routing Can.
Florian Streibelt (MPI[1]), Franziska Lichtblau (MPI), Robert Beverly (NPS[2]), Anja Feldmann (MPI), Cristel Pelsser (U. Strasbourg), Georgios Smaragdakis (TU Berlin), Randy Bush (IIJ[3]).
ACM IMC 2018.

[1]Max Planck Institute for Informatics
[2]Naval Postgraduate School
[3]Internet Initiative Japan

BGP

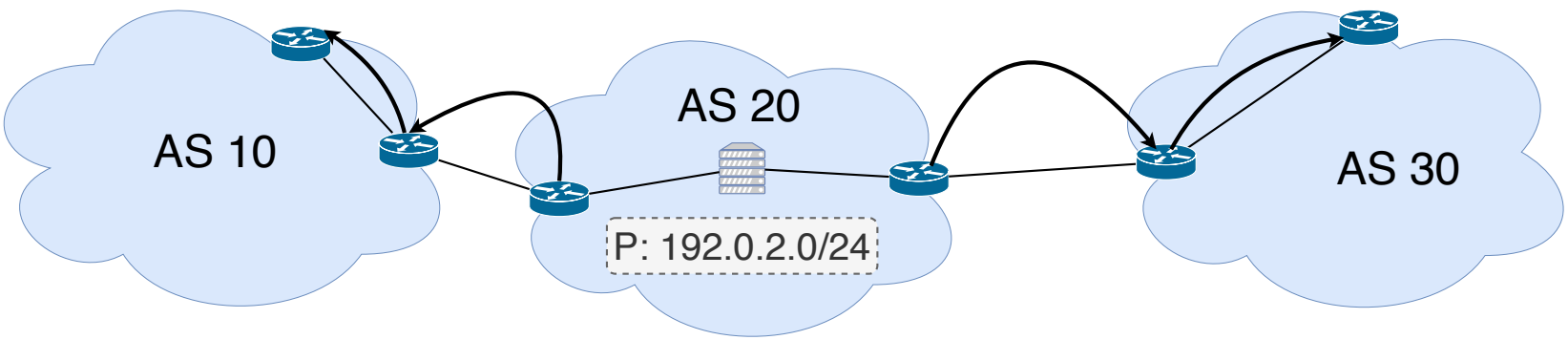
Internet is composed of **Autonomous Systems** (AS): one or more networks under the control of a single entity.



BGP

Internet is composed of **Autonomous Systems** (AS): one or more networks under the control of a single entity.

Prefixes of the AS are advertised to the outside using BGP.

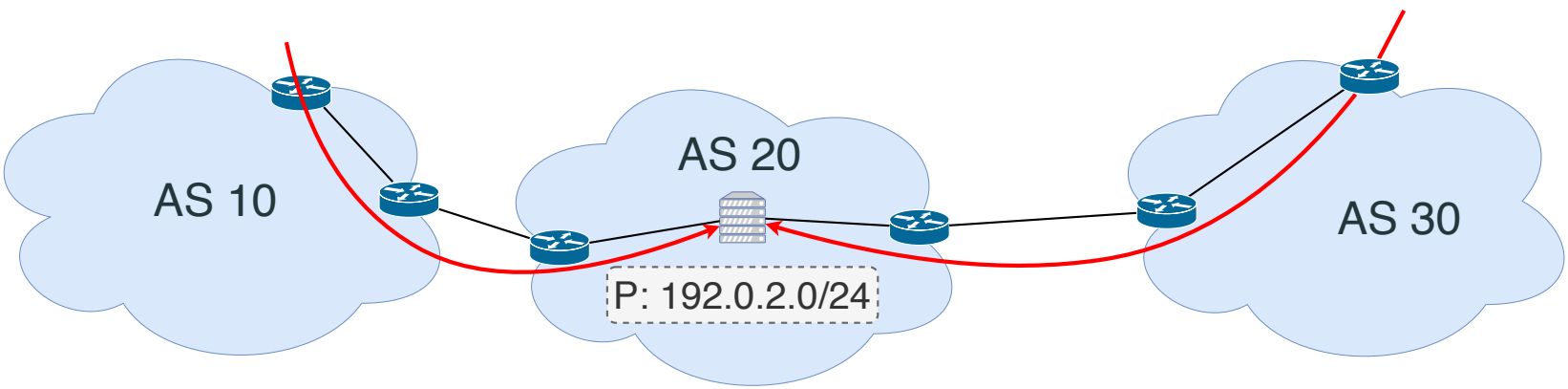


BGP

Internet is composed of **Autonomous Systems** (AS): one or more networks under the control of a single entity.

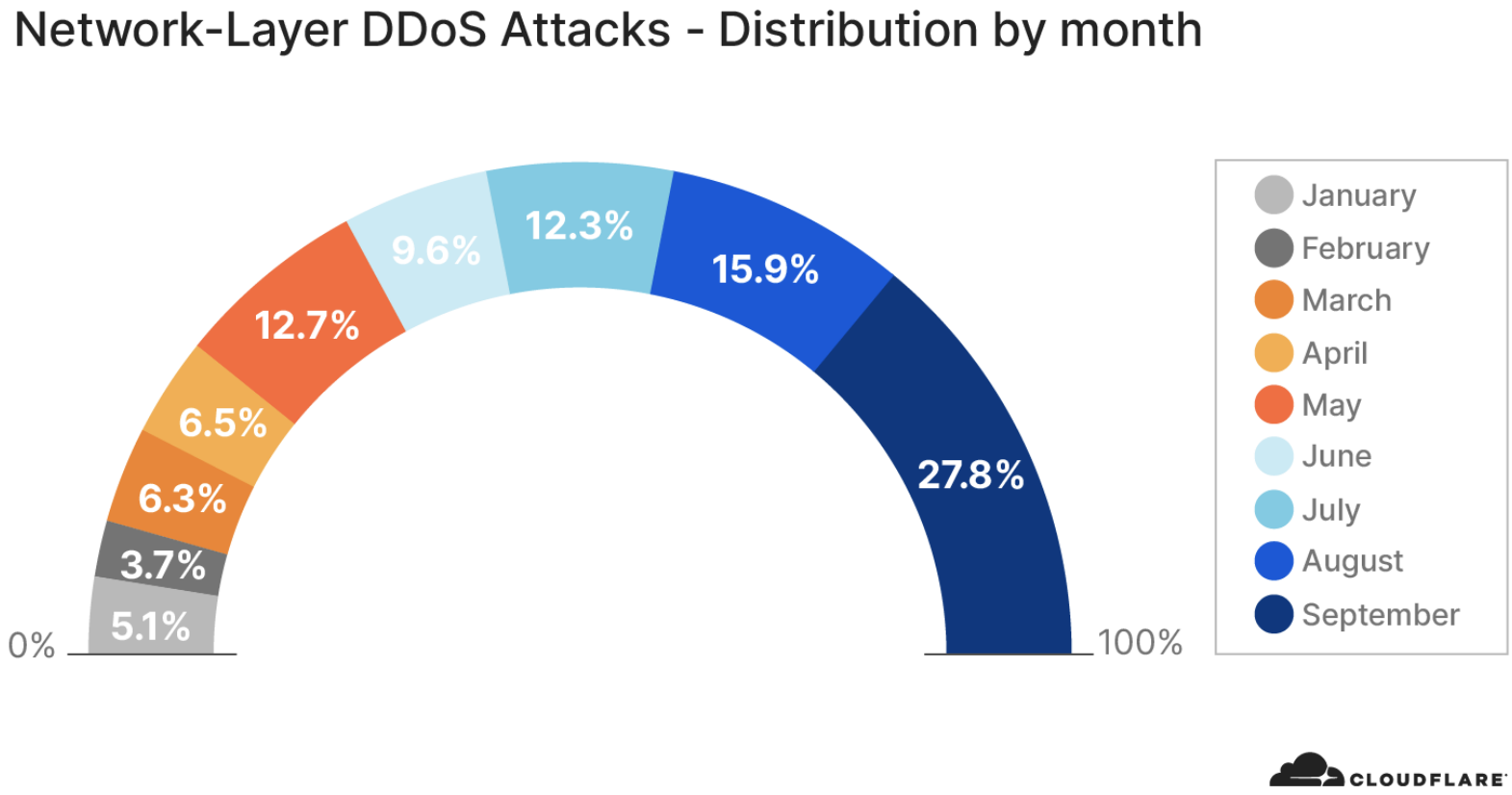
Prefixes of the AS are advertised to the outside using BGP.

Traffic flows in the reverse direction.



DDoS are frequent

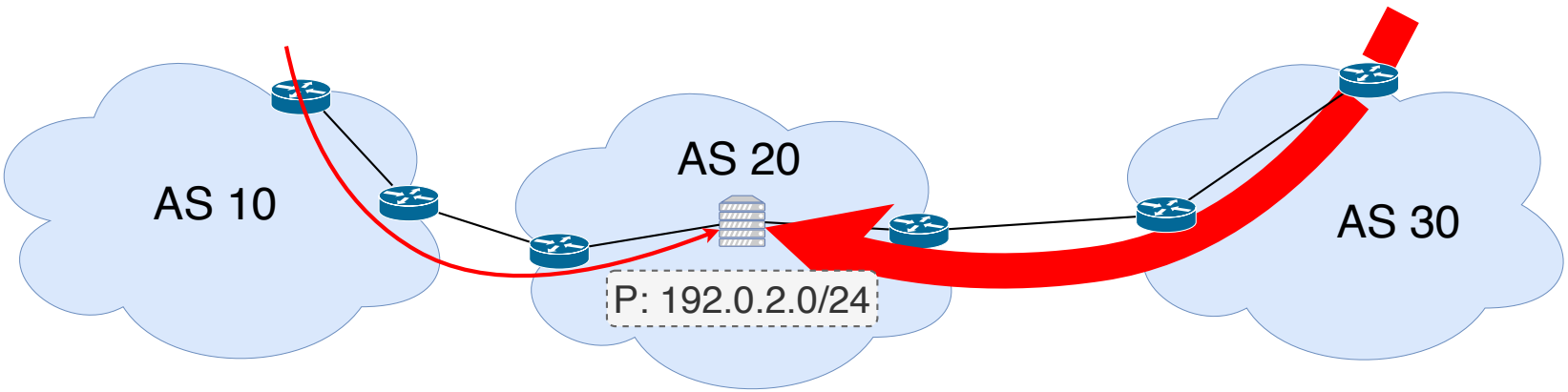
For examples Cloudflare reports that the number of DDoS quadrupled compared to pre-covid levels



Source: `https://blog.cloudflare.com/network-layer-ddos-attack-trends-for-q3-2020/`

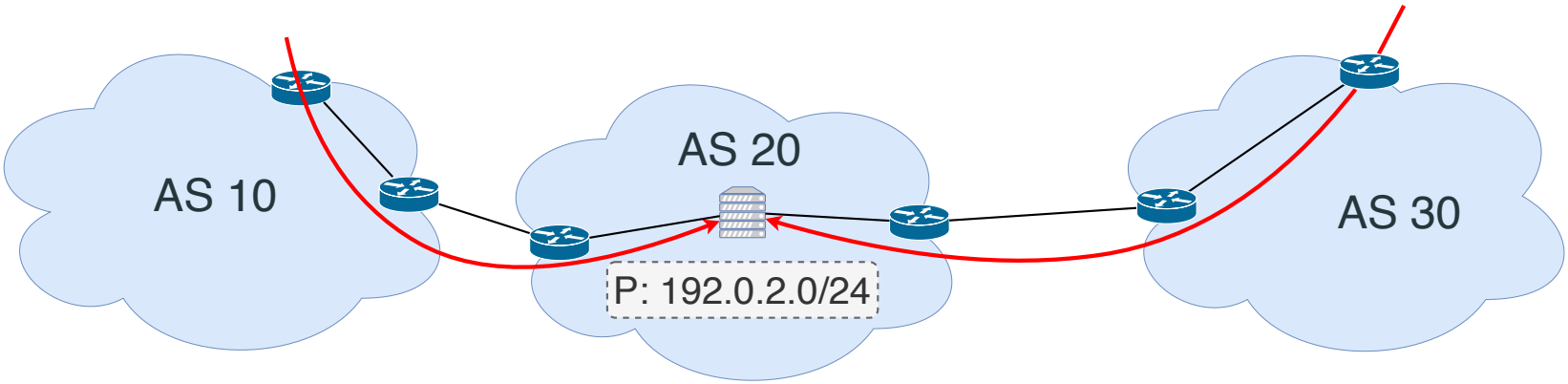
DDoS

In a denial of service attack, the infractucture may be congested.



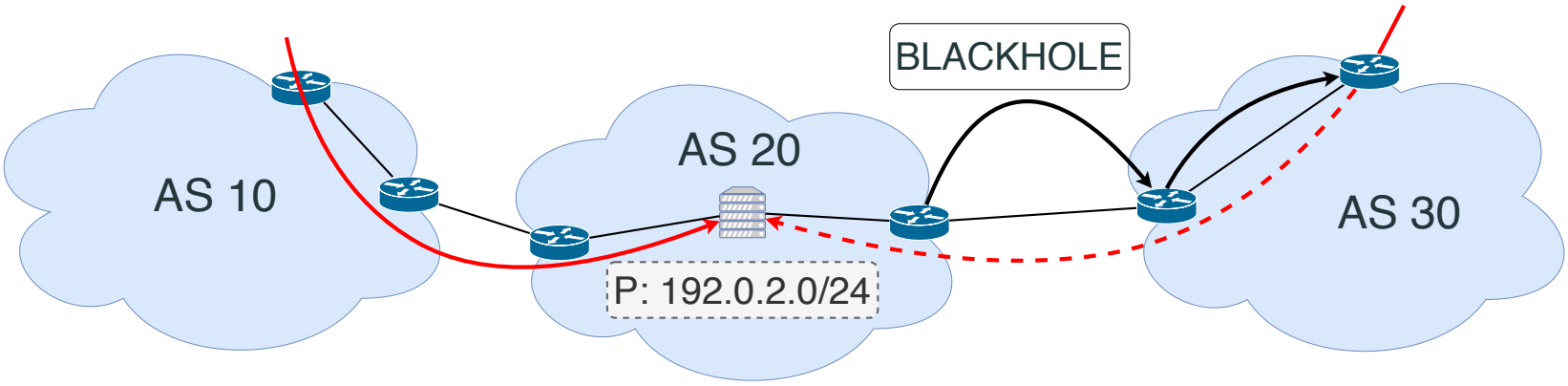
BGP Blackholing

Blackholing is a **DDoS mitigation** technique signaled via **BGP**.



BGP Blackholing

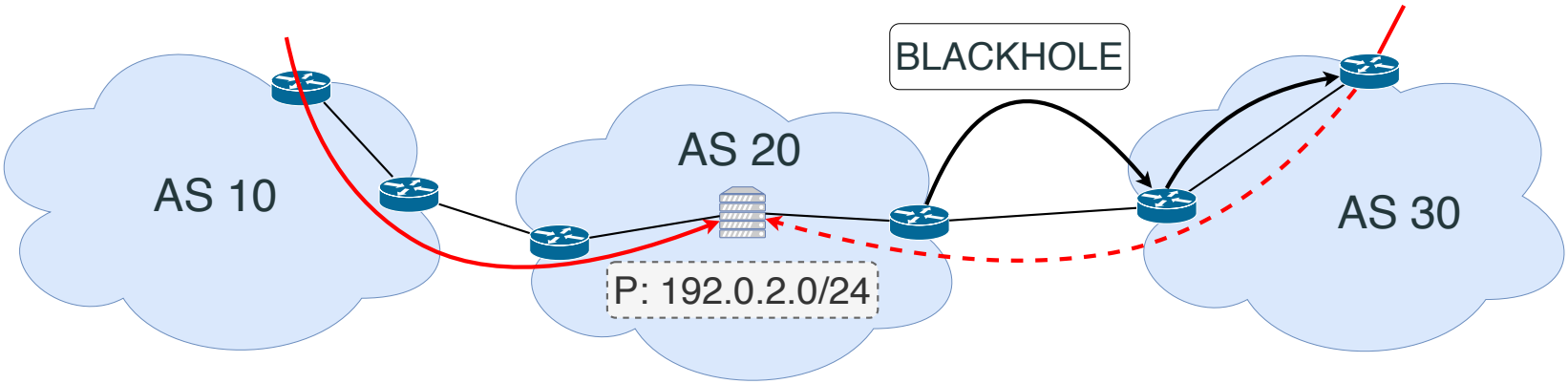
Blackholing is a **DDoS mitigation** technique signaled via **BGP**.



Blackholing has a double-edged sword effect: **all** traffic is dropped.

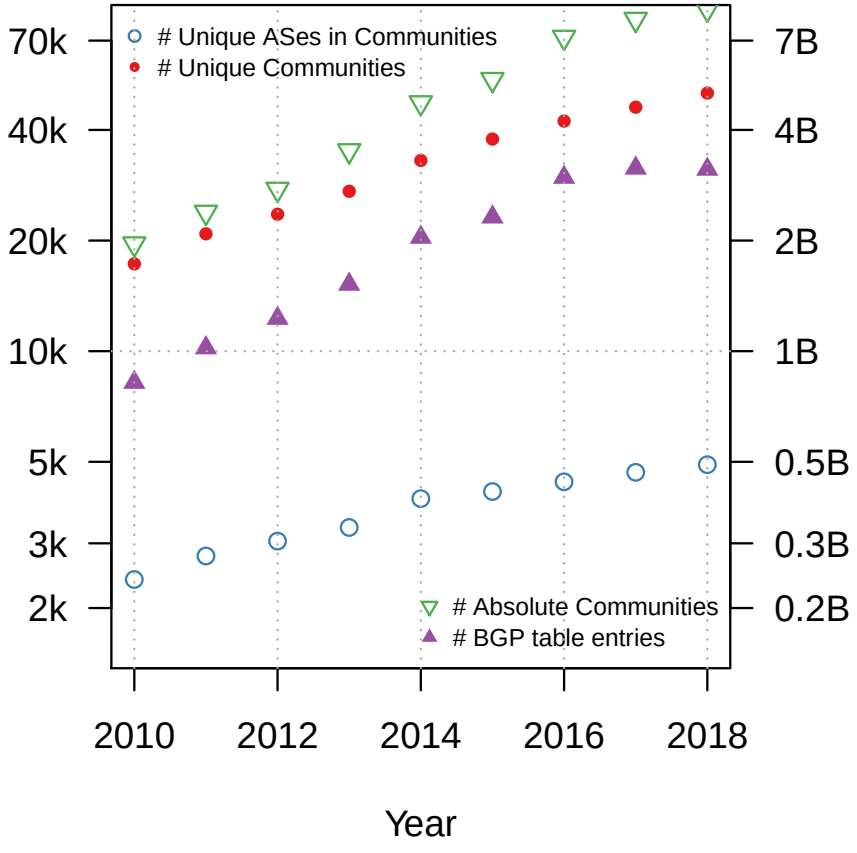
BGP Blackholing

Blackholing is a **DDoS mitigation** technique signaled via **BGP**.



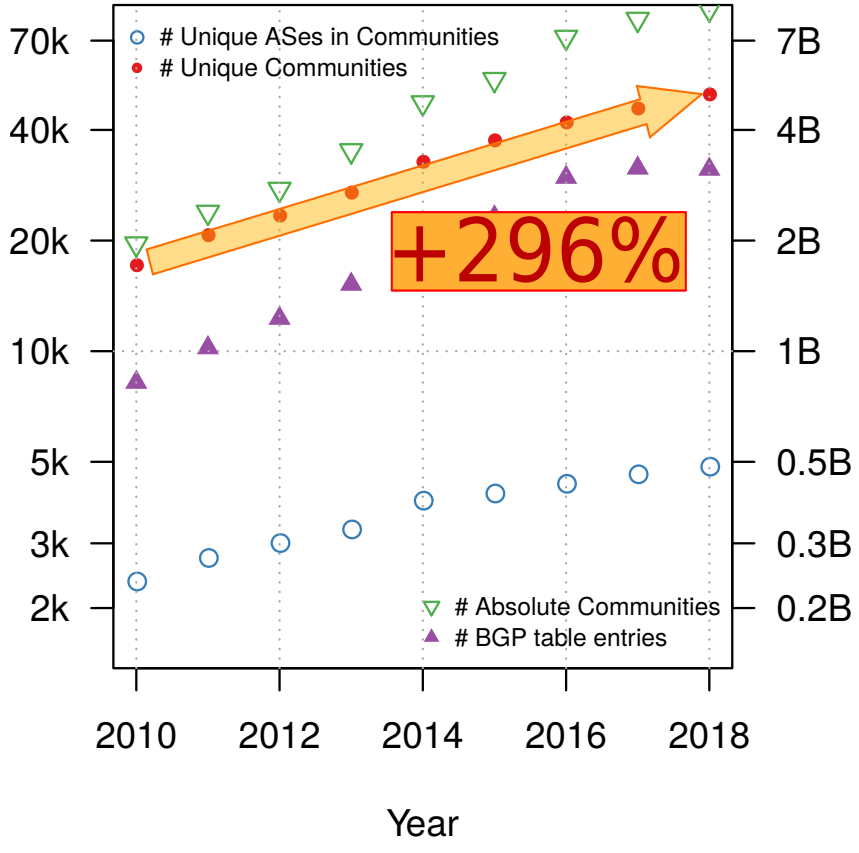
Blackholing is announced via what is called a BGP community.

BGP Community usage is increasing



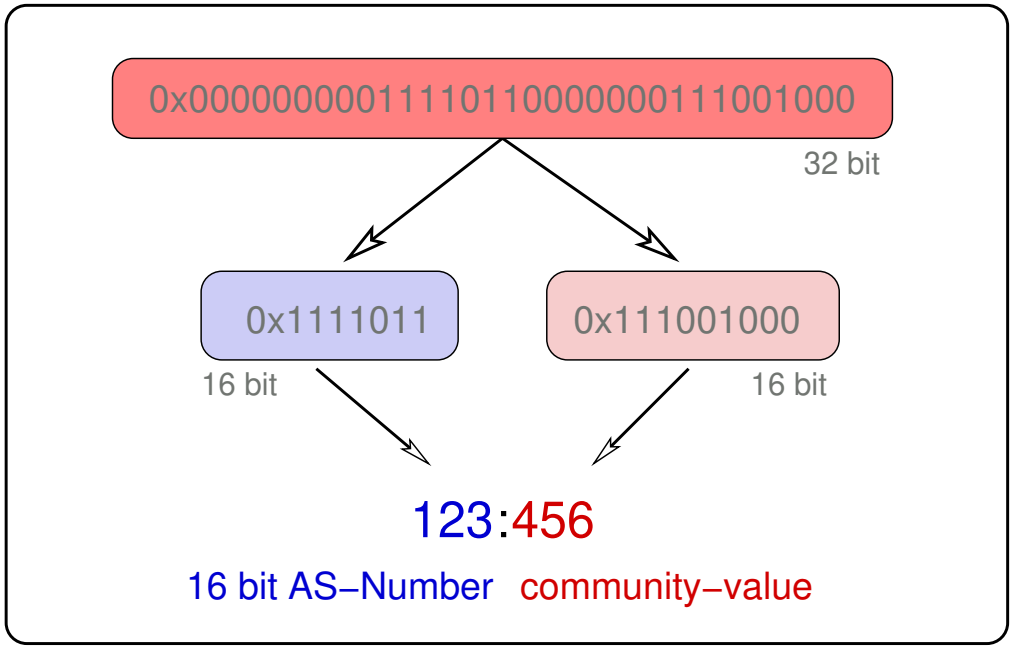
Increasing usage warrants a closer look.

BGP Community usage is increasing



Increasing usage warrants a closer look.

BGP Communities (RFC 1997)



By convention written *ASN:VALUE*

ASN can be both sender or intended 'recipient'

It's up to the peers to agree upon 'values' used

Every network decides on the semantics of values

BGP Communities: Usage (examples)

Informational Communities (Passive Semantics)
Location tagging
RTT tagging

Action Communities (Active Semantics)
Remote triggered blackholing
Path prepending
Local pref/MED
Selective announcements

Without documentation, you can not tell if a community is active or passive!

Blackhole community value is :666 (RFC 7999)

What This Talk Is About

Given the **increasing popularity** of BGP communities
and the ability to **trigger actions** as well as **relay information**,
the first question that comes to the mind of an
Internet measurement researcher is. . .

What This Talk Is About

What could possibly go wrong?

Objectives

Objectives

Can blackholing be used with malicious intent?

Objectives

Can blackholing be used with malicious intent?

Are there different types of attacks?

Objectives

Can blackholing be used with malicious intent?

Are there different types of attacks?

Are there any existing and relevant security mechanisms?

Objectives

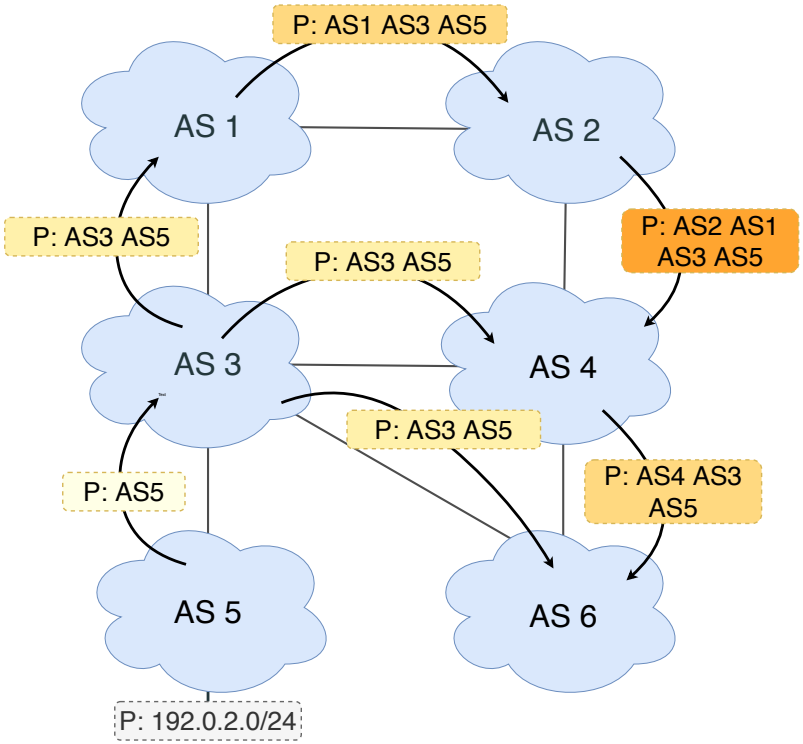
Can blackholing be used with malicious intent?

Are there different types of attacks?

Are there any existing and relevant security mechanisms?Are these mechanisms enough?

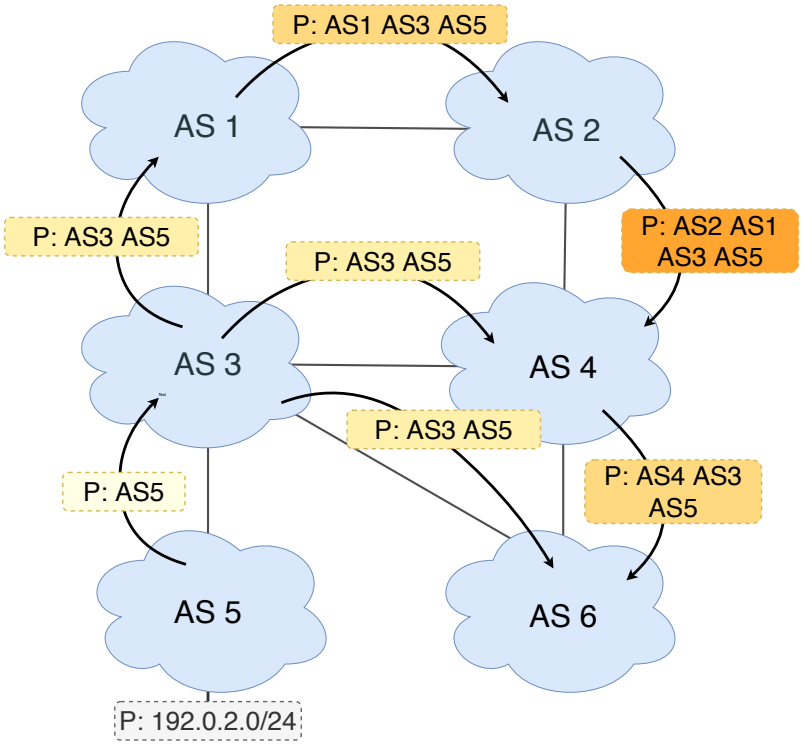
While the focus is on blackholing, malicious route manipulation may take place with other types of communities.

Example topology

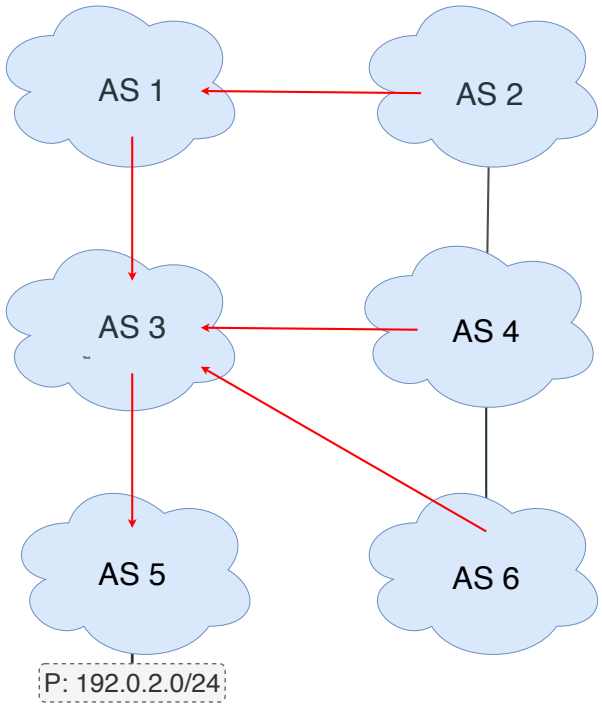


BGP update propagation

Example topology

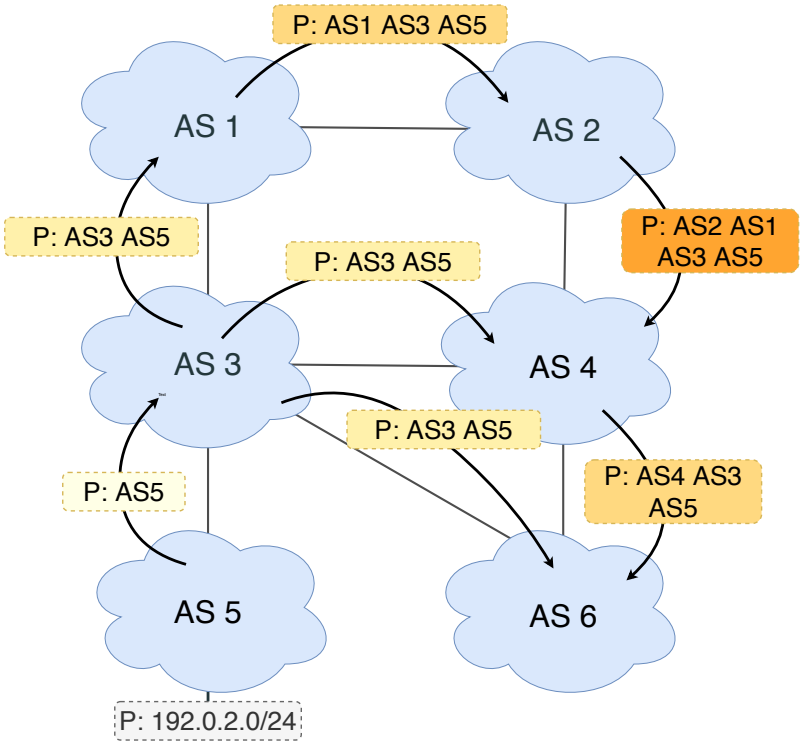


BGP update propagation

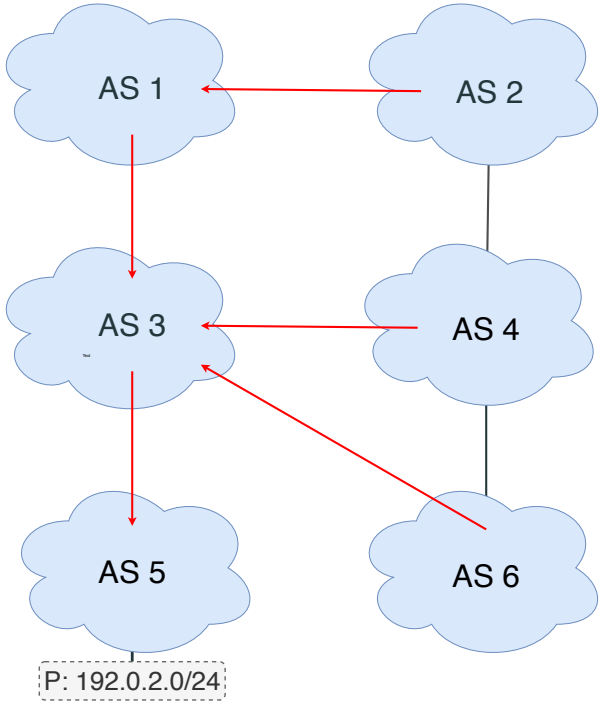


Traffic flow

Example topology



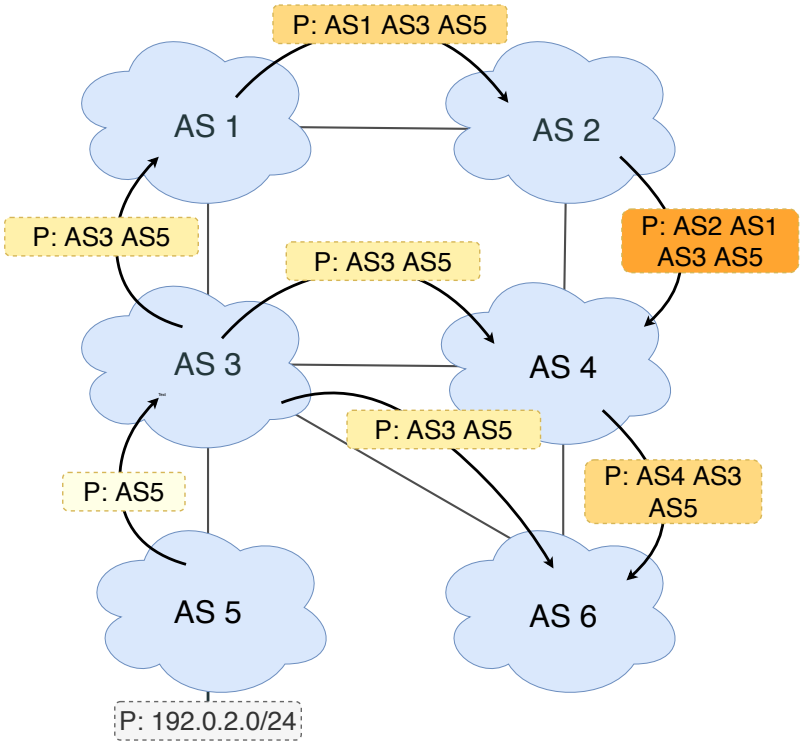
BGP update propagation



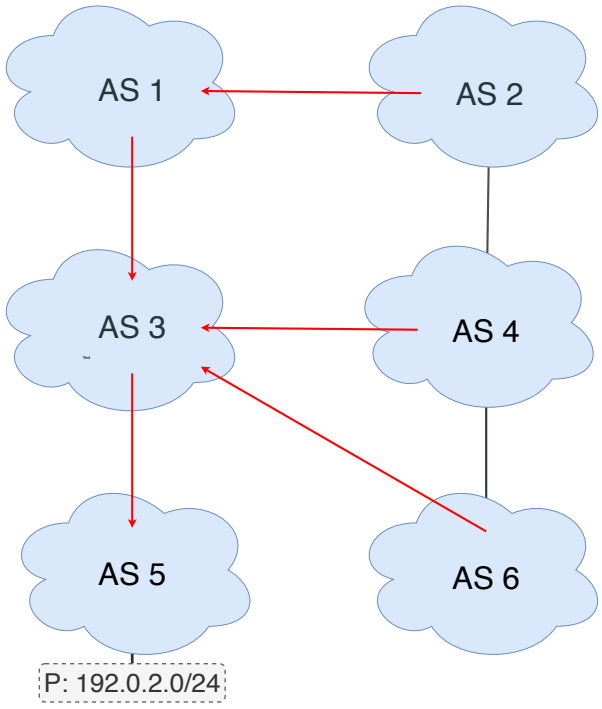
Traffic flow

BGP policies make AS2 not learn the path via AS4

Example topology



BGP update propagation

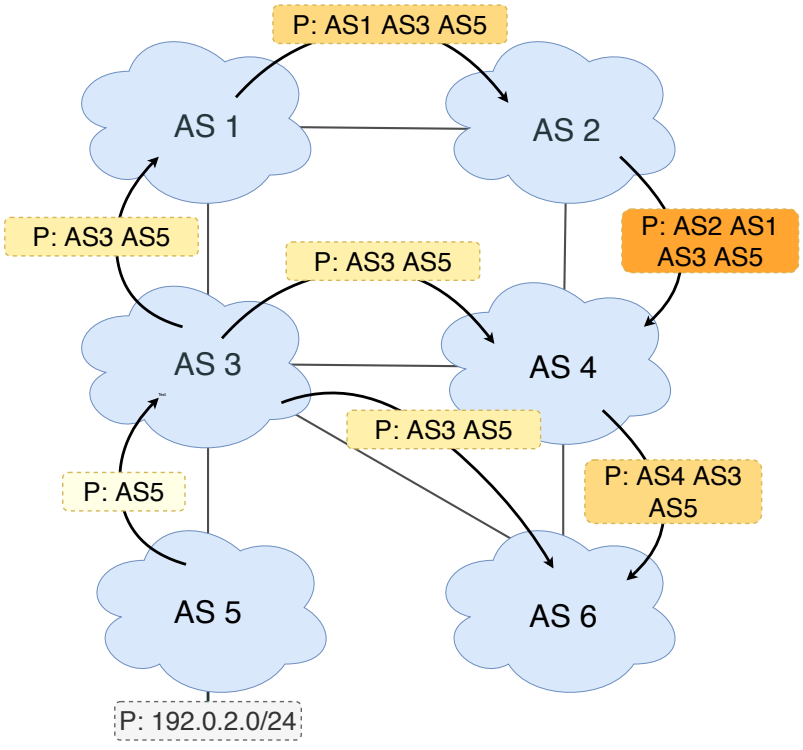


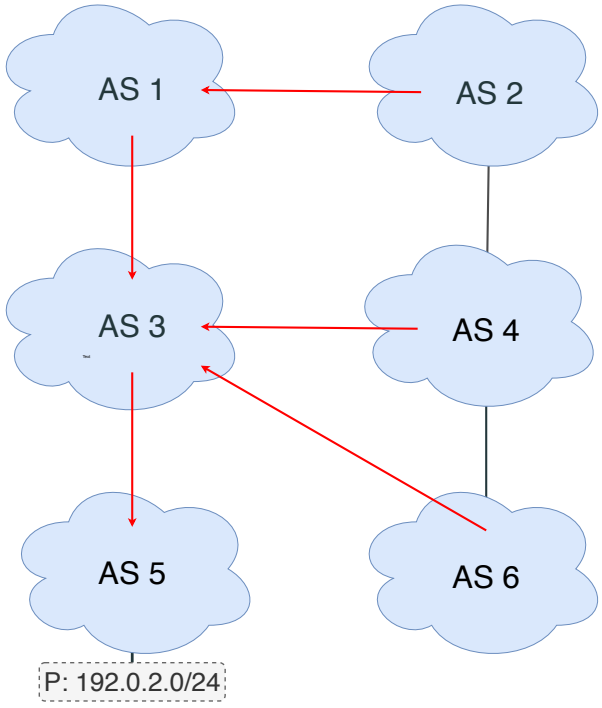
Traffic flow

BGP policies make AS2 not learn the path via AS4

BGP policies are distributed in the AS using BGP communities

Example topology





BGP update propagation **Traffic flow**

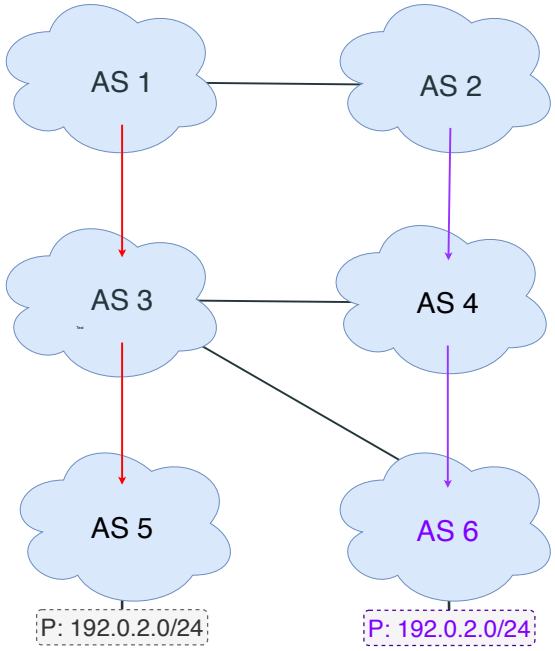
BGP policies make AS2 not learn the path via AS4

BGP policies are distributed in the AS using BGP communities

In the next slides AS6 is the attacker

Hijack-0 and Blackjack-0

Sermpezis 2018 (Artemis)

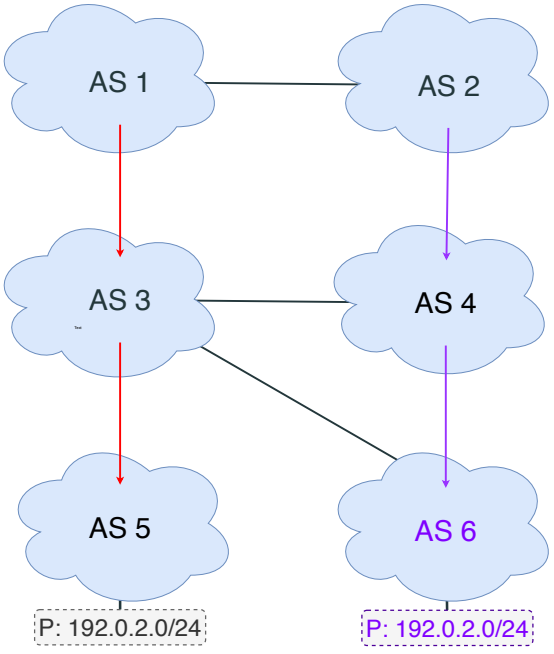


Hijack type-0

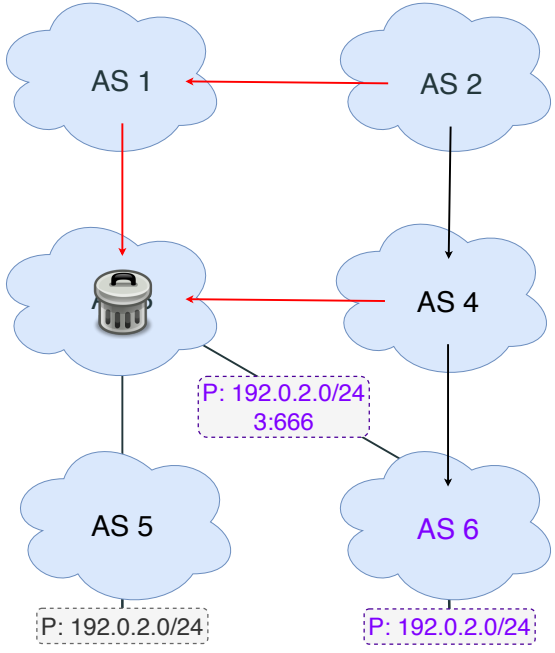
AS2 and AS4 traffic is de-routed to AS6 because the advertised path is shorter.

Hijack-0 and Blackjack-0

Sermpezis 2018 (Artemis)



Miller et Pelsser 2019



Hijack type-0

AS2 and AS4 traffic is de-routed to AS6 because the advertised path is shorter.

Blackjack type-0

All traffic to P is blackholed at AS3.

Hijacking + blackholing

Best practices for legitimate blackholing empower blackjacks

Best Practices for blackholing[4]

Give a **higher priority** to blackholing.

Do **not propagate** the advertisement across AS borders.

[4] Cisco, **Remotely Triggered Black Hole Filtering - Destination Based and Source Based**.

Best practices for legitimate blackholing empower blackjacks

Best Practices for blackholing[4]

Give a **higher priority** to blackholing.

Do **not propagate** the advertisement across AS borders.

Consequences

Reach: Precedence over AS path length. Even ASes far away are vulnerable.

Stealth: The attacker is not dropping traffic himself.

---

[4] Cisco, **Remotely Triggered Black Hole Filtering - Destination Based and Source Based**.

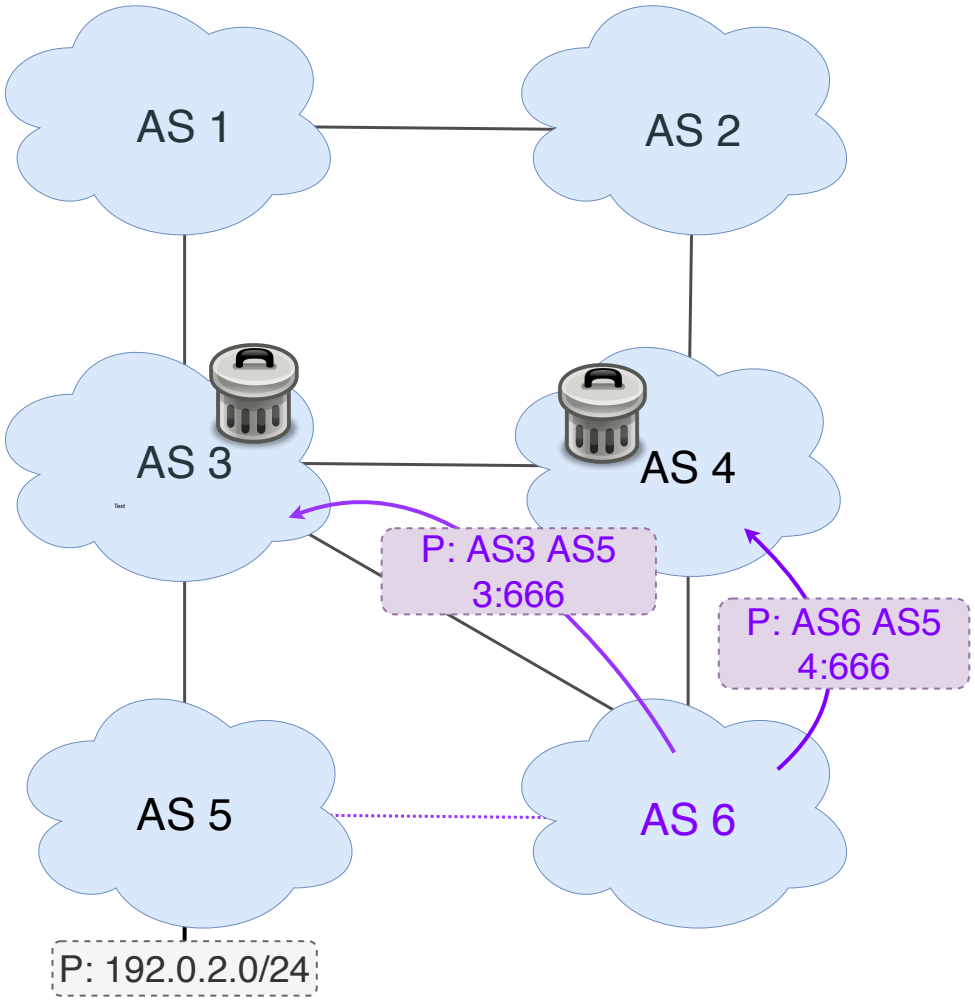
RPKI ROA and ROV provide some protection against hijacks

ROA Route Origin Authorizations are digitally signed objects attesting that a given AS is **authorized to originate** routes for a set of prefixes.

ROV With Route Origin validation, an AS **validates the origin** of the BGP updates with regard to the content of the RPKI Objects.

But other attacks are possible.

BGP Blackjacks - Type-N



The origin AS is legit. The AS-path is not.

BGPsec[5]

BGPsec allow ASes to **sign** advertisements.

This guarantees the AS path reflects the **actual path** the advertisement went through.

But on-paths attacks are still possible.

[5] Lepinski and Sriram, **BGPsec Protocol Specification**.

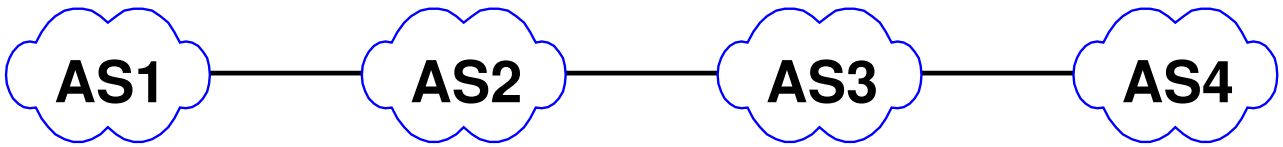
Experimental validation

How far do BGP communities propagate?

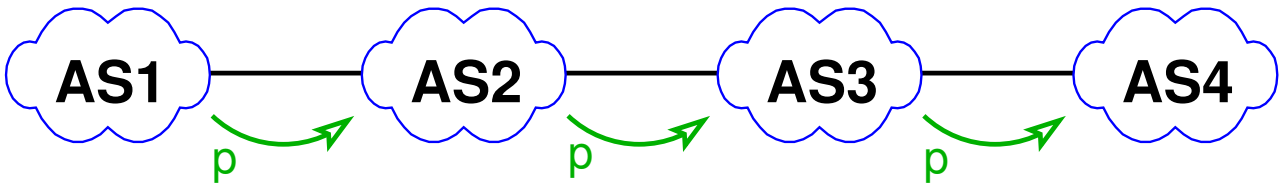
Feasability of the attacks in a lab and in the wild.

BGP Communities propagation

BGP Communities propagation

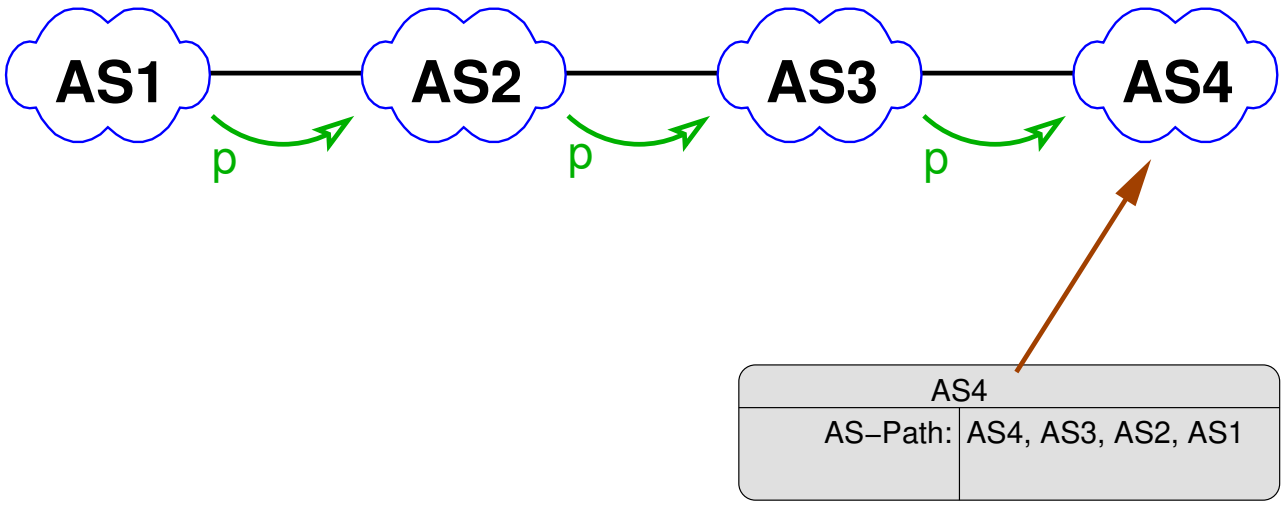


BGP Communities propagation



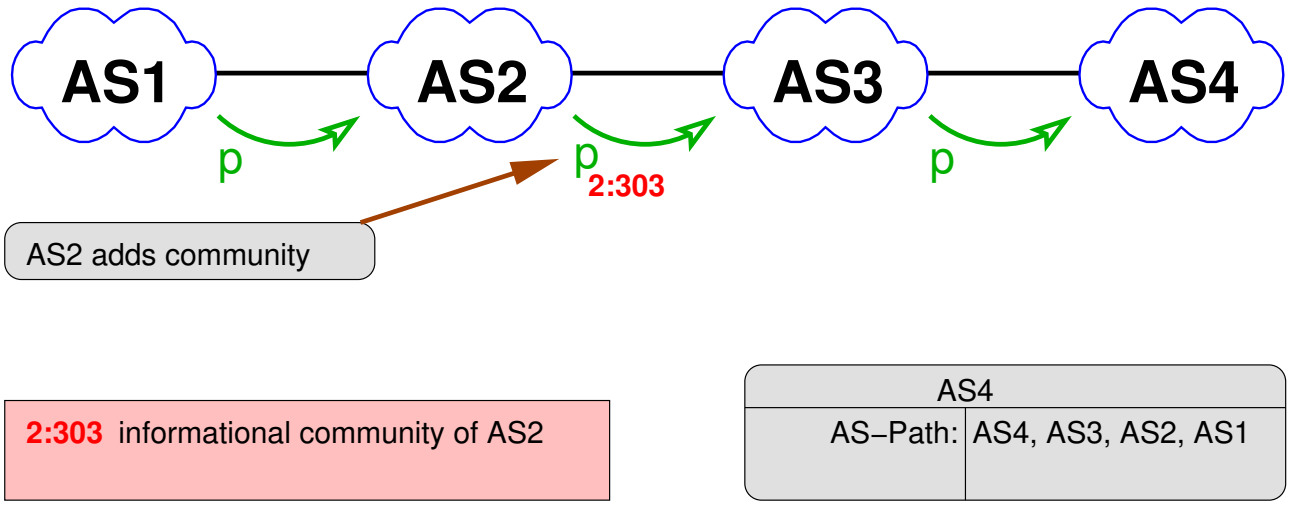
AS1 announces prefix p

BGP Communities propagation



AS1 announces prefix p, AS4 receives announcement

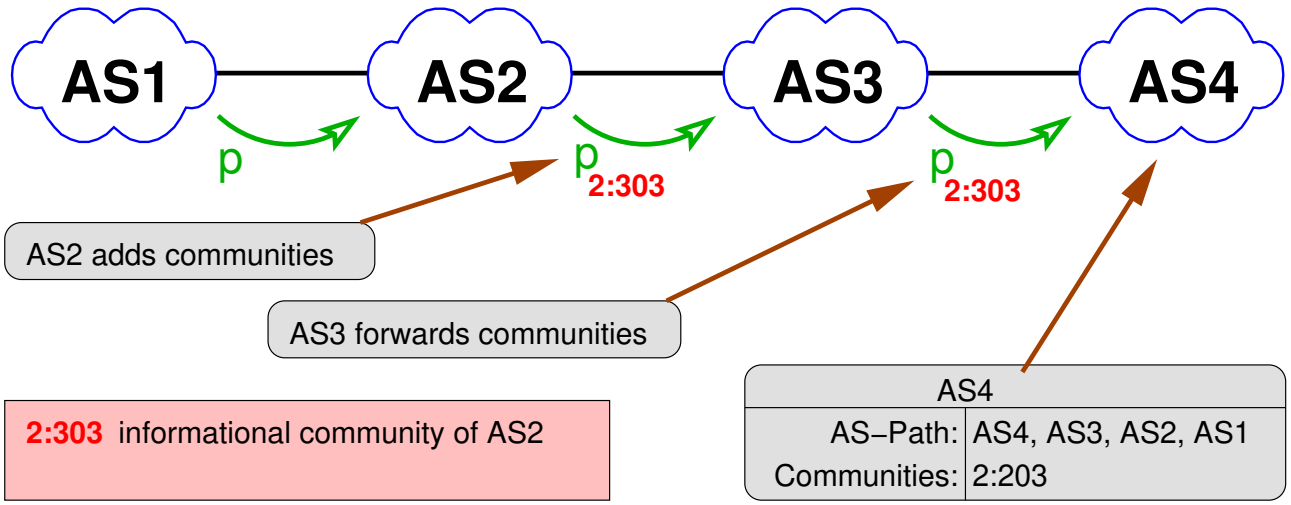
BGP Communities propagation



AS1 announces prefix p, AS4 receives announcement

Informational community *2:303* is added by AS2

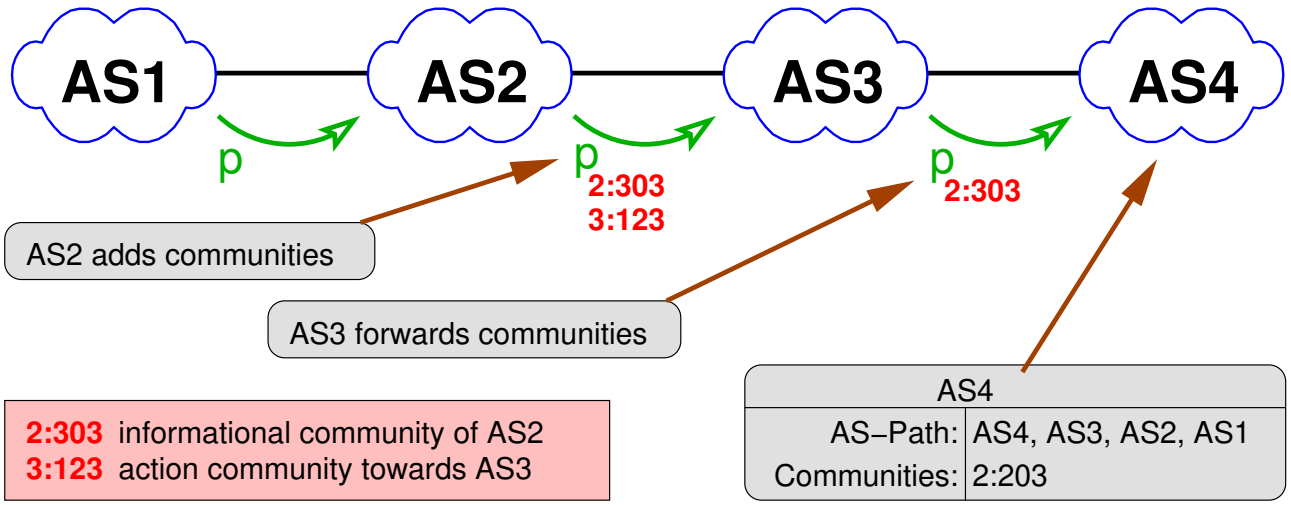
BGP Communities propagation



AS1 announces prefix p, AS4 receives announcement

Informational community *2:303* is added by AS2

BGP Communities propagation

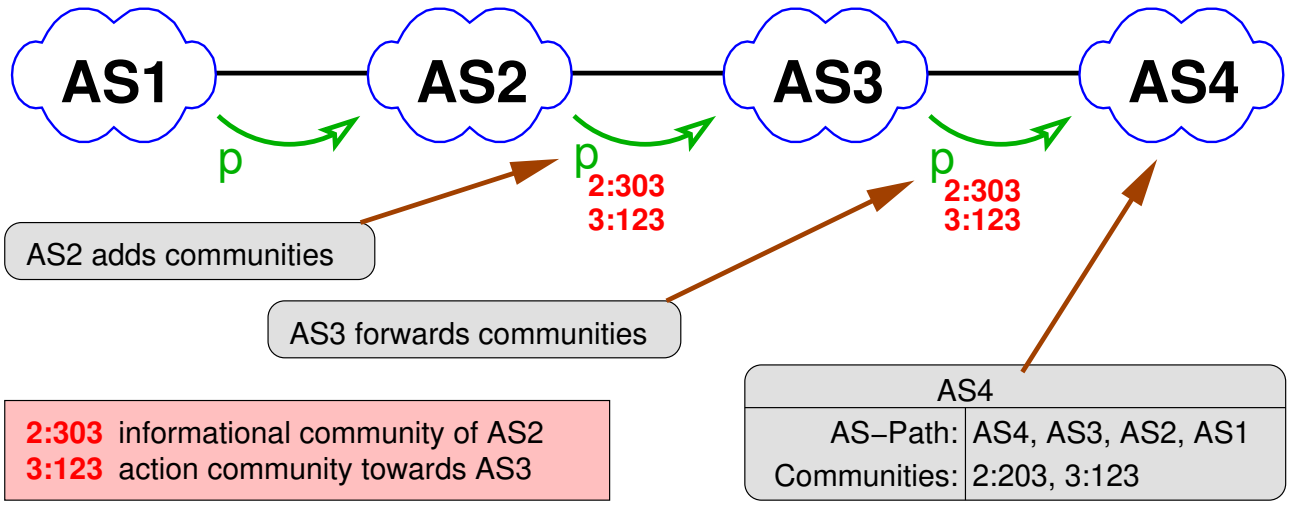


AS1 announces prefix p, AS4 receives announcement

Informational community *2:303* is added by AS2

AS2 also adds action community *3:123* for AS3

BGP Communities propagation



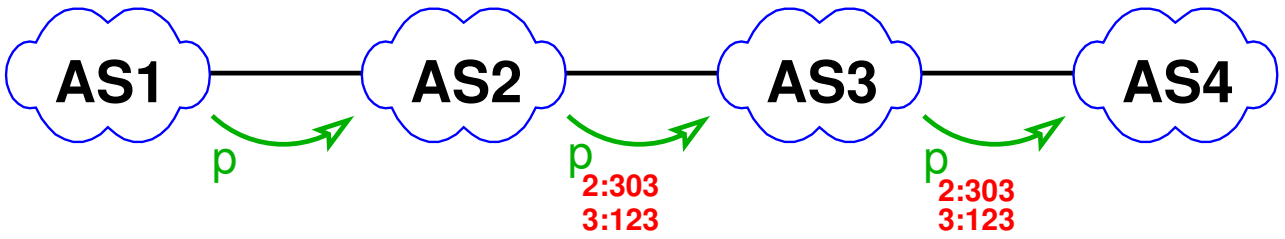
AS1 announces prefix p, AS4 receives announcement

Informational community *2:303* is added by AS2

AS2 also adds action community *3:123* for AS3

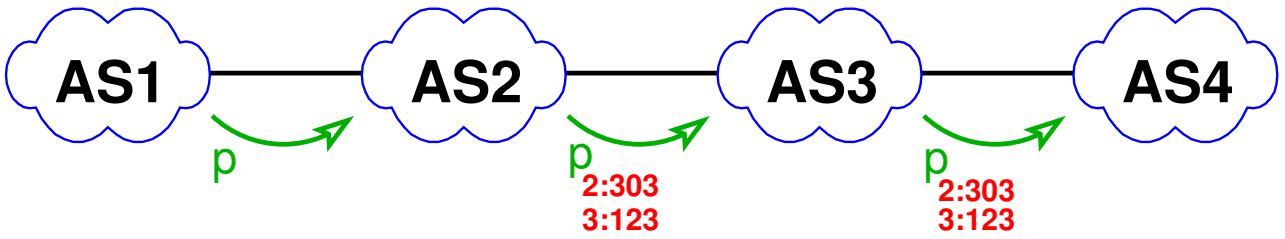
Both communities are forwarded by AS3 to AS4

BGP Communities propagation



AS4	
AS–Path:	AS4, AS3, AS2, AS1
Communities:	2:203, 3:123

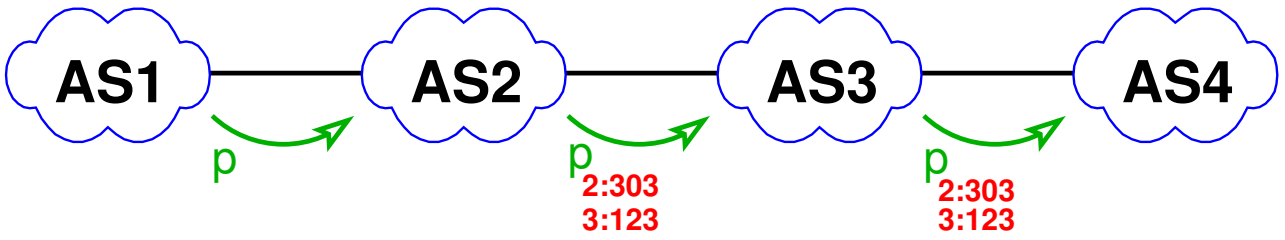
BGP Communities propagation



AS4	
AS–Path:	AS4, AS3, AS2, AS1
Communities:	2:203, 3:123

We can only infer which AS added a specific community

BGP Communities propagation

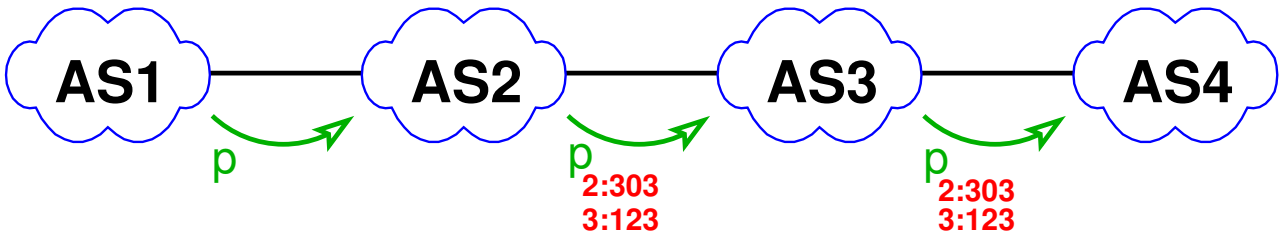


AS4	
AS–Path:	AS4, AS3, AS2, AS1
Communities:	2:203, 3:123

We can only infer which AS added a specific community

We assume that a community *n:value* was added by AS n

BGP Communities propagation



inferred travel–distance is a lower bound!

2:303	traversed at least two AS–links
3:123	traversed at least one AS–link

AS4	
AS–Path:	AS4, AS3, AS2, AS1
Communities:	2:203, 3:123

We can only infer which AS added a specific community

We assume that a community *n:value* was added by AS n

This gives a **lower bound** for the 'travel distance'

In above example we calculate AS-hop-count 1 for *3:123*

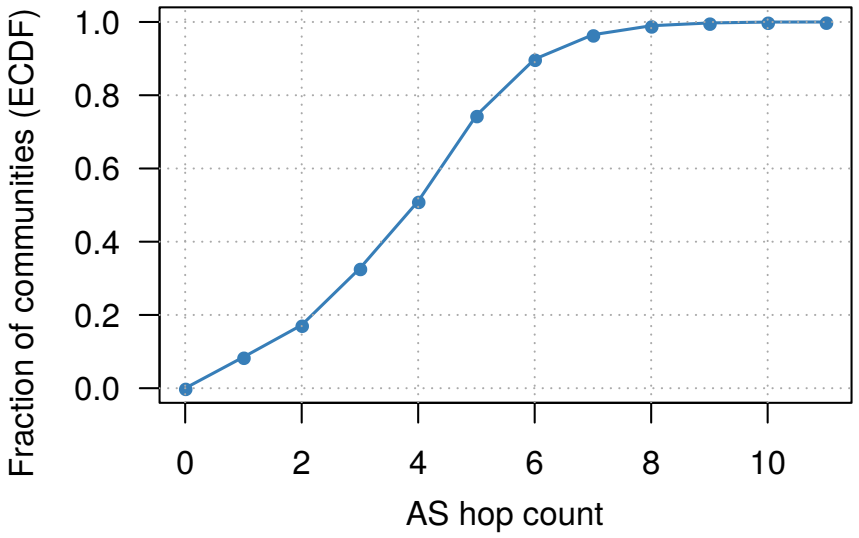
Communities propagate in the wild $\rightarrow$ pre-condition for the attacks is met

BGP updates and table dumps of April 2018 from publicly available BGP Collector Projects: RIPE RIS, Routeviews, Isolario, PCH.

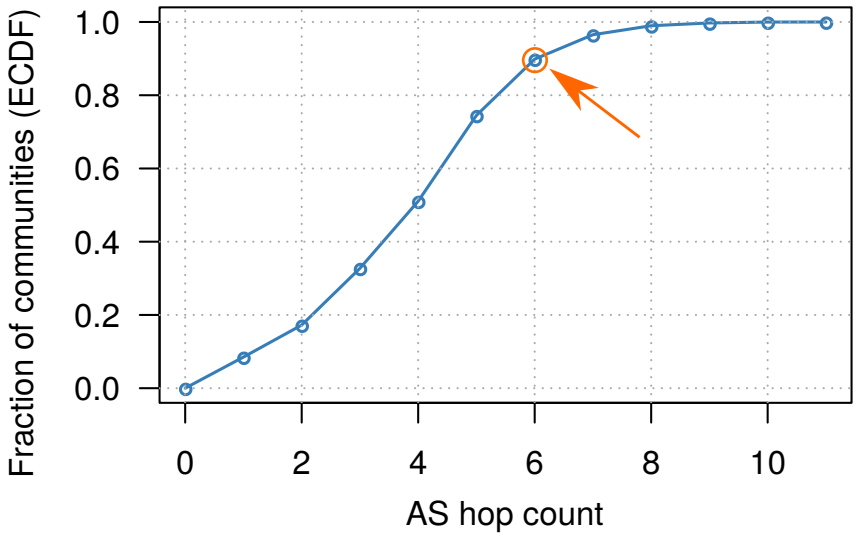
BGP messages	38.98 bn
IPv4 prefixes	967,499
IPv6 prefixes	84,953
Collectors	194
AS peers	2,133
Communities	63,797

More than 75% of BGP announcements have at least one BGP community set, 5,659 ASes are using communities.

BGP Community Propagation Observations

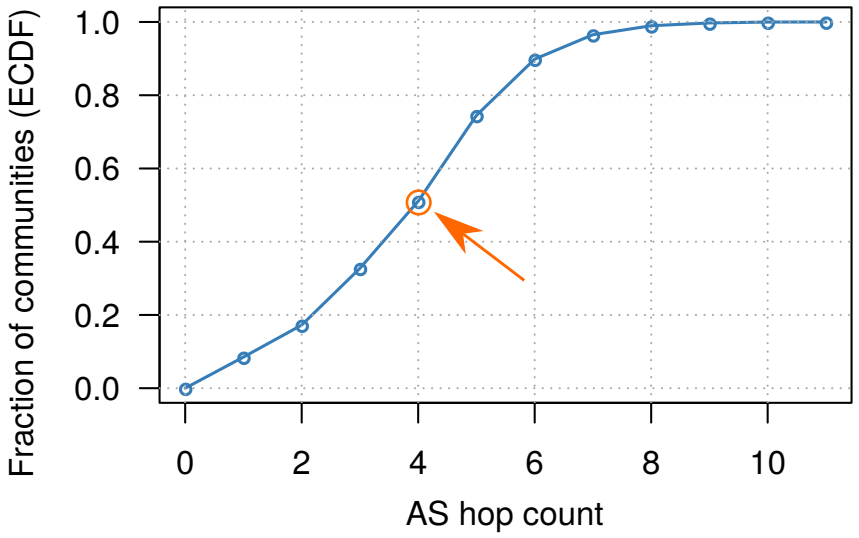


BGP Community Propagation Observations



10% of communities have an AS hop count of more than six

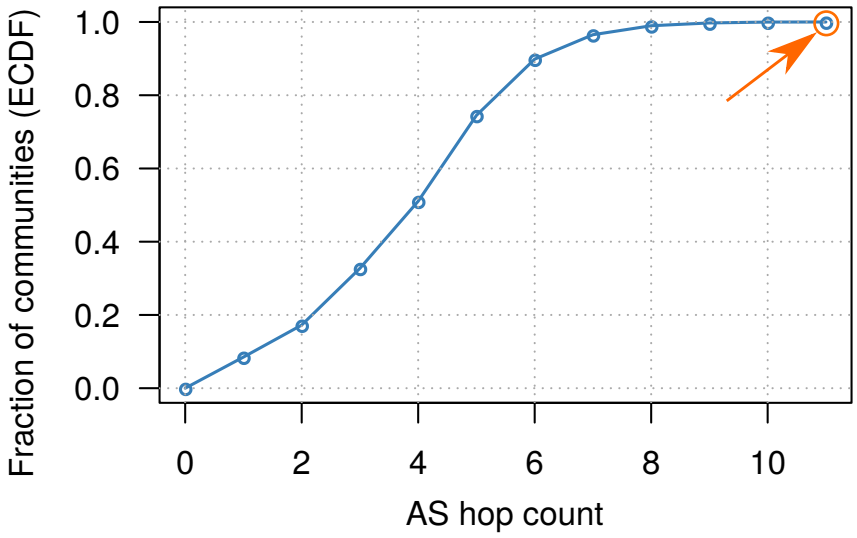
BGP Community Propagation Observations



10% of communities have an AS hop count of more than six

More than 50% of communities traverse more than four ASes

BGP Community Propagation Observations



10% of communities have an AS hop count of more than six

More than 50% of communities traverse more than four ASes

Longest community propagation observed: 11 AS hops

Feasability of the attacks

Blackjack type-0 conducted in a lab environment[6]

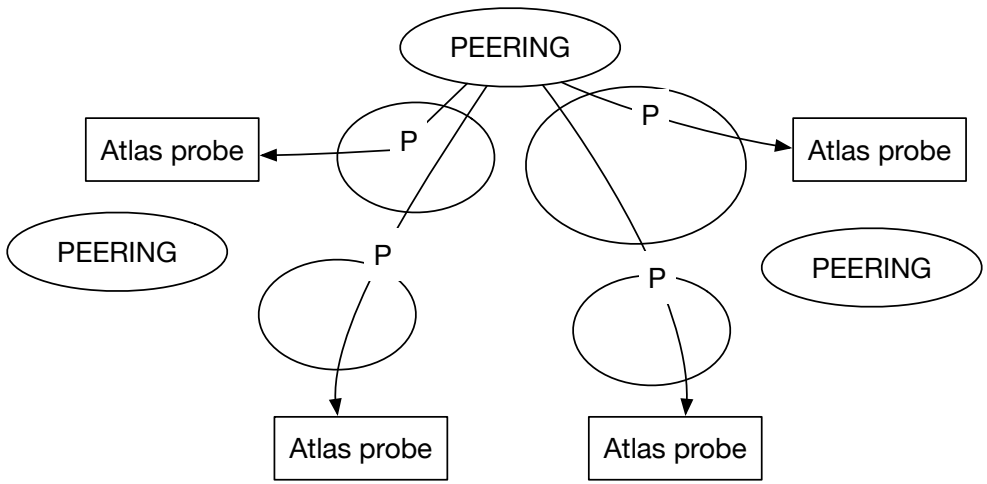
Blackjack type-0 validated on the Internet

[6] Configurations available at: `https://www.cmand.org/caas/`

Attack in the wild using the PEERING testbed

Automated experiment exploring the 307 verified blackhole communities identified Giotsas et al.[7]

1. Announce Prefix lented by operator from one VP

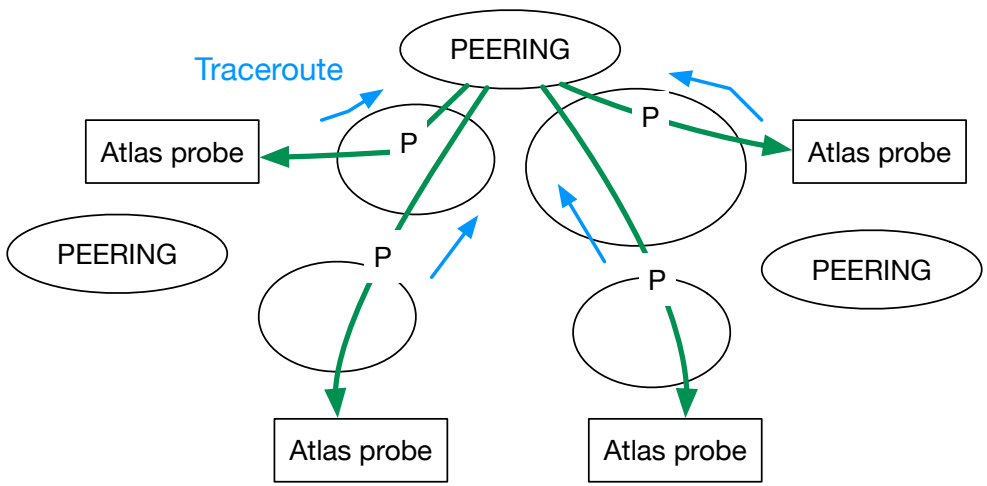


[7] V. Giotsas et al., "Inferring BGP Blackholing Activity in the Internet".

Attack in the wild using the PEERING testbed

Automated experiment exploring the 307 verified blackhole communities identified Giotsas et al.[7]

1. Announce Prefix lented by operator from one VP
2. Check connectivity from 200 RIPE Atlas probes

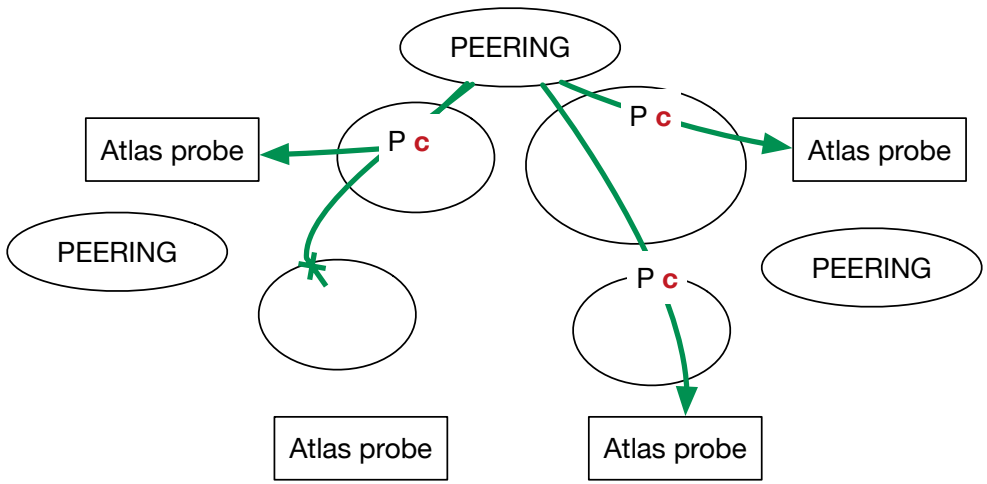


[7] V. Giotsas et al., "Inferring BGP Blackholing Activity in the Internet".

Attack in the wild using the PEERING testbed

Automated experiment exploring the 307 verified blackhole communities identified Giotsas et al.[7]

1. Announce Prefix lented by operator from one VP
2. Check connectivity from 200 RIPE Atlas probes
3. Add community to announce

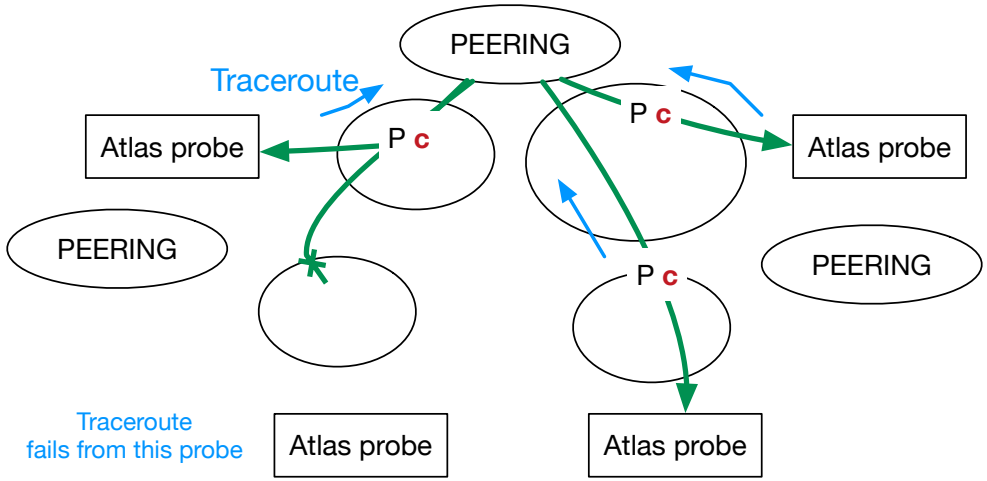


[7] V. Giotsas et al., "Inferring BGP Blackholing Activity in the Internet".

Attack in the wild using the PEERING testbed

Automated experiment exploring the 307 verified blackhole communities identified Giotsas et al.[7]

1. Announce Prefix lented by operator from one VP
2. Check connectivity from 200 RIPE Atlas probes
3. Add community to announce
4. Check connectivity from the 200 RIPE Atlas probes

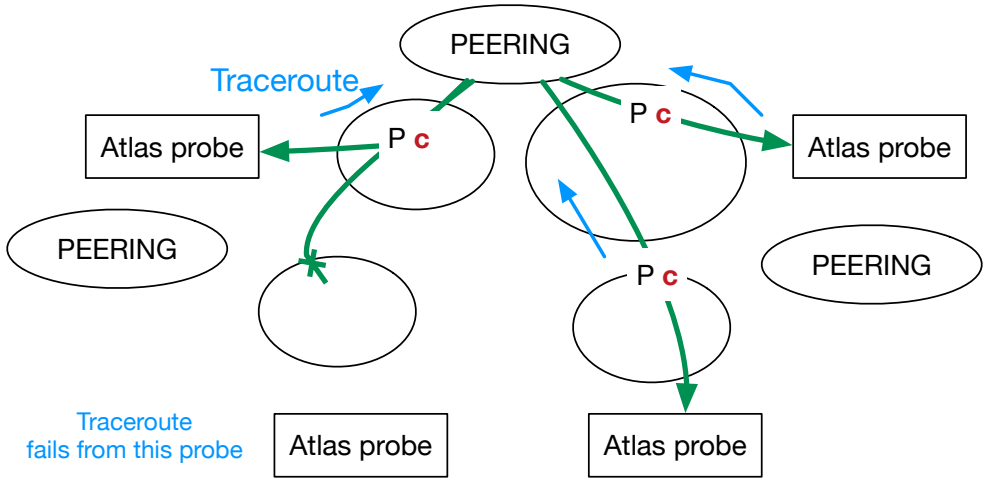


[7] V. Giotsas et al., "Inferring BGP Blackholing Activity in the Internet".

Attack in the wild using the PEERING testbed

Automated experiment exploring the 307 verified blackhole communities identified Giotsas et al.[7]

1. Announce Prefix lented by operator from one VP
2. Check connectivity from 200 RIPE Atlas probes
3. Add community to announce
4. Check connectivity from the 200 RIPE Atlas probes
5. Repeat over communities and VPs



[7] V. Giotsas et al., "Inferring BGP Blackholing Activity in the Internet".

Observations

We find 25 distinct communities (8.1%) that induce at least one vantage point to be fully responsive prior to advertising the community and then unresponsive once c is attached to the advertisement.
These 25 communities affect a total of 48 (24%) of the vantage points.

We presented blackjack attacks relying on the blackholing community

These attacks are possible in the wild

Because there is no authenticity/security in place for communities

Contact

Cristel Pelsser <pelsser@unistra.fr>

Images:

Unicorn illustration: Telegram stickers by Darya Ogneva:
https://tlgrm.eu/stickers/BornToBeAUnicorn