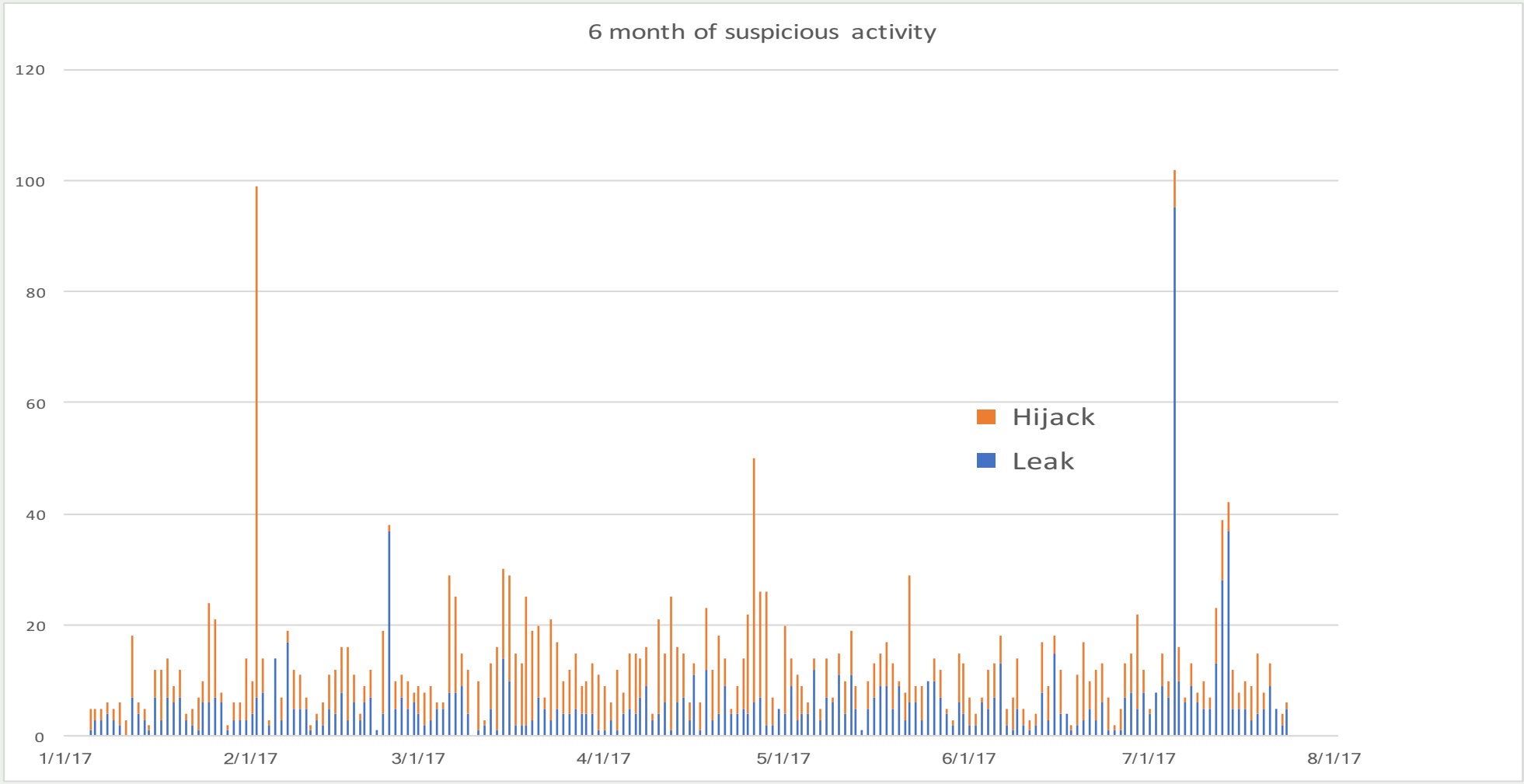
Routing Is At Risk.
Let's Secure It Together

Andrei Robachevsky
robachevsky@isoc.org

No Day Without an Incident



http://bgpstream.com/

A year in review: 14000 incidents

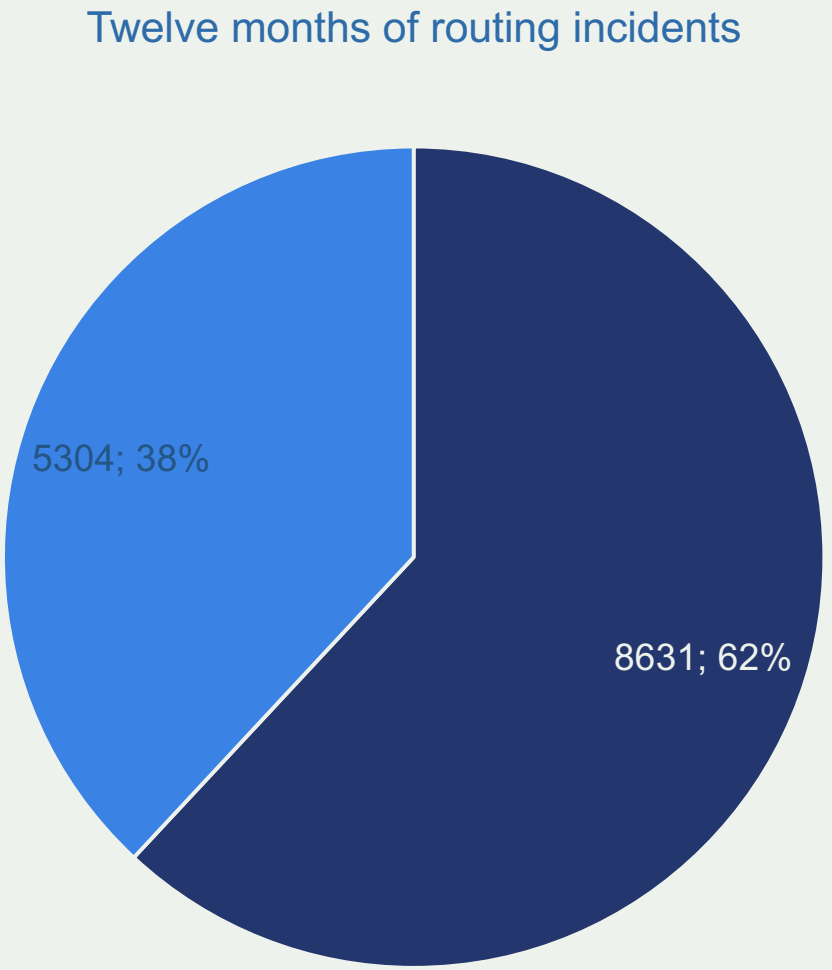
Statistics of routing incidents generated from BGPStream data

Caveats:

- Sometimes it is impossible to distinguish an attack from a legitimate (or consented) routing change
- CC attribution is based on geolocation MaxMind's GeoLite City data set

The routing system is constantly under attack (2017)

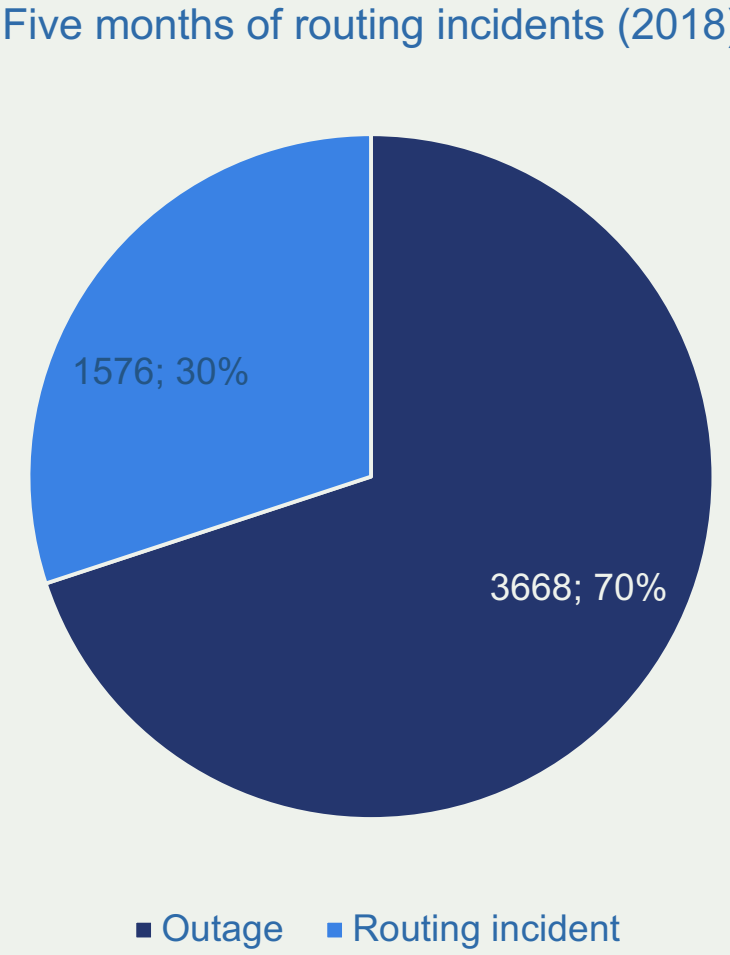
- 13,935 total incidents (either outages or attacks, like route leaks and hijacks)
- Over 10% of all Autonomous Systems on the Internet were affected
- 3,106 Autonomous Systems were a victim of at least one routing incident
- 1,546 networks were responsible for 5304 routing incidents



Source: https://www.bgpstream.com/

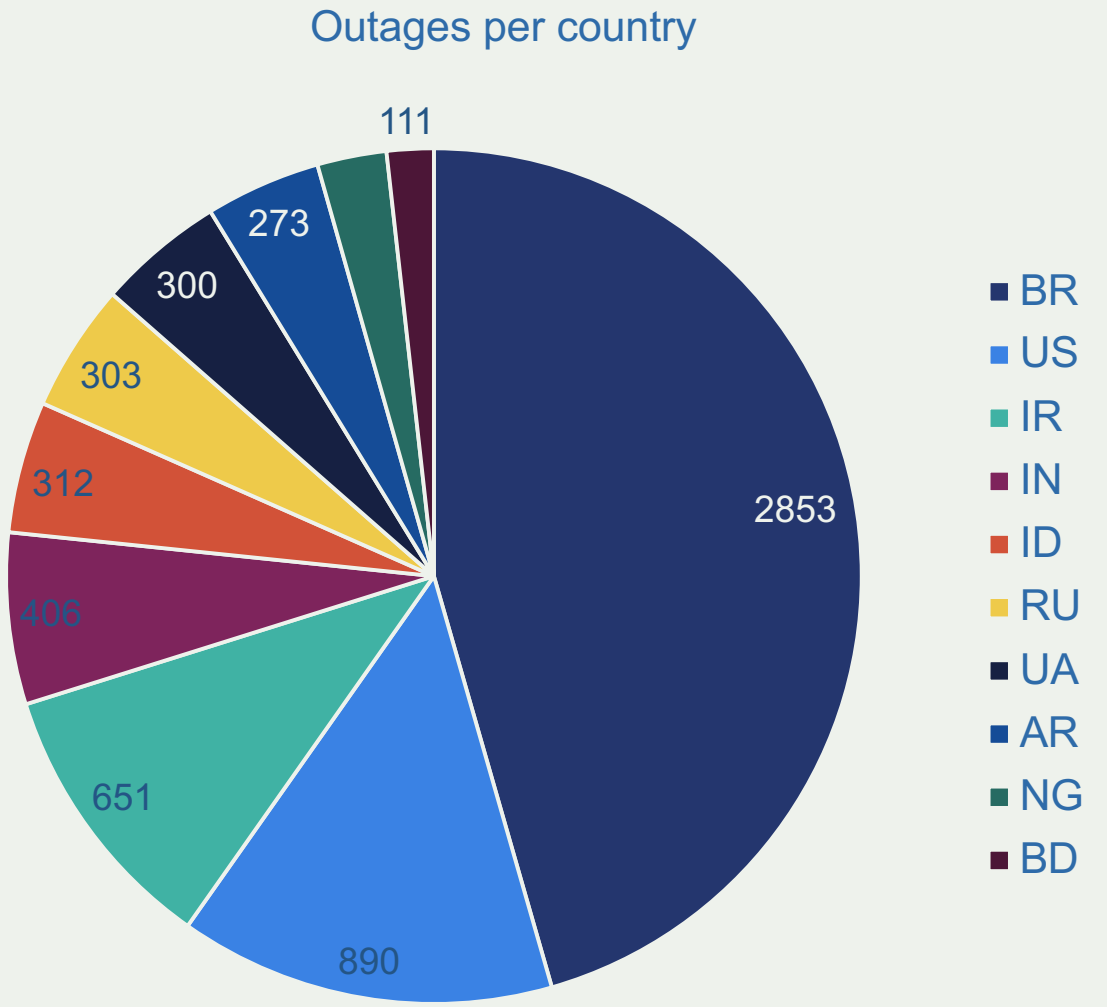
The routing system is constantly under attack (2017 → 2018)

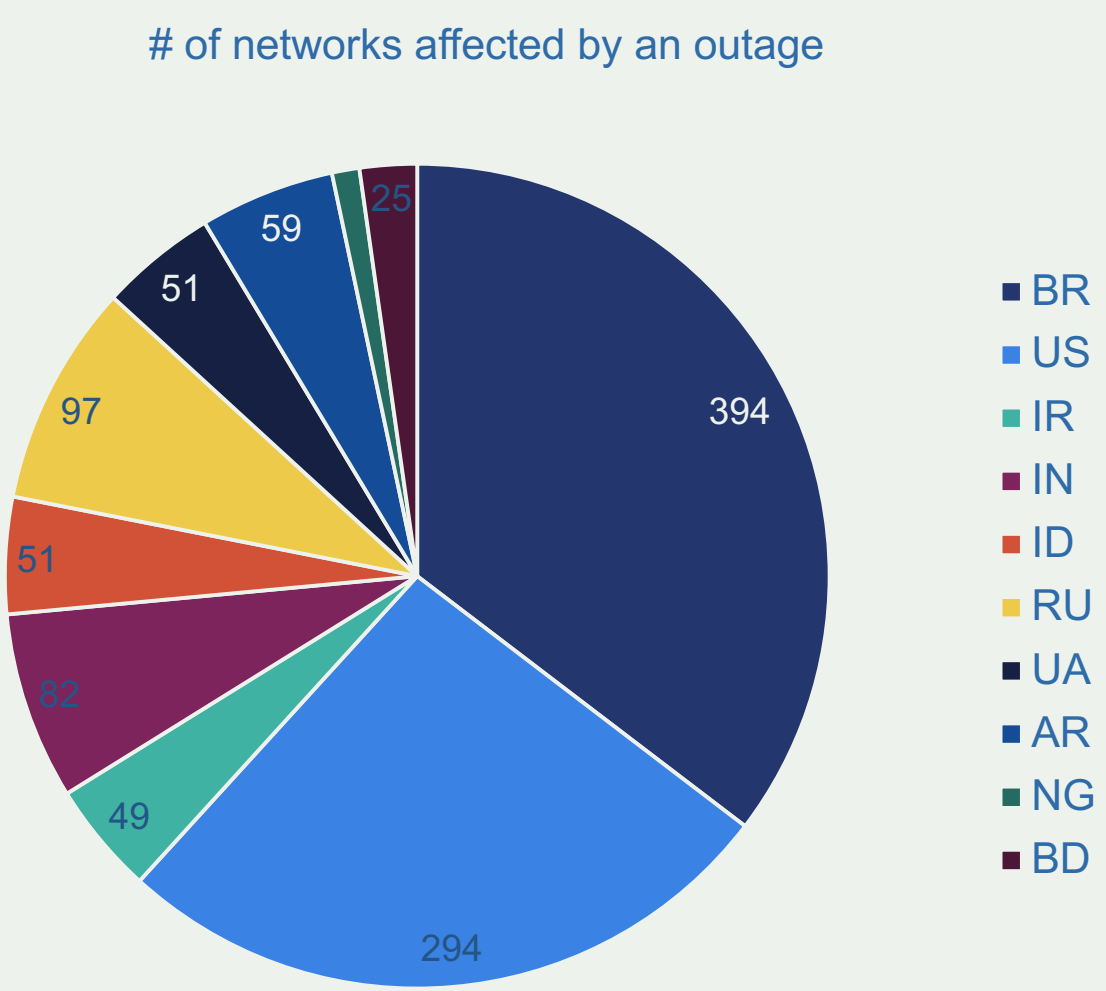
- 13,935 total incidents (either outages or attacks like route leaks and hijacks)
- Over 10% of all Autonomous Systems on the Internet were affected
- 3,106 Autonomous Systems were a victim of at least one routing incident
- **1,546 networks were responsible for 5304 routing incidents**
- **547 networks were responsible for 1576 routing incidents**
- **LAC: 82 networks responsible for 177 incidents**



Source: https://www.bgpstream.com/

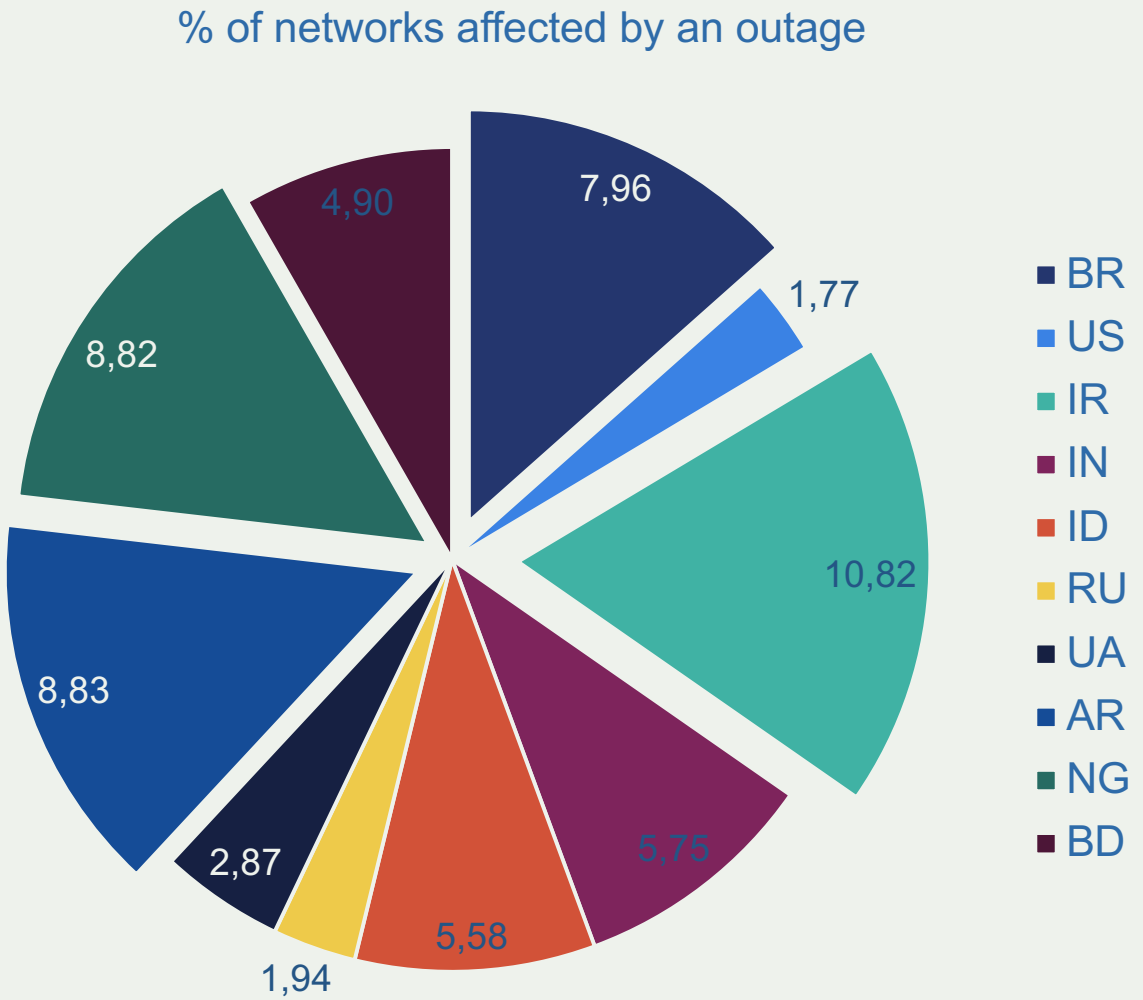
Outages 2017





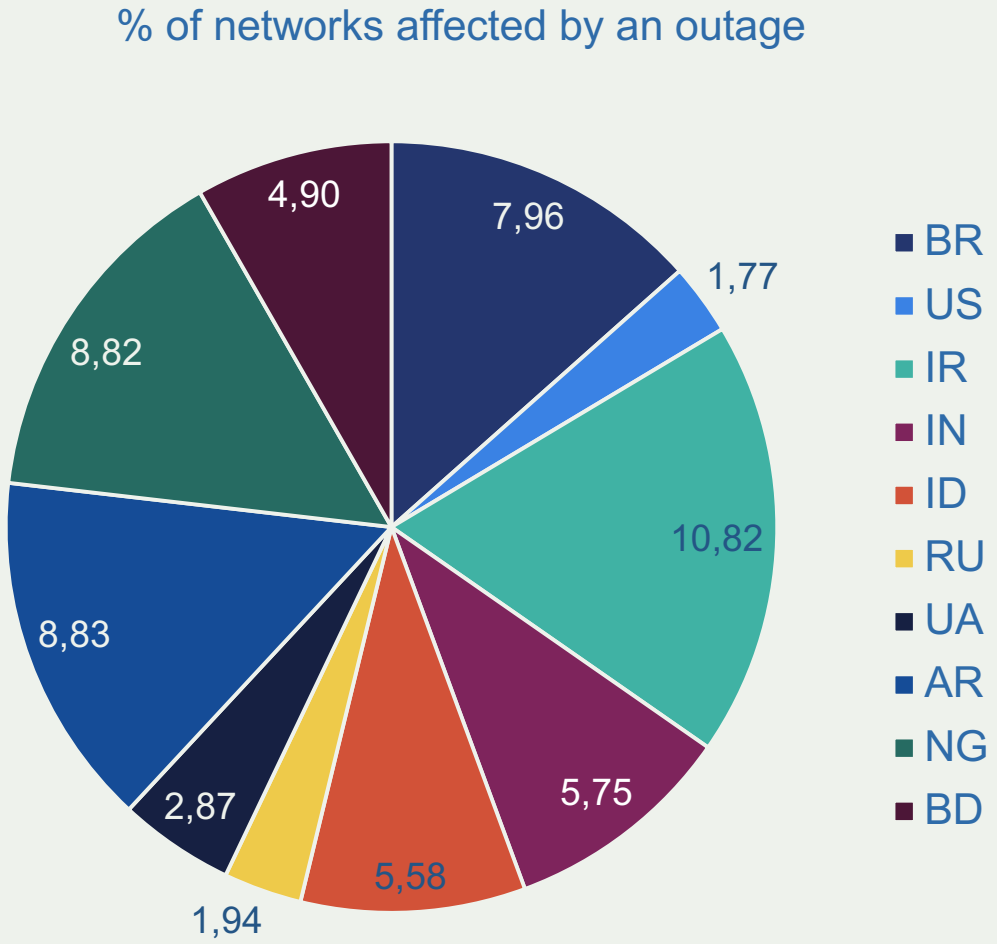
Source: https://www.bgpstream.com/

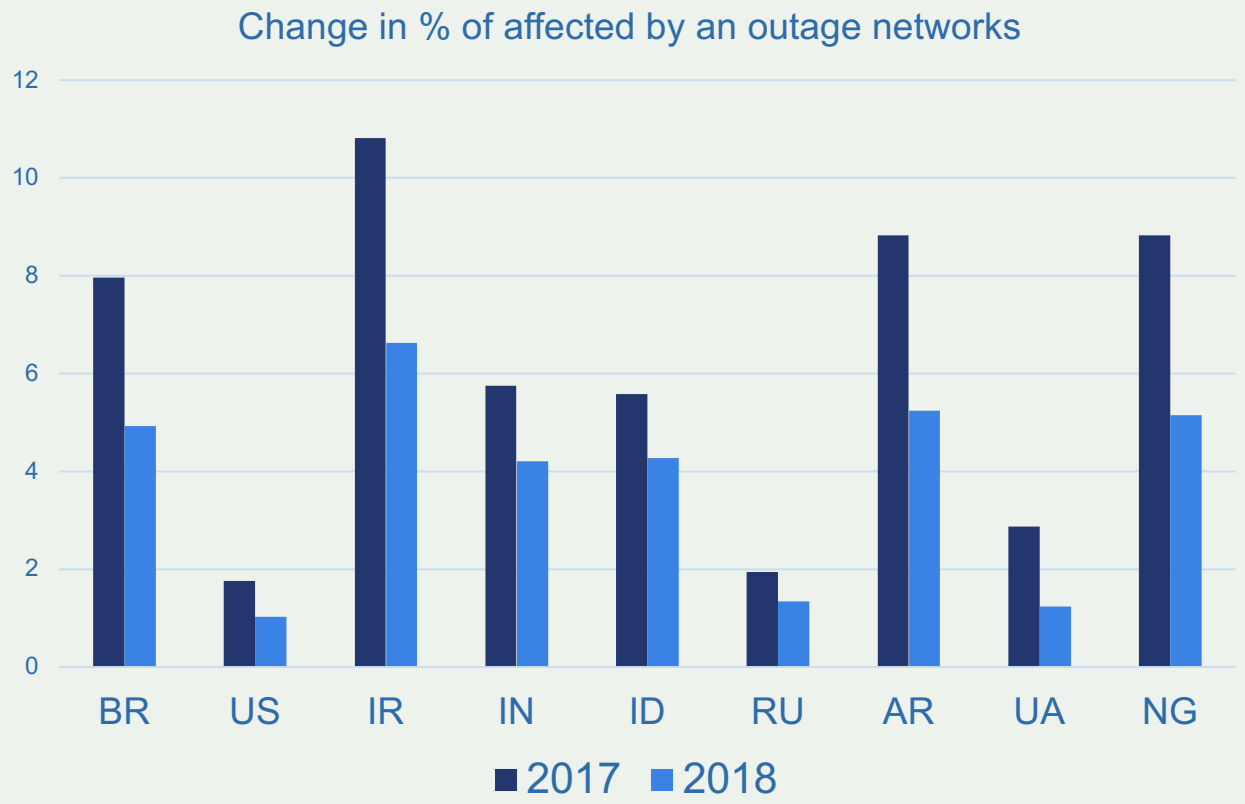
Outages 2017



Source: https://www.bgpstream.com/

Outages 2017 → 2018

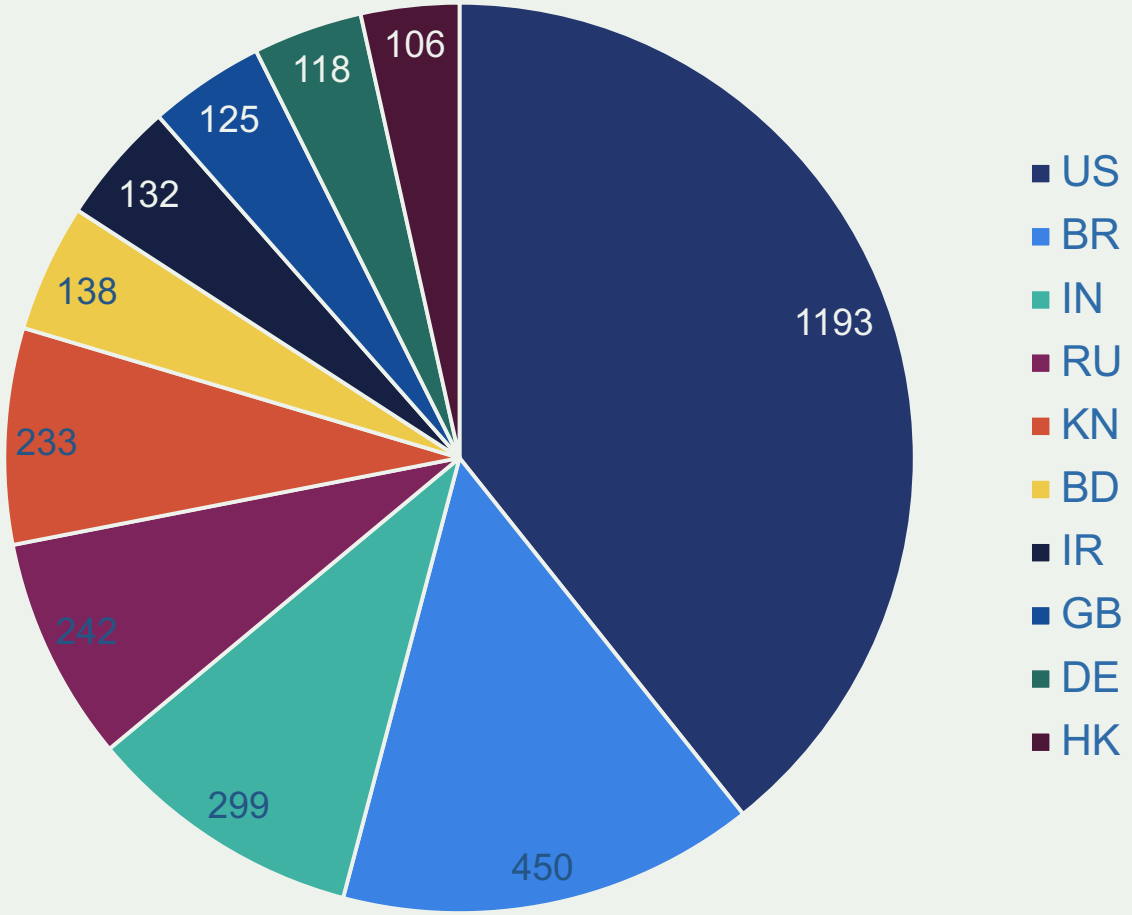


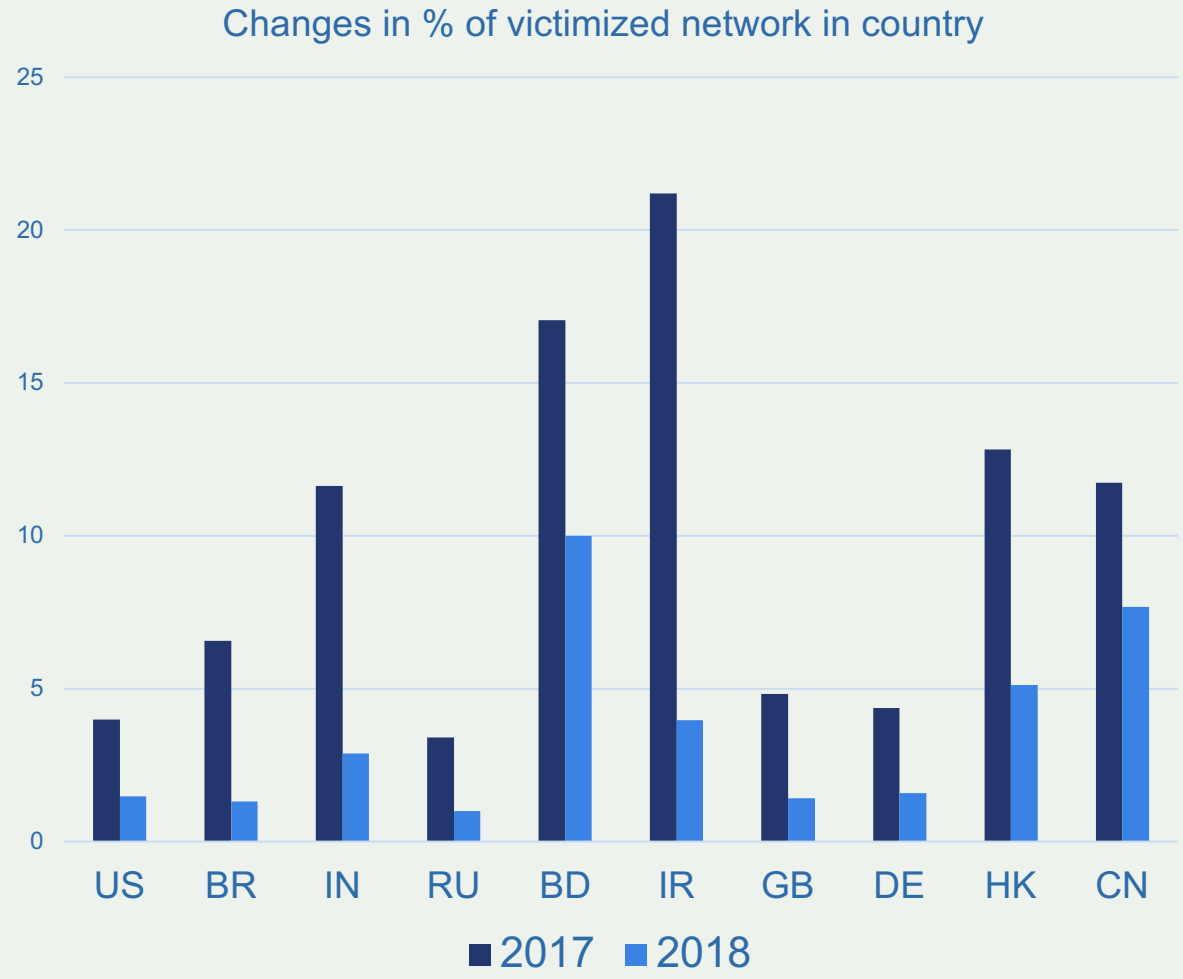


Source: https://www.bgpstream.com/

Potential victims

Incidents with a victim in a country, Top 10, 2017

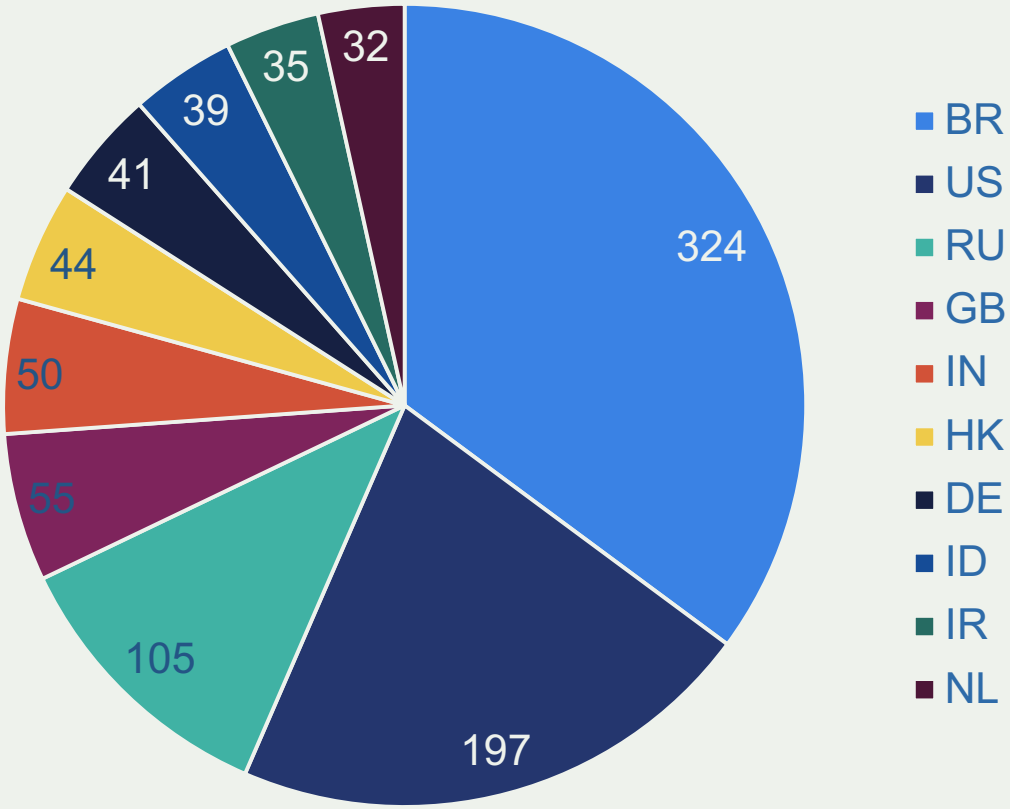




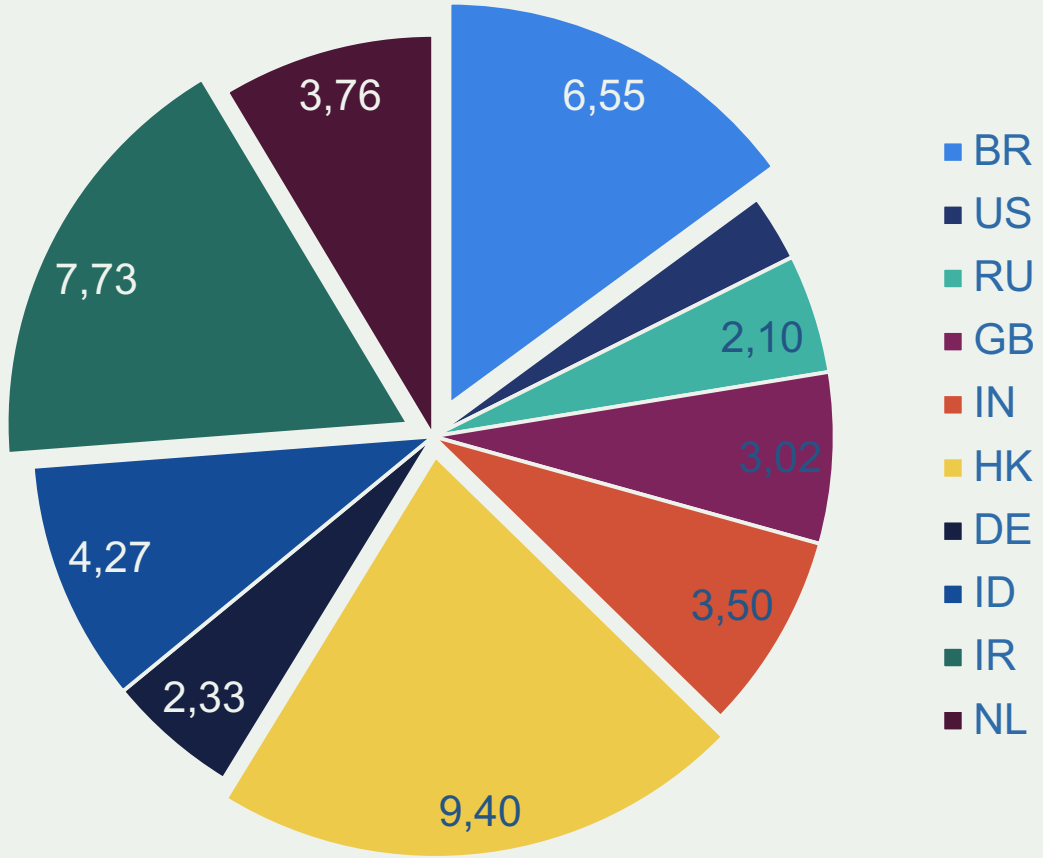
Source: https://www.bgpstream.com/

Potential culprits 2017

Number of AS's in a country responsible for a routing incident (a route leak or hijack)

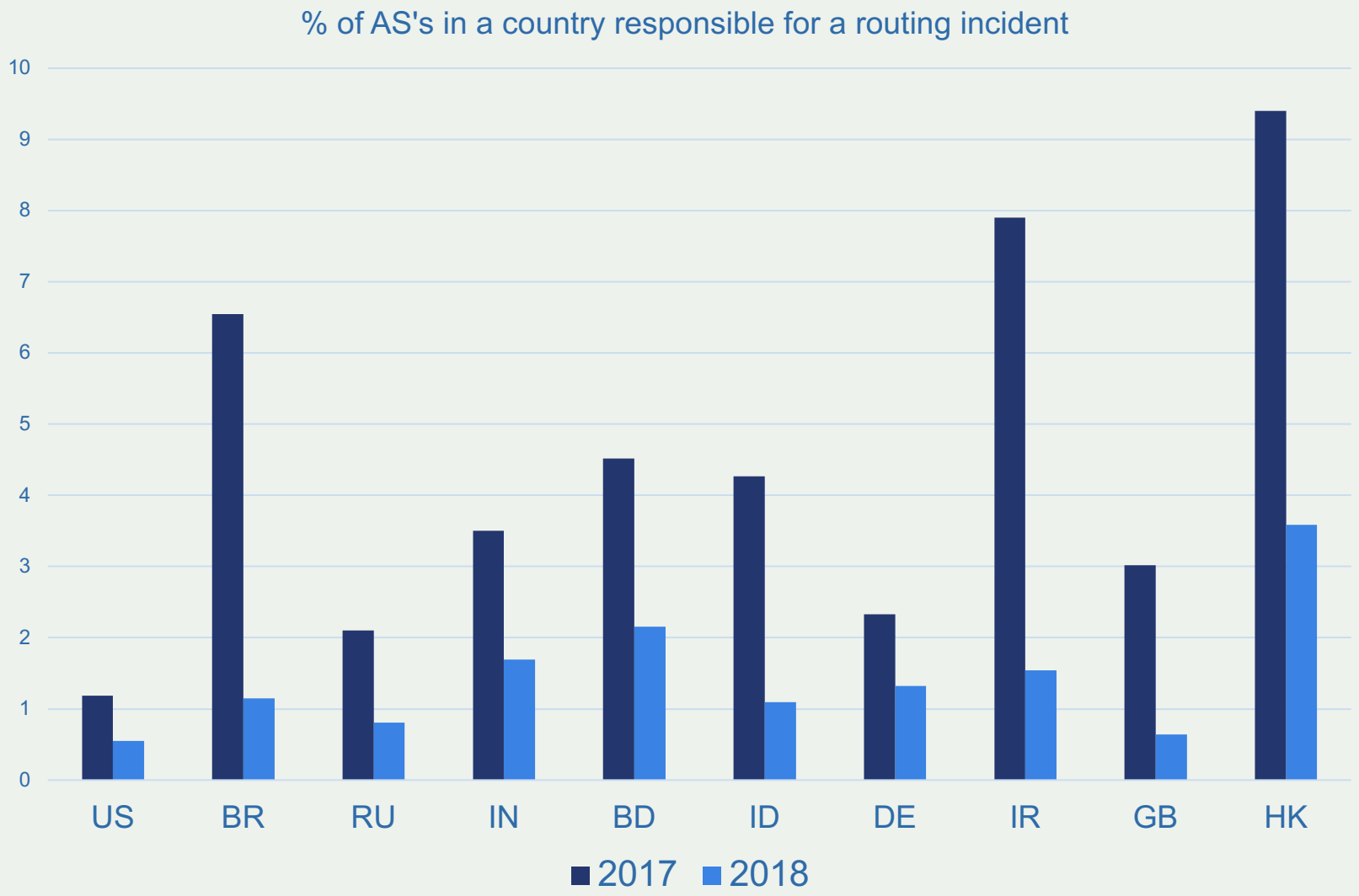


Percent of AS's in a country responsible for a routing incident (a route leak or hijack)



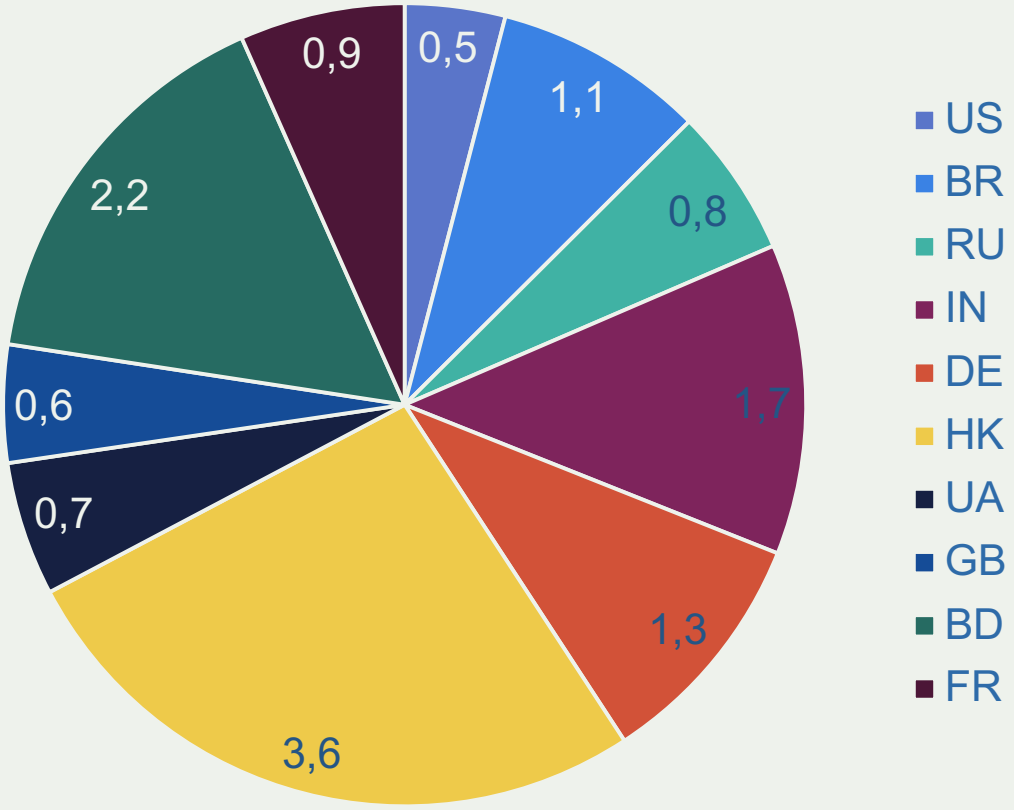
Source: https://www.bgpstream.com/

Positive dynamics

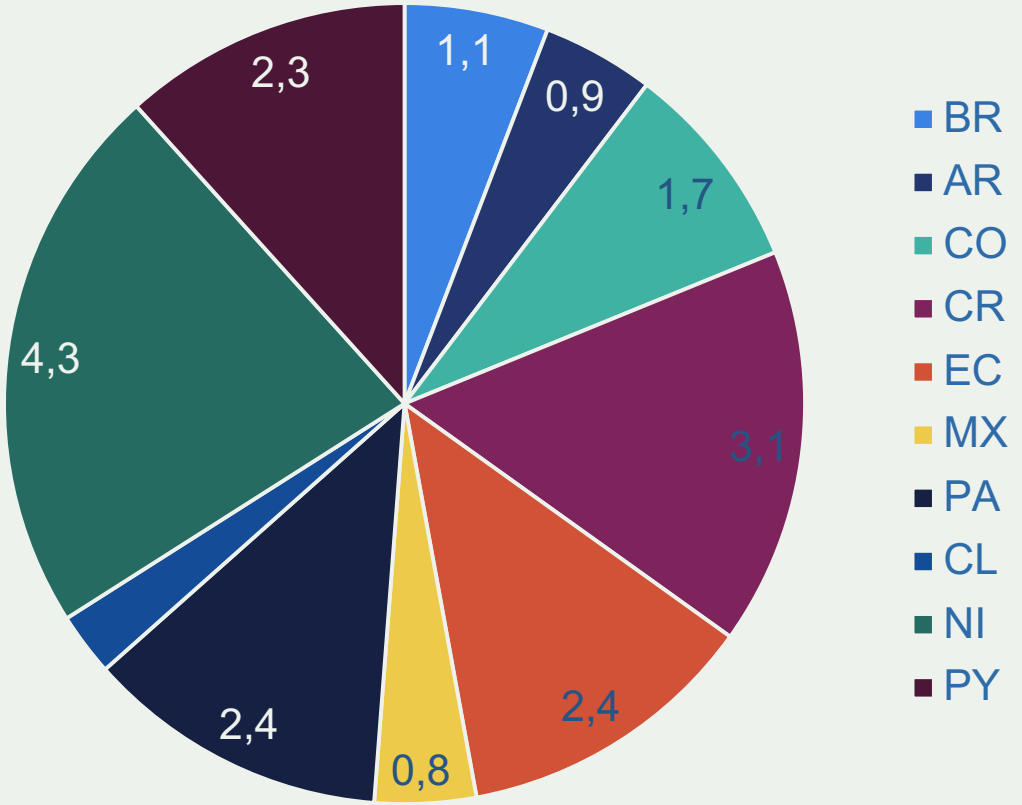


2018 The World and LAC

Percent of AS's in a country responsible for a routing incident (a route leak or hijack)



Percent of AS's in a country responsible for a routing incident (a route leak or hijack)



Source: https://www.bgpstream.com/

The Basics: How Routing Works

There are ~60,000 networks (Autonomous Systems) across the Internet, each using a unique Autonomous System Number (ASN) to identify itself to other networks.

Routers use Border Gateway Protocol (BGP) to exchange “reachability information” - networks they know how to reach.

Routers build a “routing table” and pick the best route when sending a packet, typically based on the shortest path.

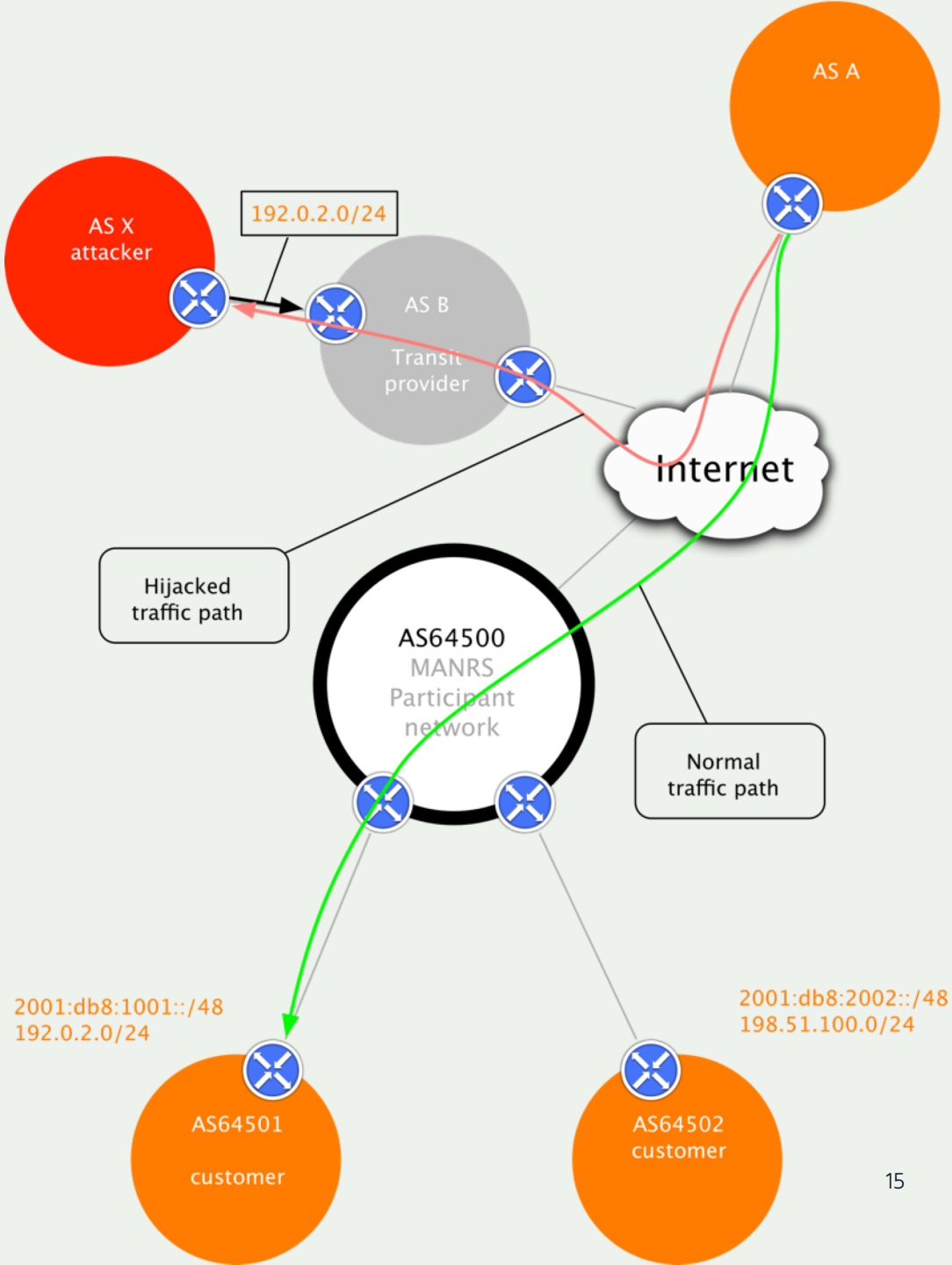
Routing Incidents Cause Real World Problems

Event	Explanation	Repercussions	Example
Prefix/Route Hijacking	A network operator or attacker impersonates another network operator, pretending that a server or network is their client.	Packets are forwarded to the wrong place, and can cause Denial of Service (DoS) attacks or traffic interception.	*The 2008 YouTube hijack April 2018 Amazon Route 53 hijack*
Route Leak	A network operator with multiple upstream providers (often due to accidental misconfiguration) announces to one upstream provider that is has a route to a destination through the other upstream provider.	Can be used for a MITM, including traffic inspection, modification and reconnaissance.	*September 2014. VolumeDrive began announcing to Atrato nearly all the BGP routes it learned from Cogent causing disruptions to traffic in places as far-flung from the USA as Pakistan and Bulgaria.*
IP Address Spoofing	Someone creates IP packets with a false source IP address to hide the identity of the sender or to impersonate another computing system.	The root cause of reflection DDoS attacks	*March 1, 2018. Memcached 1.3Tb/s reflection-amplificationattack reported by Akamai*

Route Hijacking

Route hijacking, also known as “BGP hijacking” when a network operator or attacker (accidentally or deliberately) impersonates another network operator or pretends that the network is their client. This routes traffic to the attacker, while the victim suffers an outage.

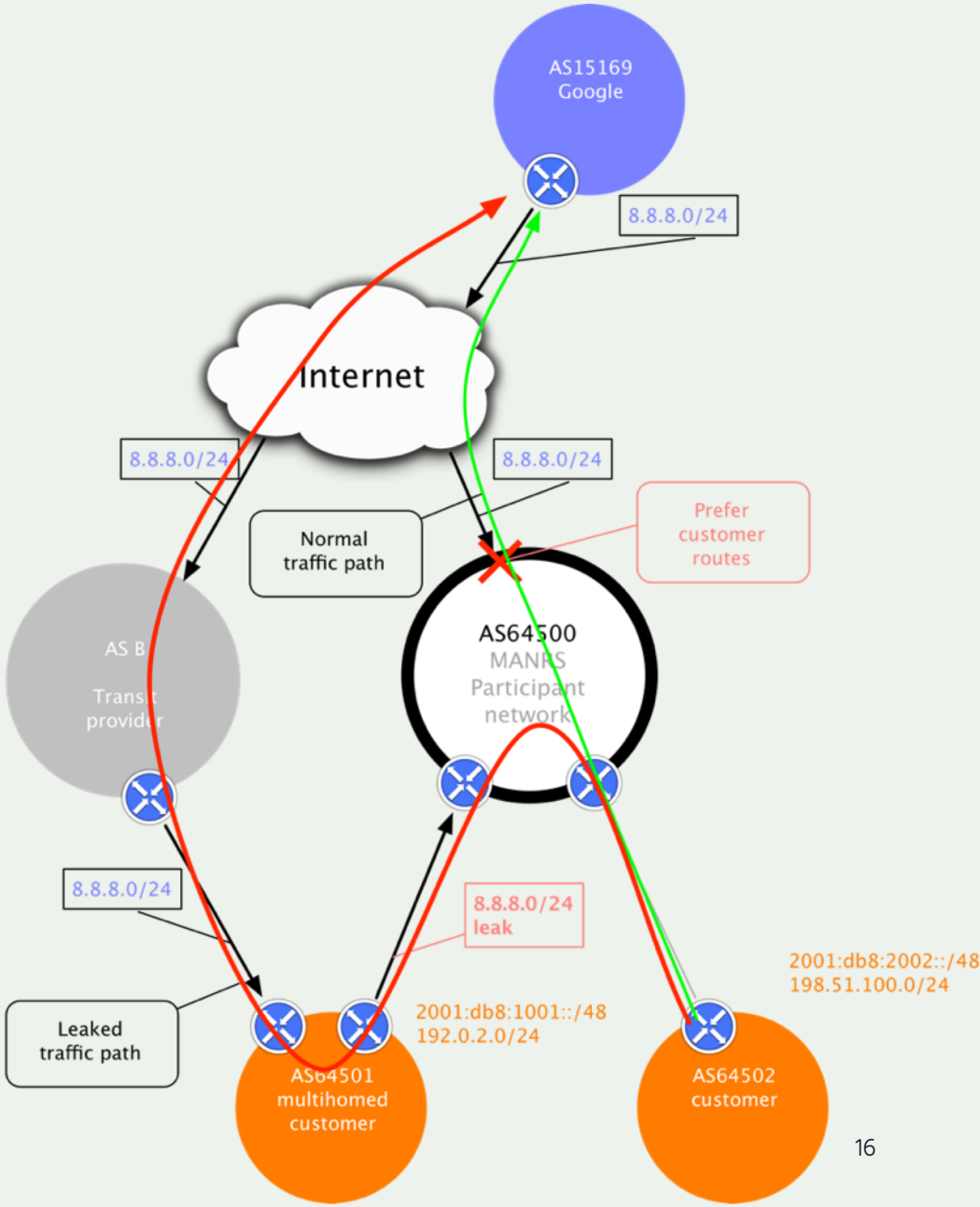
Example: *The 2008 YouTube hijack; an attempt to block Youtube through route hijacking led to much of the traffic to Youtube being dropped around the world (https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study)*



Route Leak

A Route leak is a problem where a network operator with multiple upstream providers accidentally announces to one of its upstream providers that is has a route to a destination through the other upstream provider. This makes the network an intermediary network between the two upstream providers. With one sending traffic now through it to get to the other.

Example: *September 2014. VolumeDrive (AS46664) is a Pennsylvania-based hosting company that uses Cogent (AS174) and Atrato (AS5580) for Internet transit. VolumeDrive began announcing to Atrato nearly all the BGP routes it learned from Cogent causing disruptions to traffic in places as far-flung from the USA as Pakistan and Bulgaria. (https://dyn.com/blog/why-the-internet-broke-today/)*

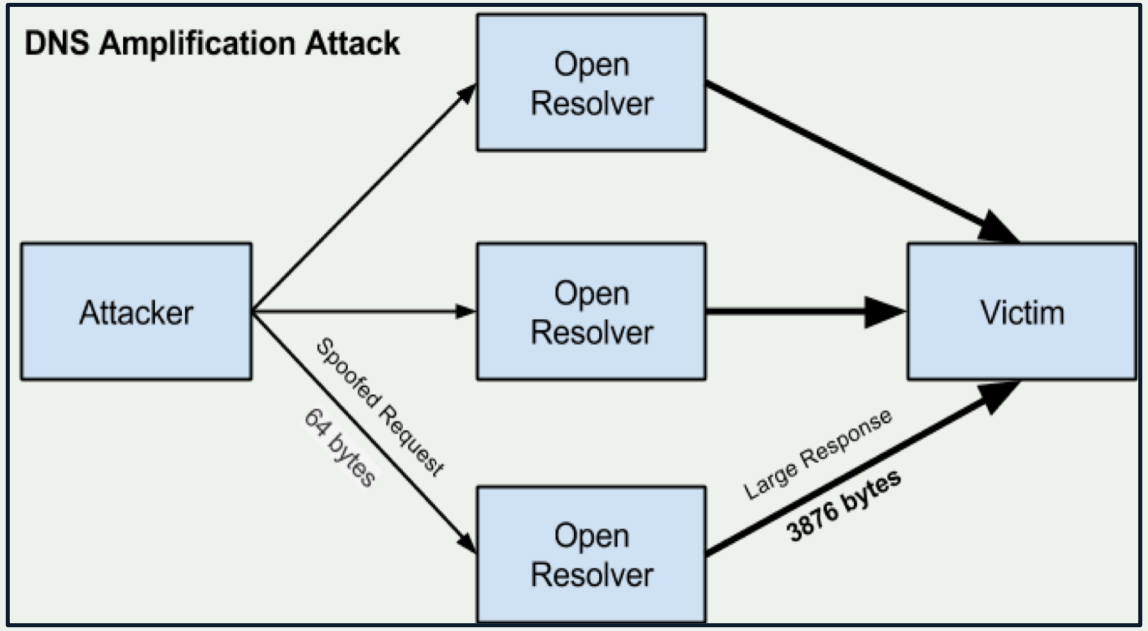


IP Address Spoofing

IP address spoofing is used to hide the true identity of the server or to impersonate another server. This technique can be used to amplify an attack.

Example: DNS amplification attack. By sending multiple spoofed requests to different DNS resolvers, an attacker can prompt many responses from the DNS resolver to be sent to a target, while only using one system to attack.

Fix: Source address validation: systems for source address validation can help tell if the end users and customer networks have correct source IP addresses (combined with filtering).



Tools to Help

- Prefix and AS-PATH filtering
- RPKI validator, IRR toolset, IRRPT, BGPQ3
- BGPSEC is standardized

But…

- Not enough deployment
- Lack of reliable data

We need a systemic approach to improving routing security

We Are In This Together

Network operators have a responsibility to ensure a globally robust and secure routing infrastructure.

Your network's safety depends on a routing infrastructure that weeds out bad actors and accidental misconfigurations that wreak havoc on the Internet.

The more network operators work together, the fewer incidents there will be, and the less damage they can do.

Mutually Agreed Norms for Routing Security (MANRS)

Provides crucial fixes to reduce the most common routing threats

Mutually Agreed Norms for Routing Security

MANRS defines four simple but concrete actions that network operators must implement to improve Internet security and reliability.

- The first two operational improvements eliminate the root causes of common routing issues and attacks, while the second two procedural steps improve mitigation and decrease the likelihood of future incidents.

MANRS builds a visible community of security minded network operators and IXPs

MANRS

MANRS Actions

Filtering

Prevent propagation of incorrect routing information

Ensure the correctness of your own announcements and announcements from your customers to adjacent networks with prefix and AS-path granularity

Anti-spoofing

Prevent traffic with spoofed source IP addresses

Enable source address validation for at least single-homed stub customer networks, their own end-users, and infrastructure

Coordination

Facilitate global operational communication and coordination between network operators

Maintain globally accessible up-to-date contact information in common routing databases

Global Validation

Facilitate validation of routing information on a global scale

Publish your data, so others can validate

MANRS is an Important Step

Security is a process, not a state. MANRS provides a structure and a consistent approach to solving security issues facing the Internet.

MANRS is the minimum an operator should consider, with low risk and cost-effective actions.

MANRS is not a one-stop solution to all of the Internet's routing woes, but it is an important step toward a globally robust and secure routing infrastructure.

The Business Case for MANRS and Routing Security

Engaged 451 Research to better understand the attitudes and perceptions of Internet service providers and the broader enterprise community around the project

What We Learned from the Study

Security is Vital to Enterprises

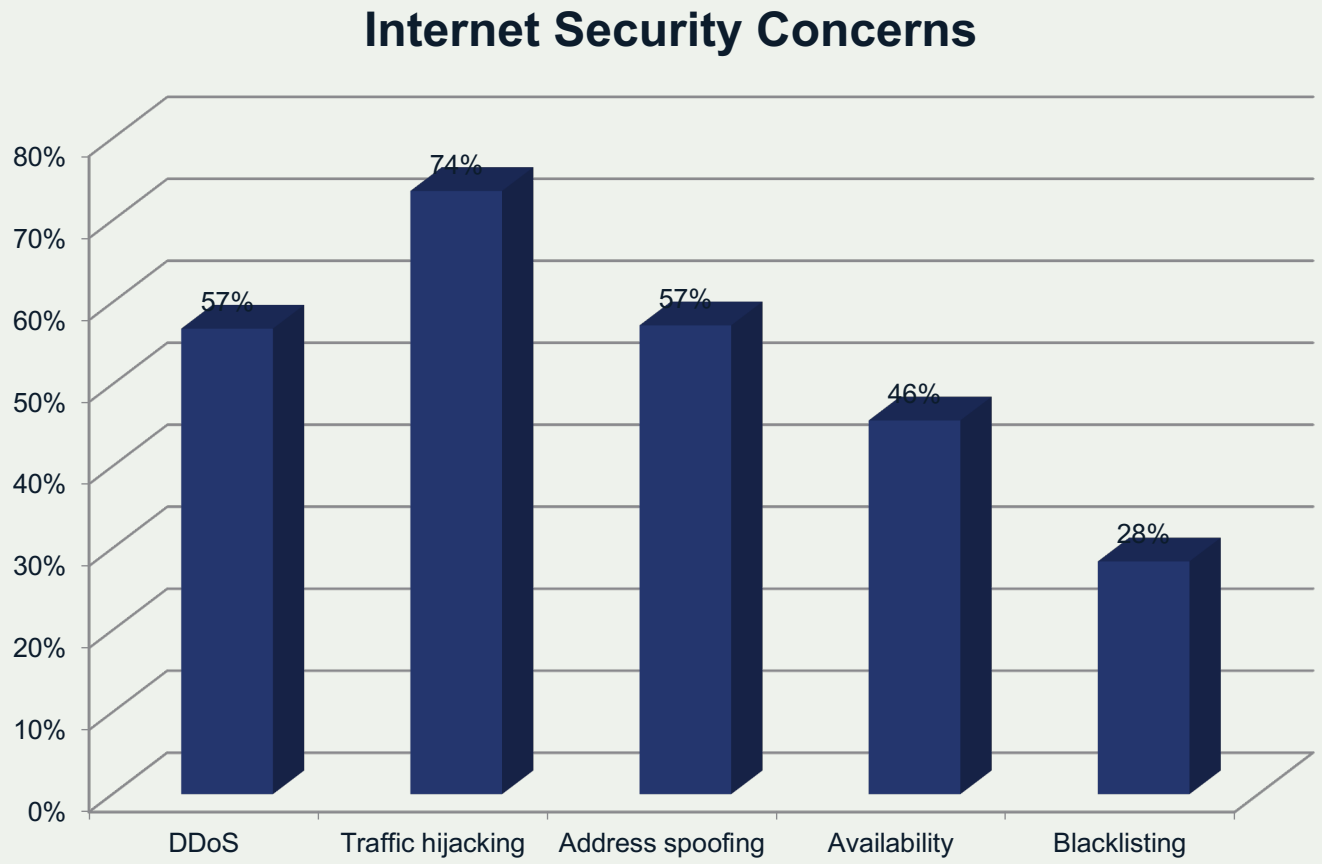
- MANRS knowledge is low, but the desire for security is high
- Enterprises are willing to require MANRS compliance of their service providers

MANRS Adds Value for Service Providers

- Security can help service providers differentiate from their competitors; Identifiable value in a vague market
- Service providers may be able to add additional revenue streams based on information security feeds and other add-on services

Enterprise Security Concerns

- Widely varying concerns across a range of issues, with traffic hijacking leading the list
- Security focus is aligned with types of issues MANRS is looking to address
- Confidence that MANRS can help long-term routing security



Implementing MANRS Actions:

Signals an organization's security-forward posture and can eliminate SLA violations that reduce profitability or cost customer relationships.

Heads off routing incidents, helping networks readily identify and address problems with customers or peers.

Improves a network's operational efficiency by establishing better and cleaner peering communication pathways, while also providing granular insight for troubleshooting.

Addresses many concerns of security-focused enterprises and other customers.

MANRS – increasing adoption

MANRS IXP Programme

There is synergy between MANRS and IXPs

- IXPs form a community with a common operational objective
- MANRS is a reference point with a global presence – useful for building a “safe neighborhood”

How can IXPs contribute?

- Implement a set of Actions that demonstrate the IXP commitment and also bring significant improvement to the resilience and security of the routing system

MANRS IXP Program – launched on April 23!

IXP Participants

IXPs are important partners in the MANRS community

IXPs can be a collaborative focal point to discuss and promote the importance of routing security. To address the unique needs and concerns of IXPs, the community created a related but separate set of MANRS actions for IXP members.

Click Here to Join!

Organization	Country	Action 1: Prevent Incorrect Routing Information	Action 2.1 Assist in Correct Routing Information	Action 2.2 Assist in MANRS ISP Actions	Action 2.3 Indicate MANRS participation	Action 2.4 Incentives for MANRS Participation	Action 3. Protect the Peering Platform	Action 4. Facilitate Global Communication	Action 5. Provide Monitoring and Debugging Tools
INEX (Internet Neutral Exchange Association CLG)	IE	✓	✓		✓		✓	✓	✓
TorIX (Toronto Internet Exchange Community)	CA	✓	✓		✓		✓	✓	✓
DE-CIX	DE	✓	✓				✓	✓	✓
MSK-IX	RU	✓	✓		✓		✓	✓	✓
Netnod	SE	✓	✓		✓		✓	✓	
CRIX (NIC Costa Rica)	CR	✓	✓	✓	✓	✓		✓	✓
Asteroid (Asteroid		✓	✓	✓	✓		✓	✓	✓

MANRS Implementation Guide

A resource to help Operators implement MANRS Actions.

- Based on Best Current Operational Practices deployed by network operators around the world
- https://www.manrs.org/bcop/
- Has received recognition from the RIPE community by being published as RIPE-706

Mutually Agreed Norms for Routing Security (MANRS) Implementation Guide

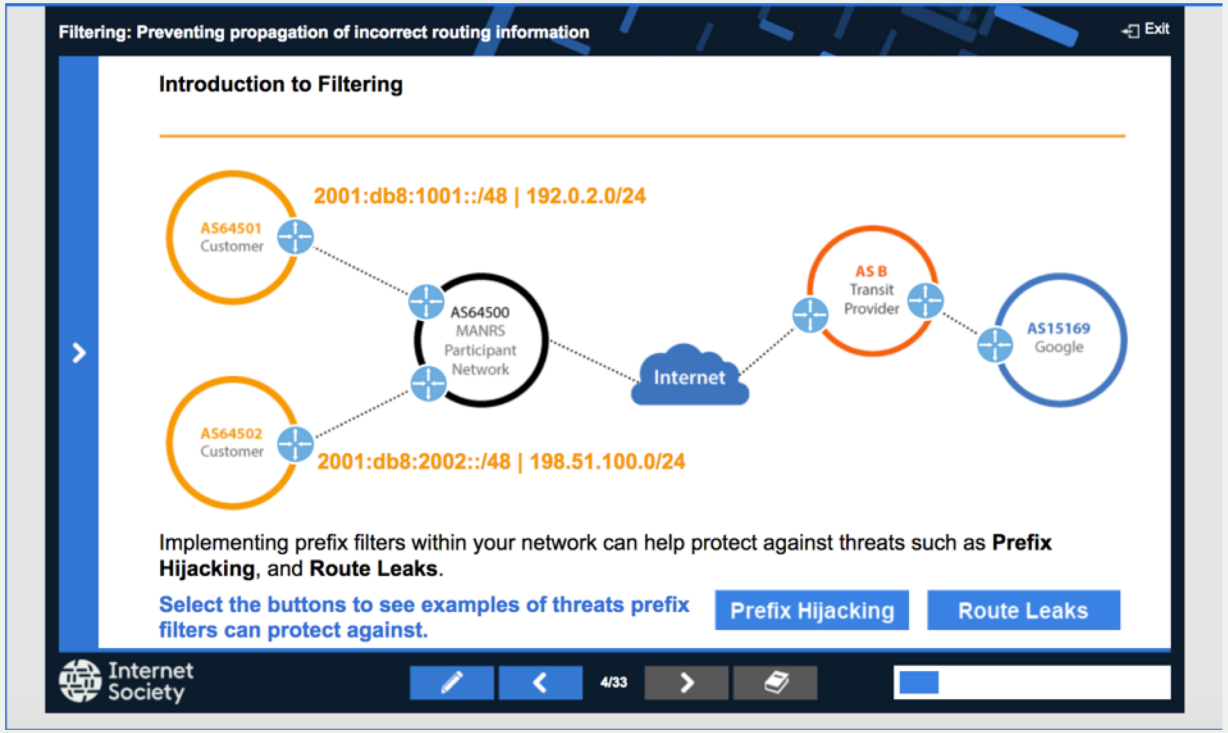
Version 1.0, BCOP series
Publication Date: 25 January 2017

MANRS Training Tutorials and a Hands-on Lab

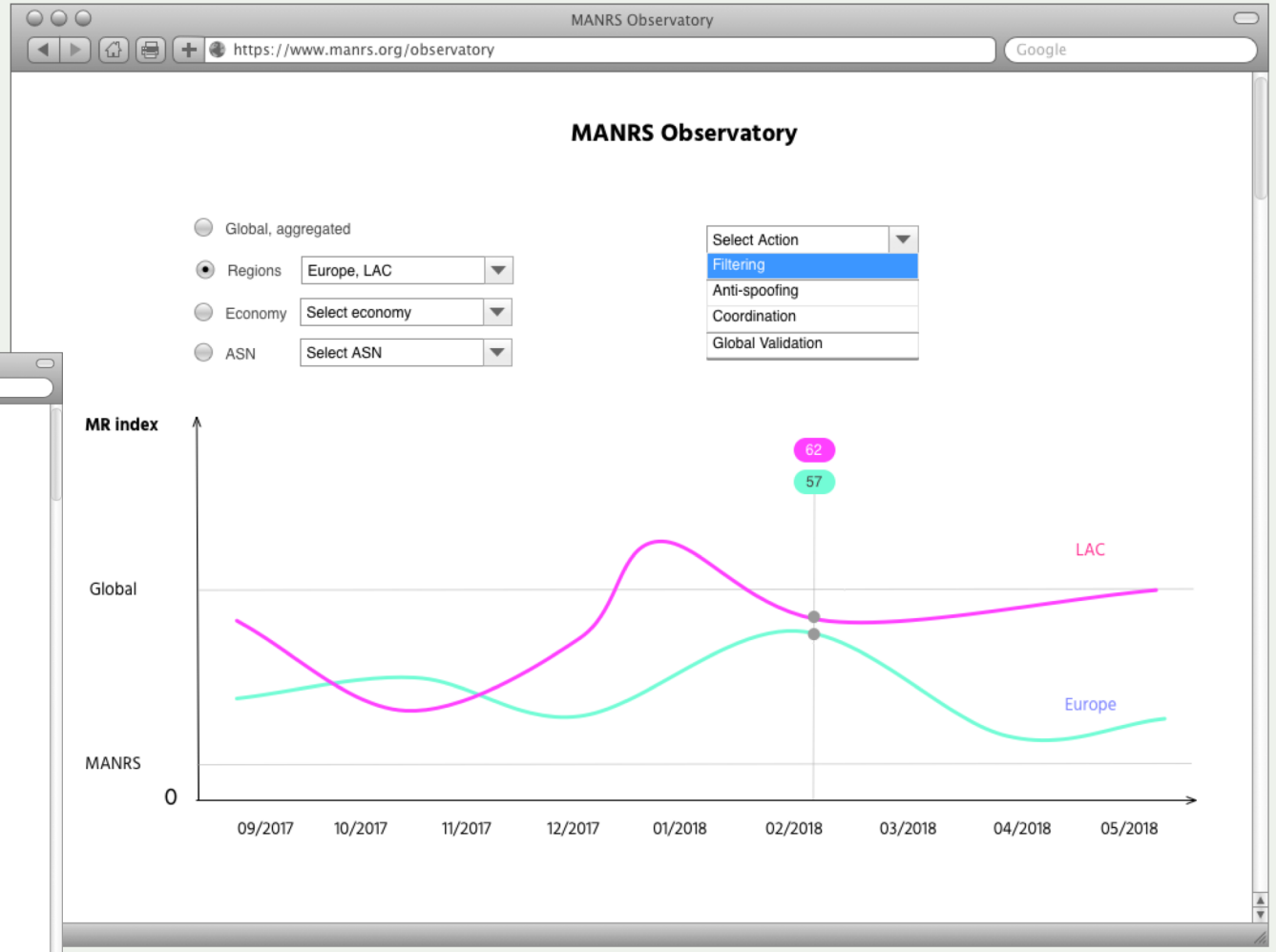
6 training tutorials based on information in the Implementation Guide. A test at the end of each tutorial. https://www.manrs.org/tutorials

About to begin training moderators for online classes (43 applications received!)

The prototype lab is ready, finalizing the production version.



MANRS Member Report and MANRS Observatory



Why join MANRS?

- Improve your security posture and reduce the number and impact of routing incidents
- Join a community of security-minded operators working together to make the Internet better
- Use MANRS as a competitive differentiator

Join Us

Visit https://www.manrs.org

- Fill out the sign up form with as much detail as possible.
- We may ask questions and run tests

Get Involved in the Community

- Members support the initiative and implement the actions in their own networks
- Members maintain and improve the document and promote MANRS objectives

manrs.org

#ProtectTheCore

MANRS Video:
https://www.youtube.com/embed/nJINk5p-HEE