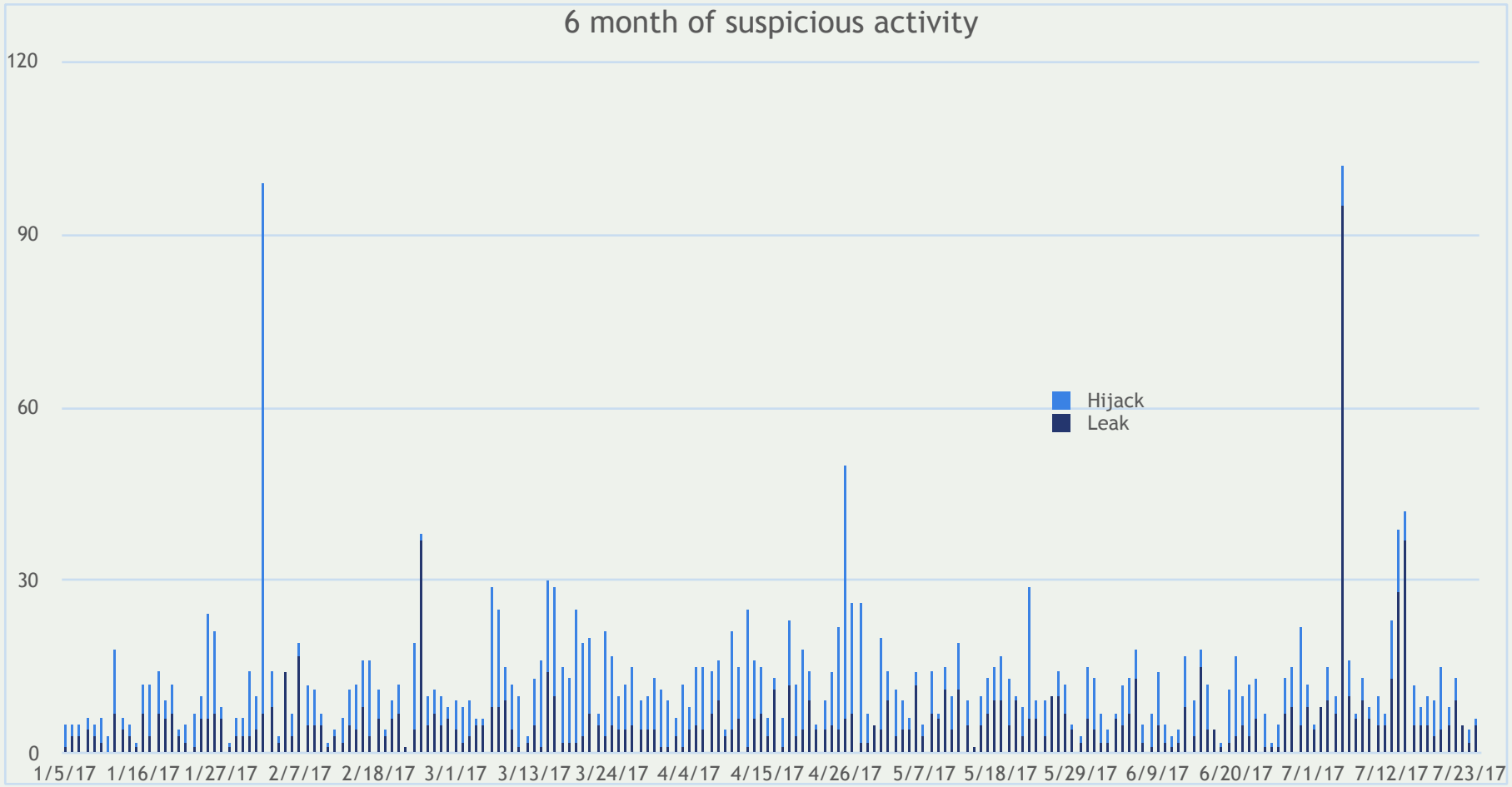
Routing Security – We can do better!

And how MANRS can help

Andrei Robachevsky

robachevsky@isoc.org

No Day Without an Incident



http://bgpstream.com/

Routing Incidents Cause Real World Problems

Insecure routing is one of the most common paths for malicious threats.

Attacks can take anywhere from hours to months to even recognize.

Inadvertent errors can take entire countries offline, while attackers can steal an individual’s data or hold an organization’s network hostage.

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.

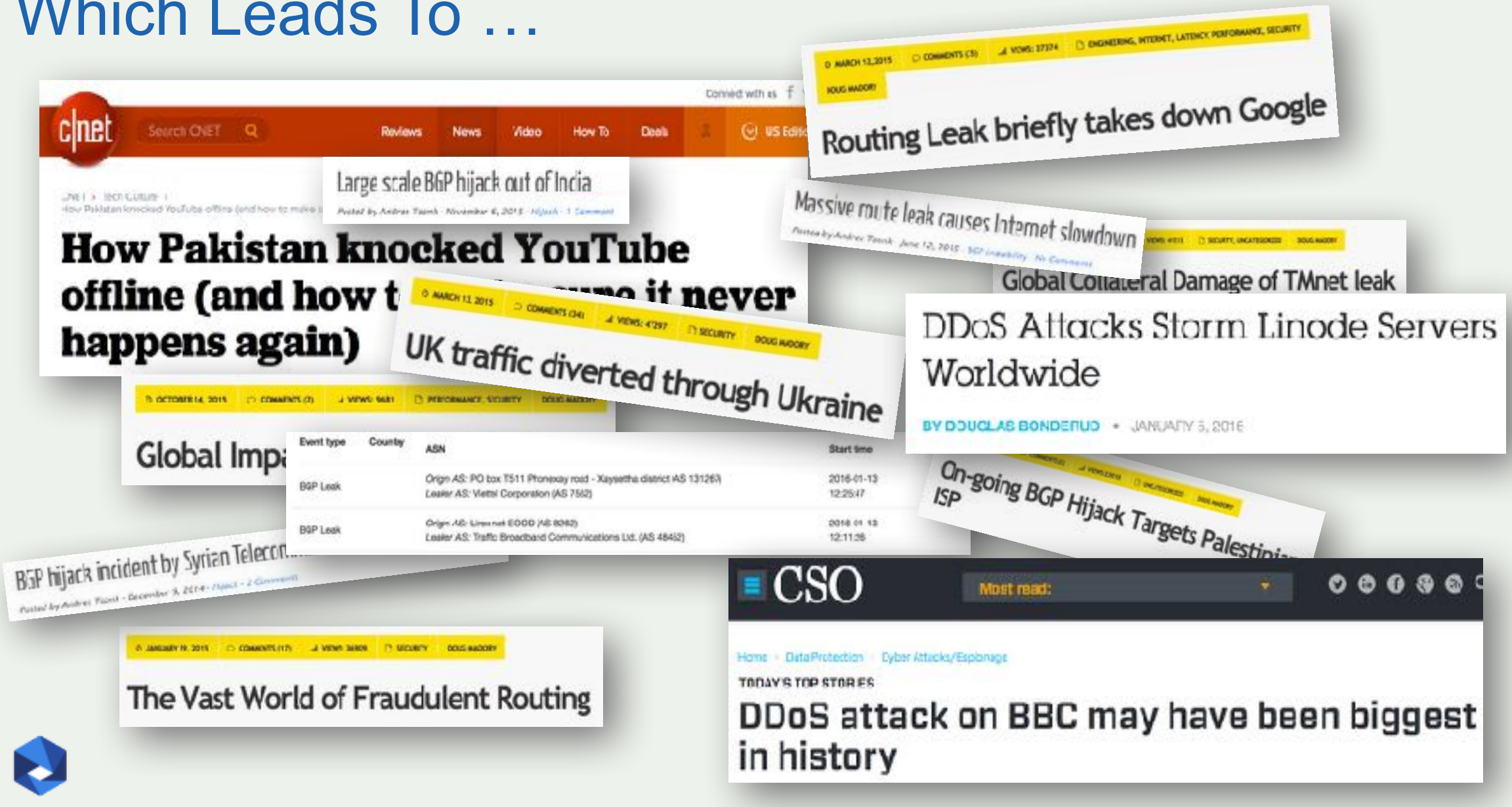
Routers build a “routing table” and pick the best route when sending a packet, typically based on the shortest path.

The Honor System: Routing Issues

Border Gateway Protocol (BGP) is based entirely on trust between networks

- No built-in validation that updates are legitimate
- The chain of trust spans continents
- Lack of reliable resource data

Which Leads To …



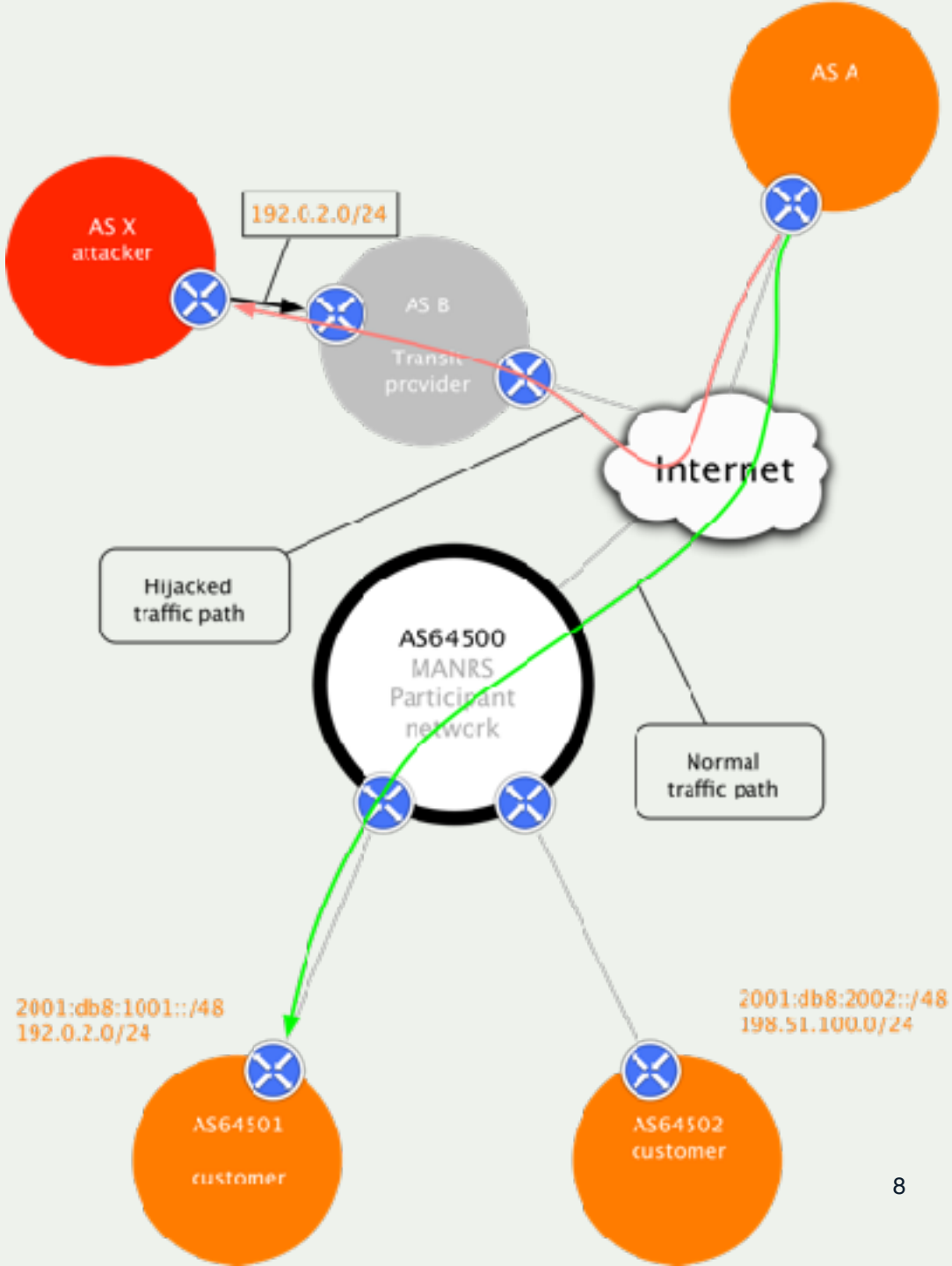
The Threats: What's Happening?

Event	Explanation	Repercussions	Solution
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.	Stronger filtering policies
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 traffic inspection and reconnaissance.	Stronger filtering policies
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	Source address validation

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.

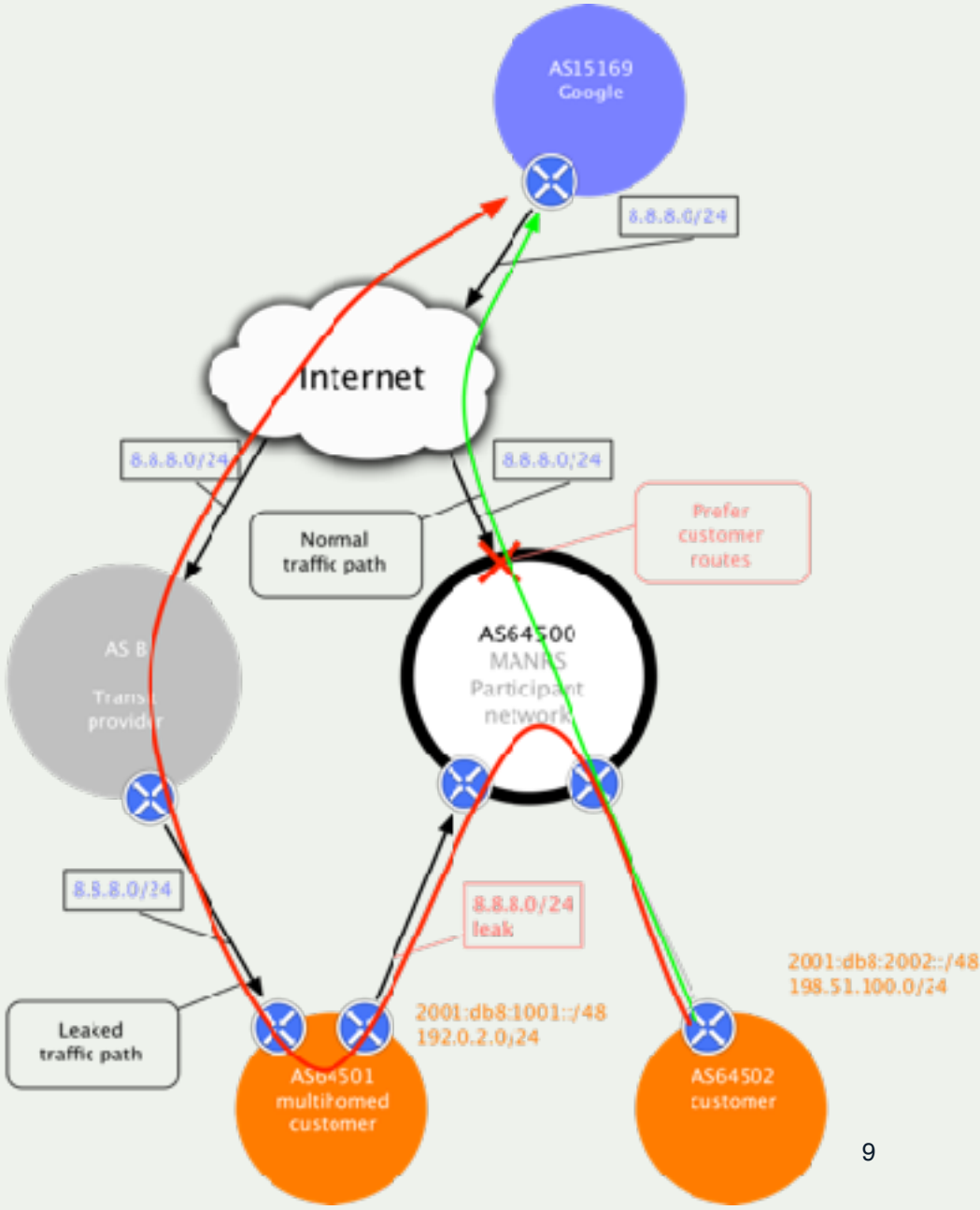
Example: *The 2008 YouTube hijack; an attempt to block Youtube through route hijacking led to much of the traffic to Youtube being dropped around the world (https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study)*



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/)*

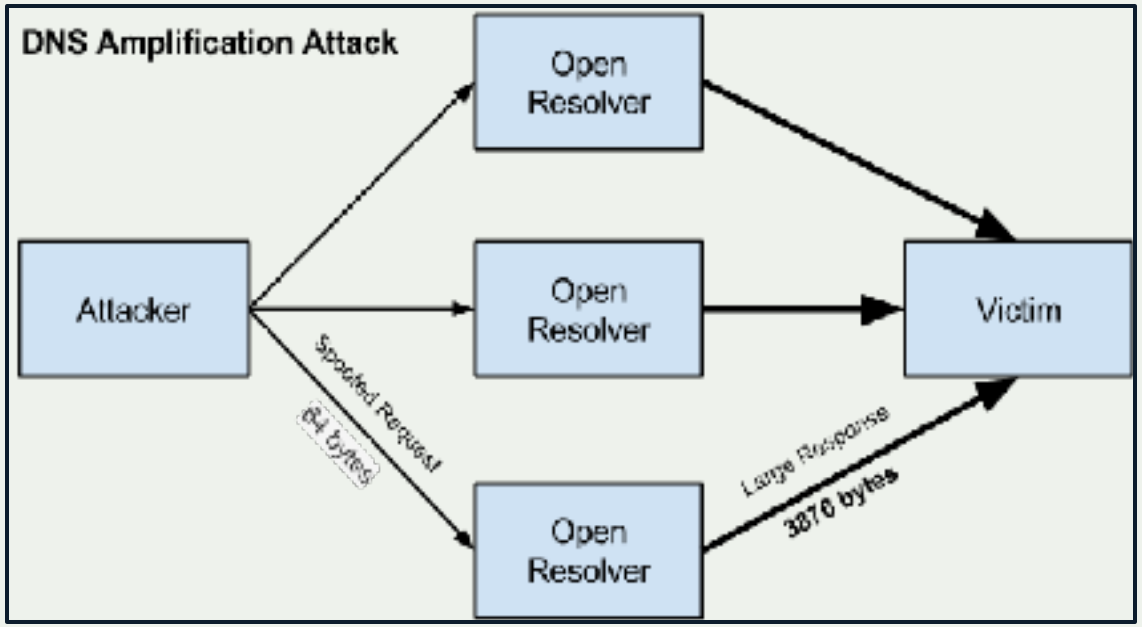


IP Address Spoofing

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).



2017 in review: 14000 routing incidents

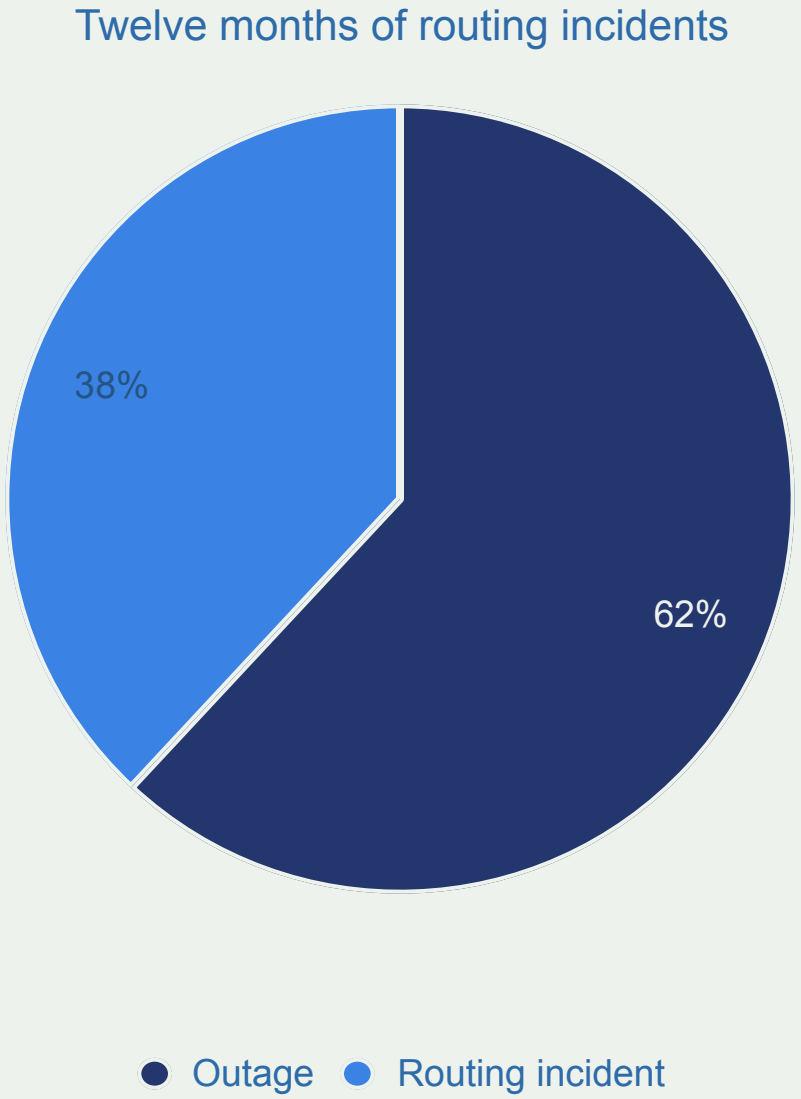
Statistics of routing incidents generated from BGPStream data

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

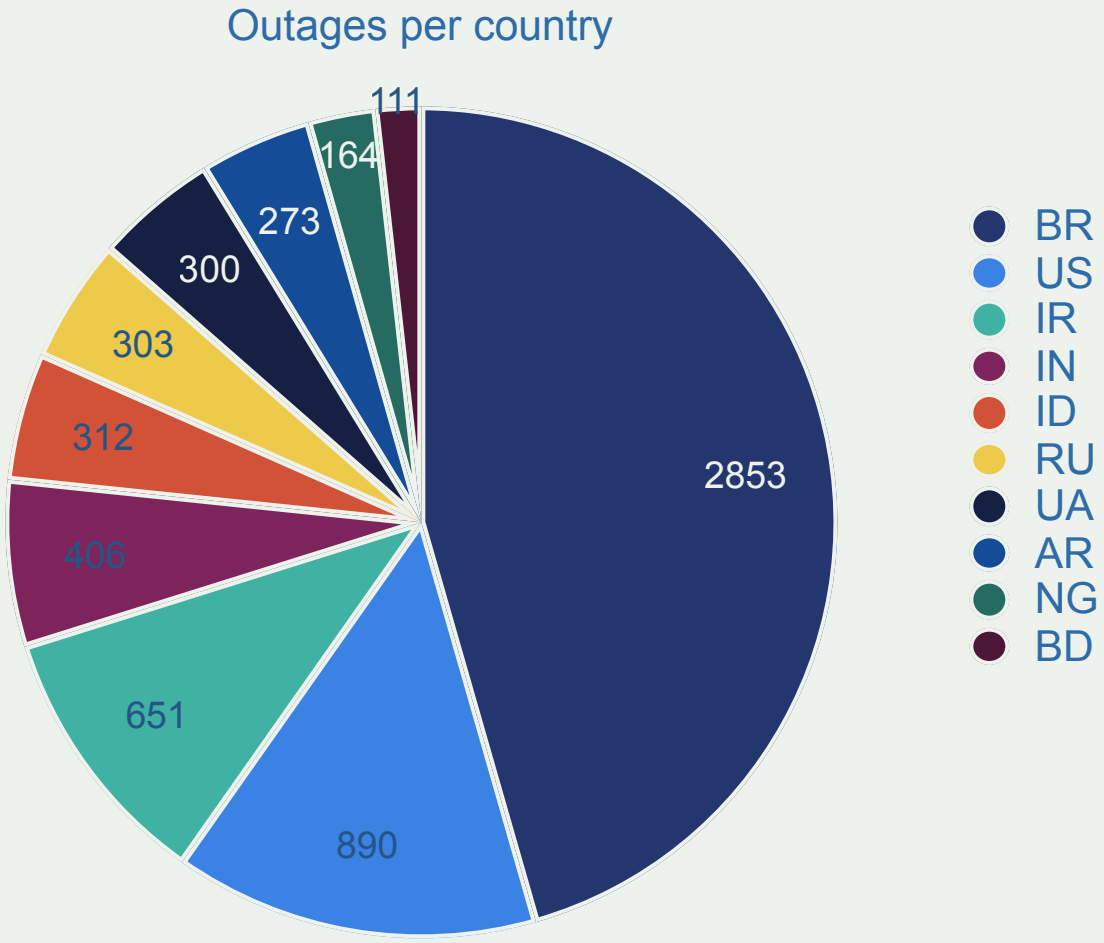
Global stats

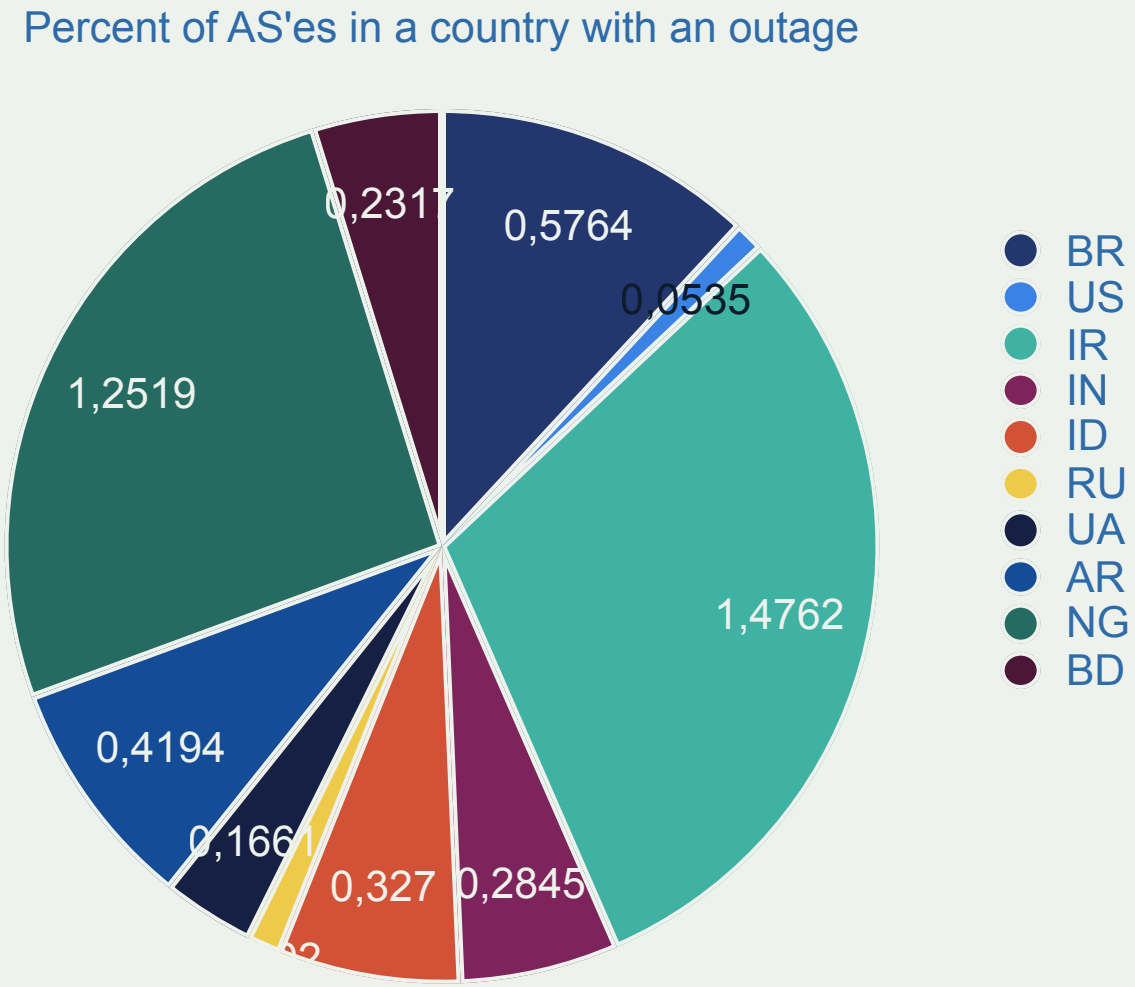
- 13,935 total incidents (either outages or attacks like route leaks and hijacks)
- Over 10% of all Autonomous Systems on the Internet were affected
- 3,106 Autonomous Systems were a victim of at least one routing incident
- 1,546 networks caused at least one incident



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

Outages

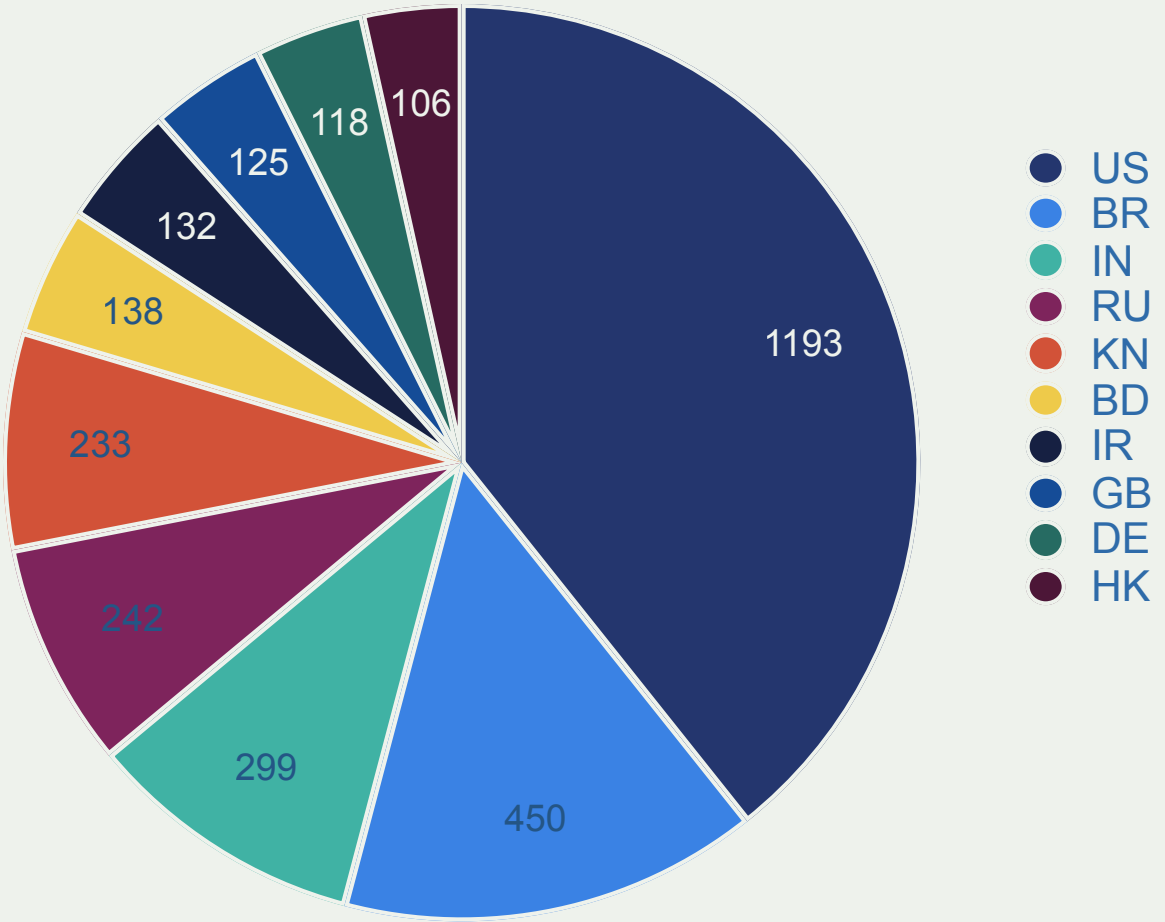




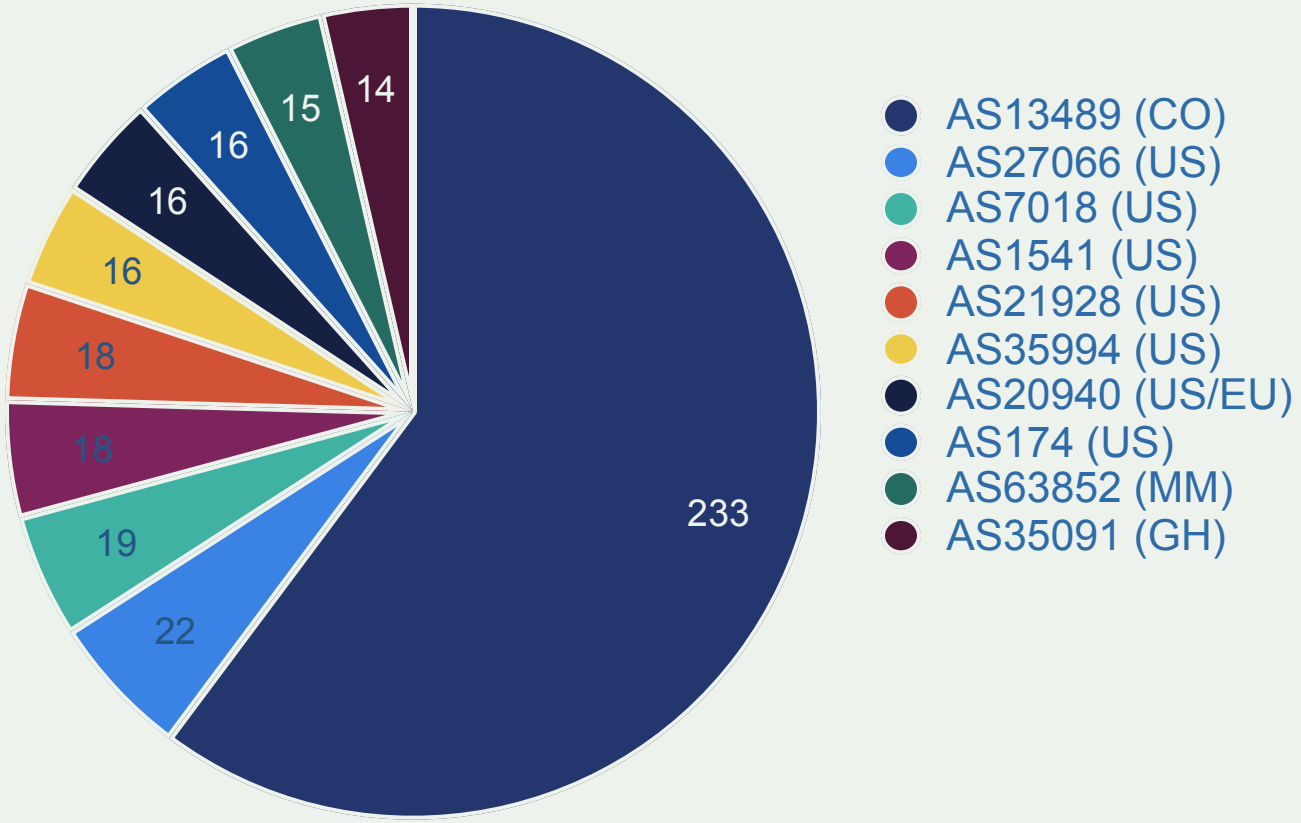
Source: https://www.bgpstream.com/

Potential victims

Incidents with a victim in a country, Top 10



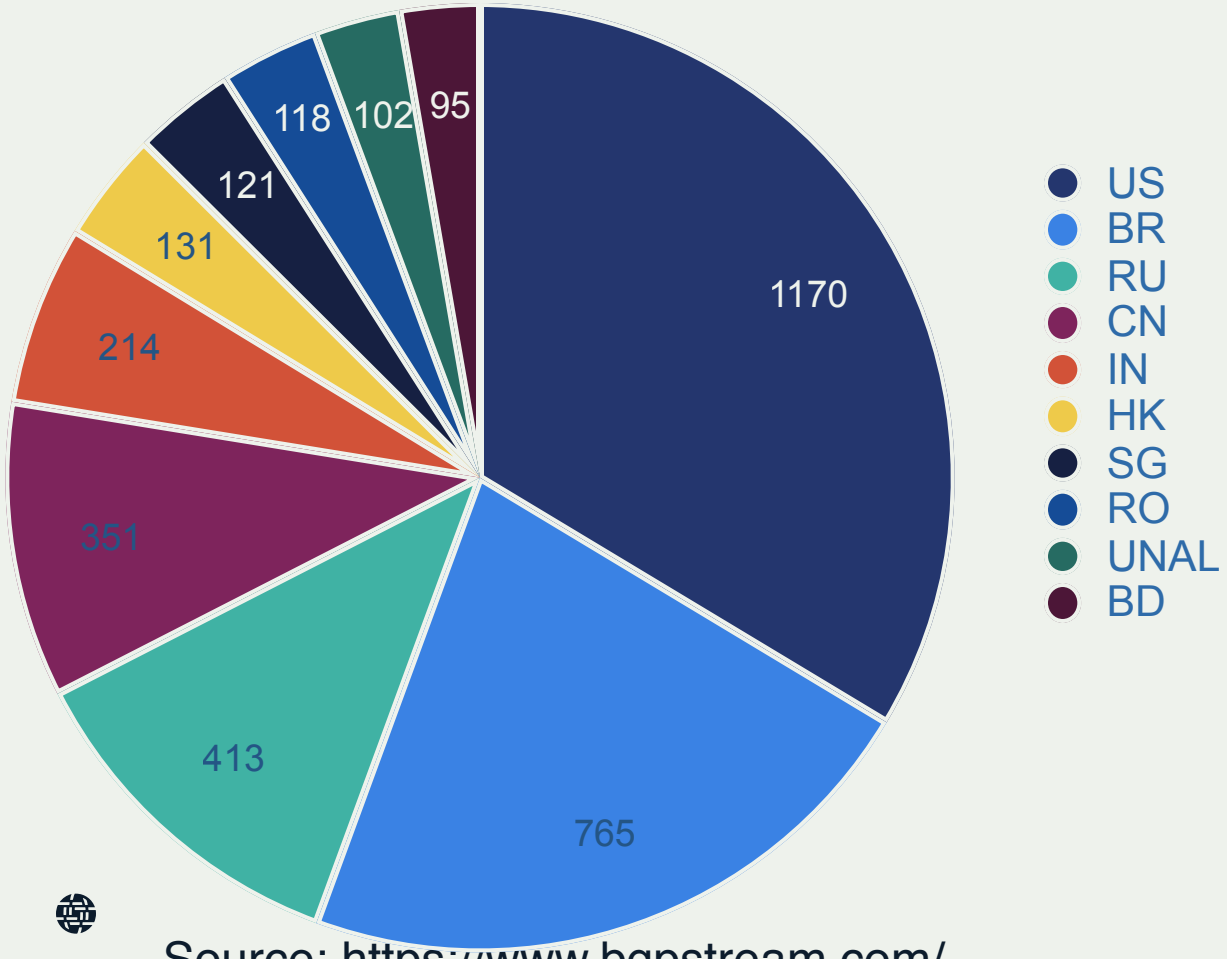
Top 10 victims of routing incidents



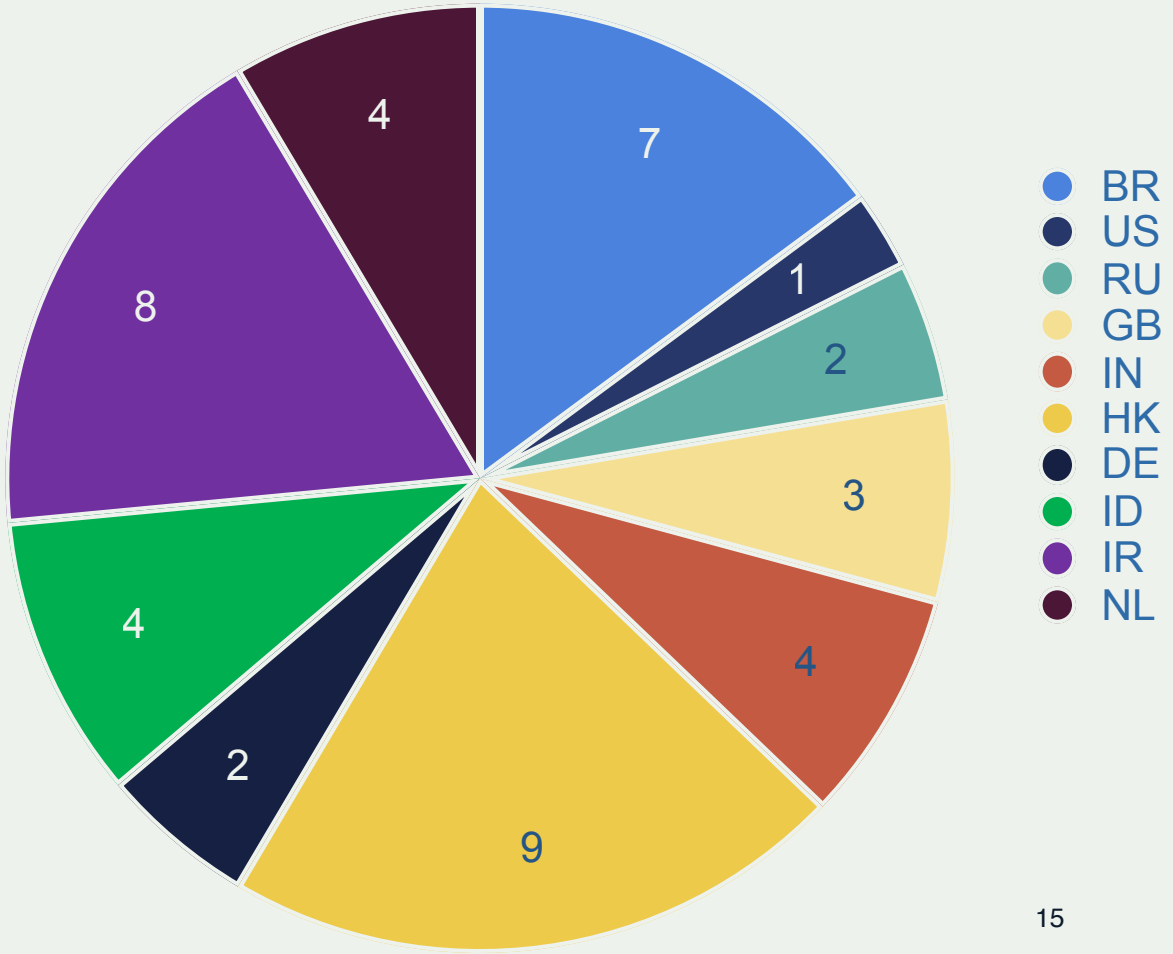
Source: https://www.bgpstream.com/

Potential culprits

Incidents with a culprit in a country, top 10



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



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

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 eliminate the most common routing threats

MANRS improves the security and reliability of the global Internet routing system, based on collaboration among participants and shared responsibility for the Internet infrastructure.

MANRS sets a new norm in routing hygiene

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

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

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.

Implementing best practices alleviates many routing concerns of security-focused enterprises and other customers.

Everyone Benefits

Joining MANRS means joining a community of security-minded network operators committed to making the global routing infrastructure more robust and secure.

Consistent MANRS adoption yields steady improvement, but we need more networks to implement the actions and more customers to demand routing security best practices.

The more network operators apply MANRS actions, the fewer incidents there will be, and the less damage they can do.

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.

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 Implementation Guide

If you're not ready to join yet, implementation guidance is available to help you.

- Based on Best Current Operational Practices deployed by network operators around the world
- https://www.manrs.org/bcop/

Mutually Agreed Norms for Routing Security (MANRS) Implementation Guide

Version 1.0, BCOP series
Publication Date: 25 January 2017

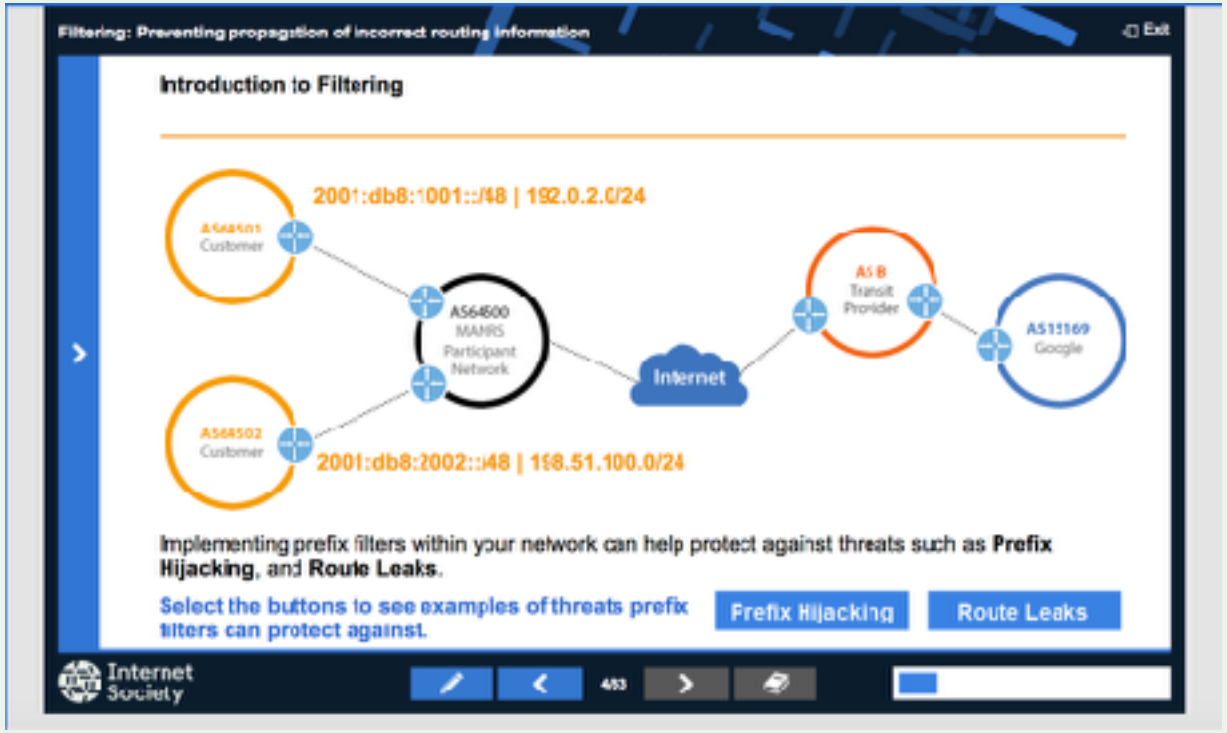
MANRS Training Modules

6 training modules based on information in the Implementation Guide.

Walks through the tutorial with a test at the end of each module.

Working with and looking for partners that are interested in integrating it in their curricula.

https://www.manrs.org/tutorials



What's Next: MANRS IXP Partnership 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?

- Technical measures: Route Server with validation, alerting on unwanted traffic, providing debugging and monitoring tools
- Social measures: MANRS ambassadors, local audit as part of the on-boarding process
- A development team is working on a set of useful actions

LEARN MORE:
https://www.manrs.org

Thank you.

Andrei Robachevsky
robachevsky@isoc.org

manrs.org