MANRS

Mutually Agreed Norms for Routing Security

manrs@isoc.org

Insecurity by Design

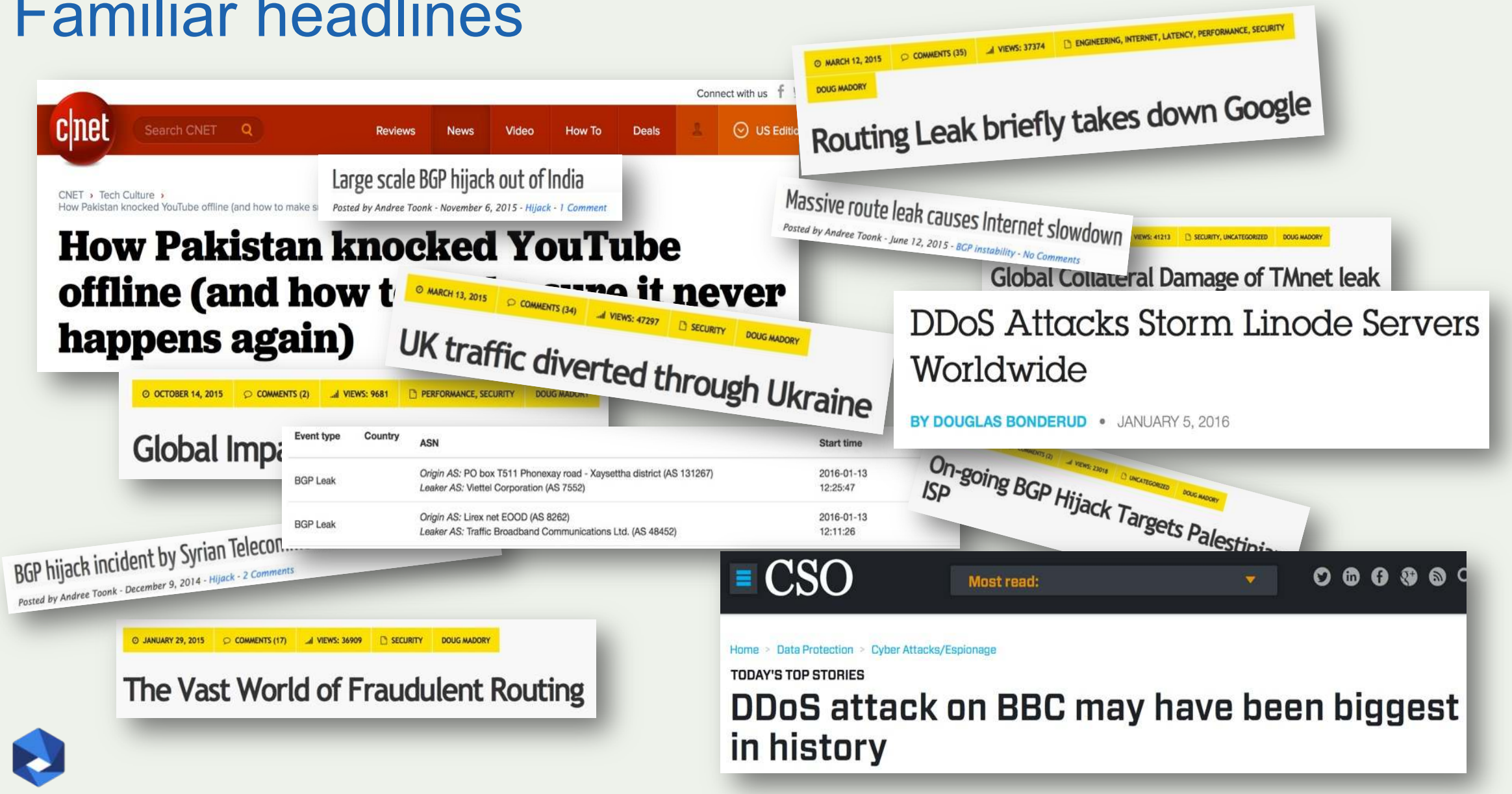
When the Internet was developed, they didn’t build in security by design.

The objective was resilience, simplicity and ease of deployment

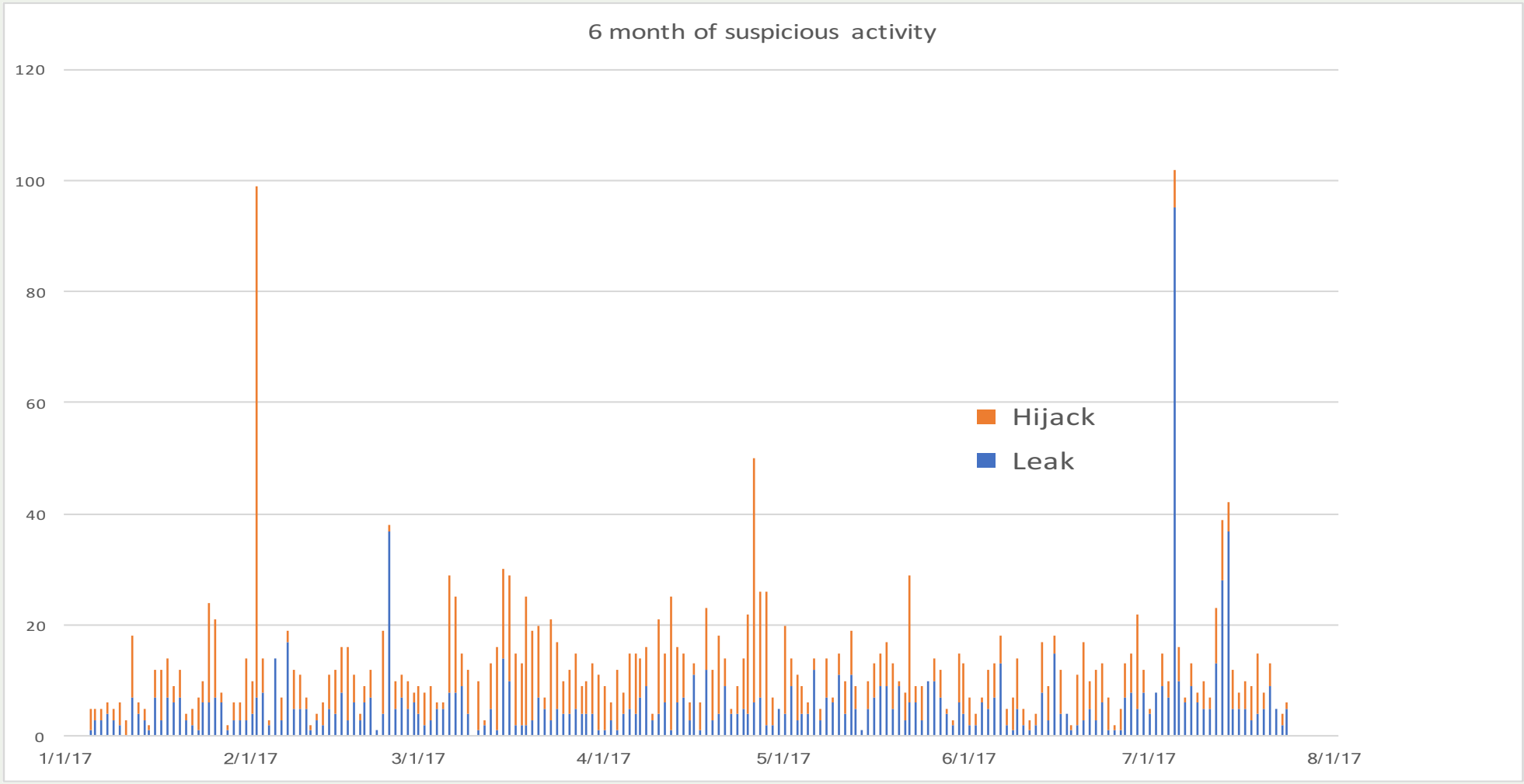
That created the Internet as the best effort, interdependent, general purpose network of networks supporting permission-less innovation.

While these qualities have made the Internet so successful, they also contribute to many of its security issues.

Familiar headlines



No Day Without an Incident



http://bgpstream.com/

The routing system is constantly under attack

- 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/

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*
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.	*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*

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

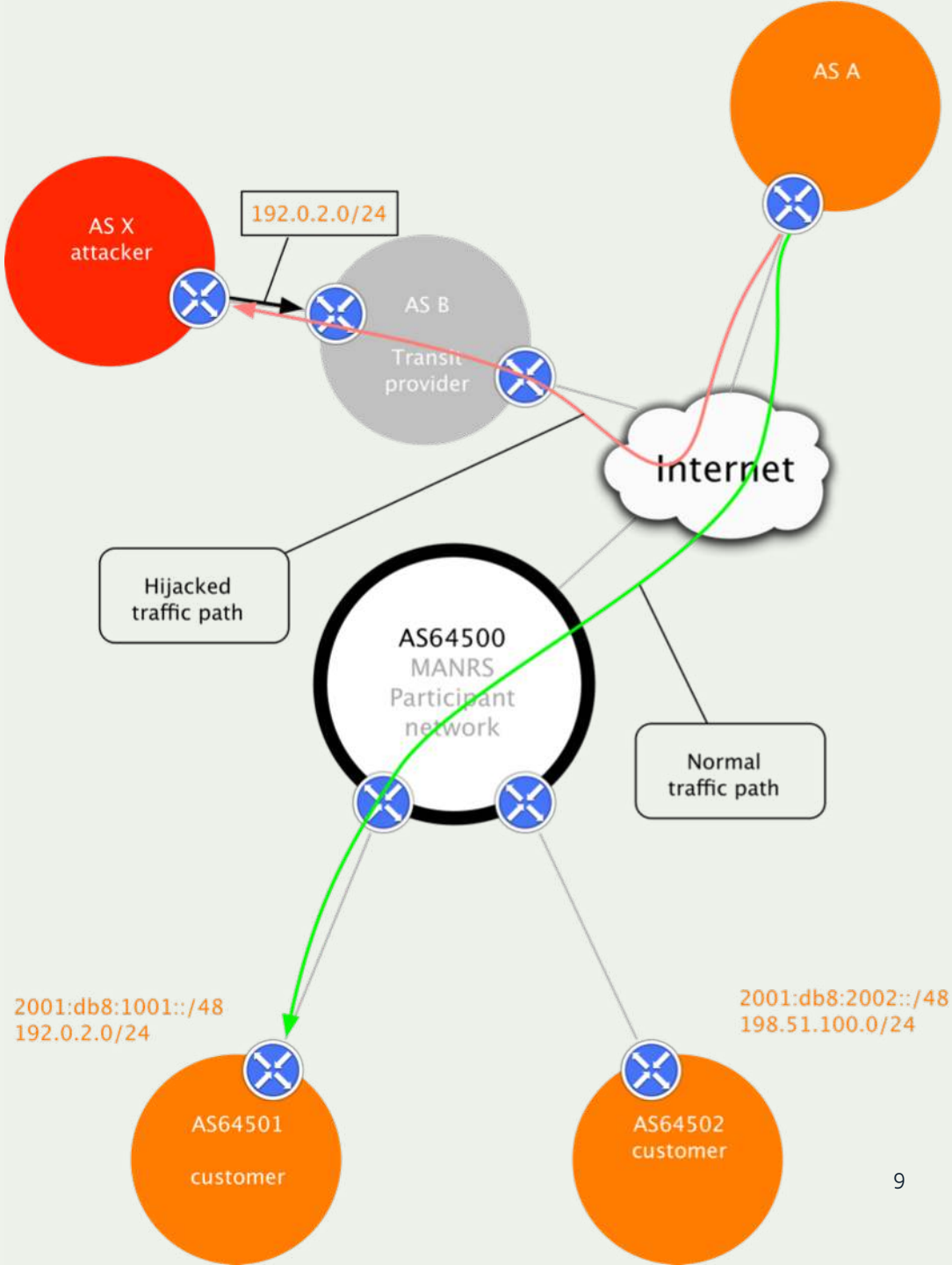
Border Gateway Protocol (BGP) is based entirely on trust between networks

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

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.

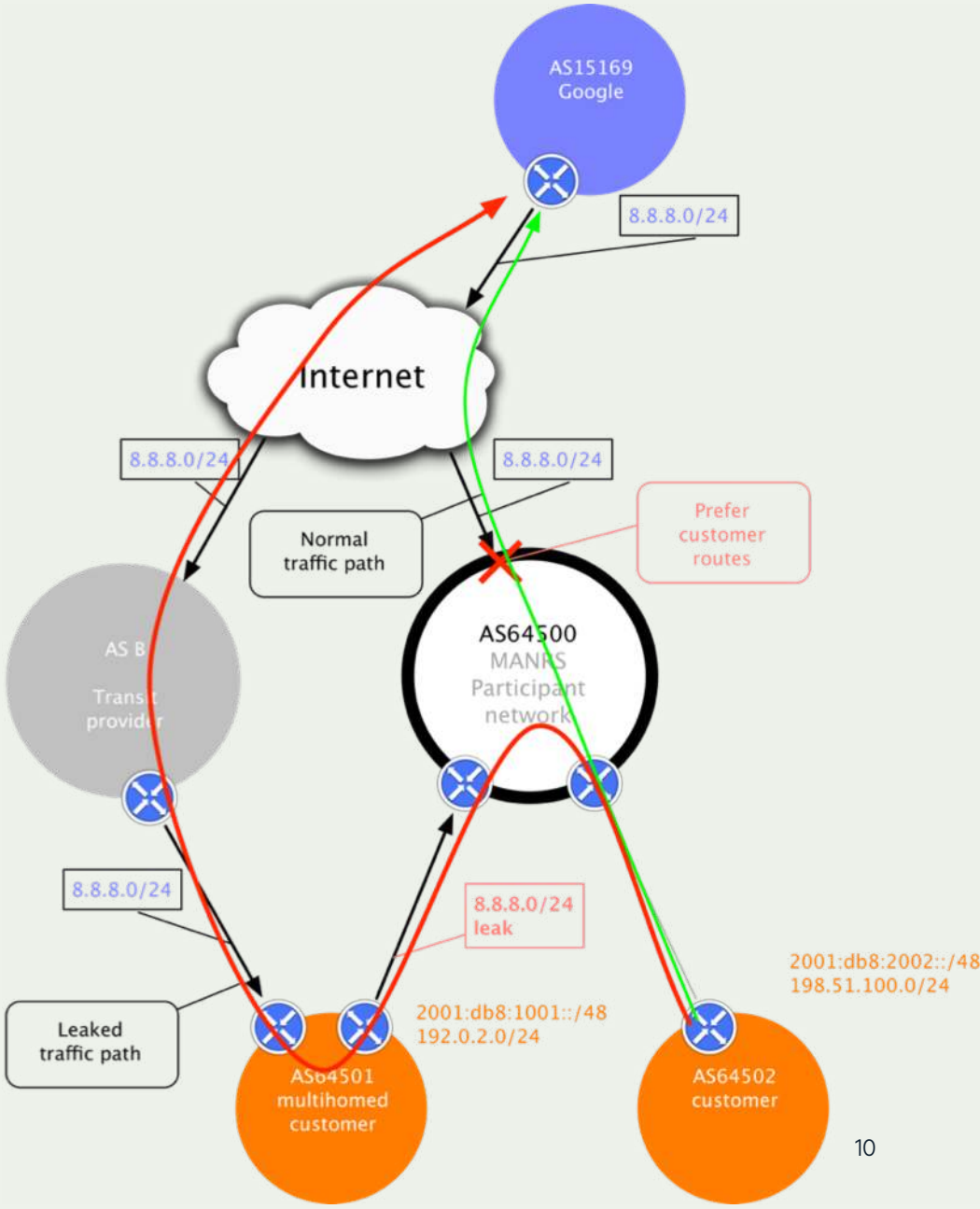
Example: *The 2008 YouTube hijack; an attempt to block Youtube through route hijacking led to much of the traffic to Youtube being dropped around the world (https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study)*



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/)*

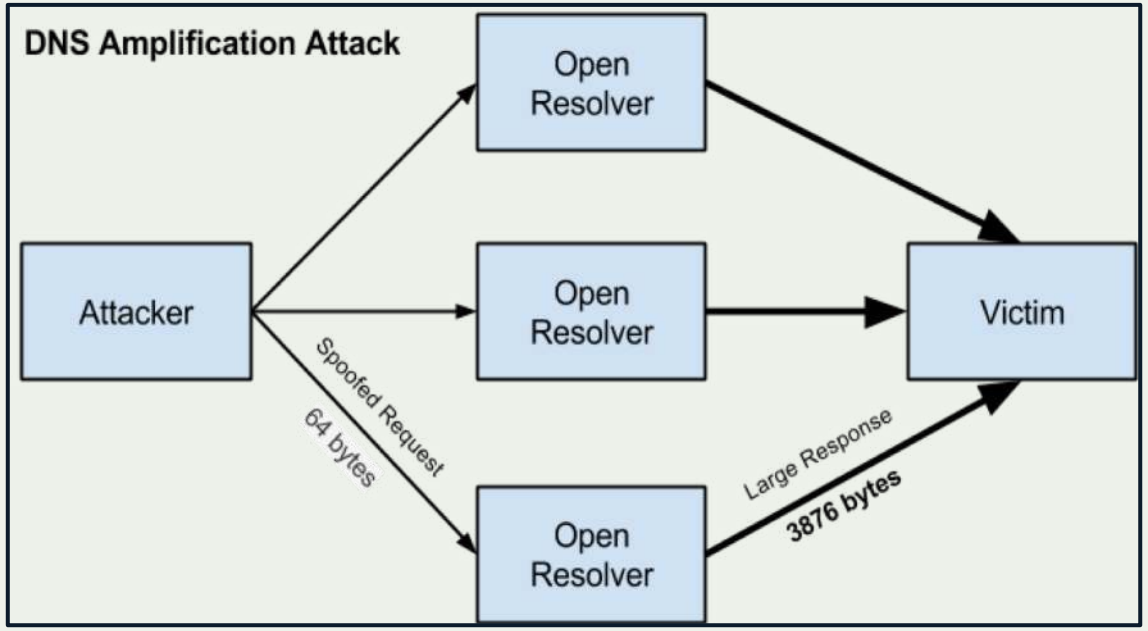


IP Address Spoofing

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

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 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

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.

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.

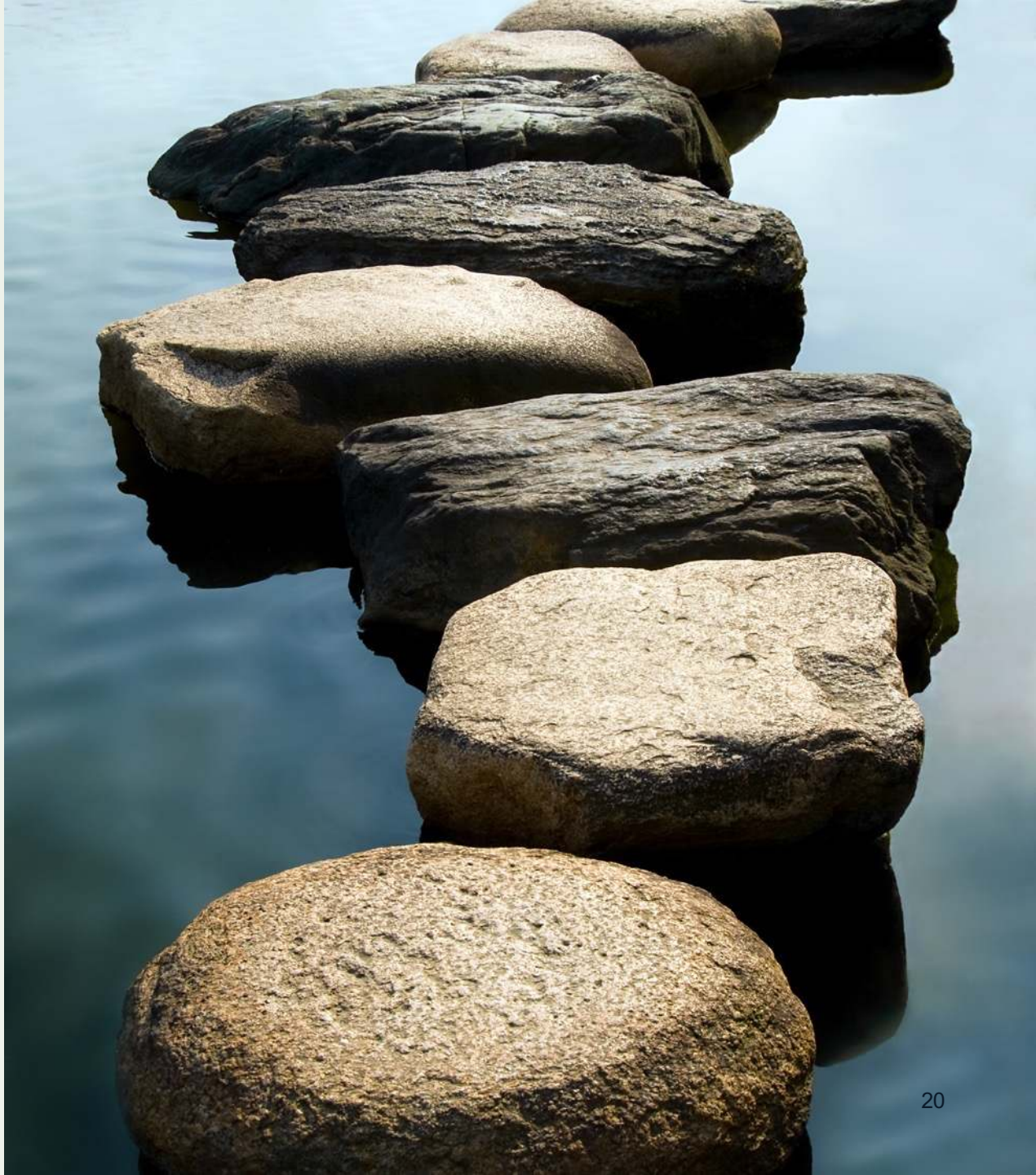
The more network operators apply MANRS actions, the fewer incidents there will be, and the less damage they can do.

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

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?

- 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 Programme – 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

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

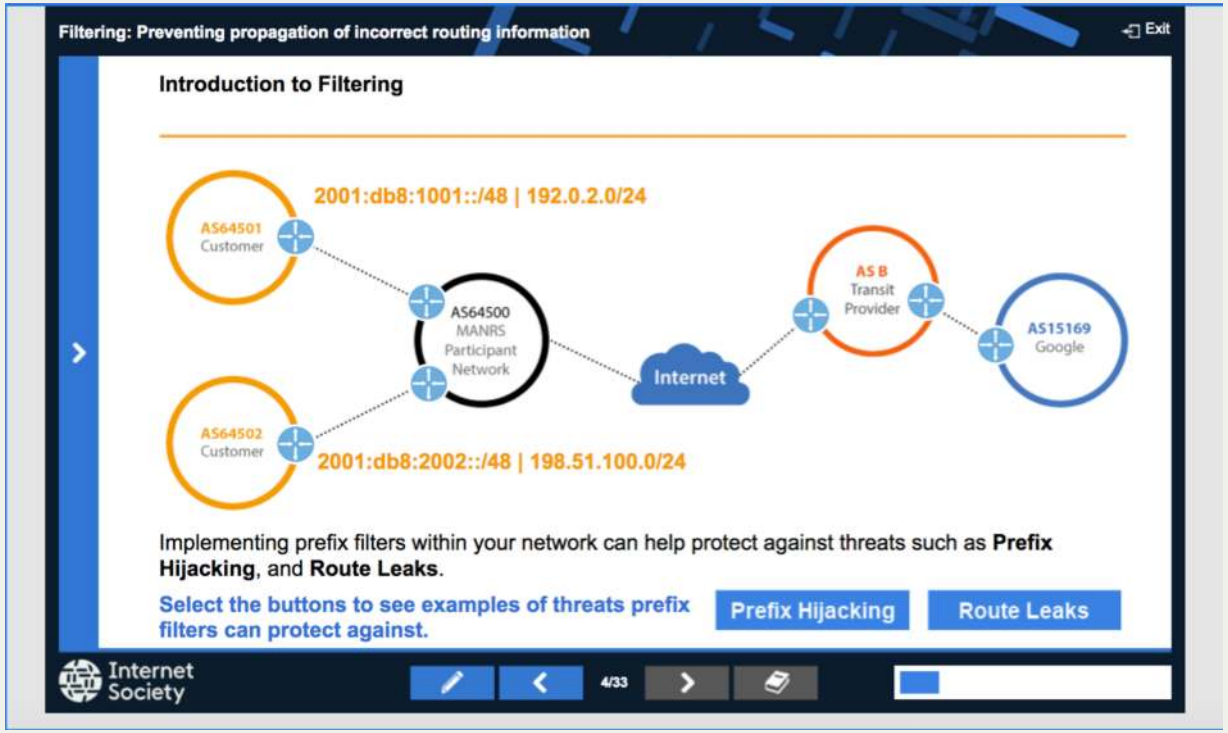
MANRS Training Modules

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



MANRS Training Modules

Module 1: Introduction to MANRS

What is MANRS, and why should you join? MANRS is a global initiative to implement crucial fixes needed to eliminate the most common routing threats. In this module you will learn about vulnerabilities of the Internet routing system and how four simple steps, called MANRS Actions, can help dramatically improve Internet security and reliability.

Module 2: IRRs, RPKI, and PeeringDB

This module helps you understand the databases and repositories MANRS participants should use to document routing policy and maintain contact information. You'll learn what database objects to use to document routing information related to your network and how to register information in the RPKI system. Finally, you will learn how to use the Peering DB and other databases to publish your contact information.

Module 3: Global Validation: Facilitating validation of routing information on a global scale

In this module, you will learn how to prevent incorrect routing announcements from your customers and your own network. The module explains how filters can be built, including the tools used to build them. It also shows how to signal to other networks which announcements from the network are correct.

Module 4: Filtering: Preventing propagation of incorrect routing information

This module will help you apply anti-spoofing measures within your network. After this module you will be able to identify points/devices in the network topology where anti-spoofing measures should be applied, identify adequate techniques to be used (for example, uRPF, or ACL filtering), configure your devices to prevent IP spoofing, and verify that the protection works.

Module 5: Anti-Spoofing: Preventing traffic with spoofed source IP addresses

This module is to understand how to create and maintain contact information in publicly accessible places. It explains why it is important to publish and maintain contact information, how to publish contact information to Regional Internet Registries (RIRs), Internet Routing Registries (IRRs), and PeeringDB, and what contact information you should publish to a company website.

Module 6: Coordination: Global communication between network operators

This module helps you understand how to enable others to validate route announcements originating from your network by documenting a Network Routing Policy. You'll learn what a Network Routing Policy is, how to document your organization's Network Routing Policy and make it publicly available in order to signal to other networks which announcements from your network are correct.

Training modules – an opportunity?

Can be taken by anyone at their own pace

Can also be done as part of a moderated class

- Using the Internet Society Inforum platform
- A virtual class of 10-20 interested individuals
- Periodic Zoom calls with Q&A
- Performance and completion tracking
- Train-the-trainer programme

MANRS Train-the-Trainer Programme

- A 4-week training course geared towards familiarizing future moderators with the MANRS requirements
- The course will also include components on how to effectively moderate online courses
- The course will be led by one of the Internet Society's Expert Moderators
- The Expert Moderator will be supported by a Subject Matter Expert (SME) with deep knowledge and experience in the implementation of the full set of the MANRS requirements

MANRS – you can help!

Some ideas

Work on a proposal to present MANRS to two stakeholders in your region

Create a 90 second video in your own language explaining the importance of MANRS for network operators and distribute via social media

Community training on MANRS and routing security: Webinars, training sessions, become a moderator for the online tutorial in your region, promote the tutorials

Translate MANRS materials into more languages

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

Brainstorming session

A video says more than a thousand words

Create a script for a 60 second video on routing security and how MANRS can reduce the most common threats

Record the video using a smartphone

Be prepared to share the video with the group – tell us how you decided on the most important messages to include

Explain how you would use a video in your region to interest network operators in MANRS

The winning table gets MANRS T-shirts!

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

Thank you.

Andrei Robachevsky

robachevsky@isoc.org

manrs.org

2017 in review: 14000 routing incidents

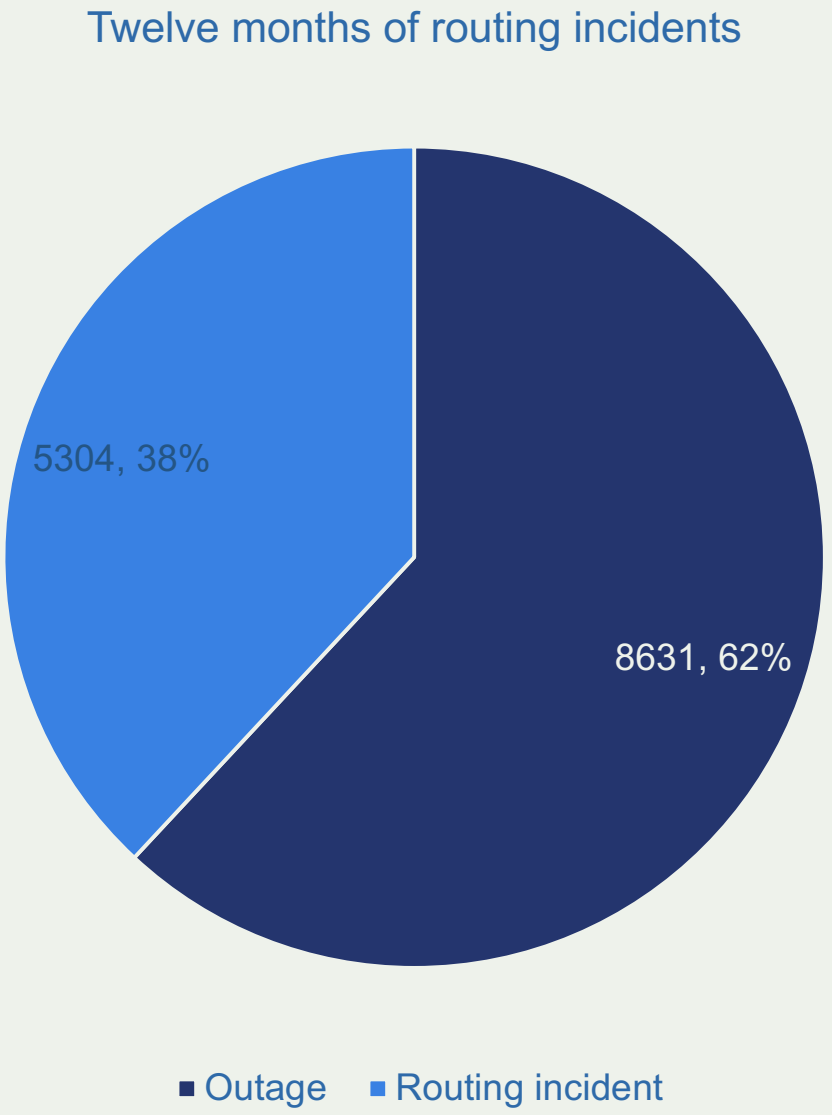
Statistics of routing incidents generated from BGPStream data

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

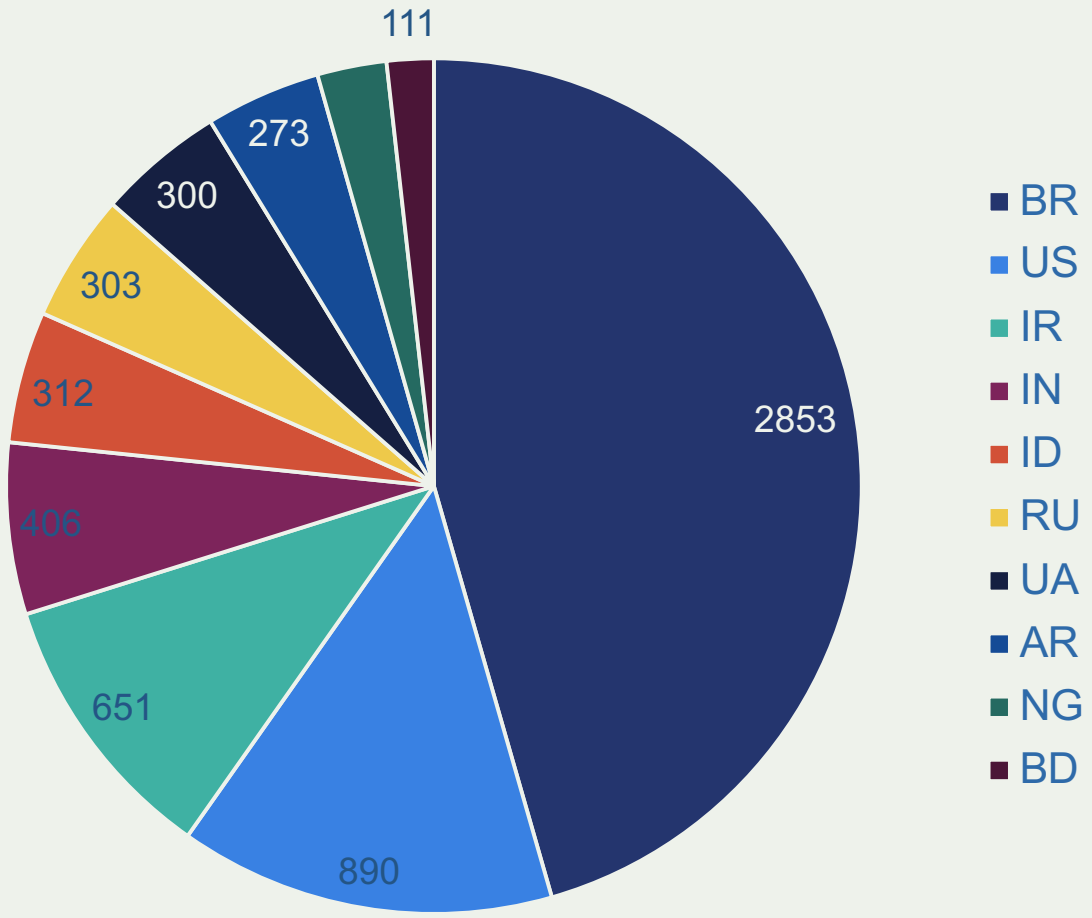
- 13,935 total incidents (either outages or attacks like route leaks and hijacks)
- Over 10% of all Autonomous Systems on the Internet were affected
- 3,106 Autonomous Systems were a victim of at least one routing incident
- 1,546 networks caused at least one incident



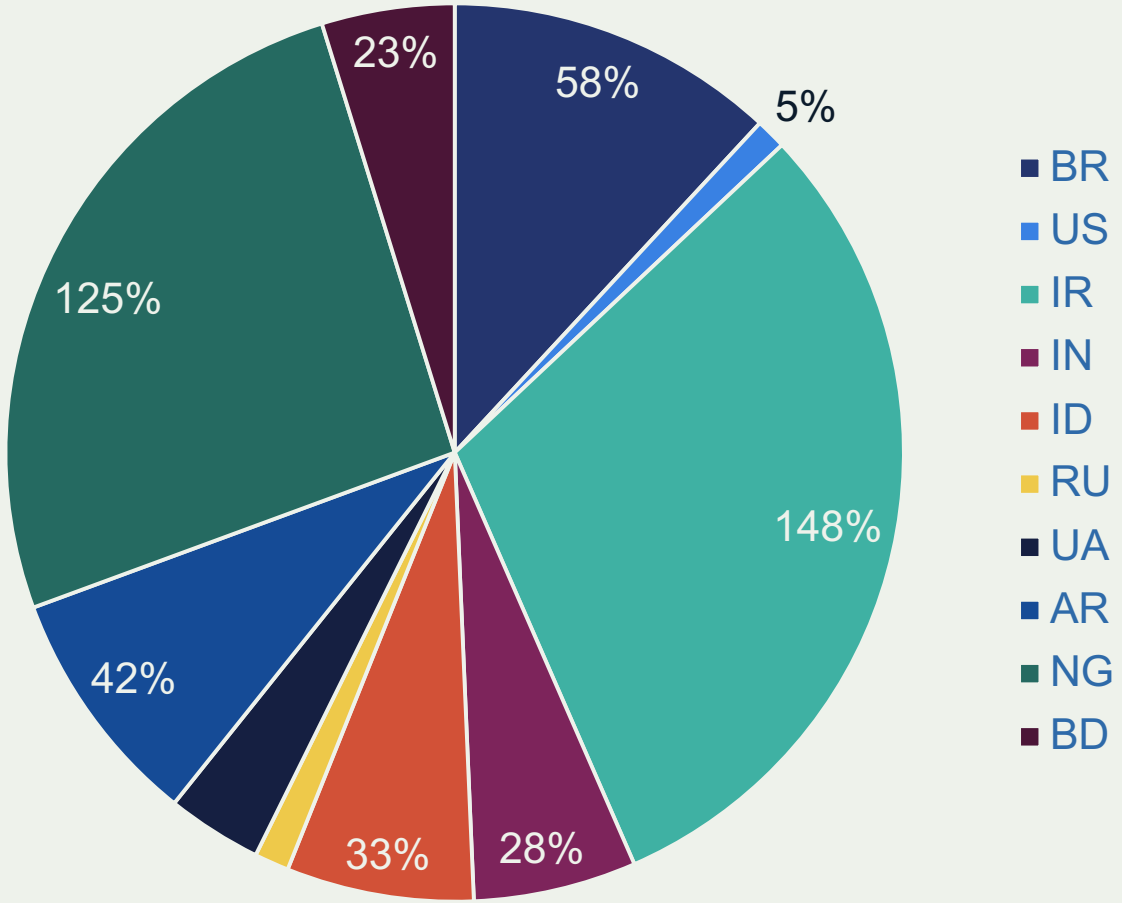
Source: https://www.bgpstream.com/

Outages

Outages per country



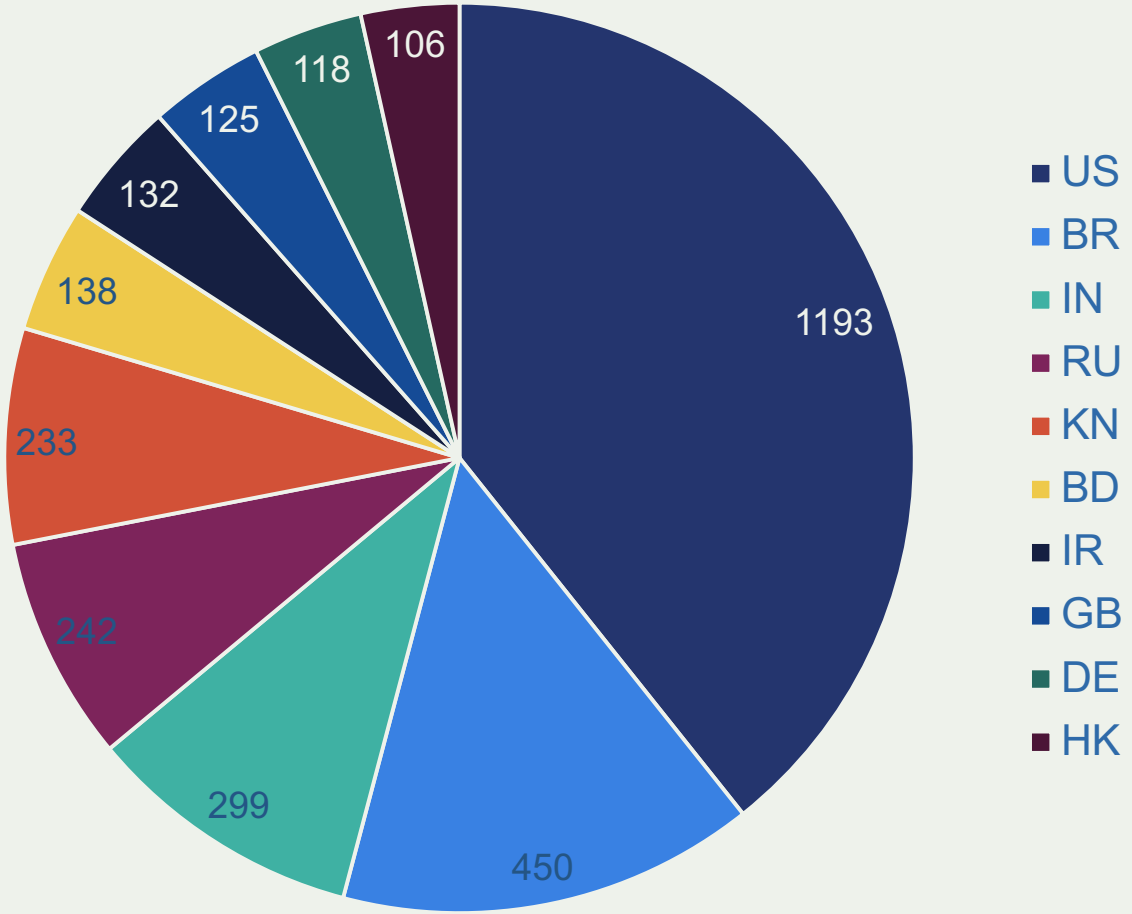
Percent of AS'es in a country with an outage



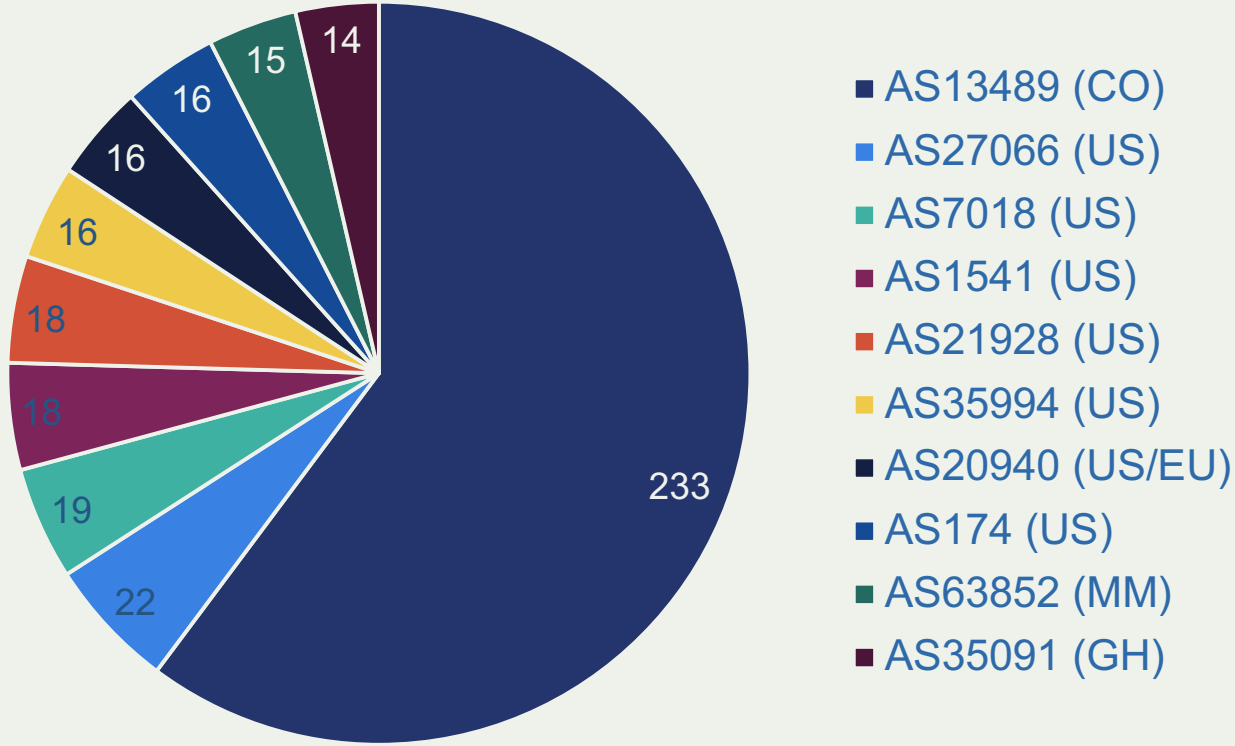
Source: https://www.bgpstream.com/

Potential victims

Incidents with a victim in a country, Top 10



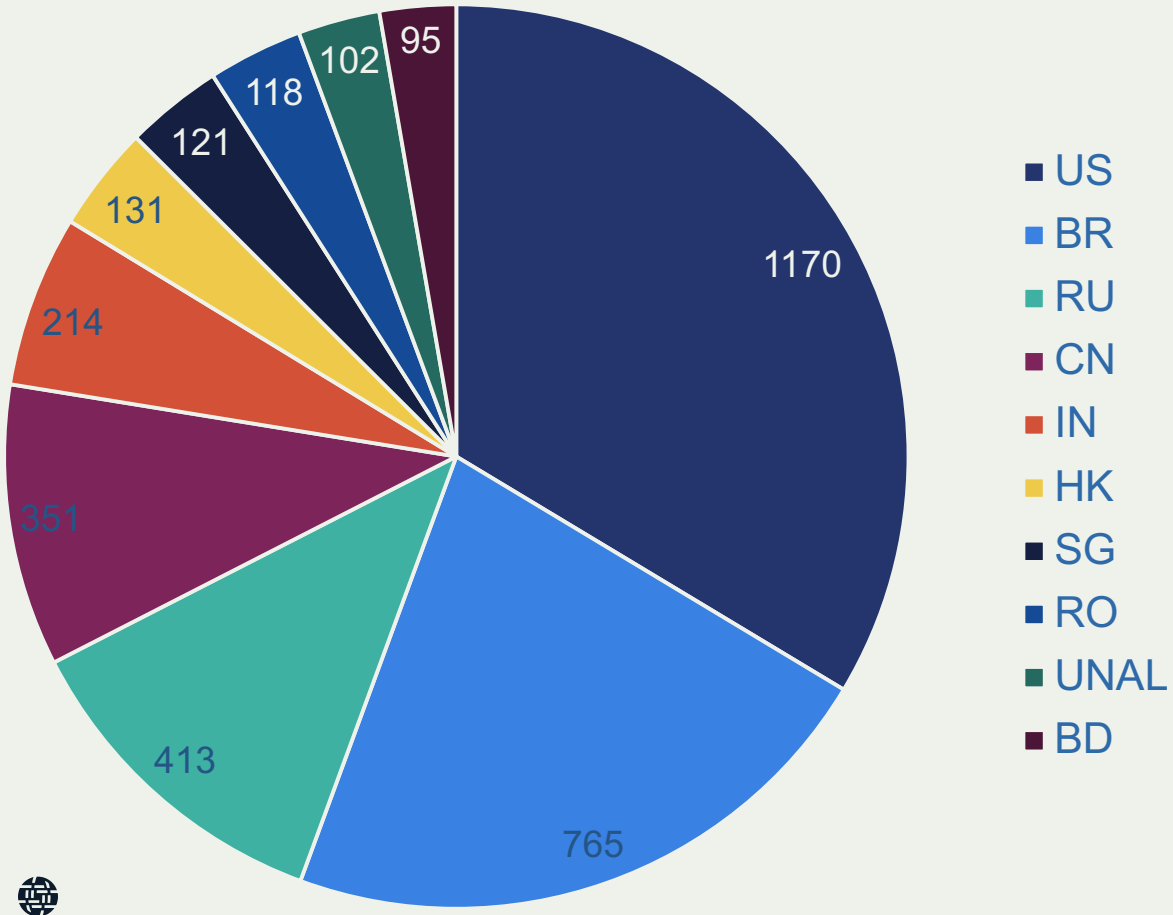
Top 10 victims of routing incidents



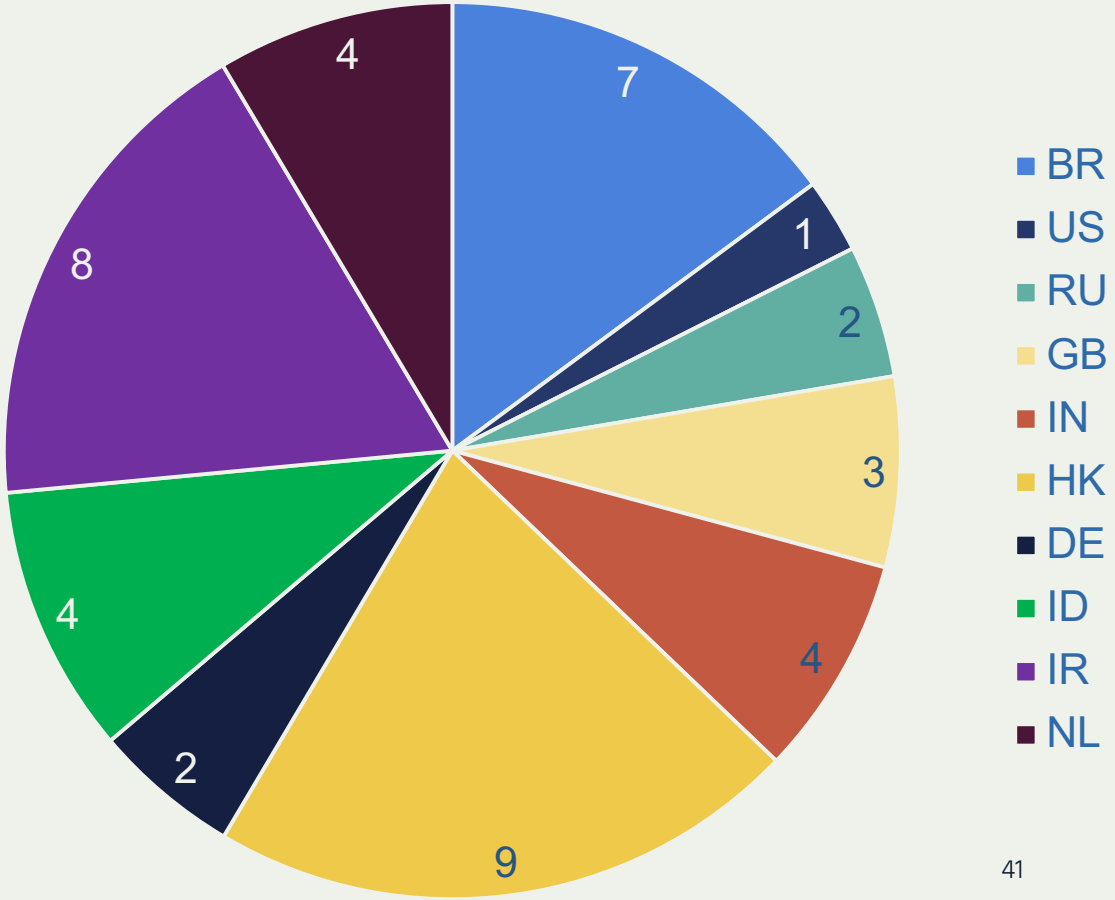
Source: https://www.bgpstream.com/

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/