MANRS

Mutually Agreed Norms for Routing Security

Aftab Siddiqui

siddiqui@isoc.org

The Problem

A Routing Security Overview

Routing Incidents are Increasing

In 2017 alone, 14,000 routing outages or attacks – such as hijacking, leaks, and spoofing – led to a range of problems including stolen data, lost revenue, reputational damage, and more.

About 40% of all network incidents are attacks, with the mean duration per incident lasting 19 hours.

Incidents are global in scale, with one operator's routing problems cascading to impact others.

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

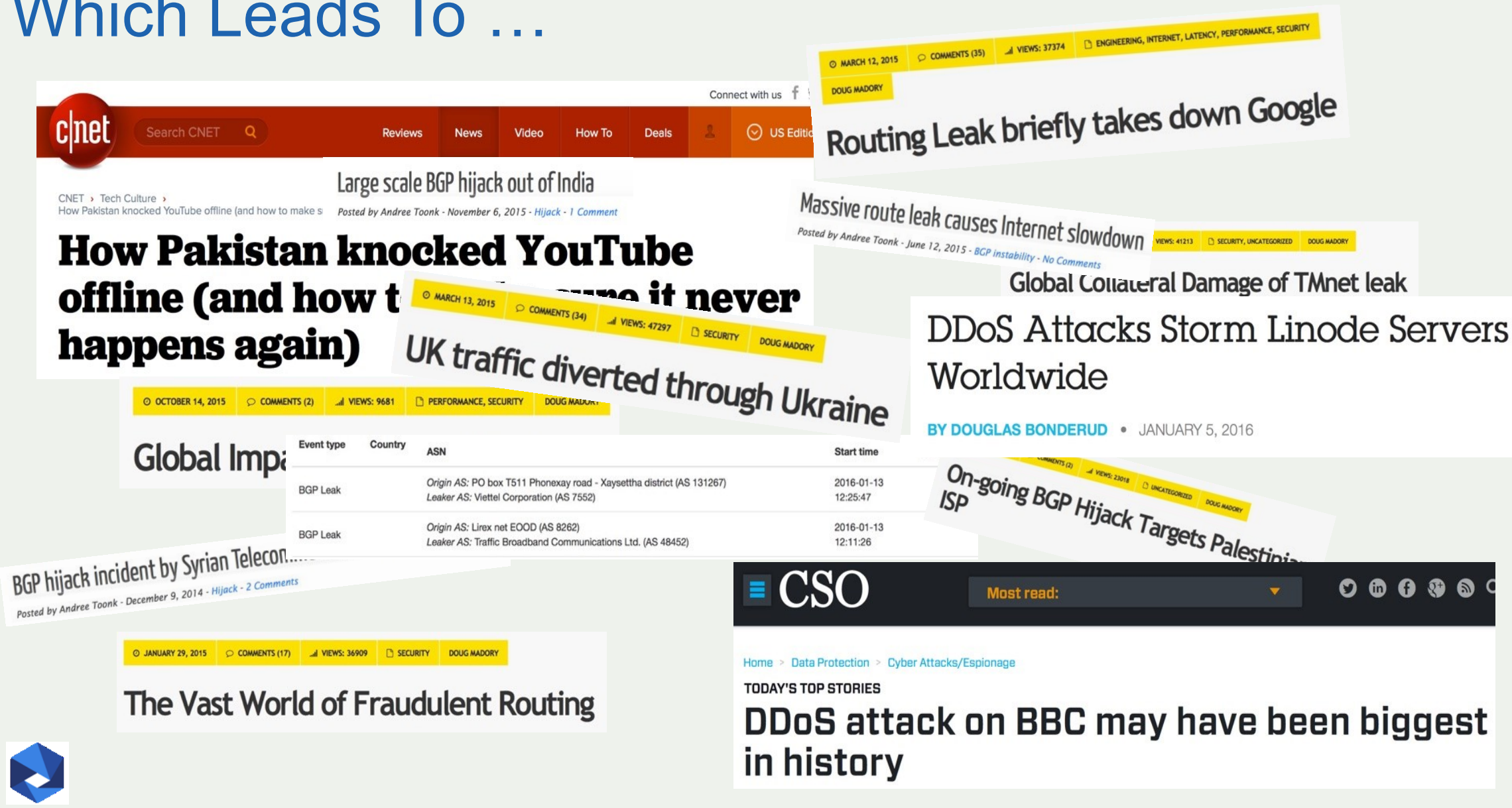
Routing Incidents Cause Real World Problems

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.

Which Leads To …



EDITION: AS

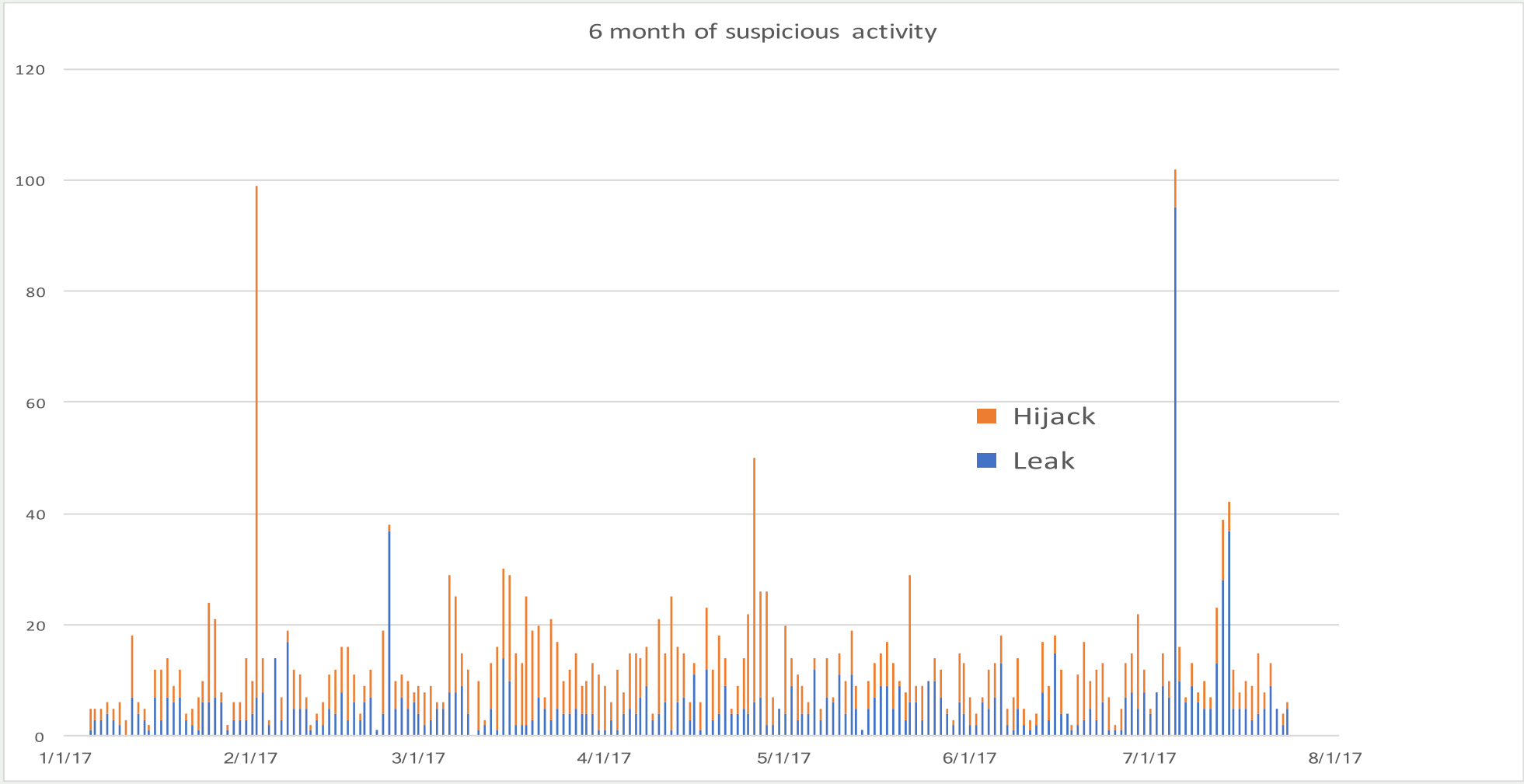
ZDNet

SECURITY CLOUD STORAGE CXO HARDWARE MICROSOFT INNOVATION MORE NEWSLETTERS

MUST READ I ASKED APPLE FOR ALL MY DATA. HERE'S WHAT WAS SENT BACK

AWS traffic hijack: Users sent to phishing site in two-hour cryptocurrency heist

No Day Without an Incident



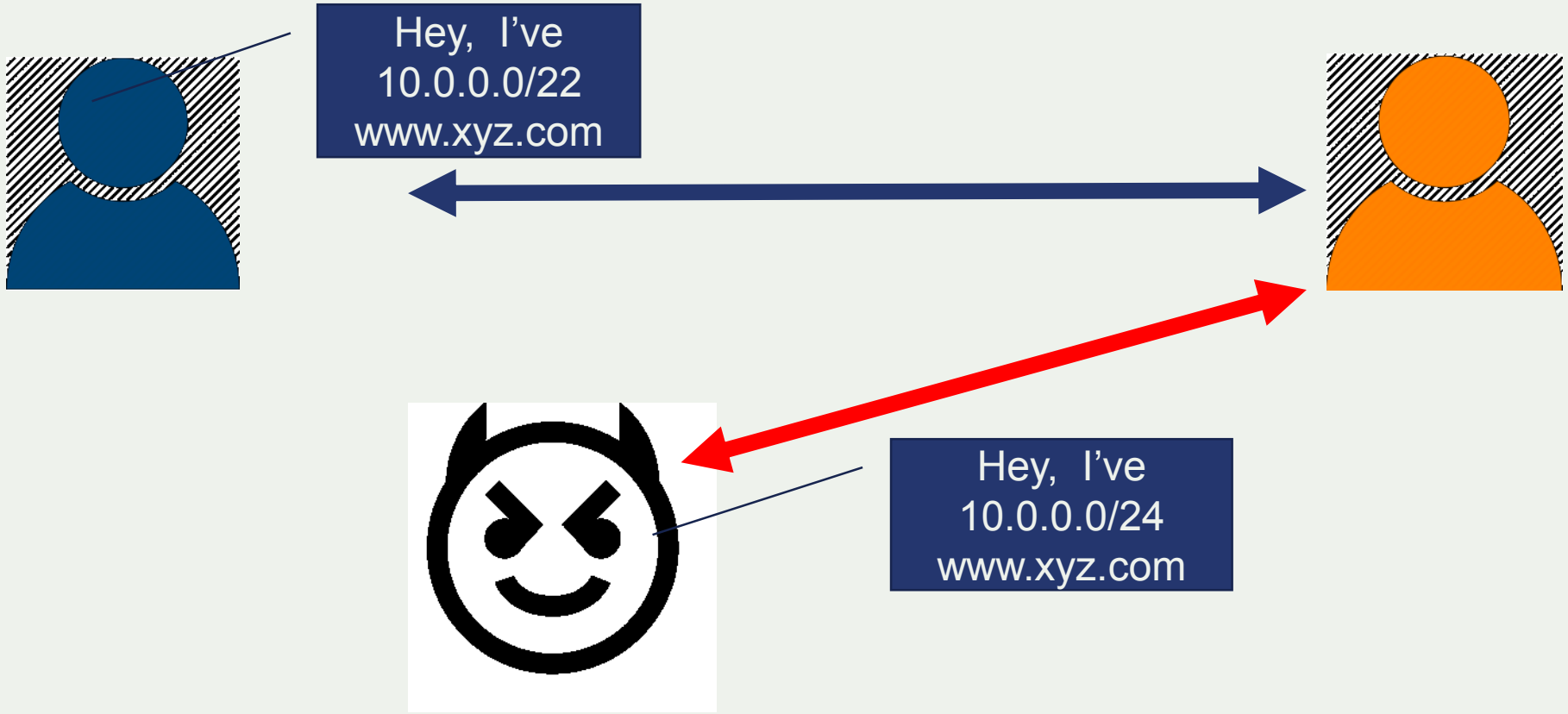
http://bgpstream.com/

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

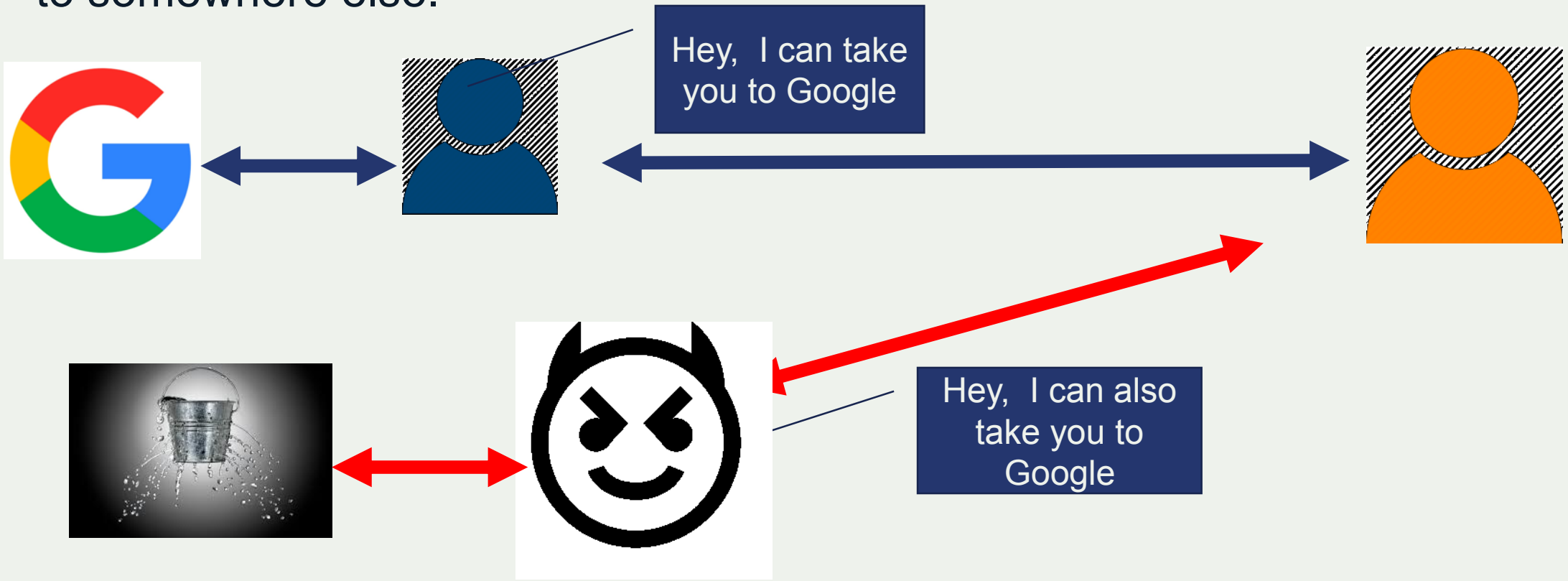
Route/Prefix Hijacking

Somebody else sending BGP messages that contain (part of) your IP address ranges



Route/Prefix Leaking

Route leaks involve the illegitimate advertisement of prefixes, blocks of IP addresses, which propagate across networks and lead to incorrect or suboptimal routing. A router misconfiguration directing internet traffic from its intended path to somewhere else.

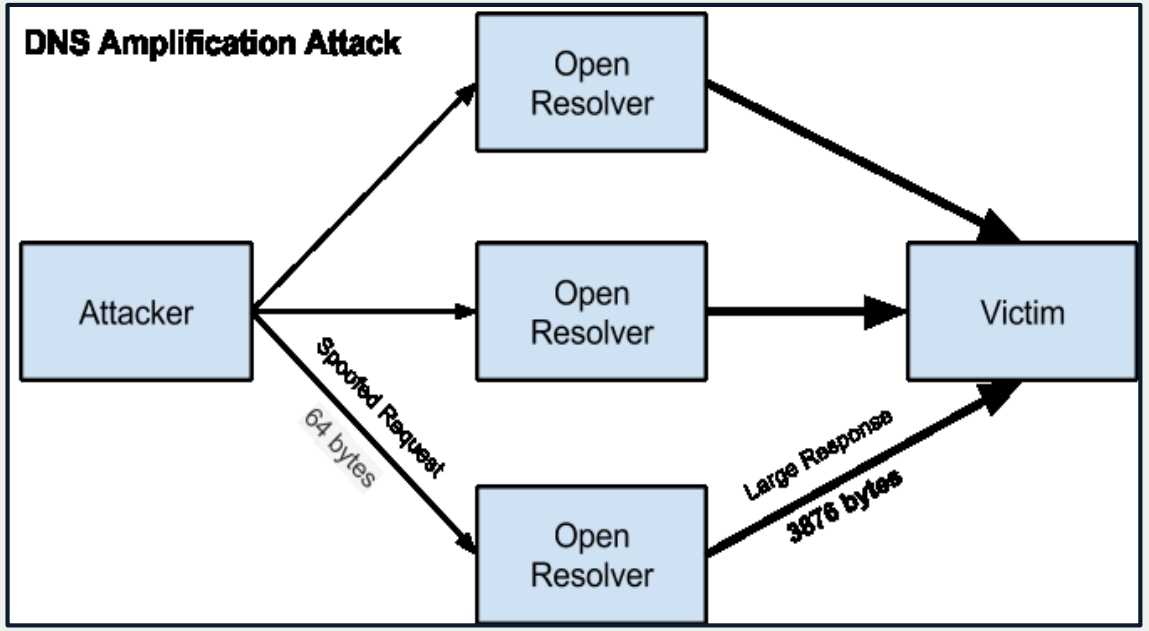


IP Address Spoofing

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.

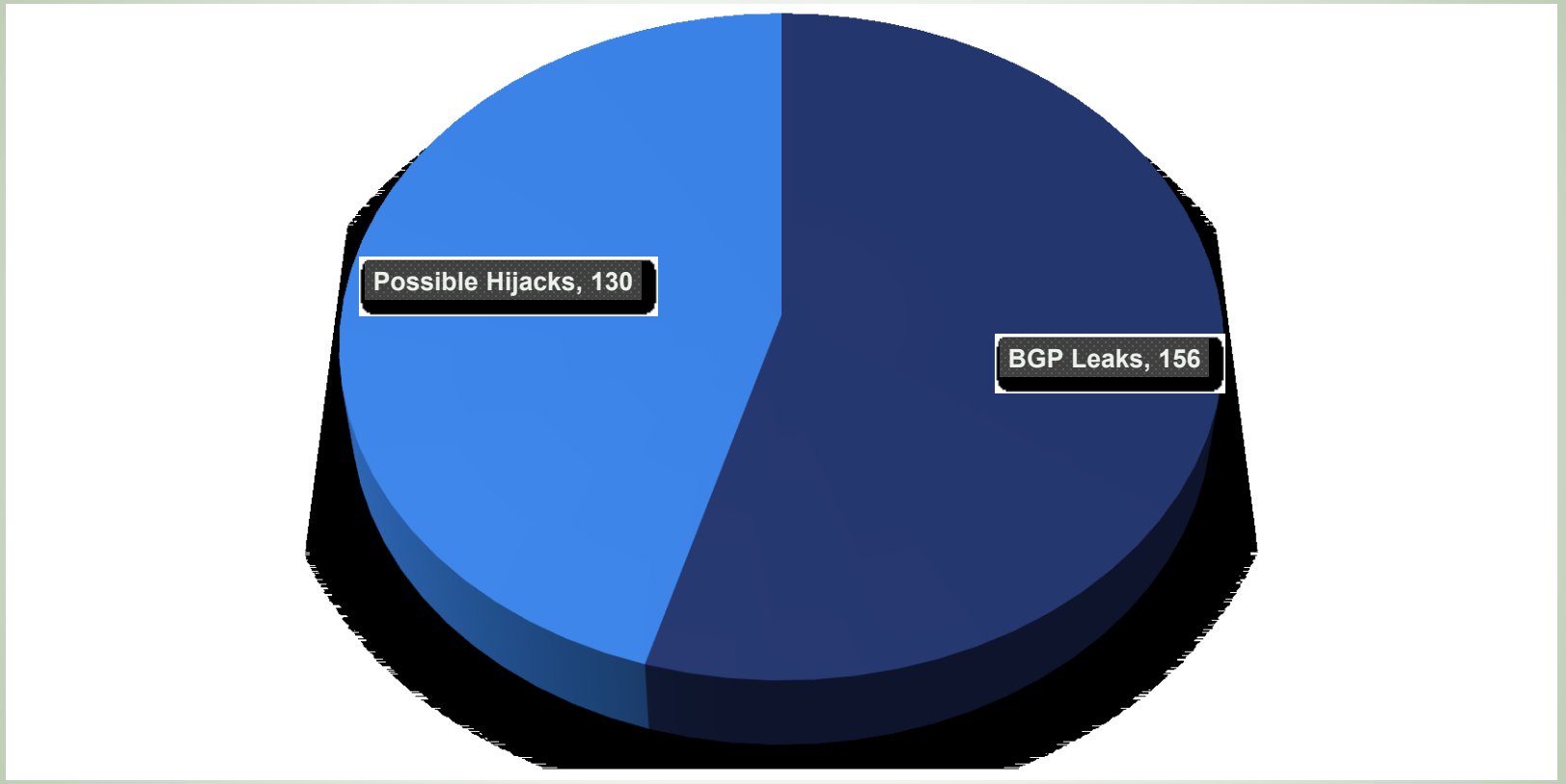
Example: DNS amplification attack. By sending multiple spoofed requests to different DNS resolvers, an attacker can prompt many responses from the DNS resolver to be sent to a target, while only using one system to attack.

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).



Routing Security Incidents: 19th May 2018

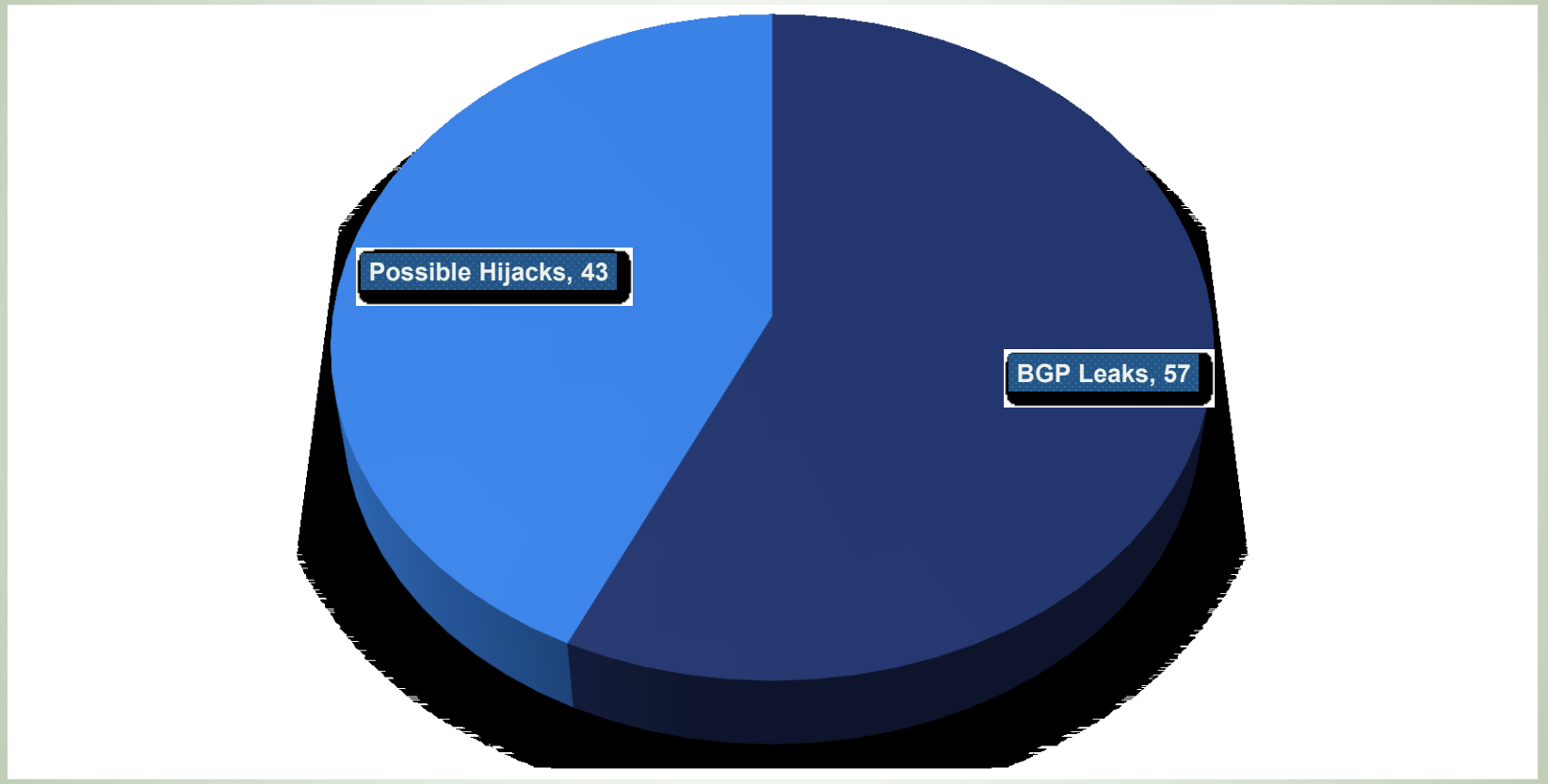
Total Incidents: 286



Source: www.bgpstream.com

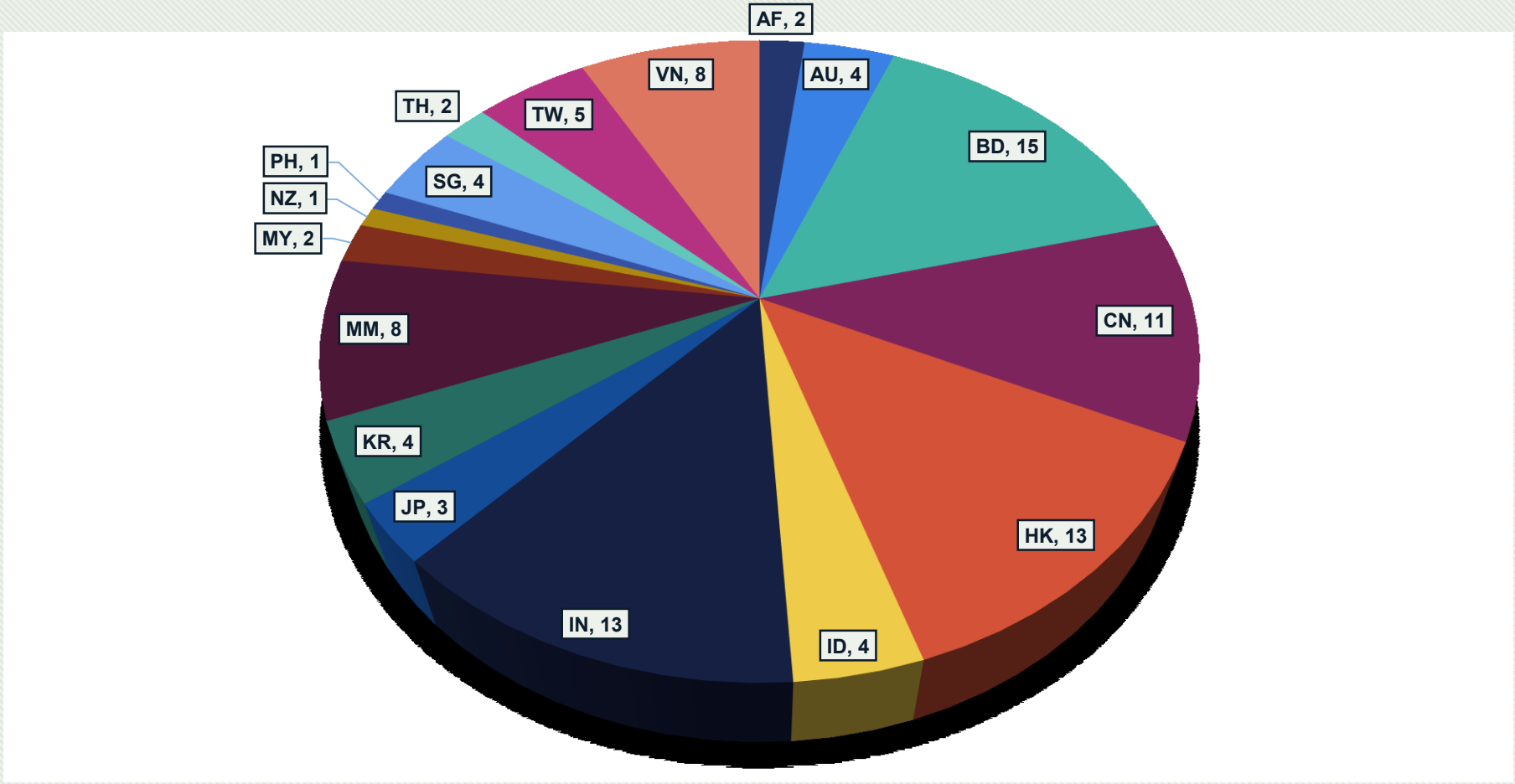
Routing Security Incidents: 19th May 2018

Total APAC Incidents: 100



Source: www.bgpstream.com

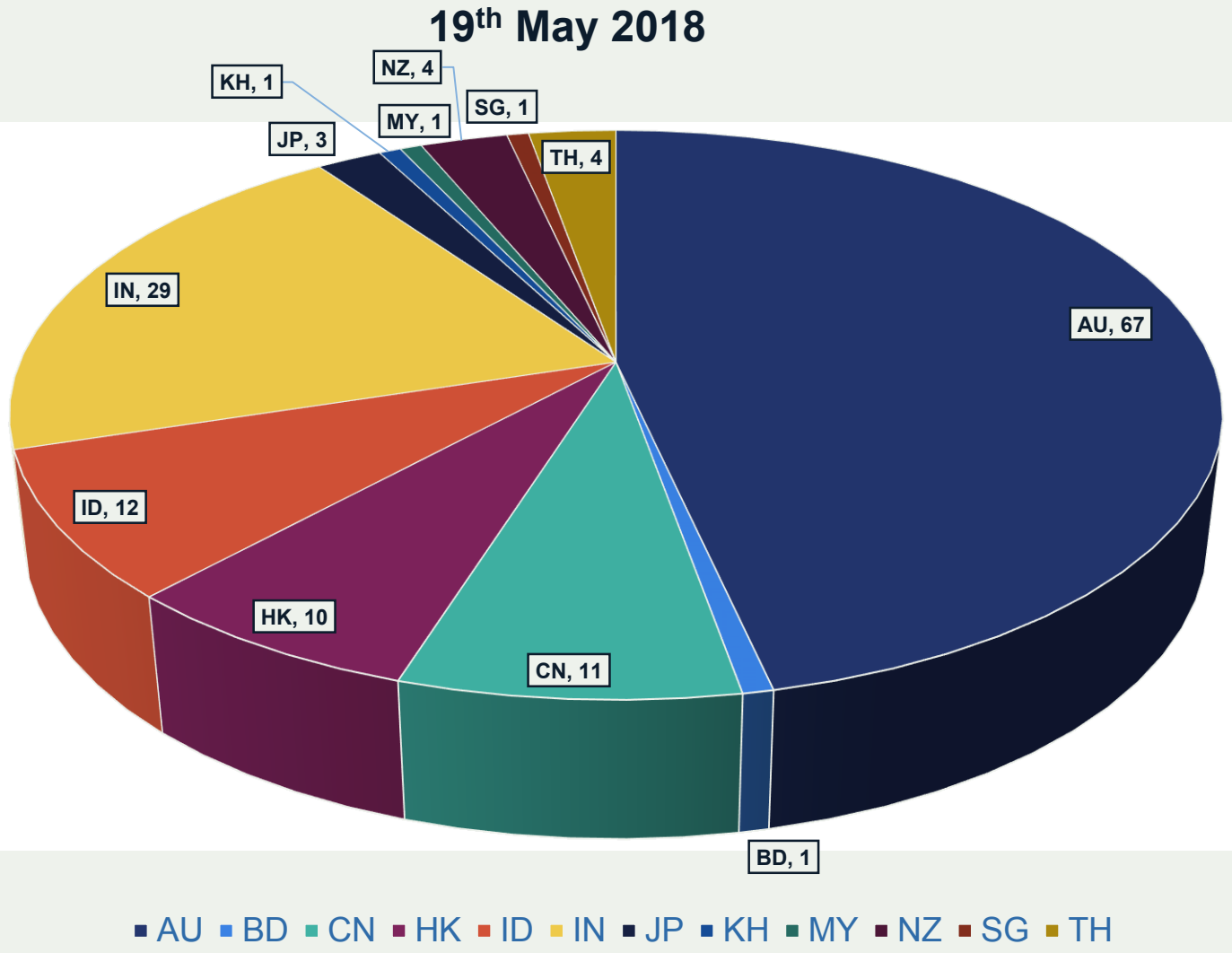
Routing Security Incidents: 19th May 2018



Source: www.bgpstream.com

Bogon Advertisement

A bogon route is a type of route which shouldn't exist on the global Internet. More specifically, "bogon" (derived from the word "bogus") refers to an advertisement for a prefix within a reserved or otherwise unallocated IP network.



Source: www.cidr-report.org

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.

The Solution: 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.

Mutually Agreed Norms for Routing Security

MANRS defines four simple but concrete actions that network operators must implement to dramatically 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 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

Benefits of Improved Routing Security

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.

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

Why SERVICE PROVIDERS Should Join MANRS

To help solve global network problems

- Lead by example to improve routing security and ensure a globally robust and secure routing infrastructure
- Being part of the MANRS community can strengthen enterprise security credentials

To add competitive value and differentiate in a flat, price-driven market

- Growing demand from enterprise customers for managed security services (info feeds)
- To signal security proficiency and commitment to your customers

To "lock-in" - from a connectivity provider to a security partner

- Information feeds and other add-on services may increase revenue and reduce customer churn
- Enterprises indicate willingness to pay more for secure services

Why ENTERPRISES Should Require MANRS

To improve your organizational security posture

- MANRS-ready infrastructure partners increase security and service reliability, while eliminating common outages or attacks
- Requiring MANRS adoption can help enterprises demonstrate due diligence and regulatory compliance

To prevent and address security incidents

- Preventing traffic hijacking, detouring, and malicious traffic helps prevent data loss, denial of service, reputational damage, and more
- Attacks and outages are resolved promptly by MANRS participants who are part of a broad network of security-minded operators

MANRS provides a foundation for value-added services

- Incident information sharing and information feeds can directly impact the bottom line
- Organizations can improve SLA compliance and address a host of routing deficiencies by simply seeking providers that adopt MANRS

Why GOVERNMENTS Should Promote MANRS

To drive the development or adoption of best practices across the country

- Encourage industry associations to develop or strengthen and promote existing voluntary codes of conduct for network operators. MANRS can serve as both a baseline set of best practices and as a foundation to complimentary voluntary codes of conduct.

To encourage the use of routing security as a competitive best practice

- Encourage local industry to better convey security to consumers, and specify security during procurement practices.

To lead by example

- Improve infrastructure reliability and security by adopting best practices in their own networks.

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

MANRS

Version 1.0, BCOP series
Publication Date: 25 January 2017

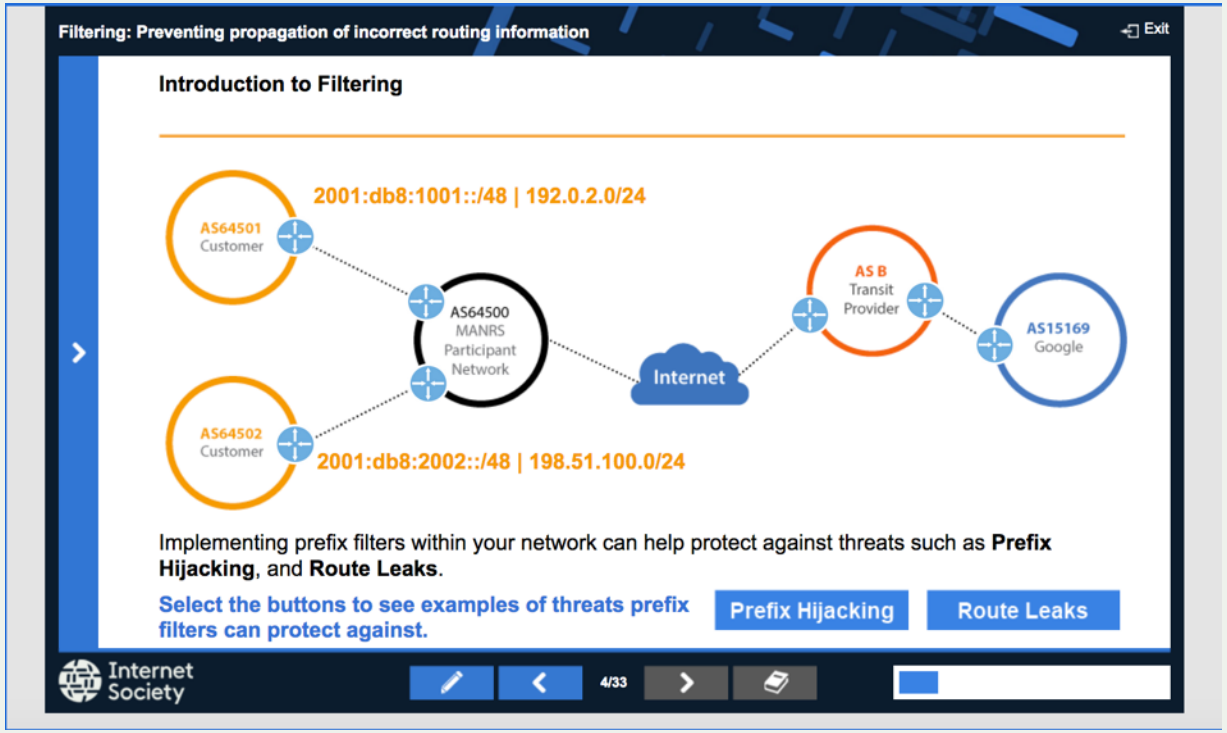
MANRS Training Modules

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



How to avoid these routing issues?

Filter all incoming customer announcements

- Only allow ASNs and prefixes that are really assigned or allocated to them

Filter all your outgoing BGP announcements

- You can also make that typo

If every network applies this logic, you can trust the core of the network to be clean and secure

“The good we secure for ourselves is precarious and uncertain until it is secured for all of us and incorporated into our common life.”

— **Jane Addams** (Nobel Peace Prize Winner)

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

Thank you.

Aftab Siddiqui

siddiqui@isoc.org

manrs.org