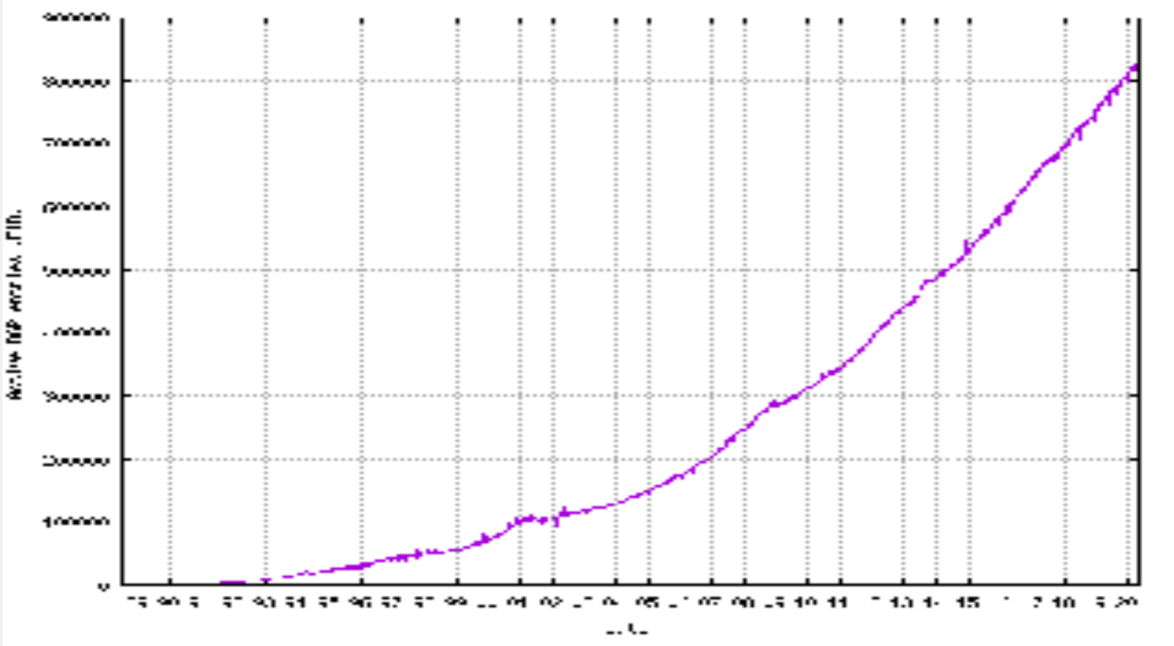
MANRS Brief - AoNOG

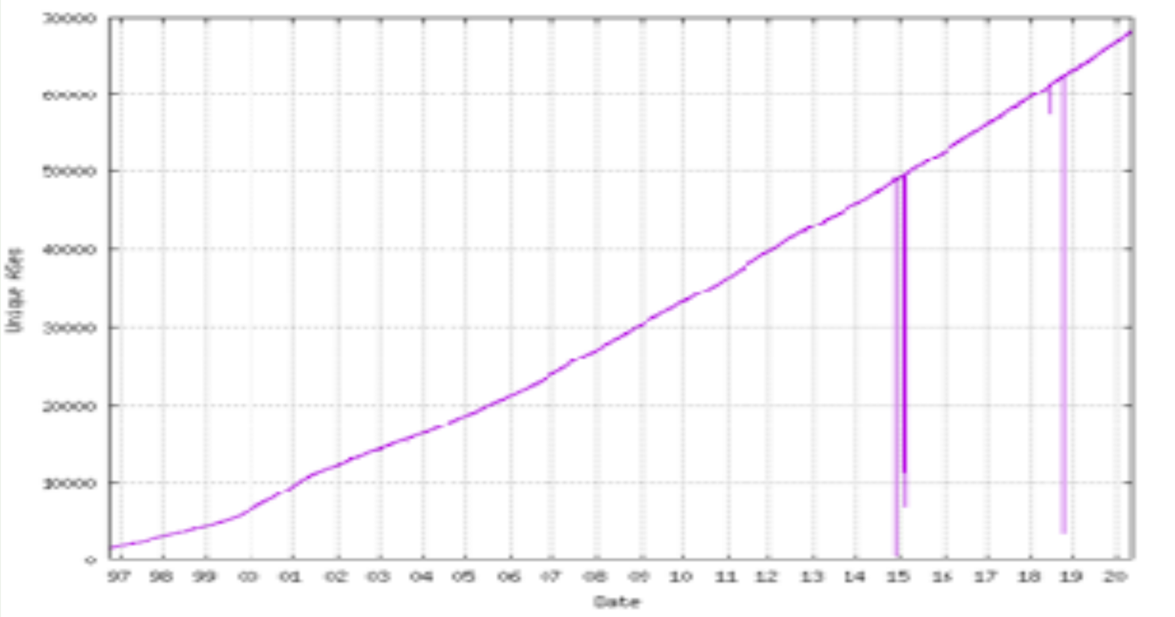
Hiba Eltigani - MANRS Fellow

The Internet

- There are ~69,000 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.



Plot Range: 30-Jun-1988 1430 to 28-Apr-2020 0128



Plot Range: 30-Sep-1996 1430 to 28-Apr-2020 0128

https://www.cidr-report.org

The Honor System: Routing Issues

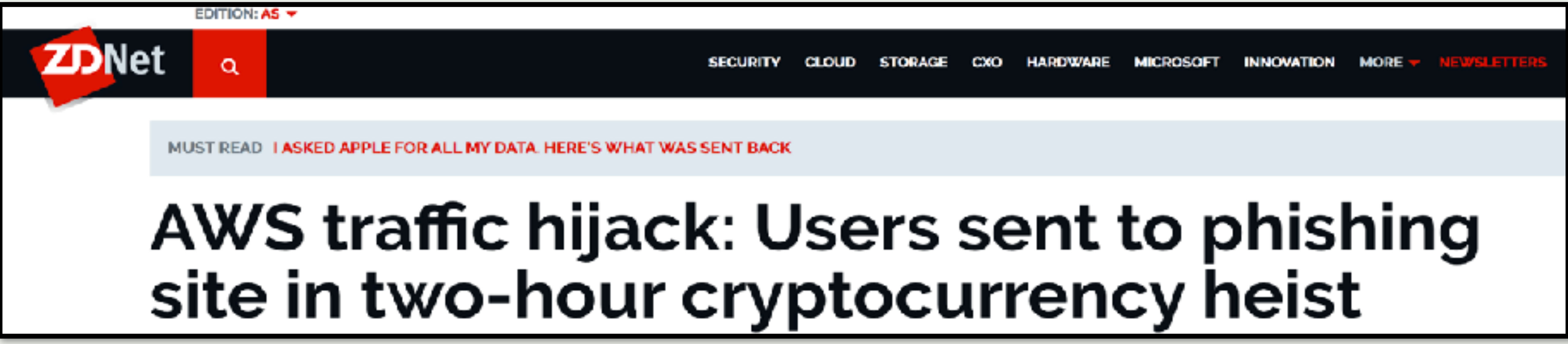
Border Gateway Protocol (BGP) is based entirely on trust between networks

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

Routing Incidents are Increasing

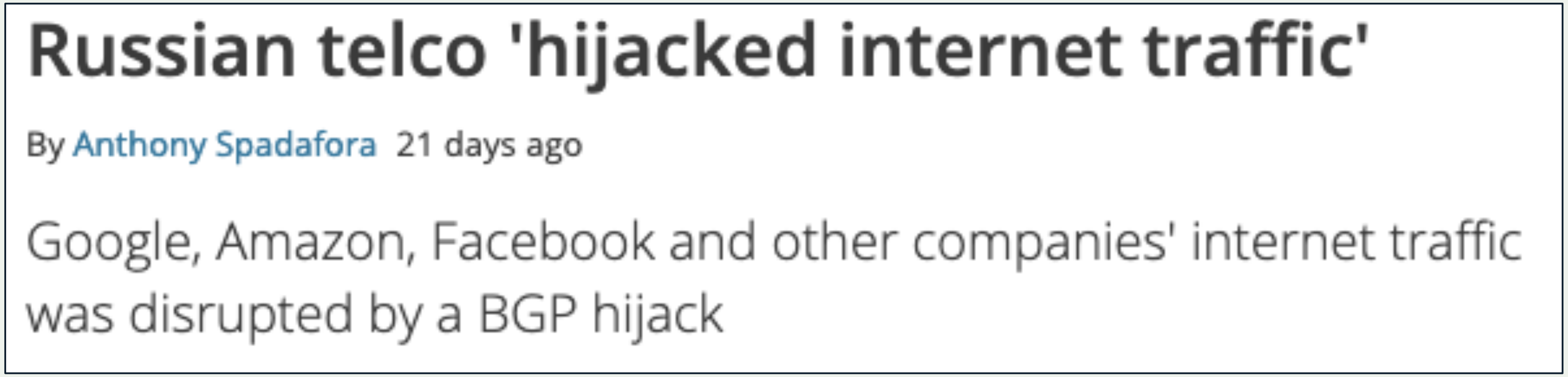
- Unsecured routing is one of the most common problem for malicious threats.
- Inadvertent errors can take entire countries offline, while attackers can steal an individual's data or hold an organization's network hostage.
- Attacks can take anywhere from hours to months until even being identified.
- Incidents are global in scale, with one operator's routing problems cascading to impact others.
- These hijacks led to a range of problems including stolen data, lost revenue, reputation damage, and more.
- In 2019, 1,810 BGP Hijacks were recorded by bgpstream.com

Recent Events (April - 2020)



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

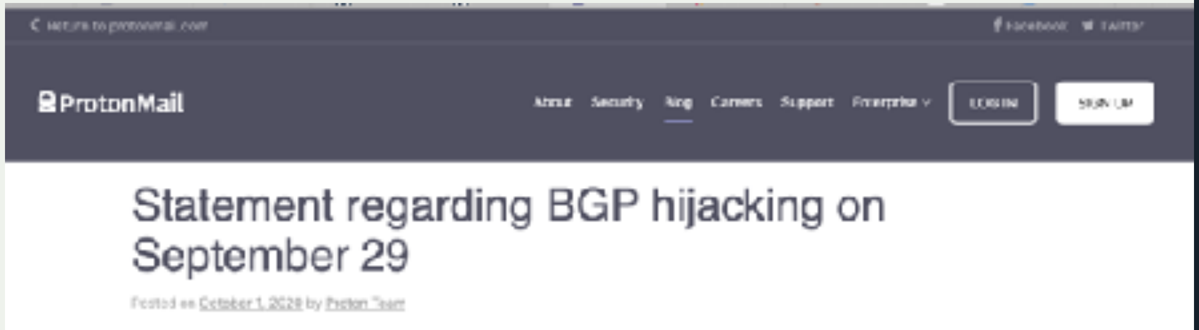


Russian telco 'hijacked internet traffic'

By Anthony Spadafora 21 days ago

Google, Amazon, Facebook and other companies' internet traffic was disrupted by a BGP hijack

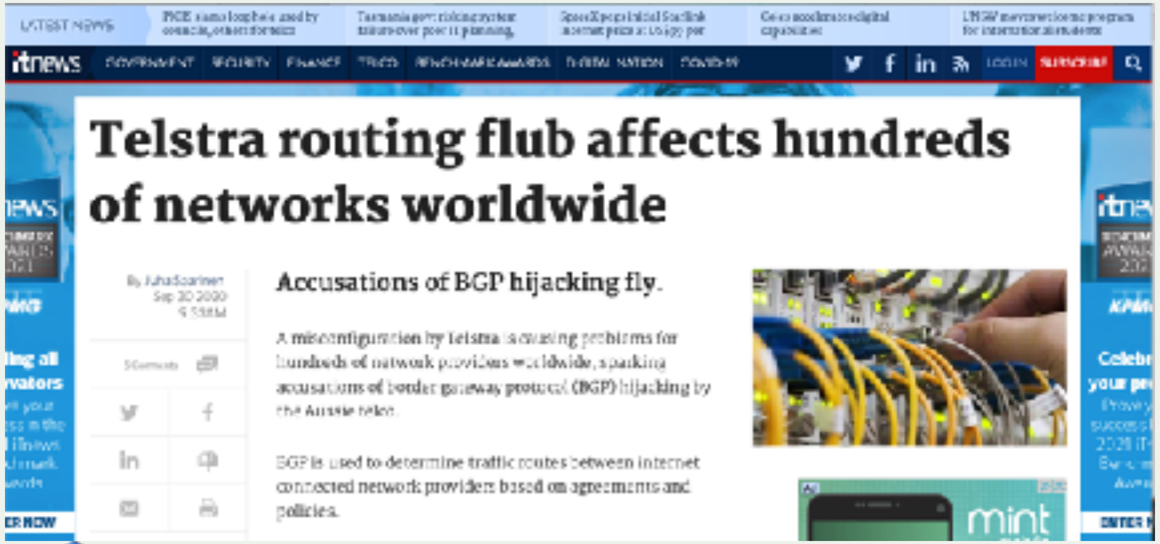
Recent Events (September - 2020)



Statement regarding BGP hijacking on September 29

Posted on October 1, 2020 by Proton Team

https://protonmail.com/blog/bgp-hijacking-september-2020/



Telstra routing flub affects hundreds of networks worldwide

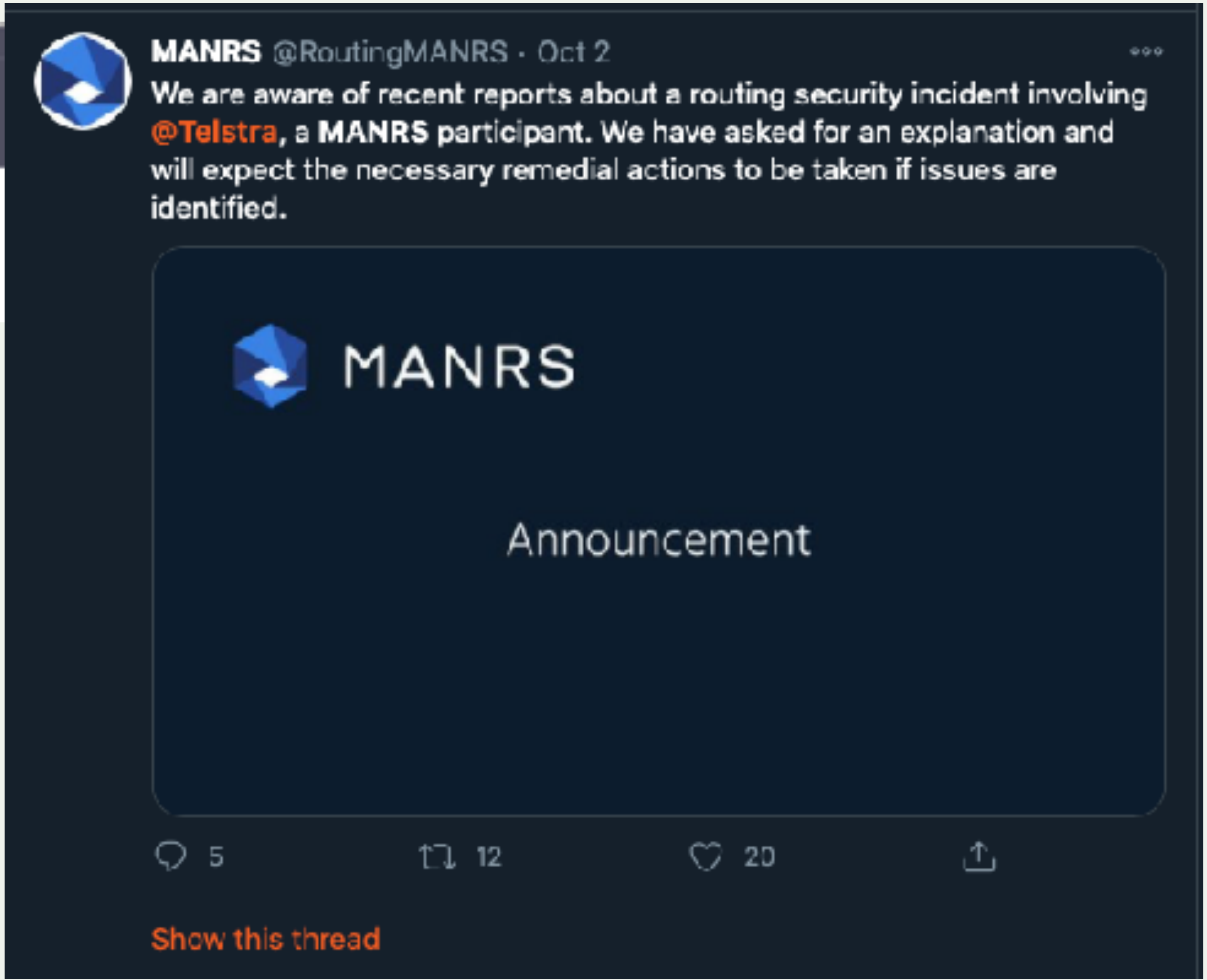
By Juha Saarinen
Sep 30 2020
9:53AM

Accusations of BGP hijacking fly.

A misconfiguration by Telstra is causing problems for hundreds of network providers worldwide, sparking accusations of border gateway protocol (BGP) hijacking by the Aussie telco.

BGP is used to determine traffic routes between internet connected network providers based on agreements and policies.

https://www.itnews.com.au/news/telstra-routing-flub-affects-hundreds-of-networks-worldwide-554097



MANRS @RoutingMANRS · Oct 2

We are aware of recent reports about a routing security incident involving @Telstra, a **MANRS participant**. We have asked for an explanation and will expect the necessary remedial actions to be taken if issues are identified.

Common Causes

Prefix/Route Hijacking

Route Leaks

IP address spoofing

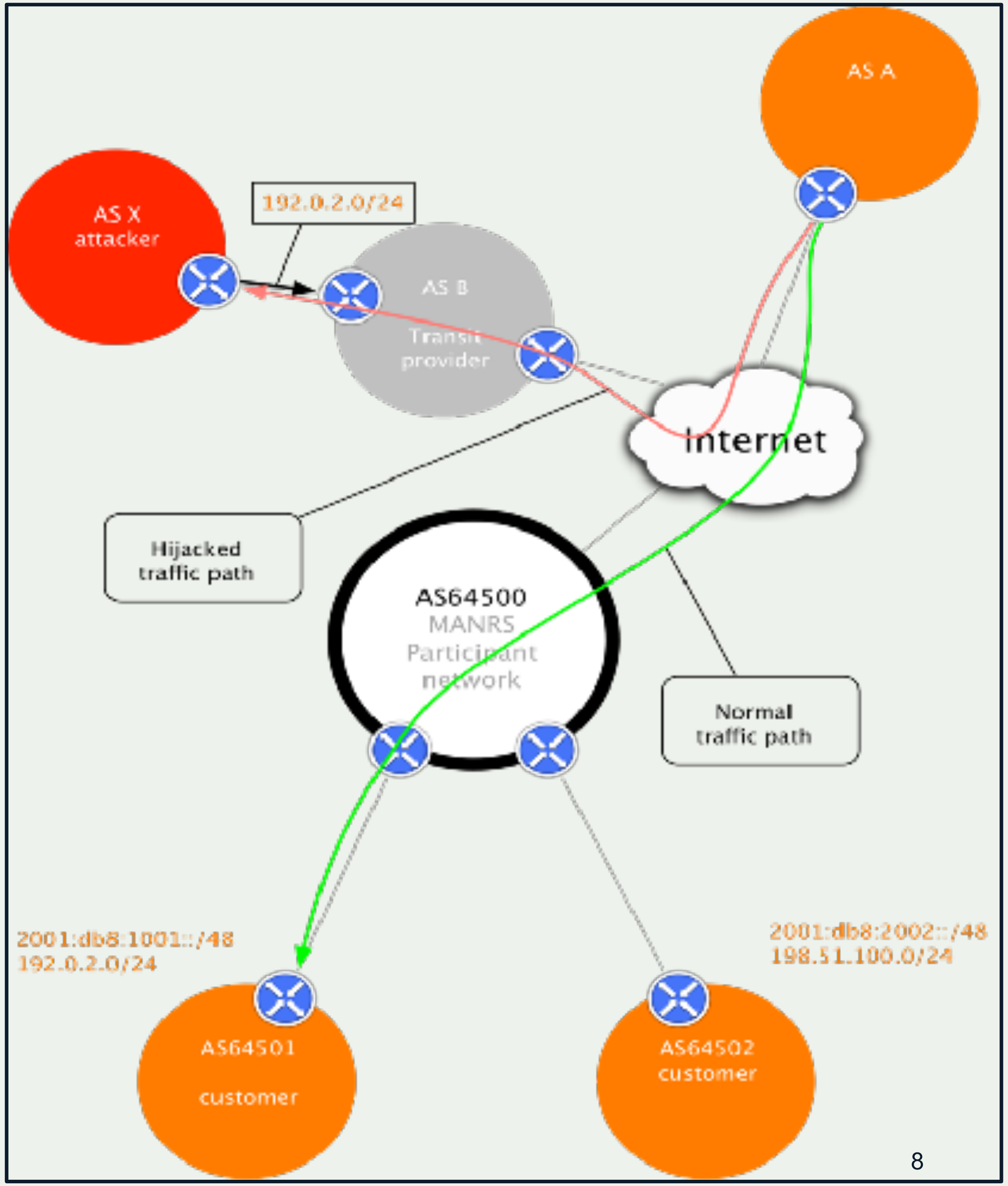
Prefix/Route Hijacking

Route hijacking, also known as "BGP hijacking" when a network operator or attacker (accidentally or deliberately) impersonates another network operator or pretending that a server or a network is a client. This routes traffic to a network operator, when another real route is available.

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.

Issue: Packets are forwarded to the wrong place, and can cause Denial of Service (DoS) attacks or traffic interception.

Solution: Stronger filtering policies



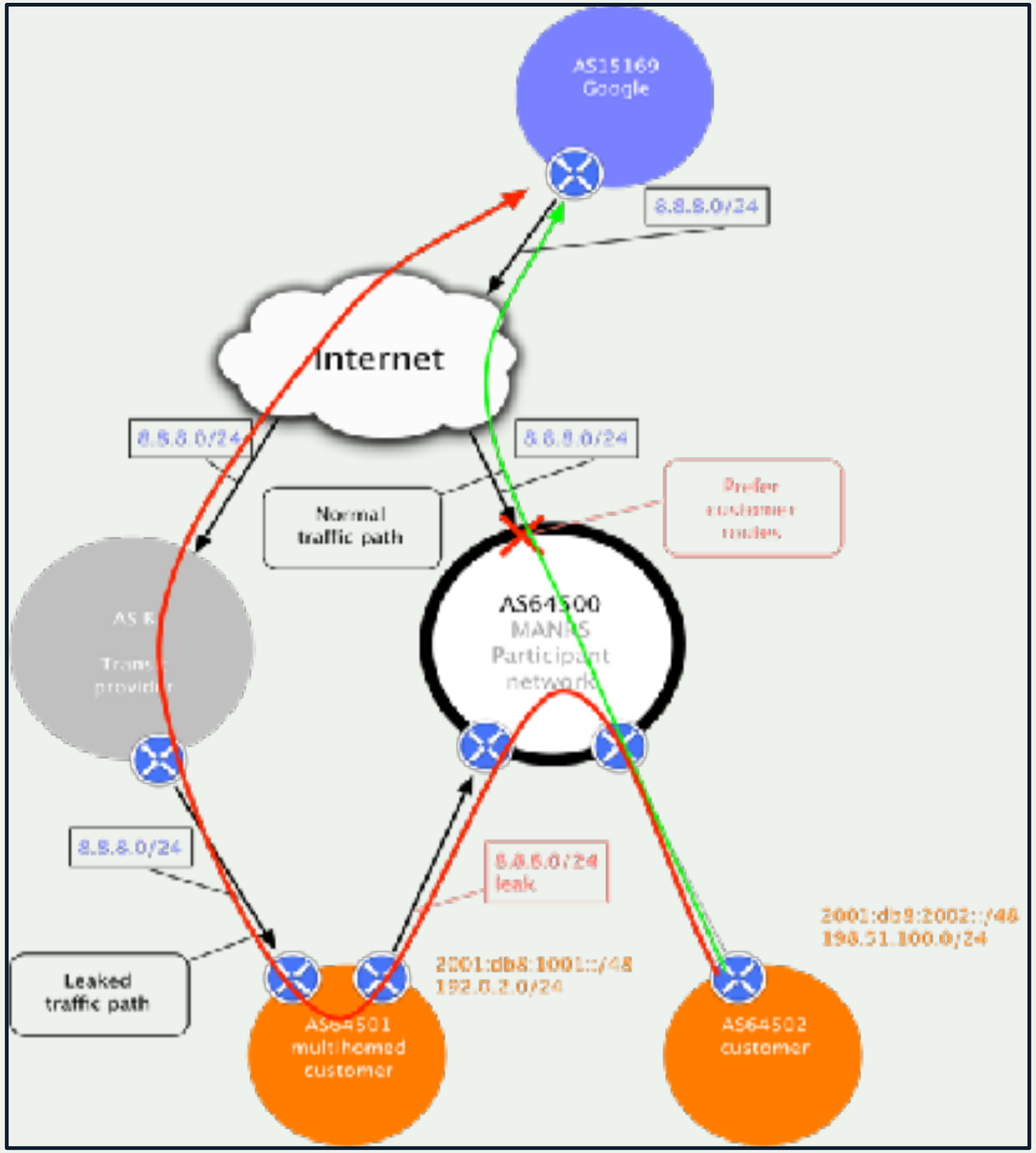
Route Leak

A route leak is a problem where a network operator with multiple upstream providers accidentally announces to one of its upstream providers that 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: 2015, Malaysia Telecom and Level 3, a major backbone provider. Malaysia Telecom told one of Level 3's networks that it was capable of delivering traffic to anywhere on the Internet. Once Level 3 decided the route through Malaysia Telecom looked like the best option, it diverted a huge amount of traffic to Malaysia Telecom.

Issue: Can be used for traffic inspection.

Solution: Stronger filtering policies .



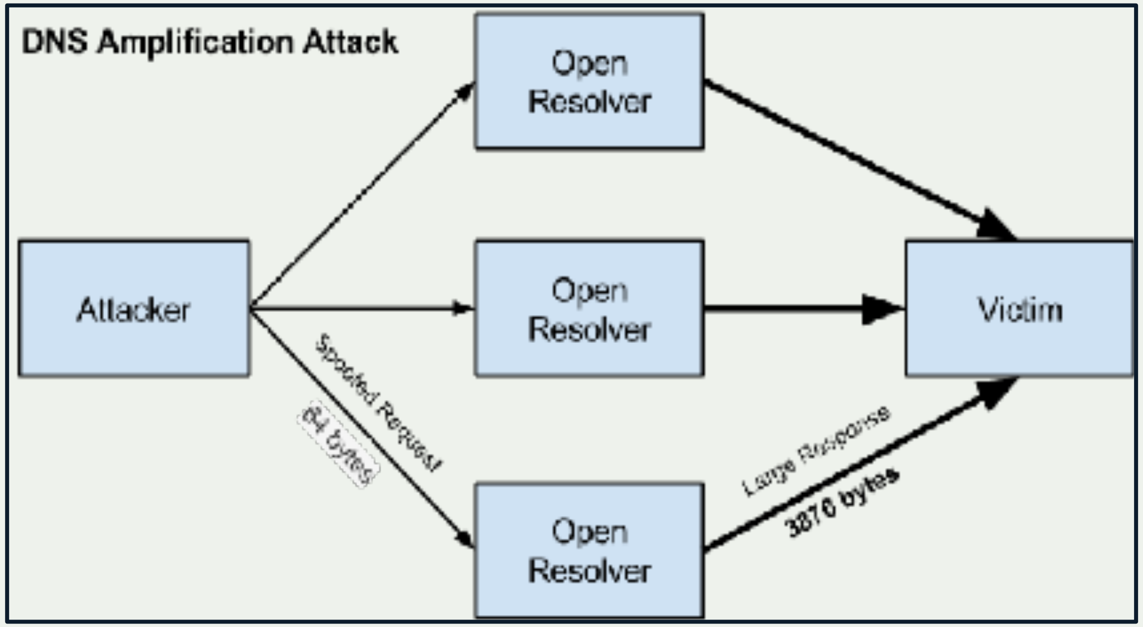
IP Address Spoofing

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.

Issue: The root cause of reflection DDoS attacks

Solution: 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).



The Tools

How we can combat the issues?

BCP - 194

BCP - 38
BCP - 84

IRR

RPKI

BCP - 194

- RFC 7454, published February 2015.
- Different Security Considerations:
  - Protection of BGP speaker and BGP sessions.
  - Prefix and AS-Path filtering.
  - Maximum prefixes, BGP communities and Next-Hop filtering.
- Why filtering:
  - Your first line of defense
  - You control what you are announcing
  - You have **no control** over what **other networks** announce
  - To avoid issues, **you have to decide** what to accept from other networks

BCP - 38
BCP - 84

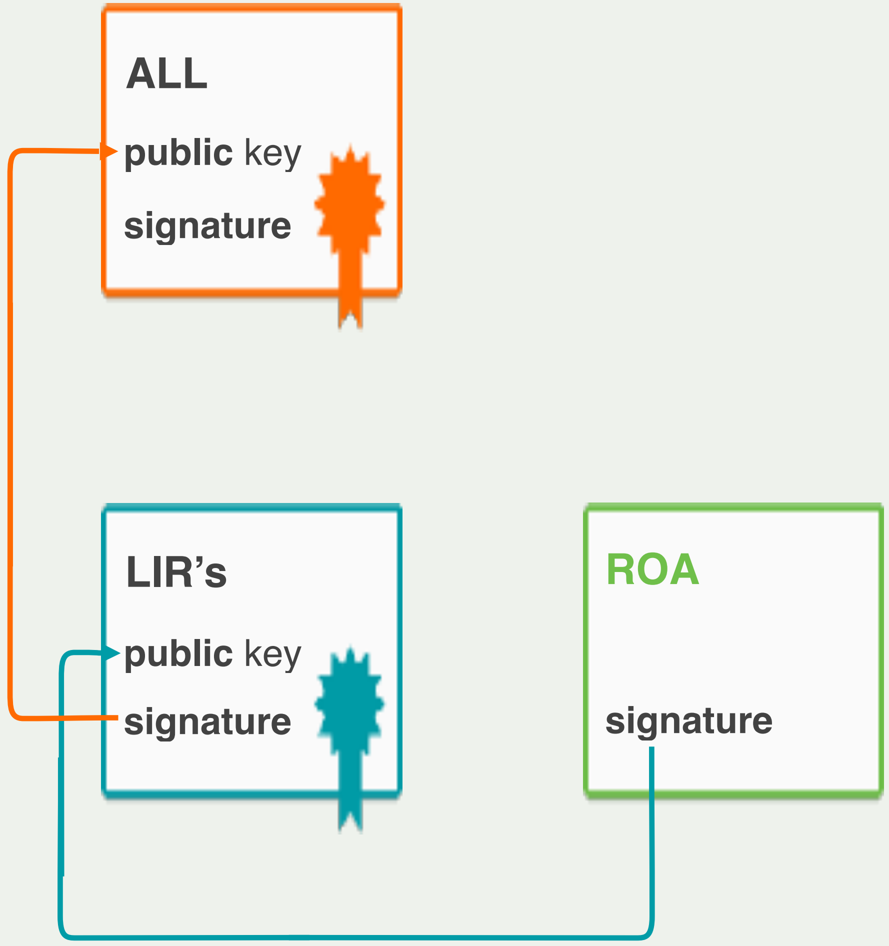
- Several RFCs (2267, 2827, 3704, 8704), first one published in 2000 and the latest in February 2020.
- Different implementations for network ingress filtering:
  - Access Lists
  - uRPF (Unicast Reverse Path Forwarding) - Loose, strict, feasible, enhanced feasible
  - VRF tables

IRR

- Internet Routing Registries are public repositories (databases) of Internet routing policy information.
- Use Routing Policy Specification Language “RPSL” to define policies (RFC 2622, RFC 2650).
- Provides routing information which can be used by the BGP for policy based decisions.
- Routing policy information is expressed in a series of objects (aut-num, inetnum, inet6num, route, route6, as-set, role, ….etc).

RPKI

- RFCs - 6480 in 2012.
- Resource Public Key Infrastructure uses public keys to tie IP prefixes to ASNs.
- Follows the hierarchy of the registries and allow resource holders to make authorized statements.



But…

- Not enough deployment
- Lack of reliable data

We need a standard approach to improving routing security.

Mutually Agreed Norms for Routing Security (MANRS)

Provides crucial fixes to eliminate the most common routing threats

We Are In This Together

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

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.

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 Actions

Optional

Mandatory

Network Operators

Action 1
Filtering
Prevent propagation of incorrect routing information

Action 2
Anti-spoofing
Prevent traffic with spoofed source IP addresses

Action 3
Coordination
Facilitate global operational communication and coordination

Action 4
Global Validation
Facilitate validation of routing information on a global scale

IXPs

Action 1
Prevent propagation of incorrect routing information

Action 2
Promote MANRS to the IXP membership

Action 3
Protect the peering platform

Action 4
Facilitate global operational communication and coordination

Action 5
Provide monitoring and debugging tools to the members

CDNs Cloud

Action 1
Prevent propagation of incorrect routing information

Action 2
Prevent traffic with spoofed source IP addresses

Action 3
Facilitate global operational communication and coordination

Action 4
Facilitate validation of routing information on a global scale

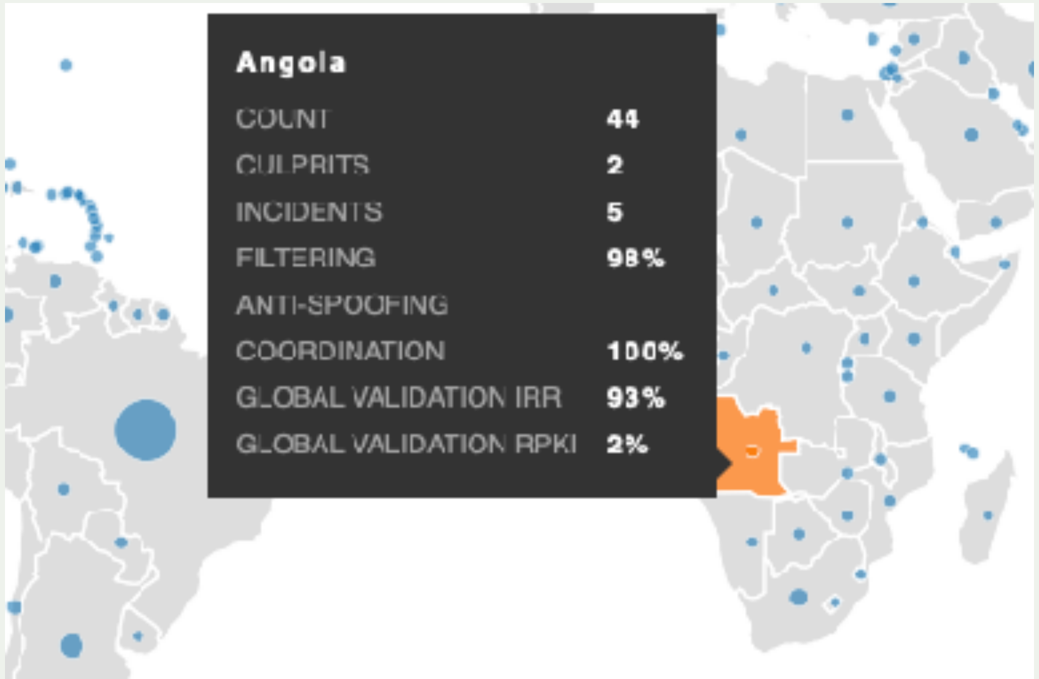
Action 5
Encourage MANRS adoption

Action 6
Provide monitoring and debugging tools to peering partners

Country View

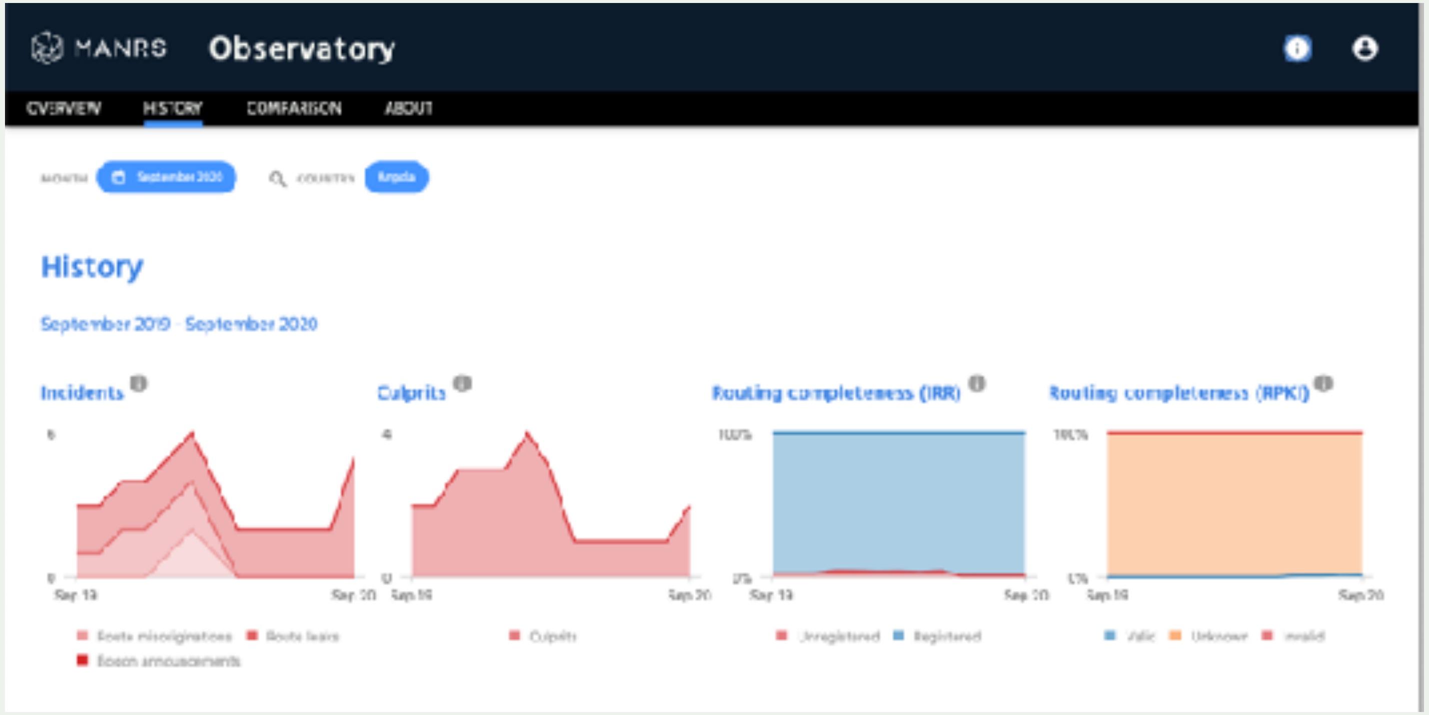
What is happening?

Overview



Angola	
COUNT	44
CULPRITS	2
INCIDENTS	5
FILTERING	98%
ANTI-SPOOFING	
COORDINATION	100%
GLOBAL VALIDATION IRR	93%
GLOBAL VALIDATION RPKI	2%

Source: https://observatory.manrs.org - 20 Sept 2020

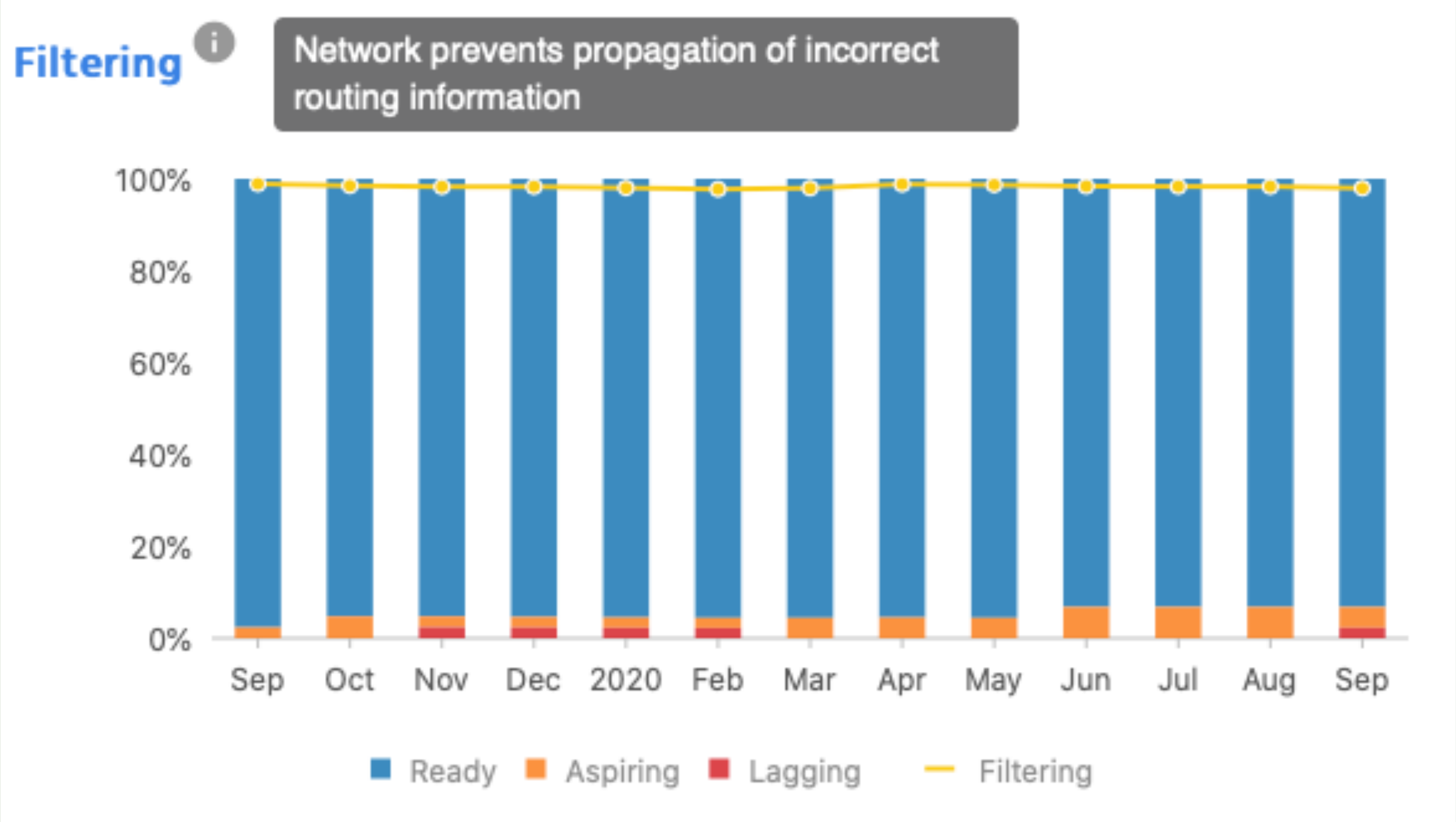


History

September 2019 - September 2020

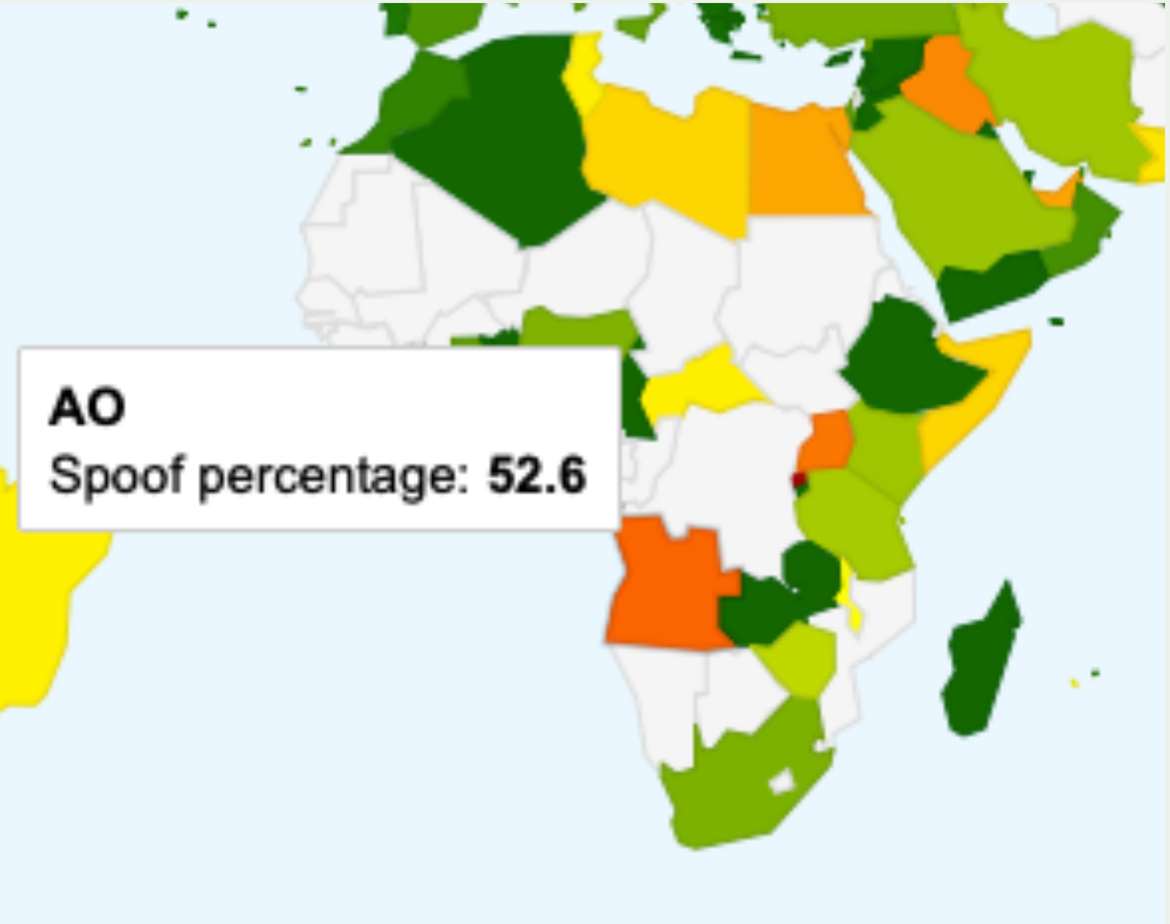
Source: https://observatory.manrs.org - 20 Sept 2020

Filtering

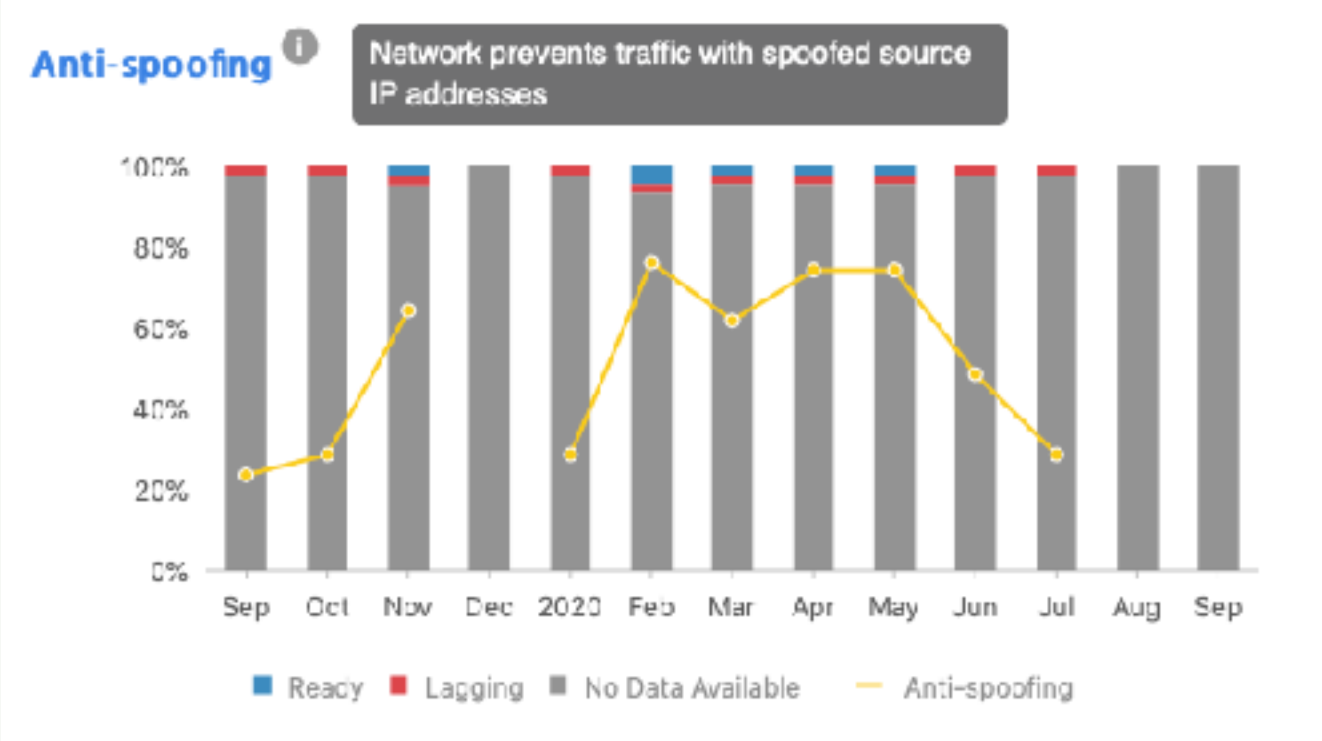


Source: https://observatory.manrs.org

IP Address Spoofing

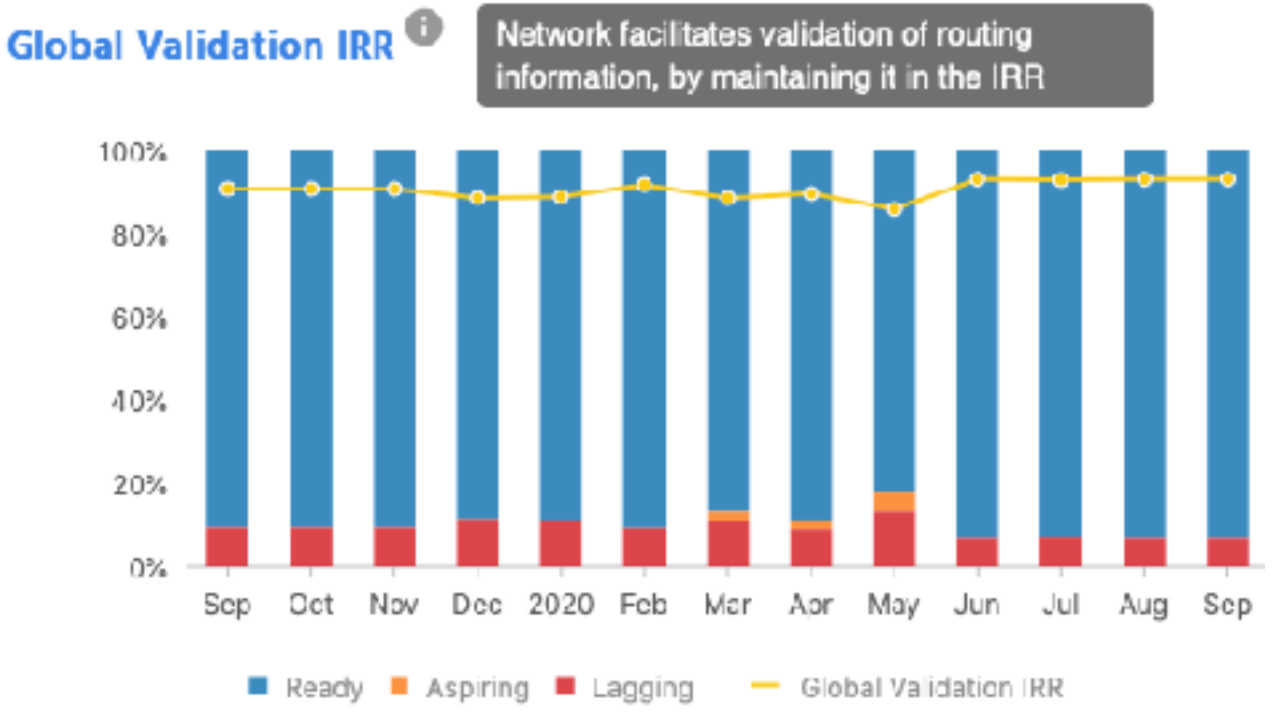


Source: https://spoofer.caida.org/country_stats.php



Source: https://observatory.manrs.org

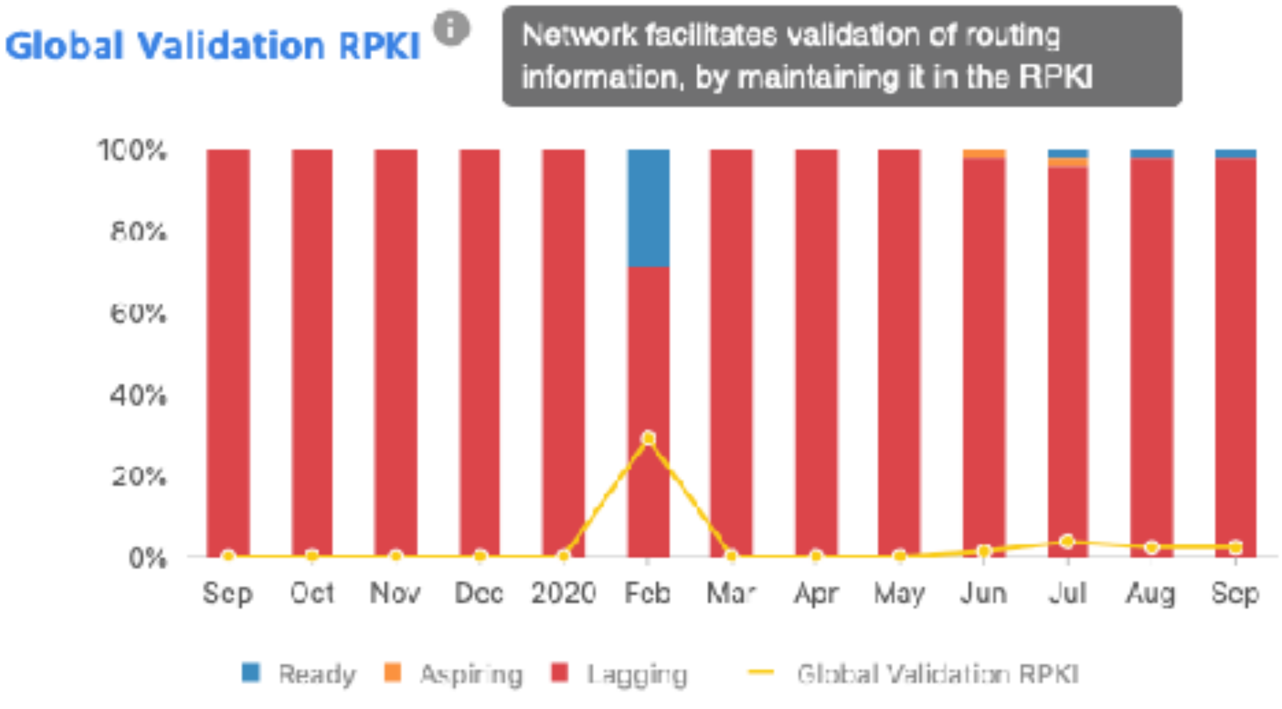
Global Validation



Global Validation IRR

Network facilitates validation of routing information, by maintaining it in the IRR

Source: https://observatory.manrs.org

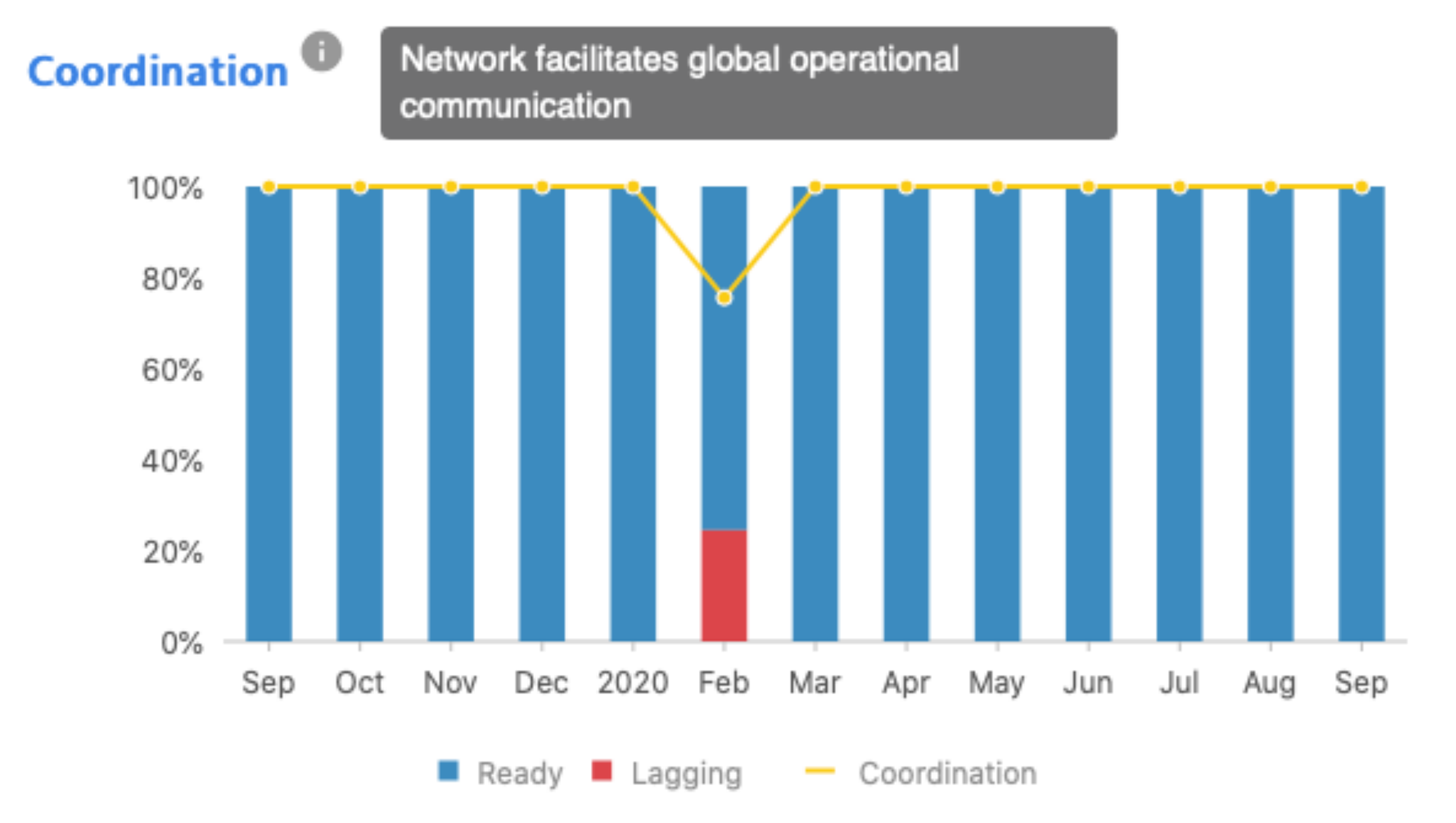


Global Validation RPKI

Network facilitates validation of routing information, by maintaining it in the RPKI

Source: https://observatory.manrs.org

Coordination



Source: https://observatory.manrs.org

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

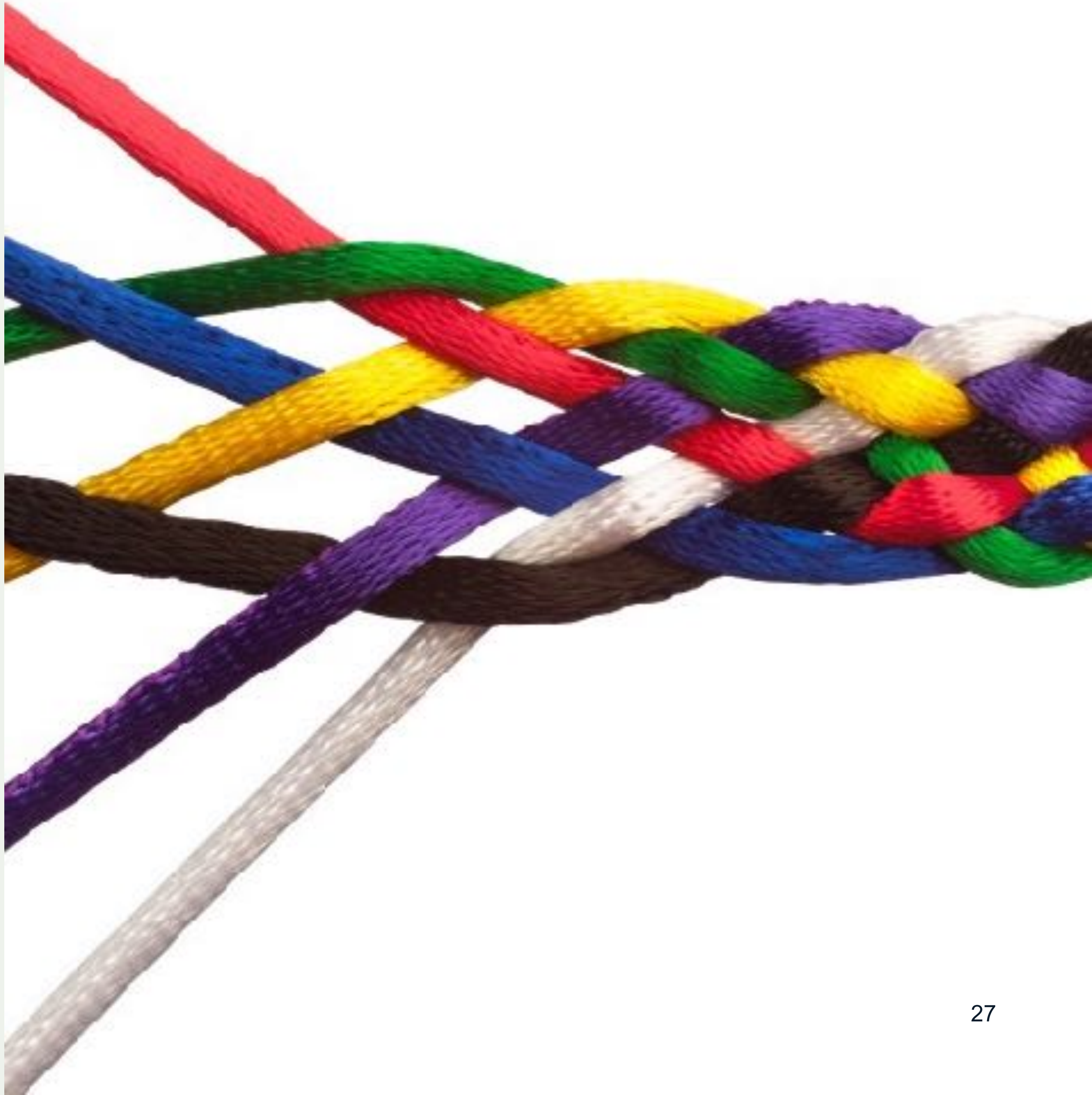
Get Involved in the Community

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

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/

Training modules are also available.



Thank you.

manrs.org