Is Your Connectivity Provider a Threat Vector or a First Line of Defense?

Routing Security is Supply Chain Security

Megan Kruse
Internet Society / MANRS
kruse@isoc.org

About the Internet Society

We are a global nonprofit organization connecting and empowering communities to protect this essential resource since 1992.

Community members of Pu'uhonua O Waimanalo work together with the Internet Society to learn how to use and install the Internet during a training session.
© Elyse Butler

The Internet Society Community: A Global Network of People

91,000

Global Members

130

Chapters, Special Interest Groups, and Standing Groups

90

Organization Members

140

Internet Society Staff

The Internet is for everyone.

The whole of the Internet Society works towards this vision by building, promoting, and defending a bigger and stronger Internet.

About Me

Megan Kruse

Director, Advocacy and Communications

Internet Society since 2011

Specialty: Geek-to-English translation

Working on routing security since 2014

Let’s Get Into It!

First, A Scary Story

(don’t panic, we’ll explain the acronyms)

KLAYswap: $1.9M USD Stolen

BANK INFO SECURITY®

Topics News Training Resources Events Jobs

TRENDING: The Latest From RSAC 2023! • Strategies for CISOs in the Age of Increasing Vulnerabilities •

Blockchain & Cryptocurrency , Cryptocurrency Fraud , Fraud Management & Cybercrime

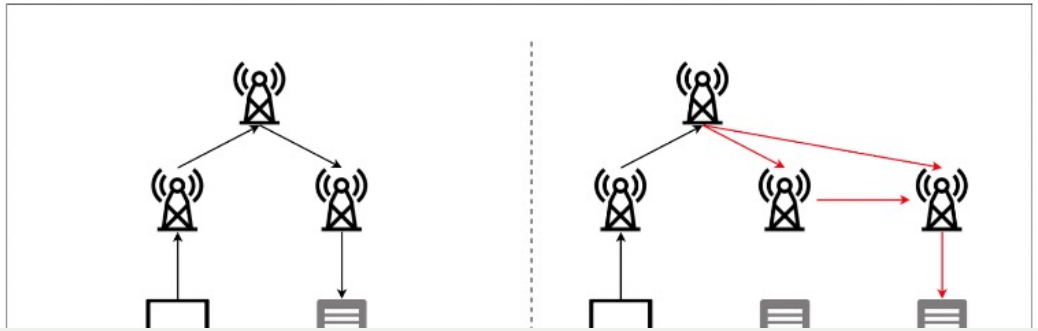
Crypto Exchange KLAYswap Loses $1.9M After BGP Hijack

Hackers Performed Border Gateway Protocol Hack to Conduct Illegal Transactions

Prajeet Nair (@prajeetspeaks) • February 16, 2022

Credit Eligible

Get Permission



What Happened?

Hackers stole ~1.9M USD worth of cryptocurrency assets.

They didn’t attack KLAYswap directly; they went after the server infrastructure of KakaoTalk, a contracted marketing and tech support service.

Attackers used a BGP hijack to serve a malicious version of KakaoTalk’s JavaScript software development kit (SDK) file.

This was a supply chain attack.

This hijack could have been avoided - or at least minimized - if KakaoTalk had valid RPKI Route Origin Authorizations (ROAs) for its ASNs.

RPKI, ROA, ASN, What?

Let’s Back Up A Minute …

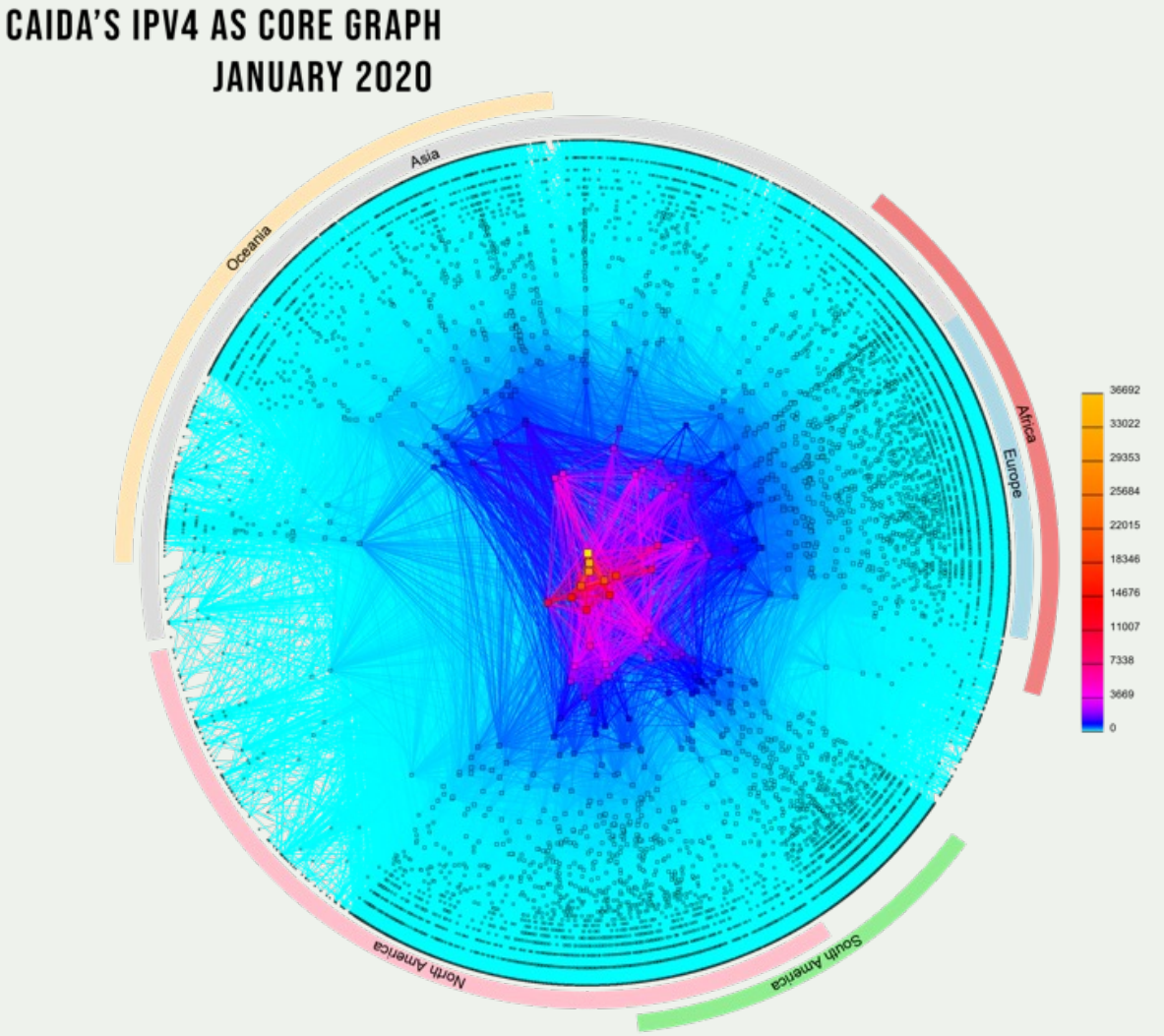
An Extremely Condensed Routing 101

There are ~74,000 independent networks that together make up the Internet.

Each network is identified by an **Autonomous System Number, or ASN**.

Each ASN makes its own decisions about how to move Internet traffic using a language called **Border Gateway Protocol, or BGP.**

BGP is a fundamental underpinning of the Internet.



The Problem with BGP

BGP was created in 1989, before Internet security was a concern.

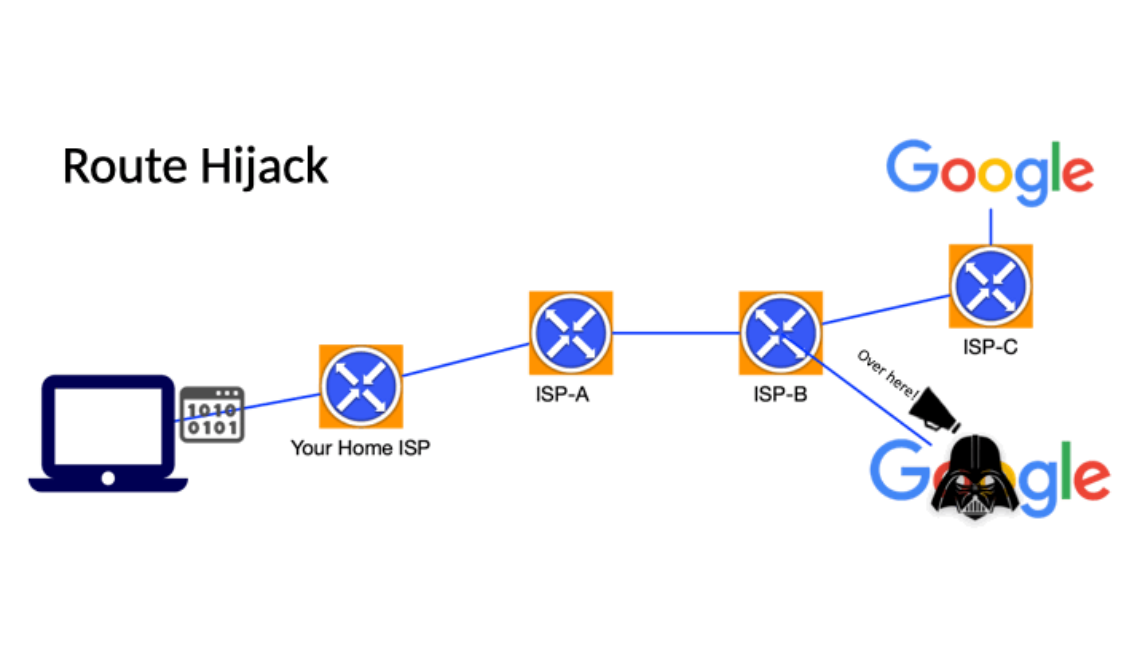
BGP assumes all networks are trustworthy. Any network can announce it has a path to any other network, even if it does not.

There is no built-in security mechanism to check if traffic is legitimate or not.

On today's Internet, this is a problem.

BGP is vulnerable to both malicious attacks and human mistakes.

Problem: BGP Hijacks

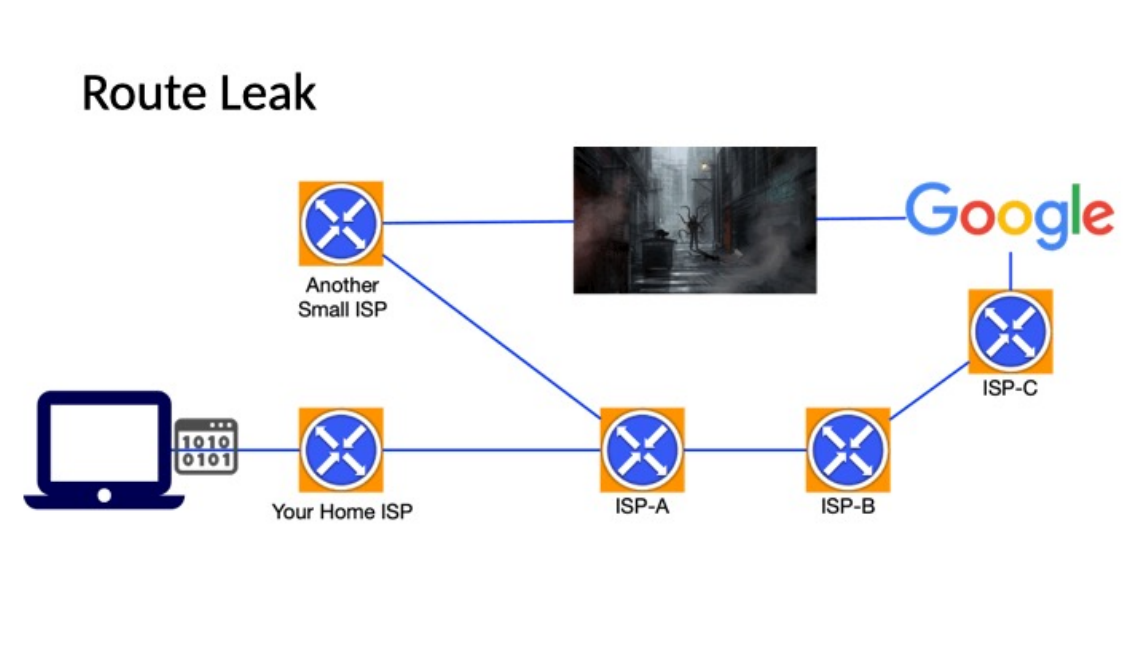


A network or attacker impersonates another network, pretending that a server or network is their client.

Result: Packets are forwarded to the wrong place; this can cause Denial of Service (DoS) attacks or traffic interception.

Hijacks are usually intentional.

Problem: BGP Leak

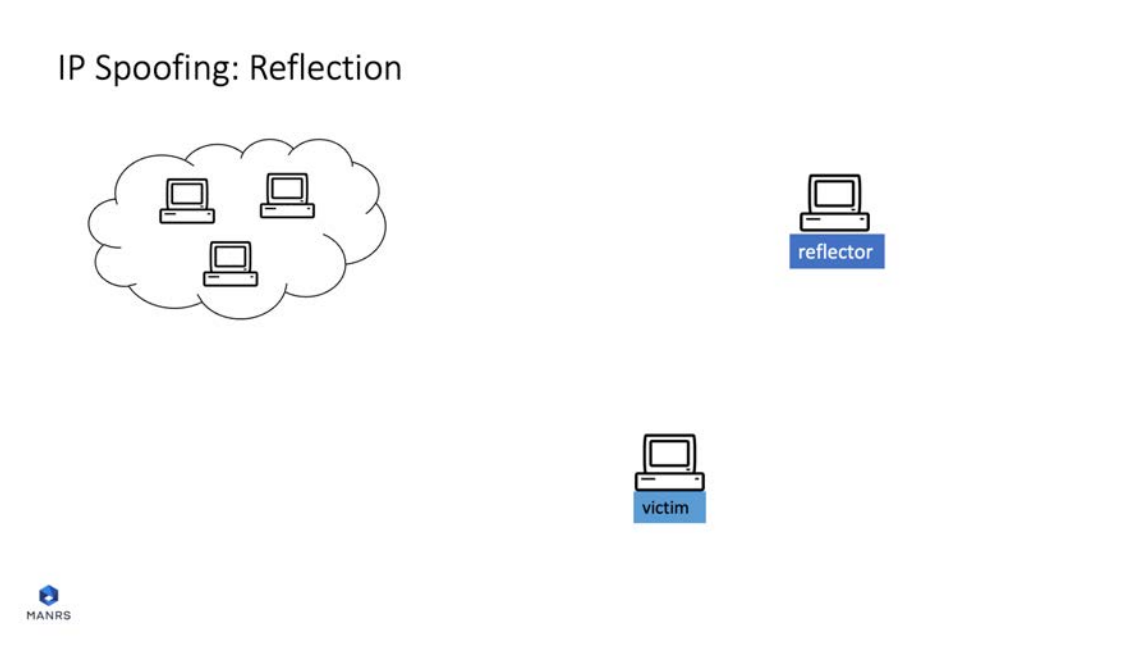


A network or attacker advertises illegitimate IP prefixes, which propagate across networks and lead to incorrect or suboptimal routing.

Result: Packets can be redirected through a path that could enable eavesdropping or traffic analysis.

Leaks can be malicious, but are often accidental misconfigurations.

Problem: IP Address Spoofing



Someone creates IP packets with a false source IP address to hide the identity of the sender or to impersonate another network.

Result: Attackers magnify the amount of malicious traffic and obscure the sources of the attack traffic, causing a reflection DDoS attack.

Why is Routing Security Hard?

Every network has a responsibility to implement basic routing security practices to mitigate threats.

But implementing best practices does not bring many immediate benefits. It costs time and money, and you probably can’t charge extra for it.

Even if you do everything right, your security is still in the hands of other networks.

This is a classic collective action problem.

Mutually Agreed Norms for Routing Security (MANRS)

Industry-led initiative of almost 1000 participating networks to implement best practices and collaborate toward a shared vision of a secure routing infrastructure.

MANRS provides concrete actions for Network Operators, IXPs, CDN/Cloud Providers & Vendors to reduce or eliminate the most common threats to routing.

There are no fees to join MANRS. MANRS is currently supported by the Internet Society.

MANRS

How to Improve Your Network

MANRS Actions

Filtering

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

Anti-Spoofing

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

Coordination

Maintain globally accessible up-to-date contact information

Routing Information

Publish your data, so others can validate routing information on a global scale

Tools

Provide monitoring and debugging tools to help others

Promotion

Actively encourage MANRS adoption among peers, customers, and partners

Routing Security Solutions

Filtering or Route Validation mitigates the risk of traffic being hijacked. When a router filters traffic, it checks that networks are only announcing the ASNs and IP prefixes they or their customers are legitimately authorized to originate.

Anti-spoofing prevents traffic with fake source IP addresses from leaving a network. This can help detect suspicious activity on your network (e.g. botnets).

Routing Information is telling other networks what to expect from you. This lets other networks protect traffic going to and from your network via filtering.

Coordination means ensuring your network has up-to-date contact information and responding in a timely fashion when incidents occur.

Routing Information: Help Others Help You

Internet Routing Registry (IRR)

Public databases where network operators publish their IP resources and routing policies.

Almost anyone can enter information, which leads to inconsistencies, stale data, and lack of real verification.

It isn’t perfect, but it’s better than nothing.

Resource Public Key Infrastructure (RPKI)

A security layer that provides full cryptographic trust toward ownership where the owners have a publicly available identifier.

Operators sign Route Origin Authorizations (ROAs), cryptographic assertions of which ASNs are authorized to originate which IP resources.

RPKI allows much better route validation.

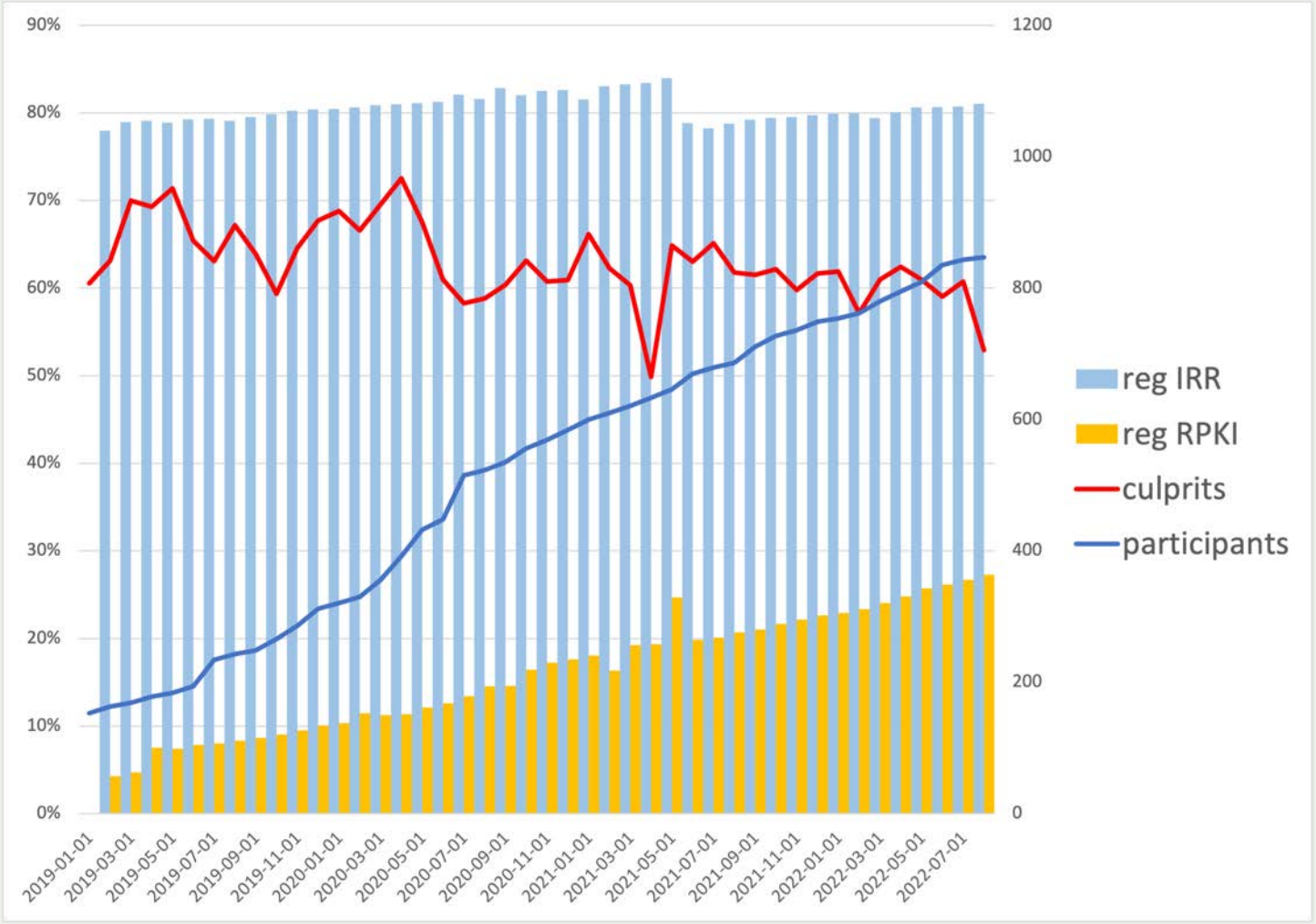
It is newer and under-deployed.

We Are Making Progress

81% of all ASNs have their routes registered in an IRR and 27% in RPKI, and these numbers are growing.

Number of “culprits” – ASNs implicated in one or more suspicious routing events – is declining.

But there’s still a lot of work to do.



Data sources: MANRS Observatory, BGPStream, GRIP.

Improve Your Connectivity and Cloud Providers

You Are Not An Island

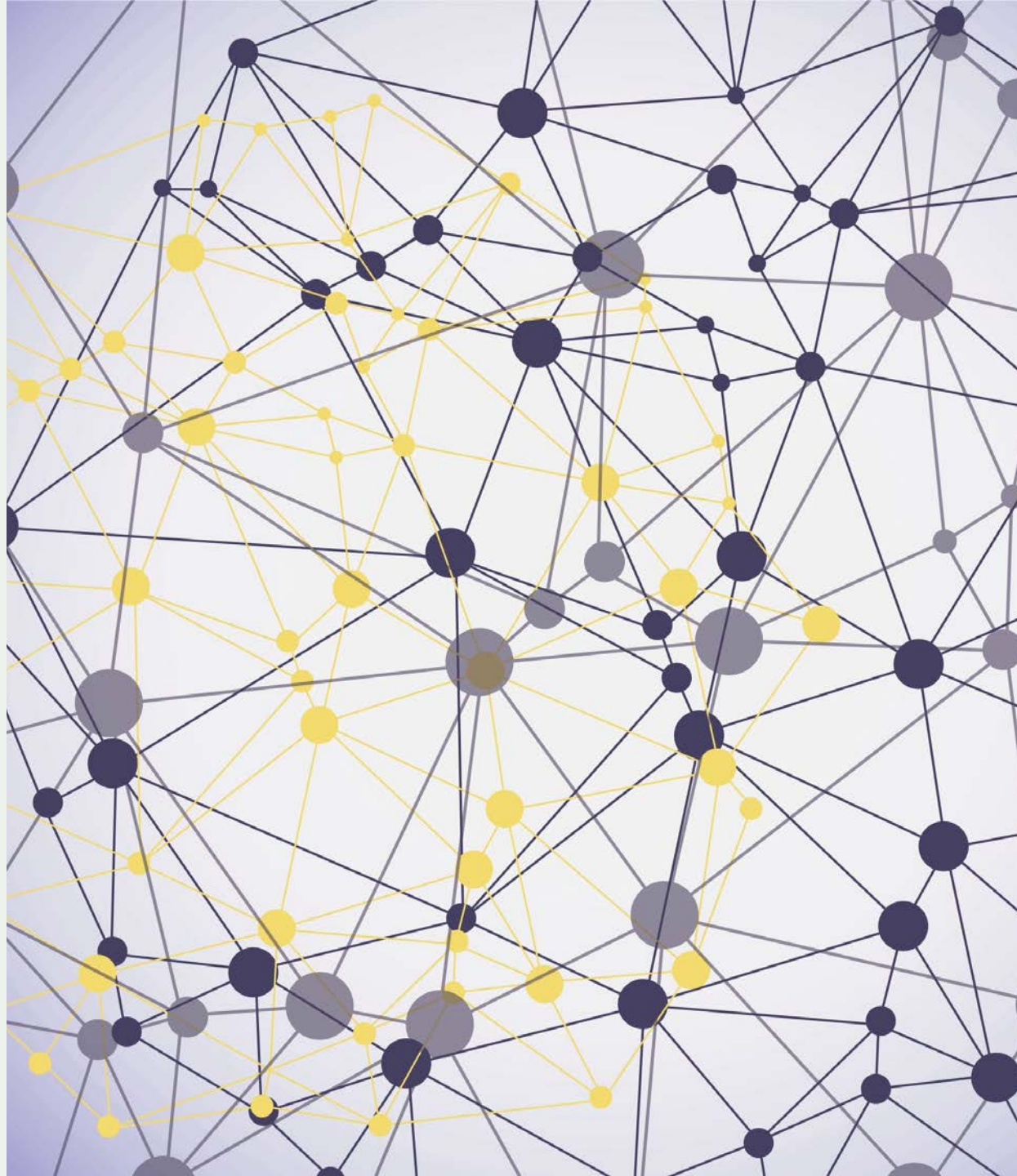
You are one of 74,000 intertwined networks on the Internet.

You use at least one Internet Service Provider. You most likely use some Cloud services.

It’s important to use best practices on your network. It is even more important to choose connectivity and cloud providers that are committed to mitigating routing security threats.

Your connectivity or cloud provider could be your weakest link.

Routing security thus becomes an important part of your supply chain security.



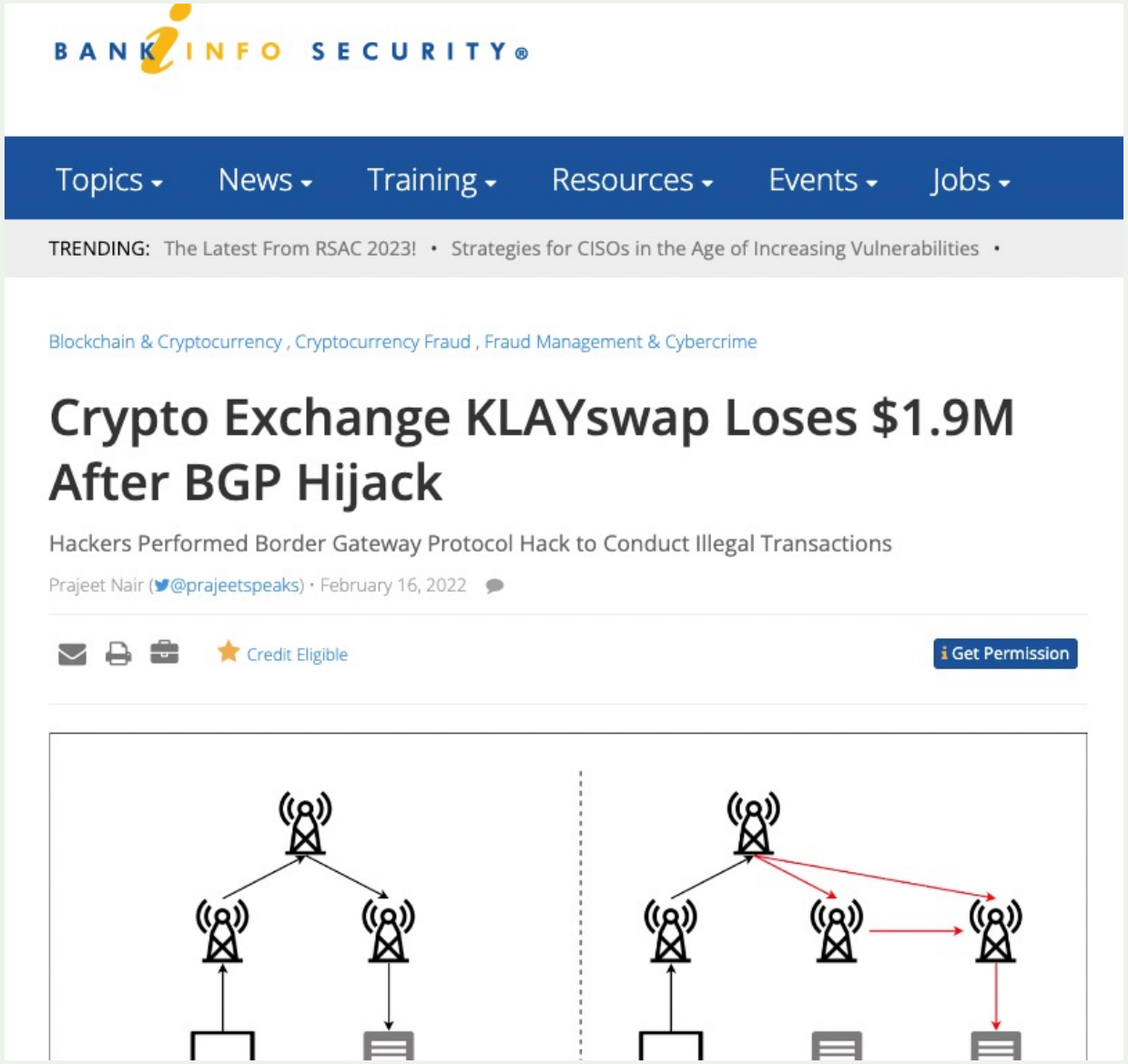
Back to KLAYswap

Repeat: This hijack could have been avoided - or at least minimized - if KakaoTalk had valid RPKI Route Origin Authorizations (ROAs) for its ASNs.

KLAYswap used a service with insecure routing infrastructure.

It cost them $1.9M.

These attacks happen surprisingly often.



BGP Insecurity Causes Real World Issues

3 Feb 2022	KLAYswap incident allows hackers to steal ~$1.9M USD in cryptocurrency assets
17 Apr 2021	Vodafone mistakenly announces 30K BGP routes causing a 13x increase in inbound traffic
1 Feb 2021	Myanmar military tries to block Twitter and accidentally hijacks Twitter's BGP traffic (Update: Twitter shored up its security!)
1 Apr 2020	Russian ISP Rostelecom announces prefixes belonging to Akamai, Cloudflare, Hetzner, Digital Ocean, Amazon AWS, and others
24 Jun 2019	Verizon caused outages at Cloudflare, Facebook, Amazon, and others after it wrongly accepted a network misconfiguration from a small ISP in Pennsylvania, USA.

https://www.manrs.org/2022/02/klayswap-another-bgp-hijack-targeting-crypto-wallets/
https://www.manrs.org/2021/04/a-major-bgp-hijack-by-as55410-vodafone-idea-ltd/
https://www.manrs.org/2021/02/did-someone-try-to-hijack-twitter-yes/
https://www.manrs.org/2022/03/lesson-learned-twitter-shored-up-its-routing-security/
https://www.manrs.org/2020/04/not-just-another-bgp-hijack/
https://www.manrs.org/2019/06/bgp-super-blunder-how-verizon-today-sparked-a-cascading-catastrophic-failure-that-knackered-cloudflare-amazon-etc/

Connectivity Providers and Enterprise Customers Must Work Together To Improve Routing Security

MANRS+

A second, elevated tier of MANRS participation for network operators that comply with more stringent requirements and auditing.

Work with industry partners to increase demand for security from their connectivity providers.

Connectivity Providers and their customers setting the requirements of the future quality mark for traffic security with the goal of eventually incorporating it in procurement policies and recommendations.

MANRS vs. MANRS+

MANRS

Established in 2014, nearly 1000 network operators, vendors, Internet exchange points, and CDN and cloud providers have joined.

Best practices including filtering, anti-spoofing, routing information, and coordination.

A security baseline – the bare minimum organizations of all sizes should be doing.

Historically, very little input from enterprise customers.

MANRS+

Currently in development by a MANRS+ Working Group. Please join!

Stronger and more detailed requirements enforcing best practices in traffic security.

High level of assurance of conformance. More profound technical audit and process audit.

Extended requirements, covering a broader set of risks related to routing and traffic security.

More focus on customer demands.

Proposed Requirements for MANRS+ Providers

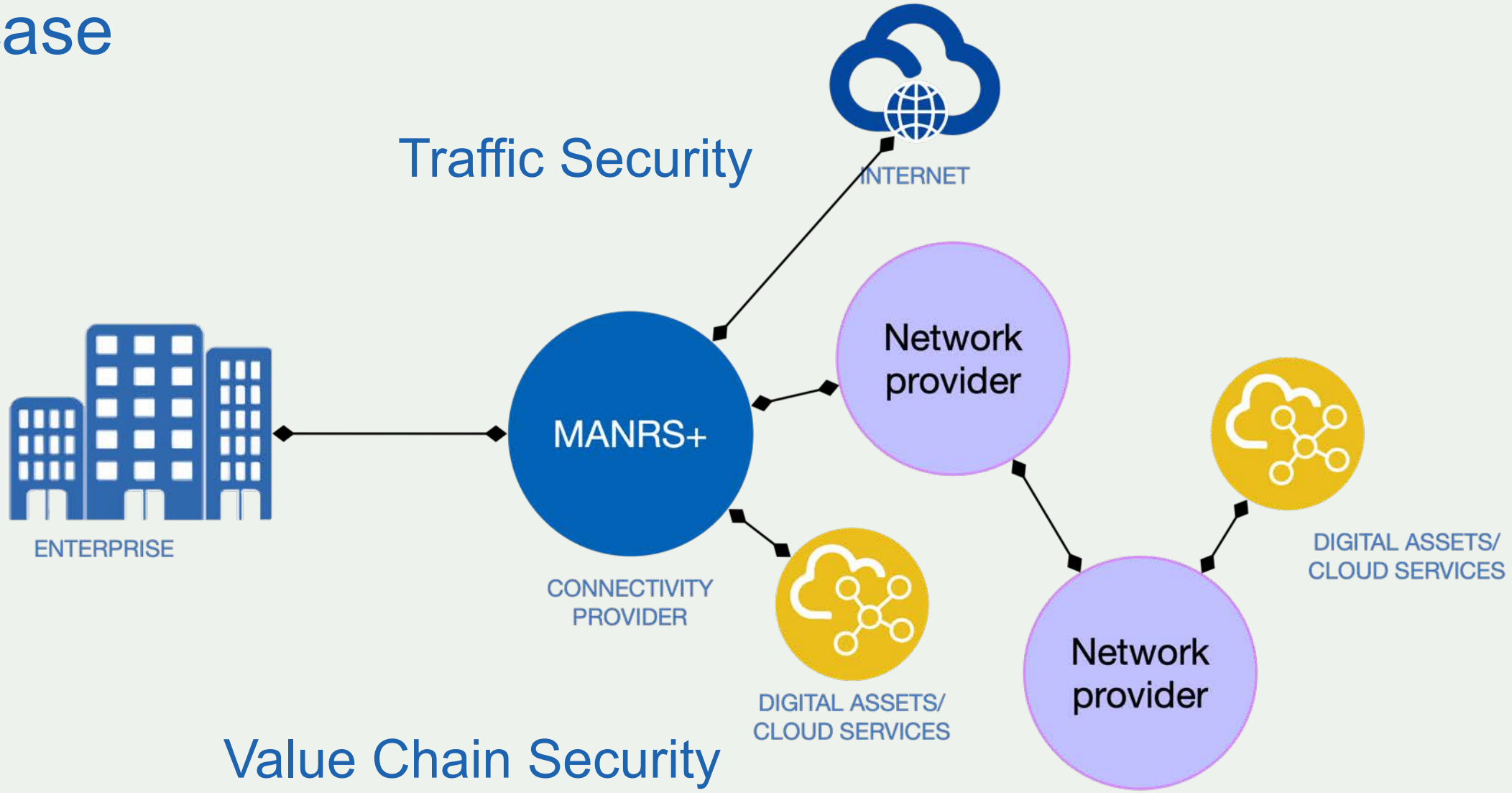
Path Security - Connectivity provider has detection capabilities and can mitigate the risk that traffic will be hijacked or detoured as a result of a mistake or an attack.

DDoS Attack Protection - Connectivity provider has detection and mitigating capabilities reducing the risk of a (volumetric) DoS attack.

Anti-Spoofing Protection - Connectivity provider detects and prevents traffic from their direct customers or peers with spoofed source IP addresses.

Routing Information - Connectivity provider has accessible complete and up-to-date documentation of the intended routing announcements (e.g. RPKI ROAs) and other information on its routing policy (e.g AS-SET) that is necessary for deploying effective security controls by the network.

A use case


Traffic Security
INTERNET
Network provider
MANRS+
ENTERPRISE
CONNECTIVITY PROVIDER
DIGITAL ASSETS/ CLOUD SERVICES
DIGITAL ASSETS/ CLOUD SERVICES
Network provider
Value Chain Security

Join the MANRS+ Working Group

Help identify your industry's needs and share what would make MANRS+ compelling to your business.

The group meets virtually 2x/month.

Membership is open to everyone. MANRS participation is not required.

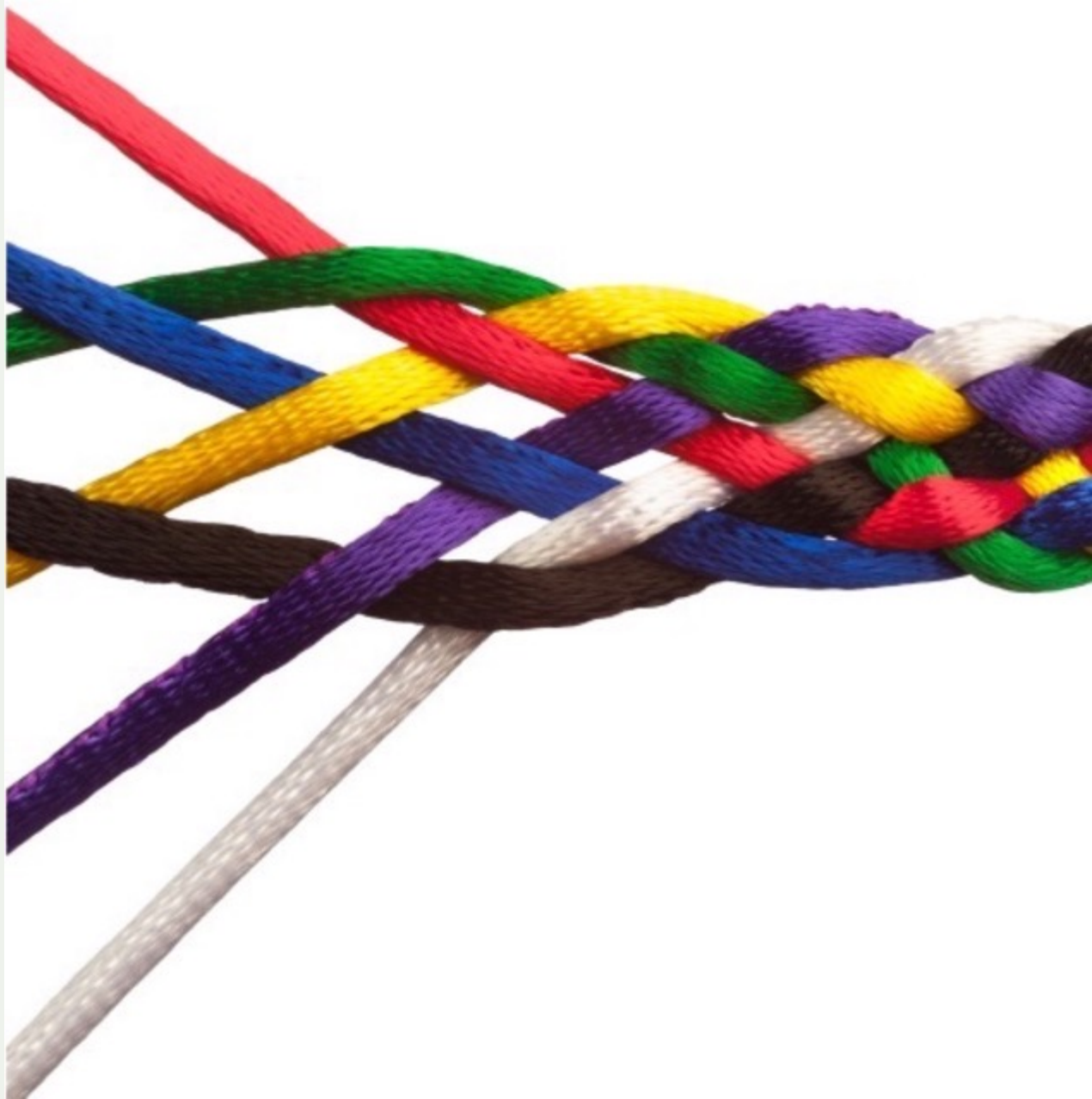
Join MANRS

Visit https://www.manrs.org and join as a network operator.

We can help you implement best practices:

- 1-pagers and primers for decision-makers
- Technical implementation guides
- Training courses
- MANRS Observatory & Tools

Contact us: contact@manrs.org



Thank you.

contact@manrs.org

manrs.org