# How can computer security incident response teams improve global routing security?

*Information for CSIRTs*

Today, the Internet plays an essential role in the majority of societies around the world. From banking to education, health to logistics, just about every sector relies on Internet-based applications and services to function.

The Internet is made up of many thousands of interconnected networks running the TCP/IP protocols (72,000 in June 2021). These networks are connected to each other using border gateway protocol (BGP). BGP is the only gateway protocol currently available.

The problem with BGP is that it was designed for a predominantly academic environment. Security wasn't a significant consideration, as participating networks could be expected to cooperate to keep the network in good health. BGP is therefore based entirely on unverified trust between networks.

Unfortunately, this makes the Internet's global routing system inherently insecure. It is increasingly under attack, either by organized criminals who see the opportunity to steal data and cause disruption, or because of misconfiguration and mistakes.

## What do CSIRTs have to do with routing security?

As a member of a computer security incident response team (CSIRT), you're involved in developing security awareness and mitigation measures for your end users. Yet most CSIRTs don't include routing security as part of infrastructure security within their service portfolios. This is despite the routing system being a key element of critical national and international infrastructure.

While CSIRTs generally don't run networks, you do possess specialized knowledge of attacks and threats, as well as mitigation and resolution strategies. You're also responsible for recommending best practices for securing systems, networks, and critical data and assets, along with other incident prevention.

In support of the Internet security portfolio, as part of a CSIRT, we'd like to encourage you to work with others to improve global routing security, while taking a holistic view of the Internet security ecosystem. This is where MANRS comes in.

## What is MANRS?

Mutually Agreed Norms for Routing Security (MANRS) is supported by the Internet Society. It's a community of responsible network operators, content providers and IXPs committed to improving the security and resilience of the Internet. It offers a set of best practices based on existing norms for network operators to improve the security of the global Internet routing system.

By choosing service providers that are MANRS compliant, organizations can both help improve their network and encourage other providers into improving their infrastructure.

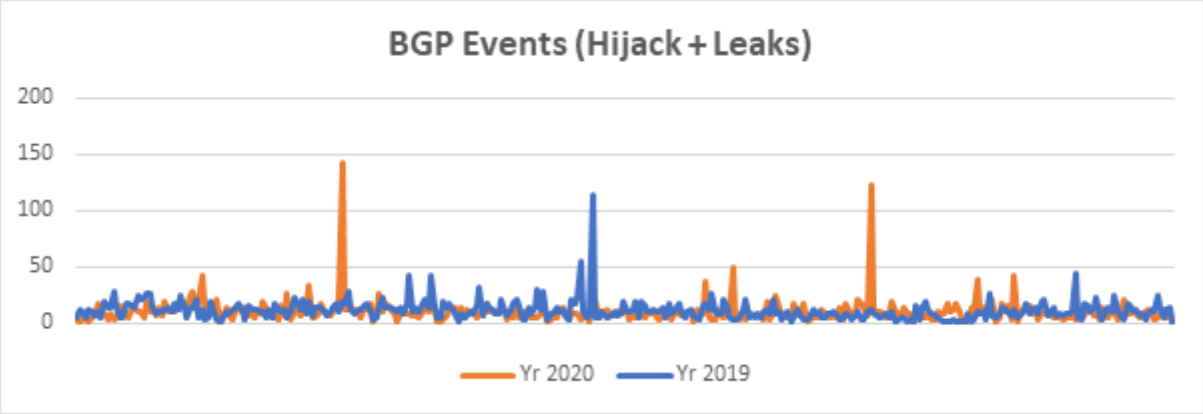
MANRS defines four simple but concrete actions for network operators to implement to greatly improve Internet security and reliability. These include:

1. **Filtering** – defining a clear routing policy and implementing a system to ensure that announcements to adjacent networks are correct.
2. **Anti-spoofing** – enabling source address validation (SAV) and implementing anti-spoofing to prevent packets with incorrect source IP addresses from entering and leaving the network.
3. **Coordination** – maintaining globally accessible up-to-date contact information to assist with incident response.
4. **Global validation** – publishing data that enables other stakeholders to validate routing information on a global scale.

The MANRS actions define outcomes rather than specific methods. This allows implementation to change with technology and helps establish the MANRS actions as best practice.

## Why does MANRS matter?

In 2020, there were a total of 3,873 major network incidents that involved border gateway protocol (BGP) related attacks. Of these, 64% were hijacks and the rest were route leaks.




In 2019, there were 4,232 major network incidents that involved BGP, of which:

- 3.8% of all networks were affected by a routing incident
- 2% of all networks were responsible for the 4,232 routing security incidents.

These incidents can:

- create a serious strain on infrastructure
- result in dropped traffic
- allow for unauthorized inspection of traffic
- be used to perform Denial of Service (DoS) attacks.

## Routing incidents cause real-world problems

In July 2020, there were two significant routing incidents in the global BGP routing system[2], impacting more than 1,500 networks worldwide. This highlighted the need for network operators to implement good routing security practices. These incidents impacted major North American network providers including TWC, Rogers and Charter, among others[3].

Aside from these headline cases, routing incidents are happening every day and the stability and security of the Internet routing system is at significant risk.

An independent study by 451 Research commissioned by the Internet Society[1] found that traffic routing, hijacking and interception were the leading security concern for enterprises. Distributed denial of service (DDoS) attacks and address spoofing were second.

94% of enterprises said that, in a competitive situation, they'd be willing to pay more for a vendor who was an MANRS member.

This shows that MANRS implementation is a good indicator of a network operator's sound security practices. However, this research also showed that there's a general lack of understanding that simple steps can dramatically reduce such incidents.

## How can MANRS help?

As part of MANRS' capacity building and community engagement initiatives, we'd like to support CSIRT communities in the following areas:

- raising awareness of routing security issues within your communities
- encouraging other CSIRTs to add routing security incident monitoring and incident handling to their service portfolios
- encouraging CSIRTS to adopt the MANRS Observatory monitoring tool to provide situational awareness of routing security
- extending the reach of the MANRS initiative within CSIRT constituencies, as well as into national critical infrastructure initiatives
- holding practical routing security workshops or co-developing a routing security curriculum in the context of training-the-trainers and/or network forensics capacity building programs
- adding routing security to network security auditing programs.

In turn, CSIRTs can:

- help encourage their parent organizations or constituents to take routing security issues more seriously
- raise awareness with governments of how routing security issues can affect critical infrastructure
- encourage the adoption of routing security recommendations (such as NIST standards).

Given the significant impact of routing incidents on critical networks, we need to give high priority to protecting and improving our network infrastructure.

- Find out more about MANRS: manrs.org/resources/policy
- Read about the Internet Society's work: internetsociety.org

[1] MANRS project study report: https://www.manrs.org/wp-content/uploads/2017/10/MANRS-451-Study-Report.pdf