



# MANRS

Mutually Agreed Norms for Routing Security

Christian O'Flaherty

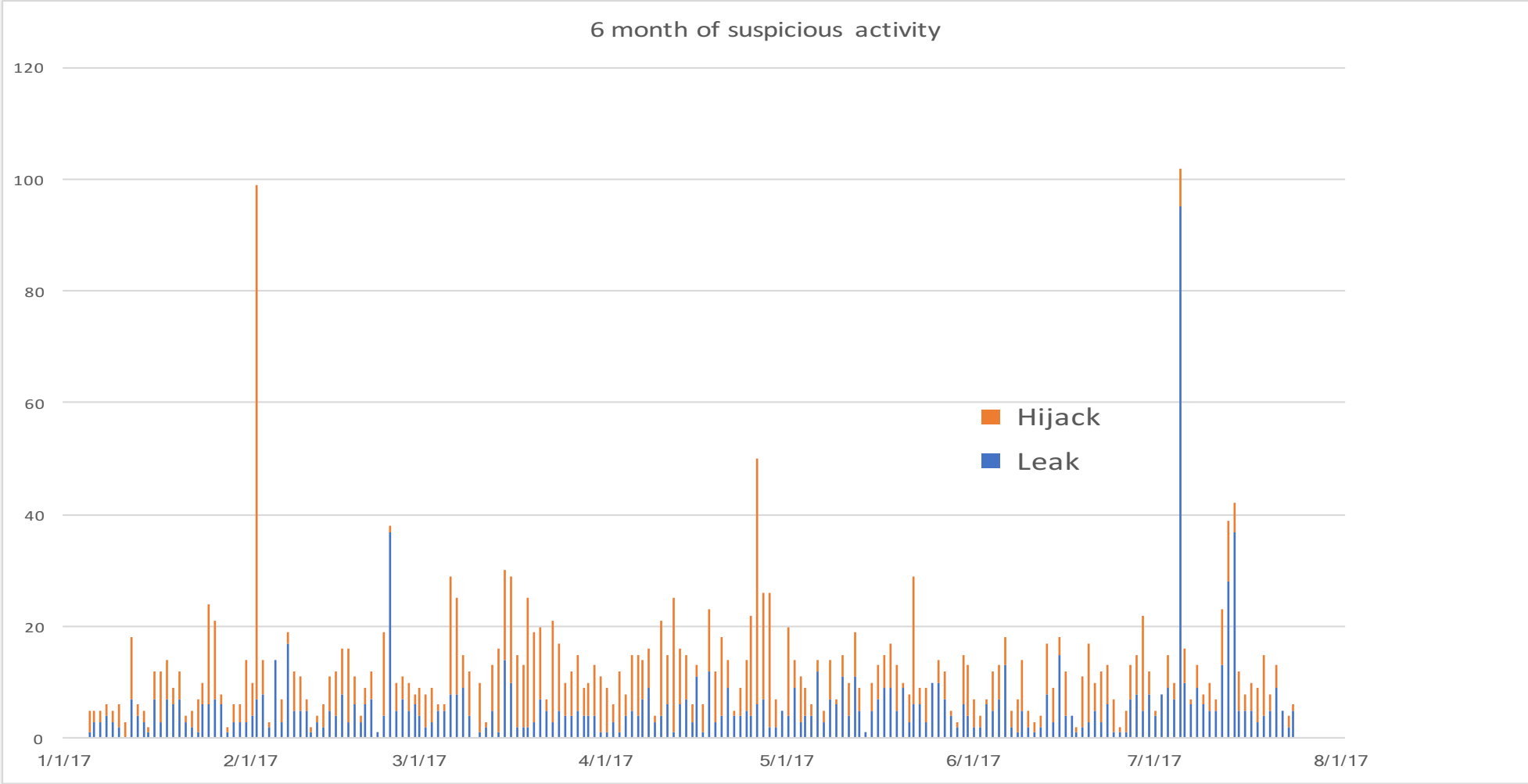
[oflaherty@isoc.org](mailto:oflaherty@isoc.org)

# The Problem

A Routing Security Overview



# No Day Without a Routing Incident



# The Threats: What's Happening?

Event	Explanation	Repercussions	Solution
<b>Prefix/Route Hijacking</b>	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
<b>Route Leak</b>	A network operator with multiple upstream providers (often due to accidental misconfiguration) announces to one upstream provider that it has a route to a destination through the other upstream provider.	Can be used for traffic inspection and reconnaissance.	Stronger filtering policies
<b>IP Address Spoofing</b>	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

# 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 standard 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.



# 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.





# MANRS four simple but concrete 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



# 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



# 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.

Christian O'Flaherty  
oflaherty@isoc.org

manrs.org

