

What if Public Administration demanded educated MANRS from ISPs?

What is the problem

we would like to solve?



General Data Protection Regulation

WHAT ARE YOU WORKING ON?

TRYING TO FIX THE PROBLEMS I
CREATED WHEN I TRIED TO FIX
THE PROBLEMS I CREATED WHEN
I TRIED TO FIX THE PROBLEMS
I CREATED WHEN...



The Problem

A Routing Security Overview

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.

Imagine the outrage if a route leak impacted the ability of Italians to watch the Serie A Final next year!



The Honor System: Routing Issues

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

- Created before security was a concern
- Assumes all networks are trustworthy
- No built-in validation that updates are legitimate
- The chain of trust spans continents
- Lack of reliable resource data



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 it 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

Collaboration and Consensus

Your security is in someone else's hands. The actions of others directly impact you and your network security (and vice versa).

Why should they help you? You can start by helping them.

Where is the line between good and bad routing security?

We need globally recognized security expectations for all network operators to raise the bar on 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.

Solutions?



BLOCKCHAIN



The Solution: Mutually Agreed Norms for Routing Security (MANRS)

Provides crucial fixes to reduce 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 sets a new norm for routing security.



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.

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

MANRS Actions for Operators

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 Italian 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 complaints
- Enterprises indicate willingness to pay more for secure services

How the Italian Government can strengthen routing security

Leading by example

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

Driving 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.

Encouraging 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.

Italian PA - Some Background

SPC(1)

Public System for Connectivity first edition



2005

Won by

Fastweb (AS12874), BT Italia (AS8968)

Wind Telecomunicazioni (AS1267) e Telecom Italia (AS3269)

SPC1 contents:

Connectivity (transport, support, voip, interoperability, maintenance)

Security (firewall, antivirus, network intrusion detection, log, vpn...)

SPC1 ended in May, 2017

Italian PA - Some Background

SPC2

Public System for Connectivity second edition

2015

Won by

Fastweb (formerly Tiscali) (AS12874)

BT Italia (AS8968), **Vodafone Italia** (AS30722)

SPC2 contents: IP data transport, network security services and VOIP services

IP, SECURITY, VOIP

Duration 7 years

Value not to exceed **2.4 billion** euros

Italian PA - Some Background

Central State administrations distribution to winning ISPs

<p> Agenzia Sp... Italiana Agenzia de... D... e... (M... poli) Agenzia IC... Agenzia Nazionale per il Turismo - ENIT Agenzia Nazionale Sicurezza Ferrovie - ANSF Agenzia per la Logistica in Agricoltura - AEA Arma Car... Avvocatura Generale dello Stato Ente Nazionale Assistenza Civile - ENAC INPS Istituto Nazionale di Geologia e Vulcanologia - ING Istituto Superiore di Sanità - ISS Istituto Superiore per la Produzione e la Ricerca Ambientale - ISPRA Ministero Economia e Finanze - MEF ed Agenzie fiscali Scuola Nazionale dell'Amministrazione Istituto per lo sviluppo della formazione professionale dei lavoratori Istituto Nazionale di Ricerca per gli Alimenti e la Nutrizione FASTWEB </p>	<p> Agenzia Italiana per la cooperazione allo sviluppo Consiglio Nazionale delle Ricerche - CNR Corte dei Conti Ministero Affari Esteri - MAE Ministero della Difesa Ministero della Giustizia Ministero dell'Ambiente e della Tutela del Territorio e del Mare Ministero delle Politiche Agricole e Forestali - MIPAF Ministero dell'Istruzione, dell'Università e della Ricerca Ministero dello Sviluppo Economico - MISE Parlamento del Consiglio dei Ministri Presidenza del Consiglio dei Ministri Dipartimento Protezione Civile BT </p>	<p> ACLI Agenzia Italiana di Fianco - AIFA Consiglio di Stato Consiglio per la Ricerca in Agricoltura e Analisi dell'economia agraria Guardia di Finanza INAIL Istituto Nazionale di Statistica - ISTAT Istituto Geografico e Zecca dello Stato Ministero dei Beni e delle Attività Culturali e del Turismo Ministero del Lavoro e delle Politiche Sociali Ministero della Salute Ministero delle Infrastrutture e dei Trasporti - MIT Ministero Inter... Vodafone SBI 59715 AP </p>
--	--	---

Italian PA - Some Background

Territorial administrations

20 Regions

14 Big Cities

93 Provinces

7984 Municipalities

FASTWEB



SBT
5 9 7 1 5
AP

MANRS as a requirement

A suggestion for CONSIP or other public procurement entities in Italy:

To strengthen routing security in Italy, MANRS participation should be a **requirement** (or at least a strong **consideration**) for an ISP to win the next main Internet transit agreement valid for the

MANRS: who is there?

Currently only 5 Italian
ASes out of 1,000 declare
to be MANRS compliant

{None of the former or present winning Internet providers of the Italian PA has qualified for MANRS so far.}

Join Us

Visit <https://www.manrs.org>

- Fill out the sign up form with as much detail as possible.
- In response we may ask questions and test your network.

Get Involved in the Community

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

Internet

Help Is Available

If you're not ready to join yet, implementation guidance is available to help you:

- **an Implementation Guide** based on Best Current Operational Practices deployed by network operators around the world
- **six training modules** based on information in the Implementation Guide.

2001:db8:1001::/48
192.0.2.0/24

2001:db8:2002::/48
198.51.100.0/24

AS64500
MANRS
Participant
network

BCP38 filter
applied on
downstream
interface on the
PE router

AS64501
Single-homed
stub customer

AS64502
Single-homed
stub customer

What's Next: MANRS Observatory

Provide a factual state of security and resilience of the Internet routing system and track it over time.

Measurements will be:

- Transparent – using publicly accessible data
- Passive – no cooperation from networks required
- Evolving – the MANRS community will decide what gets measured and how

Grand totals for all repositories

	Object accepted	Manifest interval overruns certificate	certificate has expired	Policy Qualifier CPS	Stale CRL or manifest
None .cer	5501			773	
None .crl	5496				1
None .gbr	3				
None .mft	5496	1	1	773	1
None .roa	5463			580	
Total	21959	1	1	2126	2

Current total object counts (distinct URIs)

Repository	.cer	.crl	.gbr	.mft	.roa
ca.rg.net					
ca0.rpki.net					
localcert.ripe.net					
repository.lacnic.net					
rpki-pilot.lab.dtag.de					
rpki.afrinic.net					
rpki.apnic.net					
rpki.ripe.net					
Total	0	0	0	0	0

Overview for repository ca.rg.net

	Object accepted	Manifest interval overruns certificate	certificate has expired	Policy Qualifier CPS	Stale CRL or manifest
None .cer	1				
None .crl	2				1
None .gbr	1				
None .mft	2				1
None .roa	35				

What's Next: Hands-on Lab

We are designing a lab that will allow engineers to practically implement MANRS in a simulated network environment. The lab will be available:

- Via MANRS training partners
- Online

Get in touch with us if you would like to host the MANRS training lab environment!

