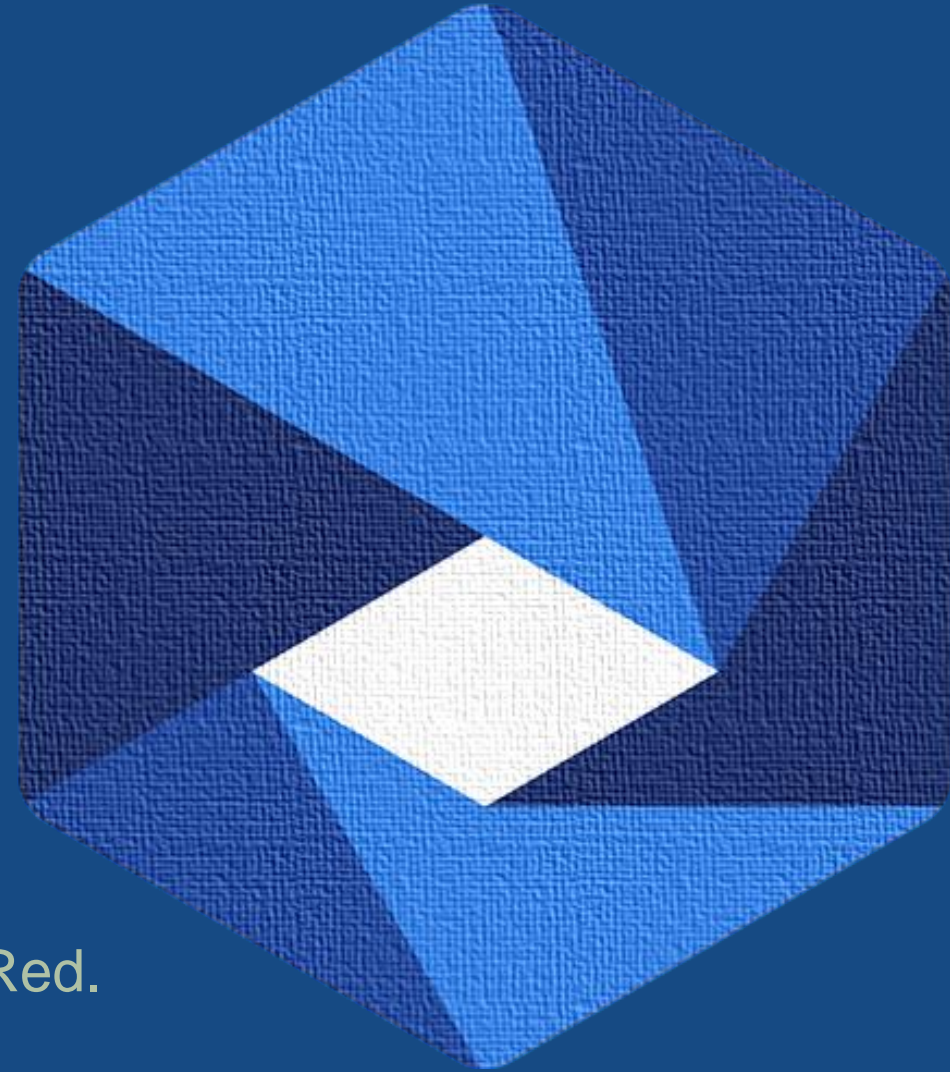


Seguridad en el Core de Internet

MANRS para Operadores de Red.





MANRS

Mutually Agreed Norms for Routing Security

Daniel Mondragón

Email: dmondragon@nic.cr

Emmanuel Serrano

Email: spina@correo.uady.mx

Temas de la Sesión

Sesión 1: Introducción a MANRS

Sesión 2:

- IRRs, RPKI, and PeeringDB
- Coordinación y Validación Global
- Filtrado: prevención de la propagación de información de enrutamiento incorrecta
- Anti-Suplantación: Prevención del tráfico con direcciones IP de origen falsificadas



TE INVITAMOS A SER PARTE DEL TUTORIAL

MANRS PARA OPERADORES DE RED IXSY Y WIPSMX

Fecha: 27 de junio, 17:00 hrs. MEX, 19:00 hrs. ARG



Instructores:
Mauricio Oviedo MANRS Fellow 2022
Emmanuel Serrano MANRS Fellow 2021

Registro: <https://ixsy.org.mx/eventos-2022>



Sesión 1: Contenido

Introducción y Antecedentes: El problema

- Estadísticas
- Incidencias de Enrutamiento

MANRS: Programas

Recursos Disponibles y Autoevaluación

MANRS Observatory

Caso de Negocio

Conclusiones



¿Por qué es importante la seguridad de las rutas?

A Routing Overview



Conceptos Básicos: Cómo funciona el enrutamiento

Existen ~70,000 redes centrales (Sistemas Autónomos) en Internet, cada una de las cuales utiliza un único Número de Sistema Autónomo (ASN) para identificarse con otras redes.

Los Ruteadores utilizan Border Gateway Protocol (BGP) para intercambiar “información alcanzable” – redes a las que saben cómo llegar.

Los Ruteadores construyen una “tabla de ruteo” y elijen la mejor ruta al enviar un paquete, generalmente basado en la ruta más corta.



El problema

A Routing Security Overview



Los incidentes de enrutamiento están incrementando

En 2020, hubo un total de 3,873 incidentes de red importantes que involucraron ataques relacionados con Border Gateway Protocol (BGP). De estos, el 64% fueron secuestros y el resto fueron fugas de ruta.

En 2019, hubo 4,232 incidentes importantes en la red que involucraron a BGP, de los cuales:

- el **3.8%** de todas las redes fueron afectadas por un incidente de enrutamiento
- el **2%** de todas las redes fueron responsables de los 4,232 incidentes de seguridad de enrutamiento.

En lo que va del año 2022, se han presentado +4,000 incidentes de ruteo (27 de junio), de los cuales +1,200 han sido críticos y registrados en bgpstream.com



Los incidentes son de escala global, con efecto cascada.



Los incidentes de enrutamiento están incrementando

Estos incidentes de secuestro de rutas provocaron una serie de problemas que incluyen:

- datos robados;
- pérdida de ingresos;
- daño en la reputación;

Algunos de estos secuestros duraron muchas horas.



El Sistema de Honor: Problemas de Enrutamiento

Border Gateway Protocol (BGP) está basado enteramente en la confianza entre ambas redes

- Creado antes de que la seguridad fuera una preocupación.
- Asume que todas las redes son confiables.
- Sin validación de que las actualizaciones son legítimas.
- La cadena de confianza se extiende por continentes.
- Falta de datos de recursos confiables.



Los incidentes de Enrutamiento causan problemas del mundo real

El enrutamiento inseguro es uno de los caminos más comunes para las amenazas maliciosas.

Los ataques pueden tardar desde horas hasta meses en reconocerse.

Estos ataques o incidentes pueden:

- causar estragos graves en la infraestructura;
- conllevar la caída del tráfico;
- permitir la inspección no autorizada del tráfico;
- utilizarse para realizar ataques de denegación de servicio (DoS).

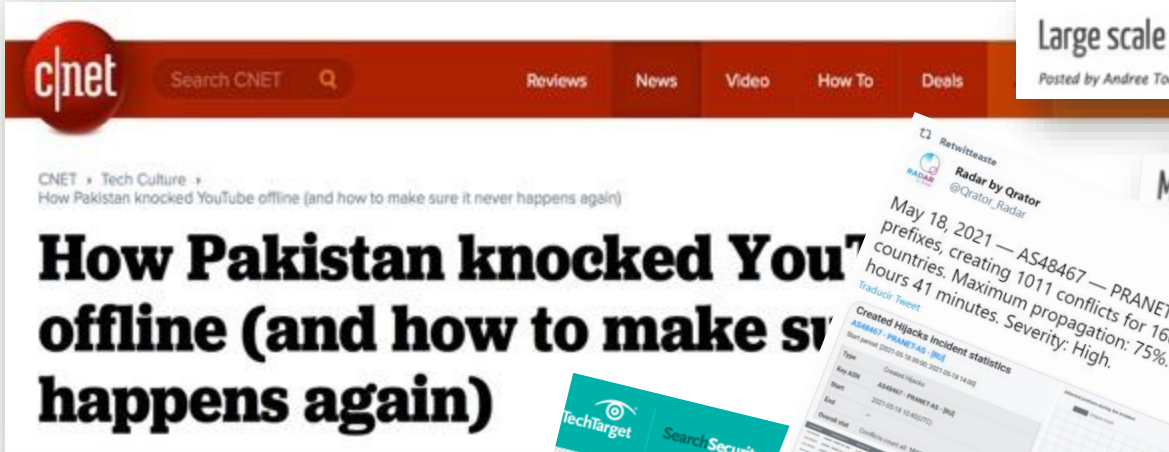
Los errores involuntarios pueden desconectar a países enteros, mientras que los atacantes pueden robar los datos de una persona o retener la red de una organización.



Lo cual lleva a ...

A Major BGP Hijack by AS55410-Vodafone Idea Ltd

April 17, 2021 by Afab Siddiqui Leave a Comment



c|net Search CNET Q Reviews News Video How To Deals

CNET • Tech Culture • How Pakistan knocked YouTube offline (and how to make sure it never happens again)

How Pakistan knocked YouTube offline (and how to make sure it never happens again)



Large scale BGP hijack out of India

Posted by Andree Toonk - November 6, 2015 - Hijack - 1 Comment



Routing Leak briefly takes down Google

MARCH 12, 2015 COMMENTS (15) VIEWS: 37374 ENGINEERING, INTERNET, LATENCY, PERFORMANCE, SECURITY DOUG MADORY



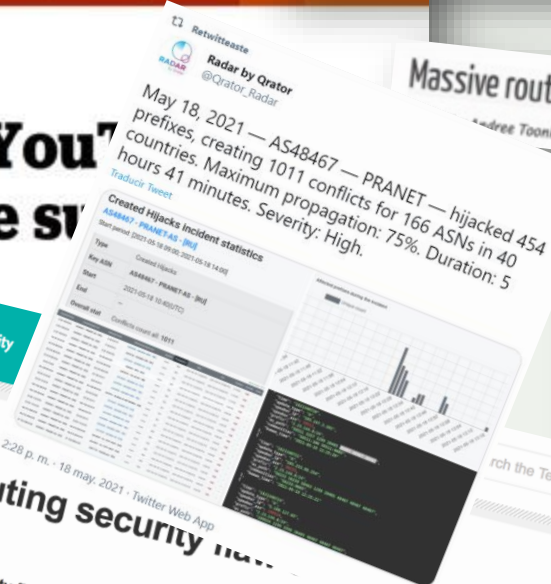
UK traffic diverted through Ukraine

VIEWS: 47297 SECURITY DOUG MADORY



Massive route leak causes Internet slowdown

Andree Toonk - June 12, 2015 - BGP instability - No Comments



Retweet Radar by Qrator @Qrator_Radar

May 18, 2021 — AS48467 — PRANET — hijacked 454 prefixes, creating 1011 conflicts for 166 ASNs in 40 hours 41 minutes. Severity: High.

Type	Created Hijacks
AS48467 - PRANET AS - IN	454

Created Hijacks Incident statistics

AS48467 - PRANET AS - IN

Start period: 2021-05-18 09:00:00 2021-05-18 14:00:00

Row ASN Created Hijacks

Start 2021-05-18 10:00:00

End 2021-05-18 10:00:00

Prefix list Conflicts count: 1011



DDoS Attacks Storm Linode Servers Worldwide

BY DOUGLAS BONDERUD • JANUARY 5, 2016



Global Impacts of Recent L

OCTOBER 14, 2015 COMMENTS (2) VIEWS: 9681 PERFORMANCE, SECURITY



BGP routing security incident

2:28 p. m. - 18 may, 2021 - Twitter Web App

A BGP routing security flaw enabled unknown threat actors to steal cryptocurrency by hijacking internet routing and rerouting traffic to a phishing site in Russia.



BGP hijack incident by Syrian Telecommunications Estab

Posted by Andree Toonk - December 9, 2014 - Hijack - 2 Comments

COMMENTS (17) VIEWS: 36909 SECURITY DOUG MADORY



Amazon Route 53



Hijack Targets Palestinian



The Vast World of Fraudulent Routing



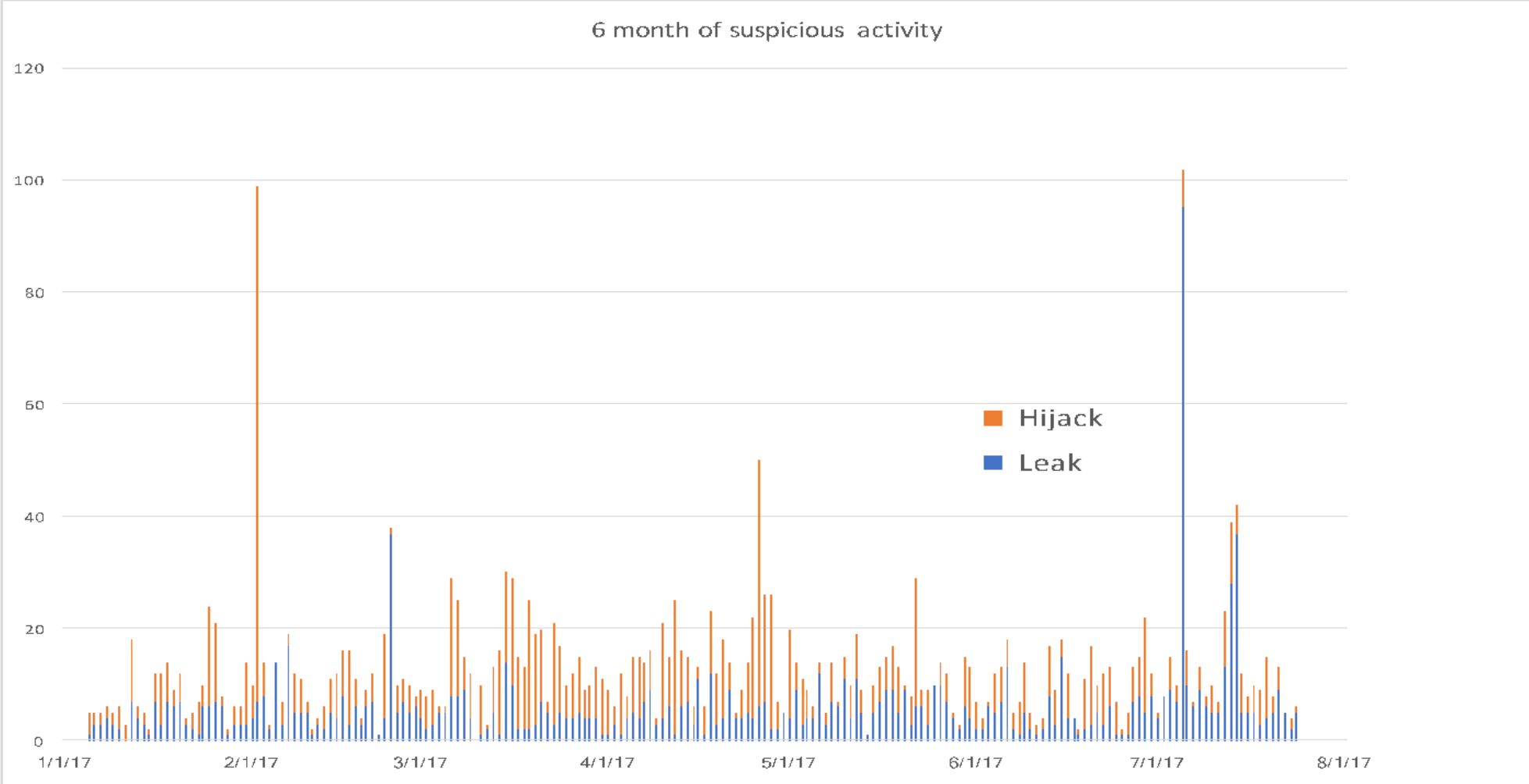
DDoS attack on BBC may have been biggest



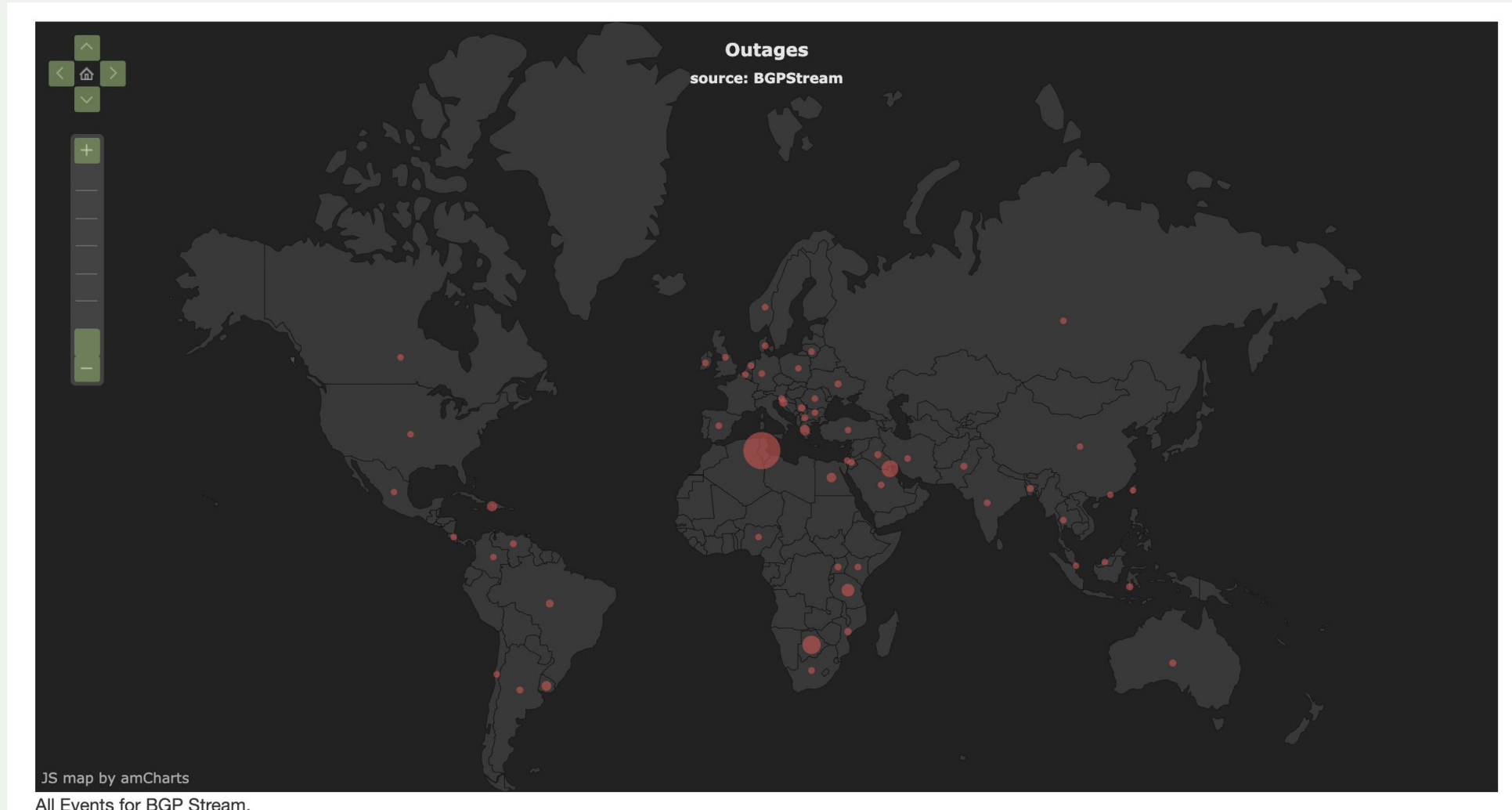
CRYPTO NEWS

MyEtherWallet DNS Hijacked, \$150,000 Worth of Eth Stolen

No hay día sin un Incidente



No hay día sin un Incidente



Incidentes del 27/06/22

<http://bgpstream.com/>



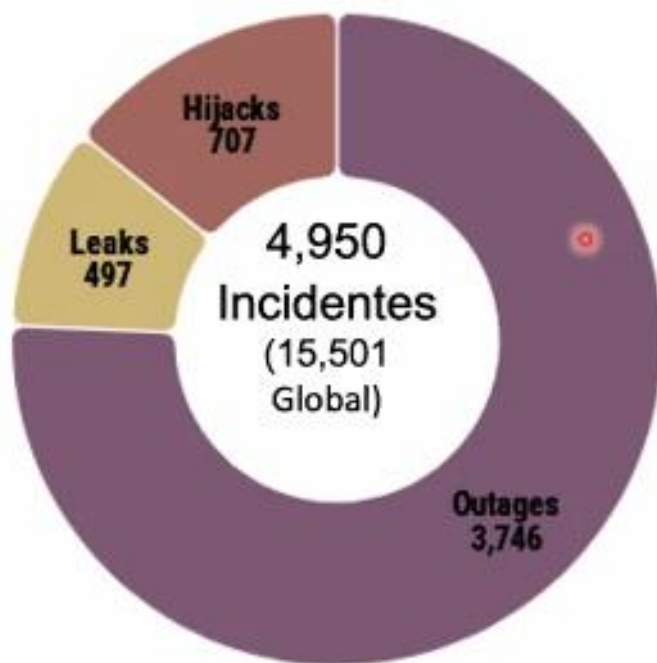
Cantidad de incidentes en LAC

Fuente: Informe sobre seguridad en el ruteo de LAC – Augusto Mathurín, 2019

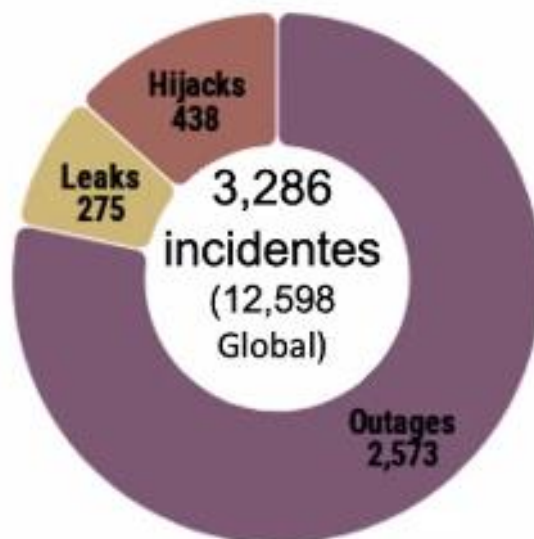
<https://www.lacnic.net/innovaportal/file/4297/1/fort-informe-seguridad-ruteo-es.pdf>

■ Outages ■ Leaks ■ Hijacks

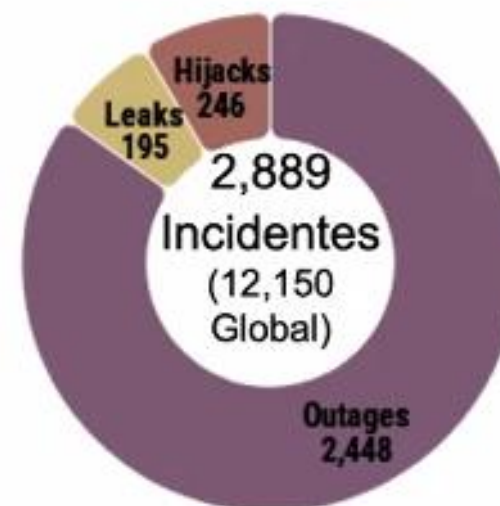
2017



2018



2019 (proyectado)



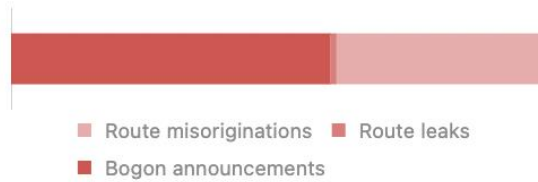
Overview

State of Routing Security

Number of incidents, networks involved and quality of published routing information in the IRR and RPKI in the selected region and time period

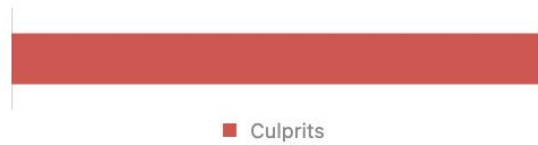
Incidents

Route misoriginations	66
Route leaks	2
Bogon announcements	104
Total	172



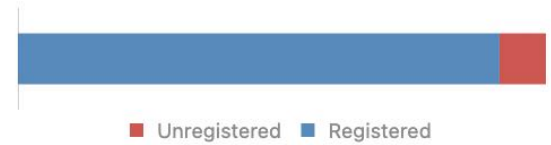
Culprits

Culprits 130



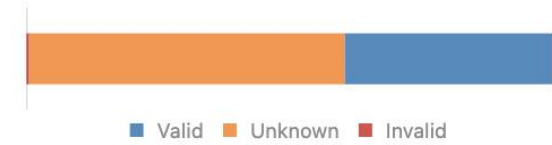
Routing completeness (IRR)

Unregistered	14,371	8.8%
Registered	148,801	91.2%



Routing completeness (RPKI)

Valid	64,714	39.6%
Unknown	97,692	59.9%
Invalid	766	0.5%



MANRS Readiness

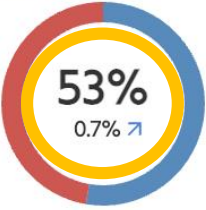
Filtering



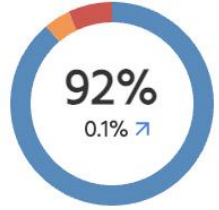
Anti-spoofing



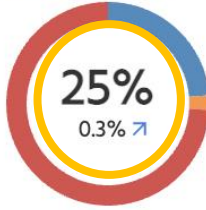
Coordination



Global Validation IRR



Global Validation RPKI



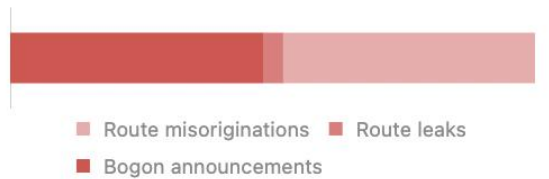
Overview

State of Routing Security

Number of incidents, networks involved and quality of published routing information in the IRR and RPKI in the selected region and time period

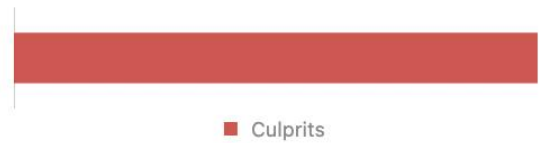
Incidents ⓘ

Route misoriginations	714
Route leaks	57
Bogon announcements	717
Total	1,488



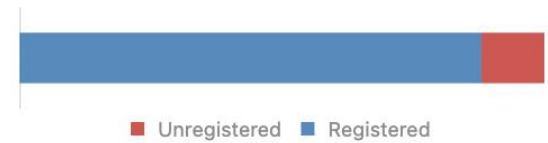
Culprits ⓘ

Culprits: 1,043



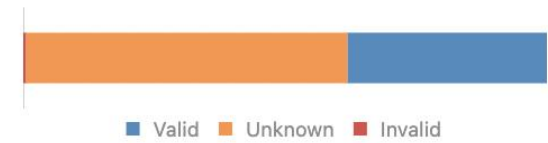
Routing completeness (IRR) ⓘ

Unregistered	133,477	12.0%
Registered	974,284	88.0%



Routing completeness (RPKI) ⓘ

Valid	422,603	38.1%
Unknown	679,823	61.4%
Invalid	5,335	0.5%

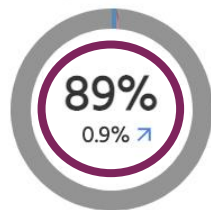


MANRS Readiness ⓘ

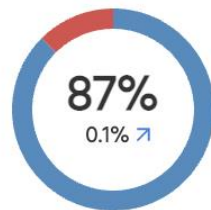
Filtering ⓘ



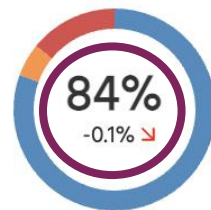
Anti-spoofing ⓘ



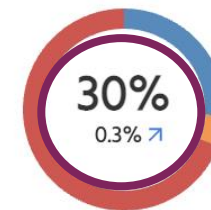
Coordination ⓘ



Global Validation IRR ⓘ



Global Validation RPKI ⓘ



Incidentes en el ruteo



Los Incidentes de Enrutamiento causan problemas del mundo real

Prefix/Route Hijacking

Secuestro de prefijo/ruta

Route Leak

Fuga de Ruta

IP Address Spoofing

Direcciones ip falsificadas

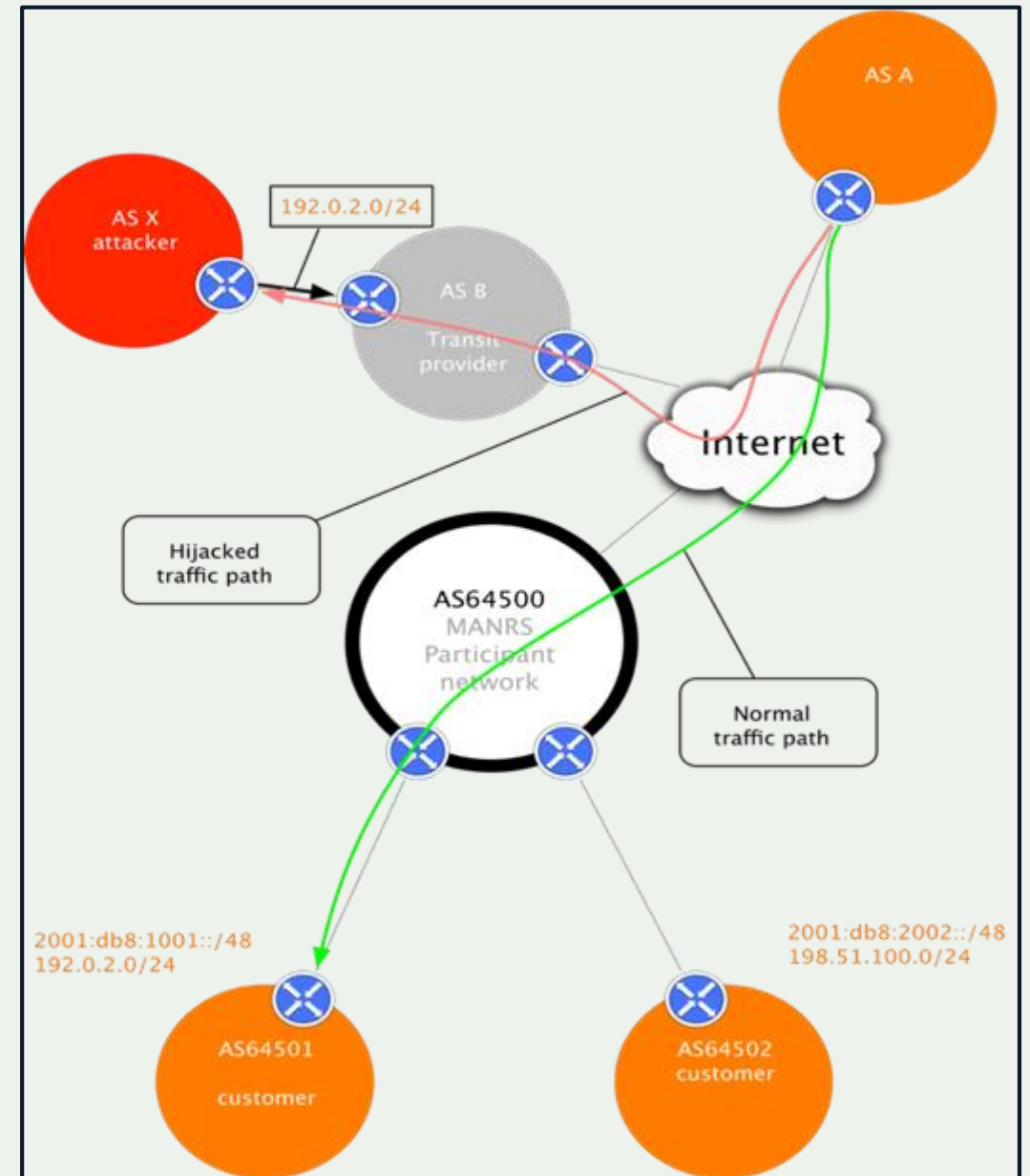


Prefix/Route Hijacking

Route hijacking, también conocido como “BGP hijacking” cuando un operador de red o atacante (accidentalmente o deliberadamente) se hace pasar por otro operador de red o finge que un servidor o red es su cliente. Esto enruta el tráfico a un operador de red, cuando hay otra ruta real disponible.

Ejemplo: El 2008 YouTube hijack; un intento de bloquear YouTube mediante el secuestro de rutas provocó que gran parte del tráfico de YouTube se cayera en todo el mundo.

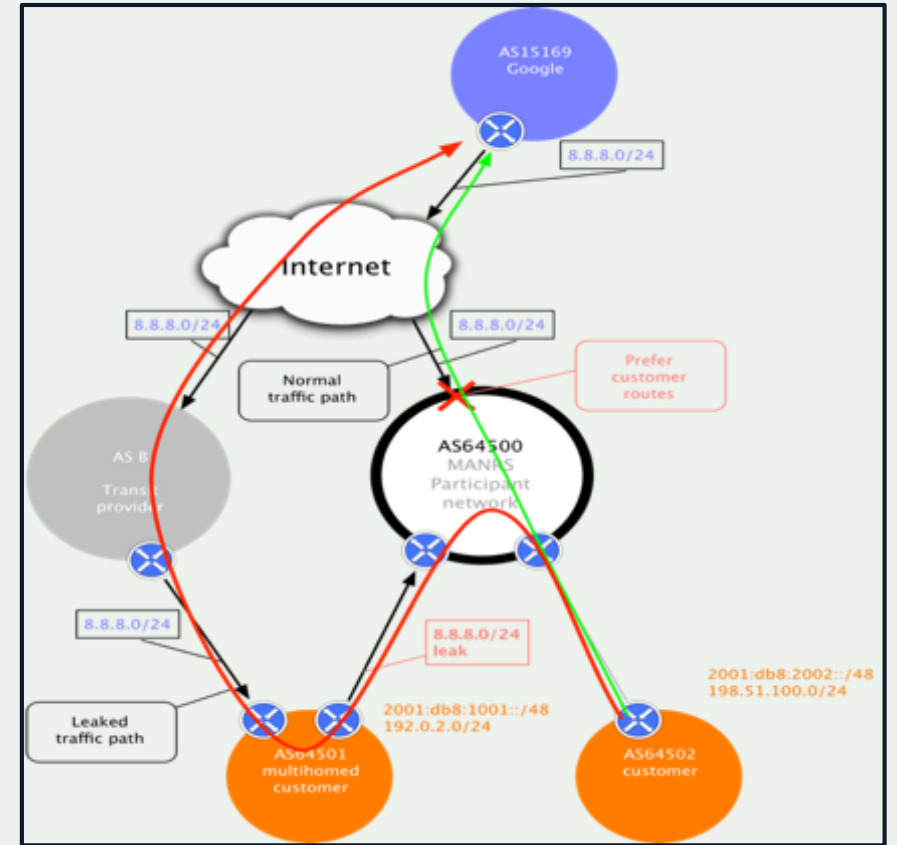
Solución: Políticas de filtrado sólidas (las redes adyacentes deben fortalecer sus políticas de filtrado para evitar anuncios falsos).



Route Leak

Un Route Leak o fuga de ruta es un problema en el que el operador de red con varios proveedores upstream anuncia accidentalmente a uno de sus proveedores upstream que tiene una ruta a un destino a través del otro proveedor upstream. Esto hace que la red sea una red intermedia entre los dos proveedores de upstream. Con uno enviando tráfico ahora a través de él para llegar al otro.

Ejemplo: 2015, Malaysia Telecom y Level 3, un importante proveedor de backbone. Malaysia Telecom dijo a una de las redes de Level 3 que era capaz de enviar tráfico a cualquier lugar de Internet. Una vez que Level 3 decidió que la ruta a través de Malaysia Telecom parecía la mejor opción, desvió una gran cantidad de tráfico a Malaysia Telecom.



Solución: Políticas de filtrado sólidas (Las redes adyacentes deben fortalecer sus políticas de filtrado para evitar aceptar anuncios que no tienen sentido).

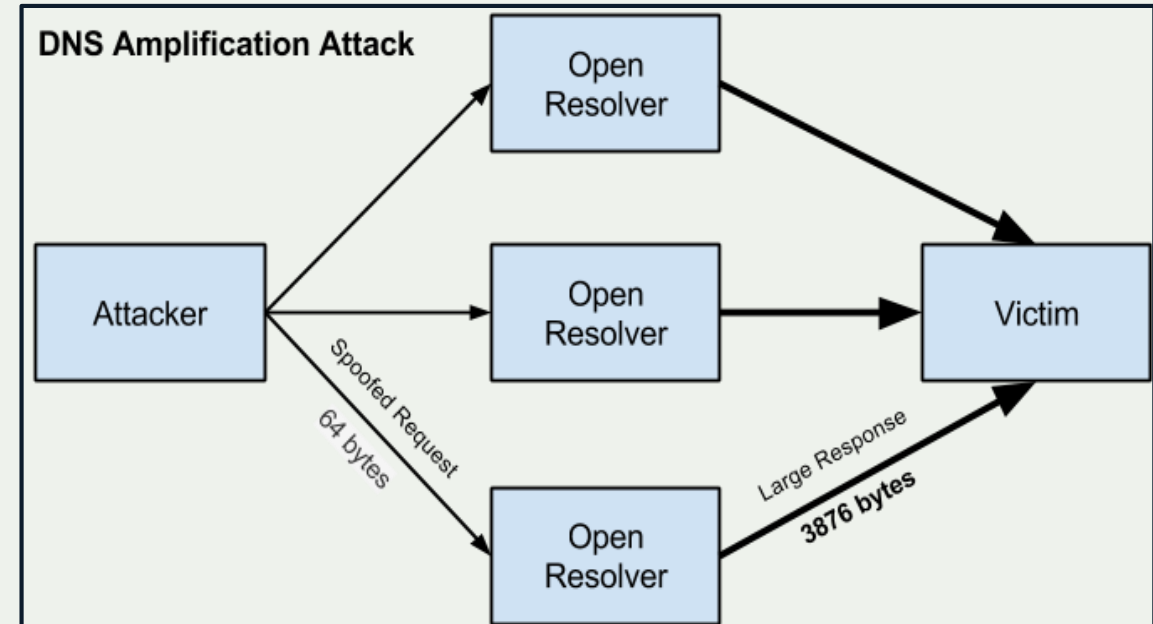


IP Address Spoofing

IP address spoofing se utiliza para ocultar la verdadera identidad del servidor o para hacerse pasar por otro servidor. Esta técnica se puede utilizar para amplificar un ataque.

Ejemplo: Ataque de amplificación de DNS. Al enviar múltiples solicitudes falsificadas a diferentes resolutores de DNS, un atacante puede solicitar que se envíen muchas respuestas del resolutor de DNS a un objetivo, mientras que solo usa un Sistema para atacar.

Solución: Validación de la dirección de origen: los sistemas para validación de la dirección de origen pueden ayudar a determinar si los usuarios finales y las redes de los clientes tienen direcciones IP de origen correctas (combinadas con el filtrado)



Herramientas para ayudar

- Prefix y filtrado AS-PATH
- RPKI validator, IRR toolset, IRRPT, BGPQ3
- BGPSEC

Pero...

- Despliegue insuficiente.
- Falta de datos confiables.

Necesitamos un enfoque estándar para mejorar la seguridad en el enrutamiento.



Colaboración y Consenso

Tu seguridad está en manos de otra persona. Las acciones de otros lo afectan directamente a usted y a la seguridad de su red (y viceversa).

¿Por qué deberían ayudarte? Puedes empezar ayudándolos.

Necesitamos expectativas de seguridad reconocidas a nivel mundial para todos los operadores de red para elevar el nivel de seguridad de enrutamiento.



Estamos en esto juntos

Los Operadores de Red tienen la responsabilidad de garantizar una infraestructura de enrutamiento segura y sólida a nivel mundial.

La seguridad de su red depende de una infraestructura de enrutamiento que elimine a los malos actores y las configuraciones incorrectas accidentales que causan estragos en Internet.

Cuanto más operadores de red trabajen juntos, menos incidentes habrá y menos daño pueden hacer.



La solución: Mutually Agreed Norms for Routing Security (MANRS)

Proporciona soluciones cruciales para reducir las amenazas de enrutamiento más comunes.



MANRS mejora la seguridad y confiabilidad del sistema global de enrutamiento de Internet, basado en la colaboración entre los participantes y la responsabilidad compartida de la infraestructura de Internet.

MANRS establece una nueva norma para la seguridad de enrutamiento.



Implementación de Acciones MANRS:

Señala la postura de seguridad avanzada de una organización y puede eliminar las violaciones de SLA que reducen la rentabilidad o el costo de las relaciones con los clientes.

Evita los incidentes de enrutamiento, lo que ayuda a las redes a identificar y abordar fácilmente los problemas con los clientes o peers.

Mejora la eficiencia operativa de una red al establecer vías de comunicación de intercambio de tráfico mejores y más limpias, al mismo tiempo que proporciona información detallada para la resolución de problemas.

Identifica muchas preocupaciones de empresas centradas en la seguridad y otros clientes.



Todos se benefician

Unirse a MANRS significa unirse a una comunidad preocupada por la seguridad y comprometida con hacer que la infraestructura de enrutamiento global sea más robusta y segura.

La adopción constante de MANRS produce una mejora constante, pero necesitamos más redes para implementar las acciones y más clientes para exigir las mejores prácticas de seguridad de enrutamiento.

Cuantos más operadores de red apliquen acciones MANRS, menos incidentes habrán y menos daños pueden hacer.

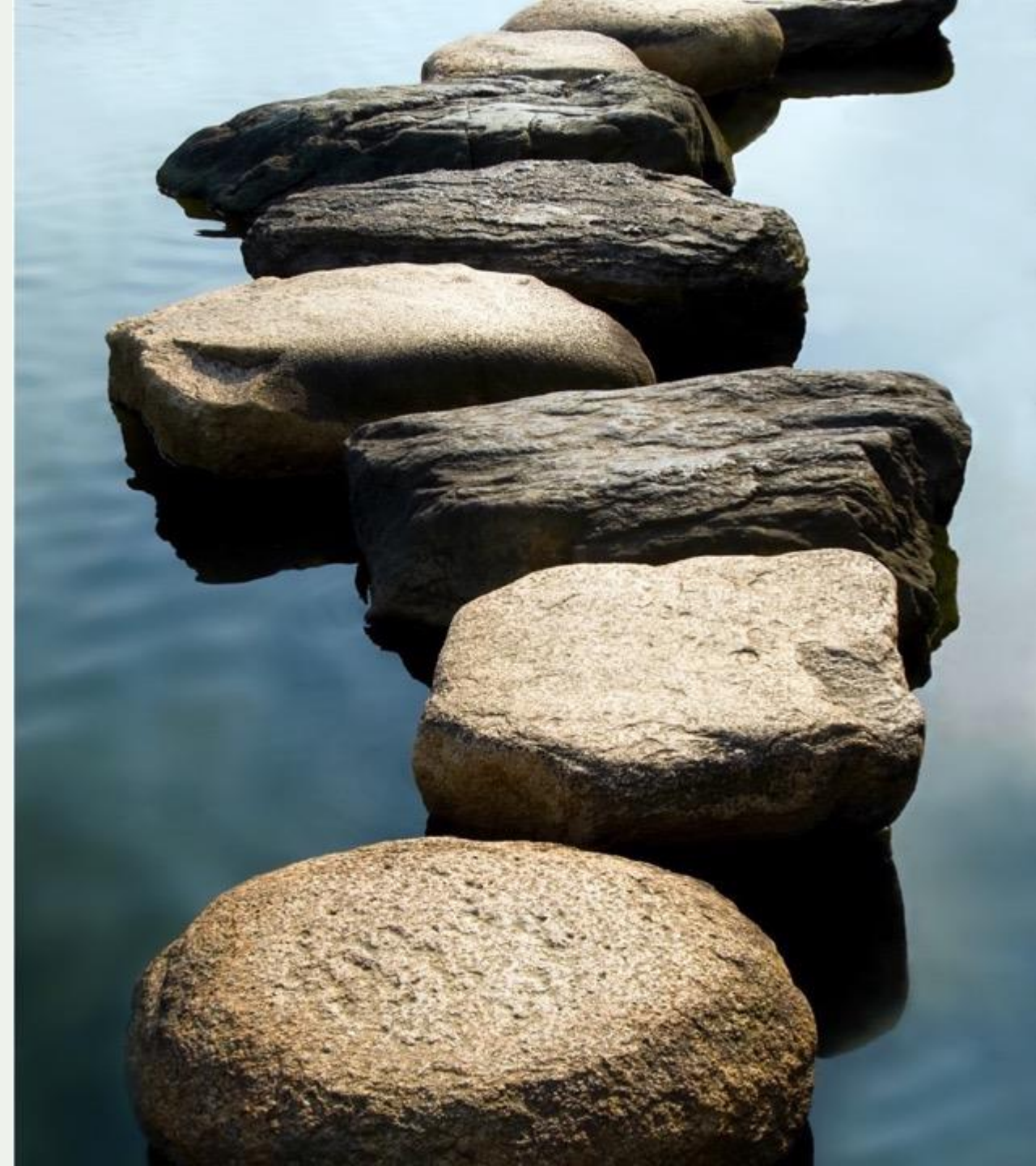


MANRS es un Paso importante

La seguridad es un proceso, no un estado. MANRS proporciona una estructura y un enfoque coherente para resolver los problemas de seguridad que enfrenta Internet.

MANRS es lo mínimo que un operador podría considerar, con acciones rentables y de bajo costo.

MANRS no es una solución integral para todos los problemas de enrutamiento de Internet, pero es un paso importante hacia una infraestructura de enrutamiento segura y robusta a nivel mundial.



Programas de MANRS



MANRS para Operadores de Red



MANRS para IXPs



MANRS para CDNs y Proveedores de Nube



MANRS para vendedores de equipos.



MANRS para Operadores de Red



Mutually Agreed Norms for Routing Security

MANRS define cuatro simples pero concretas acciones que los operadores de redes deben implementar para mejorar dramáticamente la seguridad y confiabilidad de Internet.

- Las dos primeras mejoras operativas eliminan las causas fundamentales de los problemas y ataques comunes de enrutamiento, mientras que los dos segundos pasos del procedimiento mejoran la mitigación y disminuye la probabilidad de incidentes futuros.



MANRS

MANRS Acciones para Operadores

Filtrado

Prevenir la propagación de información de enrutamiento incorrecta

Asegure la exactitud de sus propios anuncios y anuncios de sus clientes a redes adyacentes con prefijo y granularidad AS-path.

Anti-spoofing

Prevenir tráfico con direcciones IP de origen falsificadas

Habilite la validación de la dirección de origen para al menos una red del cliente que tiene un único punto de entrada y salida, sus propios usuarios finales e infraestructura

Coordinación

Facilitar la comunicación operativa global y la coordinación entre los operadores de red

Mantener la información de contacto actualizada y accesible a nivel mundial en bases de datos de enrutamiento comunes

Validación Global

Facilitar la validación de la información de enrutamiento a escala global

Publique sus datos para que otros puedan validar.



MANRS para Operadores de Red

¡ **705** participantes !
Al 27 de junio 2022

Organization Name	Areas Served	ASNs	Action 1 Filtering	Action 2 Anti-Spoofing	Action 3 Coordination	Action 4 Global Validation
.pt	PT	199993	✓	✓	✓	✓
10110770 Manitoba O/A Vulpine Networks	CA, US	400442	✓		✓	✓
3WACCES	BR	269053	✓	✓	✓	✓
76 Telecom Telecomunicações Ltda	BR	262760, 262363	✓		✓	✓
84 Grams AB	SE	57630	✓		✓	✓
A B DA SILVA MULTIMIDIA - ME	BR	270370	✓		✓	✓
AARNet Pty Ltd	AU	7575	✓	✓	✓	✓
ABASE Telecom	BR	22431	✓	✓	✓	✓
Acesso.net	BR	53236	✓		✓	✓
ACOnet	AT	1853	✓		✓	✓
Organization Name	Areas Served	ASNs	Action 1 Filtering	Action 2 Anti-Spoofing	Action 3 Coordination	Action 4 Global Validation



El Programa IXP



Internet Exchange Points son Socios Cruciales

El programa IXP fue lanzado en Abril del 2018 inicialmente con 12 IXP participantes.

Un conjunto separado de acciones MANRS generadas por la comunidad satisface las necesidades particulares de la comunidad IXP.

Cada IXP forma una comunidad local con un objetivo operativo común. Contribuyen de forma tangible a mejorar significativa la seguridad del enrutamiento.

MANRS permite a los IXPs construir 'safe neighborhoods,' aprovechando la línea base de seguridad de MANRS.

Los participantes deben implementar 3/5 acciones para IXP, incluyendo las dos primeras acciones obligatorias.



MANRS Acciones para IXPs

Acción 1 Filtrado

El IXP implementa filtrado de anuncios de ruta en el servidor de ruta basado en datos de información de enrutamiento (IRR y/o RPKI)

***Obligatorio**



Acción 2 Promover MANRS

Cuatro opciones: (a) asistencia en el mantenimiento de registros, (b) Asistencia en la implementación de acciones del operador, (c) Guía de la Membresía de MANRS, e (d) incentivos para la preparación de MANRS

***Obligatorio**

Acción 3 Proteger la Plataforma de intercambio de información

El IXP tiene una política publicada de tráfico no permitido en la estructura de intercambio de tráfico y realiza el filtrado de dicho tráfico.

Acción 4 Facilitar la Comunicación Global

El IXP facilita la comunicación entre los miembros proporcionando listas de correo y directorios de miembros necesarios.

Acción 5 Monitoreo y Depuración

El IXP provee un looking glass para sus miembros.

MANRS para IXPs

104 IXPs
Junio 2022

<https://www.manrs.org/ixps/participants/>

IXP	Action 1 Prevent	Action 2 Promote	Action 3 Protect	Action 4 Coordinate	Action 5 Tools
IXDO (DO)	✓	<ul style="list-style-type: none">2-1: Assist (1)2-2: Assist (2)2-3: Promote	✓	✓	✓
IXpy (PY)	✓	<ul style="list-style-type: none">2-1: Assist (1)2-2: Assist (2)2-3: Promote		✓	✓
IXSaI (SV)	✓	<ul style="list-style-type: none">2-1: Assist (1)2-2: Assist (2)2-3: Promote		✓	✓
IXSY (MX)	✓	<ul style="list-style-type: none">2-1: Assist (1)2-2: Assist (2)2-3: Promote	✓	✓	✓
JBIX (MY)	✓	<ul style="list-style-type: none">2-2: Assist (2)2-3: Promote		✓	✓
JPIX (JP)	✓	<ul style="list-style-type: none">2-1: Assist (1)		✓	✓
JPNAP (JP)	✓	<ul style="list-style-type: none">2-1: Assist (1)	✓		✓
KIXP (KE)	✓	<ul style="list-style-type: none">2-1: Assist (1)2-2: Assist (2)	✓	✓	✓
KolkataIX (IN)	✓	<ul style="list-style-type: none">2-1: Assist (1)2-2: Assist (2)2-4: Incent	✓	✓	
Lambda Internet Exchange (US)	✓	<ul style="list-style-type: none">2-1: Assist (1)2-2: Assist (2)2-3: Promote	✓	✓	
IXP	Action 1 Prevent	Action 2 Promote	Action 3 Protect	Action 4 Coordinate	Action 5 Tools

Showing 51 to 60 of 104 entries



MANRS para CDNs y Proveedores de Nube



MANRS Acciones para CDNs y Proveedores de Nube

Acción 1

Prevenir la propagación de información de enrutamiento incorrecta

Garantizar la corrección de los anuncios propios y de sus pares (no de tránsito) implementando un filtrado explícito (lista blanca) con granularidad de prefijos.

Acción 2

Prevenir tráfico con direcciones IP de origen falsificadas

Implementar controles anti-spoofing para evitar que los paquetes con direcciones IP de origen ilegítimas salgan de la red (filtros de salida).

Acción 3

Facilitar la comunicación operativa global y la coordinación entre los operadores de red

Mantener información de contacto actualizada y accesible a nivel mundial en PeeringDB y en las bases de datos RIR pertinentes.

Acción 4

Facilitar la validación de la información de enrutamiento a escala global

Documentar públicamente los ASN y los prefijos que están destinados a ser anunciados a partes externas (RIR y/o RPKI)

Acción 5

Fomentar la adopción de MANRS

Fomentar activamente la adopción de MANRS entre los pares

Acción 6

Proporcionar herramientas de monitoreo y depuración a los socios de la red.

Proporcionar un mecanismo para informar a los socios de peering si los anuncios no cumplen los requisitos de la política de peering.



Fondo Azul = Acción Obligatoria

MANRS para CDNs y Proveedores de Nube

20 participantes
(Junio 2022)



Organization Name	ASNs	Action 1 Filtering	Action 2 Anti-Spoofing	Action 3 Coordination	Action 4 Global Validation	Action 5 MANRS Adoption	Action 6 Tools
Akamai Technologies	20940	✓	✓	✓	✓ IRR	✓	
Amazon Web Services	16509	✓ ✓ ROV ✓ AS-SET	✓	✓	✓ IRR ✓ RPKI	✓	
Azion Technologies	52580	✓	✓	✓	✓ IRR	✓	
Biznet Gio	133800	✓	✓	✓	✓ IRR	✓	✓
Cloud Himalaya Pvt Ltd	135337	✓	✓	✓	✓ IRR	✓	
Cloudflare	13335	✓	✓	✓	✓ IRR	✓	✓
cloudscale.ch	59414	✓	✓	✓	✓ IRR	✓	
DigitalOcean	14061	✓ ✓ ROV ✓ AS-SET	✓	✓	✓ IRR	✓	
Equinix Metal	54825	✓ ✓ ROV ✓ AS-SET	✓	✓	✓ IRR ✓ RPKI	✓	
Facebook	32934	✓	✓	✓	✓ IRR	✓	✓
Organization Name	ASNs	Action 1 Filtering	Action 2 Anti-Spoofing	Action 3 Coordination	Action 4 Global Validation	Action 5 MANRS Adoption	Action 6 Tools

Showing 1 to 10 of 20 entries



MANRS para vendedores de equipos



MANRS Acciones para Vendedores de Equipos

Acción 1

Proveer soluciones para la implementación de acciones específicas de MANRS para otros participantes.

Acción 2

Promover MANRS a través de entrenamiento y contenido técnico.



MANRS para Vendedores de equipo

6 Vendedores Junio 2022



Organization Name	Action 1 Provide Solutions	Action 2-1 Training	Action 2-2 Lab	Action 2-3 Technical Resources	Action 2-4 Hands-on
Arista Networks	<ul style="list-style-type: none"> Scenario 1 Filtering Scenario 2 Anti-spoofing Scenario 4 Protect L2 (IXP) 	📅	✓	✓	📅
Arrcus Inc	<ul style="list-style-type: none"> Scenario 1 Filtering Scenario 2 Anti-spoofing Scenario 3 Filtering (IXP) 	📅	✓	📅	📅
Cisco	<ul style="list-style-type: none"> Scenario 1 Filtering Scenario 2 Anti-spoofing Scenario 3 Filtering (IXP) Scenario 4 Protect L2 (IXP) 	✗	✓	📅	✗
Huawei Technologies Co., Ltd.	<ul style="list-style-type: none"> Scenario 1 Filtering Scenario 2 Anti-spoofing Scenario 3 Filtering (IXP) Scenario 4 Protect L2 (IXP) 	📅	📅	✓	📅
Juniper Networks	<ul style="list-style-type: none"> Scenario 1 Filtering Scenario 2 Anti-spoofing Scenario 3 Filtering (IXP) Scenario 4 Protect L2 (IXP) 	📅	✓	✓	📅
Nokia	<ul style="list-style-type: none"> Scenario 1 Filtering Scenario 2 Anti-spoofing Scenario 4 Protect L2 (IXP) 	✗	✓	✗	✗
Organization Name	Action 1 Provide Solutions	Action 2-1 Training	Action 2-2 Lab	Action 2-3 Technical Resources	Action 2-4 Hands-on

Showing 1 to 6 of 6 entries



Comparativa de acciones

Scenario	Program	Action
Scenario 1 Filtering	<u>Network Operators</u>	<u>Action 1. Prevent propagation of incorrect routing information</u>
	<u>CDN and Cloud Providers</u>	<u>Action 1. Prevent propagation of incorrect routing information</u>
Scenario 2 Anti-spoofing	<u>Network Operators</u>	<u>Action 2: Prevent traffic with spoofed source IP addresses</u>
	<u>CDN and Cloud Providers</u>	<u>Action 2. Prevent traffic with illegitimate source IP addresses</u>
Scenario 3 Filtering (IXP)	<u>IXPs</u>	<u>Action 1. Prevent propagation of incorrect routing information. (Route Server)</u>
Scenario 4 Protect L2 (IXP)	<u>IXPs</u>	<u>Action 3. Protect the peering platform (layer 2)</u>



MANRS Primers

¿Cómo puedo apoyar en la Seguridad del Ruteo?



MANRs Primers

Mientras las decisiones de ruteo son realizadas solo por los operadores de red, los incidentes de ruteo pueden impactar y afectan a todos en Internet, incluyendo negocios y servicios públicos.

Afortunadamente podemos tomar medidas para protegernos de las incidencias comunes a través de buenas prácticas, considerando y envolviendo a los diferentes niveles de usuarios o perfiles de la organización.

De tal modo que se consideran los siguientes perfiles:

- Formuladores de políticas.
- Ejecutivos de Negocios.
- Ejecutivos de TI.
- Equipos de Respuesta de Atención a Incidentes de Seguridad en Computo (CSIRTs)



RECURSOS DISPONIBLES Y AUTOEVALUACION



Participa:

Visite

<https://www.manrs.org>

Complete el formulario de registro con el mayor detalle posible:

<https://www.manrs.org/isps/join/>



MANRS Network Operator Application
Fields marked with an asterisk (*) are required.
The form can be filled out either in English, or in your native language.

1 Operator Information 2 MANRS Actions 3 Consent & Review

Organization Name *

Organization Website *

Areas Served * Select the countries where your organization is based and/or provides services. We use [ISO 3166-1 Alpha-2 country codes](#).

AS Number(s) of Your Networks * Add each AS Number on its own line by using the "+" key.

Organization Logo
Upload a .jpg or .png version of your company's logo, suitable for display on a white background. This image will be published with your listing if your application is accepted.

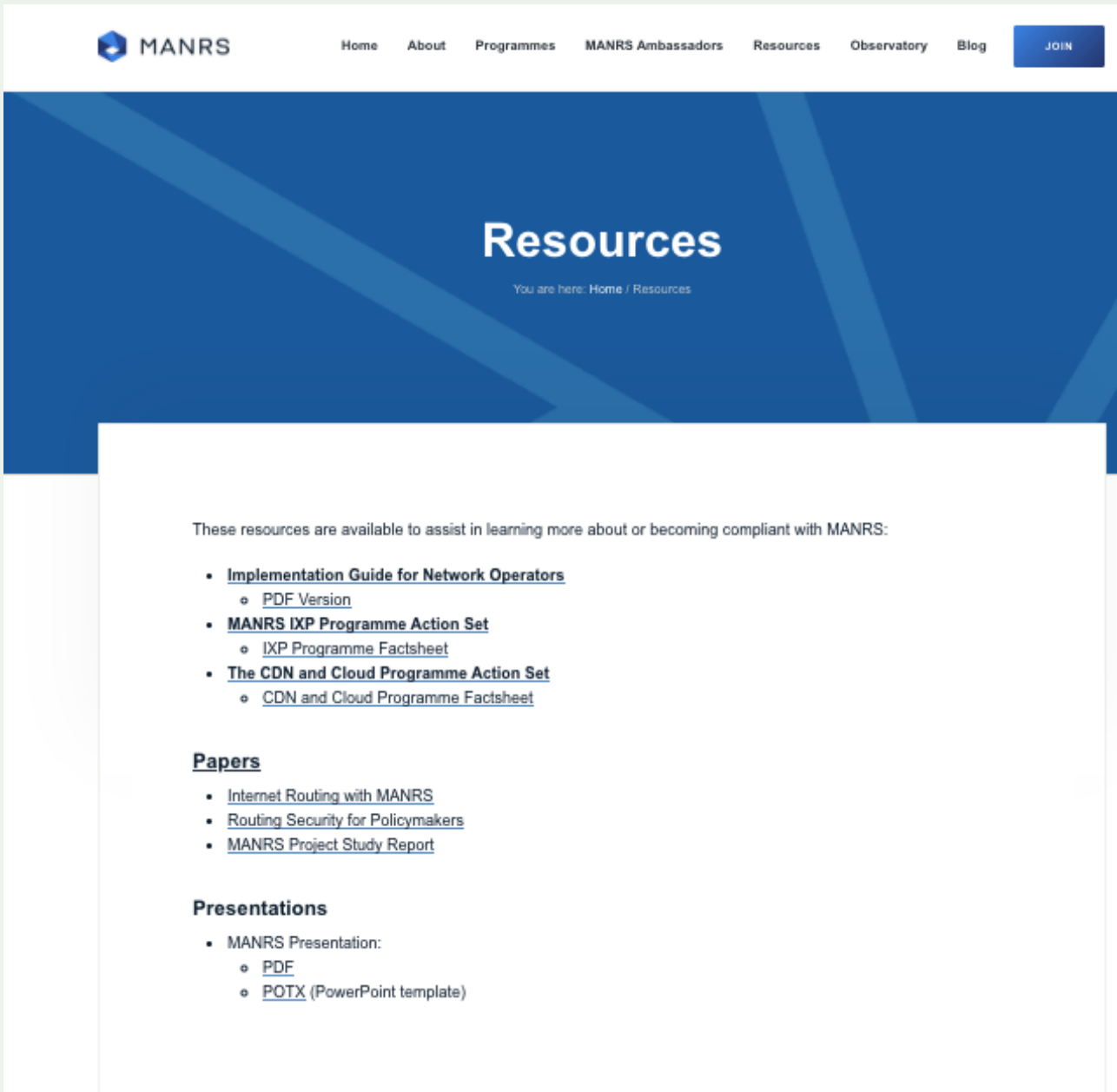
Contact Name *

First Last

Contact Job Title

Contact Email *

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



MANRS

Home About Programmes MANRS Ambassadors Resources Observatory Blog JOIN

Resources

You are here: Home / Resources

These resources are available to assist in learning more about or becoming compliant with MANRS:

- **Implementation Guide for Network Operators**
 - [PDF Version](#)
- **MANRS IXP Programme Action Set**
 - [IXP Programme Factsheet](#)
- **The CDN and Cloud Programme Action Set**
 - [CDN and Cloud Programme Factsheet](#)

Papers

- [Internet Routing with MANRS](#)
- [Routing Security for Policymakers](#)
- [MANRS Project Study Report](#)

Presentations

- MANRS Presentation:
 - [PDF](#)
 - [POTX](#) (PowerPoint template)

<https://www.manrs.org/wp-content/uploads/2018/03/MANRS-BCOP-20170125.pdf>

Mutually Agreed Norms for Routing Security (MANRS) Implementation Guide



MANRS

Version 1.0, BCOP series

Publication Date: 25 January 2017

[1. What is a BCOP?](#)

[2. Summary](#)

[3. MANRS](#)

[4. Implementation guidelines for the MANRS Actions](#)

[4.1. Coordination - Facilitating global operational communication and coordination between network operators](#)

[4.1.1. Maintaining Contact Information in Regional Internet Registries \(RIRs\): AFRINIC, APNIC, RIPE](#)

[4.1.1.1. MNTNER objects](#)

[4.1.1.1.1. Creating a new maintainer in the AFRINIC IRR](#)

[4.1.1.1.2. Creating a new maintainer in the APNIC IRR](#)

[4.1.1.1.3. Creating a new maintainer in the RIPE IRR](#)

[4.1.1.2. ROLE objects](#)

[4.1.1.3. INETNUM and INET6NUM objects](#)

[4.1.1.4. AUT-NUM objects](#)

[4.1.2. Maintaining Contact Information in Regional Internet Registries \(RIRs\): LACNIC](#)

[4.1.3. Maintaining Contact Information in Regional Internet Registries \(RIRs\): ARIN](#)

[4.1.3.1. Point of Contact \(POC\) Object Example:](#)

[4.1.3.2. OrgNOCHandle in Network Object Example:](#)

[4.1.4. Maintaining Contact Information in Internet Routing Registries](#)

[4.1.5. Maintaining Contact Information in PeeringDB](#)

[4.1.6. Company Website](#)

[4.2. Global Validation - Facilitating validation of routing information on a global scale](#)

[4.2.1. Valid Origin documentation](#)

[4.2.1.1. Providing information through the IRR system](#)

[4.2.1.1.1. Registering expected announcements in the IRR](#)

[4.2.1.2. Providing information through the RPKI system](#)

[4.2.1.2.1. RIR-Listed Resource Certification services](#)

MANRS Acciones para Operadores

Filtrado

Prevenir la propagación de información de enrutamiento incorrecta

Asegure la exactitud de sus propios anuncios y anuncios de sus clientes a redes adyacentes con prefijo y granularidad AS-path.

Anti-spoofing

Prevenir tráfico con direcciones IP de origen falsificadas

Habilite la validación de la dirección de origen para al menos una red del cliente que tiene un único punto de entrada y salida, sus propios usuarios finales e infraestructura

Coordinación

Facilitar la comunicación operativa global y la coordinación entre los operadores de red

Mantener la información de contacto actualizada y accesible a nivel mundial en bases de datos de enrutamiento comunes

Validación Global

Facilitar la validación de la información de enrutamiento a escala global

Publique sus datos para que otros puedan validar.



Autoevaluación - Filtrado:

- ❖ Comprobar que el ASN no anuncia bogons
 - ❖ Utiliza CIDR Report
<https://www.cidr-report.org/as2.0/>
- ❖ Comprobar que el ASN no ha estado implicado en incidentes recientes.
 - ❖ <https://bgpstream.com/>



Autoevaluación - Anti-Spoofing

- ❖ Comprobar que el ASN no aparece en la base de datos de spoofer de CAIDA.
 - ❖ [https://spoofer.caida.org/provider.php?asn=\[ASN\]](https://spoofer.caida.org/provider.php?asn=[ASN])
 - ❖ [https://spoofer.caida.org/as.php?asn=\[ASN\]](https://spoofer.caida.org/as.php?asn=[ASN])
- ❖ Si no hay, o no hay resultados recientes, ejecute el Spoofer.
 - ❖ <https://www.caida.org/projects/spoofer/>
 - ❖ <https://www.caida.org/projects/spoofer/#download-client-software>



Autoevaluación - Coordinación

- ❖ Compruebe que los contactos están en el whois
 - ❖ `whois -h whois.lacnic.net prefix`
 - ❖ [https://bgp.he.net/AS\[ANS\]#_whois](https://bgp.he.net/AS[ANS]#_whois)
- ❖ Compruebe que la información del contacto esta registrado en el PeeringDB:
 - ❖ [https://www.peeringdb.com/asn/\[ASN\]](https://www.peeringdb.com/asn/[ASN])



Autoevaluación - Validación Global

- ❖ Compruebe que la información del enrutamiento está registrada en un IRR o tiene un ROA.
 - ❖ <https://inforedes.labs.lacnic.net/>
 - ❖ <https://rpki-validator.ripe.net/bgp-preview>
 - ❖ <https://monitor.fortproject.net/es/overview#technical>
 - ❖ <https://bgp.he.net/>



MANRS Observatory



MANRS Observatory

Es una herramienta en línea que proporciona un estado factual de la seguridad y la resiliencia del sistema de enrutamiento de Internet y hace un seguimiento en el tiempo.

Las mediciones son:

- Transparentes: utilizan datos de acceso público
- Pasivas: no se requiere la cooperación de las redes
- En evolución: la comunidad MANRS decide qué se mide y cómo.

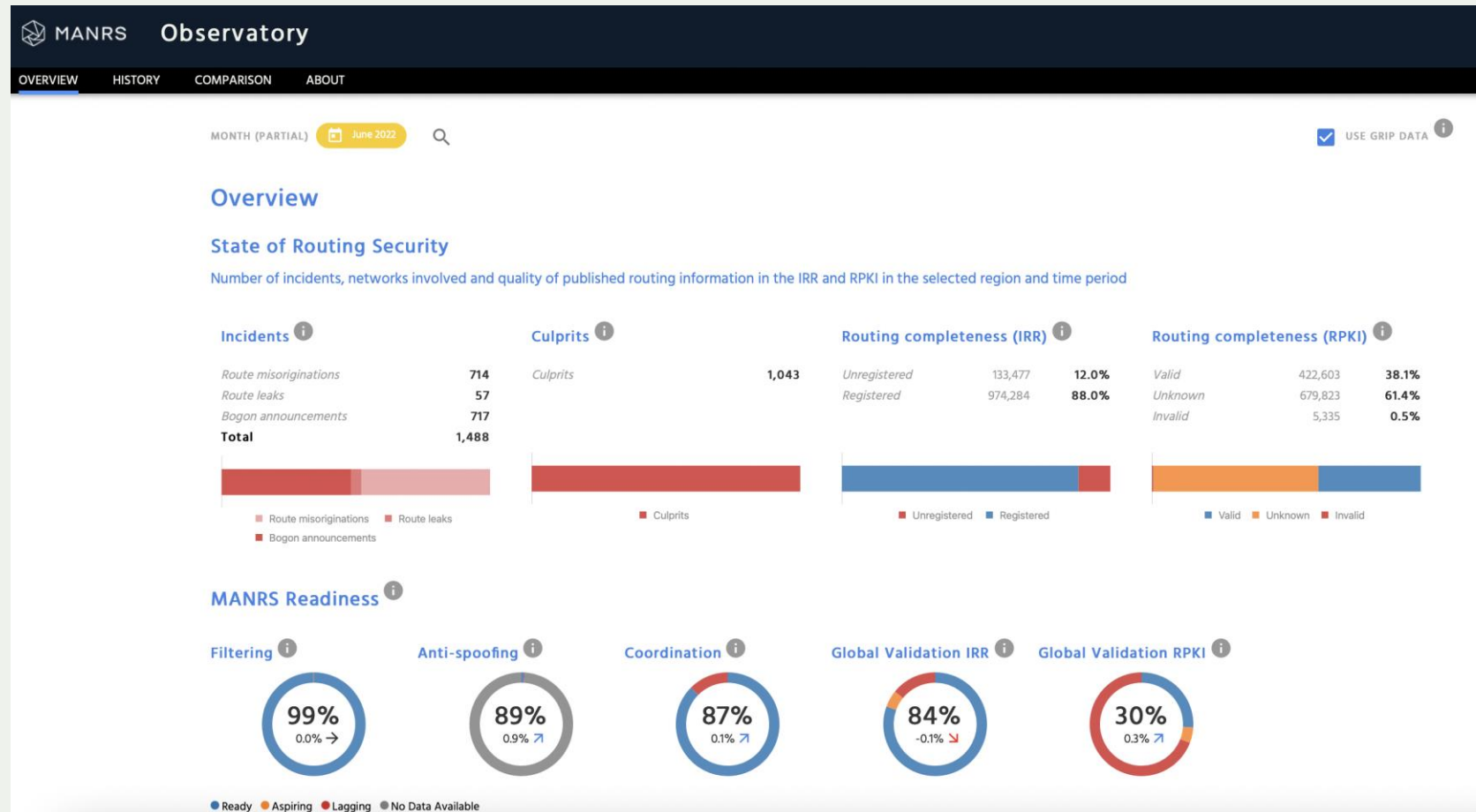


<https://observatory.manrs.org>



<https://observatory.manrs.org>

Mide los niveles de conformidad con las acciones MANRS, un indicador clave del estado de seguridad de enrutamiento y resistencia de Internet.



Overview

State of Routing Security

Number of incidents, networks involved and quality of published routing information in the IRR and RPKI in the selected region and time period

Incidents

Route misoriginations	1
Route leaks	0
Bogon announcements	13
Total	14



Culprits

Culprits	12
----------	----



Routing completeness (IRR)

Unregistered	1,381	4.9%
Registered	27,092	95.1%



Routing completeness (RPKI)

Valid	9,188	32.3%
Unknown	19,277	67.7%
Invalid	8	0.0%



MANRS Readiness

Filtering



Anti-spoofing



Coordination



Global Validation IRR



Global Validation RPKI



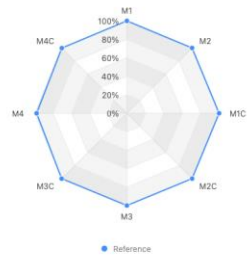
● Ready ● Aspiring ● Lagging ● No Data Available

Comparison

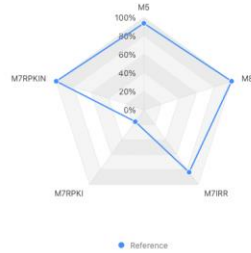
Click the button below to compare different scenarios



Filtering



Anti-spoofing, global validation & coordination



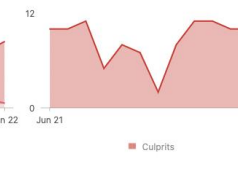
History

June 2021 - June 2022

Incidents



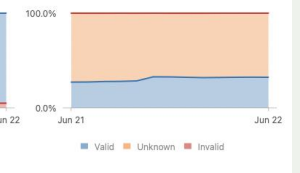
Culprits



Routing completeness (IRR)



Routing completeness (RPKI)



MANRS Readiness

Absolute | Relative

Filtering



Anti-spoofing



Crecimiento de Operadores en México

Junio 2021

Mexico	
Count	348
Culprits	10
Incidents	13
MANRS Readiness	
Filtering	99%
Anti-spoofing	84%
Coordination	94%
Global Validation IRR	84%
Global Validation RPKI	11%

Junio 2022

Mexico	
Count	370
Culprits	12
Incidents	14
MANRS Readiness	
Filtering	99%
Anti-spoofing	94%
Coordination	100%
Global Validation IRR	84%
Global Validation RPKI	16%



¿De dónde provienen los datos?

MANRS Observatory utiliza datos disponibles públicamente para medir las actividades de enrutamiento en Internet. Agrega datos de una serie de fuentes confiables de terceros.

Las métricas y estadísticas para medir la preparación de MANRS se calculan rastreando el número de incidentes y redes involucradas, sus capacidades anti-spoofing y la integridad de la información de enrutamiento en repositorios públicos, como IRR y RPKI.



- BGP Stream (<https://bgpstream.com/>)
- CIDR Report (<https://www.cidr-report.org/>)
- CAIDA Spoofer (<https://www.caida.org/projects/spoofer/>)
- RIPE Stats (<https://stat.ripe.net/>)
- RPKI Validator (<https://github.com/RIPE-NCC/rpki-validator-3>)

El Observatorio tiene dos puntos de vista:

Pública, está dirigida a cualquier persona interesada en la seguridad de enrutamiento. Los usuarios pueden ver en un vistazo el estado de cada país en un mapa global interactivo y profundizar en los datos.

Privada, está destinada a operadores de red participantes de MANRS. Les permite medir su preparación MANRS e identificar rápidamente las áreas problemáticas para ayudarlos a mejorar la seguridad de sus redes. Pueden ver el rendimiento de las redes individuales (¡de más de 64,000!)



Caso empresarial para MANRS y la seguridad de enrutamiento

Participación de 451 investigaciones para comprender mejor las actitudes y percepciones de los Proveedores de Servicios de Internet y la comunidad empresarial en general, en torno al Proyecto.



¿ Por qué unirse a MANRS?

Mejora su postura de seguridad y reduzca la cantidad y el impacto de los incidentes de enrutamiento.

Ser parte de una comunidad de operadores preocupados por la seguridad, que trabajan juntos para mejorar Internet.

MANRS: como un diferenciador competitivo.



Lo que aprendimos del estudio

La seguridad es vital para las empresas

- El conocimiento de MANRS es bajo, pero el deseo de seguridad es alto.
- Las empresas están dispuestas a exigir el cumplimiento de MANRS a sus proveedores de servicios.

MANRS agrega valor a los Proveedores de Servicios

- La seguridad puede ayudar a los Proveedores de Servicios a diferenciarse de sus competidores; Valor identificable en un Mercado impreciso.
- Los Proveedores de Servicios pueden ser capaces de agregar fuentes de ingreso adicionales basadas en fuentes de seguridad de la información y otros servicios adicionales.



¿Por qué los operadores deberían unirse a MANRS?

Para ayudar a resolver problemas de red globales:

- Liderar con el ejemplo para mejorar la seguridad del enrutamiento y garantizar una infraestructura de enrutamiento segura y robusta a nivel mundial.
- Formar parte de la comunidad MANRS puede fortalecer las credenciales de seguridad empresarial

Para agregar valor competitivo y diferenciarse en un mercado plano impulsado por los precios:

- Creciente demanda de los clientes empresariales de servicios de seguridad gestionados (fuentes de información).
- Para señalar la competencia en seguridad y el compromiso con sus clientes.

Para "lock-in" – de un proveedor de conectividad a un socio de seguridad:

- Las fuentes de información y otros servicios complementarios pueden incrementar los ingresos y reducir la rotación de clientes.
- Las empresas manifiestan su disposición a pagar más por servicios mas seguros.



Ponentes

Conclusiones



Involúcrate

Necesitamos que más redes participen e implementen las acciones, y más clientes para exigir las mejores prácticas de seguridad de enrutamiento.

¡Cuantas más organizaciones apliquen las acciones de MANRS, menos serán los incidentes de seguridad, y aportaremos en la seguridad y resistencia del Internet!



Preparación próxima sesión

1. Efectuar y documentar las actividades de autoevaluación.
2. Validar el acceso al portal de Mi Lacnic.
3. Conocer y tener a disposición sus recursos numéricos.



Bibliografía

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

<https://www.manrs.org/wp-content/uploads/sites/14/2018/03/MANRS-BCOP-20170125.pdf>

<https://www.internetsociety.org/es/issues/manrs-es/>

<https://www.internetsociety.org/es/blog/2018/08/tech-companies-endorse-manrs-routing-security-actions/>

https://www.lacnic.net/innovaportal/file/3512/1/bgp_buenas_practicas_2019a.pdf

https://www.lacnic.net/innovaportal/file/3512/1/20190510_marns_universidades_tutorial_peeringlacnic31.pdf

<https://www.lacnic.net/innovaportal/file/3139/1/bgp-rosario-lacnic30.pdf>

<https://www.youtube.com/watch?v=eUSjVqj5ib4>

Lecturas complementarias

- IRR Power Tools (IRRPT) <https://github.com/6connect/irrpt>
- Internet Routing Registry Toolset (IRRToolset)
 - <https://github.com/irrtoolset/irrtoolset>
- BGPQ3 <https://github.com/snar/bgpq3>
- Ansible <http://www.ansible.com/>
- Cisco Network Services Orchestrator <http://www.cisco.com/go/nso>
- IRR Explorer <http://irrexplorer.nlnog.net/>
- RPKI <https://www.lacnic.net/980/1/lacnic/certificacion-de-recursos-rpki>

Gracias.

Emmanuel Serrano

Email: isc.emmanuel.serrano@gmail.com

Mauricio Oviedo

Email: mauricio@socium.cr