Análisis de incidentes de enrutamiento en la región

Octubre 2023 / Octubre 2024

Autor: Erika Vega, Chair grupo de trabajo enrutamiento, LACNOG
Coordinación y revisión: Guillermo Cicileo
Edición: Área de Comunicaciones
Área: Área de Tecnología

Febrero 2025

lacnic
www.lacnic.net

Contenido

Introducción

El crecimiento continuo del ecosistema de Internet en América Latina y el Caribe (LAC) ha generado una mayor interconexión entre redes, pero también ha expuesto a la región a un aumento en la incidencia de problemas de enrutamiento que afectan la estabilidad y la seguridad del tráfico en línea. Estos incidentes, que pueden tener consecuencias significativas para usuarios y proveedores de servicios, destacan la importancia de comprender su naturaleza, causas y posibles soluciones.

Este informe tiene como objetivo analizar los incidentes de enrutamiento registrados en la región LAC durante el periodo comprendido entre octubre de 2023 y octubre de 2024. A través de un enfoque estructurado, el documento explora las tres categorías principales de incidentes a nivel global: Secuestro de rutas, Fuga de rutas y la publicación de Bogons.

El análisis se centra en la recopilación y presentación de datos clave, como la cantidad de incidentes registrados, su distribución mensual y por país, y los factores que los originaron. Además, se estudia el impacto de los incidentes más relevantes, con énfasis en la interrupción de servicios críticos y su afectación a los usuarios finales. El informe también examina los protocolos y prácticas de seguridad implementados para mitigar estos problemas, destacando el papel de iniciativas como RPKI y MANRS, así como las medidas adoptadas por los Puntos de Intercambio de Tráfico (IXPs) en la región.

Finalmente, el documento incluye una comparativa con datos de años anteriores, identificando tendencias y áreas de mejora. Basándose en los hallazgos, se presentan recomendaciones y lecciones aprendidas con el propósito de fortalecer la resiliencia y seguridad del ecosistema de enrutamiento en LAC.

Este análisis busca no solo proporcionar una visión detallada de los incidentes ocurridos, sino también contribuir al desarrollo de estrategias más efectivas para su prevención y contención en el futuro.

1. Cantidad de Incidentes reportados

En esta sección se presenta un análisis detallado del volumen de incidentes de enrutamiento registrados en la región de América Latina y el Caribe (LAC) entre octubre de 2023 y octubre de 2024. El objetivo es ofrecer una visión clara de la magnitud del problema en términos cuantitativos, desglosando los datos de manera mensual y por país.

Este análisis permite identificar tendencias temporales, patrones regionales y variaciones en la frecuencia de incidentes, proporcionando una base sólida para comprender la distribución geográfica y cronológica de los eventos, durante el periodo analizado. Además, la información presentada es crucial para contextualizar los esfuerzos de mitigación y las recomendaciones que se desarrollarán en las siguientes secciones del informe.

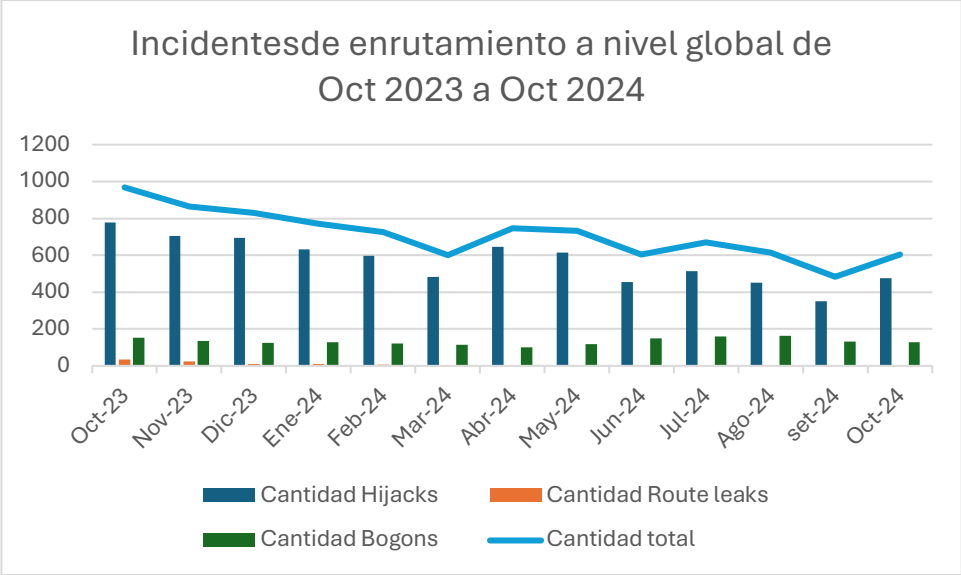
Los datos utilizados en esta sección han sido recopilados a partir de múltiples fuentes confiables, como el observatorio especializado de MANRS y reportes generados por organizaciones de monitoreo. Este enfoque asegura una cobertura amplia y representativa del panorama regional de enrutamiento durante el período analizado.

Los beneficios de este análisis trascienden la presentación de estadísticas, que ofrece insumos para comprender la evolución de los incidentes de enrutamiento, identificar áreas de mejora y orientar estrategias de mitigación en la región.

1.1. Incidentes totales reportados a nivel global de octubre 2023 a octubre 2024

Fecha	Cantidad Hijacks	Cantidad Route leaks	Cantidad Bogons	Cantidad total
oct-23	778	36	154	968
nov-23	705	25	134	864
dic-23	693	10	126	829
ene-24	632	11	128	771
feb-24	598	8	120	726

mar-24	482	3	114	599
abr-24	644	0	102	746
may-24	613	0	118	731
jun-24	456	0	149	605
jul-24	513	0	158	671
ago-24	451	0	164	615
sep-24	351	0	132	483
oct-4	474	0	129	603



En la gráfica anterior podemos visualizar que, a nivel global, los incidentes de enrutamiento mostraron una clara predominancia de los Hijacks, que promediaron 568 incidentes por mes, alcanzando un máximo de 778 en octubre de 2023 y un mínimo de 351 en septiembre de 2024.

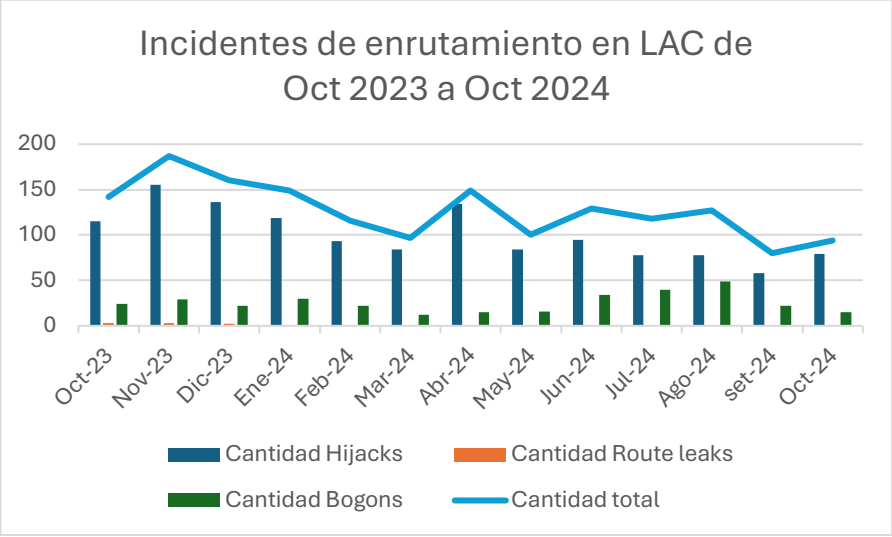
Los Bogons, aunque menos frecuentes que los Hijacks, representaron en promedio 133 incidentes por mes, con un máximo de 164 incidentes en los meses de mayor actividad.

Por otro lado, los Route Leaks tuvieron una incidencia menor, con un promedio mensual de 7,2 incidentes y un máximo de 36. Este dato refleja que, aunque estos incidentes son menos comunes, su impacto sigue siendo significativo debido a la potencial disrupción en la confiabilidad del sistema de enrutamiento u errores en configuraciones que se siguen presentando en la operatividad de las redes.

El total de incidentes mensuales osciló entre 483 y 968. Los picos más altos ocurrieron en los primeros meses del período analizado, disminuyendo paulatinamente hacia finales de 2024, lo que podría demostrar mejoras progresivas en las medidas de mitigación.

1.2. Incidentes totales reportados en Latinoamérica y el Caribe de octubre 2023 a octubre 2024

Fecha	Cantidad Hijacks	Cantidad Route leaks	Cantidad Bogons	Cantidad total
oct-23	115	3	24	142
nov-23	155	3	29	187
dic-23	136	2	22	160
ene-24	119	0	30	149
feb-24	93	1	22	116
mar-24	84	1	12	97
abr-24	134	0	15	149
may-24	84	0	16	100
jun-24	95	0	34	129
jul-24	78	0	40	118
ago-24	78	0	49	127
sep-24	58	0	22	80
oct-24	79	0	15	94



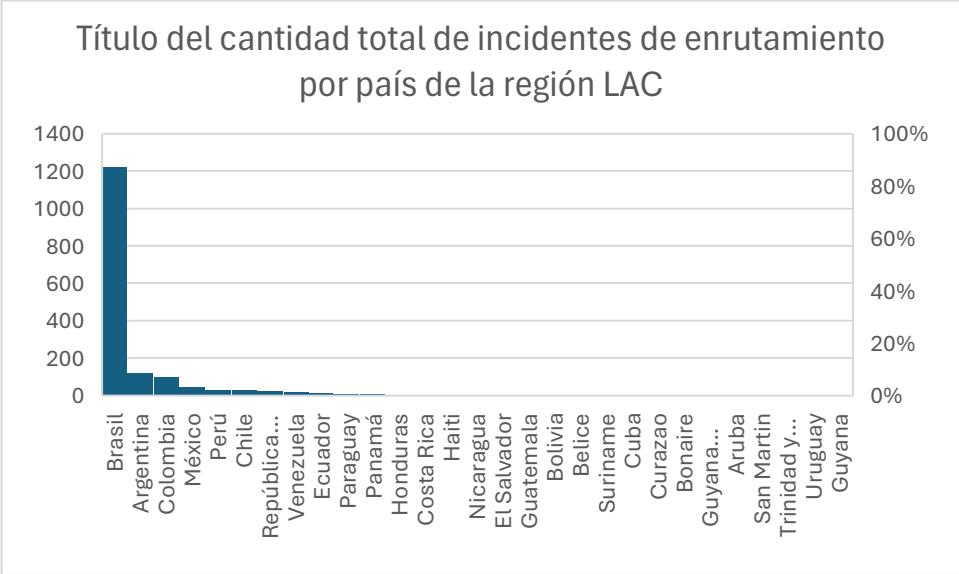
En la región de Latinoamérica y el Caribe (LAC), el panorama de incidentes de enrutamiento presenta características únicas. Aunque el número total de incidentes por país es relativamente bajo en comparación con las cifras globales, hay picos significativos en ciertos momentos, así como en algunos países.

1.3. Incidentes reportados mensualmente por país

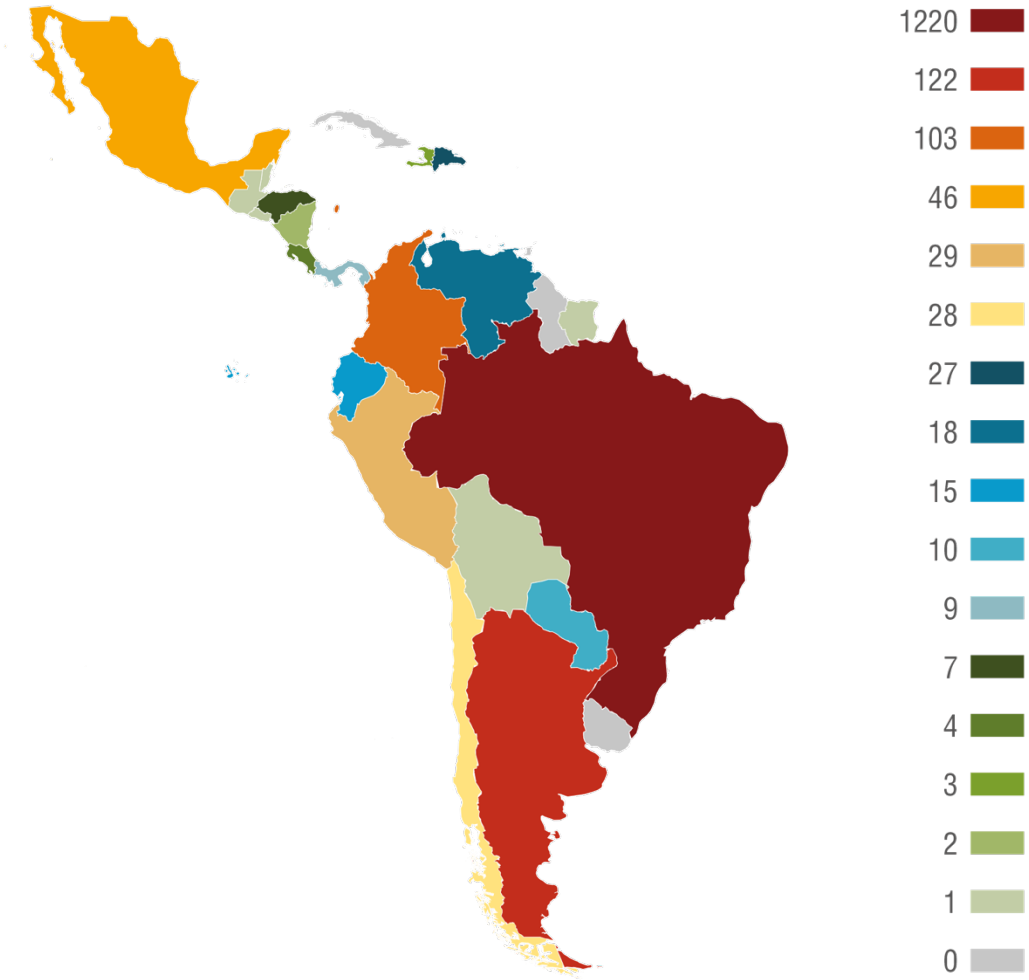
A continuación, se muestra una tabla detallada con la cantidad de incidentes totales reportados en el rango de tiempo analizado (octubre 2023 a octubre 2024) y desglosados por tipo para cada uno de los países de la región LAC, adicionalmente se muestra un análisis detallado para los 5 países de la región con más incidentes reportados. Por lo que en el archivo Anexo 1 se encuentra el detalle de la cantidad de incidentes por mes para el resto de los países de la región

País	Cantidad Hijacks	Cantidad Route leaks	Cantidad Bogons	Cantidad total
Argentina	81	0	41	122
Aruba	0	0	0	0
Belice	1	0	0	1
Bolivia	1	0	0	1
Bonaire	0	0	0	0
Brasil	1037	0	183	1220
Chile	24	0	4	28
Colombia	50	0	53	103
Costa Rica	4	0	0	4
Cuba	0	0	0	0
Curazao	0	0	0	0
Ecuador	7	0	8	15
El Salvador	0	0	1	1
Guatemala	1	0	0	1
Guyana	0	0	0	0

Guyana Francesa	0	0	0	0
Haití	3	0	0	3
Honduras	7	0	0	7
México	27	5	14	46
Nicaragua	2	0	0	2
Panamá	4	2	3	9
Paraguay	2	0	8	10
Perú	26	0	3	29
República Dominicana	21	0	6	27
San Martin	0	0	0	0
Suriname	1	0	0	1
Trinidad y Tobago	0	0	0	0
Uruguay	0	0	0	0
Venezuela	9	3	6	18



Mapa de incidentes de enrutamiento por país de la región LAC



Los incidentes de secuestro de rutas en LAC, se presentaron con un rango que varió desde 0 incidentes en algunos países en meses más estables hasta un máximo de 141 en un país específico. Sin embargo, si tomamos los datos agregados de la región LAC podemos ver que no hubo ningún mes sin incidentes de Hijacks, tal como se ve en la sección 1.2. Estos datos destacan la necesidad de continuar realizando monitoreo continuo, a nivel de mecanismos como la validación de origen, los cuales nos continúan otorgando la forma de obtener información de las razones por las cuales se generan este tipo de incidentes, y de las posibles acciones para contenerlos.

Los Route Leaks fueron menos frecuentes, con un máximo de 2 incidentes en un mes para un país, que en este caso fue Venezuela y de 5 en total en un año para México, tal como se puede ver en la sección 1.3. Aunque su incidencia es baja, los afectados podrían beneficiarse de controles más estrictos en la configuración de políticas de enrutamiento.

Los Bogons se presentaron en mayor porcentaje que los Route Leaks, y con un número considerable en países como Brasil y Colombia, pero durante el año estudiado tuvieron presencia en 10 países más de la región Esto señala la importancia de implementar mejores controles en la gestión de listas de acceso y filtros de prefijos para prevenir la propagación de direcciones IP no asignadas.

Cómo se indicó al inicio de esta sección, la gran mayoría de los datos mostrados en este segmento fueron extraídos del observatorio de MANRS, el cual utiliza las siguientes fuentes de datos:

1. I-ROV Filtering Rate (APNIC)
2. Spoofer (CAIDA)
3. CIDR Report (APNIC)
4. GRIP (Internet Intelligence Lab at Georgia Institute of Technology)
5. NRO Stats (Number Resource Organization)
6. PeeringDB
7. RIPEStat (RIPE NCC)

Pero es interesante mostrar aquí los datos procesados por Qrator, con el fin, de hacer un comparativo a nivel de las cantidades reportadas por los tres tipos de incidentes que se analizan en este documento:

	Cantidad Hijacks		Cantidad Route leaks		Cantidad Bogons	
Pais	MANRS	Qrator	MANRS	Qrator	MANRS	Qrator
Argentina	81	367	0	70	41	5
Aruba	0	2	0	1	0	0
Belice	1	8	0	1	0	0
Bolivia	1	9	0	3	0	0
Bonaire	0	1	0	0	0	0
Brasil	1037	2064	0	1302	183	210
Chile	24	81	0	31	4	0

Colombia	50	121	0	33	53	2
Costa Rica	4	22	0	7	0	0
Cuba	0	2	0	0	0	0
Curazao	0	6	0	0	0	0
Ecuador	7	41	0	13	8	0
El Salvador	0	9	0	1	1	0
Guatemala	1	22	0	8	0	0
Guiana Francesa	0	0	0	0	0	0
Guyana	0	2	0	0	0	0
Haití	3	3	0	0	0	0
Honduras	7	25	0	4	0	0
México	27	222	5	33	14	0
Nicaragua	2	9	0	2	0	0
Panamá	4	20	2	10	3	1
Paraguay	2	23	0	8	8	1
Perú	26	75	0	19	3	0
República Dominicana	21	35	0	7	6	0
Saint Martin	0	1	0	0	0	0
Suriname	1	4	0	1	0	0
Trinidad y Tobago	0	6	0	2	0	0
Uruguay	0	8	0	1	0	0
Venezuela	9	52	3	20	6	3

Para analizar estos datos, es necesario comprender cómo Qrator describe el conjunto de datos que utiliza. En las métricas que presentan en sus informes e investigaciones, emplean un identificador denominado **AS culpables únicos**, que hace referencia a la cantidad de **AS** únicos que fueron responsables de un incidente durante el período especificado. Esta métrica no depende del número de prefijos, la duración del incidente ni la periodicidad del evento. En su lugar, se centra

exclusivamente en el número de ISP que generaron incidentes, sin tener en cuenta el tamaño de estos.

Adicionalmente, podríamos señalar que la diferencia en los valores de Qrator en comparación con los de MANRS podría deberse a que tanto Qrator como MANRS utilizan sus propios algoritmos para detectar incidentes a nivel de BGP, así como recolectores propios y diversos datos abiertos, tales como bases de datos IRR, repositorios RPKI, Peering DB, entre otros.

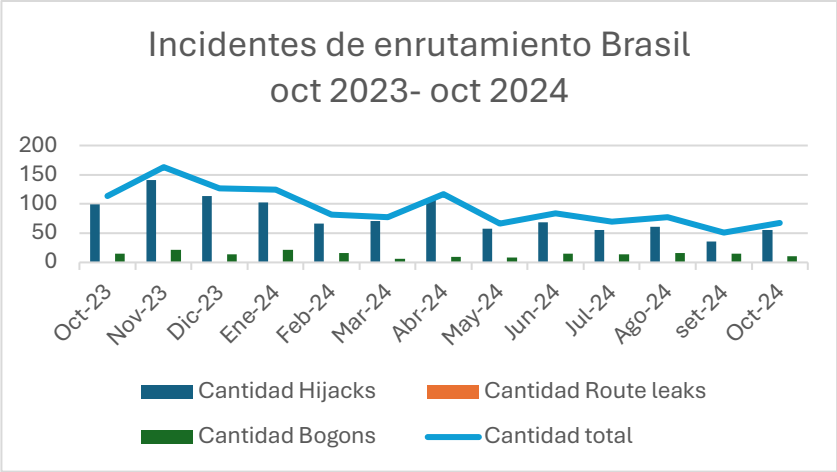
Más detalles sobre los datos enviados por Qrator como aporte para este estudio, en relación con los incidentes reportados durante el período de tiempo analizado, pueden visualizarse en la tabla del **Anexo 2**.

A continuación, se presenta un desglose del TOP 5 de países con la mayor cantidad de incidentes registrados en la región de LAC durante el período de octubre de 2023 a octubre de 2024:

1.3.1. Brasil

Fecha	Cantidad Hijacks	Cantidad Route leaks	Cantidad Bogons	Cantidad total
oct-23	99	0	15	114
nov-23	141	0	22	163
dic-23	113	0	14	127
ene-24	103	0	22	125
feb-24	66	0	16	82
mar-24	71	0	6	77
abr-24	108	0	9	117
may-24	58	0	8	66
jun-24	69	0	15	84
jul-24	56	0	14	70

ago-24	61	0	16	77
sep-24	36	0	15	51
oct-24	56	0	11	67
Total	1037	0	183	1220



Brasil reportó un total de 1,220 incidentes, siendo el país con el mayor volumen de incidentes en la región. La distribución es la siguiente:

Hijacks: 1,037 (85% del total).

Route Leaks: 0 (0% del total).

Bogons: 183 (15% del total).

Brasil reportó el mayor número de incidentes, sumando significativamente más que otros en la región.

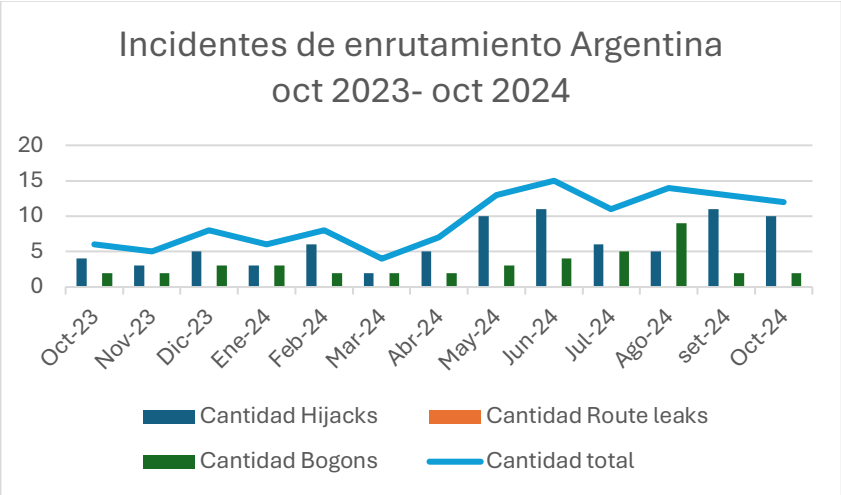
La mayor parte de los incidentes fueron secuestros de rutas, indicando un posible problema con la validación de rutas o configuraciones erróneas en sus sistemas autónomos.

Curiosamente no se reportan incidentes de Route Leaks reportados en este periodo.

Este país mostró un número alto de incidentes relacionados con direcciones no asignadas, destacando la necesidad de controles estrictos en el filtrado de prefijos.

1.3.2. Argentina

Fecha	Cantidad Hijacks	Cantidad Route leaks	Cantidad Bogons	Cantidad total
oct-23	4	0	2	6
nov-23	3	0	2	5
dic-23	5	0	3	8
ene-24	3	0	3	6
feb-24	6	0	2	8
mar-24	2	0	2	4
abr-24	5	0	2	7
may-24	10	0	3	13
jun-24	11	0	4	15
jul-24	6	0	5	11
ago-24	5	0	9	14
sep-24	11	0	2	13
oct-24	10	0	2	12
Total	81	0	41	122



Argentina reportó un total de 122 incidentes durante el período analizado, distribuidos de la siguiente manera:

Hijacks: 81 (66% del total).

Bogons: 41 (34% del total).

Route Leaks: Ninguno reportado

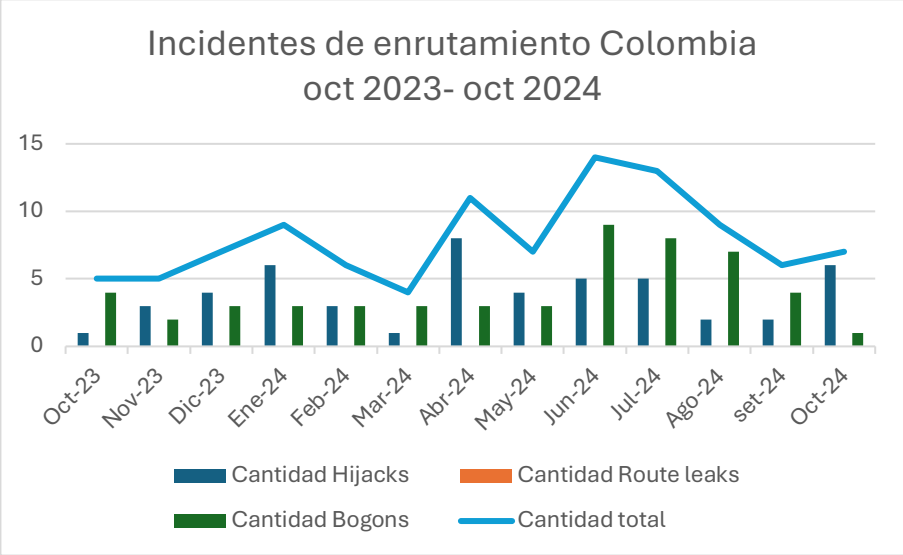
En cuanto a cantidad de incidentes, predominan los Hijacks, teniendo picos importantes en los meses de mayo, junio y septiembre de 2024. Menos frecuentes que los Hijacks, se presenta un total de 41 incidentes relacionados con Bogons que podría reflejar vulnerabilidades a evaluar relacionadas con el filtrado de prefijos IP.

Al igual que en Brasil la ausencia de Rote Leaks sugiere un buen manejo en la configuración de políticas de enrutamiento.

1.3.3. Colombia

Fecha	Cantidad Hijacks	Cantidad Route leaks	Cantidad Bogons	Cantidad total
oct-23	1	0	4	5

nov-23	3	0	2	5
dic-23	4	0	3	7
ene-24	6	0	3	9
feb-24	3	0	3	6
mar-24	1	0	3	4
abr-24	8	0	3	11
may-24	4	0	3	7
jun-24	5	0	9	14
jul-24	5	0	8	13
ago-24	2	0	7	9
sep-24	2	0	4	6
oct-24	6	0	1	7
Total	50	0	53	103



Colombia reportó un total de 103 incidentes, distribuidos de la siguiente manera:

Hijacks: 50 (48.5% del total).

Bogons: 53 (51.5% del total).

Route Leaks: No se reportaron incidentes de este tipo.

Los incidentes relacionados con **Bogons** en Colombia representan un patrón distintivo dentro de los incidentes de enrutamiento reportados, con un total de **53 casos** durante el período analizado, lo que equivale al **51.5% del total de incidentes** reportados en el país. Esta cifra es notablemente alta en comparación con otros países de la región y sugiere una serie de problemas operativos y estructurales en la gestión del enrutamiento.

Los Bogons, aunque constantes, presentaron un aumento notable en junio y julio de 2024, y representan más de la mitad del porcentaje total de los incidentes reportados en este país, lo que demuestra la necesidad de evaluar vulnerabilidades relacionadas con el filtrado de prefijos IP.

En el período analizado, los incidentes de Bogons en Colombia se comparan de la siguiente manera con los otros países de la región que se encuentran en el TOP 5 de incidentes:

- **Colombia:** 53 incidentes totales.
- **Brasil:** 183 incidentes (mayor incidencia en la región).
- **México:** 14 incidentes.
- **Argentina:** 41 incidentes.
- **Perú:** Solo 3 incidentes.

Esto evidencia que, aunque Brasil lidera con un número significativamente mayor de Bogons, Colombia ocupa el segundo lugar, indicando un problema considerable en comparación con otros países como Perú y México.

Colombia vs. Brasil: Aunque los Bogons en Colombia son menores en número absoluto comparados con Brasil, su proporción sobre el total de incidentes es considerablemente alta (51.5% en Colombia frente a 15% en Brasil). Esto indica que los Bogons son un problema estructural en Colombia. Además si tenemos en cuenta que en Brasil la cantidad de redes en operación ronda por los 8. 600 ASN asignados y en Colombia por los 350, podemos evidenciar que en efecto la cantidad de Bogons

reportados en Colombia es proporcionalmente mucho mayor que en Brasil.

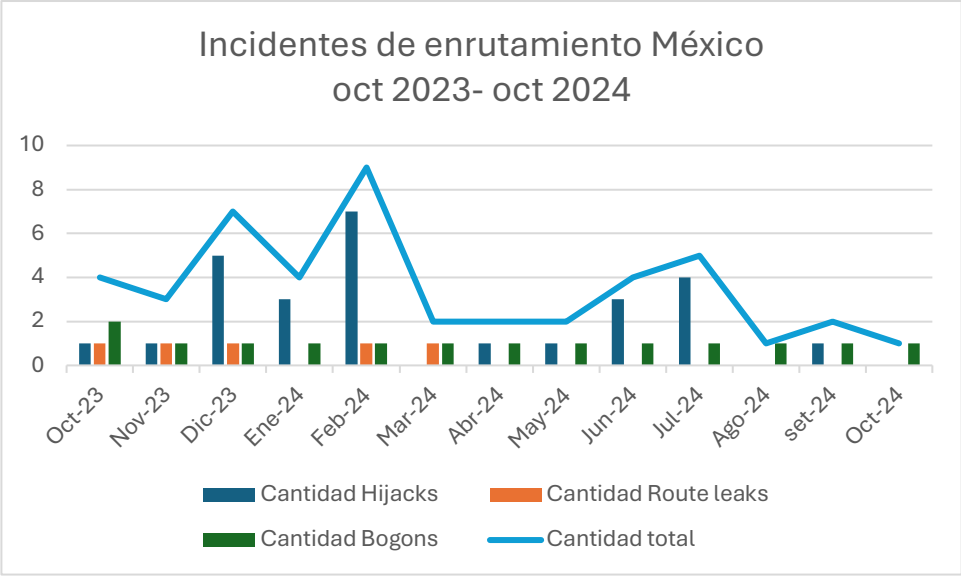
Diferencias con Perú y México: En países como Perú y México, los incidentes de Bogons son marginales, reflejando un mejor manejo de filtros de prefijos.

Los Hijacks representaron casi la mitad de los incidentes, destacándose abril de 2024 como el mes más problemático con un pico significativo.

Al igual que en Brasill y Argentina se tiene ausencia de Route Leaks.

1.3.4. México

Fecha	Cantidad Hijacks	Cantidad Route leaks	Cantidad Bogons	Cantidad total
oct-23	1	1	2	4
nov-23	1	1	1	3
dic-23	5	1	1	7
ene-24	3	0	1	4
feb-24	7	1	1	9
mar-24	0	1	1	2
abr-24	1	0	1	2
may-24	1	0	1	2
jun-24	3	0	1	4
jul-24	4	0	1	5
ago-24	0	0	1	1
sep-24	1	0	1	2
oct-24	0	0	1	1
Total	27	5	14	46



Durante el período analizado, México reportó un total de 46 incidentes, distribuidos de la siguiente manera:

Hijacks: 27 (58.7% del total).

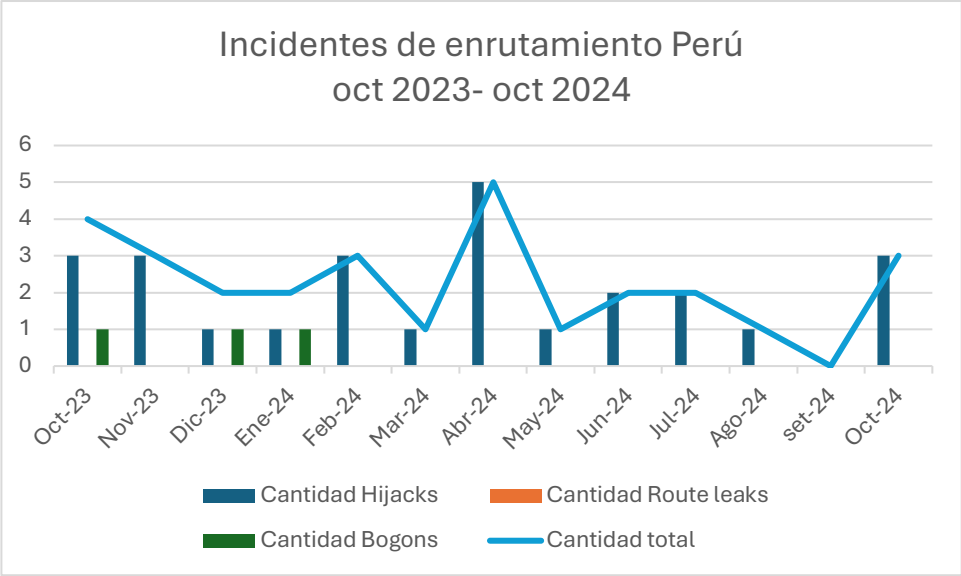
Route Leaks: 5 (10.9% del total).

Bogons: 14 (30.4% del total).

Más de la mitad de los incidentes reportados en México son secuestros de rutas, indicando vulnerabilidades significativas en la validación de rutas. Los picos en meses específicos sugieren eventos anómalos o dirigidos, mientras que la ausencia en otros meses podría reflejar una combinación de estabilidad operativa y menor actividad maliciosa. Aunque los Route Leaks son menos frecuentes, su presencia constante a finales de 2023 podría deberse a problemas específicos de configuración en sistemas autónomos de la región. Aunque no son la mayoría, los Bogons estuvieron presentes en cada mes, lo que sugiere problemas consistentes en el filtrado de prefijos IP.

1.3.5. Perú

Fecha	Cantidad Hijacks	Cantidad leaks	Route	Cantidad Bogons	Cantidad total
oct-23	3	0		1	4
nov-23	3	0		0	3
dic-23	1	0		1	2
ene-24	1	0		1	2
feb-24	3	0		0	3
mar-24	1	0		0	1
abr-24	5	0		0	5
may-24	1	0		0	1
jun-24	2	0		0	2
jul-24	2	0		0	2
ago-24	1	0		0	1
sep-24	0	0		0	0
oct-24	3	0		0	3
Total	26	0		3	29



Durante el período analizado, Perú reportó un total de 29 incidentes, distribuidos de la siguiente manera:

Hijacks: 26 (89.7% del total).

Route Leaks: 0 (0% del total)

Bogons: 3 (10.3% del total).

Los Hijacks dominaron el panorama de incidentes, representando casi el 90% de los casos reportados. Los Bogons tuvieron una incidencia baja, mientras que no se registraron Route Leaks durante el período analizado.

2. Tipos de incidentes

En esta sección se explica en detalle la naturaleza de los tres tipos de incidentes de enrutamiento analizados en el informe de la sección anterior, con el objetivo de profundizar en la comprensión de sus causas y efectos. Este enfoque permitirá una interpretación más precisa de los incidentes más relevantes registrados durante el período estudiado, los cuales serán abordados en la sección siguiente.

La información presentada en esta sección se basa, en gran medida, en el Informe de Seguridad en el Ruteo para América Latina y el Caribe elaborado por LACNIC[1], complementada con otras fuentes relevantes como los RFC 1918[2], 8190[3], 6890[4]. Este análisis busca ofrecer una base sólida para contextualizar y entender los desafíos que enfrenta la infraestructura de red en la región.

Para comprender los distintos tipos de incidentes que pueden provocarse en la capa de ruteo de Internet, primero es necesario entender cómo funciona BGP de forma más detallada. Este protocolo establece la comunicación entre sistemas autónomos que se configuran para que anuncien y/o aprendan rutas, lo que permitirá que se alcancen los destinos. Para hacer más controlado el proceso de pasaje de rutas, existen medidas como la implementación de filtros o políticas.

No obstante, la confianza en Internet radica en que cada organización anuncie solo sus propios prefijos o los prefijos de las organizaciones a las que les da tránsito. Sin embargo, eso no está garantizado en BGP, sino que se basa en el buen trabajo que hagan los operadores de las diferentes redes.

Ya sea de forma involuntaria o intencional, los dispositivos enrutadores pueden tener un comportamiento inesperado y anunciar un prefijo que no les corresponde anunciar. A esto se lo denomina *incidente de ruteo* y puede clasificarse en dos grandes tipos: *hijacks* y *leaks*.

Supongamos que queremos conectarnos a algún servicio de mensajería mediante una app. Tanto nuestro dispositivo móvil como los servidores de dicha app deben

[1] https://imasd.lacnic.net/reportes/interconexion/fort-informe-seguridad-ruteo-es.pdf

[2] https://datatracker.ietf.org/doc/html/rfc1918

[3] https://datatracker.ietf.org/doc/html/rfc8190

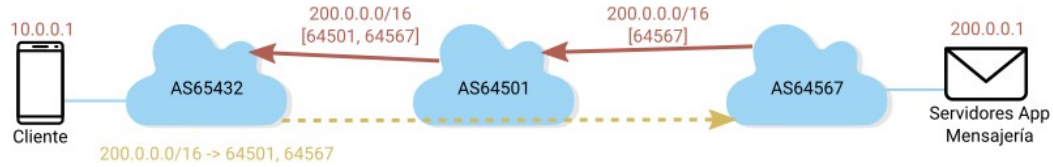
[4] https://www.rfc-editor.org/rfc/rfc6890

estar conectados a Internet y entre ambos extremos debe existir una ruta que permita establecer un flujo de información.

Ahora sabemos también que ambos extremos no estarán directamente conectados, sino que cada uno estará conectado a un sistema autónomo. Estos sistemas autónomos pertenecen a los ISP contratados por cada extremo para obtener conectividad. Para este caso, nuestro móvil tendrá asignada la dirección IP 10.0.0.1 y el ASN de nuestro proveedor será 65432, mientras que los servidores de la app estarán conectados mediante la dirección IP 200.0.0.1 y su sistema autónomo tendrá registrado el ASN 64567.

Cada sistema autónomo puede conectarse con otros sistemas autónomos; estos, a su vez, con otros yasí sucesivamente. Supongamos que en este ejemplo solo existe una red intermedia.

¿Cómo logra encontrar a dónde enviar los paquetes de datos el AS65432, que es el que nos conectapara llegar a la dirección IP 200?0.0.1? Ahí es donde entra en juego el protocolo BGP. El AS64567, propietario de dicha dirección IP, anuncia que tiene el prefijo correspondiente. Así, el AS64501, que provee tránsito a los otros dos sistemas, anuncia la ruta 64501 64567 a nuestro AS65432 para llegar a la red 200.0.0.0/16.



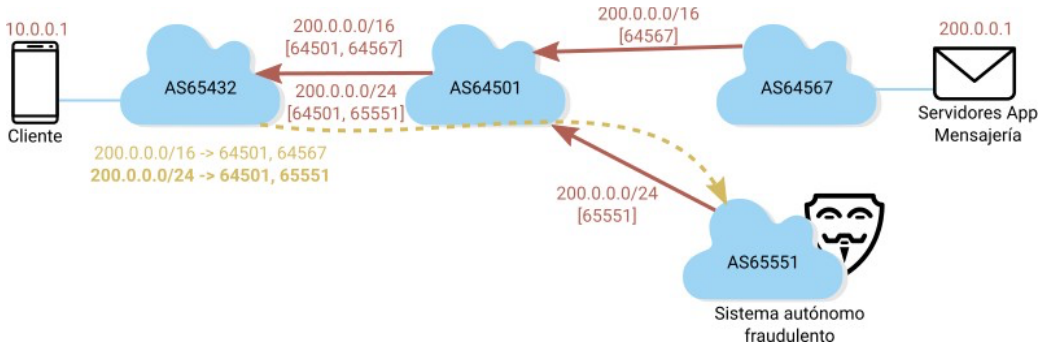
Así, cuando nuestro dispositivo quiere enviar información a la dirección 200.0.0.1, el AS65432 ya contará con la ruta adecuada para transmitir los datos desde nuestro móvil a los servidores de la app. De forma similar el AS64567 podrá obtener una ruta para llegar a nuestra dirección IP.

2.1. Secuestros de ruta (BGP *hijacks*)

Lo desarrollado anteriormente es un escenario donde no ocurren incidentes. Pero ¿qué pasa si agregamos un AS fraudulento que quiera provocar un hijack o secuestro de ruta? Se le llama «secuestro de ruta» a la acción de anunciar a Internet prefijos cuando no se está autorizado a hacerlo. Este anuncio indebido puede ser intencional o por error en la operación y logra propagarse porque ofrece una

«mejor ruta». Es decir, el anuncio es de un prefijo más específico que el que anuncia el AS original o es un anuncio de una ruta más corta, exista o no.

Volviendo a nuestro ejemplo, supongamos que aparece un operador fraudulento que quiere bloquear el acceso a nuestra app. Entonces anuncia que posee un prefijo más específico que comprende la dirección 200.0.0.1 (en este caso 200.0.0.0/24).

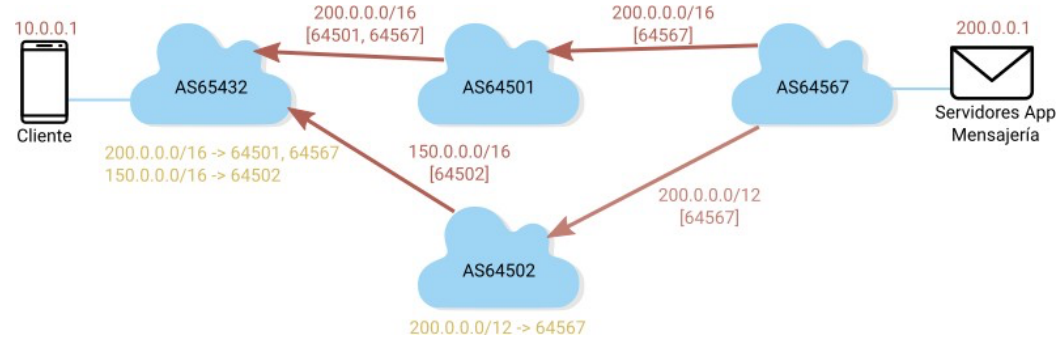


Entonces, al sistema autónomo que nos da conectividad le llegan dos rutas distintas para el mismo destino y termina eligiendo la más específica, es decir, la del AS fraudulento.

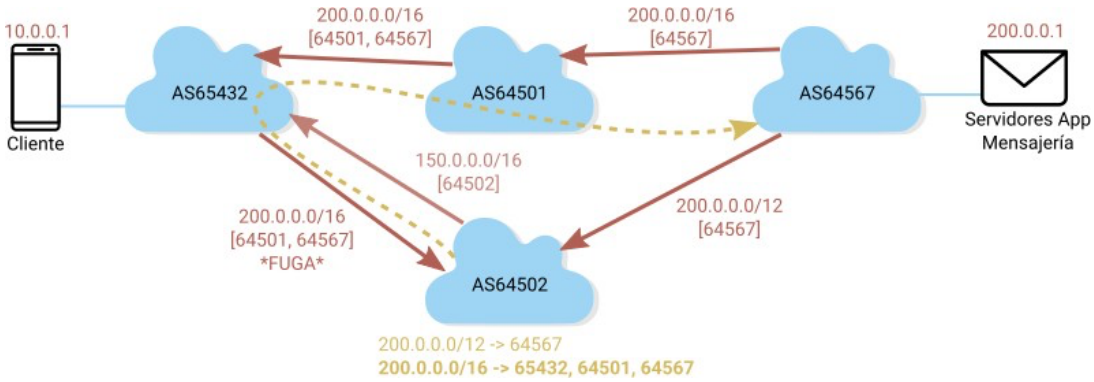
2.2. Fugas de ruta (BGP *leaks*)

Otro tipo de incidente son las fugas o leaks. Cuando se propaga un anuncio de ruteo que supera su alcance deseado, es decir, que viola las políticas del sistema emisor, receptor o alguno de los que forman parte de la ruta, se produce una fuga de ruta.6 Generalmente ocurre cuando un operador de red con más de un proveedor hacia arriba, de forma accidental, anuncia a uno de estos que posee una ruta hacia el destino a través de otro de los sistemas autónomos proveedores, transformando al operador inicial en un intermediario entre los dos proveedores de este.

Volviendo a nuestro ejemplo inicial, ahora supongamos que el AS65432, que nos brinda conectividad, cuenta con dos proveedores: el AS64501 que ya conocemos y el AS64502, que le permite llegar a la red 150.0.0.0/16. A su vez, este sistema autónomo está conectado con AS64567, aunque en principio es irrelevante para nuestro AS, ya que llega a ese destino por AS64501.



Pero, por algún error de configuración, el AS65432 anuncia la ruta con destino a 200.0.0.0/16 a AS64502. Esto no es un comportamiento esperado, porque nuestro AS es un cliente y no un proveedor de tránsito. El anuncio de ruteo supera su alcance deseado y se genera una fuga BGP. El AS64502 no filtra este anuncio y ahora cuenta con una ruta más específica para llegar a 200.0.0.1 (200.0.0.0/16 a través del AS65432, en contra de 200.0.0.0/12 a través de AS64567).



Sin importar que la ruta sea más larga, como el prefijo es más específico, el AS64502 comenzará a enviar flujos de datos hacia el AS65432, lo cual puede generar problemas de desempeño en la red e incluso cortes de servicio, tanto en el ISP, que nos brinda conectividad, como para los distintos clientes que quieran acceder a la app de mensajería.

2.3. Bogons

Los *Bogons* son direcciones IP que no deberían aparecer en la tabla de enrutamiento global, ya sea porque no están asignadas por IANA (Internet Assigned Numbers Authority) o los RIRs (Regional Internet Registries) o porque están reservadas para usos especiales según las normas del protocolo IP. Estas direcciones pueden clasificarse en dos categorías principales:

1. **Direcciones no asignadas (Unallocated IP)**: Bloques de direcciones que IANA o los RIRs aún no han asignado a ninguna organización o entidad.
2. **Direcciones reservadas**: Bloques de direcciones definidas por estándares técnicos para propósitos específicos, como las direcciones privadas (RFC 1918) o multicast, que no deben ser enrutadas públicamente.

El término *Bogon* proviene del argot de la comunidad operativa, donde se utiliza para describir "paquetes indeseados" que no deberían transitar en redes públicas. Aunque no es un término formal en los estándares RFC, su uso es común en la seguridad y operación de redes.

Características principales de los Bogons:

1. Categorías de direcciones Bogon:

- Direcciones IP privadas (como 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16)
- Direcciones de bucle invertido (127.0.0.0/8)
- Direcciones de enlace local (169.254.0.0/16)
- Direcciones reservadas para documentación y ejemplos
- Direcciones no asignadas o reservadas por IANA
- Direcciones IPv4 e IPv6 especiales

2. Relevancia en seguridad de red:

Los Bogons representan un riesgo significativo para la infraestructura de red, ya que pueden ser utilizados en:

- Ataques de spoofing
- Técnicas de evasión de filtros
- Actividades de reconnaissance
- Generación de tráfico malicioso

3. Importancia en enrutamiento:

Los routers y firewalls generalmente deben configurarse para filtrar paquetes con direcciones Bogon, previniendo que estos ingresen o salgan de la red.

3. Causas y factores de los incidentes más destacables

En esta sección, se presenta un análisis detallado de las causas y factores que contribuyeron a la ocurrencia de los incidentes de enrutamiento que fueron seleccionados para este informe como “los más destacables”. El objetivo principal es identificar los elementos técnicos, operativos y/o humanos que desencadenaron estos eventos, con el fin de generar un entendimiento profundo de su origen y así visualizar estrategias para prevenir incidentes similares en el futuro.

La selección de estos tres incidentes como los más destacables para su análisis responde a su relevancia dentro del contexto del enrutamiento en América Latina y el Caribe durante el periodo estudiado, y a su alineación con los objetivos de este documento, ya que cada uno de los incidentes seleccionados está vinculado a una de las tres categorías de incidentes que se describen en la sección anterior, así como se muestra a continuación:

- **Secuestro de rutas (route hijacking):** Representado por el **incidente del 9 de julio de 2024**, relacionado con el AS 263238, donde se anunciaron rutas que no deberían haber sido propagadas, causando implicaciones operativas significativas.
- **Fuga de rutas (route leaks):** Ilustrado por el **incidente del 24 de mayo de 2024**, en el que una discrepancia entre los AS 22381 y 262589 resultó en la propagación inadecuada de prefijos, afectando redes locales y regionales.
- **Bogons y secuestro de ruta** Representados por el **incidente del 27 de junio de 2024**, relacionado con la interrupción del servicio DNS de Cloudflare en 1.1.1.1, la cual es una dirección completamente válida para el tráfico público, aunque todavía puede haber configuraciones mal implementadas en algunas redes que tratan el rango como "bogon" (tráfico inválido), lo que podría provocar problemas de enrutamiento, ya que el rango **1.0.0.0/8**, que incluye 1.1.1.1, históricamente era considerado de uso limitado antes de ser asignado oficialmente por IANA a APNIC (Asia-Pacific Network Information Centre) en 2010. Desde entonces, el rango ha sido activamente utilizado, y Cloudflare se asoció con APNIC en 2018 para usar **1.1.1.1** específicamente como servidor DNS.

Además de esto, los tres incidentes seleccionados presentan causas y factores contribuyentes distintos, lo que permite explorar diferentes desafíos en la operación de redes:

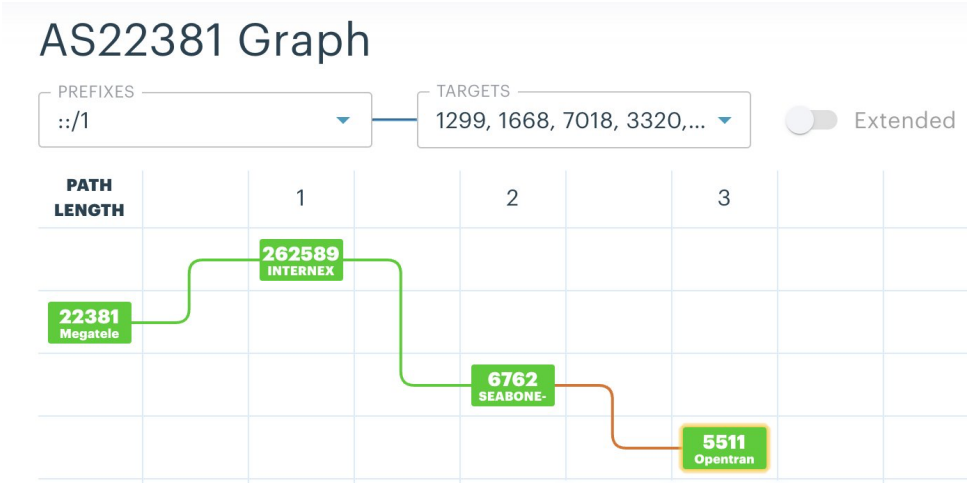
- Errores de configuración y validación **incidente del 9 de julio de 2024.**
- Políticas de enrutamiento inconsistentes entre ASNs **incidente del 24 de mayo de 2024**.
- Falta de filtros y controles sobre rangos reservados **incidente del 27 de junio de 2024.**

3.1. Incidente del 24 de mayo de 2024: Evento entre el AS 22381 y el AS 262589

El 24 de mayo de 2024 ocurrió una anomalía en el intercambio de rutas entre los AS 22381 y 262589, lo que provocó inestabilidad en el tráfico de redes locales y afectó a varios ASN en la región.

El AS22381 (Megatelecom), que es uno de los clientes del proveedor de servicio de Internet AS262589, filtró 4935 prefijos, lo que generó conflictos con 593 sistemas autónomos (ASNs) en 68 países.

La fuga incluyó el anuncio de la dirección IPv6 "::/1", que fue aceptada por proveedores de red de nivel Tier 1, lo que indica un problema grave de enrutamiento.



En la gráfica anterior se evidencia un **route leak** entre los AS22381 y AS262589, donde este último está propagando rutas del AS22381 hacia sistemas externos como SEABONE y Opentrans. Dado que el AS22381 (Megatelecom) es el punto de inicio del tráfico u origen, este sistema autónomo debería limitar el alcance de ciertos anuncios BGP. Sin embargo, los prefijos están siendo propagados más allá de su ámbito previsto.

El siguiente salto en la ruta es el AS262589, que está anunciando rutas provenientes del AS22381 a terceros (como SEABONE y Opentrans). Esto no debería ocurrir bajo condiciones normales, ya que el AS262589 propagó rutas de AS22381 sin aplicar políticas de filtrado adecuadas.

A continuación, el AS6762 (SEABONE), un proveedor de nivel Tier 1, recibe estas rutas y actúa como intermediario hacia otras redes. Finalmente, en el destino el AS5511 (Opentrans).

Causas identificadas

1. **Flujo Anómalo del Tráfico:**
    - El tráfico originado en **AS22381** debería mantenerse en un ámbito controlado y no pasar a través de AS6762 y AS5511. Sin embargo, la propagación a AS262589 causó un desvío hacia redes más grandes.
2. **Inexistencia de Políticas de Filtrado:**
    - AS262589 y AS6762 no aplicaron las políticas de filtrado adecuadas, permitiendo que las rutas de AS22381 fueran anunciadas a otros sistemas autónomos.
3. **Uso Inesperado de Prefijos:**
    - Prefijos que normalmente deberían ser locales (o con un alcance limitado) están siendo propagados a sistemas globales, lo que indica una **fuga de rutas**.

Factores contribuyentes

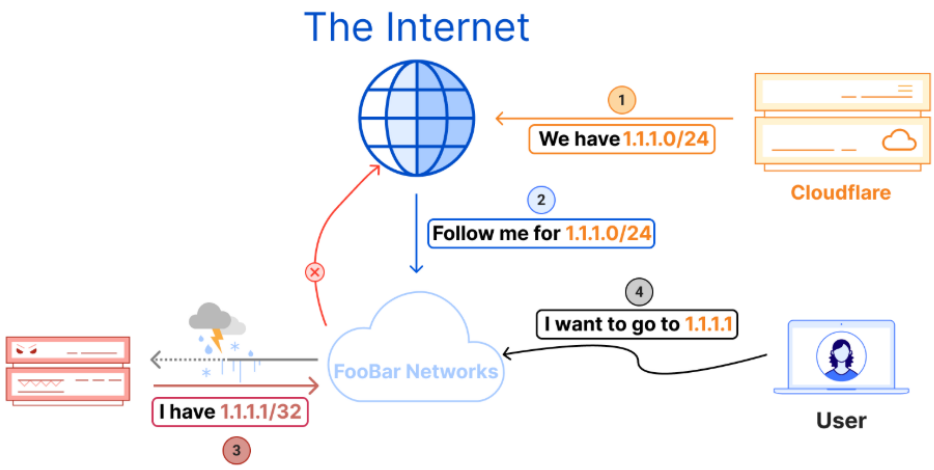
- Falta de acuerdos claros entre los AS sobre el tratamiento de rutas anunciadas.
- Ausencia de filtros adecuados para prevenir la propagación de rutas inconsistentes.

3.2. Incidente del 27 de junio de 2024: Afectación del servicio de resolución DNS de Cloudflare en 1.1.1.1.

El 27 de junio de 2024, se reportó una interrupción significativa en el servicio de resolución DNS de Cloudflare asociado a la dirección 1.1.1.1. Este incidente afectó la conectividad global al comprometer la funcionalidad de uno de los principales servicios de resolución DNS utilizados por usuarios y empresas en todo el mundo.

A pesar del crecimiento en la adopción de RPKI en los últimos años y de que el prefijo **1.1.1.0/24** cuenta con una firma válida, durante el incidente **ELETRONET S.A. (AS267613)** anunció de forma incorrecta el prefijo **1.1.1.1/32**. Este anuncio fue aceptado por diversas redes, incluyendo al menos un proveedor de nivel 1 que lo trató como una ruta de agujero negro. Como consecuencia, la dirección destinada a la resolución DNS quedó inaccesible, impactando de inmediato a más de 300 redes en 70 países.

Simultáneamente al secuestro de **1.1.1.1/32**, **Nova Rede de Telecomunicações Ltda (AS262504)** filtró accidentalmente el prefijo **1.1.1.0/24** hacia **Peer-1 Global Internet Exchange (AS1031)**, lo que amplió aún más su propagación y agravó el impacto percibido por los clientes durante el incidente.



En la anterior gráfica vemos la explicación de cómo funcionó el secuestro de ruta realizado por Electronet al empezar a anunciar el prefijo 1.1.1.1/32, indicando una ruta más específica y provocando que el tráfico de los usuarios que hacen uso del servicio de DNS, envíe las solicitudes hacía su red.

Causas identificadas

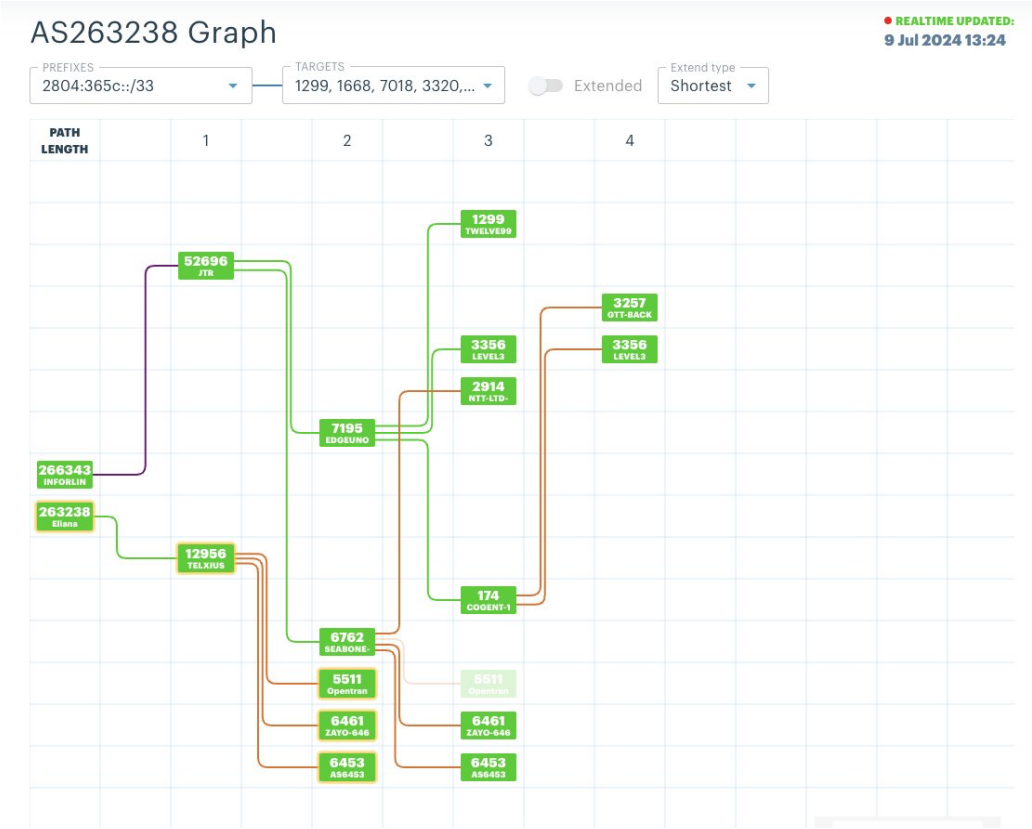
- Redirección no autorizada de tráfico hacia el prefijo 1.1.1.1/32 debido a un error de configuración en un sistema autónomo (AS).
- Ausencia de filtros estrictos en las rutas anunciadas por algunos operadores de red.
- Filtrado incorrecto de la red valida 1.1.1.0/24

Factores contribuyentes

- Falta de validación RPKI en los anuncios relacionados con el prefijo 1.1.1.0/24.
- Propagación del anuncio incorrecto debido a la falta de filtrado en múltiples AS intermedios.

3.3. Incidente del 9 de julio de 2024: Evento significativo con el AS 263238

El 9 de julio de 2024, ocurrió un incidente de enrutamiento significativo relacionado con el **AS263238**, asignado a **Fibramax** un proveedor de servicios de Internet de Ecuador. Durante el evento, este sistema autónomo comenzó a anunciar prefijos IP no autorizados, incluyendo rangos asignados a otras organizaciones y prefijos reservados. Estos anuncios incorrectos fueron aceptados y propagados por varios proveedores de nivel superior, ampliando su alcance y afectando a numerosas redes en la región y a nivel global.



Causas identificadas

- Error de configuración que resultó en el anuncio de rutas inválidas hacia AS vecinos.
- Posible uso indebido de configuraciones automáticas sin validación previa.

Factores contribuyentes

- Dependencia excesiva en un único punto de conexión para múltiples redes regionales.
- Falta de pruebas y monitoreo adecuado antes de realizar cambios en la configuración de enrutamiento.

4. Impacto de los Incidentes más destacables

Estos eventos tuvieron un impacto significativo en la conectividad de la región LAC, tanto en términos de alcance (afectando redes locales, regionales y globales) como de gravedad (interrupciones de servicios críticos). Analizar estos casos permite destacar cómo las anomalías en el enrutamiento de redes en LAC pueden tener repercusiones que trascienden sus fronteras, reforzando la importancia de implementar mejores prácticas.

4.1 Incidente del 24 de mayo de 2024: Evento entre el AS 22381 y el AS 262589

Impacto

- Afectación de redes y servicios locales en varios países de América Latina.
- Interrupciones específicas en redes que dependían de estos AS para conectividad primaria.
- Tiempo de duración del incidente 20 minutos.
- generó conflictos con 592 sistemas autónomos (ASNs) en 68 países.
- Este evento fue lo suficientemente significativo como para ser propagado por el 58% de la infraestructura de Internet, mostrando la magnitud del problema.

Key Info	Description
AS22381 - Megatelecom - [BR] Leaked **5222** prefixes: ▼ Show **2801:80:1e45::/48** from **2024-05-24 02:14** to **...** [high - 262] (**1 conflicts**) **2801:80:1e41::/48** from **2024-05-24 02:14** to **...** [high - 235] (**1 conflicts**) **2804:294:206::/48** from **2024-05-24 02:14** to **...** [high - 232] (**1 conflicts**) **2804:d4b:3c00::/40** from **2024-05-24 02:14** to **...** [medium - 12] (**1 conflicts**) **2804:d45:5800::/40** from **2024-05-24 02:14** to **2024-05-24 02:36** [high - 296] (**1 conflicts**) **2801:80:2530::/48** from **2024-05-24 02:14** to **2024-05-24 02:20** [high - 294] (**1 conflicts**) **2804:d45:5400::/40** from **2024-05-24 02:14** to **2024-05-24 02:36** [high - 291] (**1 conflicts**) **2804:d43:600::/46** from **2024-05-24 02:14** to **2024-05-24 02:36** [high - 289] (**1 conflicts**) **2804:7058:1000::/44** from **2024-05-24 02:14** to **2024-05-24 02:36** [high - 286] (**1 conflicts**) **2804:7058:9000::/44** from **2024-05-24 02:14** to **2024-05-24 02:36** [high - 286] (**1 conflicts**) **2803:b000::/32** from **2024-05-24 02:14** to **2024-05-24 02:19** [high - 280] (**1 conflicts**) **2804:d43:200::/40** from **2024-05-24 02:14** to **2024-05-24 02:37** [high - 277] (**1 conflicts**) **2804:d45:5200::/40** from **2024-05-24 02:14** to **2024-05-24 02:36** [high - 275] (**1 conflicts**) **2800:5b0::/32** from **2024-05-24 02:14** to **2024-05-24 02:19** [high - 275] (**1 conflicts**) **2804:d41:5200::/40** from **2024-05-24 02:14** to **2024-05-24 02:37** [high - 273] (**1 conflicts**) **2804:d41:1200::/40** from **2024-05-24 02:14** to **2024-05-24**	**68** countries; **592** ASNs; **5222** prefixes; **5226 conflicts** min/avg/max propagation - **2/28/296** ▼ Show ▼ **BR - Brazil** (**98** ASNs; **1564** prefixes; **1568 conflicts** min/avg/max propagation - **2/64/296**) ▶ **AS14026 - Nucleo - [BR]** (**8** prefixes; **8 conflicts** min/avg/max propagation - **19/217/262**) ▶ **AS28604 - Globo - [BR]** (**3** prefixes; **3 conflicts** min/avg/max propagation - **19/159/232**) ▶ **AS7738 - V - [BR]** (**1073** prefixes; **1076 conflicts** min/avg/max propagation - **2/60/296**) ..... ▶ **CO - Colombia** (**11** ASNs; **58** prefixes; **58 conflicts** min/avg/max propagation - **2/83/280**) ▶ **PE - Peru** (**2** ASNs; **26** prefixes; **26 conflicts** min/avg/max propagation - **12/223/232**) ▶ **US - United States** (**90** ASNs; **1459** prefixes; **1459 conflicts** min/avg/max propagation - **2/10/224**) ▶ **HK - Hong Kong** (**21** ASNs; **29** prefixes; **29 conflicts** min/avg/max propagation - **4/23/183**) ▶ **GB - United Kingdom** (**25** ASNs; **105** prefixes; **105 conflicts** min/avg/max propagation - **2/23/115**) ▶ **SA - Saudi Arabia** (**2** ASNs; **406** prefixes; **406 conflicts** min/avg/max propagation - **5/8/115**) ▶ **IT - Italy** (**18** ASNs; **35** prefixes; **35 conflicts** min/avg/max propagation - **3/7/112**) ▶ **EC - Ecuador** (**11** ASNs; **55** prefixes; **55 conflicts** min/avg/max propagation - **2/8/106**) ▶ **RU - Russian Federation** (**35** ASNs; **127** prefixes; **127 conflicts** min/avg/max propagation - **2/9/97**) ▶ **IL - Israel** (**1** ASNs; **116** prefixes; **116 conflicts** min/avg/max propagation - **6/14/95**) ▶ **HU - Hungary** (**7** ASNs; **7** prefixes; **7 conflicts** min/avg/max propagation - **4/21/94**)

Adicionalmente en la siguiente gráfica podemos evidenciar la cantidad de conflictos causados por este incidente en 4 diferentes rutas, mostrando que La ruta más problemática es **AS53087 → AS22381 → AS262589**, con **70.1%** de conflictos.

	Conflicts count
AS53087 - TELY - [BR] -> AS22381 - Megatelecom - [BR] -> AS262589 - INTERNEXA - [BR]	3664 (70.1%)
AS6762 - SEABONE-NET - [IT] -> AS22381 - Megatelecom - [BR] -> AS262589 - INTERNEXA - [BR]	1058 (20.2%)
AS3356 - LEVEL3 - [US] -> AS22381 - Megatelecom - [BR] -> AS262589 - INTERNEXA - [BR]	503 (9.6%)
AS52320 - GlobeNet - [CO] -> AS22381 - Megatelecom - [BR] -> AS262589 - INTERNEXA - [BR]	1 (0.0%)

Nota: Si bien en la imagen anterior se relaciona el nombre de InterNexa con el AS262589, cabe aclarar que el día 1 de abril de 2024 la operación de InterNexa Brasil pasó a ser parte de Megatelecom, por lo que al momento del incidente no se debe relacionar a este operador con lo ocasionado. Mas información sobre esto aquí: https://blog.internexa.com/noticias/internexa-brasil-pas%C3%B3-a-ser-parte-de-megatelecom

4.2 Incidente del 27 de junio de 2024: Afectación del servicio de resolución DNS de Cloudflare en 1.1.1.1

Impacto

- Interrupciones masivas en la navegación y acceso a servicios en línea dependientes de 1.1.1.1.
- Impacto global, con mayor incidencia en regiones que dependen en gran medida de Cloudflare para servicios de resolución.
- Duración del incidente un poco más de 7 horas
- Reportes de degradación del servicio en América Latina, Europa y Asia.
- La dirección de la resolución DNS dejara de estar disponible en más de 300 redes en 70 países.

4.3 Incidente del 9 de julio de 2024: Evento significativo con el AS 263238

Impacto

- Afectación de servicios locales en varios países, incluyendo pérdida de conectividad y aumento de la latencia en las rutas afectadas.
- Duración del incidente 5 minutos
- Compromiso de la estabilidad operativa de un gran número de redes interconectadas.
- 1.140 conflictos con 204 ASN en 13 países, siendo Brasil el país más afectado, tal como se visualiza en la siguiente imagen:

Key Info	Description
AS263238 - Eliana - [EC] Created **393** hijack prefixes ▼ Show **2804:365c::/33** from **2024-07-09 05:50** to **...** [high - 47] (**2 conflicts**) **2804:365c:8000::/33** from **2024-07-09 05:50** to **...** [high - 47] (**2 conflicts**) **2804:89ac:fffe::/47** from **2024-07-09 05:50** to **...** [high - 44] (**2 conflicts**) **2804:4eac:1601::/48** from **2024-07-09 05:50** to **...** [high - 37] (**2 conflicts**) **2804:4eac:1602::/48** from **2024-07-09 05:50** to **...** [high - 37] (**2 conflicts**) **2804:1bc8::/33** from **2024-07-09 05:50** to **...** [high - 19] (**2 conflicts**) **2804:8e4c::/32** from **2024-07-09 05:50** to **...** [high - 75] (**1 conflicts**) **2800:970::/32** from **2024-07-09 05:50** to **...** [high - 70] (**1 conflicts**) **2804:7d40:8000::/34** from **2024-07-09 05:50** to **...** [high - 62] (**1 conflicts**) **2804:8c18::/32** from **2024-07-09 05:50** to **...** [high - 48] (**3 conflicts**) **2804:365c::/32** from **2024-07-09 05:50** to **...** [high - 41] (**3 conflicts**) **2610:a1:1004::/48** from **2024-07-09 05:50** to **...** [high - 35] (**22 conflicts**) **2610:a1:1022::/48** from **2024-07-09 05:50** to **...** [high - 35] (**20 conflicts**) **2804:4eac::/32** from **2024-07-09 05:50** to **...** [high - 30] (**3 conflicts**)	**13** countries; **204** ASNs; **541** prefixes; **1140 conflicts** min/avg/max propagation - **4/34/230** ▼ Show ▶ **BR - Brazil** (**142** ASNs; **411** prefixes; **721 conflicts** min/avg/max propagation - **4/35/115**) ▶ **AR - Argentina** (**1** ASNs; **1** prefixes; **1 conflicts** min/avg/max propagation - **70/70/70**) ▶ **US - United States** (**39** ASNs; **60** prefixes; **330 conflicts** min/avg/max propagation - **4/25/35**) ▶ **EC - Ecuador** (**4** ASNs; **26** prefixes; **36 conflicts** min/avg/max propagation - **11/104/230**) ▶ **ZZ** (**2** ASNs; **4** prefixes; **4 conflicts** min/avg/max propagation - **10/43/55**) ▶ **CO - Colombia** (**5** ASNs; **20** prefixes; **20 conflicts** min/avg/max propagation - **10/33/59**) ▶ **MX - Mexico** (**2** ASNs; **6** prefixes; **14 conflicts** min/avg/max propagation - **4/4/13**) ▶ **CA - Canada** (**2** ASNs; **5** prefixes; **5 conflicts** min/avg/max propagation - **12/28/58**) ▶ **CL - Chile** (**2** ASNs; **2** prefixes; **2 conflicts** min/avg/max propagation - **10/32/55**) ▶ **AT - Austria** (**2** ASNs; **1** prefixes; **2 conflicts** min/avg/max propagation - **50/50/50**) ▶ **AU - Australia** (**1** ASNs; **2** prefixes; **2 conflicts** min/avg/max propagation - **22/22/22**) ▶ **IL - Israel** (**1** ASNs; **1** prefixes; **1 conflicts** min/avg/max propagation - **4/4/4**) ▶ **PA - Panama** (**1** ASNs; **2** prefixes; **2 conflicts** min/avg/max propagation - **4/4/4**)

5. Protocolos y prácticas de seguridad implementados para contrarrestarlos

En esta sección se analizan las medidas de corrección y las prácticas de seguridad adoptadas para mitigar y resolver los incidentes de enrutamiento, con un enfoque particular en el incidente ocurrido el 27 de junio de 2024, que describimos en detalle en las secciones anteriores. Describiendo las acciones específicas tomadas para restaurar la conectividad, incluyendo la aplicación de validación de rutas mediante RPKI, ajustes en las políticas de filtrado de prefijos y el fortalecimiento de las herramientas de monitoreo y detección temprana.

5.1. Uso de RPKI

Aparte de realizar la corrección de anuncios incorrectos por parte de los operadores de las redes involucradas, una de las principales medidas para mitigar los efectos del incidente, fue la validación de origen utilizando RPKI (Infraestructura de Claves Públicas de Enrutamiento), demostrando, que se necesita una mayor adopción global para evitar que las rutas secuestradas se propaguen. En el caso de 1.1.1.1, varias redes aceptaron y reenviaron la ruta anunciada incorrectamente por AS267613. Esto resalta la necesidad de que más redes implementen RPKI, especialmente aquellas con una gran cantidad de AS descendentes, para asegurar que las rutas sean verificadas y autenticadas antes de ser aceptadas y propagadas.

Adicional a esto, el incidente también puso en evidencia la importancia del BGP Blackhole Filtering (RTBH), que se describe en el [5] RFC5635 que describe cómo configurar BGP para recibir prefijos de enrutamiento de agujero negro, cómo crear una política de filtrado adecuada y cómo implementar el proceso de enrutamiento para que el tráfico se descarte de manera eficiente. Sin embargo, en este caso, un proveedor de nivel 1 aceptó erróneamente el prefijo 1.1.1.1/32 como una ruta de agujero negro de una fuente no autorizada, lo que resultó en un secuestro peligroso.

5.2. Implementación de MANRS

Una medida fundamental para evitar la propagación de rutas erróneas es seguir las mejores prácticas de BGP recomendadas por organizaciones como MANRS. Por

[5] https://datatracker.ietf.org/doc/html/rfc5635

ejemplo, rechazar prefijos IPv4 que tengan una longitud mayor a /24 en la Default Free Zone (DFZ) habría reducido los efectos del secuestro de 1.1.1.1/32. Implementar políticas de filtrado más estrictas sobre las rutas que se aceptan y propagan en la red es crucial para mantener la integridad de las rutas de Internet. Esta práctica debería ser parte del estándar para todas las redes de Internet, para prevenir que rutas no válidas se filtren a través de la infraestructura global.

De igual forma y dado que no es posible evitar completamente las filtraciones de ruta debido a la confianza implícita entre las redes, Cloudflare implementó medidas adicionales para limitar el impacto de incidentes similares en el futuro, las cuales están basadas en ampliar las fuentes de datos que alimentan su sistema de detección de filtraciones de ruta, lo que ahora les permite cubrir más redes y detectar filtraciones con mayor precisión. Además, se están incorporando datos en tiempo real en el sistema de monitoreo, lo que les permitirá responder más rápidamente a incidentes similares en el futuro.

5.3. Hechos destacables y acciones implementadas para la prevención de incidentes en los IXPs

En este segmento se entregará información en detalle de un caso de éxito que ocurrió fuera de nuestra región, pero que muestra el ejemplo de mitigación de un incidente de fuga de rutas, realizada entre los puntos de intercambio de FranceIX (fracia) y YYCIX (Canada) aplicando lo indicado en el RFC 9234.

¿Qué es RFC 9234 y el atributo OTC?

[6]El RFC 9234 introduce un mecanismo llamado "OTC" (Only-To-Customer), un atributo en BGP que permite identificar y bloquear rutas mal propagadas.

El atributo OTC se añade a las rutas que son enviadas de un proveedor a un cliente.

Si un router recibe una ruta con OTC de un AS que no es un cliente directo, el tráfico se bloquea. Esto evita que se propaguen más allá de su alcance legítimo.

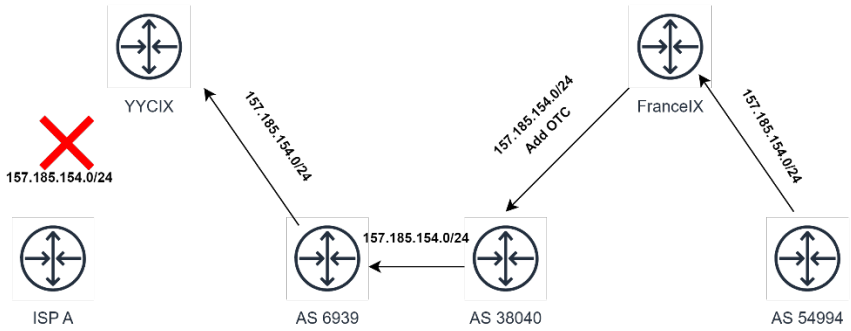
Detalle del evento

El lunes 2 de septiembre de 2024, ocurrió una pequeña fuga de rutas que involucra tanto a los servidores de rutas de YYCIX como a los de FranceIX a través de un ISP conectado a los servidores de rutas de ambos IXPs; sin embargo, la fuga fue

[6] https://datatracker.ietf.org/doc/rfc9234/

detenida en YYCIX gracias a RFC 9234.

YYCIX, implementó soporte para RFC9234 a finales de 2022 y principios de 2023 utilizando OpenBGPD; mientras que FranceIX implementó soporte utilizando BIRD en el segundo trimestre de 2024. Ambos IXPs configuraron sus servidores de rutas para rechazar rutas BGP que tengan un atributo OTC adjunto, y para agregar un atributo OTC al propagar rutas a los pares del servidor de rutas.



En la imagen anterior se observa que el AS 54994 origina el prefijo 157.185.154.0/24 y lo propaga hacia los servidores de rutas de FranceIX. FranceIX acepta esta ruta (probablemente debido a la existencia de un objeto de ruta IRR) y la propaga con el atributo "Only-To-Customer" configurado en 51706. La ruta es recibida por el AS 38040, que aparentemente la propaga a su upstream, el AS 6939. Esto sugiere que un router del AS 38040 podría estar mal configurado. Posteriormente, el AS 6939 envía las rutas de su cliente al servidor de rutas de YYCIX. Sin embargo, el servidor de rutas de YYCIX detecta que la ruta ya atravesó un "valle", la identifica como una filtración de ruta y bloquea su propagación hacia ISP_A.

Teniendo presente la anterior explicación es importante destacar que:

- El RFC 9234 es un mecanismo fácil de configurar y depurar tanto para operadores de redes pequeñas y grandes como para operadores de servidores de rutas de IXPs.

- En el escenario descrito anteriormente, es probable que YYCIX y FranceIX sean las únicas dos entidades en todo el camino de AS que soportan RFC 9234; Loque demuestra que no es necesario que todos los AS en la ruta adopten el mecanismo para que sea efectivo.

- Las implementaciones de servidores de rutas más populares del mundo (BIRD y OpenBGPD) ya soportan RFC 9234.

- La combinación del atributo OTC y políticas de enrutamiento en los IXPs asegura que las fugas de rutas, sean bloqueadas automáticamente.

6. Recomendaciones o lecciones aprendidas y conclusiones

- El análisis realizado permitió identificar tendencias temporales, patrones regionales y variaciones en la frecuencia de los incidentes de enrutamiento, proporcionando una base sólida para comprender su distribución geográfica y cronológica durante el período estudiado en la región de América Latina y el Caribe (LAC). Estos hallazgos son fundamentales para detectar áreas críticas, anticipar posibles vulnerabilidades y fomentar la adopción de mejores prácticas que contribuyan a la estabilidad y seguridad del ecosistema de enrutamiento en la región.
- Los incidentes denominados como más destacables que fueron analizados en este informe, destacan problemáticas específicas de la región, como la ausencia de validación RPKI generalizada y la necesidad de mejorar los acuerdos de enrutamiento entre operadores. Al analizarlos, se pueden extraer lecciones que sirvan para mitigar incidentes futuros.
- Los incidentes analizados reflejan desafíos comunes en el manejo del enrutamiento y la operación común en las redes de América Latina y el Caribe, como la falta de validación de rutas, errores de configuración y políticas inconsistentes entre sistemas autónomos. Abordar estos problemas requerirá un esfuerzo conjunto entre operadores de red, Puntos de intercambio de Internet - IXPs e iniciativas como MANRS para implementar mejores prácticas que garanticen la estabilidad y resiliencia del sistema de enrutamiento global.
- Los incidentes seleccionados también ofrecen un contexto adecuado para evaluar el papel de los puntos de intercambio de Internet (IXPs) en la mitigación y contención de incidentes. Dado que los IXPs actúan como puntos clave en la interconexión de redes, su análisis en estos eventos proporciona un marco para entender cómo contribuyen (o podrían contribuir) a la estabilidad del ecosistema.

Lecciones aprendidas

- Es importante continuar con la estandarización de políticas de enrutamiento y el establecimiento de acuerdos entre AS, ya que, gracias a esto, se pueden prevenir varios de los incidentes mencionados en este documento.
- Es necesario seguir apostando por entregar mayor capacitación técnica para operadores en la región para mitigar errores de configuración.
- Se sigue demostrando la necesidad de implementar validación RPKI y políticas de filtrado rigurosas en los operadores de red.

- Es necesario hacer ajustes y mejoras en los procesos de monitoreo, para lograr visualizar y obtener datos en tiempo real para detectar y mitigar incidentes similares rápidamente.
- Continúa siendo una buena práctica realizar pruebas rigurosas en entornos simulados antes de implementar configuraciones en producción.
- La diversificación de enlaces y caminos puede mitigar de cierto modo el impacto de incidentes de enrutamiento.

Agradecimientos especiales

Quisiera expresar mi más profundo agradecimiento al equipo de Investigación y Desarrollo en Infraestructura de Internet de LACNIC, liderado por Guillermo Cicileo, por brindarme la oportunidad de llevar a cabo este análisis y por su invaluable apoyo durante todo el proceso.

Mi reconocimiento también al equipo de Global Cyber Alliance, especialmente a Alejandro Fernández y Andrei Robachevsky, quienes no solo me proporcionaron datos valiosos, sino que también me facilitaron los contactos clave con personas y organizaciones que realizaron aportes esenciales para este análisis. El acompañamiento constante de ambos fue crucial para el desarrollo de este informe.

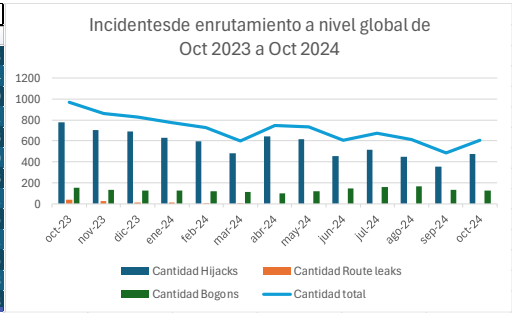
Además, quiero expresar mi sincero agradecimiento al equipo de Qrator, por el gran interés que mostraron en el trabajo realizado y por su generoso aporte de datos, tanto a través de herramientas como Qradar, sus informes periódicos, el canal de X, como de otros recursos enviados por Ivan Potapov y Alexander Lyamin, cuya contribución fue vital para estructurar este documento.

Por último, pero no menos importante, agradezco de manera especial al equipo de Georgia Tech - GaTech, cuyo interés en este estudio se reflejó en su valiosa aportación de datos que enriquecieron y validaron las fuentes utilizadas en este análisis.

ANEXO 1

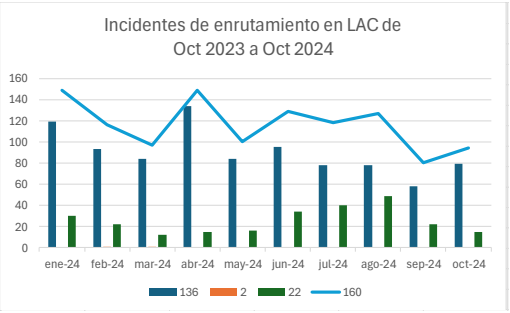
1- INCIDENTES DE ENRUTAMIENTO GLOBALES DE OCT 2023 A OCT 2024

Incidentes de enrutamiento Globales de Oct 2023 a Oct 2024				
Fecha	Cantidad Hijacks	Cantidad Route leaks	Cantidad Bogons	Cantidad total
oct-23	778	36	154	968
nov-23	705	25	134	864
dic-23	693	10	126	829
ene-24	632	11	128	771
feb-24	598	8	120	726
mar-24	482	3	114	599
abr-24	644	0	102	746
may-24	613	0	118	731
jun-24	456	0	149	605
jul-24	513	0	158	671
ago-24	451	0	164	615
sep-24	351	0	132	483
oct-24	474	0	129	603



2- INCIDENTES DE ENRUTAMIENTO EN LAC DE OCT 2023 A OCT 2024

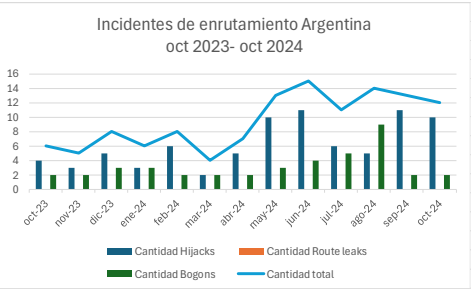
Incidentes de enrutamiento en LAC de Oct 2023 a Oct 2024				
Fecha	Cantidad Hijacks	Cantidad Route leaks	Cantidad Bogons	Cantidad total
oct-23	115	3	24	142
nov-23	155	3	29	187
dic-23	136	2	22	160
ene-24	119	0	30	149
feb-24	93	1	22	116
mar-24	84	1	12	97
abr-24	134	0	15	149
may-24	84	0	16	100
jun-24	95	0	34	129
jul-24	78	0	40	118
ago-24	78	0	49	127
sep-24	58	0	22	80
oct-24	79	0	15	94



INCIDENTES POR PAÍS

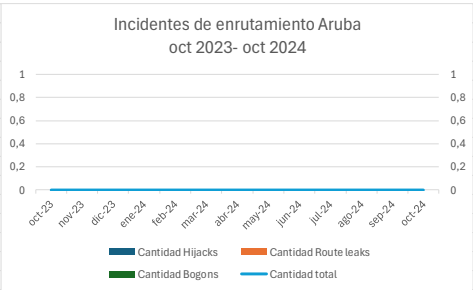
Argentina

Fecha	Cantidad Hijacks	Cantidad Route leaks	Cantidad Bogons	Cantidad total
oct-23	4	0	2	6
nov-23	3	0	2	5
dic-23	5	0	3	8
ene-24	3	0	3	6
feb-24	6	0	2	8
mar-24	2	0	2	4
abr-24	5	0	2	7
may-24	10	0	3	13
jun-24	11	0	4	15
jul-24	6	0	5	11
ago-24	5	0	9	14
sep-24	11	0	2	13
oct-24	10	0	2	12
Total	81	0	41	122



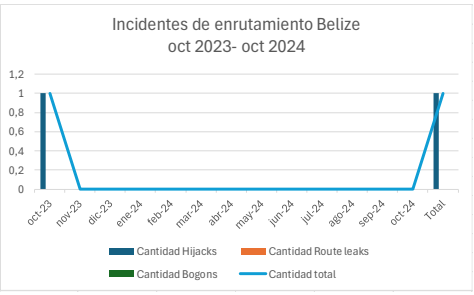
Aruba

Fecha	Cantidad Hijacks	Cantidad Route leaks	Cantidad Bogons	Cantidad total
oct-23	0	0	0	0
nov-23	0	0	0	0
dic-23	0	0	0	0
ene-24	0	0	0	0
feb-24	0	0	0	0
mar-24	0	0	0	0
abr-24	0	0	0	0
may-24	0	0	0	0
jun-24	0	0	0	0
jul-24	0	0	0	0
ago-24	0	0	0	0
sep-24	0	0	0	0
oct-24	0	0	0	0
Total	0	0	0	0



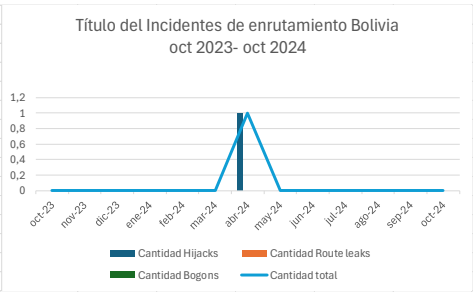
Belice

Fecha	Cantidad Hijacks	Cantidad Route leaks	Cantidad Bogons	Cantidad total
oct-23	1	0	0	1
nov-23	0	0	0	0
dic-23	0	0	0	0
ene-24	0	0	0	0
feb-24	0	0	0	0
mar-24	0	0	0	0
abr-24	0	0	0	0
may-24	0	0	0	0
jun-24	0	0	0	0
jul-24	0	0	0	0
ago-24	0	0	0	0
sep-24	0	0	0	0
oct-24	0	0	0	0
Total	1	0	0	1



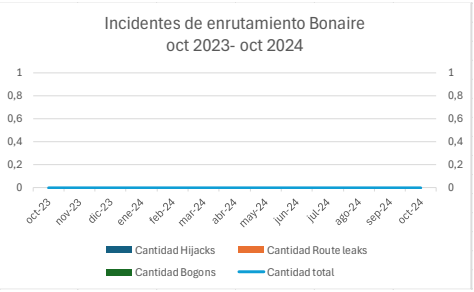
Bolivia

Fecha	Cantidad Hijacks	Cantidad Route leaks	Cantidad Bogons	Cantidad total
oct-23	0	0	0	0
nov-23	0	0	0	0
dic-23	0	0	0	0
ene-24	0	0	0	0
feb-24	0	0	0	0
mar-24	0	0	0	0
abr-24	1	0	0	1
may-24	0	0	0	0
jun-24	0	0	0	0
jul-24	0	0	0	0
ago-24	0	0	0	0
sep-24	0	0	0	0
oct-24	0	0	0	0
Total	1	0	0	1



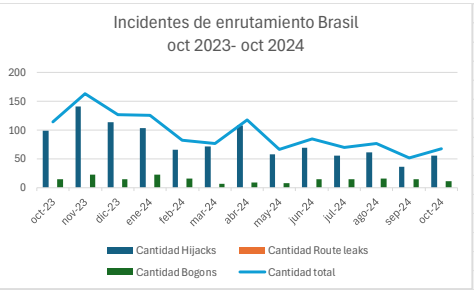
Bonaire

Fecha	Cantidad Hijacks	Cantidad Route leaks	Cantidad Bogons	Cantidad total
oct-23	0	0	0	0
nov-23	0	0	0	0
dic-23	0	0	0	0
ene-24	0	0	0	0
feb-24	0	0	0	0
mar-24	0	0	0	0
abr-24	0	0	0	0
may-24	0	0	0	0
jun-24	0	0	0	0
jul-24	0	0	0	0
ago-24	0	0	0	0
sep-24	0	0	0	0
oct-24	0	0	0	0
Total	0	0	0	0



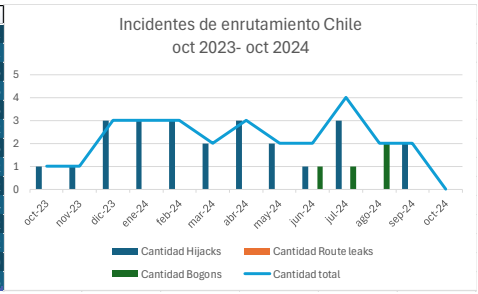
Brasil

Fecha	Cantidad Hijacks	Cantidad Route leaks	Cantidad Bogons	Cantidad total
oct-23	99	0	15	114
nov-23	141	0	22	163
dic-23	113	0	14	127
ene-24	103	0	22	125
feb-24	66	0	16	82
mar-24	71	0	6	77
abr-24	108	0	9	117
may-24	58	0	8	66
jun-24	69	0	15	84
jul-24	56	0	14	70
ago-24	61	0	16	77
sep-24	36	0	15	51
oct-24	56	0	11	67
Total	1037	0	183	1220



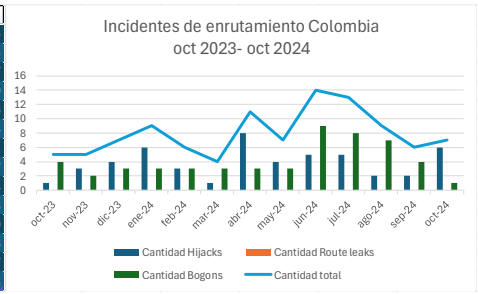
Chile

Fecha	Cantidad Hijacks	Cantidad Route leaks	Cantidad Bogons	Cantidad total
oct-23	1	0	0	1
nov-23	1	0	0	1
dic-23	3	0	0	3
ene-24	3	0	0	3
feb-24	3	0	0	3
mar-24	2	0	0	2
abr-24	3	0	0	3
may-24	2	0	0	2
jun-24	1	0	1	2
jul-24	3	0	1	4
ago-24	0	0	2	2
sep-24	2	0	0	2
oct-24	0	0	0	0
Total	24	0	4	28



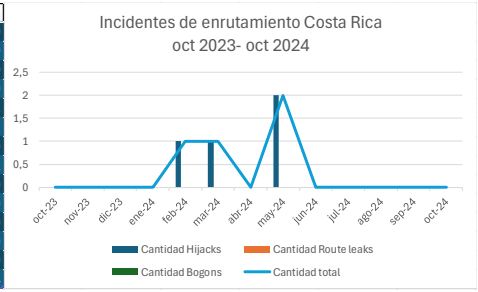
Colombia

Fecha	Cantidad Hijacks	Cantidad Route leaks	Cantidad Bogons	Cantidad total
oct-23	1	0	4	5
nov-23	3	0	2	5
dic-23	4	0	3	7
ene-24	6	0	3	9
feb-24	3	0	3	6
mar-24	1	0	3	4
abr-24	8	0	3	11
may-24	4	0	3	7
jun-24	5	0	9	14
jul-24	5	0	8	13
ago-24	2	0	7	9
sep-24	2	0	4	6
oct-24	6	0	1	7
Total	50	0	53	103



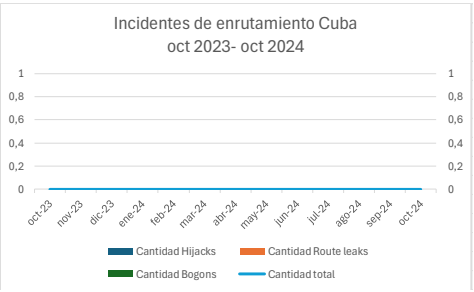
Costa Rica

Fecha	Cantidad Hijacks	Cantidad Route leaks	Cantidad Bogons	Cantidad total
oct-23	0	0	0	0
nov-23	0	0	0	0
dic-23	0	0	0	0
ene-24	0	0	0	0
feb-24	1	0	0	1
mar-24	1	0	0	1
abr-24	0	0	0	0
may-24	2	0	0	2
jun-24	0	0	0	0
jul-24	0	0	0	0
ago-24	0	0	0	0
sep-24	0	0	0	0
oct-24	0	0	0	0
Total	4	0	0	4



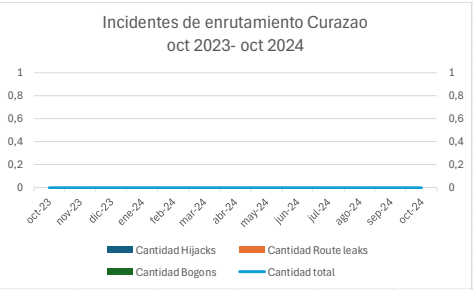
Cuba

Fecha	Cantidad Hijacks	Cantidad Route leaks	Cantidad Bogons	Cantidad total
oct-23	0	0	0	0
nov-23	0	0	0	0
dic-23	0	0	0	0
ene-24	0	0	0	0
feb-24	0	0	0	0
mar-24	0	0	0	0
abr-24	0	0	0	0
may-24	0	0	0	0
jun-24	0	0	0	0
jul-24	0	0	0	0
ago-24	0	0	0	0
sep-24	0	0	0	0
oct-24	0	0	0	0
Total	0	0	0	0



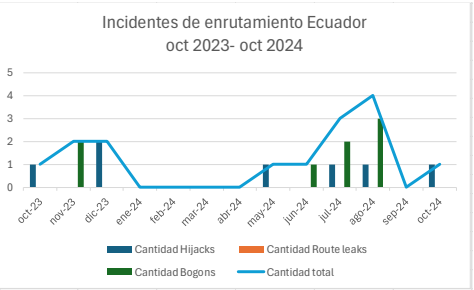
Curazao

Fecha	Cantidad Hijacks	Cantidad Route leaks	Cantidad Bogons	Cantidad total
oct-23	0	0	0	0
nov-23	0	0	0	0
dic-23	0	0	0	0
ene-24	0	0	0	0
feb-24	0	0	0	0
mar-24	0	0	0	0
abr-24	0	0	0	0
may-24	0	0	0	0
jun-24	0	0	0	0
jul-24	0	0	0	0
ago-24	0	0	0	0
sep-24	0	0	0	0
oct-24	0	0	0	0
Total	0	0	0	0



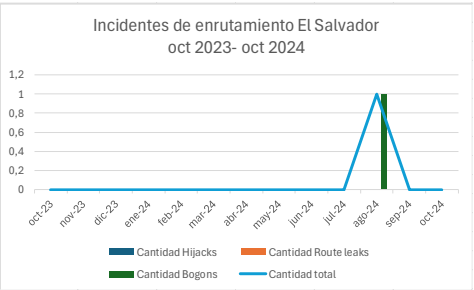
Ecuador

Fecha	Cantidad Hijacks	Cantidad Route leaks	Cantidad Bogons	Cantidad total
oct-23	1	0	0	1
nov-23	0	0	2	2
dic-23	2	0	0	2
ene-24	0	0	0	0
feb-24	0	0	0	0
mar-24	0	0	0	0
abr-24	0	0	0	0
may-24	1	0	0	1
jun-24	0	0	1	1
jul-24	1	0	2	3
ago-24	1	0	3	4
sep-24	0	0	0	0
oct-24	1	0	0	1
Total	7	0	8	15



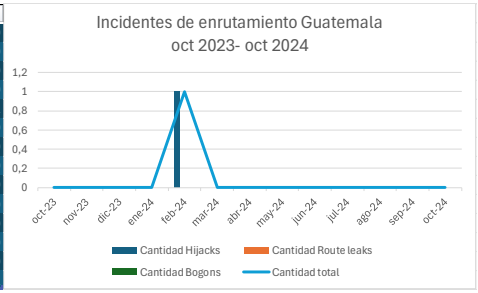
El Salvador

Fecha	Cantidad Hijacks	Cantidad Route leaks	Cantidad Bogons	Cantidad total
oct-23	0	0	0	0
nov-23	0	0	0	0
dic-23	0	0	0	0
ene-24	0	0	0	0
feb-24	0	0	0	0
mar-24	0	0	0	0
abr-24	0	0	0	0
may-24	0	0	0	0
jun-24	0	0	0	0
jul-24	0	0	0	0
ago-24	0	0	1	1
sep-24	0	0	0	0
oct-24	0	0	0	0
Total	0	0	1	1



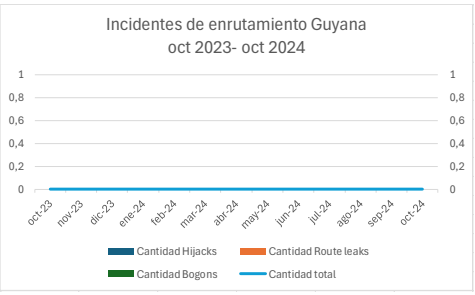
Guatemala

Fecha	Cantidad Hijacks	Cantidad Route leaks	Cantidad Bogons	Cantidad total
oct-23	0	0	0	0
nov-23	0	0	0	0
dic-23	0	0	0	0
ene-24	0	0	0	0
feb-24	1	0	0	1
mar-24	0	0	0	0
abr-24	0	0	0	0
may-24	0	0	0	0
jun-24	0	0	0	0
jul-24	0	0	0	0
ago-24	0	0	0	0
sep-24	0	0	0	0
oct-24	0	0	0	0
Total	1	0	0	1



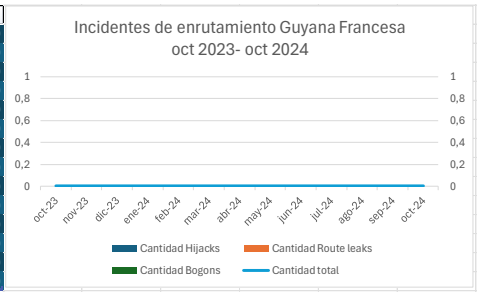
Guyana

Fecha	Cantidad Hijacks	Cantidad Route leaks	Cantidad Bogons	Cantidad total
oct-23	0	0	0	0
nov-23	0	0	0	0
dic-23	0	0	0	0
ene-24	0	0	0	0
feb-24	0	0	0	0
mar-24	0	0	0	0
abr-24	0	0	0	0
may-24	0	0	0	0
jun-24	0	0	0	0
jul-24	0	0	0	0
ago-24	0	0	0	0
sep-24	0	0	0	0
oct-24	0	0	0	0
Total	0	0	0	0



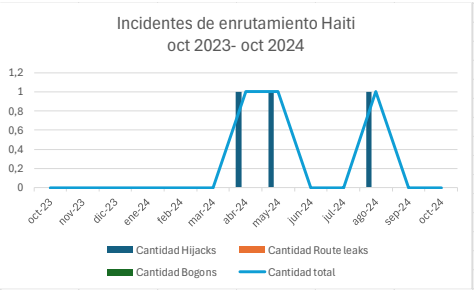
Guyana Francesa

Fecha	Cantidad Hijacks	Cantidad Route leaks	Cantidad Bogons	Cantidad total
oct-23	0	0	0	0
nov-23	0	0	0	0
dic-23	0	0	0	0
ene-24	0	0	0	0
feb-24	0	0	0	0
mar-24	0	0	0	0
abr-24	0	0	0	0
may-24	0	0	0	0
jun-24	0	0	0	0
jul-24	0	0	0	0
ago-24	0	0	0	0
sep-24	0	0	0	0
oct-24	0	0	0	0
Total	0	0	0	0



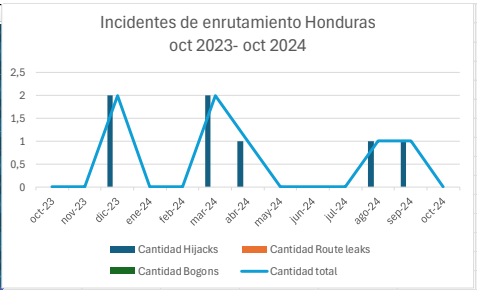
Haití

Fecha	Cantidad Hijacks	Cantidad Route leaks	Cantidad Bogons	Cantidad total
oct-23	0	0	0	0
nov-23	0	0	0	0
dic-23	0	0	0	0
ene-24	0	0	0	0
feb-24	0	0	0	0
mar-24	0	0	0	0
abr-24	1	0	0	1
may-24	1	0	0	1
jun-24	0	0	0	0
jul-24	0	0	0	0
ago-24	1	0	0	1
sep-24	0	0	0	0
oct-24	0	0	0	0
Total	3	0	0	3



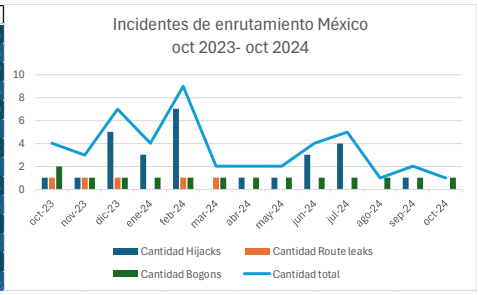
Honduras

Fecha	Cantidad Hijacks	Cantidad Route leaks	Cantidad Bogons	Cantidad total
oct-23	0	0	0	0
nov-23	0	0	0	0
dic-23	2	0	0	2
ene-24	0	0	0	0
feb-24	0	0	0	0
mar-24	2	0	0	2
abr-24	1	0	0	1
may-24	0	0	0	0
jun-24	0	0	0	0
jul-24	0	0	0	0
ago-24	1	0	0	1
sep-24	1	0	0	1
oct-24	0	0	0	0
Total	7	0	0	7



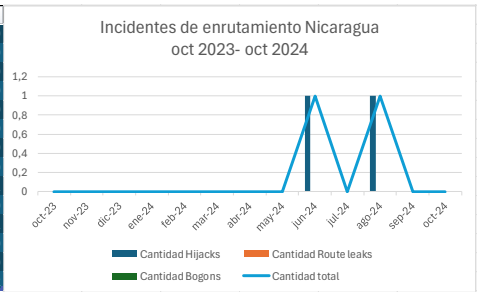
México

Fecha	Cantidad Hijacks	Cantidad Route leaks	Cantidad Bogons	Cantidad total
oct-23	1	1	2	4
nov-23	1	1	1	3
dic-23	5	1	1	7
ene-24	3	0	1	4
feb-24	7	1	1	9
mar-24	0	1	1	2
abr-24	1	0	1	2
may-24	1	0	1	2
jun-24	3	0	1	4
jul-24	4	0	1	5
ago-24	0	0	1	1
sep-24	1	0	1	2
oct-24	0	0	1	1
Total	27	5	14	46



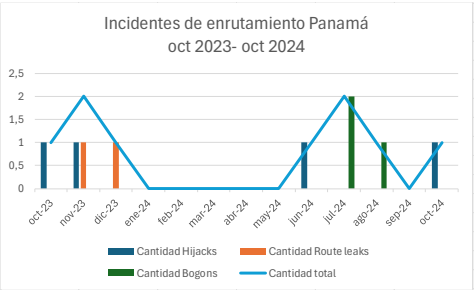
Nicaragua

Fecha	Cantidad Hijacks	Cantidad Route leaks	Cantidad Bogons	Cantidad total
oct-23	0	0	0	0
nov-23	0	0	0	0
dic-23	0	0	0	0
ene-24	0	0	0	0
feb-24	0	0	0	0
mar-24	0	0	0	0
abr-24	0	0	0	0
may-24	0	0	0	0
jun-24	1	0	0	1
jul-24	0	0	0	0
ago-24	1	0	0	1
sep-24	0	0	0	0
oct-24	0	0	0	0
Total	2	0	0	2



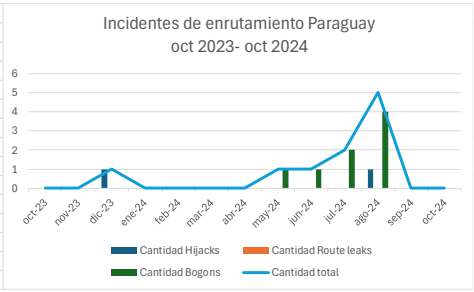
Panamá

Fecha	Cantidad Hijacks	Cantidad Route leaks	Cantidad Bogons	Cantidad total
oct-23	1	0	0	1
nov-23	1	1	0	2
dic-23	0	1	0	1
ene-24	0	0	0	0
feb-24	0	0	0	0
mar-24	0	0	0	0
abr-24	0	0	0	0
may-24	0	0	0	0
jun-24	1	0	0	1
jul-24	0	0	2	2
ago-24	0	0	1	1
sep-24	0	0	0	0
oct-24	1	0	0	1
Total	4	2	3	9



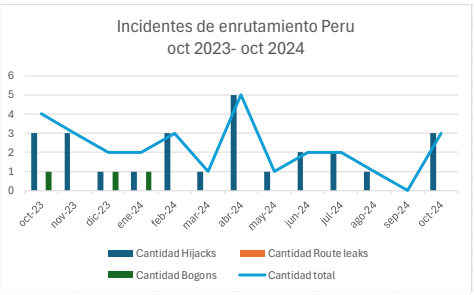
Paraguay

Fecha	Cantidad Hijacks	Cantidad Route leaks	Cantidad Bogons	Cantidad total
oct-23	0	0	0	0
nov-23	0	0	0	0
dic-23	1	0	0	1
ene-24	0	0	0	0
feb-24	0	0	0	0
mar-24	0	0	0	0
abr-24	0	0	0	0
may-24	0	0	1	1
jun-24	0	0	1	1
jul-24	0	0	2	2
ago-24	1	0	4	5
sep-24	0	0	0	0
oct-24	0	0	0	0
Total	2	0	8	10



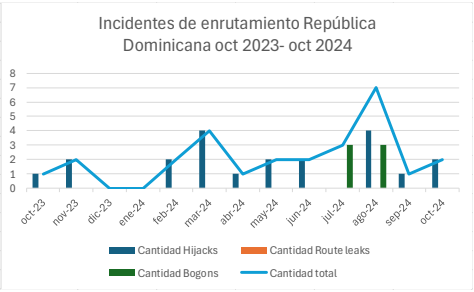
Perú

Fecha	Cantidad Hijacks	Cantidad Route leaks	Cantidad Bogons	Cantidad total
oct-23	3	0	1	4
nov-23	3	0	0	3
dic-23	1	0	1	2
ene-24	1	0	1	2
feb-24	3	0	0	3
mar-24	1	0	0	1
abr-24	5	0	0	5
may-24	1	0	0	1
jun-24	2	0	0	2
jul-24	2	0	0	2
ago-24	1	0	0	1
sep-24	0	0	0	0
oct-24	3	0	0	3
Total	26	0	3	29



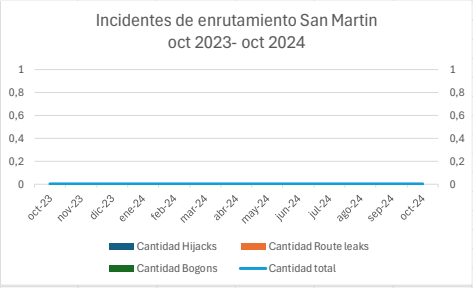
República Dominicana

Fecha	Cantidad Hijacks	Cantidad Route leaks	Cantidad Bogons	Cantidad total
oct-23	1	0	0	1
nov-23	2	0	0	2
dic-23	0	0	0	0
ene-24	0	0	0	0
feb-24	2	0	0	2
mar-24	4	0	0	4
abr-24	1	0	0	1
may-24	2	0	0	2
jun-24	2	0	0	2
jul-24	0	0	3	3
ago-24	4	0	3	7
sep-24	1	0	0	1
oct-24	2	0	0	2
Total	21	0	6	27



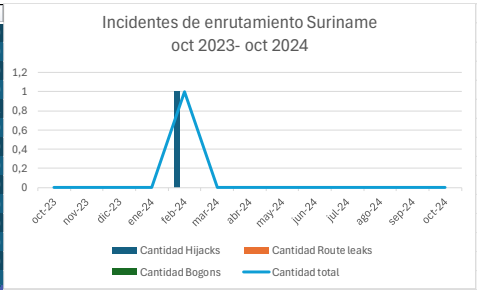
San Martin

Fecha	Cantidad Hijacks	Cantidad Route leaks	Cantidad Bogons	Cantidad total
oct-23	0	0	0	0
nov-23	0	0	0	0
dic-23	0	0	0	0
ene-24	0	0	0	0
feb-24	0	0	0	0
mar-24	0	0	0	0
abr-24	0	0	0	0
may-24	0	0	0	0
jun-24	0	0	0	0
jul-24	0	0	0	0
ago-24	0	0	0	0
sep-24	0	0	0	0
oct-24	0	0	0	0
Total	0	0	0	0



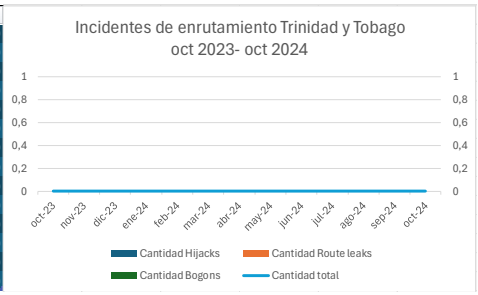
Suriname

Fecha	Cantidad Hijacks	Cantidad Route leaks	Cantidad Bogons	Cantidad total
oct-23	0	0	0	0
nov-23	0	0	0	0
dic-23	0	0	0	0
ene-24	0	0	0	0
feb-24	1	0	0	1
mar-24	0	0	0	0
abr-24	0	0	0	0
may-24	0	0	0	0
jun-24	0	0	0	0
jul-24	0	0	0	0
ago-24	0	0	0	0
sep-24	0	0	0	0
oct-24	0	0	0	0
Total	1	0	0	1



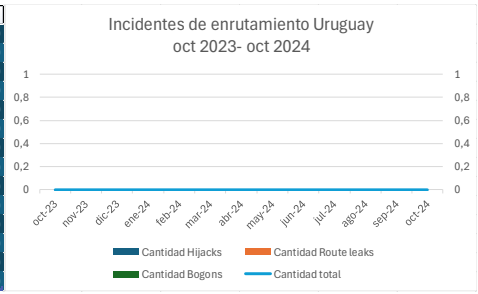
Trinidad y Tobago

Fecha	Cantidad Hijacks	Cantidad Route leaks	Cantidad Bogons	Cantidad total
oct-23	0	0	0	0
nov-23	0	0	0	0
dic-23	0	0	0	0
ene-24	0	0	0	0
feb-24	0	0	0	0
mar-24	0	0	0	0
abr-24	0	0	0	0
may-24	0	0	0	0
jun-24	0	0	0	0
jul-24	0	0	0	0
ago-24	0	0	0	0
sep-24	0	0	0	0
oct-24	0	0	0	0
Total	0	0	0	0



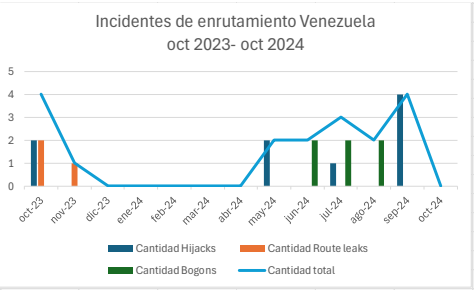
Uruguay

Fecha	Cantidad Hijacks	Cantidad Route leaks	Cantidad Bogons	Cantidad total
oct-23	0	0	0	0
nov-23	0	0	0	0
dic-23	0	0	0	0
ene-24	0	0	0	0
feb-24	0	0	0	0
mar-24	0	0	0	0
abr-24	0	0	0	0
may-24	0	0	0	0
jun-24	0	0	0	0
jul-24	0	0	0	0
ago-24	0	0	0	0
sep-24	0	0	0	0
oct-24	0	0	0	0
Total	0	0	0	0



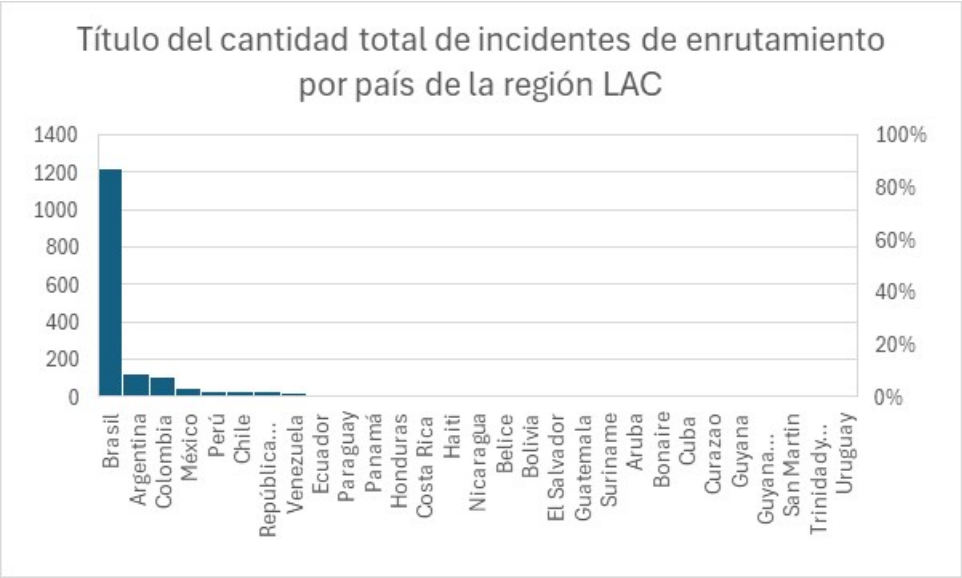
Venezuela

Fecha	Cantidad Hijacks	Cantidad Route leaks	Cantidad Bogons	Cantidad total
oct-23	2	2	0	4
nov-23	0	1	0	1
dic-23	0	0	0	0
ene-24	0	0	0	0
feb-24	0	0	0	0
mar-24	0	0	0	0
abr-24	0	0	0	0
may-24	2	0	0	2
jun-24	0	0	2	2
jul-24	1	0	2	3
ago-24	0	0	2	2
sep-24	4	0	0	4
oct-24	0	0	0	0
Total	9	3	6	18



Consolidado de incidentes de enrutamiento países LAC de Oct 2023 a Oct 2024

País	Cantidad Hijacks	Cantidad Route leaks	Cantidad Bogons	Cantidad total
Argentina	81	0	41	122
Aruba	0	0	0	0
Belice	1	0	0	1
Bolivia	1	0	0	1
Bonaire	0	0	0	0
Brasil	1037	0	183	1220
Chile	24	0	4	28
Colombia	50	0	53	103
Costa Rica	4	0	0	4
Cuba	0	0	0	0
Curazao	0	0	0	0
Ecuador	7	0	8	15
El Salvador	0	0	1	1
Guatemala	1	0	0	1
Guyana	0	0	0	0
Guyana Francesa	0	0	0	0
Haiti	3	0	0	3
Honduras	7	0	0	7
México	27	5	14	46
Nicaragua	2	0	0	2
Panamá	4	2	3	9
Paraguay	2	0	8	10
Perú	26	0	3	29
República Dominicana	21	0	6	27
San Martin	0	0	0	0
Suriname	1	0	0	1
Trinidad y Tobago	0	0	0	0
Uruguay	0	0	0	0
Venezuela	9	3	6	18


Título del cantidad total de incidentes de enrutamiento por país de la región LAC
1400
1200
1000
800
600
400
200
0
100%
80%
60%
40%
20%
0%
Brasil
Argentina
Colombia
México
Perú
Chile
República...
Venezuela
Ecuador
Paraguay
Panamá
Honduras
Costa Rica
Haití
Nicaragua
Belice
Bolivia
El Salvador
Guatemala
Suriname
Aruba
Bonaire
Cuba
Curazao
Guyana
Guyana...
San Martin
Trinidady...
Uruguay

Anexo 2

			Created Route Leaks				Created Hijacks				Bogons				
Country	Country Code	Active ASes	MANRS	Total Leaks	Uniq Leakers	Uniq Leakers Coverage, %	MANRS	Total Hijackers	Uniq Hijackers	Uniq Hijackers	MANRS	Total Prefix	Uniq ASes with Prefix	Total Path	Uniq ASes with Path Bogon
rgentina	AR	774	0	244951	70	9,04%	81	145055	367	47,42%	41	68758	5	73	6
ruba	AW	2	0	45	1	50,00%	0	4	2	100,00%	0	0	0	0	0
elize	BZ	16	0	1279	1	6,25%	1	176	8	50,00%	0	0	0	0	0
Bolivia (Plurinational State of)	BO	33	0	5306	3	9,09%	1	245	9	27,27%	0	0	0	43	1
Bonaire, Sint Eustatius and Saba	BQ	5	0	0	0	0,00%	0	37	1	20,00%	0	0	0	0	0
razil	BR	7593	0	15800389	1302	17,15%	1037	16565005	2064	27,18%	183	2313037	210	138525	74
hile	CL	201	0	848968	31	15,42%	24	5878	81	40,30%	4	0	0	1	1
olombia	CO	289	0	59012	33	11,42%	50	119855	121	41,87%	53	2559	2	992	14
osta Rica	CR	50	0	1746	7	14,00%	4	865	22	44,00%	0	0	0	0	0
uba	CU	3	0	0	0	0,00%	0	410	2	66,67%	0	0	0	0	0
uraçao	CW	10	0	0	0	0,00%	0	305	6	60,00%	0	0	0	0	0
ominican Republic (the)	DO	117	0	3055	7	5,98%	21	6163	35	29,91%	6	0	0	19	1
cuador	EC	173	0	46810	13	7,51%	7	20154	41	23,70%	8	0	0	38	1
l Salvador	SV	23	0	490	1	4,35%	0	342	9	39,13%	1	0	0	3	1
uatemala	GT	44	0	1692	8	18,18%	1	2090	22	50,00%	0	0	0	114	1
rench Guiana	GF	3	0	0	0	0,00%	0	0	0	0,00%	0	0	0	0	0
uyana	GY	3	0	0	0	0,00%	0	1001	2	66,67%	0	0	0	0	0
aiti	HT	6	0	0	0	0,00%	3	895	3	50,00%	0	0	0	0	0
onduras	HN	66	0	33583	4	6,06%	7	1325	25	37,88%	0	0	0	0	0
exico	MX	364	5	56674	33	9,07%	27	59117	222	60,99%	14	0	0	44	7
icaragua	NI	19	0	823	2	10,53%	2	311	9	47,37%	0	0	0	0	0
anama	PA	53	2	3442	10	18,87%	4	79026	20	37,74%	3	3953	1	11	1
araguay	PY	81	0	42400	8	9,88%	2	1478	23	28,40%	8	2	1	4	1
eru	PE	130	0	54753	19	14,62%	26	23183	75	57,69%	3	0	0	3	2
aint Martin (French part)	MF	2	0	0	0	0,00%	0	256	1	50,00%	0	0	0	0	0
uriname	SR	4	0	2	1	25,00%	1	958	4	100,00%	0	0	0	0	0
rinidad and Tobago	TT	12	0	511	2	16,67%	0	196	6	50,00%	0	0	0	0	0
ruguay	UY	18	0	1	1	5,56%	0	355	8	44,44%	0	0	0	0	0
Venezuela (Bolivarian Republic of)	VE	152	3	79469	20	13,16%	9	1379	52	34,21%	6	95	3	0	0