Análisis de eventos e incidentes de ruteo en Latinoamérica

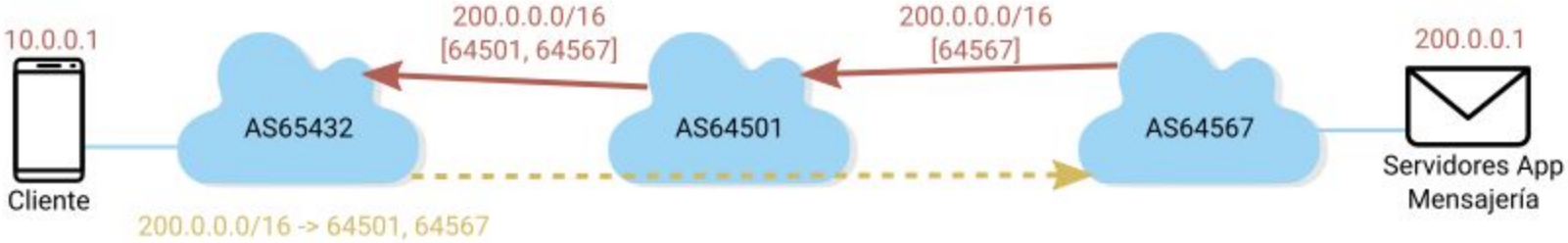
¿Qué son los incidentes de ruteo?

¿Qué son los incidentes de ruteo?

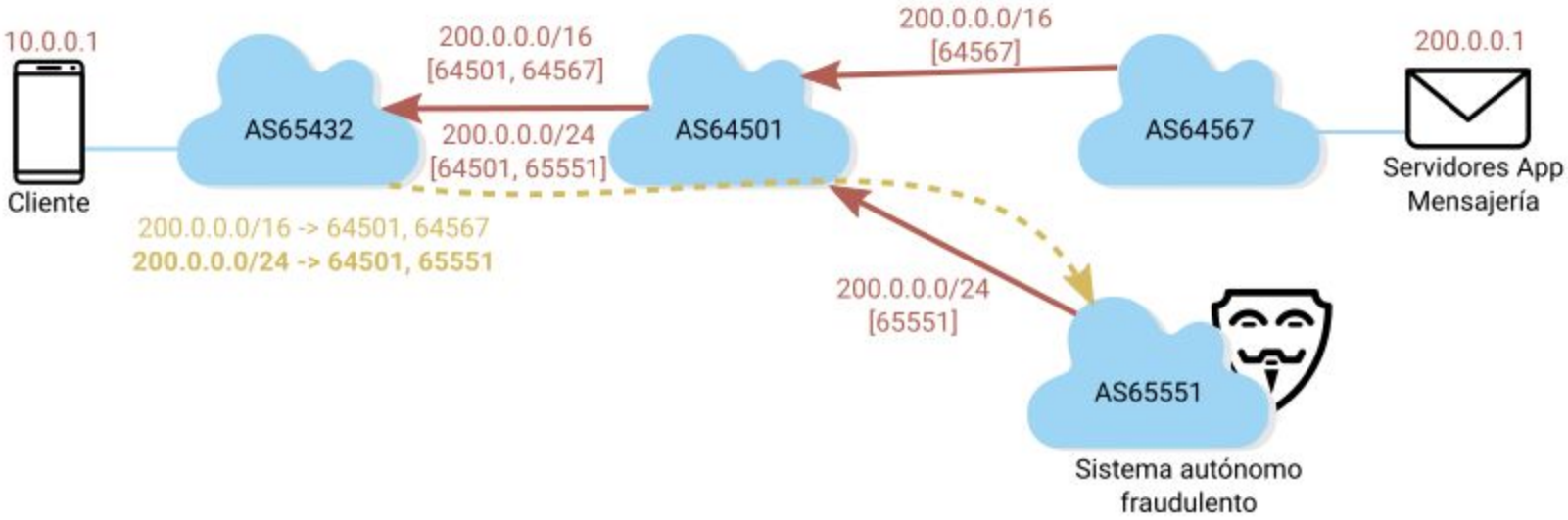
¿Qué son los incidentes de ruteo?

¿Qué son los incidentes de ruteo?

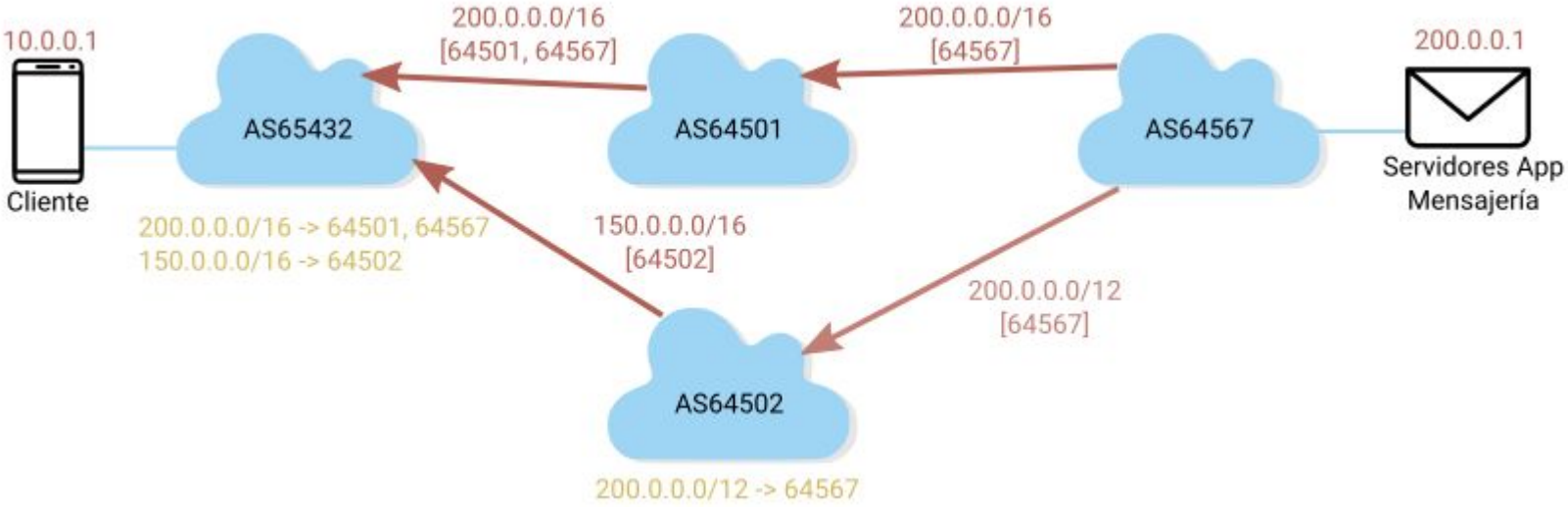
¿Qué son los incidentes de ruteo?



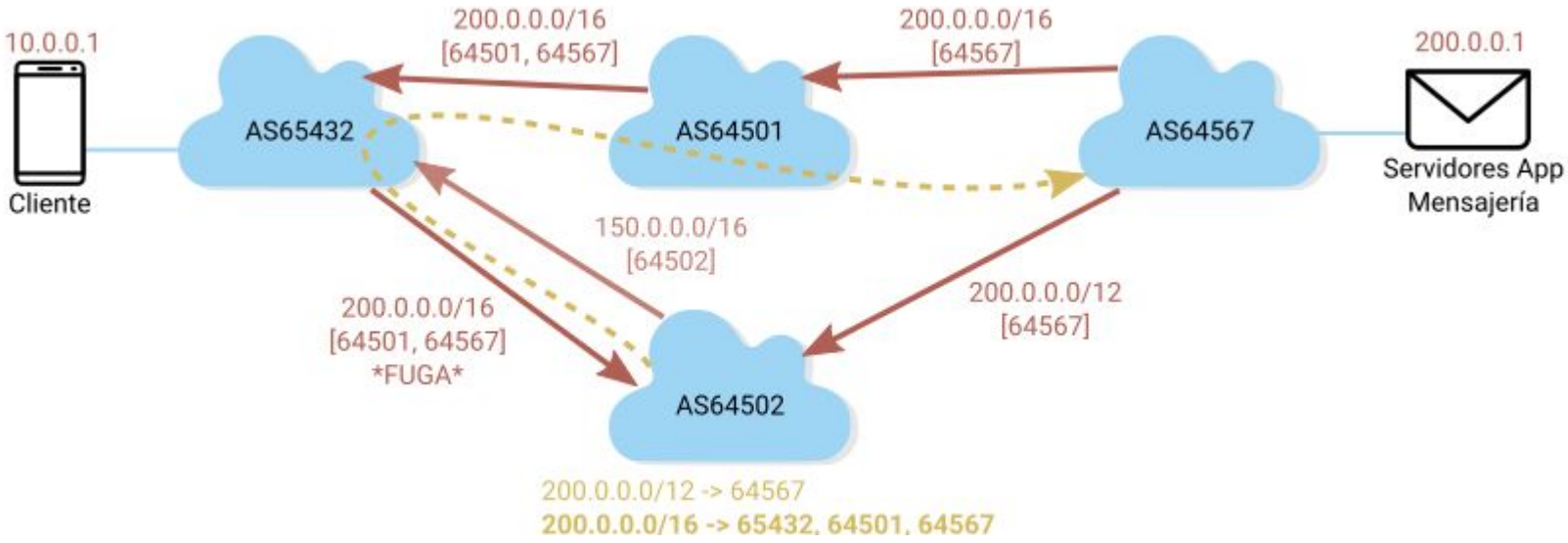
Secuestros de ruta (BGP hijacks)



Fugas de ruta (BGP leaks)



Fugas de ruta (BGP leaks)



BGP Leak (fuga de rutas)

"Propagación de un anuncio de ruteo que supera su alcance deseado" (RFC 7908)

- Suceden cuando un AS realiza un "mal anuncio".
- Pueden ocurrir por errores de configuración o ser intencionales.
- Ej: "multi-homed customer" se transforma en "transit provider"

BGP Hijack (secuestro de rutas)

AS anuncia un prefijo de forma fraudulenta (no lo posee pero logra "ofrecer" la mejor ruta):

- Anuncio de un prefijo más específico que el que anuncia el AS original.
- Anuncio de una ruta más corta, exista o no.

Esto provoca que los paquetes se desvíen por caminos incorrectos,

- Bloquear,
- Interceptar tráfico,
- Impersonar servicios.

¿Cómo me afectan estos incidentes?

¿Cómo me afecta un incidente BGP?

Flujo normal

Suplantación de identidad

Bloqueo

Desvío de tráfico

Incidentes que fueron noticia

FEB 2008

"Gobierno pakistaní intenta censurar YouTube y genera caos en todo internet"

NOV 2013

"Dyn Research presenta evidencia de tráfico de gobiernos, bancos e ISPs redirigido de forma fraudulenta"

SEP 2014

"Fuga BGP de VolumeDrive causa interrupciones de tráfico en EEUU y otros países lejanos"

MAR 2017

"Cortes en Cloudflare, Google y Banco Brazil provocados por BGP hijacks en Brasil"

ABR 2017

"Tráfico de MasterCard, Visa y otros desviado de forma fraudulenta a través de un ISP ruso"

AGO 2017

"BGP Leak accidental de Google transforma su AS en un proveedor de tránsito y causa interrupciones en todo internet, especialmente en Japón"

OCT 2017

"BGP leak en Brasil provoca desvío de tráfico hacia este país de múltiples CDNs, provocando contratiempos en servicios como Google y Twitter"

DIC 2017

"Tráfico de importantes servicios como Google, Apple, Facebook y Microsoft es desviado hacia un misterioso AS ruso que nunca antes había operado"

ABR 2018

"Rusos provocan un hijack a los prefijos de servidores DNS de Amazon y logran falsificar un sitio web de criptomonedas, robando así U$S 152.000"

JUN 2019

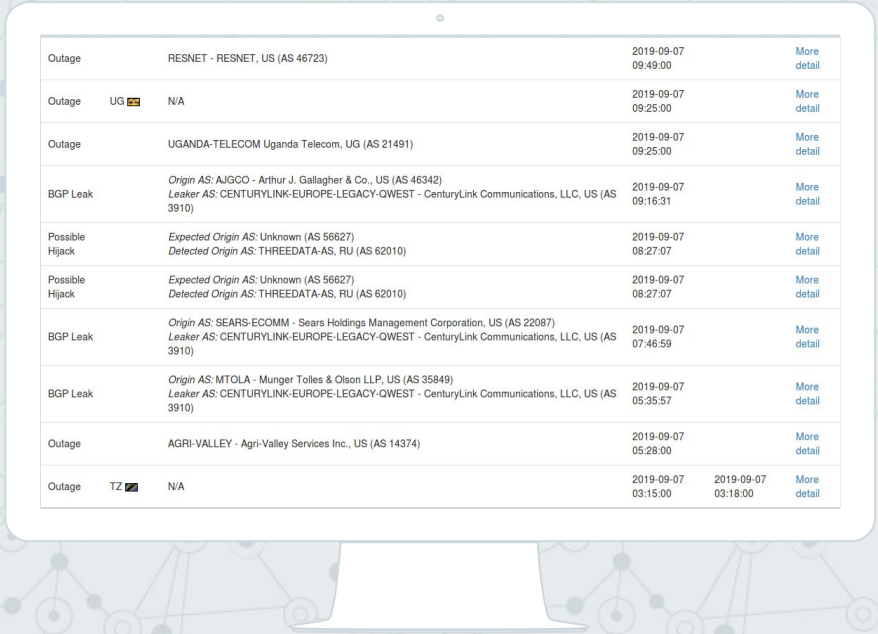
"Fuga de un pequeño ISP de Pensilvania no es filtrada por Verizon, provocando cortes en distintos servicios, como el CDN de Cloudflare"

Cantidad de incidentes BGP

Incidentes que son noticia

Incidentes “menores”

https://bgpstream.com

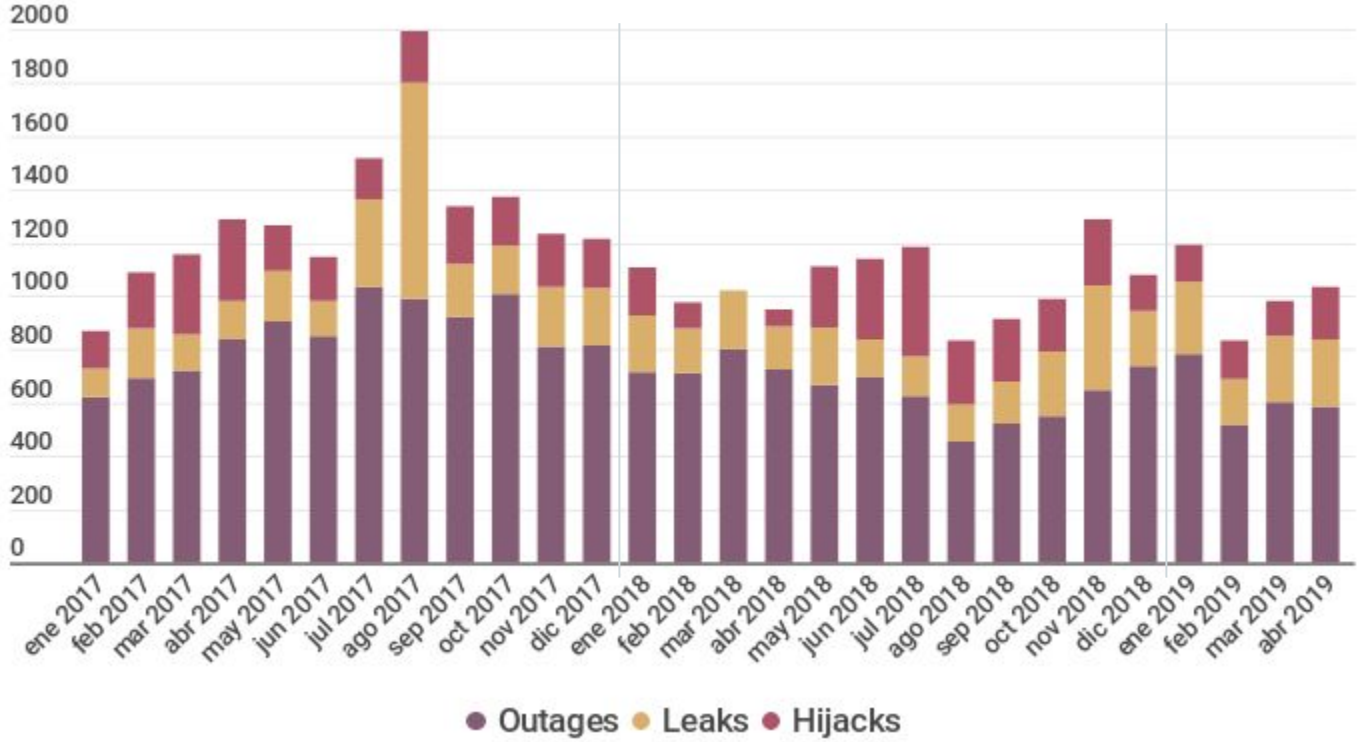


Outage		RESNET - RESNET, US (AS 46723)	2019-09-07 09:49:00		More detail
Outage	UG	N/A	2019-09-07 09:25:00		More detail
Outage		UGANDA-TELECOM Uganda Telecom, UG (AS 21491)	2019-09-07 09:25:00		More detail
BGP Leak		*Origin AS:* AJGCO - Arthur J. Gallagher & Co., US (AS 46342) *Leaker AS:* CENTURYLINK-EUROPE-LEGACY-QWEST - CenturyLink Communications, LLC, US (AS 3910)	2019-09-07 09:16:31		More detail
Possible Hijack		*Expected Origin AS:* Unknown (AS 56627) *Detected Origin AS:* THREEDATA-AS, RU (AS 62010)	2019-09-07 08:27:07		More detail
Possible Hijack		*Expected Origin AS:* Unknown (AS 56627) *Detected Origin AS:* THREEDATA-AS, RU (AS 62010)	2019-09-07 08:27:07		More detail
BGP Leak		*Origin AS:* SEARS-ECOMM - Sears Holdings Management Corporation, US (AS 22087) *Leaker AS:* CENTURYLINK-EUROPE-LEGACY-QWEST - CenturyLink Communications, LLC, US (AS 3910)	2019-09-07 07:46:59		More detail
BGP Leak		*Origin AS:* MTOLA - Munger Tolles & Olson LLP, US (AS 35849) *Leaker AS:* CENTURYLINK-EUROPE-LEGACY-QWEST - CenturyLink Communications, LLC, US (AS 3910)	2019-09-07 05:35:57		More detail
Outage		AGRI-VALLEY - Agri-Valley Services Inc., US (AS 14374)	2019-09-07 05:28:00		More detail
Outage	TZ	N/A	2019-09-07 03:15:00	2019-09-07 03:18:00	More detail

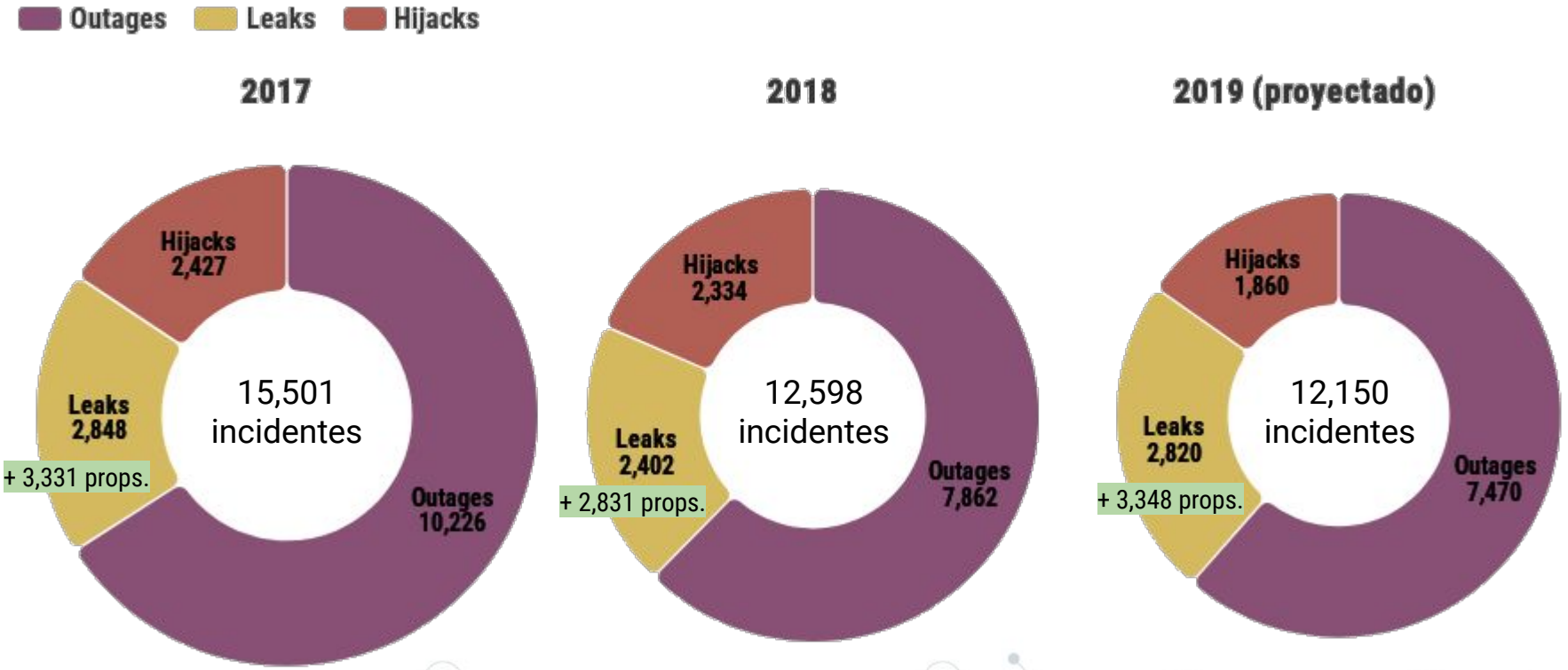
BGP Stream

leaks, hijacks, outages

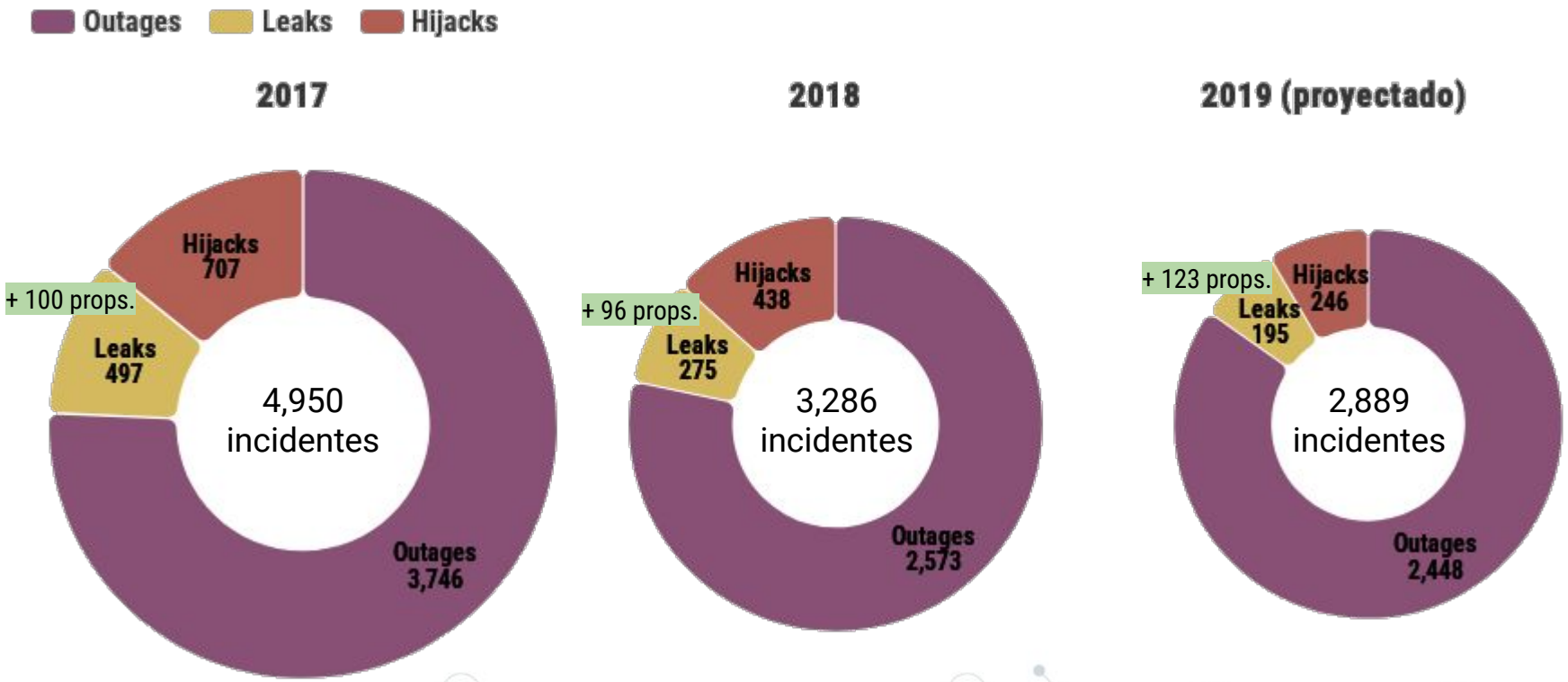
Cantidad de incidentes a nivel mundial



Cantidad de incidentes a nivel mundial



Cantidad de incidentes en LAC

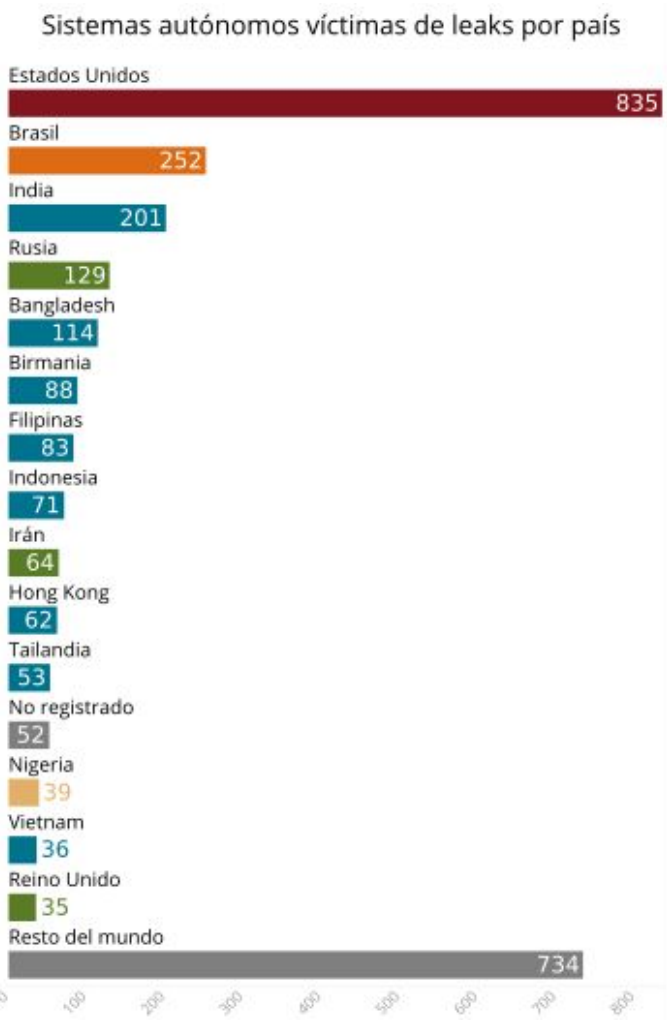


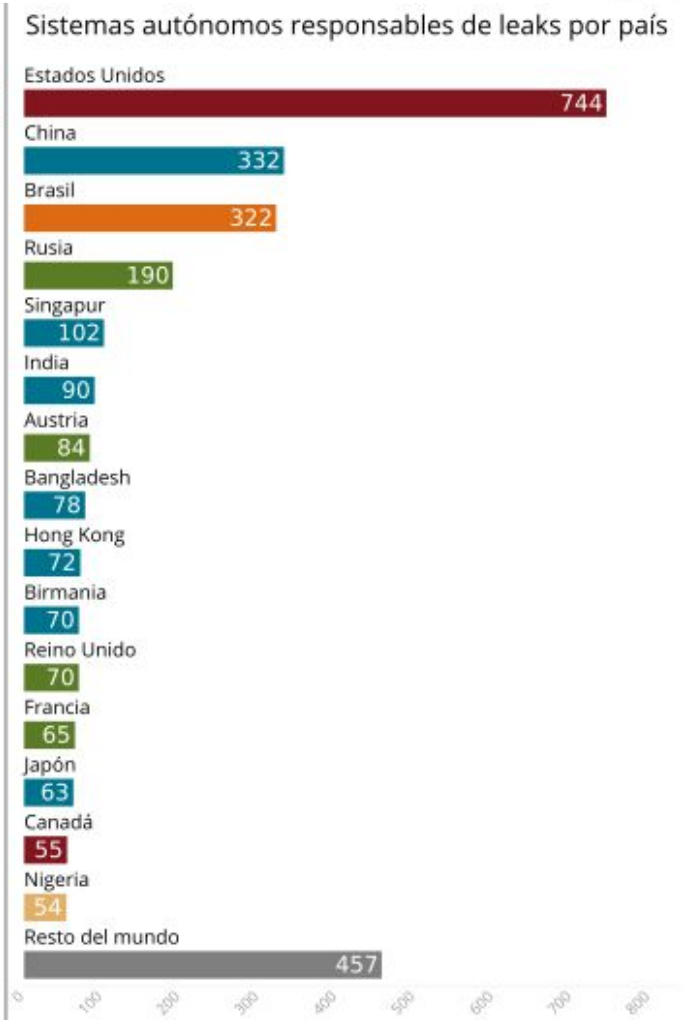
Reflexiones iniciales

- ¿Estos incidentes de ruteo están siendo cada vez más frecuentes?
- ¿Estamos mejorando o empeorando en cuanto a la seguridad del ruteo?
- ¿Todos los países son afectados por igual?

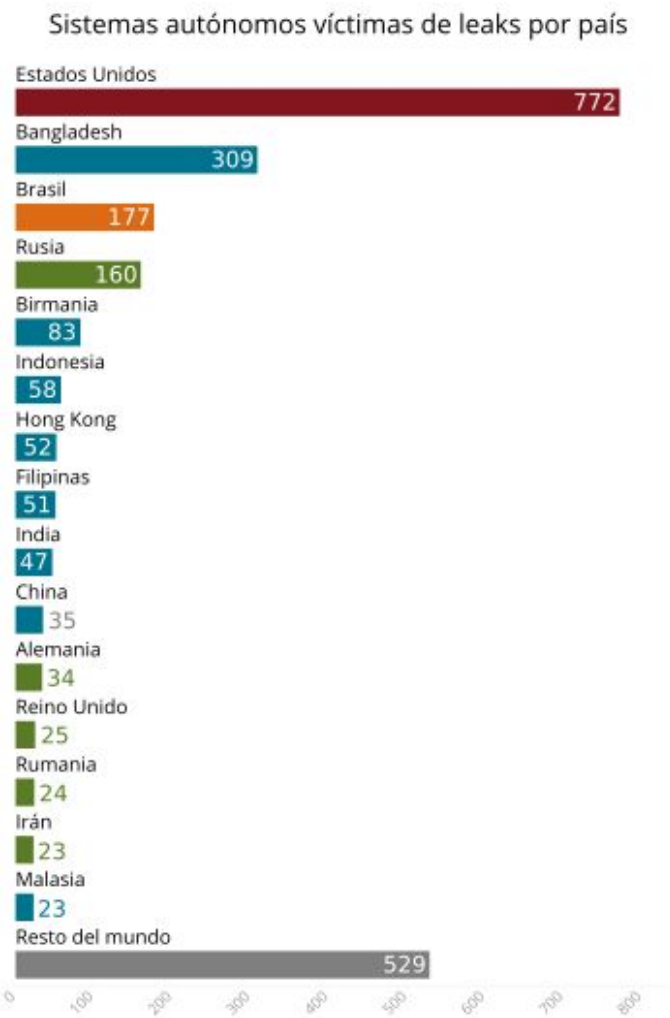
BGP Leaks

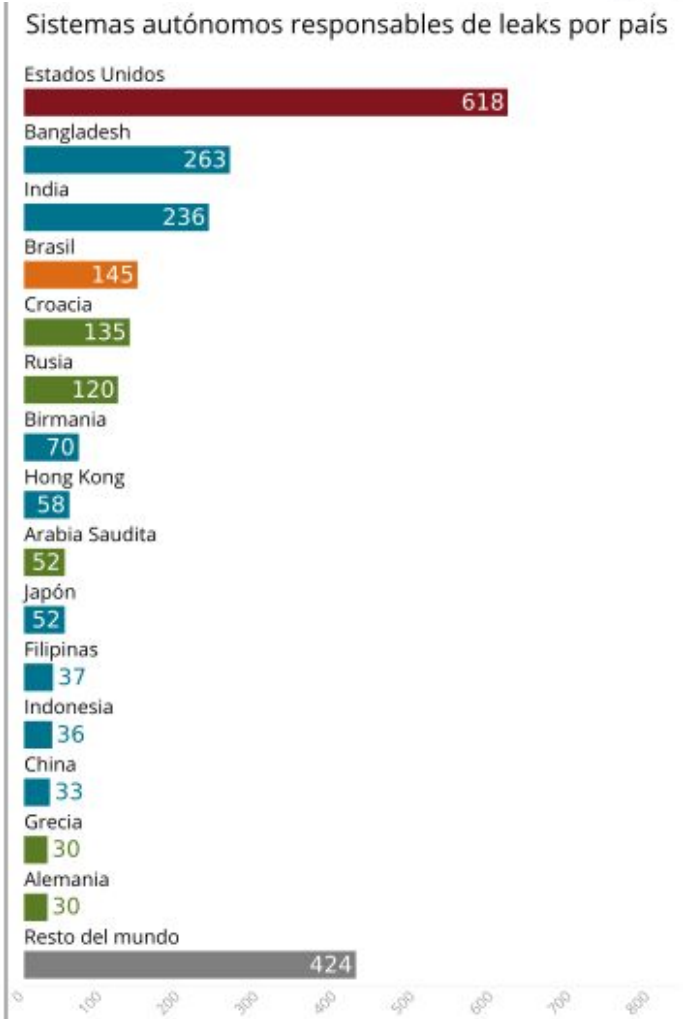
en el mundo


Sistemas autónomos víctimas de leaks por país
Estados Unidos
835
Brasil
252
India
201
Rusia
129
Bangladesh
114
Birmania
88
Filipinas
83
Indonesia
71
Irán
64
Hong Kong
62
Tailandia
53
No registrado
52
Nigeria
39
Vietnam
36
Reino Unido
35
Resto del mundo
734
0
100
200
300
400
500
600
700
800


Sistemas autónomos responsables de leaks por país
Estados Unidos
744
China
332
Brasil
322
Rusia
190
Singapur
102
India
90
Austria
84
Bangladesh
78
Hong Kong
72
Birmania
70
Reino Unido
70
Francia
65
Japón
63
Canadá
55
Nigeria
54
Resto del mundo
457
0
100
200
300
400
500
600
700
800

2017


Sistemas autónomos víctimas de leaks por país
Estados Unidos
772
Bangladesh
309
Brasil
177
Rusia
160
Birmania
83
Indonesia
58
Hong Kong
52
Filipinas
51
India
47
China
35
Alemania
34
Reino Unido
25
Rumania
24
Irán
23
Malasia
23
Resto del mundo
529
0
100
200
300
400
500
600
700
800

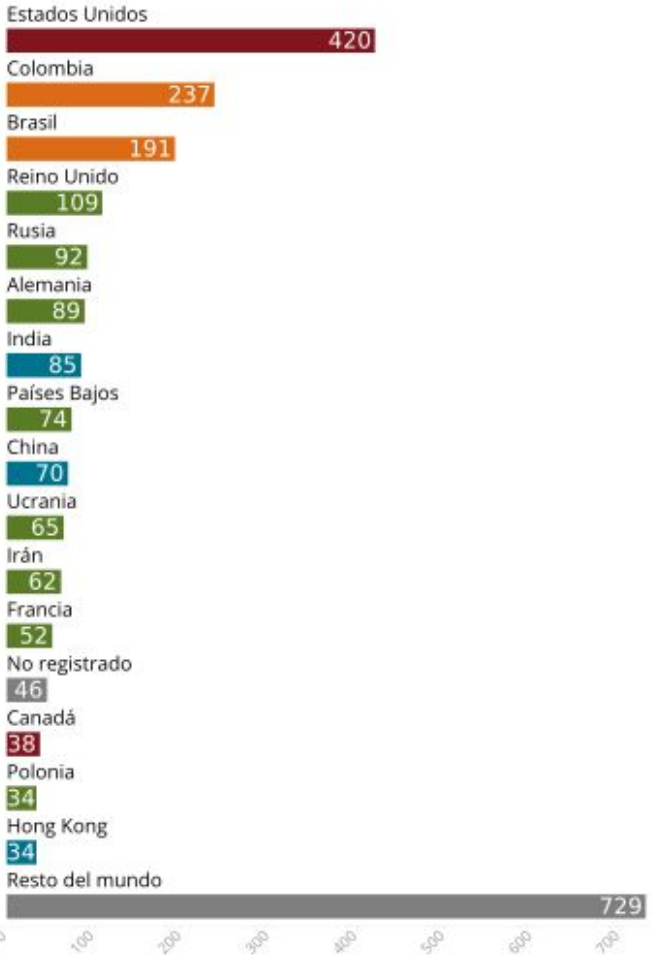

Sistemas autónomos responsables de leaks por país
Estados Unidos
618
Bangladesh
263
India
236
Brasil
145
Croacia
135
Rusia
120
Birmania
70
Hong Kong
58
Arabia Saudita
52
Japón
52
Filipinas
37
Indonesia
36
China
33
Grecia
30
Alemania
30
Resto del mundo
424
0
100
200
300
400
500
600
700
800

2018

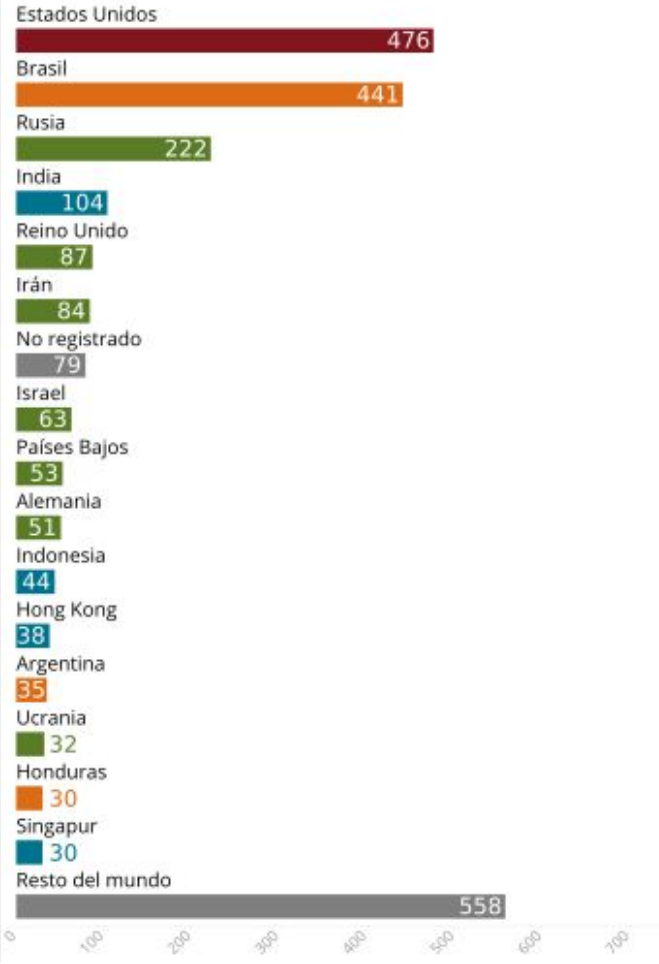
BGP Hijacks

en el mundo

Sistemas autónomos víctimas de hijacks por país

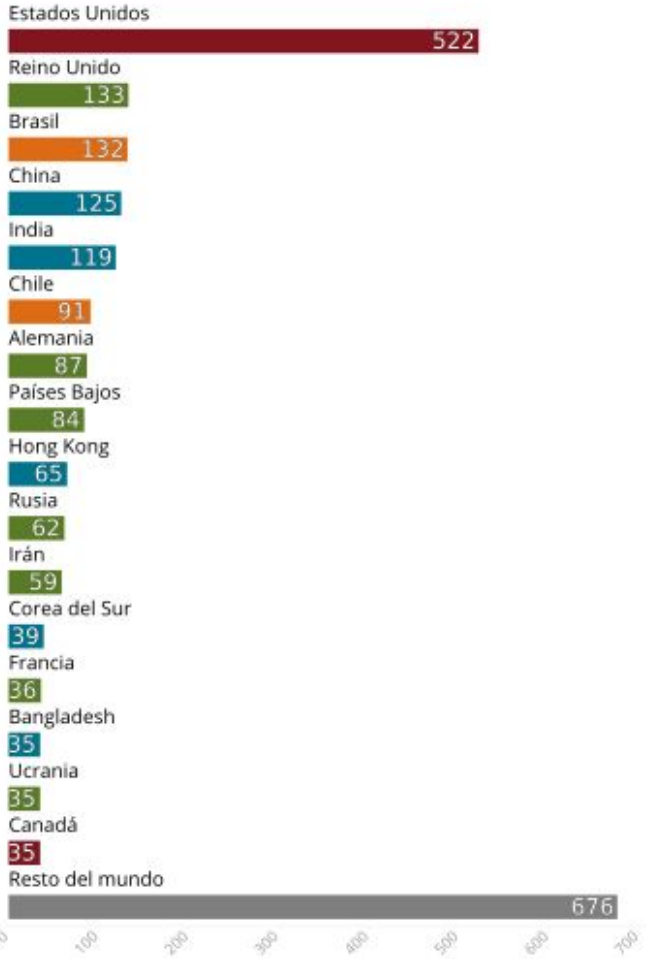


Sistemas autónomos responsables de hijacks por país

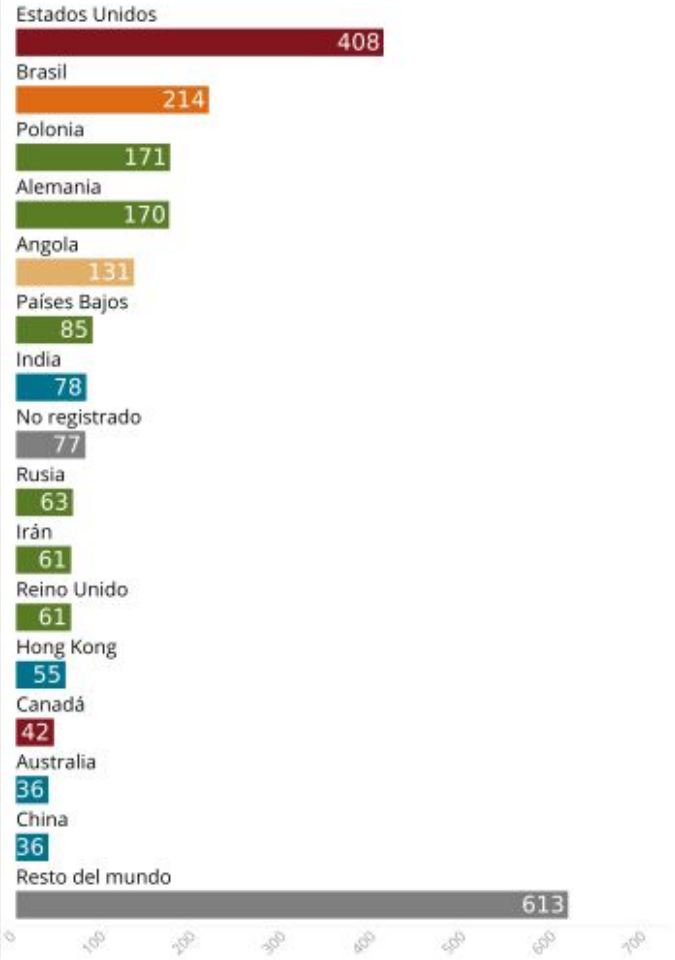


2017

Sistemas autónomos víctimas de hijacks por país



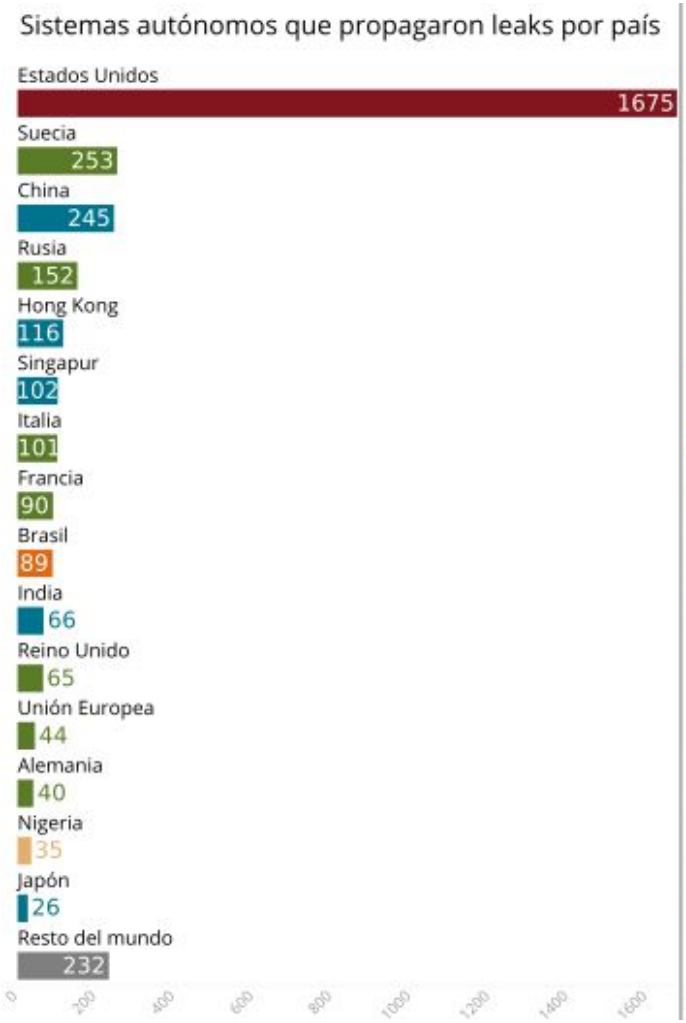
Sistemas autónomos responsables de hijacks por país

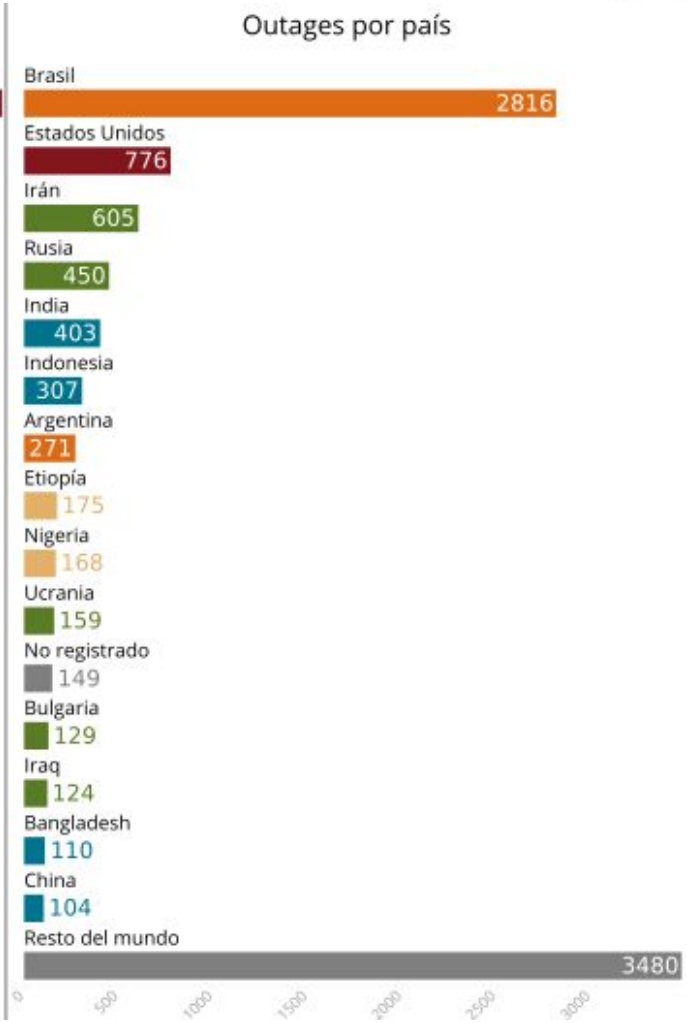


2018

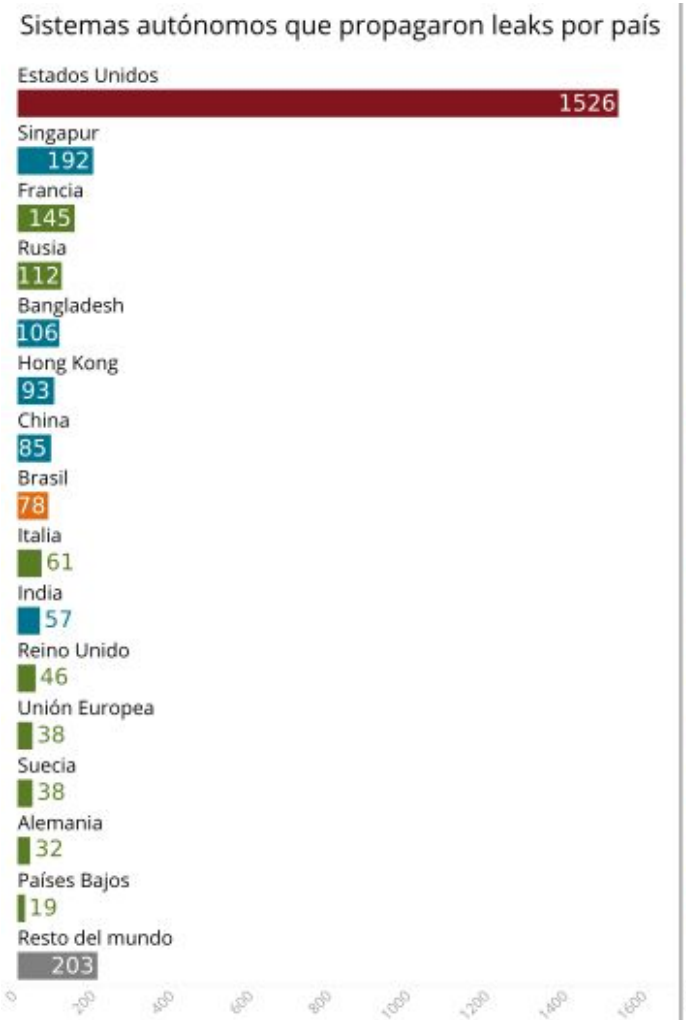
BGP Outages

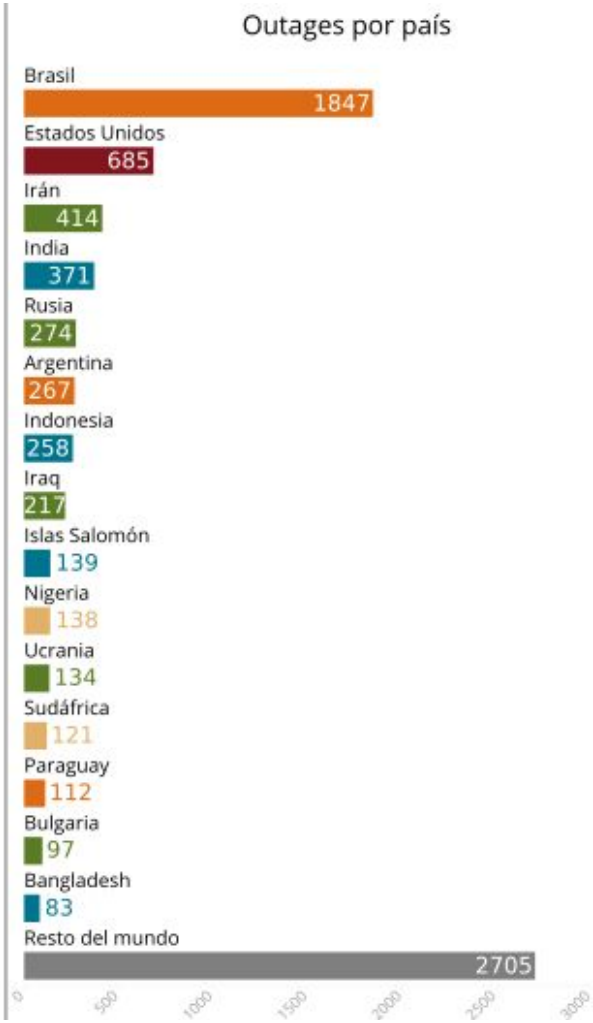
y propagación de leaks
en el mundo


Sistemas autónomos que propagaron leaks por país
Estados Unidos
1675
Suecia
253
China
245
Rusia
152
Hong Kong
116
Singapur
102
Italia
101
Francia
90
Brasil
89
India
66
Reino Unido
65
Unión Europea
44
Alemania
40
Nigeria
35
Japón
26
Resto del mundo
232
0
200
400
600
800
1000
1200
1400
1600


Outages por país
Brasil
2816
Estados Unidos
776
Irán
605
Rusia
450
India
403
Indonesia
307
Argentina
271
Etiopía
175
Nigeria
168
Ucrania
159
No registrado
149
Bulgaria
129
Iraq
124
Bangladesh
110
China
104
Resto del mundo
3480
0
500
1000
1500
2000
2500
3000

2017


Sistemas autónomos que propagaron leaks por país
Estados Unidos
1526
Singapur
192
Francia
145
Rusia
112
Bangladesh
106
Hong Kong
93
China
85
Brasil
78
Italia
61
India
57
Reino Unido
46
Unión Europea
38
Suecia
38
Alemania
32
Países Bajos
19
Resto del mundo
203
0
200
400
600
800
1000
1200
1400
1600

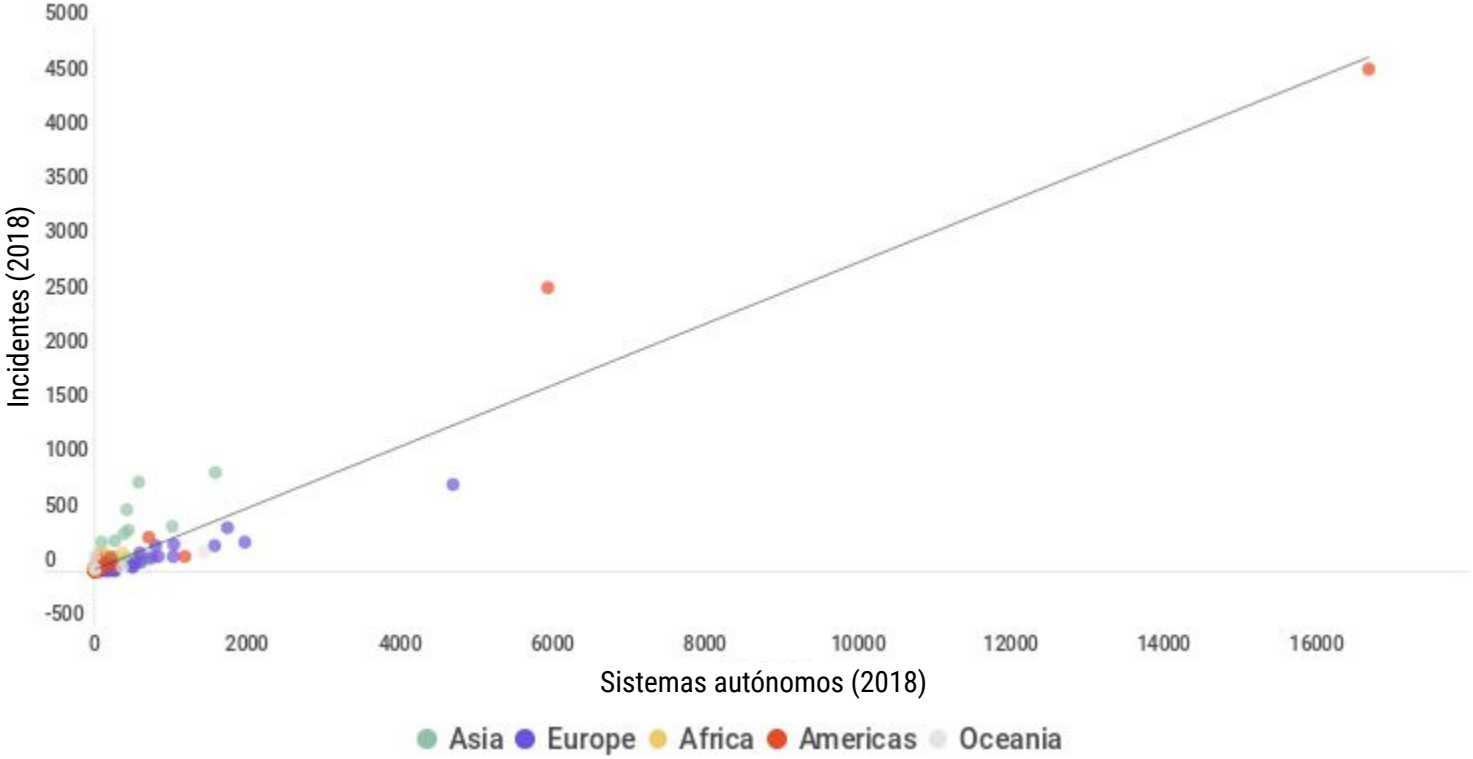

Outages por país
Brasil
1847
Estados Unidos
685
Irán
414
India
371
Rusia
274
Argentina
267
Indonesia
258
Iraq
217
Islas Salomón
139
Nigeria
138
Ucrania
134
Sudáfrica
121
Paraguay
112
Bulgaria
97
Bangladesh
83
Resto del mundo
2705
0
500
1000
1500
2000
2500
3000

2018

¿En qué país ocurren más incidentes?

¿Cómo estandarizar los resultados para poder comparar?

Correlación Incidentes vs ASNs (0.95)



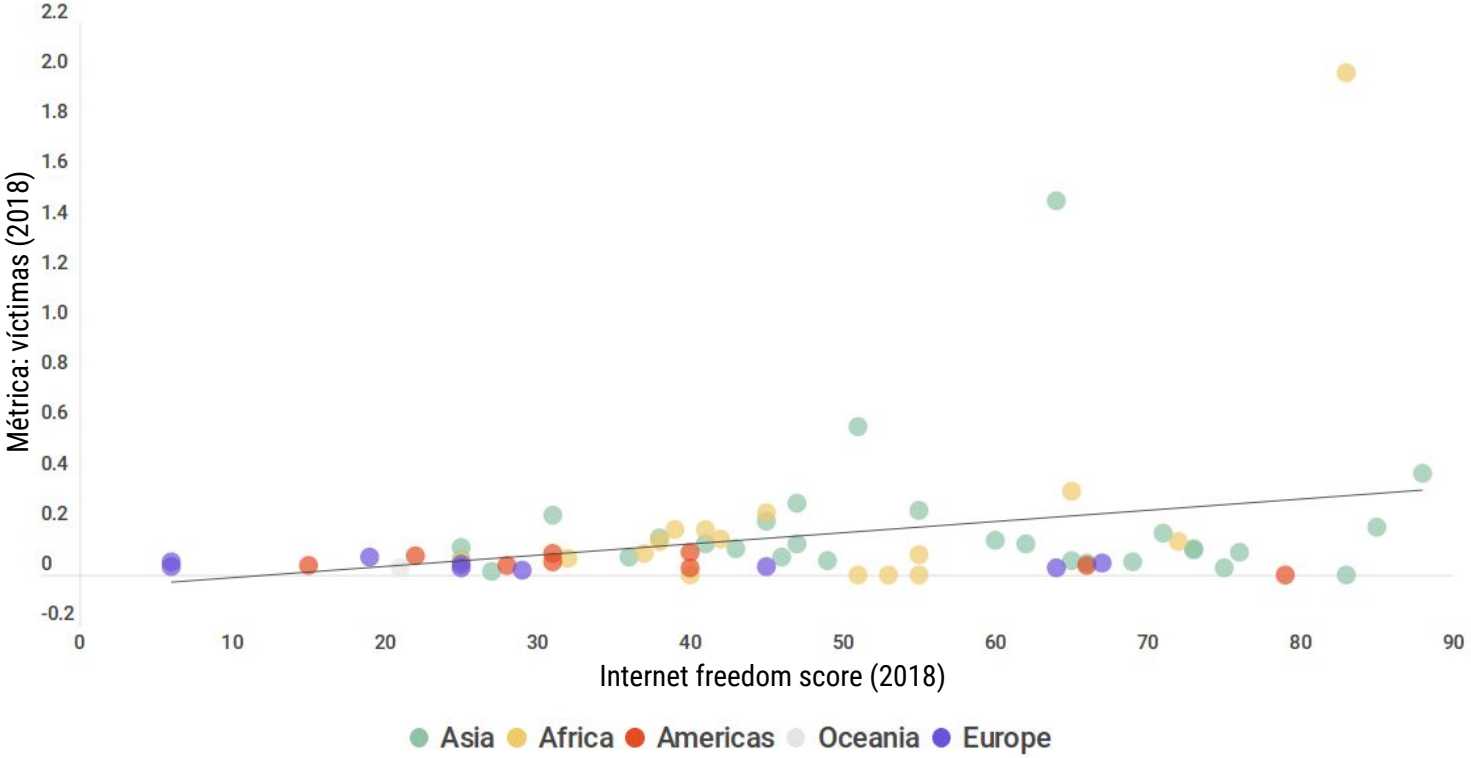
outages leaks hijacks

$$\frac{\text{Sumatoria de eventos}}{\text{Cantidad ASNs activos}}$$

Métrica

vs. otros indicadores

Correlación Incidentes vs Libertad en internet (0.29)



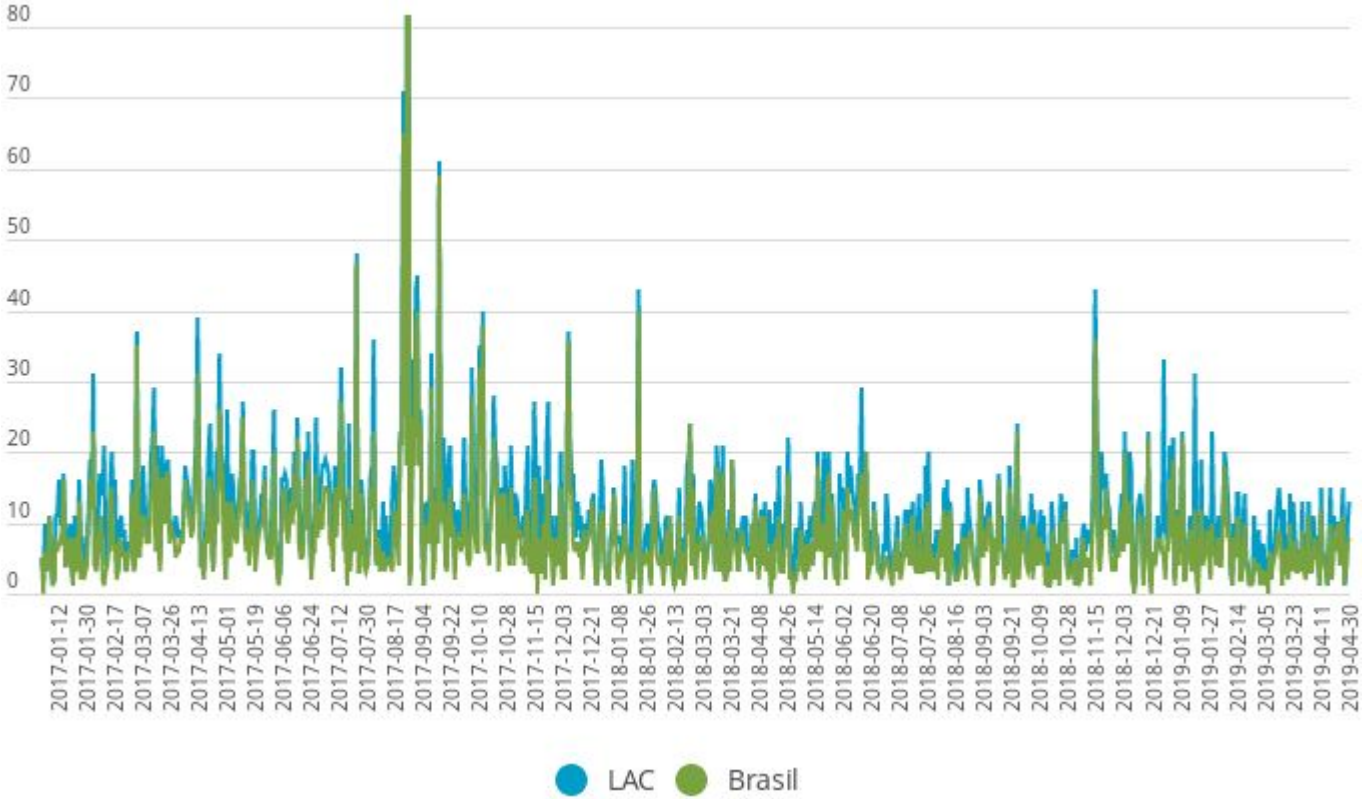
Datos en nuestra región

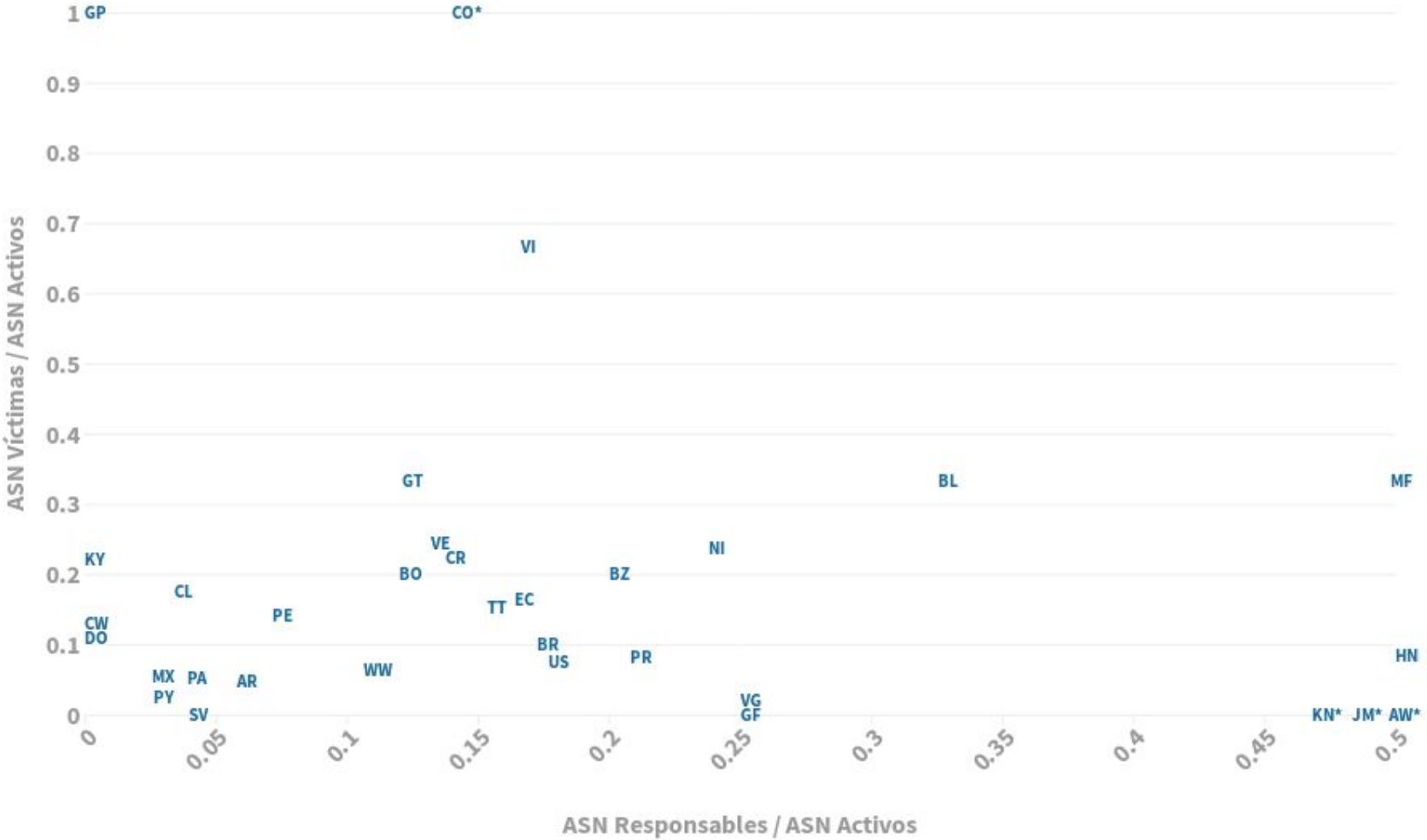
Latinoamérica y el Caribe

Cantidad de incidentes en LAC

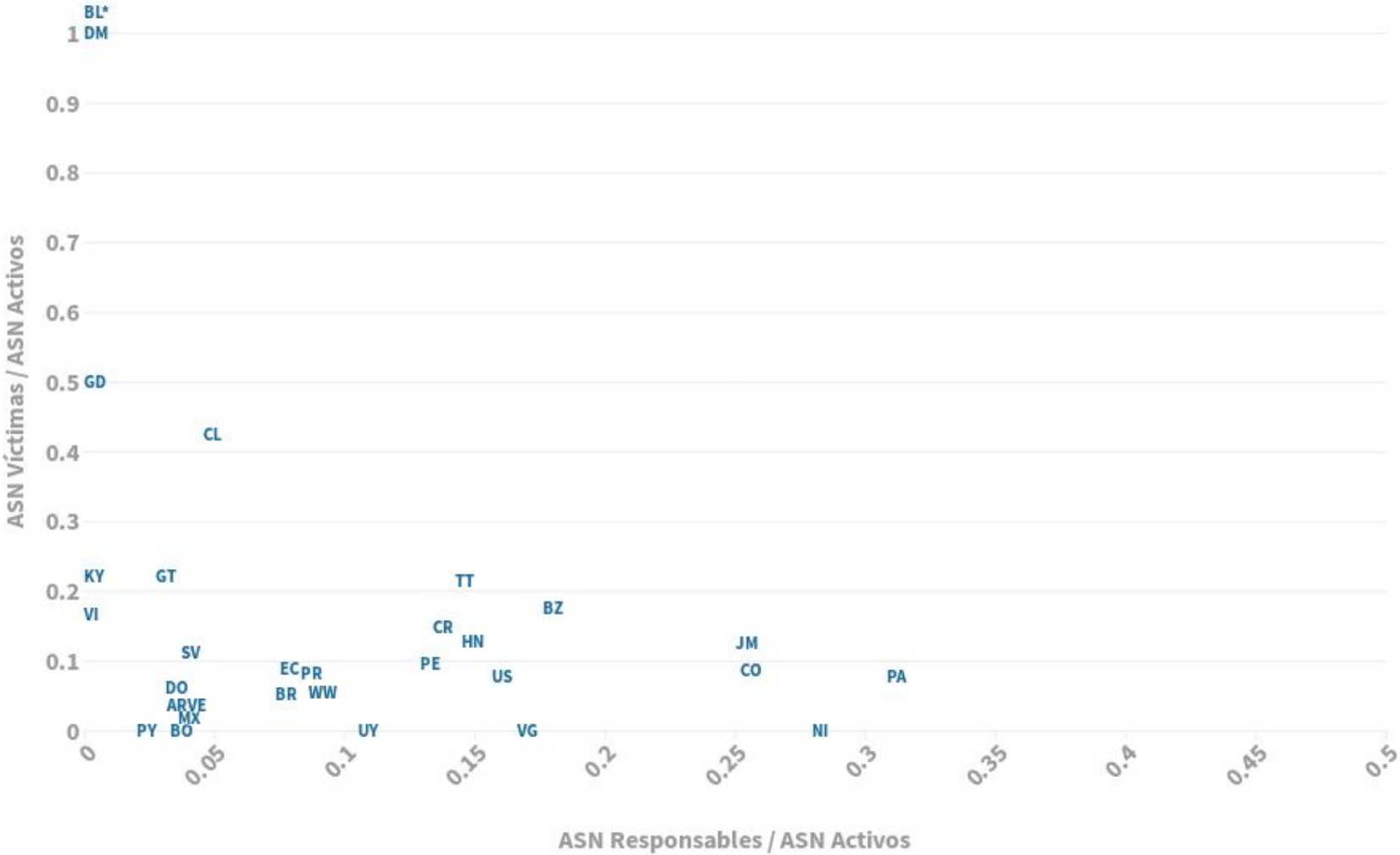
	Leaks (r) 2017/2018	Leaks (v) 2017/2018	Leaks (p) 2017/2018	Hijacks (r) 2017/2018	Hijacks (v) 2017/2018
🇧🇷 Brasil (BR)	**322** **145**	**252** **177**	**89** **78**	**441** **214**	**191** **132**
🇨🇴 Colombia (CO)	**0** **17**	**2** **3**	**7** **0**	**9** **15**	**237** **8**
🇨🇱 Chile (CL)	**1** **0**	**1** **2**	**1** **0**	**4** **10**	**30** **91**
🇦🇷 Argentina (AR)	**0** **1**	**11** **8**	**0** **1**	**35** **21**	**18** **18**
🇵🇦 Panamá (PA)	**0** **2**	**2** **3**	**0** **14**	**3** **8**	**2** **3**
Resto de LAC	**26** **10**	**51** **25**	**3** **3**	**79** **52**	**53** **49**

Cantidad de incidentes LAC vs Brasil




ASN Víctimas / ASN Activos
ASN Responsables / ASN Activos
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
0
0.05
0.1
0.15
0.2
0.25
0.3
0.35
0.4
0.45
0.5
GP
CO*
VI
GT
BL
MF
KY
VE
CR
NI
BO
BZ
CL
TT
EC
PE
CW
DO
BR
US
PR
HN
MX
PA
AR
WW
PY
SV
VG
GF
KN*
JM*
AW*

2017


BL*
DM
GD
CL
KY
GT
VI
SV
DO
ARVE
MX
PY
BO
EC
PR
BR
WW
UY
TT
BZ
CR
HN
PE
US
VG
JM
CO
PA
NI
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
0.05
0.15
0.25
0.35
0.45
ASN Víctimas / ASN Activos
ASN Responsables / ASN Activos

2018

¿Cómo pueden reducirse estos incidentes?

¿Cómo reducir los incidentes de ruteo?

🌎 https://fortproject.net

Powered by NIC MÉXICO and lacnic

- Validador de Infraestructura de clave pública para recursos de numeración de Internet (RPKI).
- Herramienta de monitoreo para estudiar incidentes de enrutamiento en la región.
- Campaña de despliegue de RPKI en América Latina y el Caribe.

Conclusiones

- Distorsiones en la región por la magnitud de Brasil.
- Mejora sustancial de reducción de incidentes en el año 2018.
- Fuerte correlación entre cantidad de ASN por país y cantidad de incidentes ocurridos.
- Una infraestructura de ruteo vulnerable puede afectar la libertad de internet.

¡Gracias!

¿Preguntas?

Augusto Mathurin - @augusthur

carolina@lacnic.net

guillermo@lacnic.net

🎁 https://bit.ly/2oMx98p

FORT

Tecnologías de Ruteo para una Internet Libre y Abierta