Panorámica sobre el secuestro de redes IPv{4|6}

online meeting
lacnic 34
lacnog 2020

Alejandro Acosta
alejandro @\ lacnic.net
@ITandNetworking

Panorámica sobre el secuestro de redes IP

Terminología

Secuestro de red o Hijack

Es el apoderamiento ilegítimo de una red IP manipulando las tablas BGP

Terminología

Secuestro de red o Hijack

Es el apoderamiento ilegítimo de una red IP manipulando las tablas BGP

Evento

Para este documento, “evento” corresponde a cualquier actividad en torno al secuestro de redes (pe, secuestrar / ser secuestrado)

Terminología

Secuestro de red o Hijack

Es el apoderamiento ilegítimo de una red IP manipulando las tablas BGP

Evento

Para este documento, “evento” corresponde a cualquier actividad en torno al secuestro de redes (pe, secuestrar / ser secuestrado)

Secuestrador

El actor que realiza el secuestro de una red.

Terminología

Secuestro de red o Hijack

Es el apoderamiento ilegítimo de una red IP manipulando las tablas BGP

Evento

Para este documento, “evento” corresponde a cualquier actividad en torno al secuestro de redes (pe, secuestrar / ser secuestrado)

Secuestrador

El actor que realiza el secuestro de una red.

Secuestrado

Es la organización dueña de los recursos que son víctima del secuestro.

Origen de los datos

Twitter: @bgpstream

Origen de los datos

Twitter: @bgpstream

Todos los tweets desde el 1 de Enero de 2016 al 31 de Mayo de 2020 de la cuenta twitter @bgpstream siendo un total de 45.000 (todos los eventos)

Origen de los datos

Twitter: @bgpstream

Todos los tweets desde el 1 de Enero de 2016 al 31 de Mayo de 2020 de la cuenta twitter @bgpstream siendo un total de 45.000 (todos los eventos)

{"usernameTweet": "bgpstream", "url": "/bgpstream/status/1041905881250758656", "datetime": "2018-09-18 00:24:54", "nbr_reply": 0, "is
_reply": false, "ID": "1041905881250758656", "text": "BGP,HJ,hijacked prefix AS3356
189.125.240.0/23, Level 3 Parent, LLC,-,By AS2660
69 Banco BMG S.A., http:// bgpstream.com/event/151944 ", "user_id": "3237083798",
"nbr_retweet": 0, "nbr_favorite": 0, "is_retweet":
 false}

Origen de los datos

Twitter: @bgpstream

Todos los tweets desde el 1 de Enero de 2016 al 31 de Mayo de 2020 de la cuenta twitter @bgpstream siendo un total de 45.000 (todos los eventos)

{"usernameTweet": "bgpstream", "url": "/bgpstream/status/1041905881250758656", "datetime": "2018-09-18 00:24:54", "nbr_reply": 0, "is_reply": false, "ID": "1041905881250758656", "text": "BGP,HJ,hijacked prefix AS3356 189.125.240.0/23, Level 3 Parent, LLC,-,By AS2660 69 Banco BMG S.A., http:// bgpstream.com/event/151944 ", "user_id": "3237083798", "nbr_retweet": 0, "nbr_favorite": 0, "is_retweet": false}

HJ = La info contentiva de este tweet que corresponde a un Hijack, un secuestro de red (estos son los tipos de tweets que precisamos)
AS3356 = AS Origen del prefijo de la red
SE = Código del país correspondiente al prefijo de la red

189.125.240.0/23 = Prefijo de red secuestrado
AS2660 = AS del secuestrador
http://bgpstream.com/event/151944 = URL para obtener más detalles

Procesamiento de los datos

TweetScraper
https://github.com/jonbakerfish/TweetScraper

Python3
https://www.python.org/

Adicionalmente se utilizó el **API de RIPE NCC** para geolocalización de varios

Resultados

Resultados

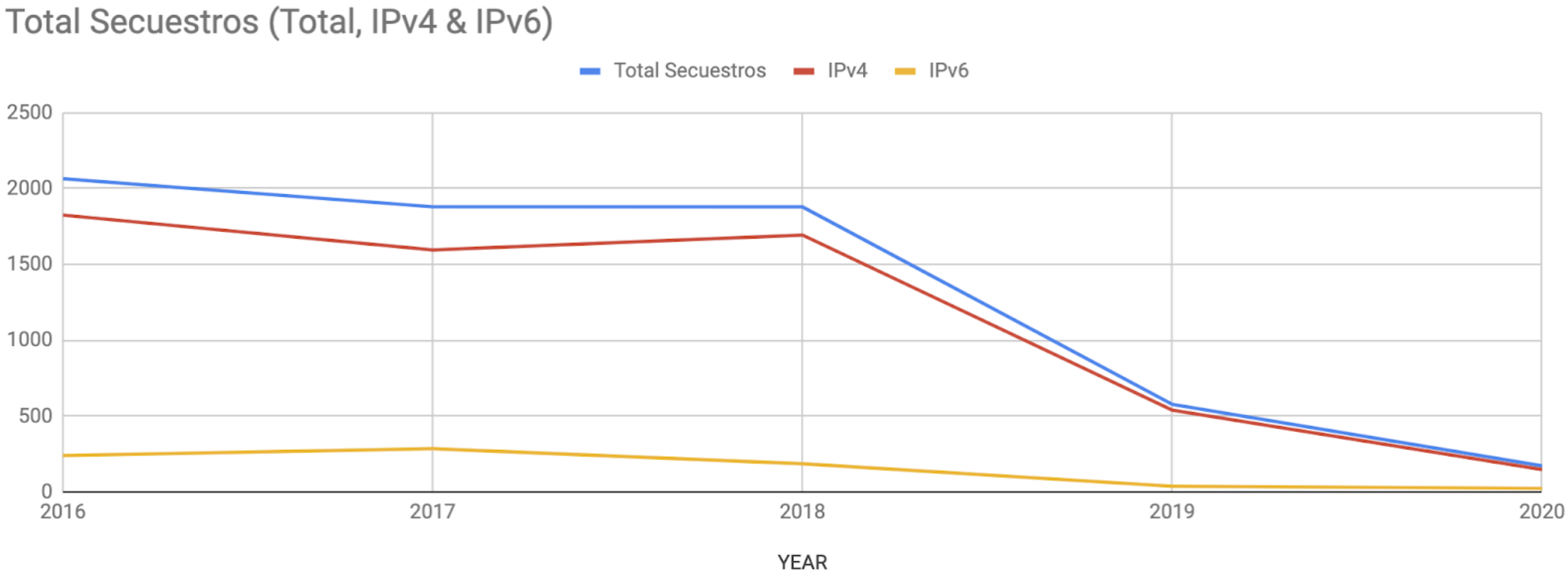
Cantidad de secuestros por año

Año	Total Secuestros	IPv4	IPv6
2016	2065	1825	240
2017	1880	1595	285
2018	1879	1693	186
2019	577	539	38
2020	172	148	24
	6573	5800	773

Recordemos que 2020 es hasta el mes de Mayo

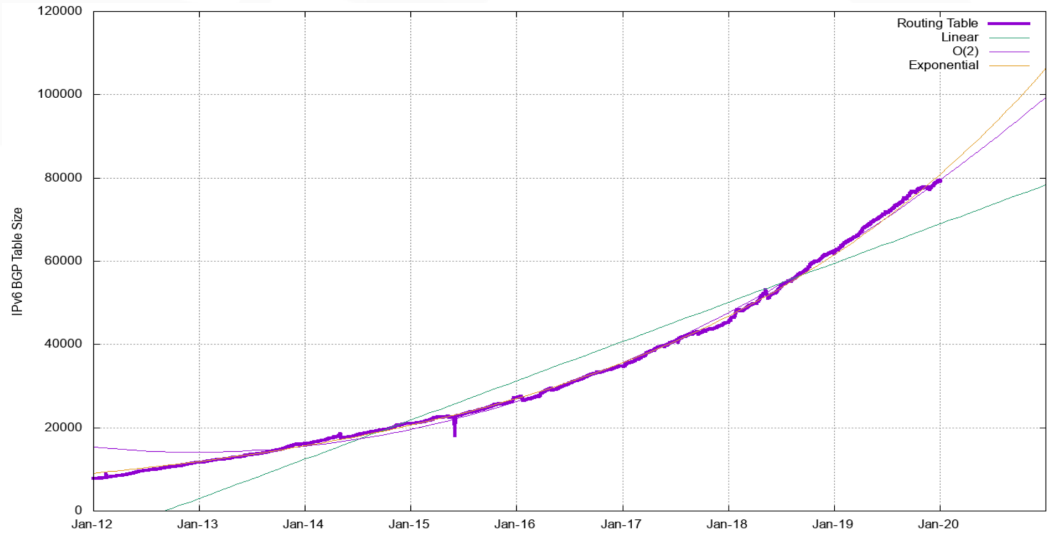
Resultados

Cantidad de secuestros por año x protocolo



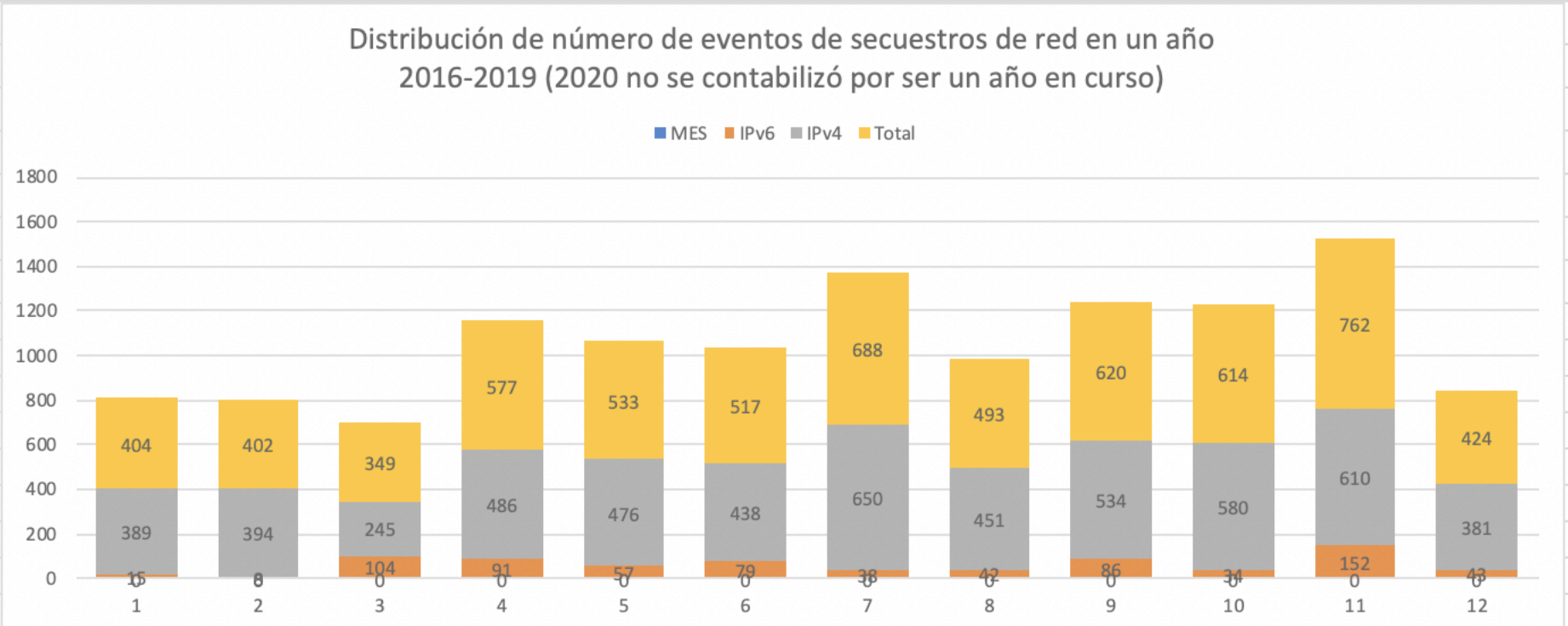
Resultados

Cantidad de secuestros po



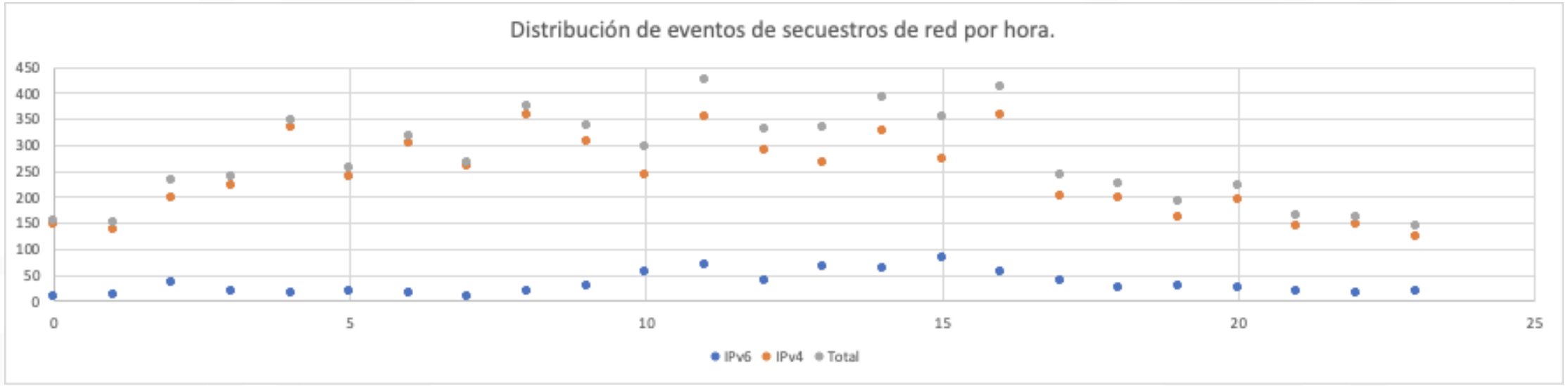
Resultados

Distribución de eventos de red por año



Resultados

Cantidad de secuestros por año x protocolo



* Según la hora reportada por **TweetScraper**

Resultados

RIR que más secuestros recibe *

	RIPE	APNIC	LACNIC	ARIN	AFRINIC
Friday	393	307	115	328	24
Monday	411	284	81	280	16
Saturday	264	130	46	140	16
Sunday	140	90	31	77	3
Thursday	**517**	280	127	372	21
Tuesday	411	183	66	282	27
Wednesday	375	240	131	284	53

* según Sistema Autónomo del secuestrado

Resultados

RIR que más secuestros realiza *

	RIPE	APNIC	LACNIC	ARIN	AFRINIC
Friday	416	213	150	341	24
Monday	362	194	168	326	14
Saturday	220	123	49	167	24
Sunday	121	87	36	86	6
Thursday	**462**	183	200	349	108
Tuesday	388	181	117	257	12
Wednesday	333	159	152	387	32

* según Sistema Autónomo del secuestrador

Resultados

Día de la semana con menos secuestros por RIR

AFRINIC	Sunday
LACNIC	Sunday
APNIC	Sunday
ARIN	Sunday
RIPE	Sunday

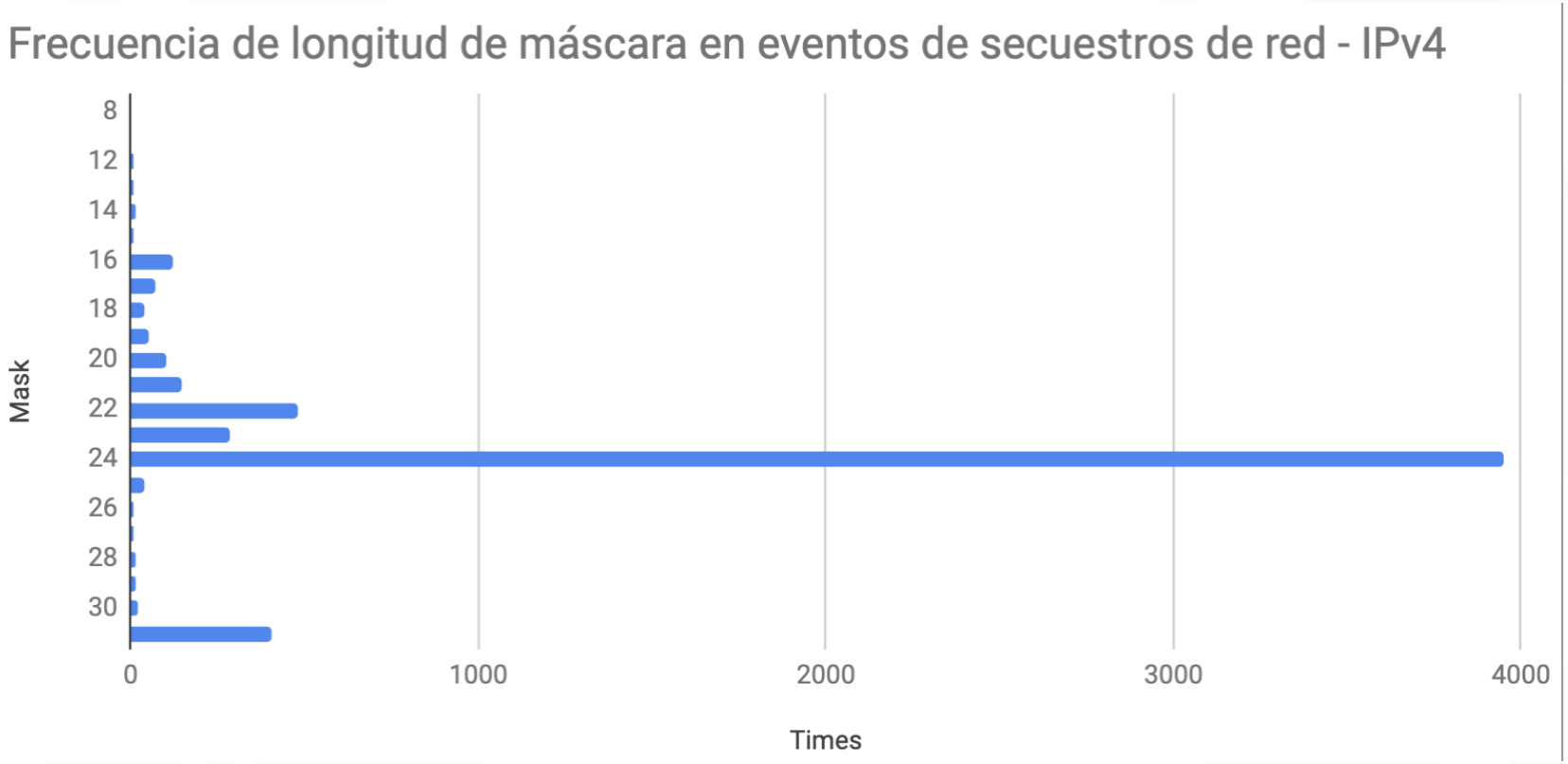
Resultados

Tabla de frecuencia. TOP Prefijos

5.5.5.0/24	5
103.15.168.0/24	7
185.58.128.0/24	7
187.16.216.0/21	7
2.2.2.0/24	7
2001:bf7:170::/44	8
80.249.208.0/21	18

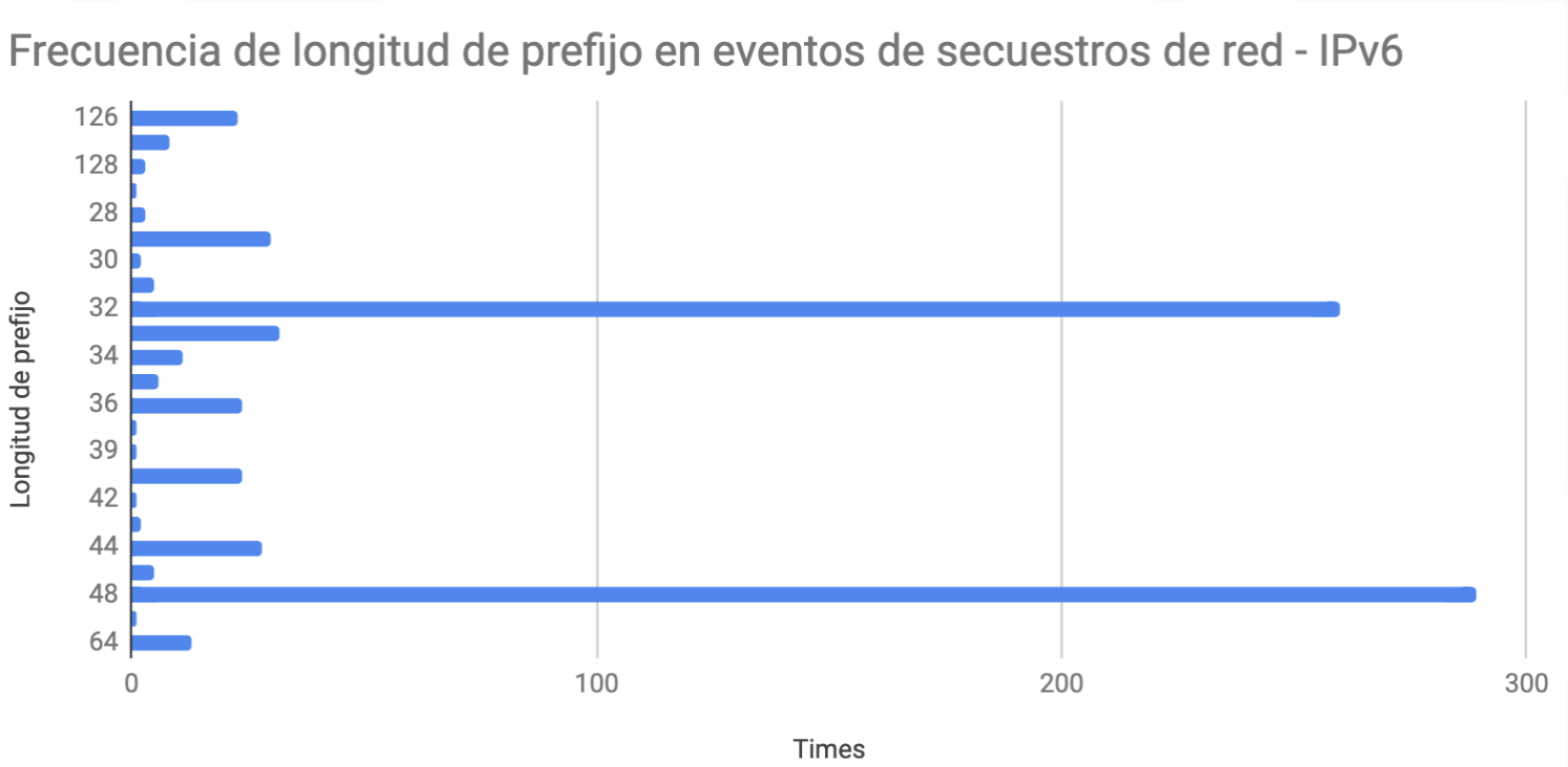
Resultados

Frecuencia longitud de máscara - IPv4



Resultados

Frecuencia longitud de prefijo – IPv6



Resultados

TOP 10 países más afectados

Posición	Country	Times
1	US	859
2	BR	702
3	IN	350
4	CN	319
5	GB	277
6	DE	264
7	RU	208
8	NL	199
9	IR	177
10	HK	172

Resultados

TOP 10 países más “secuestrador”

Ranking	Eventos	CC
1	1034	US
2	703	BR
3	307	RU
4	226	IN
5	181	DE
6	172	HK
7	172	GB
8	153	PL
9	148	IR
10	146	CH

Resultados

¿Curiosidades?

Resultados

¿Curiosidades?

AS 2147483647

Resultados

¿Curiosidades?

AS 2147483647

Este ASN es reservado; el mismo realizó un total de 36 secuestros entre el año 2016 y el 2018

¡ Muchas gracias !

¿Consultas? / ¿Preguntas?

Alejandro Acosta
alejandro @\ lacnic.net
@ITandNetworking