No, it wasn’t a hijack!!!

Aftab Siddiqui

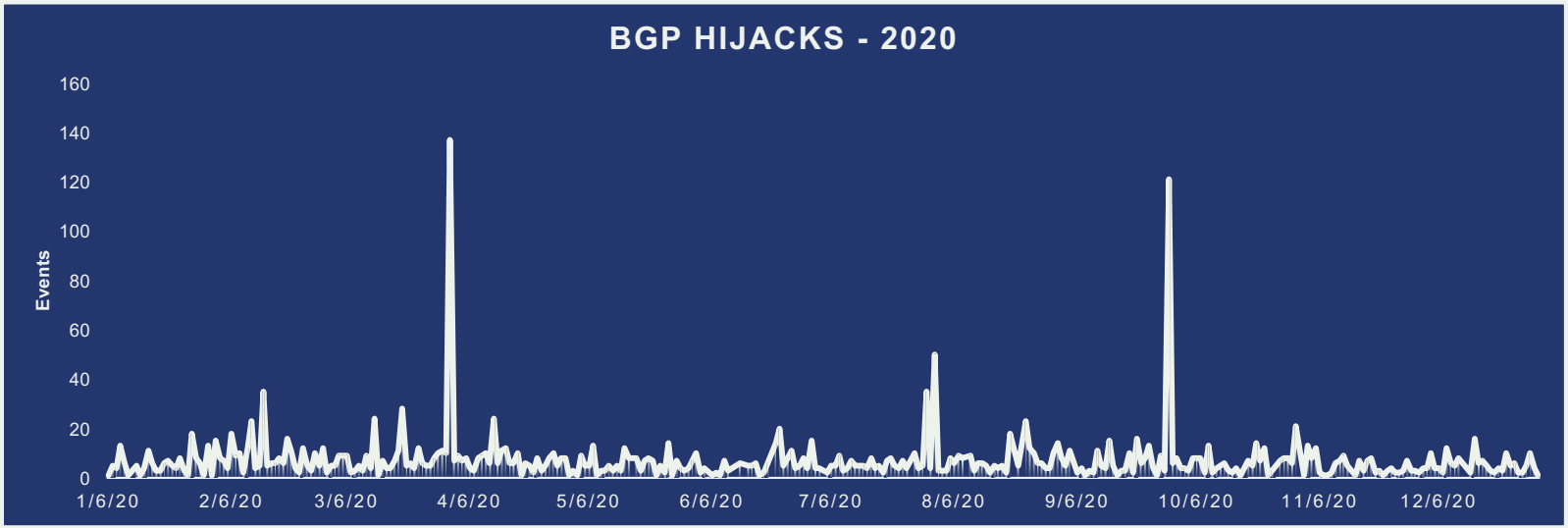
Sr Internet Technology Manager

Internet Society

The Problem

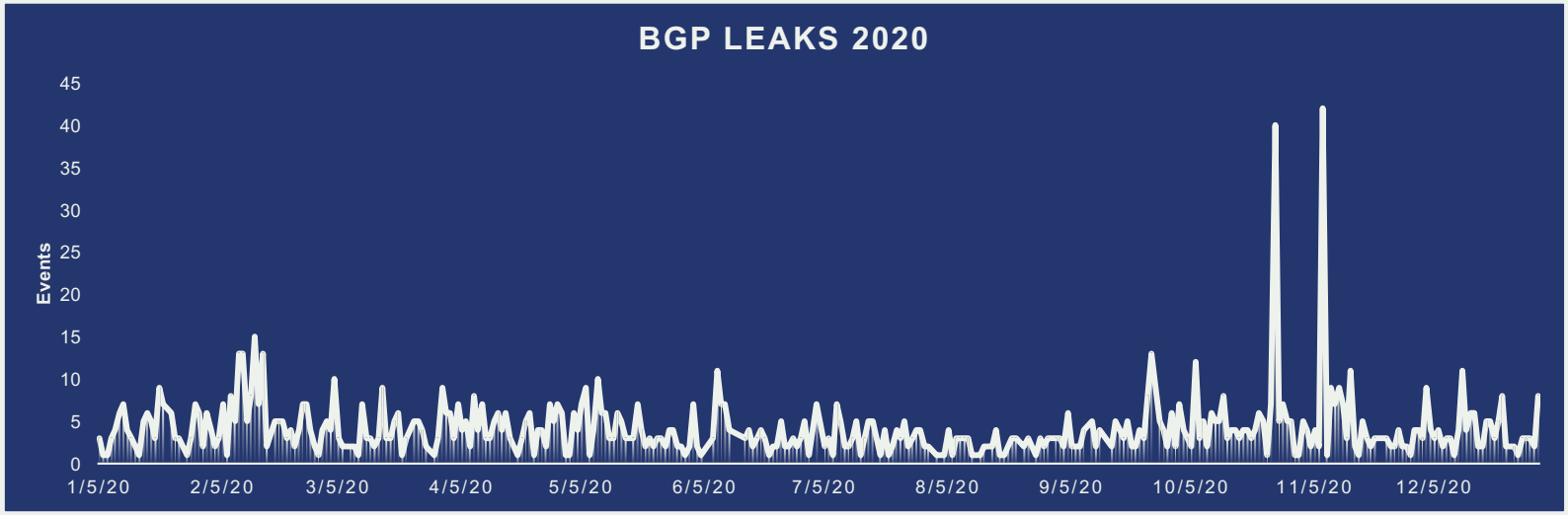
- Unsecure BGP routing is one of the most common problem for malicious threats.
- Attacks can take anywhere from hours to months to even be identified.
- **Inadvertent errors** can take networks offline

Routing Incidents.. They are not going away



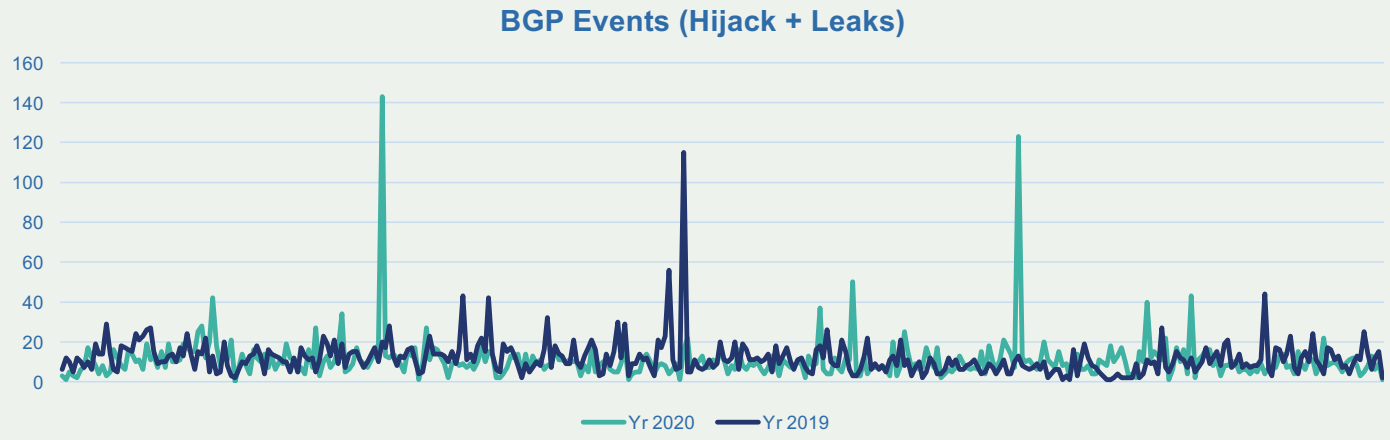
In 2020, BGPStream collectors around the world identified 2477 events termed as “Possible Hijacks”.

Routing Incidents.. They are not going away



The other category of events is BGP Leaks and in 2020 there were around 1396 events identified as “Leak”.

Routing Incidents.. They are not going away



After combining both type of events (Hijacks and Leaks) we have a graph which shows a much clearer picture of 2019-2020 comparison.

Prefix/Route Hijacking

Route hijacking, also known as “BGP hijacking” when a network operator or attacker (accidentally or deliberately) impersonates another network operator or pretending that a server or network is their client. This routes traffic to a network operator, when another real route is available.

Example: The 2008 YouTube hijack

There are Multiple classifications of Hijacks/Leaks defined in RFC7908

https://tools.ietf.org/html/rfc7908

Possible BGP hijack

Beginning at 2021-01-29 15:52:13 UTC, we detected a possible BGP hijack.
Prefix 45.143.83.0/24, is normally announced by AS212229 MICAELA-FERRARA, NL.

But beginning at 2021-01-29 15:52:13, the same prefix (45.143.83.0/24) was also announced by ASN 212056.

This was detected by 24 BGPMon peers.

Expected
Start time: 2021-01-29 15:52:13 UTC
Expected prefix: 45.143.83.0/24
Expected ASN: 212229 (MICAELA-FERRARA, NL)

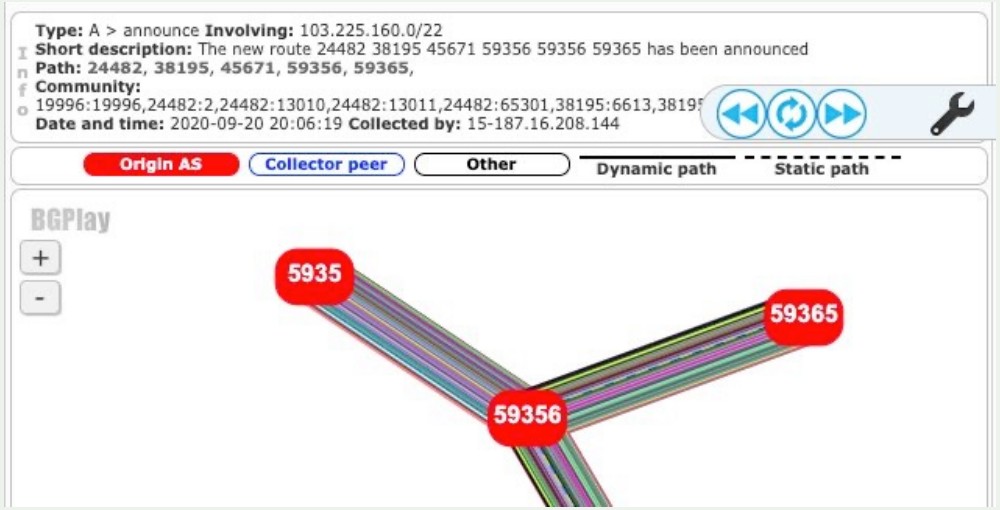
Event Details
Detected advertisement: 45.143.83.0/24
Detected Origin ASN 212056 (CELLA-CAMPANIA-ISP, NL)
Detected AS Path 14613 6939 61317 212056
Detected by number of BGPMon peers: 24

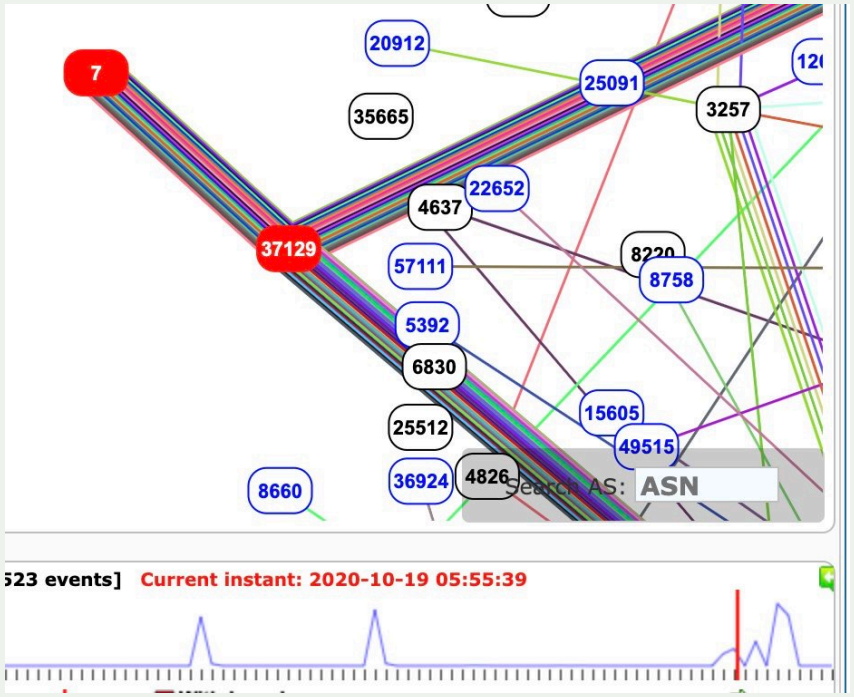
“Inadvertent Errors” aka Fat-Finger Errors

A fat-finger error is a slang term for a typing mistake. It is usually a small typo, human **error** caused by pressing the wrong key when using a computer to input data, such as an extra zero, that has out-sized consequences.

Inadvertent Errors in BGP

Its very well-known issue that network operators do make configuration mistakes (actually, everyone make mistakes, I have made it in the past). We have seen sometimes funny mistakes where people type in wrong ASNs, just in the following example.





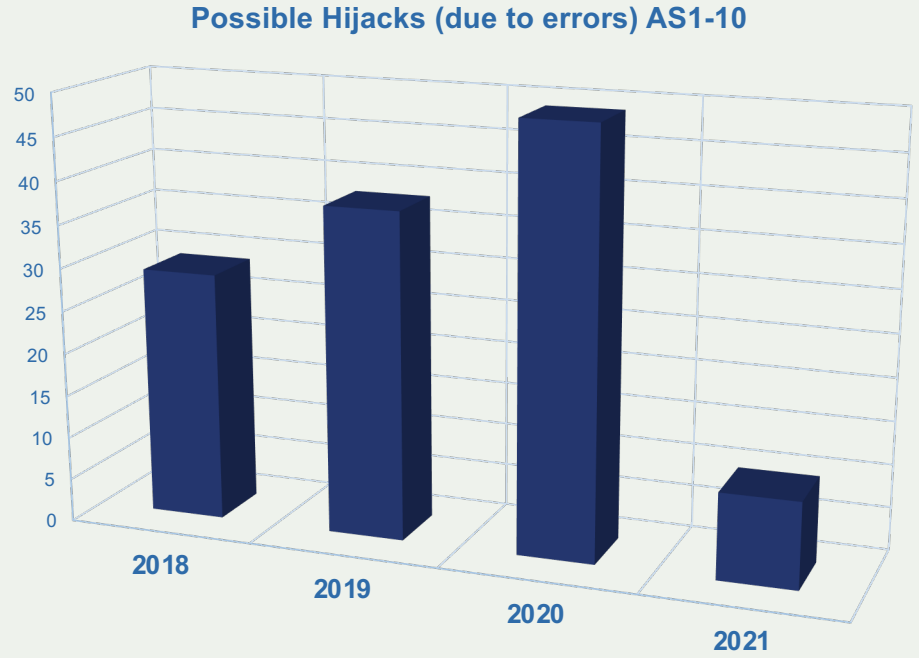
Inadvertent Errors in BGP

But during twitter conversation with Doug Madory (Kentik Inc), he mentioned that it is a very common problem with single digit ASN (as in previous example of AS7). In fact my friend Anurag Bhatia (HE) wrote about this as early as 2013 [1].

[1] - https://anuragbhatia.com/2013/08/networking/as-number-hijacking-due-to-misconfiguration/

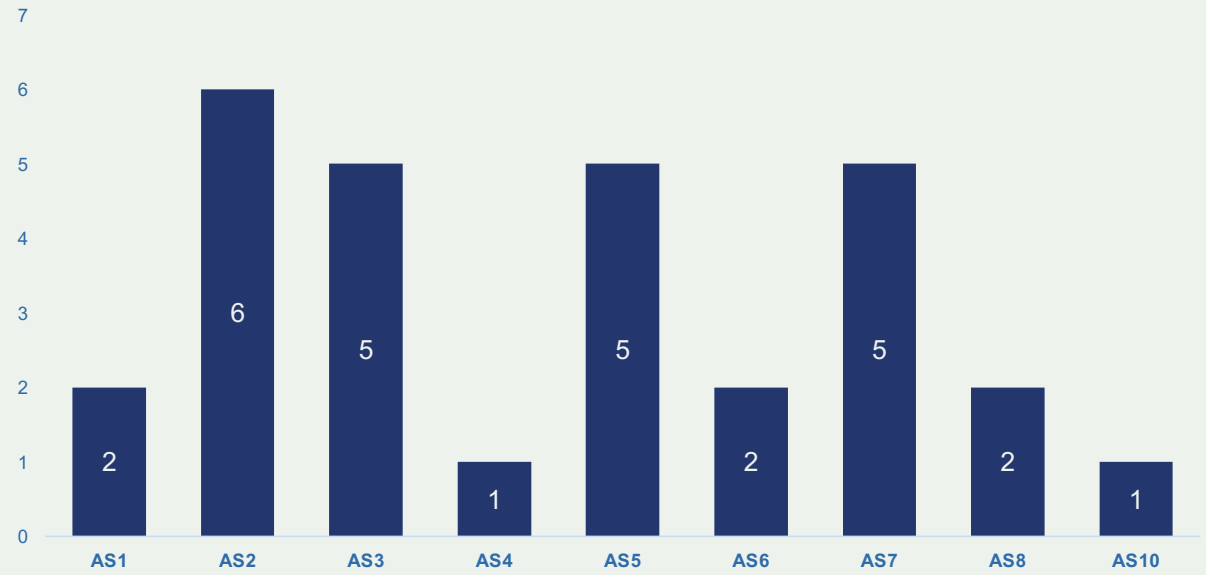
Inadvertent Errors in BGP

Just to find out how bad the problem is I looked up the data from MANRS Observatory [source: bgpstream.com] for last 3 years to check any possible hijack event involving ASN from 1 – 10 and any ASN which doesn't look right e.g. AS1111111 and the result is exactly what Doug said.



Inadvertent Errors in BGP - 2018

In 2018, AS2 is the most impacted ASN in the range of 1-10, followed by 3,5 and 7.

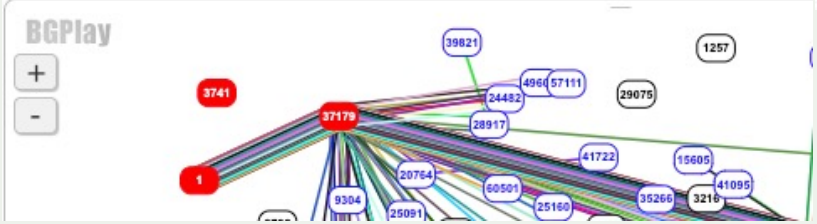


Inadvertent Errors in BGP - 2018

AS1

Type: A > announce **Involving:** 168.164.0.0/16
Short description: The new route 262757 4230 3356 37179 37179 1 has been announced
Path: 262757, 4230, 3356, 37179, 1,
Community: 4230:1
Date and time: 2018-10-06 17:25:30 **Collected by:** 15-187.16.223.117

Origin AS | Collector peer | Other | Dynamic path

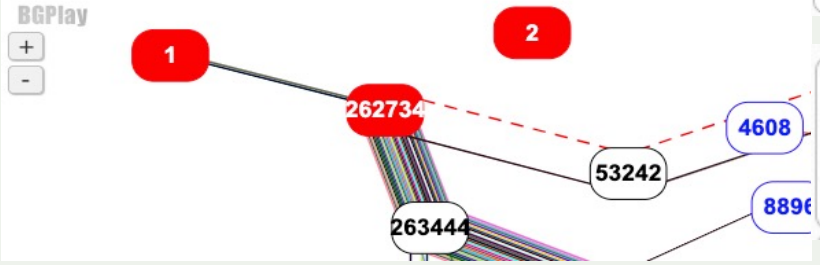


Type: A > pathchange **Involving:** 168.164.0.0/16
Short description: The route 395152 14007 6939 37179 1 is changed to 395152 63297 6939 37179
Path: 395152, 63297, 6939, 37179,
Community: 63297:1000
Date and time: 2018-10-06 18:01:14 **Collected by:** 00-192.102.254.1

AS2

Type: A > pathchange **Involving:** 186.195.0.0/20
Short description: The route 13030 52320 263444 263444 263444 263444 262734 is changed to 13030 52320 263444 263444 263444 263444 262734 1
Path: 13030, 52320, 263444, 262734, 1,
Community: 13030:1,13030:1013,13030:51904,13030:7184
Date and time: 2018-07-13 10:56:11 **Collected by:** 01-195.66.224.175

Origin AS | Collector peer | Other | Dynamic path | Static path

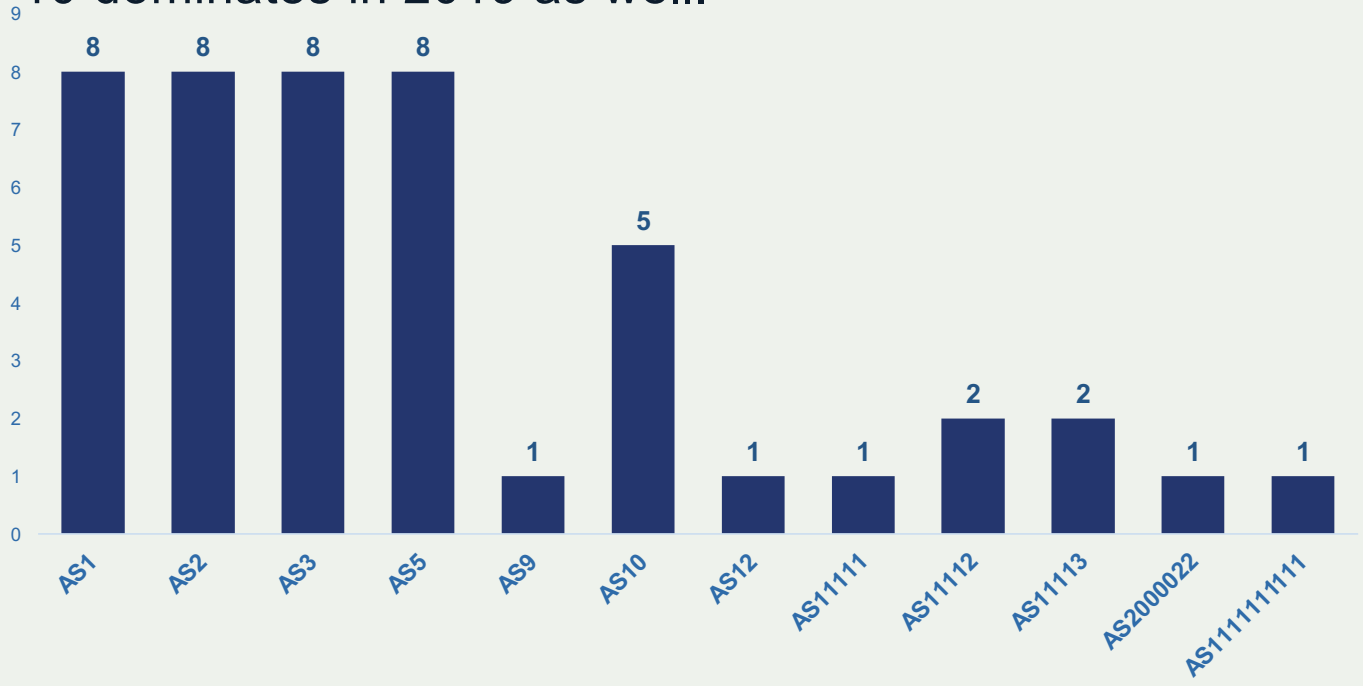


Type: A > pathchange **Involving:** 186.195.0.0/20
Short description: The route 56730 3356 3549 28347 263444 262734 1 is changed to 56730 6939 52320 263444 263444 263444 263444 262734 2
Path: 56730, 6939, 52320, 263444, 262734, 2,
Community: 56730:5459
Date and time: 2018-07-16 20:15:09 **Collected by:** 01-195.66.226.20

Type: A > pathchange **Involving:** 186.195.0.0/20
Short description: The route 2914 52320 263444 263444 263444 263444 262734 2 is changed to 2914 52320 263444 263444 263444 263444 262734 262734
Path: 2914, 52320, 263444, 262734,
Community: 2914:410,2914:1009,2914:2000,2914:3000
Date and time: 2018-07-17 15:23:14 **Collected by:** 01-195.66.224.138

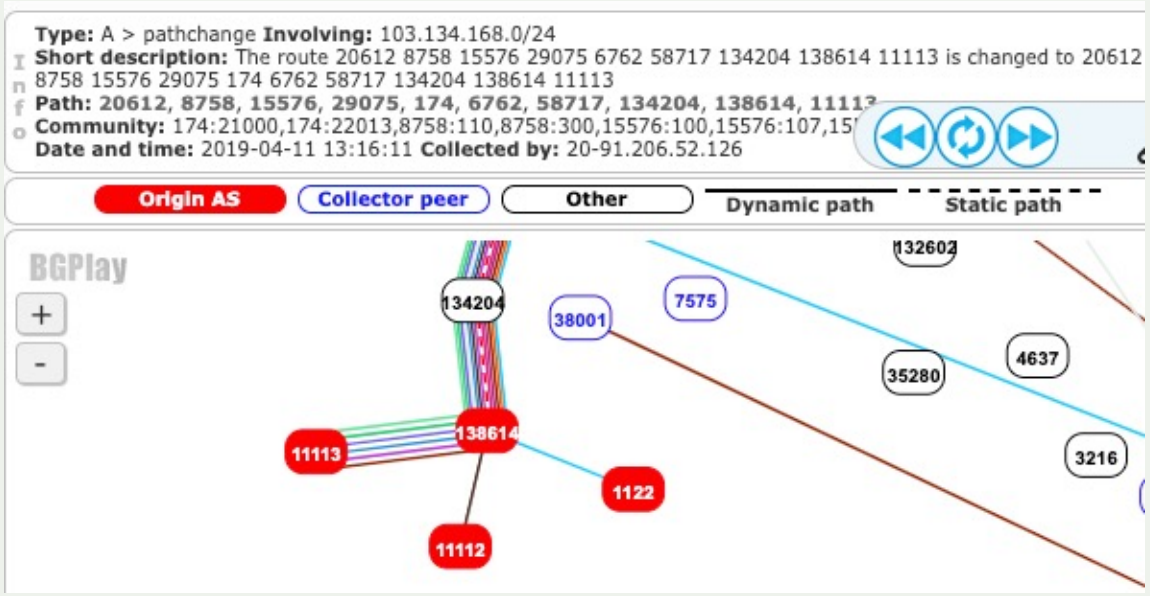
Inadvertent Errors in BGP - 2019

Other then 1-10 ASN range, there are other ASNs with no relationship with the legitimate originator and most likely leaked from lab environment or wrong input. Still AS 1-10 dominates in 2019 as well.



Inadvertent Errors in BGP - 2019

start_time	Detected_ASN	ASN Name	hijack_announced_prefix	hijack_as_path
11/4/19 13:14	11113	Unknown	103.134.168.0/24	262149 20299 262206 174 6762 58717 134204 138614 11113
11/4/19 13:14	11113	Unknown	103.134.171.0/24	37100 174 6762 58717 134204 138614 11113
11/4/19 13:13	11112	Unknown	103.134.168.0/24	199981 42739 3257 6762 58717 134204 138614 11112
11/4/19 13:13	11112	Unknown	103.134.171.0/24	63956 703 6762 58717 134204 138614 11112



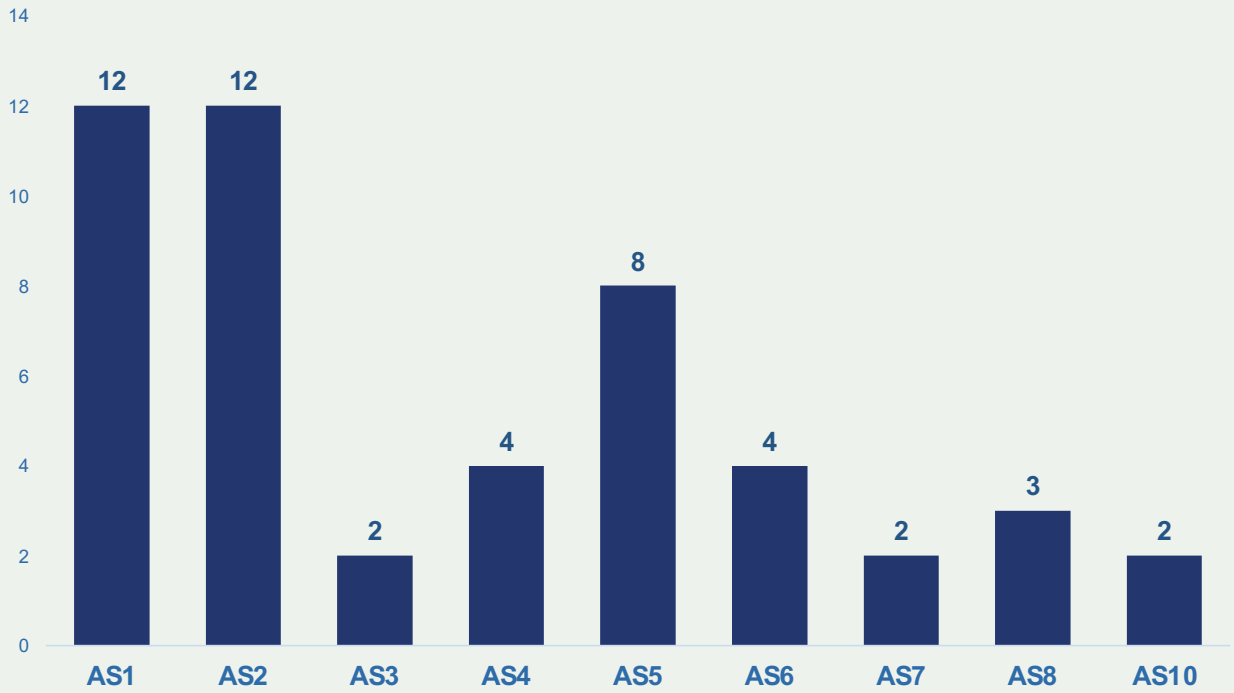
Type: W > withdrawal **Involving:** 103.134.168.0/24
Short description: The route 262757, 3549, 3356, 6762, 58717, 134204, 138614, 11112 has been withdrawn.
Date and time: 2019-04-11 **13:22:16** **Collected by:** 15-187.16.223.117

Inadvertent Errors in BGP - 2019

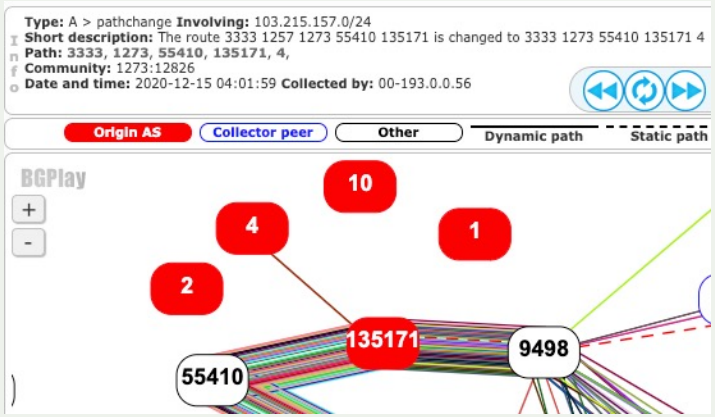
Start time	Expected ASN	ASN Name	Detected_ASN	Hijack prefix
26/8/19 10:25	200022	AIRNET-AS, RU	2000022	141.101.210.0/24
6/3/19 20:40	394119	EXPERIMENTAL-COMPUTING-FACILITY, US	1111111111	23.169.96.0/24

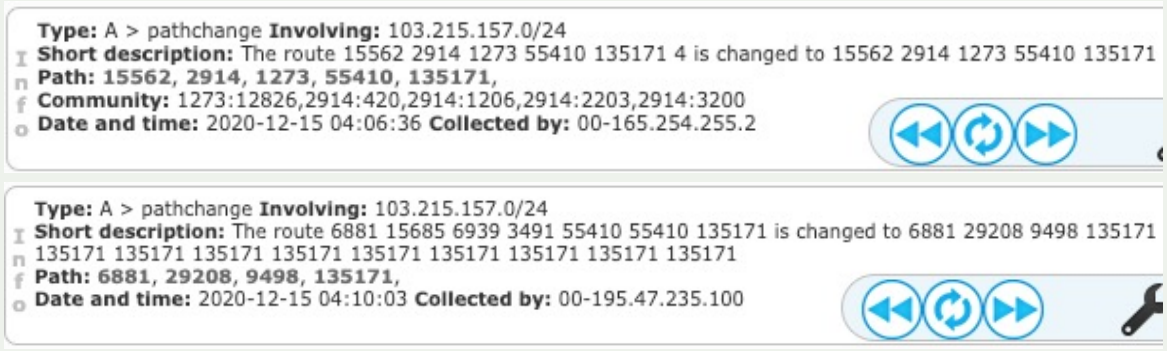
Inadvertent Errors in BGP - 2020

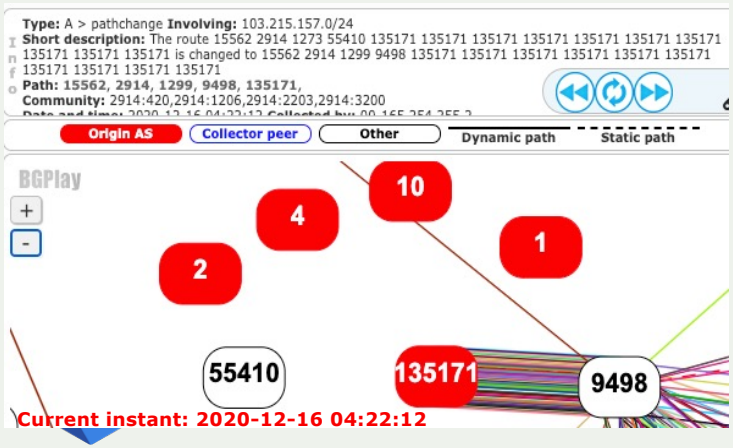
Clearly, 2020 was the year of AS 1-10 hijacks, where AS1 and AS2 were dominant ASNs.



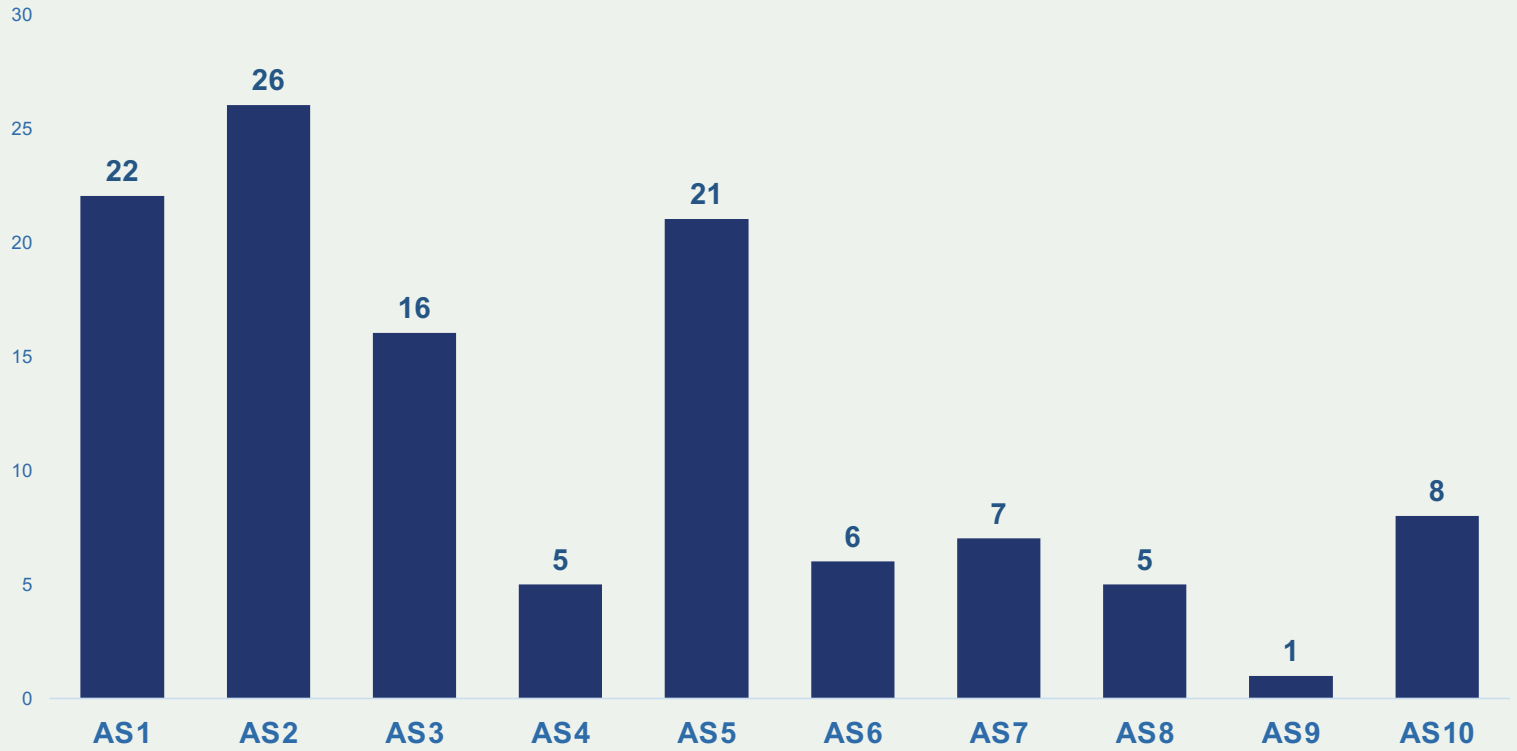
Inadvertent Errors in BGP - 2020







Inadvertent Errors in BGP 2018 – 2021 (AS1 – AS10)



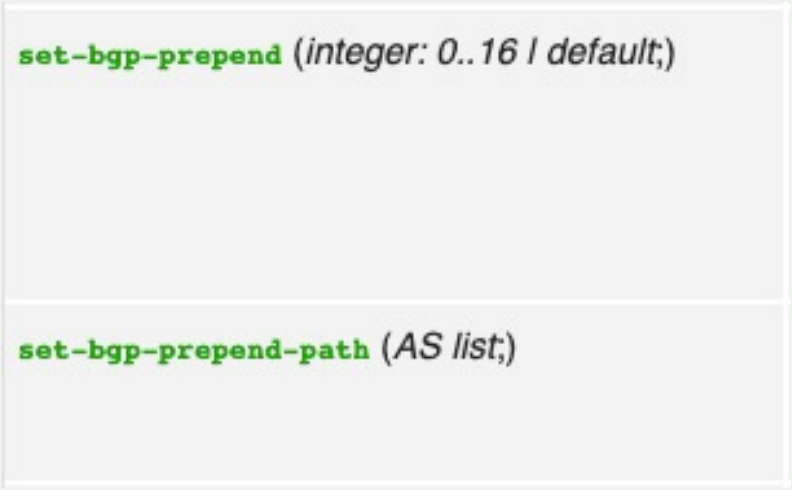
Current Status 12th April 2021

	Network	Next Hop	Metric	LocPrf	Weight	Path
*>	12.51.30.0/24	169.254.169.254		50	0	64515 65534 20473 3491 7018 29855 1 i
*>	45.134.201.0/24	169.254.169.254		50	0	64515 65534 20473 2914 5511 12975 208473 1 i
*>	45.182.198.0/23	169.254.169.254		50	0	64515 65534 20473 2914 6762 25933 269235 1 i
*>	45.188.73.0/24	169.254.169.254		50	0	64515 65534 20473 17819 38195 174 23106 52862 269517 1 i
*>	91.210.36.0/24	169.254.169.254		50	0	64515 65534 20473 17819 4826 6939 6702 48085 1 1 1 1 1 i
*>	91.210.37.0/24	169.254.169.254		50	0	64515 65534 20473 17819 4826 6939 6702 48085 1 1 1 1 1 i
*>	91.210.38.0/24	169.254.169.254		50	0	64515 65534 20473 17819 4826 6939 6702 48085 1 1 1 1 1 i
*>	91.227.30.0/24	169.254.169.254		50	0	64515 65534 20473 3491 12389 56720 1 i
*>	177.10.218.0/24	169.254.169.254		50	0	64515 65534 20473 2914 3356 28146 265076 263036 1 i
*>	205.207.214.0/24	169.254.169.254		50	0	64515 65534 20473 3491 701 7046 1 i
*>	212.94.84.0/22	169.254.169.254		50	0	64515 65534 20473 3491 1299 47605 29132 1 i

	Network	Next Hop	Metric	LocPrf	Weight	Path
*>	12.35.70.0/23	169.254.169.254		50	0	64515 65534 20473 2914 7018 55257 2 2 i
*>	31.129.245.0/24	169.254.169.254		50	0	64515 65534 20473 6939 50581 207422 2 i
*>	38.126.196.0/24	169.254.169.254		50	0	64515 65534 20473 3491 174 35978 2 i
*>	45.188.74.0/24	169.254.169.254		50	0	64515 65534 20473 2914 13786 52840 52840 269517 2 i
*>	45.237.219.0/24	169.254.169.254		50	0	64515 65534 20473 3491 3356 265442 265457 268299 2 i
*>	91.143.144.0/20	169.254.169.254		50	0	64515 65534 20473 2914 3356 12389 41837 41837 2 i
*>	103.54.102.0/24	169.254.169.254		50	0	64515 65534 20473 3491 55644 55410 4755 133967 133967 2 i
*>	103.54.103.0/24	169.254.169.254		50	0	64515 65534 20473 3491 55644 55410 4755 133967 133967 2 i
*>	103.152.216.0/24	169.254.169.254		50	0	64515 65534 20473 6939 9299 140927 2 i
*>	128.4.0.0/16	169.254.169.254		50	0	64515 65534 20473 3491 174 34 34 34 34 34 34 2 i
*>	188.191.208.0/21	169.254.169.254		50	0	64515 65534 20473 3491 174 50084 56491 2 i

Why is it happening? And why AS1-10?

- Most likely due to RouterOS
- When engineers use the following 2 commands interchangeably



How many times to prepend router's own AS number to **AS_PATH** attribute

SetBgpPrepend ::= default | Num
  Num ::= 0..16 (integer number)

add specified list of AS numbers to **AS_PATH** attribute
If both **set-bgp-prepend** and **set-bgp-prepend-path** are used, then **set-bgp-prepend** will have highest priority.

SetBgpPrependPath ::= As[,SetBgpPrependPath]
  As ::= 0..4294967295

https://wiki.mikrotik.com/wiki/Manual:Routing/Routing_filters

What should we call these incidents?

- AS Prepend Hijack?
- MikroTik Prepend Hijack?
- Something else?

Lessons Learned!!!

- Filtering ASNs is as important as prefix filtering
- Create filters before configuring neighbors
- Practice Regex (its complicated, its boring but its important)
- Try to avoid unnecessary prepend
- Test in the lab not connected to your production edge
- Talk to other members of the community for help if not sure
- It shows how easy it is to hijack ASN and remain undetected.
- **Combining ASN + Prefix hijack makes ROA useless ☹**

MANRS Actions - Network operators

Filtering

Prevent propagation of incorrect routing information

Ensure the correctness of your own announcements and announcements from your customers to adjacent networks with prefix and AS-path granularity

Anti-spoofing

Prevent traffic with spoofed source IP addresses

Enable source address validation for at least single-homed stub customer networks, their own end-users, and infrastructure

Coordination

Facilitate global operational communication and coordination between network operators

Maintain globally accessible up-to-date contact information in common routing databases

Global Validation

Facilitate validation of routing information on a global scale

Publish your data, so others can validate

MANRS Implementation Guide

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

- Based on Best Current Operational Practices deployed by network operators around the world
- https://www.manrs.org/bcop/

Mutually Agreed Norms for Routing Security (MANRS) Implementation Guide

Version 1.0, BCOP series
Publication Date: 25 January 2017

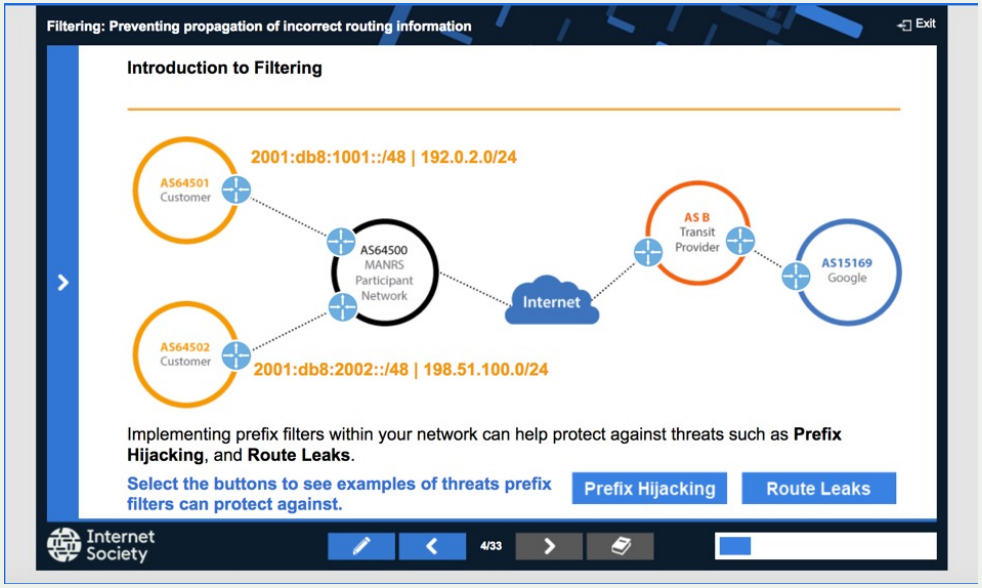
MANRS Training Modules

6 training modules based on information in the Implementation Guide.

Walks through the tutorial with a test at the end of each module.

Working with and looking for partners that are interested in integrating it in their curricula.

https://academy.apnic.net/en/course/manrs/



Thanks to APNIC for hosting MANRS Tutorial

LEARN MORE:
https://www.manrs.org

Thank you.

manrs.org