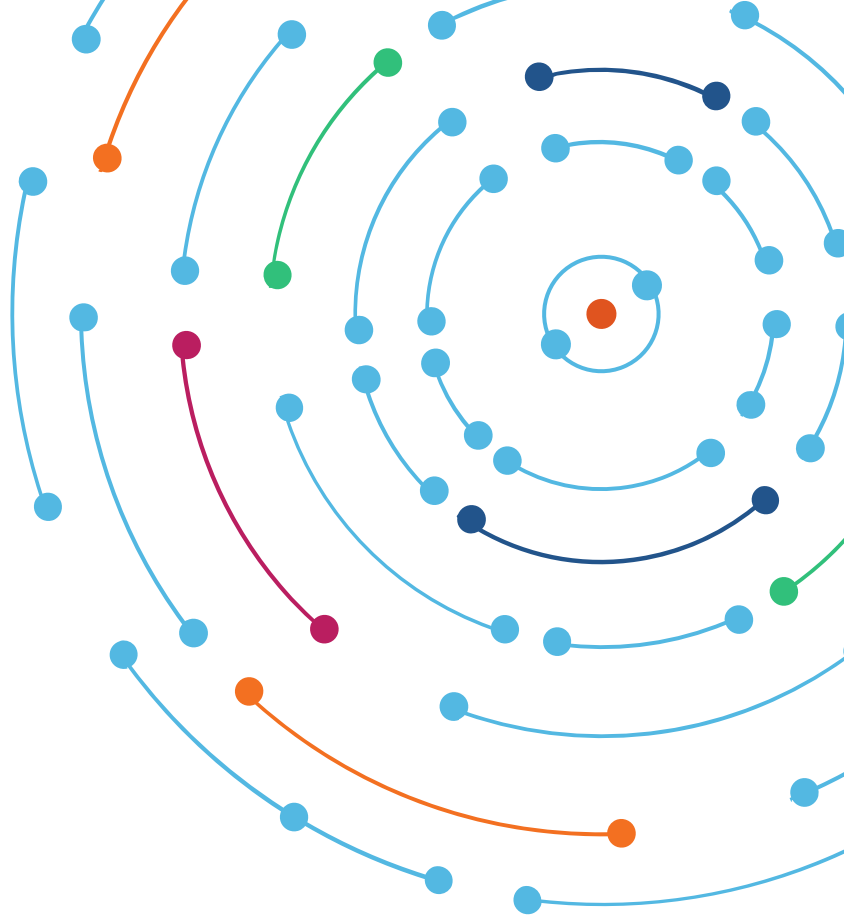





*Analyzing the Recent Routing Leak  
from India with BGP & Netflow*

Doug Madory  
Director of Internet Analysis



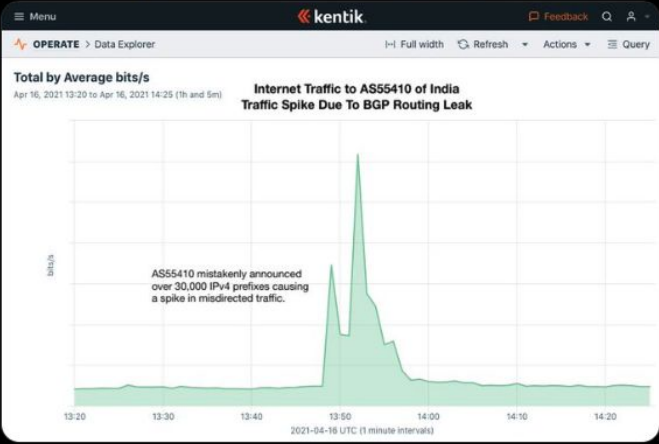
# Another BGP Leak!

 **Doug Madory**  
@DougMadory

Large BGP routing leak out of India this morning.

AS55410 mistakenly announced over 30,000 BGP prefixes causing a 13x spike in inbound traffic to their network according to @kentikinc netflow data.


(cc: @anurag\_bhatia, @aftabsiddiqui, @jaredmauch)



3:21 PM · Apr 16, 2021 · Twitter Web App

- At 13:48 UTC on 16-April-2021, AS55410 originated over 30,000 prefixes.
- Routes were propagated to the greater internet via AS1273 and AS9498.
- While the leak announcements circulated for over an hour, the impact to traffic lasted only about 10 minutes based on Kentik's netflow data.
- *Follow me at @dougmadory* 🙄

# BGP-based Analyses of Leak



**Radar by Qrator**  
@Qrator\_Radar

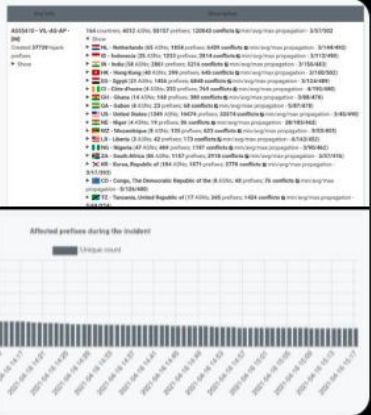
**April 16, 2021 - AS55410 - VIL-AS-AP (Vodafone Idea) - hijacked 37739 prefixes - countries affected 164 - ASNs affected 4012 - duration 1:30:00**

**Created Hijacks incident statistics**

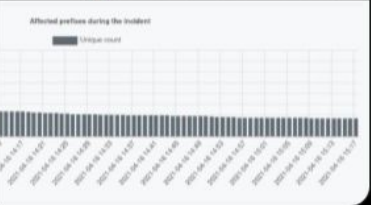
**AS55410 - VIL-AS-AP - [IN]**

Start period: [2021-04-16 13:45; 2021-04-16 14:00]

Type	Created Hijacks
Key ASN	AS55410 - VIL-AS-AP - [IN]
Start	2021-04-16 13:49(UTC)
End	---
Overall stat	Conflicts count all: 120843 ASNs affected: 4012 Countries affected: 164 ▶ Show all stat
Prefixes stat	Prefixes created: 37739 Prefixes affected: 50157 Prefixes specific: 3876 more, 37735 equal, 26463 less ▶ Show all stat
Propagations	Max propagation: 502 ▶ Show all stat
Duration	Total duration: 1:30:00 104862/120843 (86%) finished



**Affected prefixes during the incident**



7:36 AM · Apr 17, 2021 · Twitter Web App

At around 13:48 UTC, AS55410 started originating routes that don't belong to them.

```
04/16/21 13:48:58.863838 5.160.54.0/23 6939 9498 55410 55410 55410
04/16/21 13:48:58.863838 8.34.9.0/24 6939 9498 55410 55410 55410
04/16/21 13:48:59.009165 8.34.9.0/24 34224 9498 55410 55410 55410
04/16/21 13:48:59.036987 8.34.9.0/24 1299 9498 55410 55410 55410
04/16/21 13:48:59.103513 66.111.63.0/24 3257 1299 9498 55410 55410 55410
04/16/21 13:48:59.103513 142.131.200.0/23 3257 1299 9498 55410 55410 55410
04/16/21 13:48:59.255774 141.98.68.0/23 22652 6453 9498 55410 55410 55410
```

Figure 5 — Route dump, AS55410 to t

**BGP** A major BGP route leak by AS55410  
By Aftab Siddiqui on 26 Apr 2021

## Updates from Vodafone AS55410 - 16 April 2021



**anuragbhatia.com**  
DNS, BGP, IPv6 and more!

# Top Impacted Prefixes from Spain by Peercount (Routeviews)

Top 10

Peers	Prefixes	Org	City	Country
231	23.60.208.0/20	Akamai	Madrid	ES
230	23.60.224.0/19	Akamai	Madrid	ES
228	23.214.72.0/23	Akamai	Madrid	ES
228	23.214.124.0/22	Akamai	Madrid	ES
227	23.214.208.0/20	Akamai	Madrid	ES
227	23.14.136.0/22	Akamai	Madrid	ES
226	23.47.32.0/20	Akamai	Madrid	ES
226	23.47.156.0/22	Akamai	Madrid	ES
226	23.39.64.0/20	Akamai	Madrid	ES
225	23.47.8.0/21	Akamai	Madrid	ES

Top-10 geo distro

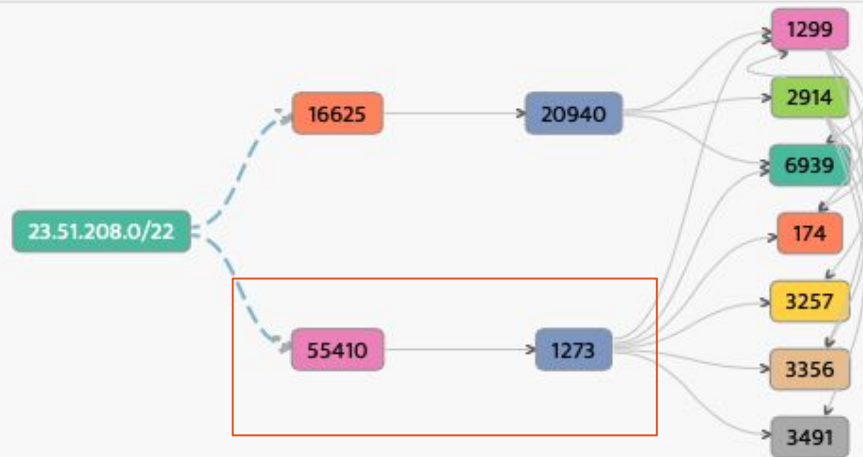
11847 US  
2702 IN  
1423 CA  
1420 RU  
1286 EG  
833 DE  
778 KR  
771 TR  
765 ID  
711 ZA

Other ES orgs

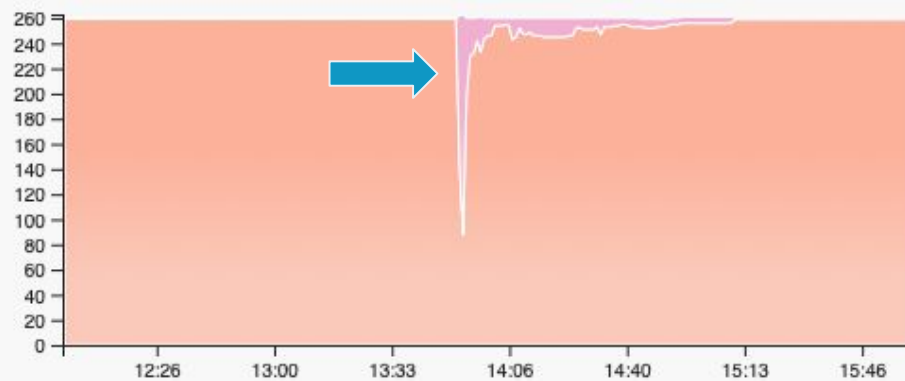
117	31.187.68.0/24	MEDIAPRO CLOUD S.L.		ES
115	5.189.222.0/24	G-Core Labs S.A.	Madrid	ES
115	31.13.188.0/24	M247 Ltd	Madrid	ES
108	8.44.3.0/24	Cloudflare, Inc.	Barcelona	ES
106	23.246.48.0/24	Netflix	Madrid	ES
105	23.246.49.0/24	Netflix	Madrid	ES
99	8.42.161.0/24	Cloudflare, Inc.	Madrid	ES
92	31.3.127.0/24	Prored Comunicaciones		ES
92	31.3.125.0/24	Prored Comunicaciones		ES
92	31.3.124.0/24	Prored Comunicaciones		ES
92	31.3.120.0/24	Prored Comunicaciones		ES

## Network diagram

23.51.208.0/22

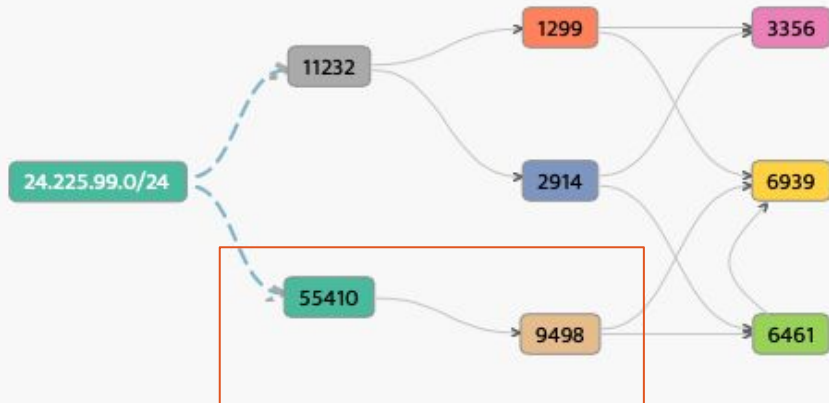


## Upstream view for: 23.51.208.0/22

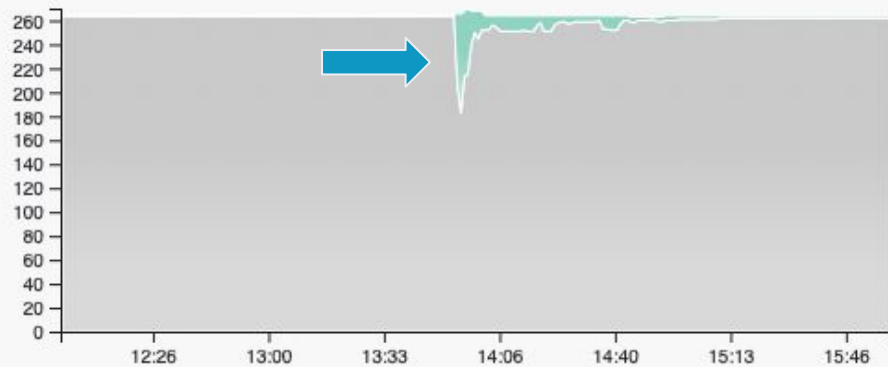


Network diagram

24.225.99.0/24



Upstream view for: 24.225.99.0/24



# Did RPKI help?

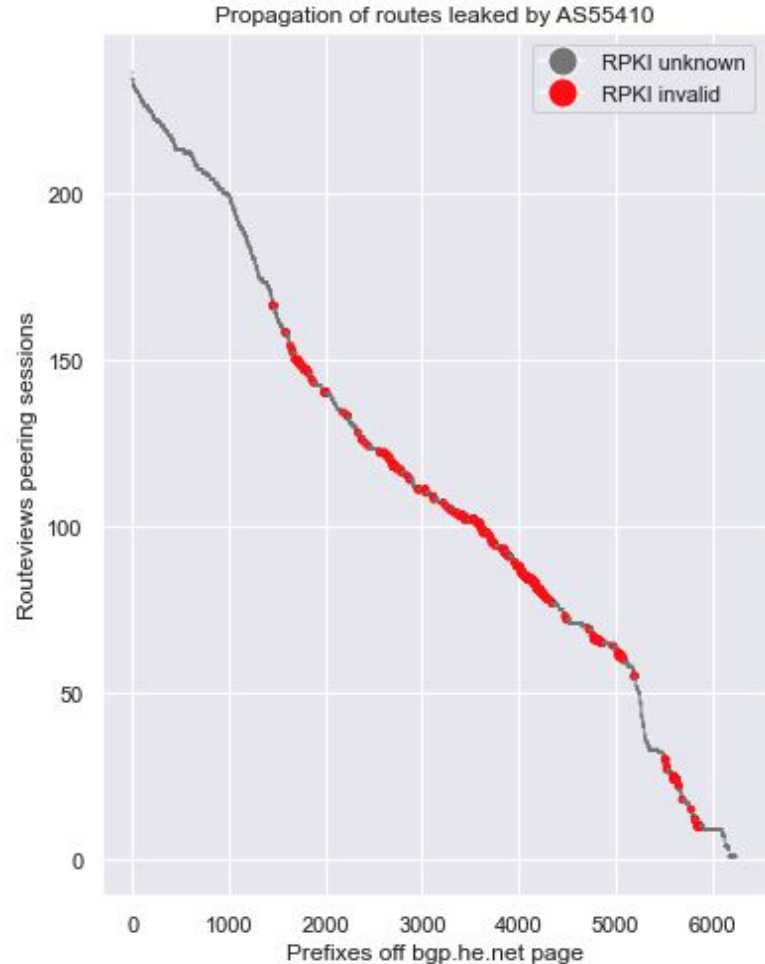
A couple of days after the leak, bgp.he.net was still reporting AS55410 as the origin of most of the routes it leaked with a ROV results.

I scraped the page and plotted the RPKI unknowns and RPKI invalids against the number of peers that accepted the leaked routes.

The invalids were generally lower on the plot but occasionally were still propagated widely.

*80% of leaked prefixes had no ROA.*

- Aftab Siddiqui, Internet Society



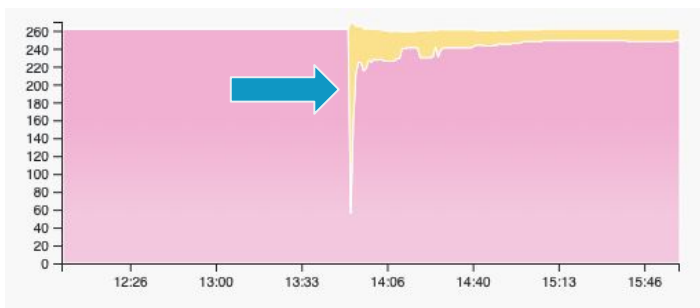
# Did RPKI help at all? *A Tale of Two Prefixes*

Two similar Akamai prefixes were leaked: one signed, one not.

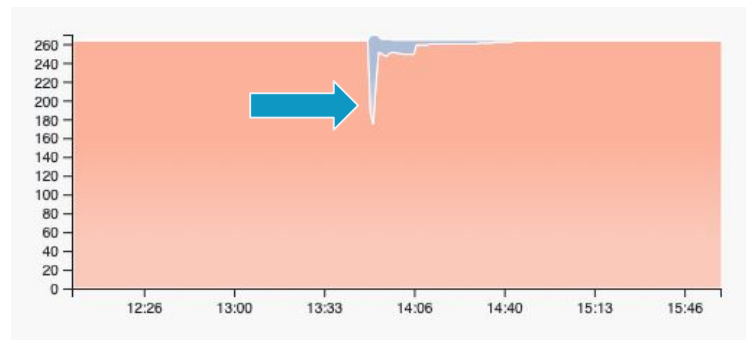
<u>2.17.148.0/22</u>	✓	Akamai Technologies
<u>2.17.192.0/22</u>	✗	Akamai Technologies

Did signing the route limit the leaked route's propagation?

2.17.148.0/22 (224 peers)



2.17.192.0/22 (101 peers)



Difficult to know all of the factors contributing to the propagation of a route.



# Netflow Analysis of BGP Leak

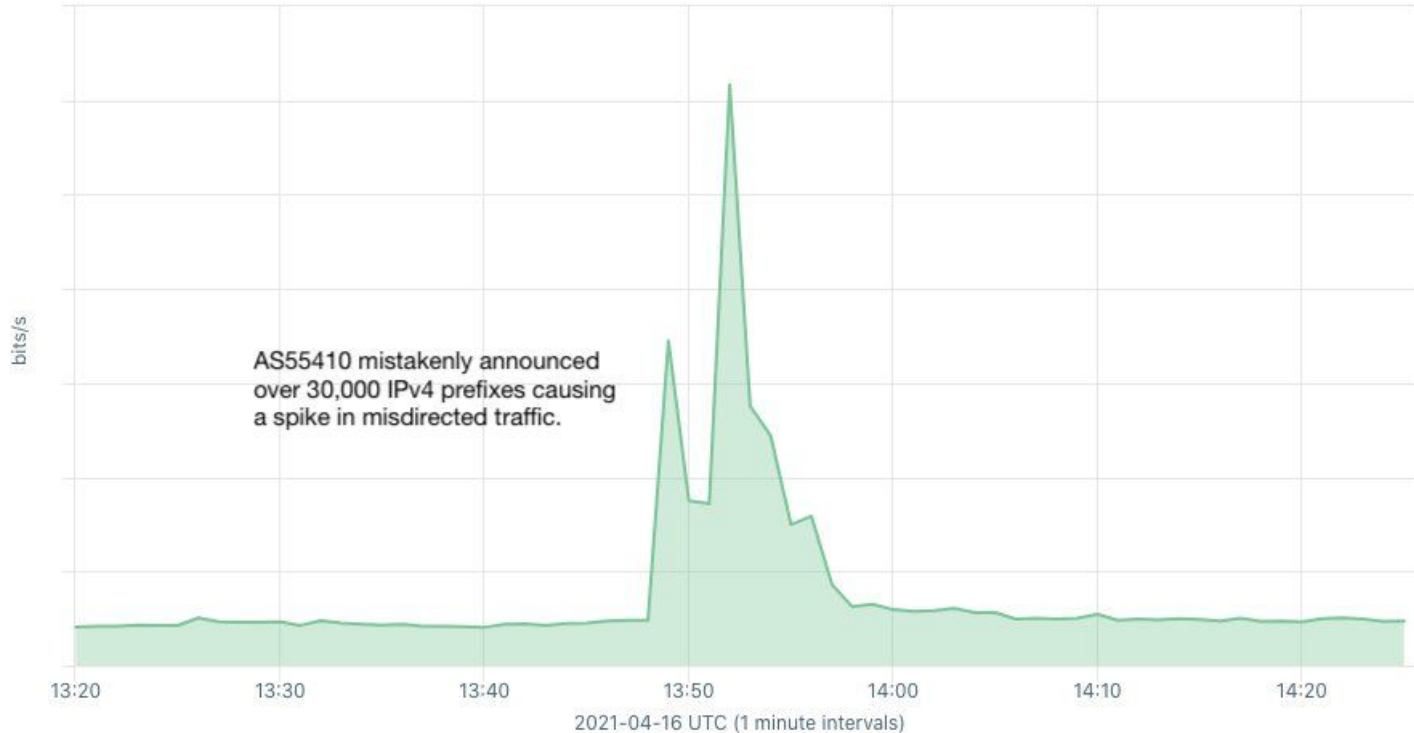


- When analyzing BGP leaks using only BGP data, it is impossible to know the operational impact of the incident.
  - Routes represent *potential traffic paths*.
  - Even active measurement (traceroutes, etc) is artificial.
- It is possible to have a routing incident that had *little to no operational impact*.
- Kentik provides netflow analysis to >300 companies including major telecoms and internet firms.
- By aggregating the netflow data, we can get a sense of how much traffic was affected by the routing leak.

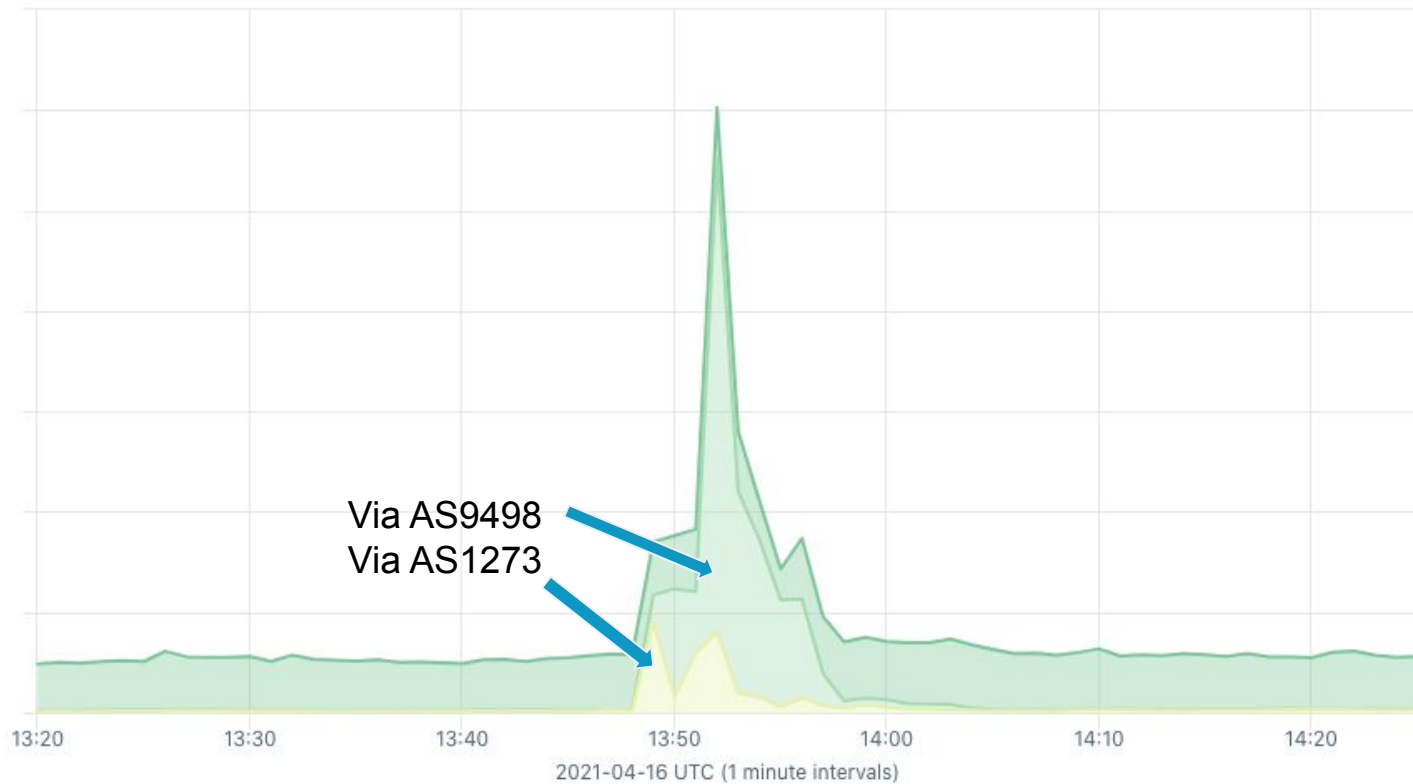
### Total by Average bits/s

Apr 16, 2021 13:20 to Apr 16, 2021 14:25 (1h and 5m)

### Internet Traffic to AS55410 of India Traffic Spike Due To BGP Routing Leak



Which upstreams carried more traffic due to the leak:



# Conclusions

- This was a re-origination leak so ROV could have helped.
  - Leaked routes that had ROAs propagated less.
- Leaker (55410) and upstreams (1273, 9498) did not filter.
- ASes who do ROV were not fooled for the minority of prefixes that had ROAs.
- Prefixes with ROAs generally propagated less.
- *Netflow can be used to understand operational impact of a BGP leak.*

## RPKI To-do:

- Sign your routes *to help yourself*
- Drop invalids *to help everyone*