

# New Milestones in RPKI ROV Adoption

Jac Kloots (Kentik)



The network observability company

# **This is a presentation originally from:**

**Doug Madory (Kentik)  
Job Snijders (Fastly)**



# Orange España outage (Jan 3, 2024)

Orange suffers a drop in Internet service throughout Spain due to a cyber attack

The company recognizes “improper access” that would not have compromised its customers' data and warns that the service is “practically restored”

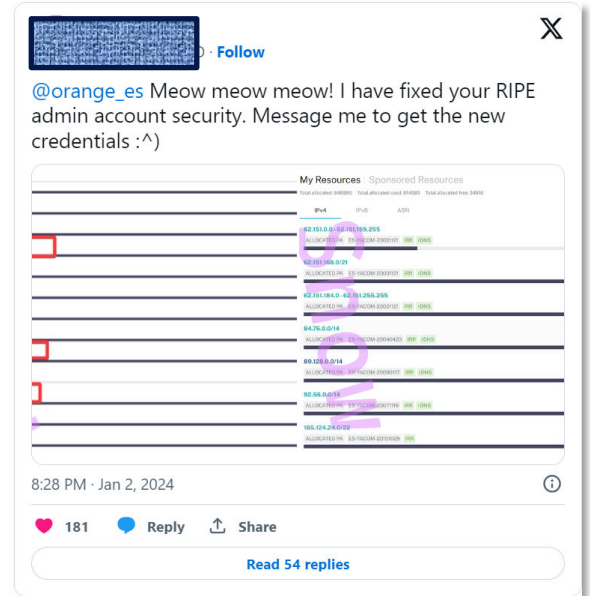
The screenshot shows the top portion of a news article on the EL PAÍS website. The page is in Spanish. At the top right, there are buttons for 'SUSCRIBETE' and 'INICIAR SESIÓN'. Below the navigation bar, the article title is 'Orange sufre una caída del servicio de Internet en toda España por culpa de un ciberataque'. The sub-headline reads: 'La compañía reconoce un “acceso indebido” que no habría comprometido los datos de sus clientes y avisa de que el servicio está “prácticamente restablecido”'. The article is categorized under 'INTERNET'.



The screenshot shows a tweet from Orange España (@orange\_es) posted on Jan 3, 2024, at 12:49 PM with 583 views. The tweet text in Spanish is: 'Tenemos detectada una incidencia generalizada con nuestro servicio a nivel nacional, pero que afortunadamente ha sido detectada muy rápido (gracias en gran parte a todos vuestros comentarios y avisos) y ya estamos trabajando para solucionarla cuanto antes. 1/2'. Below the tweet is its English translation: 'We have detected a widespread incident with our service nationwide, but fortunately it has been detected very quickly (thanks in large part to all your comments and warnings) and we are already working to solve it as soon as possible. 1/2'. The tweet interface shows 2 replies, 2 retweets, and a bookmark icon.

# Why did Orange España suffer an outage?

- Hacker was able to log into company's RIPE NCC portal using the password "ripeadmin" found in a public leak of stolen credentials. Oops!
- Hacker altered Orange España's RPKI configuration, rendering many of its BGP routes RPKI-invalid.
- No traffic was misdirected, no data was compromised.
- Outage marked the first time RPKI ROV was used as a vector for a denial-of-service.



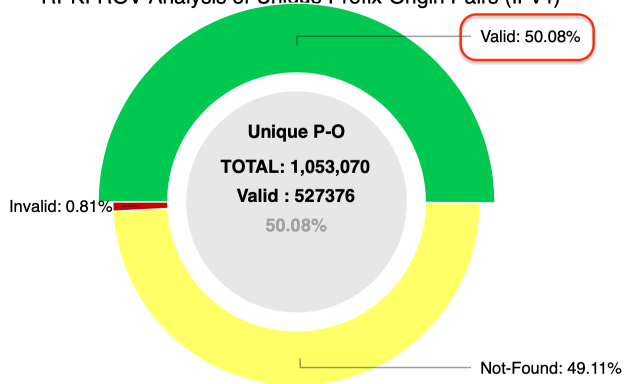
The image shows a tweet from @orange\_es and a screenshot of the RIPE NCC portal. The tweet, dated Jan 2, 2024, at 8:28 PM, says: "@orange\_es Meow meow meow! I have fixed your RIPE admin account security. Message me to get the new credentials :^)". The screenshot of the RIPE NCC portal shows a table of resources with columns for IPv4, IPv6, and ASIN. Several rows are highlighted in red, indicating RPKI-invalid status. The table includes the following data:

IPv4	IPv6	ASIN
82.151.0-82.151.255	2001:191:1000:0001::/48	AS151
42.151.184.0-42.151.255.255	2001:191:1000:0001::/48	AS151
44.76.0/14	2001:191:1000:0004::/48	AS151
88.128.0/14	2001:191:1000:0007::/48	AS151
92.151.0/14	2001:191:1000:0007::/48	AS151
98.124.2.0/22	2001:191:1000:0007::/48	AS151

***But to really understand the significance of the outage, we must understand RPKI and the state of BGP security***

<https://www.kentik.com/blog/digging-into-the-orange-espana-hack/>

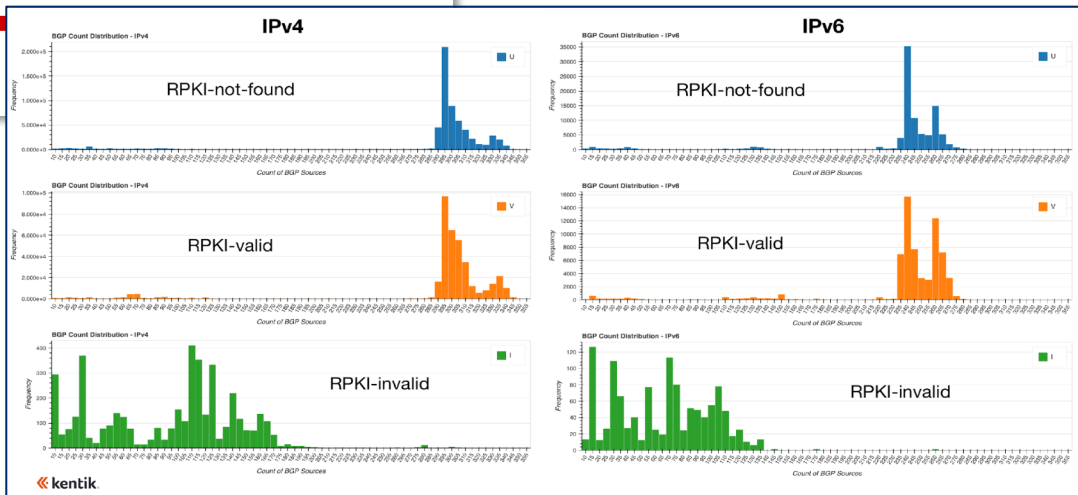
# RPKI-ROV Analysis of Unique Prefix-Origin Pairs (IPv4)



Valid: 527,376    Not-Found: 517,151

NIST RPKI Monitor: RPKI-ROV Analysis    Protocol: IPv4    RIR: All

Let's understand the current state of RPKI ROV adoption



# Measuring RPKI deployment progress

- Two steps needed to identify and reject RPKI-Invalid BGP routes.

1

Create ROAs to define correct origins for address space

---

2

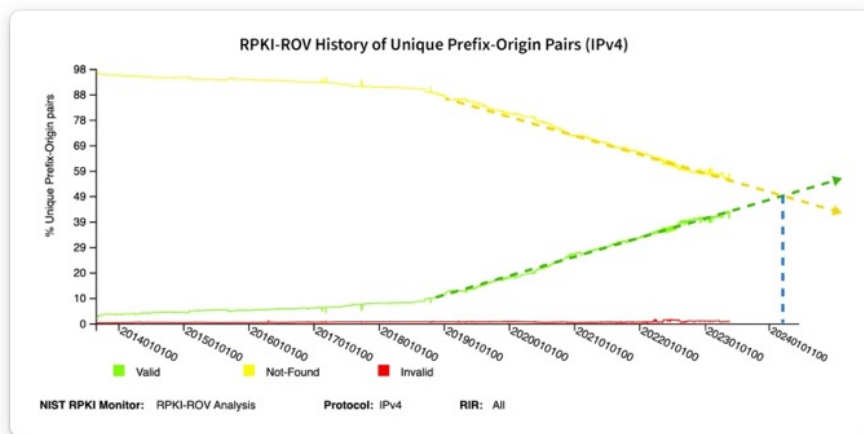
ASes reject RPKI-invalid routes that don't match ROAs

---

# ROA Creation Predictions

- Last year, we made this bold prediction in our post:


If we are to assume steady growth of the share of BGP routes with ROAs, it should become the majority case in about a year from now (May 2024). Mark your calendars!



<https://www.kentik.com/blog/exploring-the-latest-rpki-rov-adoption-numbers/>

# ROA Creation Predictions

- But y'all were doubters!


 **Doug Madory** ✓  
@DougMadory

Ok BGP/RPKI nerds... what's your prediction on when these (very faint!) lines will cross and the majority of globally routed IPv4 routes have ROAs? (IPv6 is already there)  
[rpk-monitor.antd.nist.gov](https://rpk-monitor.antd.nist.gov)

Jan-Feb 2024	9.8%
Mar-Apr 2024	19.6%
May-Jun 2024	17.6%
<b>Jul-Aug 2024</b>	<b>52.9%</b>

51 votes · Final results  
12:04 PM · Dec 15, 2023 · **1,907** Views

2 3 1 1

 **Doug Madory** · You  
Director of Internet Analysis at Kentik  
4mo · 🌐

Ok BGP/RPKI nerds... what's your prediction on when the majority of globally routed IPv4 routes will have ROAs?

IPv6 is already there according to <https://lnkd.in/efkMeP83> (cc: [Doug Montgomery](#))

Twitter/X version of this poll is here: <https://lnkd.in/eX9VqubD>

**When will the majority of IPv4 BGP routes have ROAs? (we're currently at 47.15% according to NIST)**  
You can see how people vote. [Learn more](#)

Jan-Feb 2024 ✓	0%
Mar-Apr 2024 ✓	9%
May-Jun 2024 ✓	18%
<b>Jul 2024 or later ✓</b>	<b>73%</b>

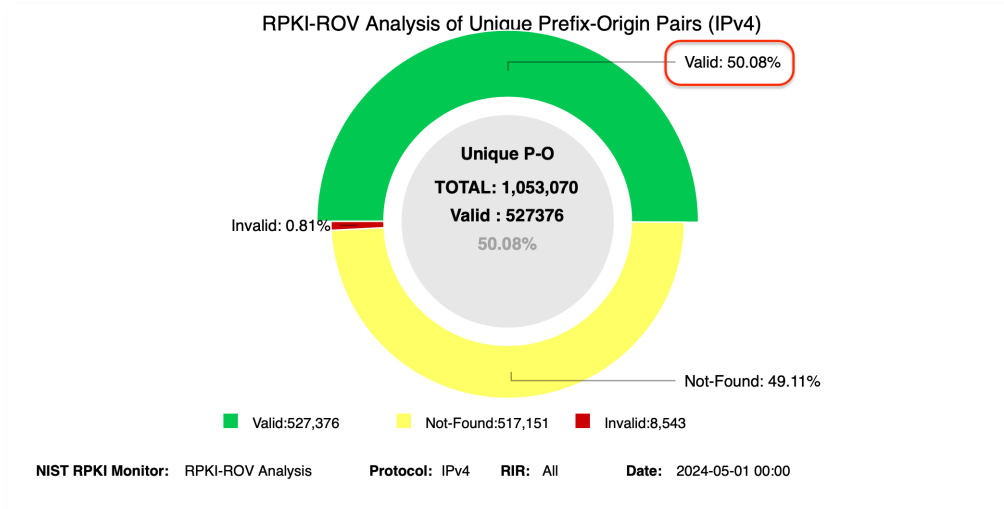
**55 votes** · Poll closed

8 1 comment · 1 repost



# Measuring RPKI deployment progress

- We recently passed a milestone (May 1):
  - >50% of IPv4 routes in global routing table have ROAs (NIST RPKI monitor)



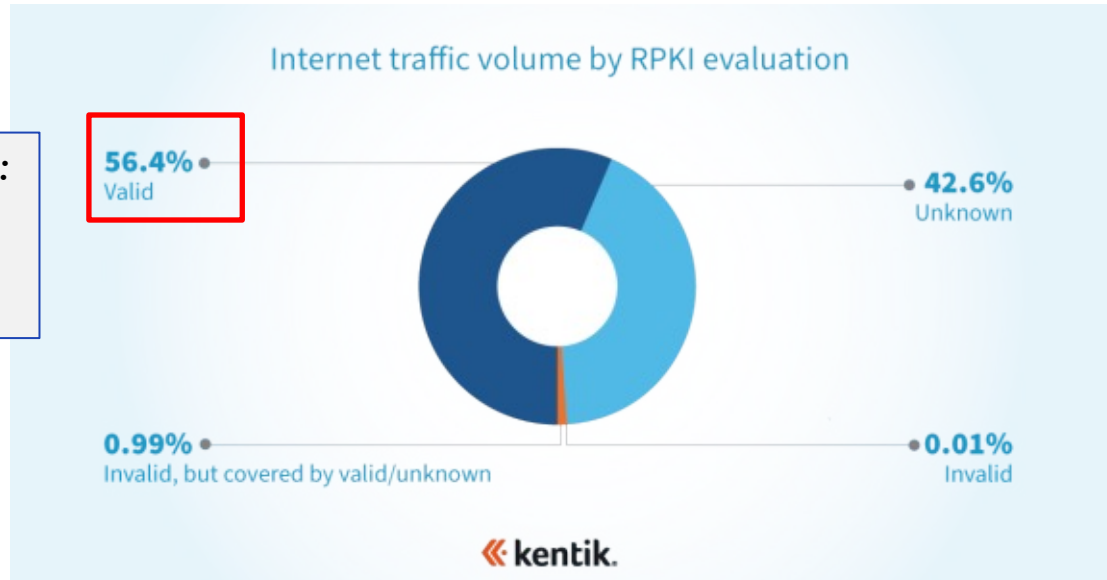
*IPv6 achieved this late last year*

# Measuring RPKI deployment progress

- But RPKI ROV is ultimately about protecting traffic, so ...
- At NANOG 84 in Austin, TX, we explored ROA creation (1.) using Kentik's aggregate NetFlow
  - 1/3 of BGP routes had ROAs, just >1/2 of traffic (bps) went to routes with ROAs

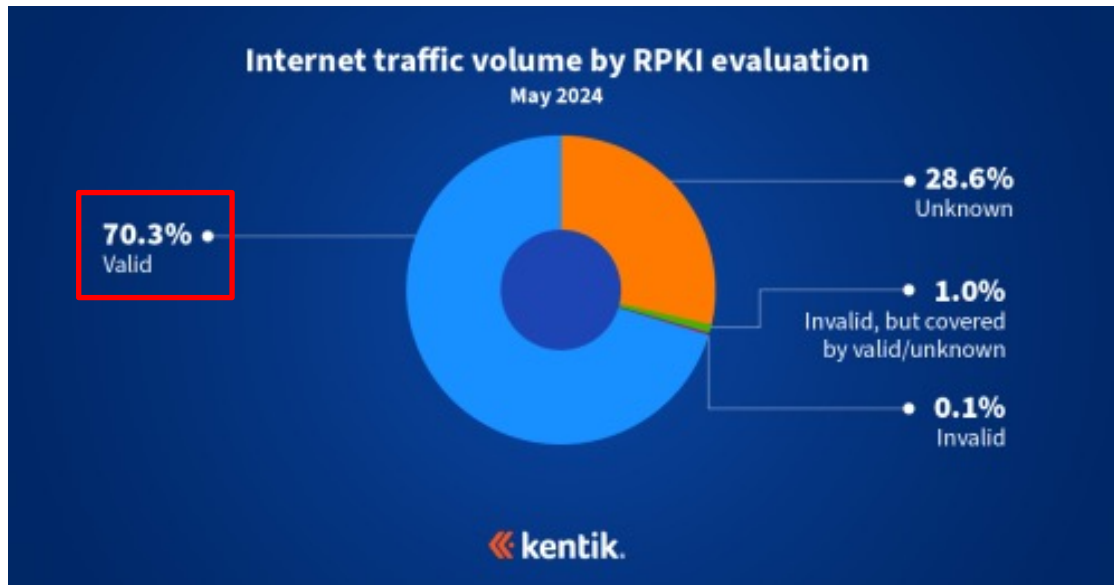
*Stats from Feb 2022:*

*How has this changed since?*



# Measuring RPKI deployment progress

- But RPKI ROV is ultimately about protecting traffic, so ...
- At NANOG 84 in Austin, TX, I explored ROA creation (1.) using Kentik's aggregate NetFlow
  - Feb 2022: 1/3 of BGP routes had ROAs, >1/2 of traffic (bps) went to routes with ROAs
  - Apr 2024: 1/2 of BGP routes have ROAs, >2/3 of traffic (bps) went to routes with ROAs

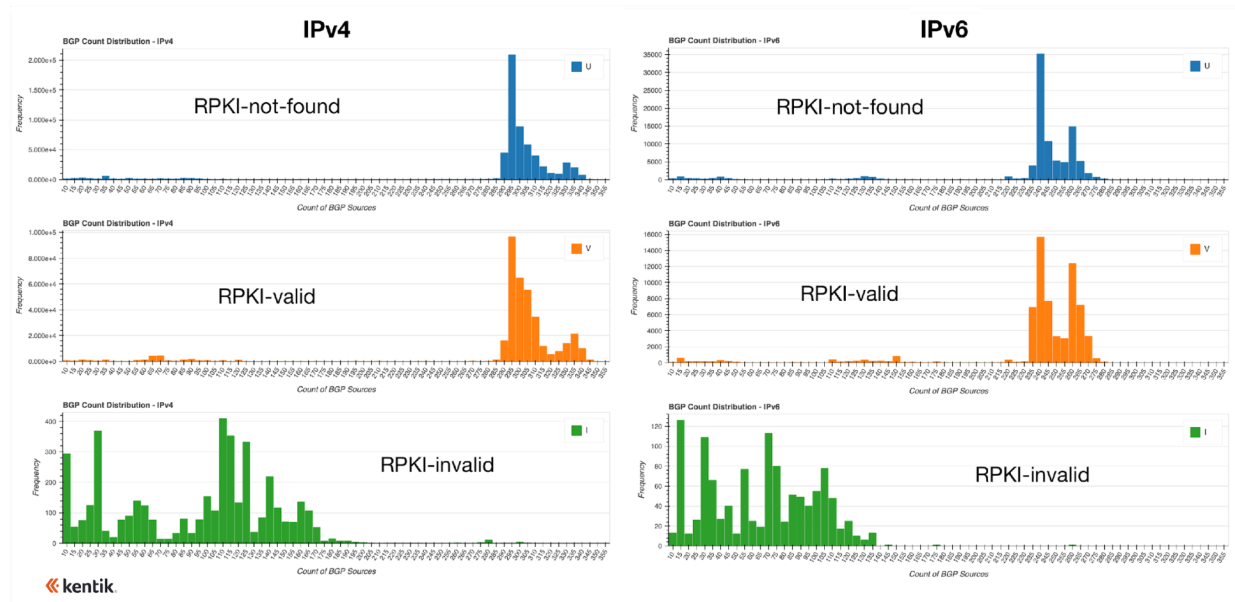


# Propagation Reduction of RPKI-Invalids

- ROAs alone are useless if only a few networks are rejecting invalid routes.
- 2022 analysis showed propagation of RPKI-invalid routes is half or less than other types.

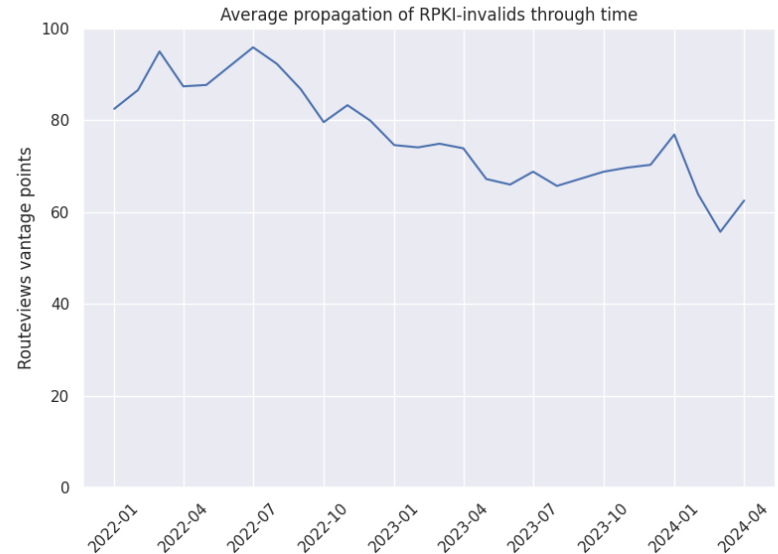
*Stats from Aug 2022*

*How has this changed since?*



# RPKI-Invalid Propagation Declining

- 24% decline in the propagation of RPKI-invalids
- Analyzing propagation of RPKI-invalid routes over time faces challenges:
  - Set of persistently RPKI-invalid routes not guaranteed to stay constant.
  - Propagation is heavily influenced by which providers are transiting a route.
- Does the trend hold for RPKI-invalid beacons?



# RPKI-Invalid Propagation Declining

- RIPE NCC and Job Snijders (AS15562) announce RPKI-invalid (and RPKI valid) routes for measurement of RPKI ROV deployment.
- Invalid routes from each of these beacons all experienced an overall decline in propagation while the control routes saw increased propagation.



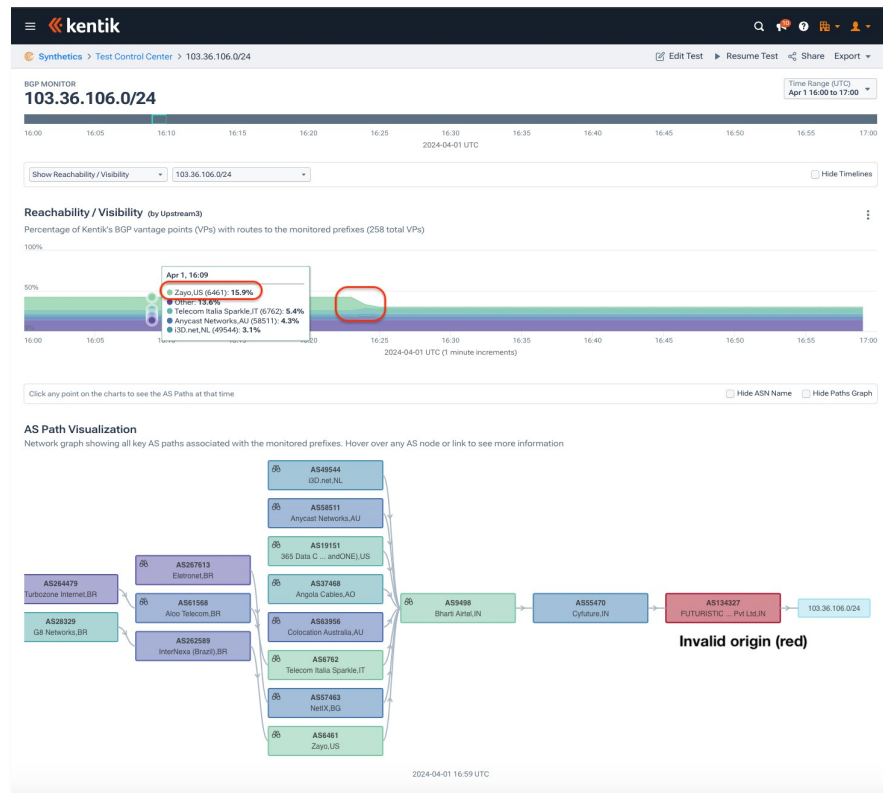
# Invalid Propagation Different for ARIN and RIPE

- Final observation:
  - Two RPKI-invalid routes in “Job’s Beacons” experience slightly different propagation.
- ROAs published in different RIR TALs:
  - 209.24.0.0/24 (green) is in the ARIN TAL
  - 194.32.71.0/24 (orange) is in the RIPE TAL
- Accepting the ARIN TAL requires a lengthy Relying Party Agreement that some providers refuse to accept.
- Result:
  - ROAs published by ARIN are seen by fewer networks.
  - Slightly reducing the efficacy of RPKI ROV for ARIN managed IP space.



# Another Tier-1 AS Rejecting RPKI-Invalids

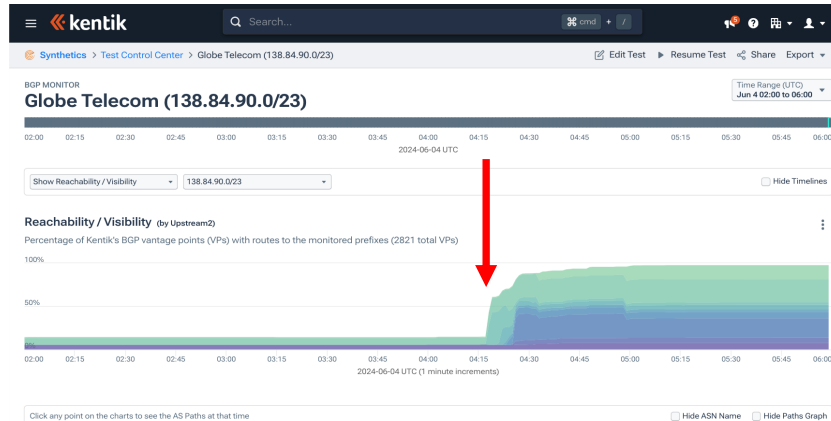
- Much of the reduction of propagation of RPKI-invalid routes is due to the rejection of invalids by Tier-1 (DFZ) ASes.
- Another RPKI milestone in April:
  - An additional Tier-1 AS began rejecting RPKI-invalid routes from customer networks.
  - On April 1 at 16:24 UTC, we saw Zayo (AS6461) begin rejecting RPKI-invalid routes.





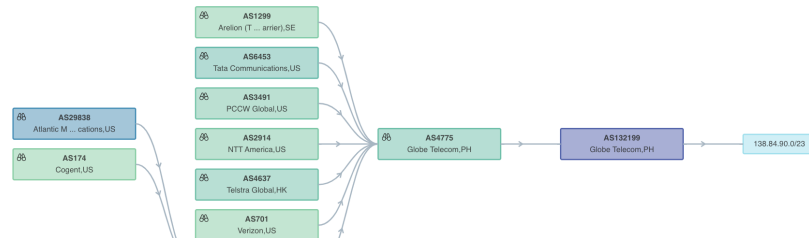
# Fixing ROA misconfigurations

- Globe Telecom (PH) recently fixed several ROAs causing routes to be RPKI-invalid.

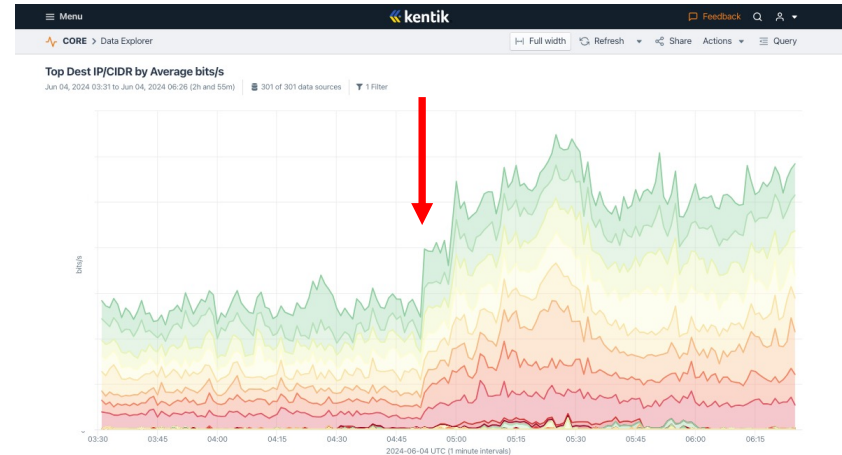


## AS Path Visualization

Network graph showing all key AS paths associated with the monitored prefixes. Hover over any AS node or link to see more information



*Traffic volume to previously RPKI-invalid routes increased.*



# Coming back to the Orange España hack

- Hacker gained access to Orange España's RIPE NCC account and altered RPKI configuration, rendering many of its BGP routes RPKI-invalid.
- The wielding of RPKI as a tool for denial of service was only possible due to the pervasive extent to which ASes reject RPKI-invalid routes.



<https://www.kentik.com/blog/digging-into-the-orange-espana-hack/>



Thank you!

Jac Kloots  
jac@kentik.com

 @jkloots

 in/jackloots

