New Milestones in RPKI ROV Adoption

Jac Kloots (Kentik)

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”

Seleccione: AMÉRICA

SUSCRÍBETE INICIAR SESIÓN

EL PAÍS

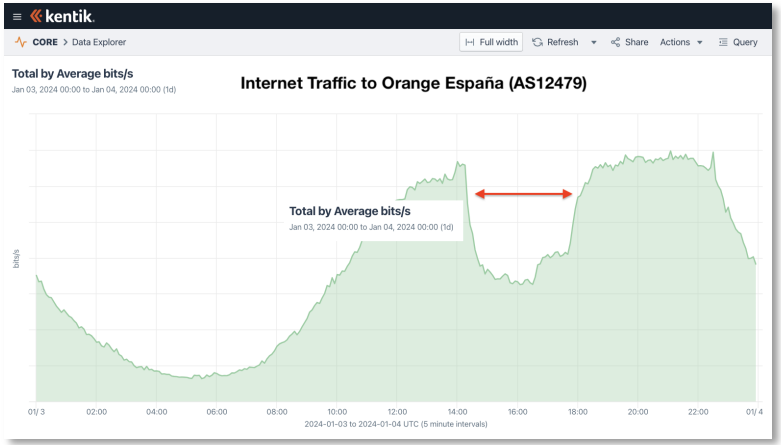
Tecnología

TU TECNOLOGÍA · CIBERSEGURIDAD · PRIVACIDAD · INTELIGENCIA ARTIFICIAL · INTERNET · GRANDES TECNOLÓGICAS · ÚLTIMAS NOTICIAS

INTERNET >

Orange sufre una caída del servicio de Internet en toda España por culpa de un ciberataque

La compañía reconoce un “acceso indebido” que no habría comprometido los datos de sus clientes y avisa de que el servicio está “prácticamente restablecido”



Orange España

@orange_es

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

Translated from Spanish by Google

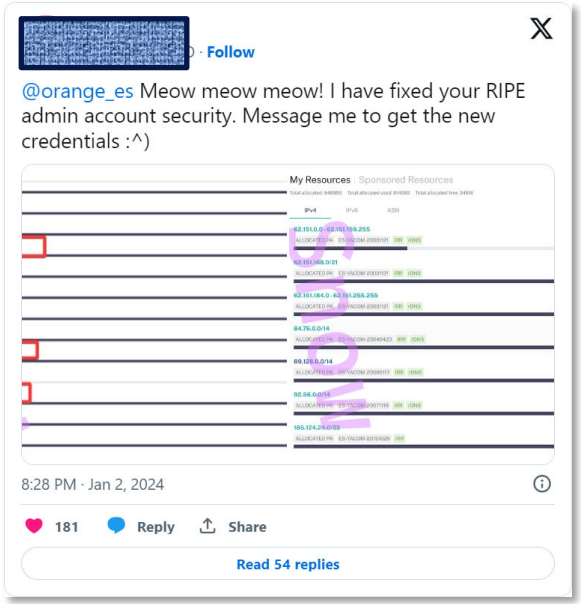
We have detected a widespread incident with our service nationwide, but fortunately it has been detected very quickly (thanks in large part to all your comments and warnings) and we are already working to solve it as soon as possible. 1/2

12:49 PM · Jan 3, 2024 · **583** Views

2 2

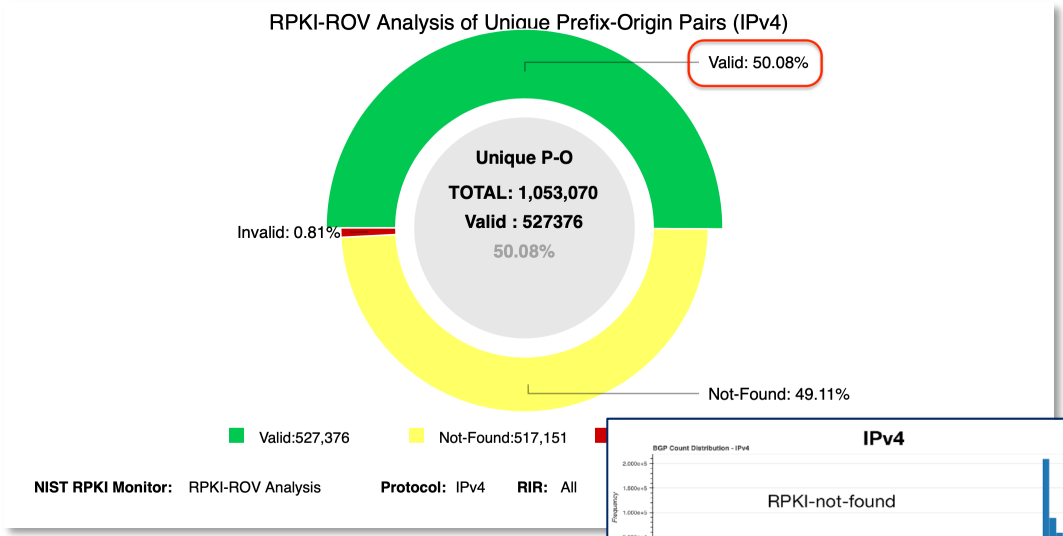
Why did Orange España suffer an outage?

- 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.

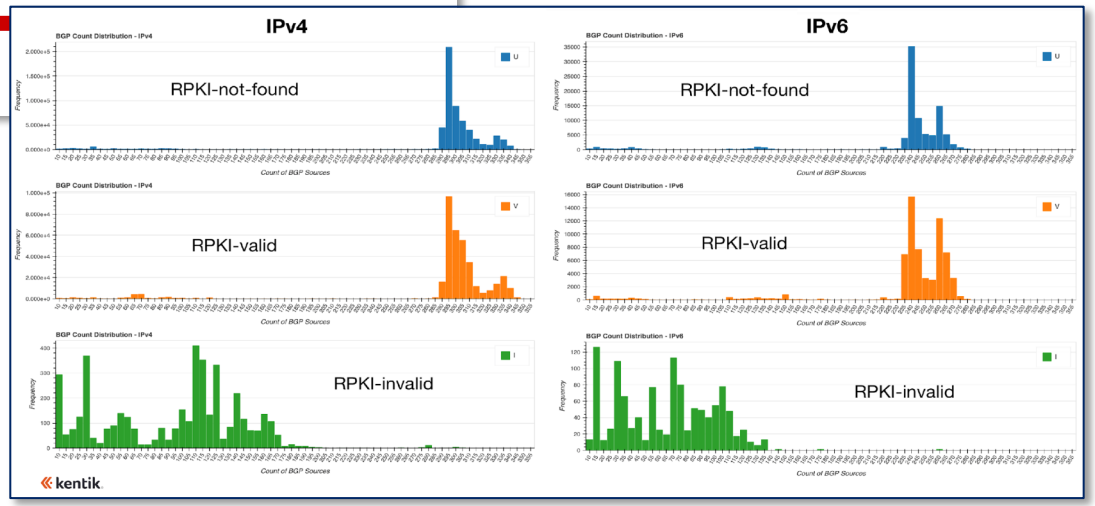


But to really understand the significance of the outage, we must understand RPKI and the state of BGP security

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



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

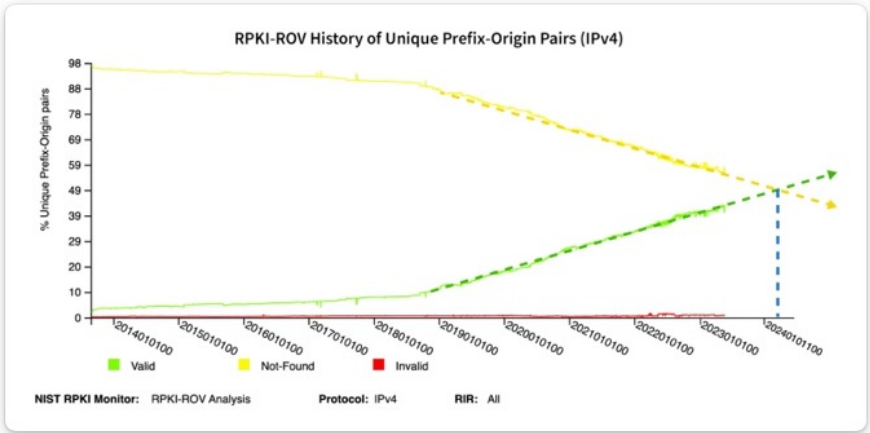
2

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

ROA Creation Predictions

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

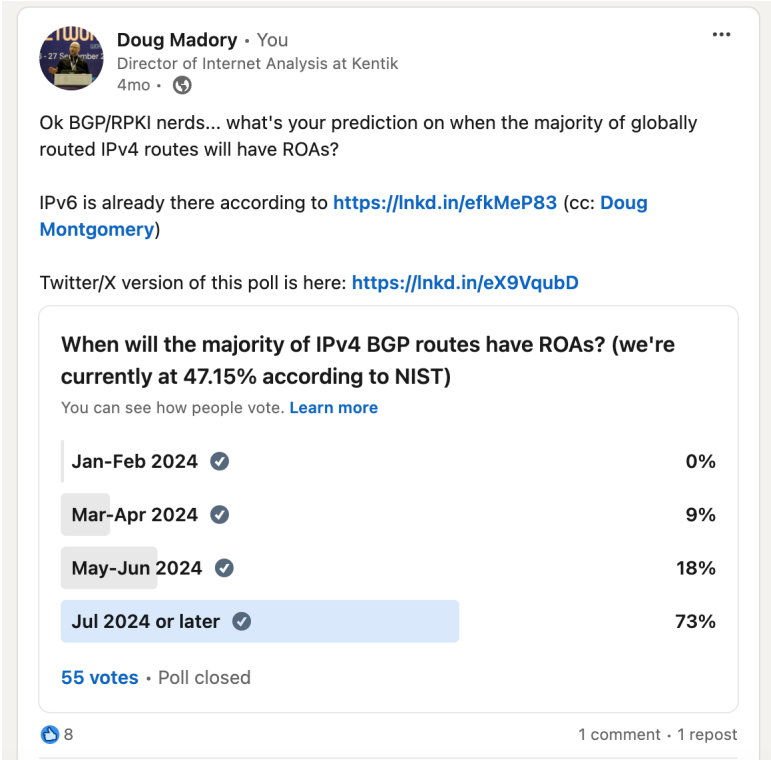
If we are to assume steady growth of the share of BGP routes with ROAs, it should become the majority case in about a year from now (May 2024). Mark your calendars!



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

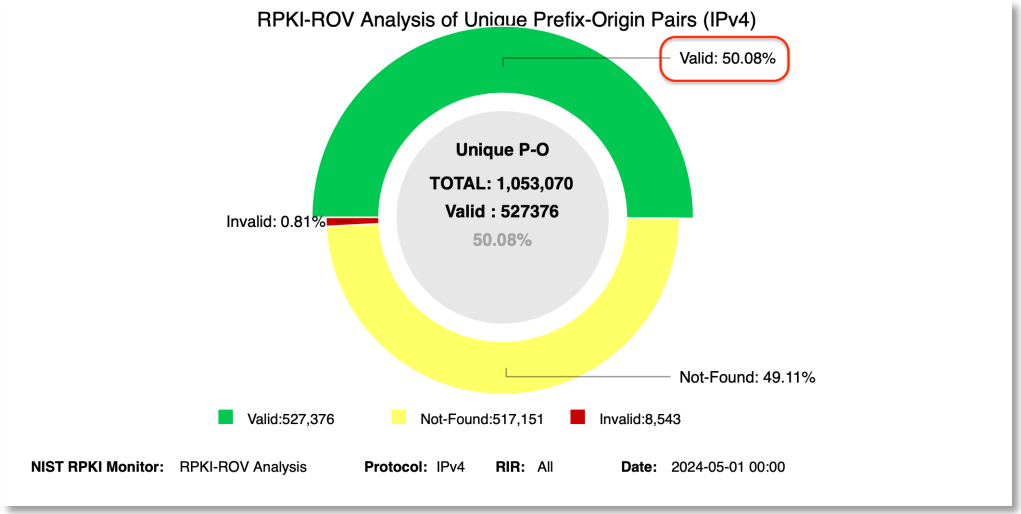
ROA Creation Predictions

- But y’all were doubters!



Measuring RPKI deployment progress

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



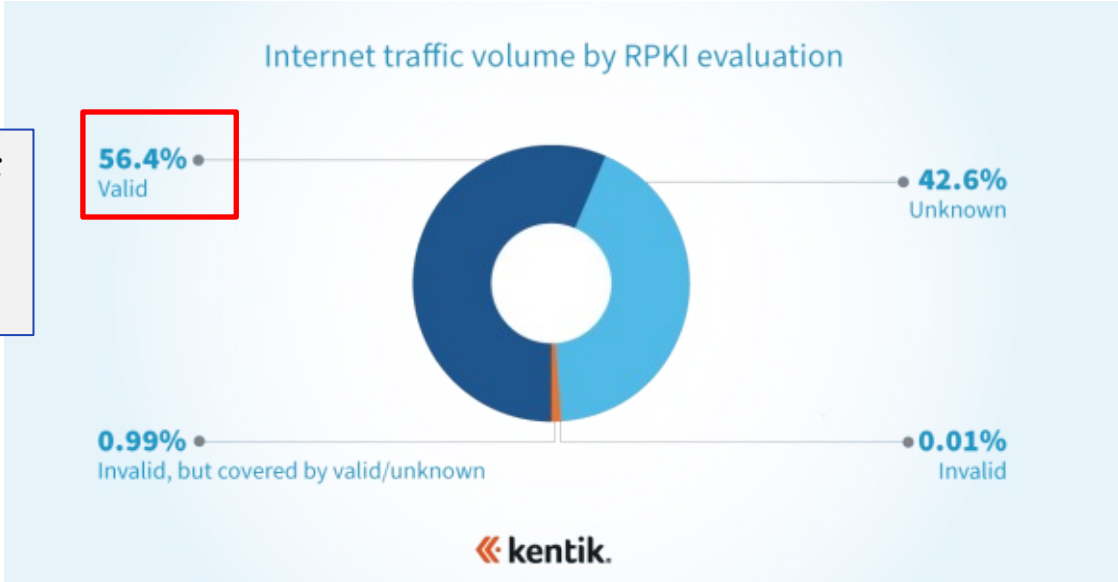
IPv6 achieved this late last year

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

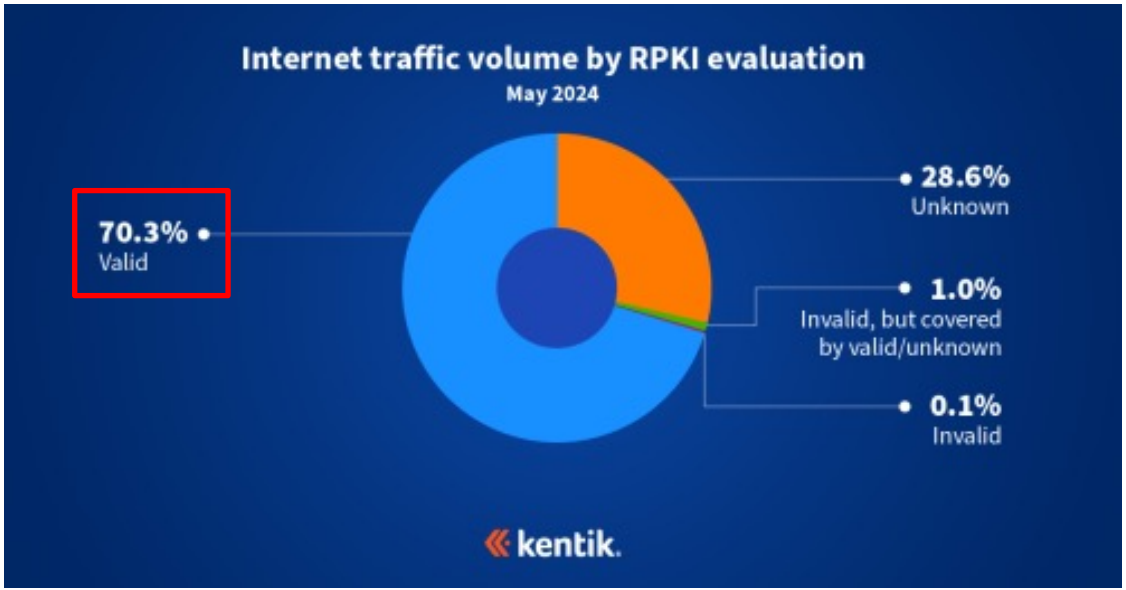
Stats from Feb 2022:

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

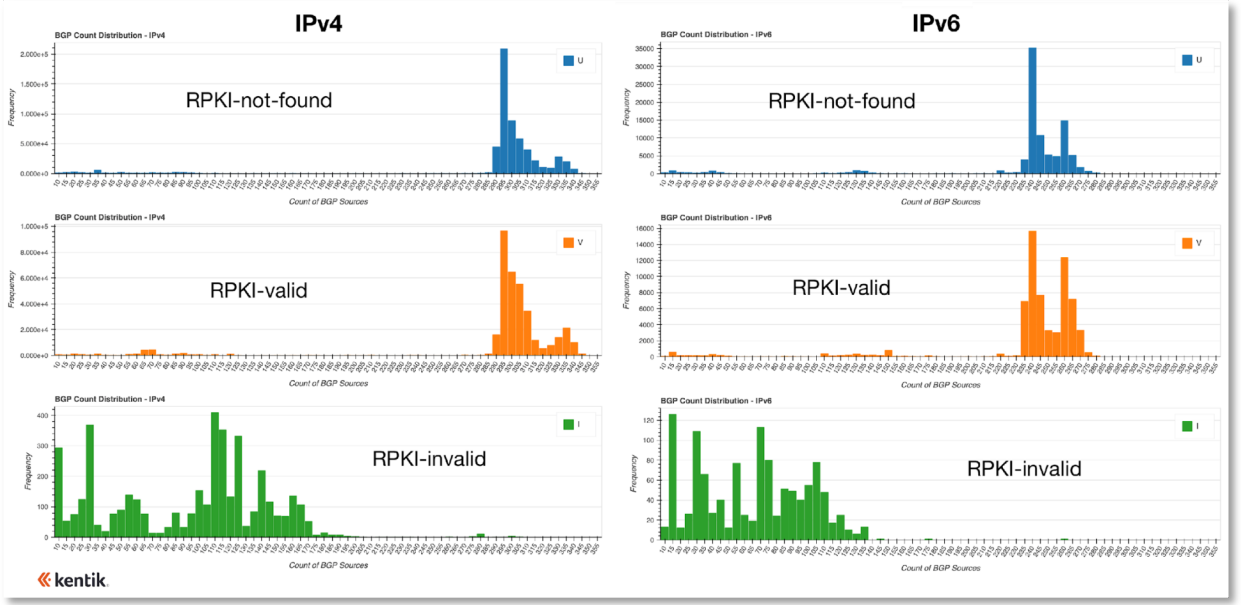


Propagation Reduction of RPKI-Invalids

- 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

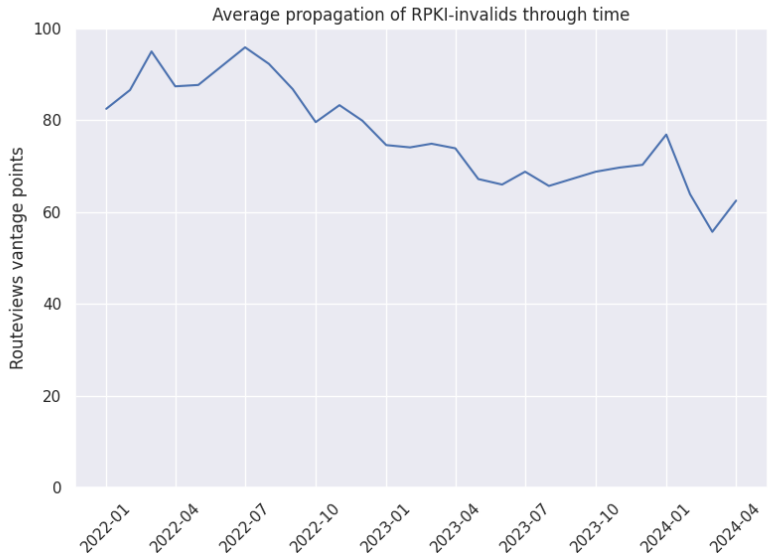
How has this changed since?



https://www.kentik.com/blog/how-much-does-rpki-rov-reduce-the-propagation-of-invalid-routes/

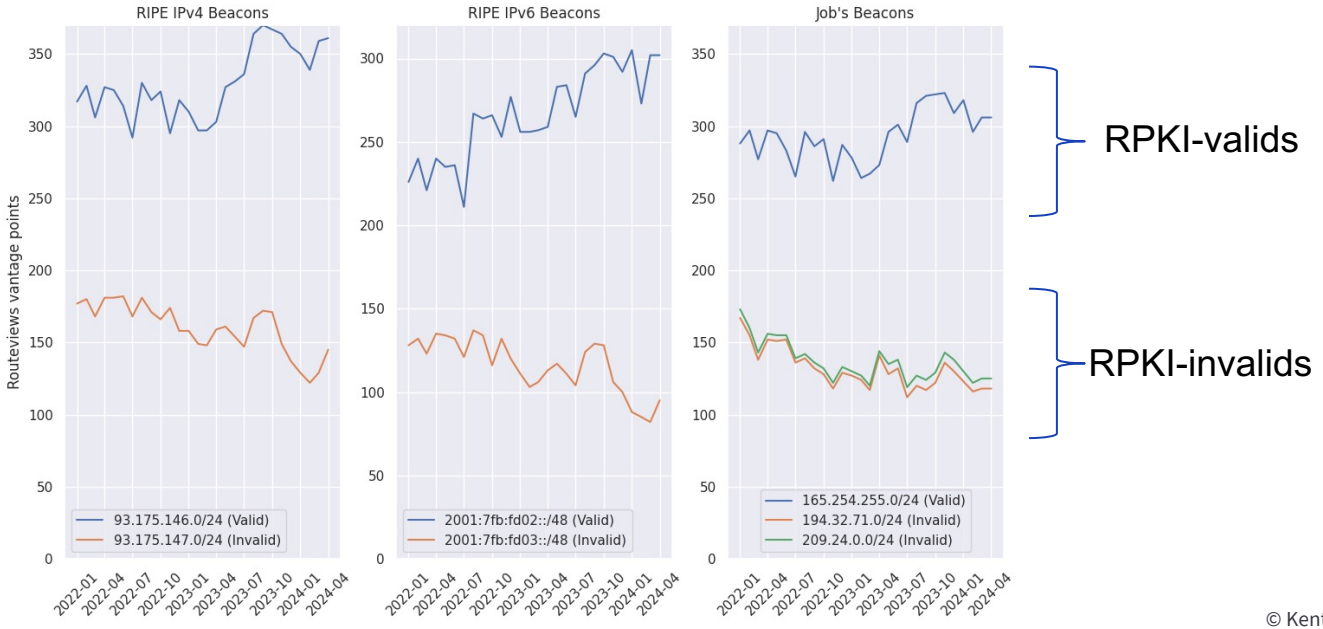
RPKI-Invalid Propagation Declining

- 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.

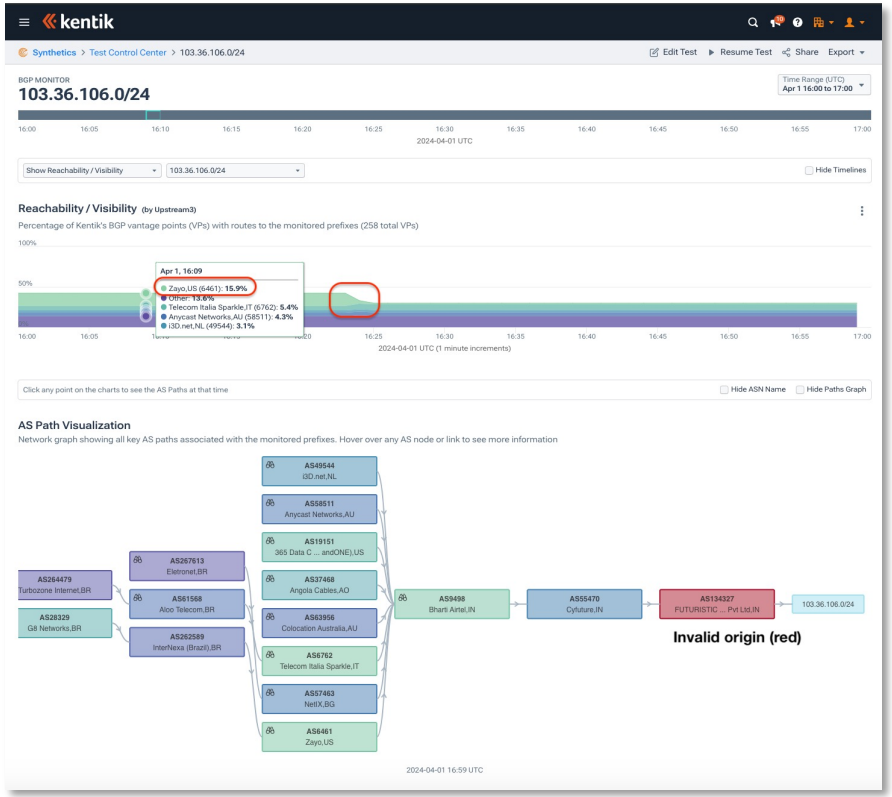


Invalid Propagation Different for ARIN and RIPE

- 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.

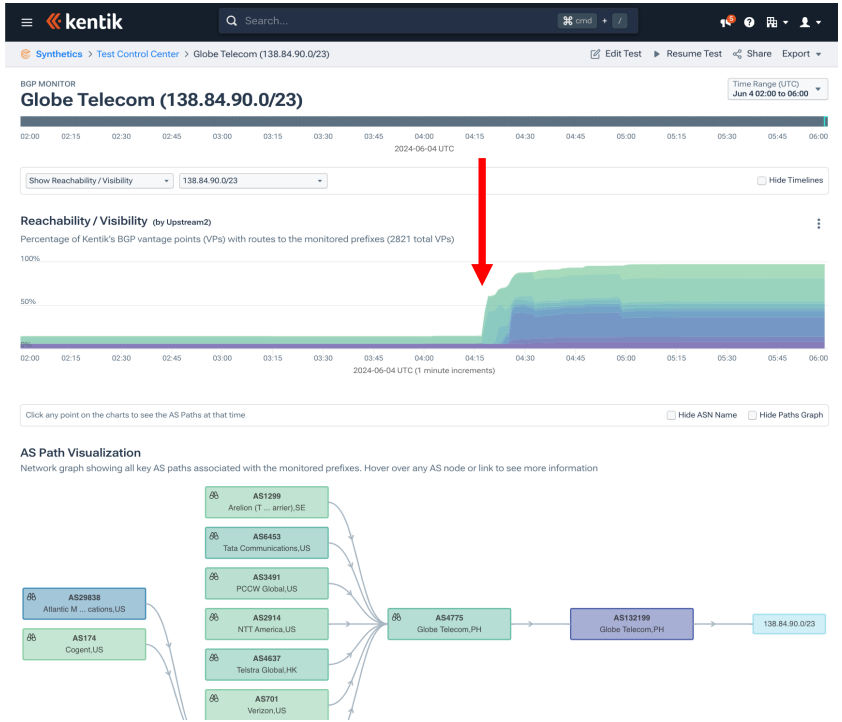
Another Tier-1 AS Rejecting RPKI-Invalids

- 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.

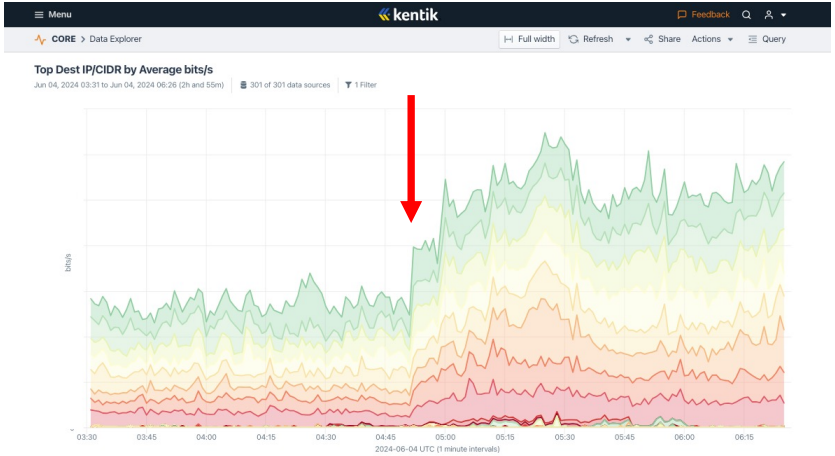


Fixing ROA misconfigurations

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

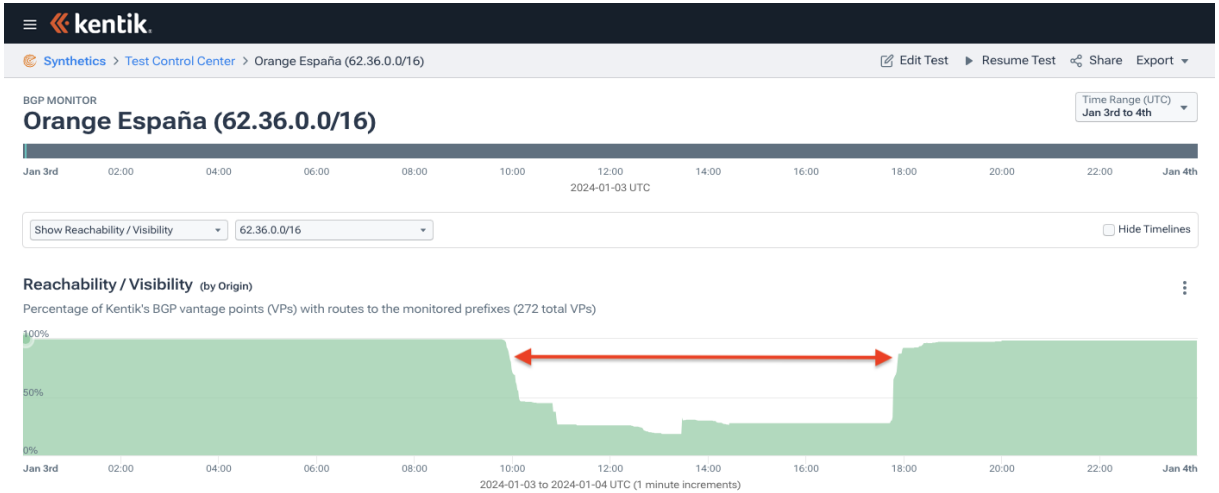


Traffic volume to previously RPKI-invalid routes increased.



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/

kentik

Thank you!

Jac Kloots
jac@kentik.com

@jkloots
in/jackloots