

The Internet's Biggest BGP Incidents

A Brief History

Nina Bargisen



Who am I ?

Current

Evangelizer and SP expert - [Kentik](#)

Past

20 years in networking
built networks, engineered traffic and ran peering and
interconnection and partner engagement

More details

 [/in/ninabargisen](#)

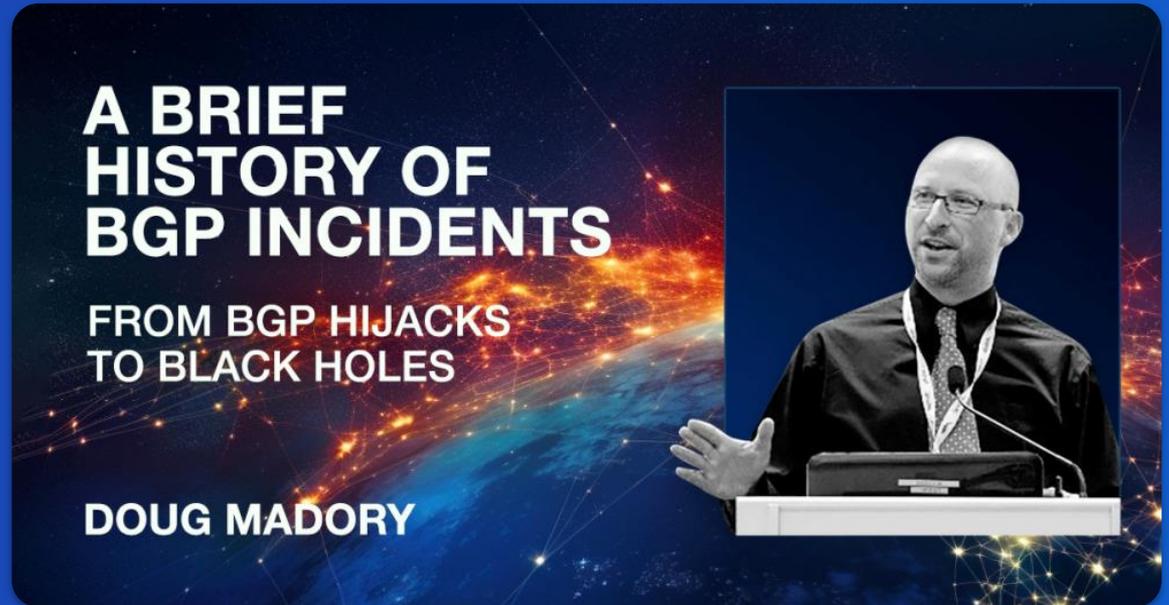
Credit Where Due

Talk based on the work of Doug Madory, “The Man Who Sees the Internet”

 [@DougMadory](https://twitter.com/DougMadory)

 [/in/dougmadory](https://www.linkedin.com/in/dougmadory)

Great resource to follow on social media for news on this topic.



**A BRIEF
HISTORY OF
BGP INCIDENTS**

**FROM BGP HIJACKS
TO BLACK HOLES**

DOUG MADORY

The graphic features a dark blue background with a glowing network of orange and yellow nodes and lines, resembling a globe or a complex network. On the right side, there is a black and white photograph of Doug Madory, a man with glasses, wearing a dark suit and tie, speaking at a podium with a microphone. The text is overlaid on the left side of the graphic.

BGP Incident Definitions

Hijacks

- *Prefix hijacking happens when a network, whether intentionally or mistakenly, originates a prefix that belongs to another network without its permission. [MANRS]*
- Presumes malicious intent
- Generally used to describe an illegitimate origination of a prefix

Route Leaks

- *A route leak is the propagation of routing announcement(s) beyond their intended scope. [RFC7908]*
- Often occur accidentally due to configuration errors
- Malicious actors may also attempt to hide attacks as a leak
- Generally used to describe a leak of prefixes upstream for the legitimate origin of the prefix

Even experts debate the definitions

Definitions for Our Purposes

Origination Errors

- Occurs when an AS originates (announces with its ASN as the origin) a new advertisement of a route to an IP address block over which it does not possess legitimate control
- Solicits traffic destined to those IP addresses to the new ASN

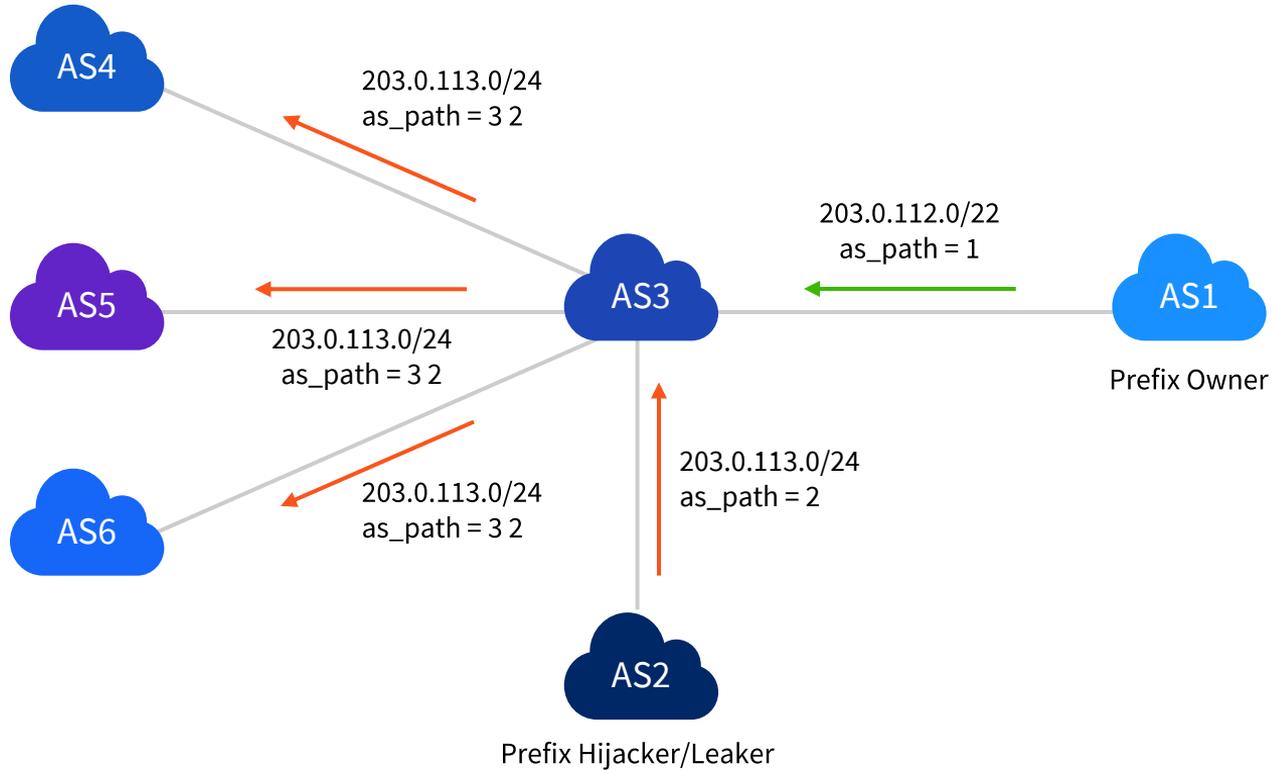
AS Path Errors

- Occurs when an AS inserts itself as an illegitimate intermediary into the forwarding path of traffic bound for a different destination
- Traffic may still reach its ultimate destination, albeit along a sub-optimal path

IP Squatting

- Occurs when an AS announces IP address ranges that are normally unrouted on the global Internet
- Typically for the purpose of evading IP-based blocklists and complicating attribution

Origination Error

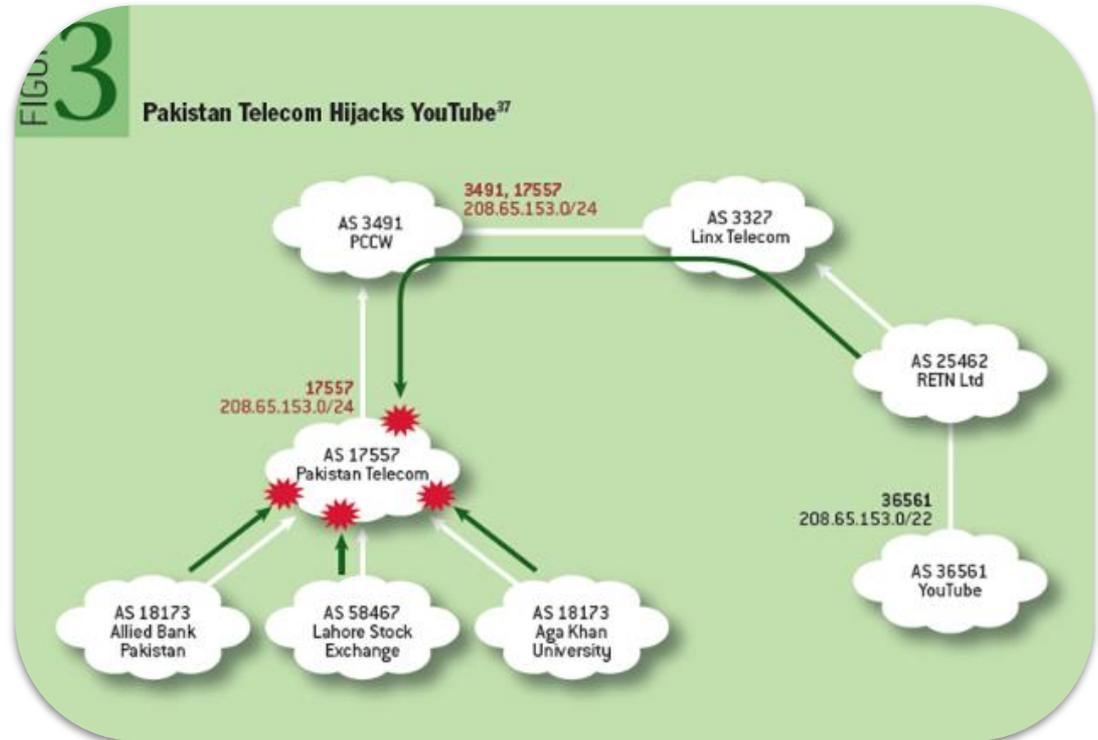


Pakistan Telecom Hijack of YouTube (2008)

- Government of Pakistan ordered access to YouTube to be blocked in the country due to a video it deemed anti-Islamic
- Pakistan Telecom intended to blackhole traffic inside their network
- Leaked it to their upstream providers

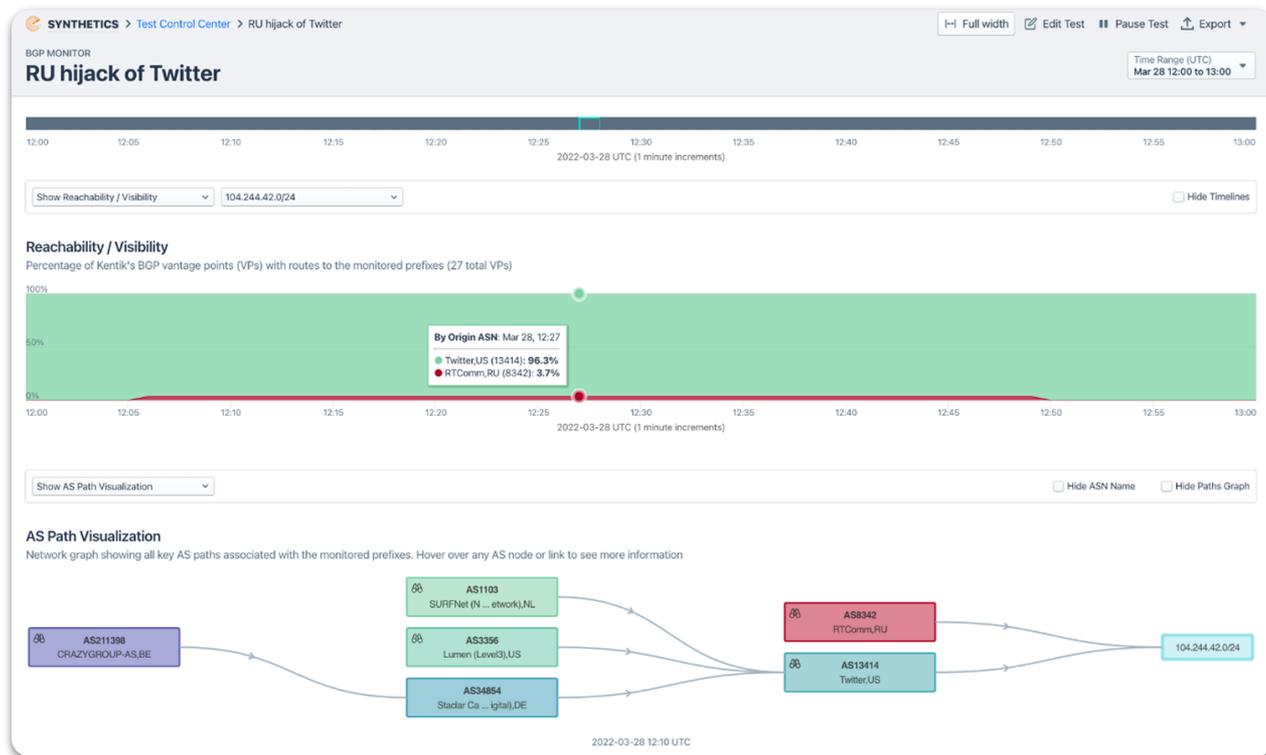
Image source:

<https://dl.acm.org/doi/fullHtml/10.1145/2668152.2668966>

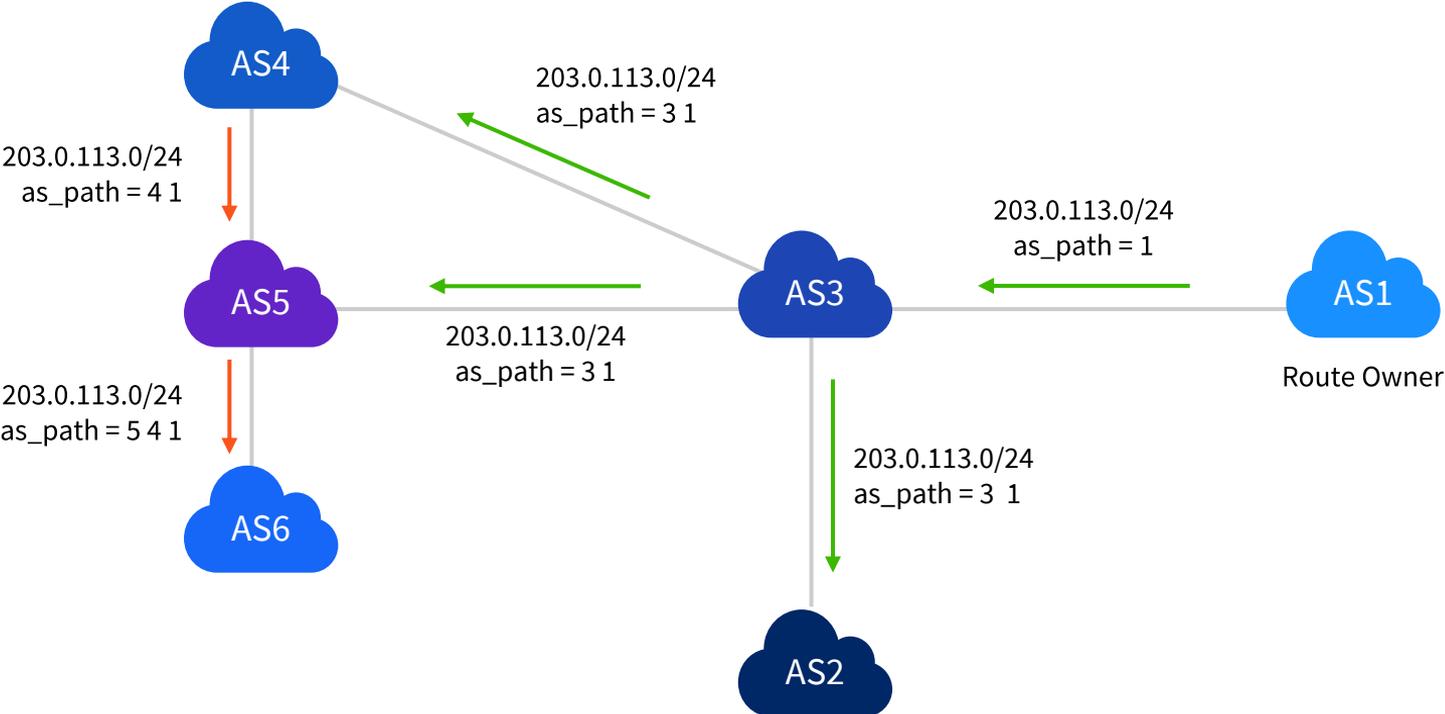


Russian Hijack of Twitter (2022)

- Twitter prefix (104.244.42.0/24) announced by Russian Telecom RTComm during the Russian invasion of the Ukraine
- Same prefix was hijacked during the military coup in Myanmar in 2021
- Less propagation this time due to RPKI ROA



AS Path Error

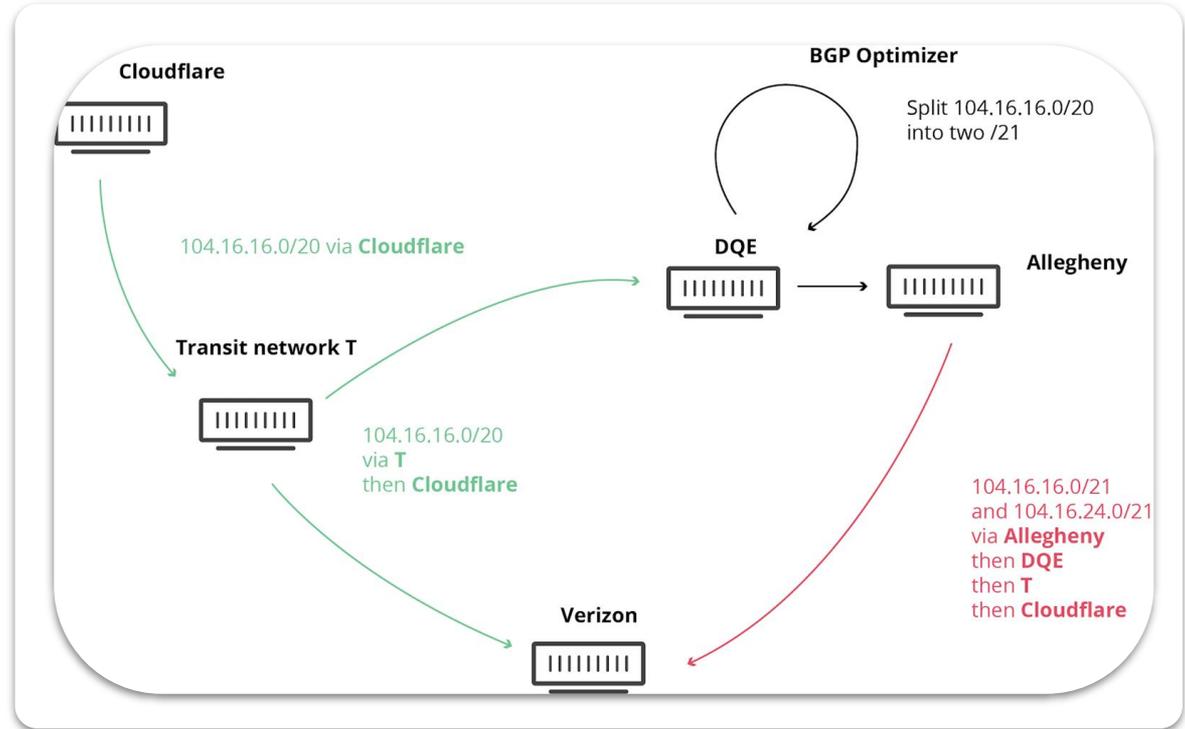


AS7007 Incident (1997)

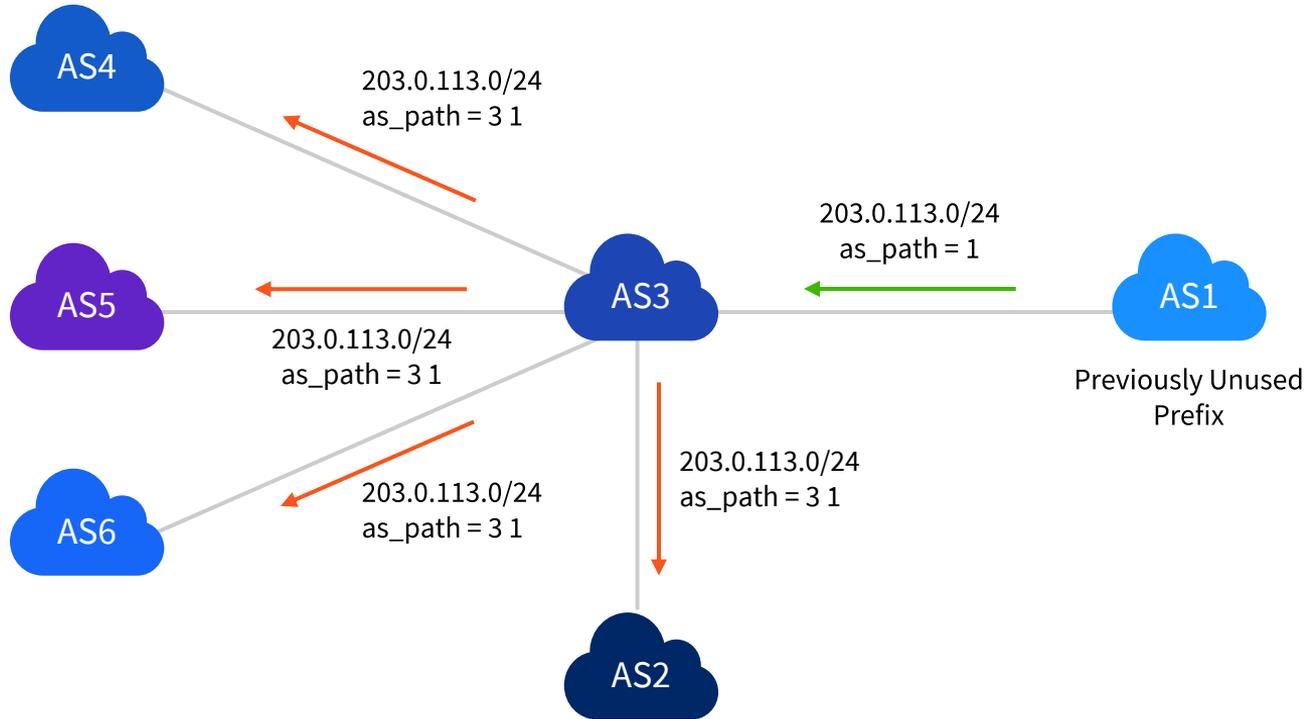
- The OG of BGP Incidents
- Code bug caused a router inside AS7007 (MAI Network Services) to leak routes to the Internet
- Existing prefixes de-aggregated to /24 prefixes and originated from AS7007
- Routes remained even after the originating router had been taken offline

Allegheny Leak (2019)

- BGP Optimizer inside DQE split $104.16.16.0/20$ into two $/21$ prefixes
- Advertised those routes to their customer, Allegheny
- Allegheny in turn advertised upstream to Verizon
- BGP prefers a $/21$ over a $/20$ so all of the Internet connected to Verizon preferred the route through DQE

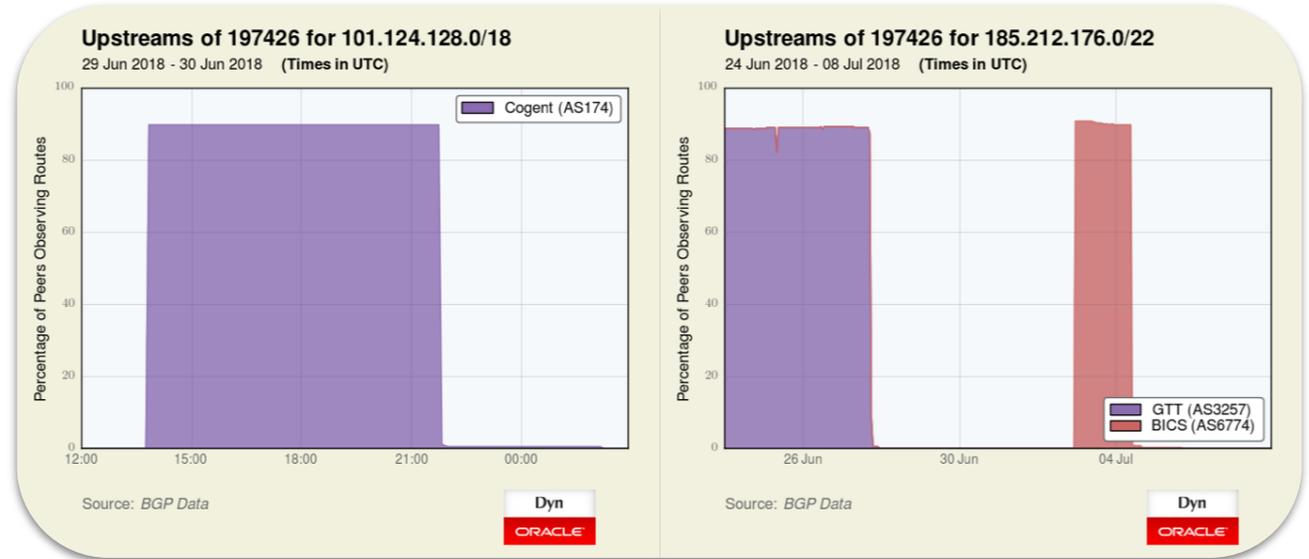


IP Squatting



Bitcanal

- IP Squatting on 101.124.128.0/18 until Cogent disconnected them
- Then moved to 185.212.176.0/22 via GTT and BICS
- Used IPs as source of spam to avoid IP Blacklist



Impact of a BGP Incident



Disrupt the flow of legitimate internet traffic



Nation state control on flow of information



Misdirection of communications



Security risk from interception or manipulation



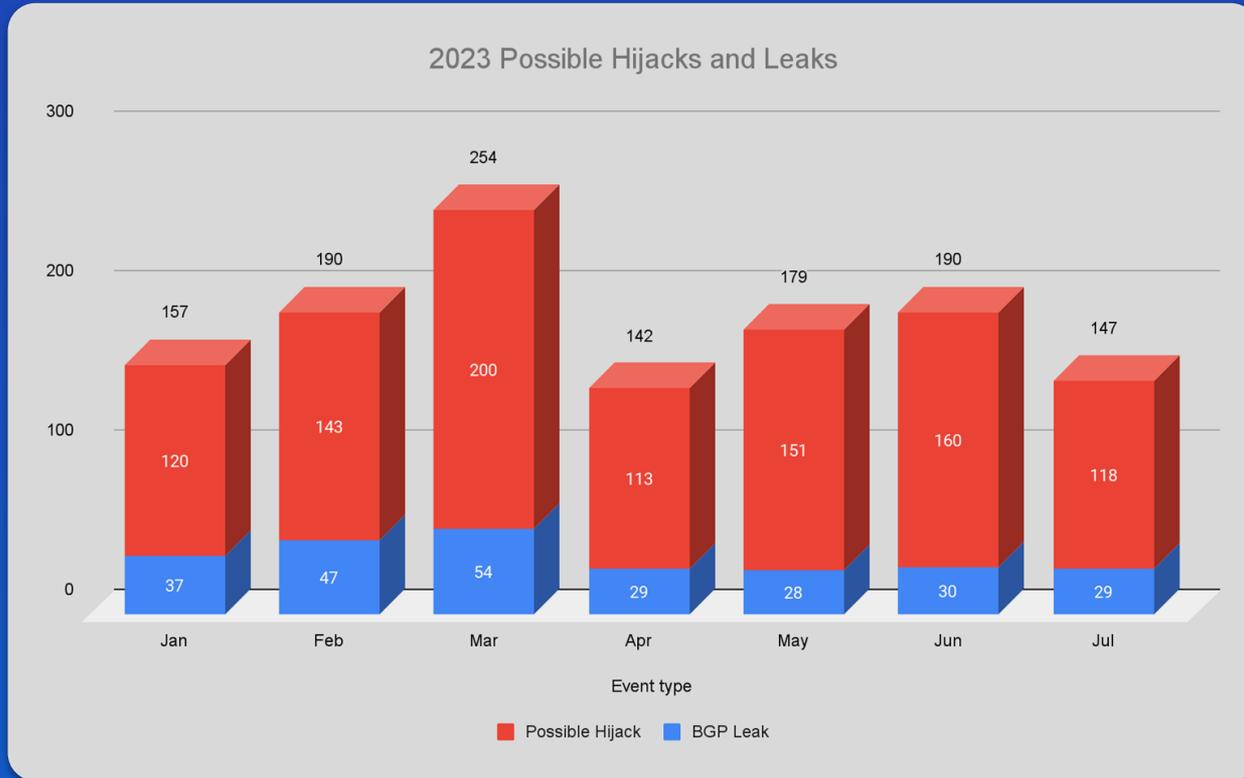
Attacks on cryptocurrency services



BGP session flaps

Not covered here but unknown BGP attributes also affect the stability of the global routing table

Frequency



Source: <https://bgpstream.com>

What can operators do?



Watch BGP monitoring solutions to respond quickly



RPKI ROV by creating ROAs for your prefixes

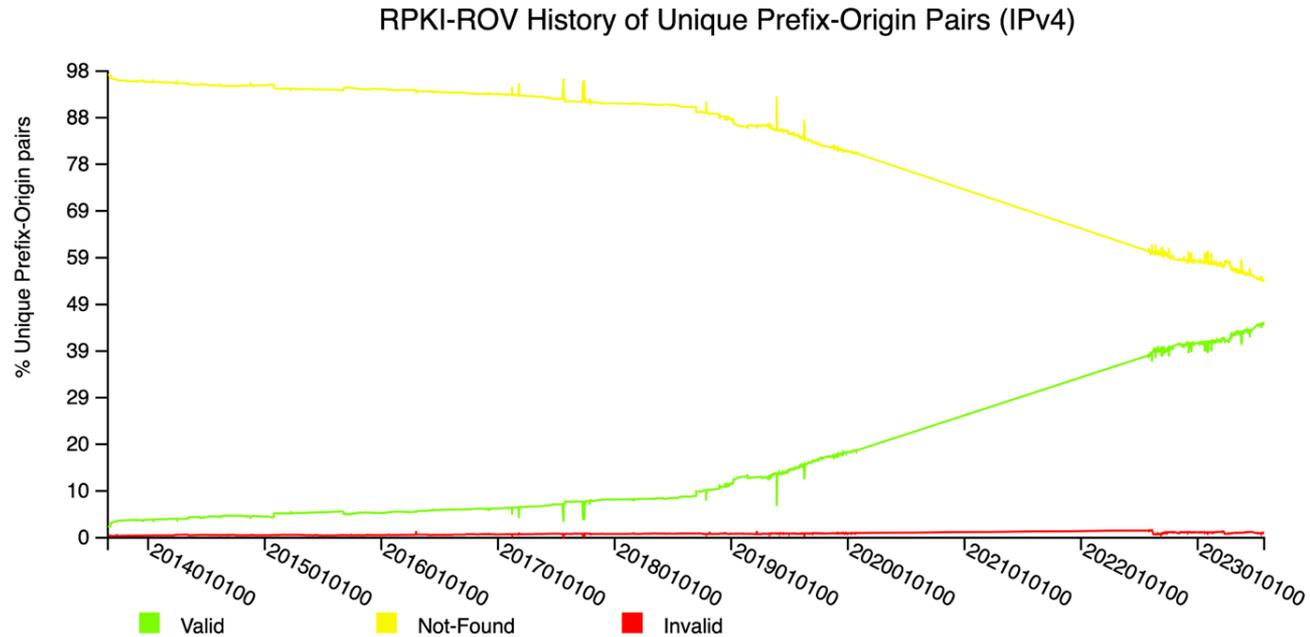


Configure your routers to reject RPKI Invalid routes



Mutually Agreed Norms for Routing Security (MANRS)

We are making progress



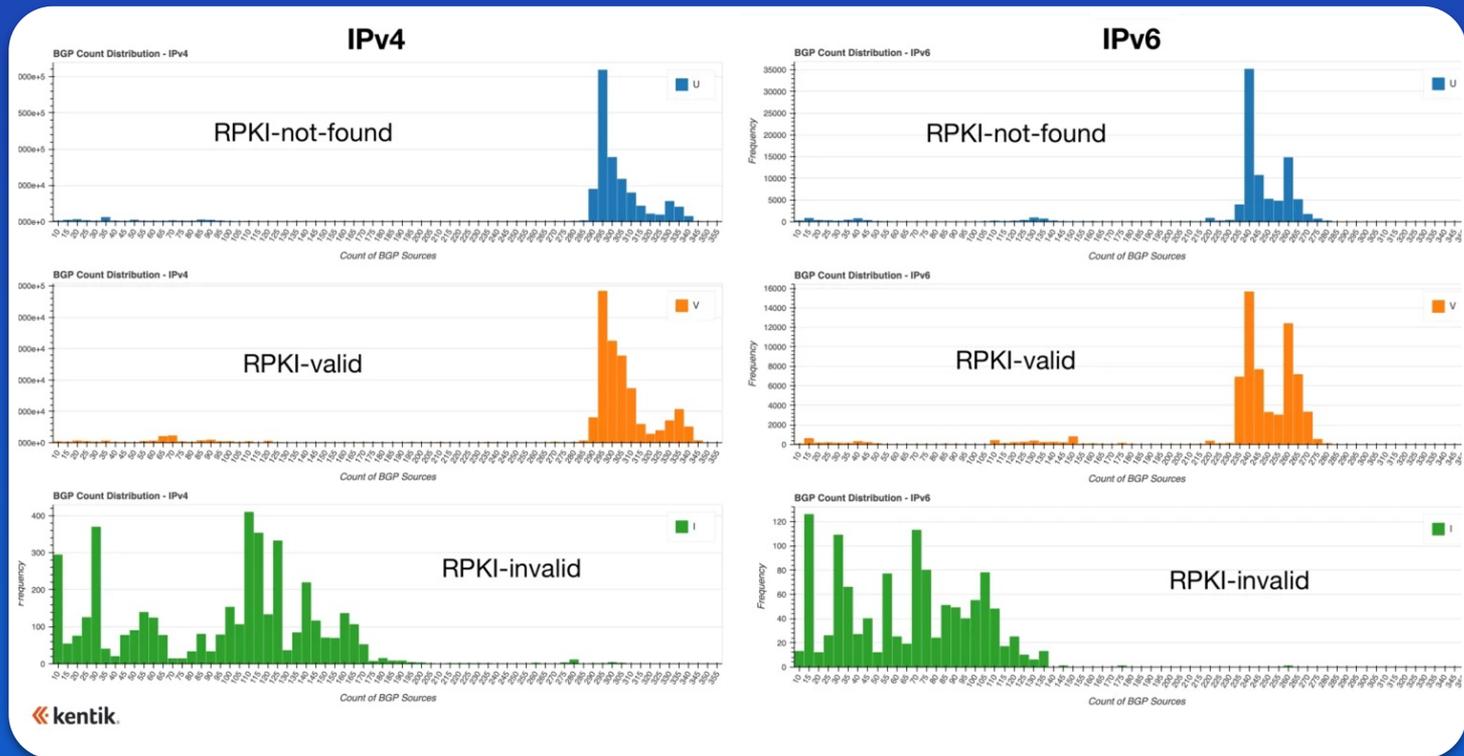
NIST RPKI Monitor: RPKI-ROV Analysis

Protocol: IPv4

RIR: All

Source: <https://rpki-monitor.antd.nist.gov/>

We are making progress



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

Additional Resources

- A Brief History of the Internet's Biggest BGP Incidents - <https://www.kentik.com/blog/a-brief-history-of-the-internets-biggest-bgp-incidents/>
- AS7007 Incident - https://en.wikipedia.org/wiki/AS_7007_incident
- Pakistan's Accidental YouTube Re-Routing Exposes Trust Flaw in Net - <https://www.wired.com/2008/02/pakistans-accid/>
- How Verizon and a BGP Optimizer Knocked Large Parts of the Internet Offline Today - <https://blog.cloudflare.com/how-verizon-and-a-bgp-optimizer-knocked-large-parts-of-the-internet-offline-today/>
- Some Twitter traffic briefly funneled through Russian ISP, thanks to BGP mishap - <https://arstechnica.com/information-technology/2022/03/absence-of-malice-russian-isps-hijacking-of-twitter-ips-appears-to-be-a-goof/>
- Shutting Down the BGP Hijack Factory - <https://blog.apnic.net/2018/07/12/shutting-down-the-bgp-hijack-factory/>
- MANRS - <https://www.manrs.org/>
- How much does RPKI ROV reduce the propagation of invalid routes? - <https://www.kentik.com/blog/how-much-does-rpki-rov-reduce-the-propagation-of-invalid-routes/>
- Exploring the Latest RPKI ROV Adoption Numbers - <https://www.kentik.com/blog/exploring-the-latest-rpki-rov-adoption-numbers/>
- Problem Definition and Classification of BGP Route Leaks - <https://www.ietf.org/rfc/rfc7908.txt>
- BGP Operations and Security - <https://www.ietf.org/rfc/rfc7454.txt>
- Autonomous System Provider Authorization (ASPA) - <https://www.ietf.org/archive/id/draft-ietf-sidrops-aspa-verification-15.txt>
- Unknown Attribute 23 - <https://labs.ripe.net/author/emileaben/unknown-attribute-28-a-source-of-entropy-in-interdomain-routing>

Questions?



Thank you!

Nina Bargisen
nina@kentic.com

 [Join Kentik on Slack](#)

