infoblox®

THE BGP ANALYST'S NOTEBOOK
17 YEARS IN

DOUG MADORY

HEAD OF INTERNET ANALYSIS, INFOBLOX

About Me



- Native of Poughkeepsie, New York
  - Father was an engineer at IBM.
  - Mother was a journalism major.
- Attended Univ. of Virginia on ROTC scholarship.
- Later Dartmouth for a master's degree.

About Me

- 5+ years as a communications engineer in US Air Force



NATO Air Meet (Sep 2003)
Poznan, Poland



Al Udeid Air Base, Qatar (Mar 2004)
(following deployment to Iraq)

infoblox

About Me





- Started work on BGP analysis in 2009
- Renesys (small startup working on Internet measurement)
  - Dyn Research after acquisition by Dyn (2014)
  - Oracle Internet Intelligence after acquisition by Oracle (2017)
- Kentik (since 2020)
  - Acquired by Infoblox (Aug 2026)



infoblox

Doug’s approach to BGP analysis

How do we turn this into insight about routing?

```
BGP4MP_ET|1790922002.441565|A|123.108.8.111|7597|103.158.56.0/24|17884 17884|IGP|123.108.8.132|0|0||NAG||
BGP4MP_ET|1790922002.441565|A|123.108.8.111|7597|103.158.57.0/24|17884 17884|IGP|123.108.8.132|0|0||NAG||
BGP4MP_ET|1790922002.441565|A|123.108.8.111|7597|103.174.234.0/24|17884 17884|IGP|123.108.8.132|0|0||NAG||
BGP4MP_ET|1790922002.441565|A|123.108.8.111|7597|103.174.235.0/24|17884 17884|IGP|123.108.8.132|0|0||NAG||
BGP4MP_ET|1790922003.120238|A|123.108.9.111|7597|103.155.250.0/24|17884 17884|IGP|123.108.8.132|0|0||NAG||
BGP4MP_ET|1790922003.120238|A|123.108.9.111|7597|103.155.251.0/24|17884 17884|IGP|123.108.8.132|0|0||NAG||
BGP4MP_ET|1790922003.120238|A|123.108.9.111|7597|103.158.56.0/24|17884 17884|IGP|123.108.8.132|0|0||NAG||
BGP4MP_ET|1790922003.120238|A|123.108.9.111|7597|103.158.57.0/24|17884 17884|IGP|123.108.8.132|0|0||NAG||
BGP4MP_ET|1790922003.120238|A|123.108.9.111|7597|103.174.234.0/24|17884 17884|IGP|123.108.8.132|0|0||NAG||
BGP4MP_ET|1790922003.120238|A|123.108.9.111|7597|103.174.235.0/24|17884 17884|IGP|123.108.8.132|0|0||NAG||
BGP4MP_ET|1790922004.830092|A|123.108.8.111|7597|121.50.34.0/24|56258 38750 38750 38750 38750|IGP|123.108.8.197|0|0|56258:1000|
BGP4MP_ET|1790922004.830092|A|123.108.8.111|7597|103.136.24.0/24|56258 38750 38750 38750 38750|IGP|123.108.8.197|0|0|56258:1000
BGP4MP_ET|1790922005.419424|A|123.108.8.111|7597|103.155.251.0/24|17884 17884|IGP|123.108.8.132|0|0|17884:17884|NAG||
BGP4MP_ET|1790922005.419424|A|123.108.8.111|7597|103.158.56.0/24|17884 17884|IGP|123.108.8.132|0|0|17884:17884|NAG||
BGP4MP_ET|1790922005.419424|A|123.108.8.111|7597|103.158.57.0/24|17884 17884|IGP|123.108.8.132|0|0|17884:17884|NAG||
BGP4MP_ET|1790922006.654424|A|123.108.9.111|7597|103.155.251.0/24|17884 17884|IGP|123.108.8.132|0|0|17884:17884|NAG||
BGP4MP_ET|1790922006.654424|A|123.108.9.111|7597|103.158.56.0/24|17884 17884|IGP|123.108.8.132|0|0|17884:17884|NAG||
BGP4MP_ET|1790922006.654424|A|123.108.9.111|7597|103.158.57.0/24|17884 17884|IGP|123.108.8.132|0|0|17884:17884|NAG||
BGP4MP_ET|1790922007.280854|A|123.108.9.111|7597|121.50.34.0/24|56258 38750 38750 38750 38750|IGP|123.108.8.197|0|0|56258:1000|
BGP4MP_ET|1790922007.280854|A|123.108.9.111|7597|103.136.24.0/24|56258 38750 38750 38750 38750|IGP|123.108.8.197|0|0|56258:1000
BGP4MP_ET|1790922007.952003|A|2001:7fa:2:5:7597::111|7597|2001:df0:2f2::/48|32787 132351 132351 132351|IGP|2001:7fa:2:5::43c|0|
BGP4MP_ET|1790922007.952169|A|2001:7fa:2:5:7597:2::111|7597|2001:df0:2f2::/48|32787 132351 132351 132351|IGP|2001:7fa:2:5::43c|
BGP4MP_ET|1790922011.321898|A|123.108.8.111|7597|121.50.34.0/24|56258 38750|INCOMPLETE|123.108.8.197|0|0|56258:1000|NAG||
BGP4MP_ET|1790922011.321898|A|123.108.8.111|7597|103.136.24.0/24|56258 38750|INCOMPLETE|123.108.8.197|0|0|56258:1000|NAG||
BGP4MP_ET|1790922011.343104|A|123.108.9.111|7597|121.50.34.0/24|56258 38750|INCOMPLETE|123.108.8.197|0|0|56258:1000|NAG||
BGP4MP_ET|1790922011.343104|A|123.108.9.111|7597|103.136.24.0/24|56258 38750|INCOMPLETE|123.108.8.197|0|0|56258:1000|NAG||
BGP4MP_ET|1790922013.643466|A|123.108.8.111|7597|103.174.234.0/24|17884 17884|IGP|123.108.8.132|0|0|17884:17884|NAG||
```

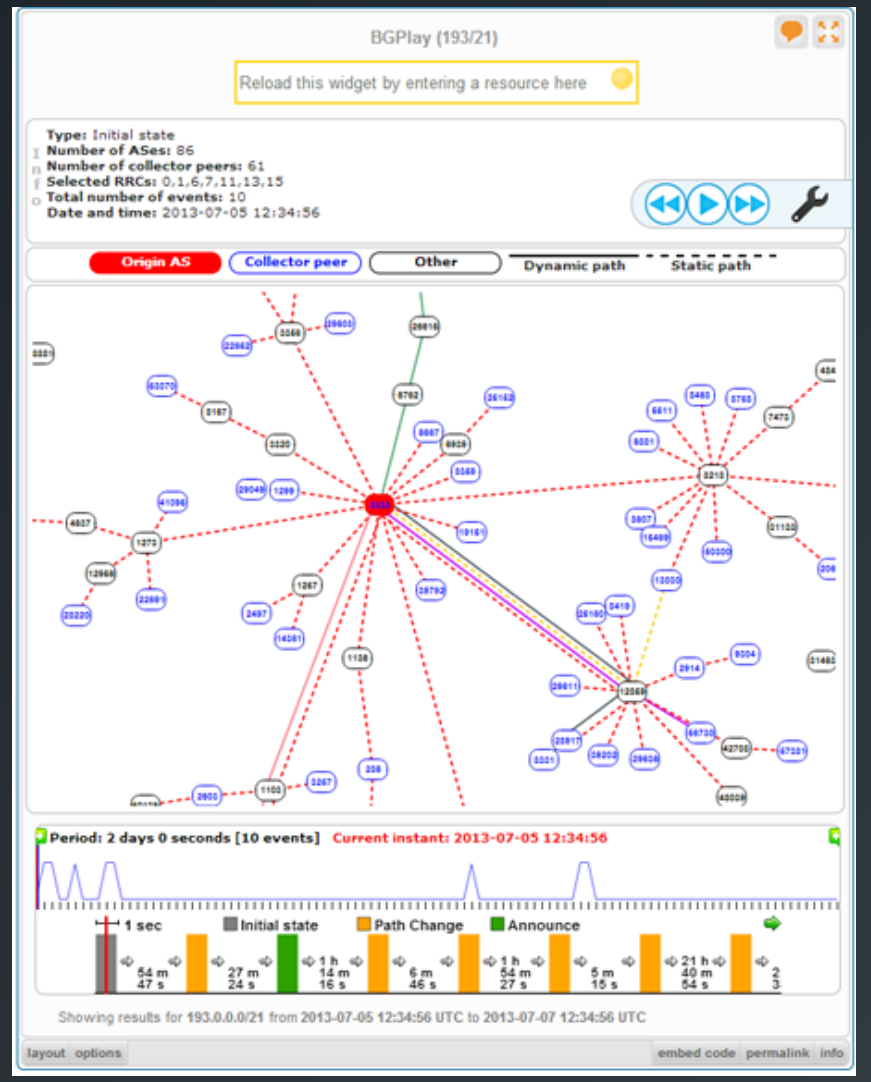

infoblox.

My approach to BGP analysis

- Challenge:
  - Understanding BGP dynamics is a highly dimensional problem.
- For any BGP event, we wish to understand three things:
  1. **Scope** (i.e. How far did it propagate? What is the footprint?)
  2. **Duration** (i.e. How long did it last?)
  3. **Context** (i.e. What were the ASes involved?)

My approach to BGP analysis

- BGPlay still used today, but animating individual announcements doesn't meet our goals.
  - Need to gain insight without watching an extended animation.
- Counts of announcements are also weak measures of a BGP event.
  - Could be nothing, could be something
  - If it's something, what is it? 🤷‍♀️



infoblox

My approach to BGP analysis

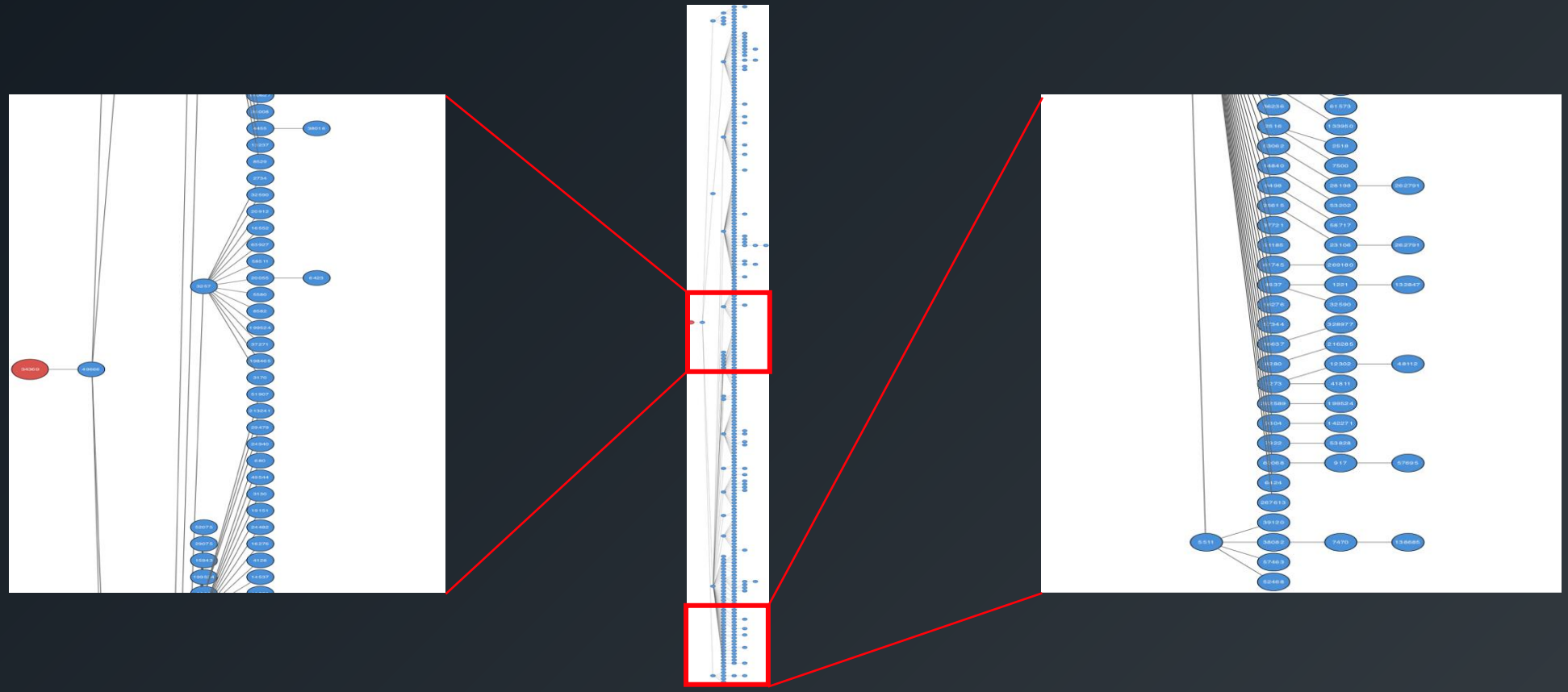
- Goal: Estimate how the Internet's routing tables change over time.
  - We're also trying to merge many views.
- Shift focus from individual announcements to the **hidden state**.
  - Announcements just the observables of that hidden state.
- We must keep state and pay the computational cost.
  - What is the state of the route for each AS over time.

infoblox

Let’s take an example:

What happened to 37.148.92.0/24 during 14:00-16:00 UTC on Sep-8?

- What happened to 37.148.92.0/24 during 14:00-16:00 UTC on Sep-8?
  - If you start by plotting all the AS-AS edges of the route at the beginning of the timeline with RouteViews, it is unreadable.



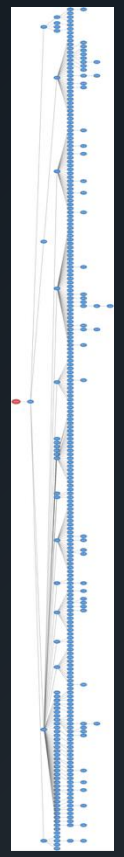
infoblox

- What happened to 37.148.92.0/24 during 14:00-16:00 UTC on Sep-8?

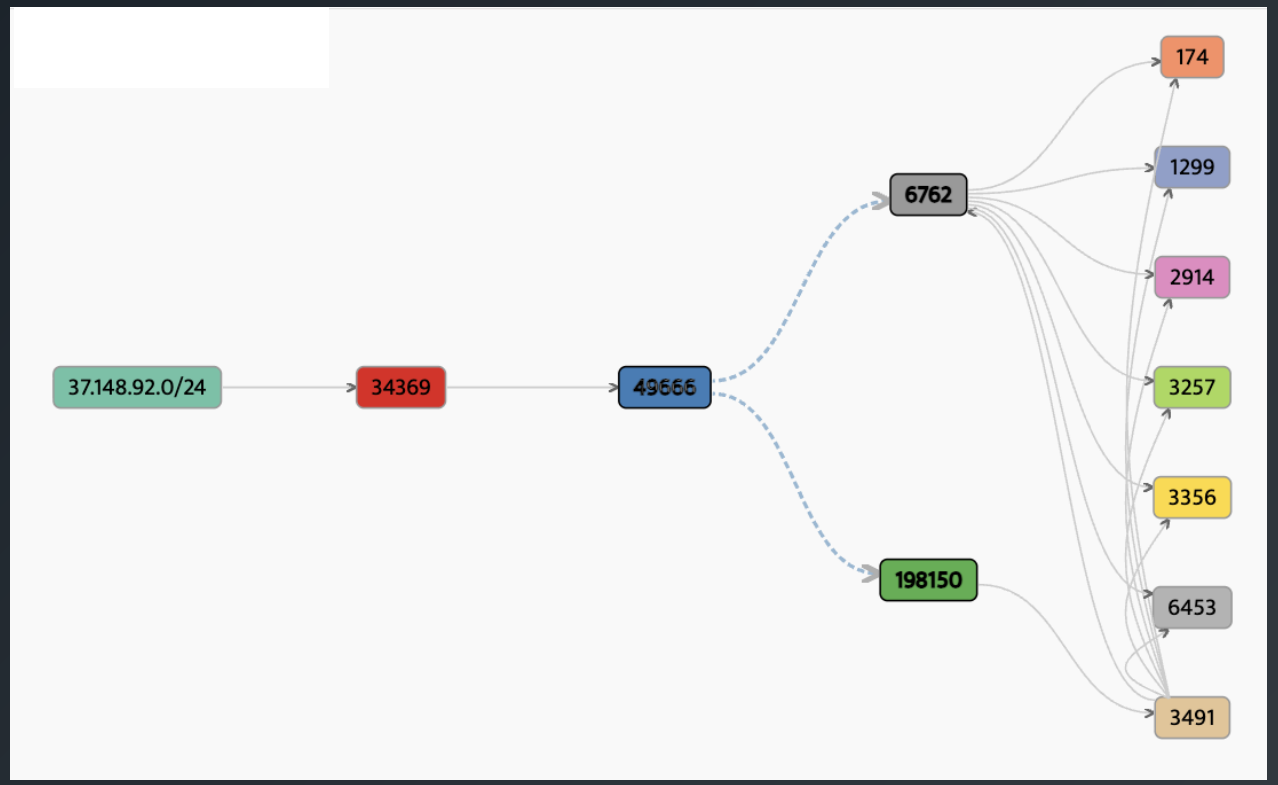
  - If you start by plotting all the AS-AS edges of the route at the beginning of the timeline with RouteViews, it is unreadable.
  - You either must greatly reduce the number of BGP sources you use (sacrificing information) or …
  - Prune the ball-and-stick.
    - Insight: most of the activity you care about is closer to the origin.
    - Drawing every AS edge wastes time and space.
    - Allows the use of nearly unlimited BGP sources.

- What happened to 37.148.92.0/24 during 14:00-16:00 UTC on Sep-8?

  - By restricting the ball-and-stick to things seen by ~1% of BGP sources, you focus on what matters most.



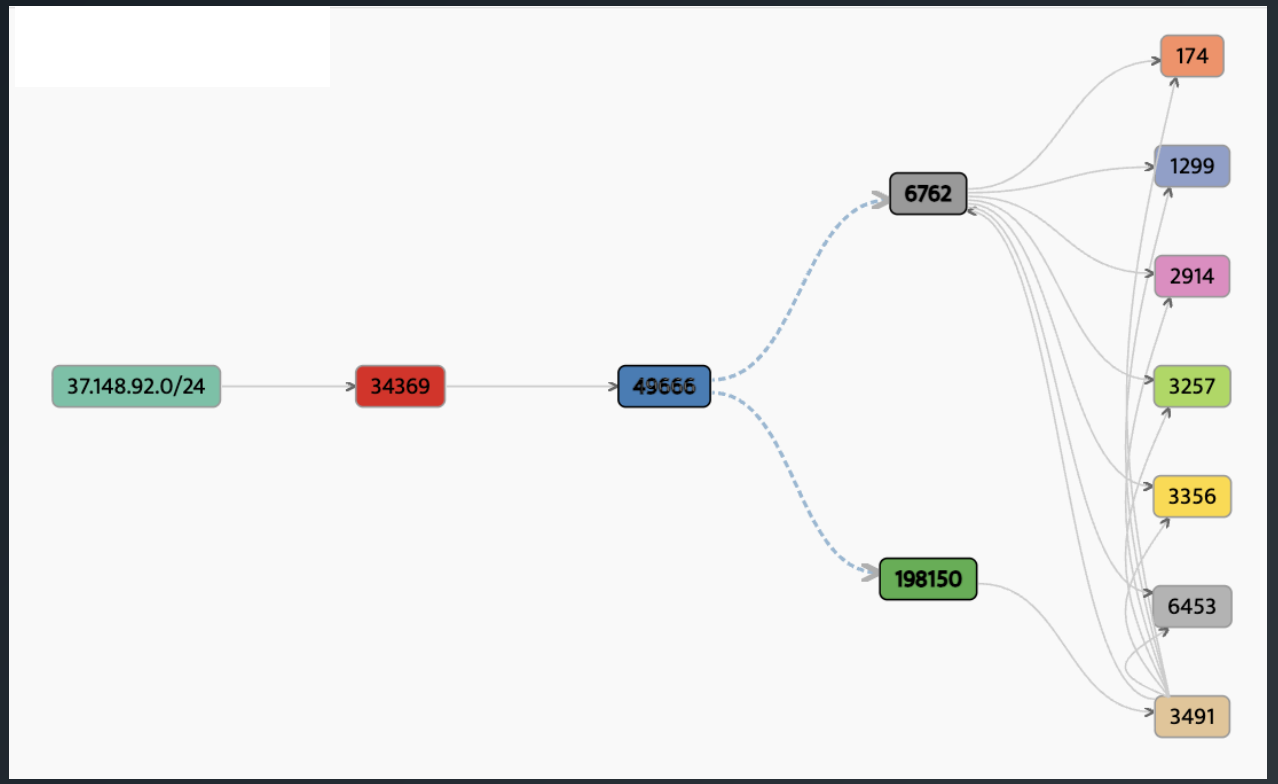
becomes



infoblox

- What happened to 37.148.92.0/24 during 14:00-16:00 UTC on Sep-8?

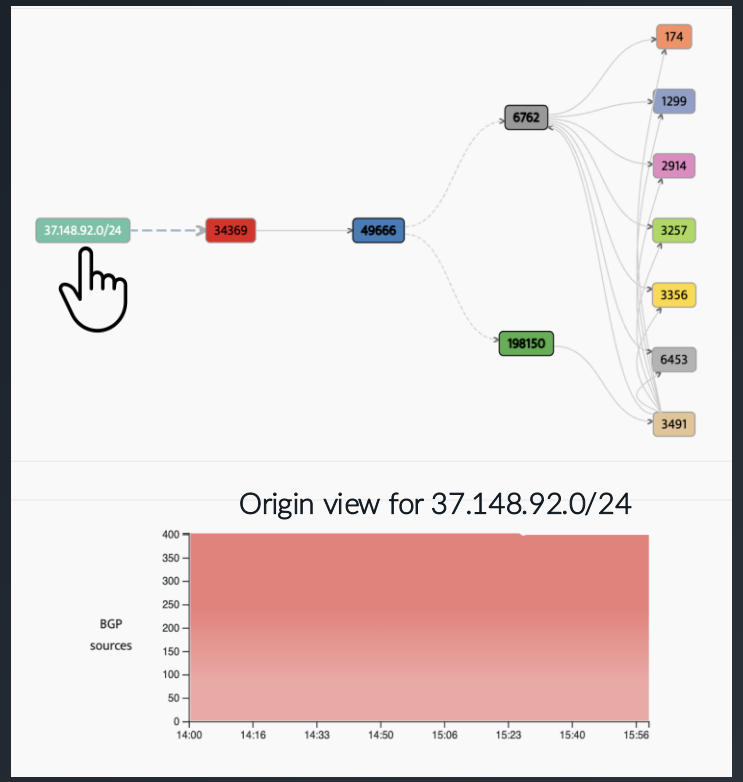
  - This covers “context” but not scope and duration.
  - For those, we’ll need something else.

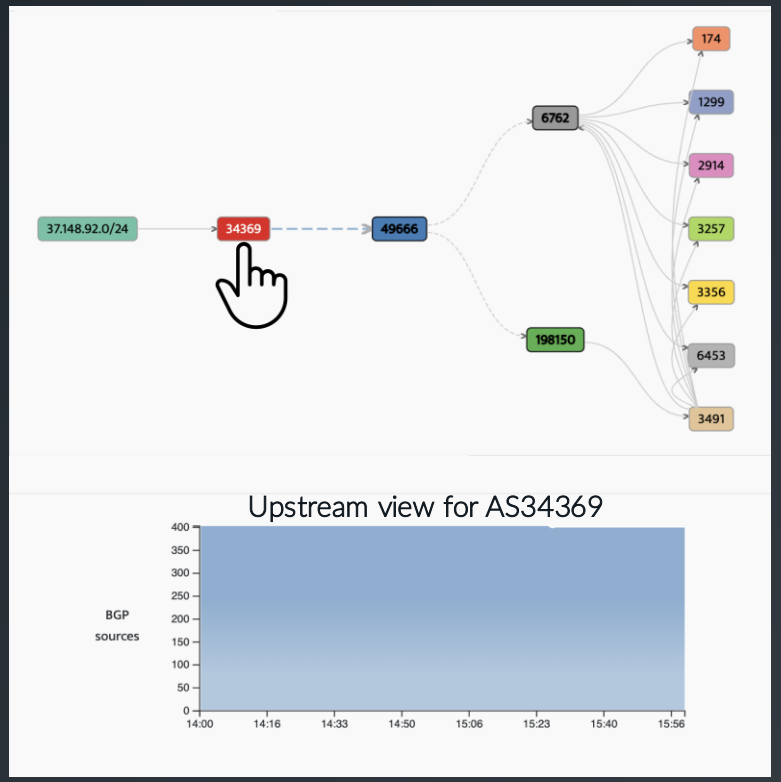


infoblox

- What happened to 37.148.92.0/24 during 14:00-16:00 UTC on Sep-8?

  - For years I've used these stack plots to represent the aggregate views of large numbers of BGP sources.
  - In this case, one can see that not much changed in the origination of this prefix or in the first hop of transit.
  - We can't limit ourselves to just activity at the origin or first-level upstream.



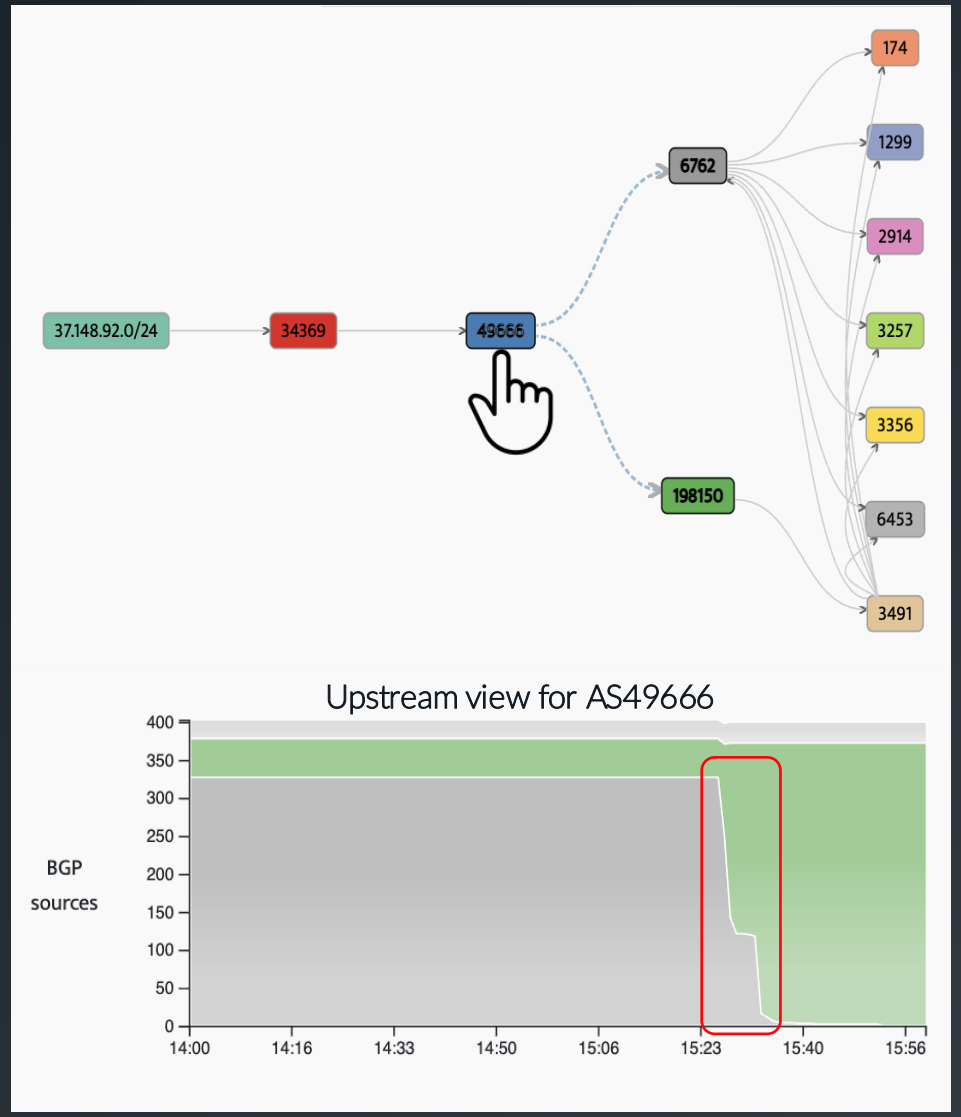


infoblox

What happened to 37.148.92.0/24 during 14:00-16:00 UTC on Sep-8?

- But if we search far enough, we can instantly see that normally AS49666 has primarily two upstreams however AS6762 dropped away beginning at 15:26 UTC being completely replaced by AS198150.

- 1025 update messages processed.
  - Not necessary to know this!
  - We're focused on the change in hidden state, not the count of messages.

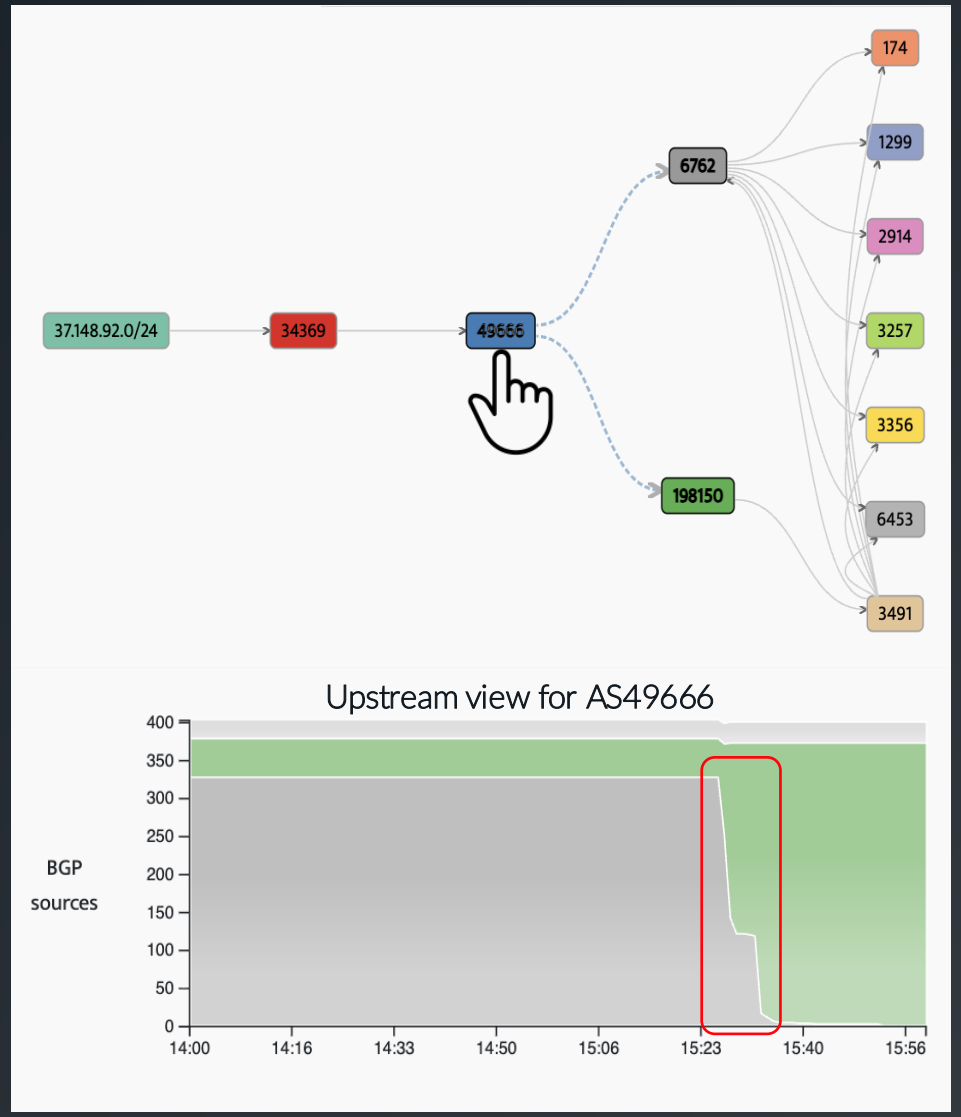


infoblox

- What happened to 37.148.92.0/24 during 14:00-16:00 UTC on Sep-8?

  - This is how we can address **scope**, **duration** and **context** in a single analytical approach.

  - More than just a visualization, it is an approach to understanding dynamism in BGP.



2 1

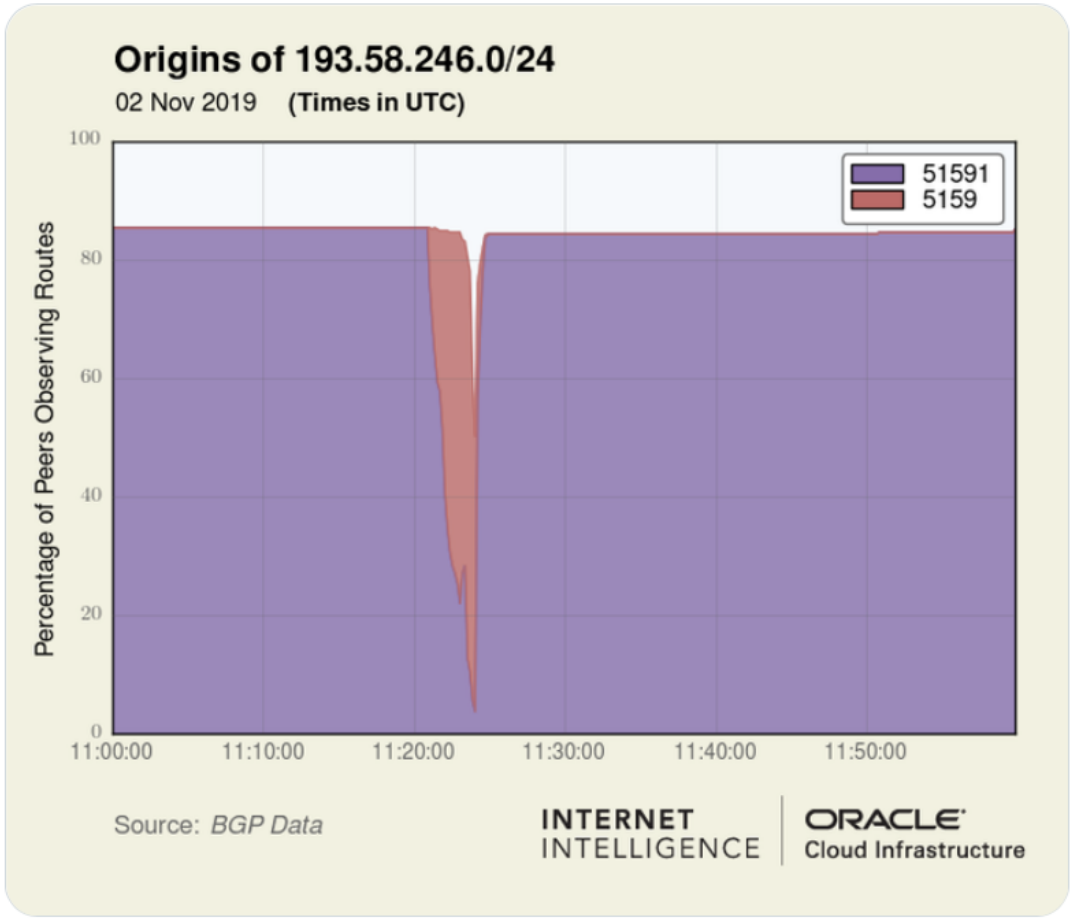
Anurag Bhatia @anurag_bhatia · Nov 4, 2019

Sometimes I wonder what all cool stuff you see by this kind of active logging of the whole table (plus associated compute challenges) :)

1

Doug Madory (also on Bluesky) @DougMadory · Nov 4, 2019

Mostly typos! :-)



Nov 4, 2019

Anurag Bhatia:
Sometimes I wonder what all cool stuff you see by this kind of active logging of the whole table (plus associated compute challenges) :)

Me:
Mostly typos! :-)

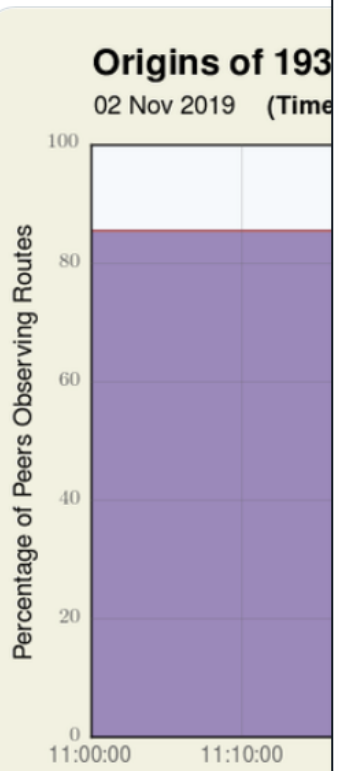
infoblox.

2 1

Anurag Bhatia @anurag
Sometimes I wonder wha
logging of the whole tabl

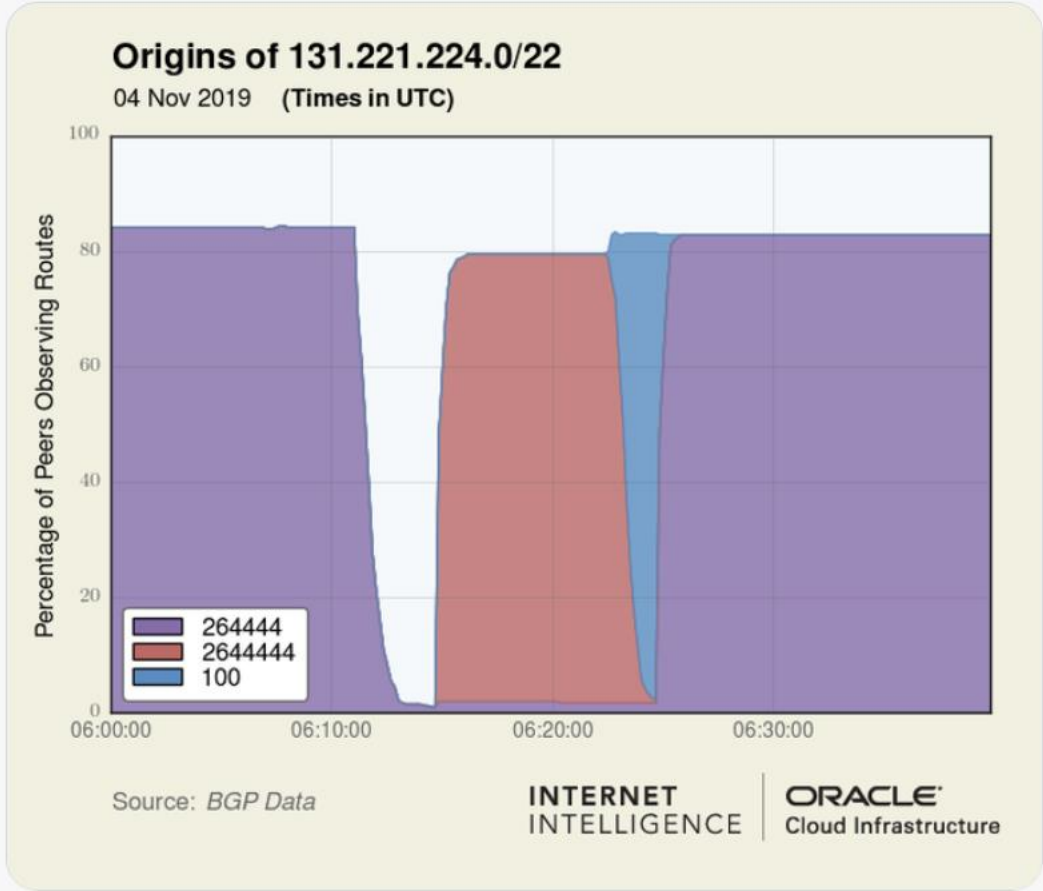
1

Doug Madory (also on B
Mostly typos! :-)



2 2 2

Doug Madory (also on Bluesky) @DougMadory · Nov 5, 2019
And more typos...



2 1 2

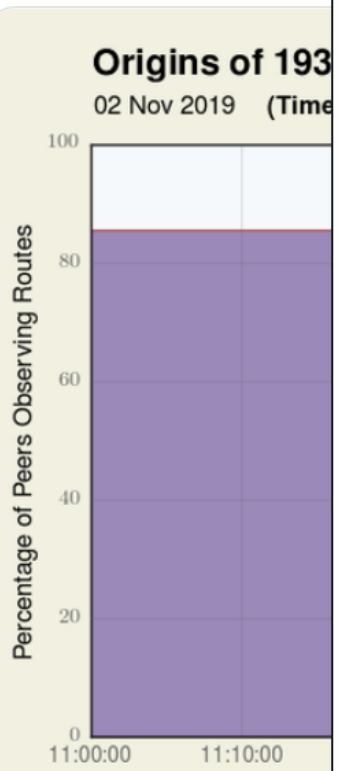
infoblox

2 1

Anurag Bhatia @anurag_
Sometimes I wonder wha
logging of the whole tabl

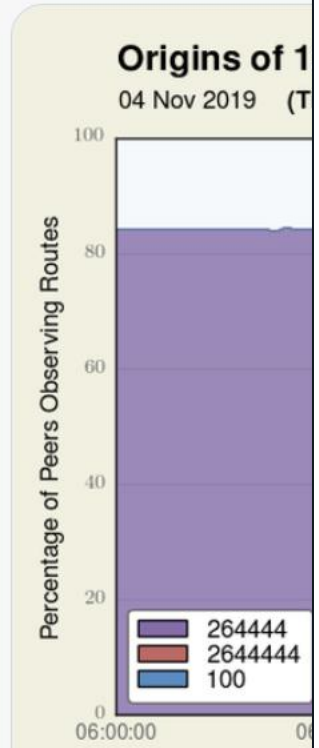
1

Doug Madory (also on B
Mostly typos! :-)



2 2 2

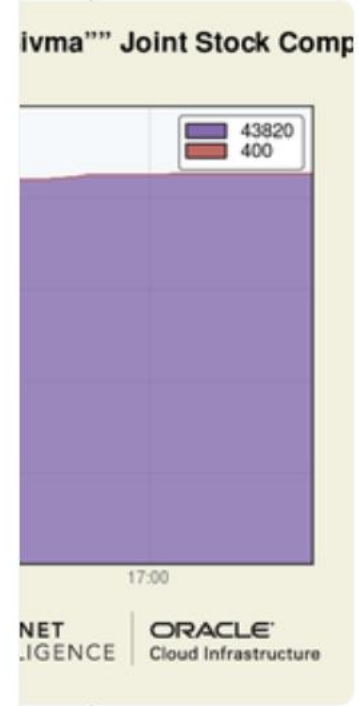
Doug Madory (also on
And more typos...

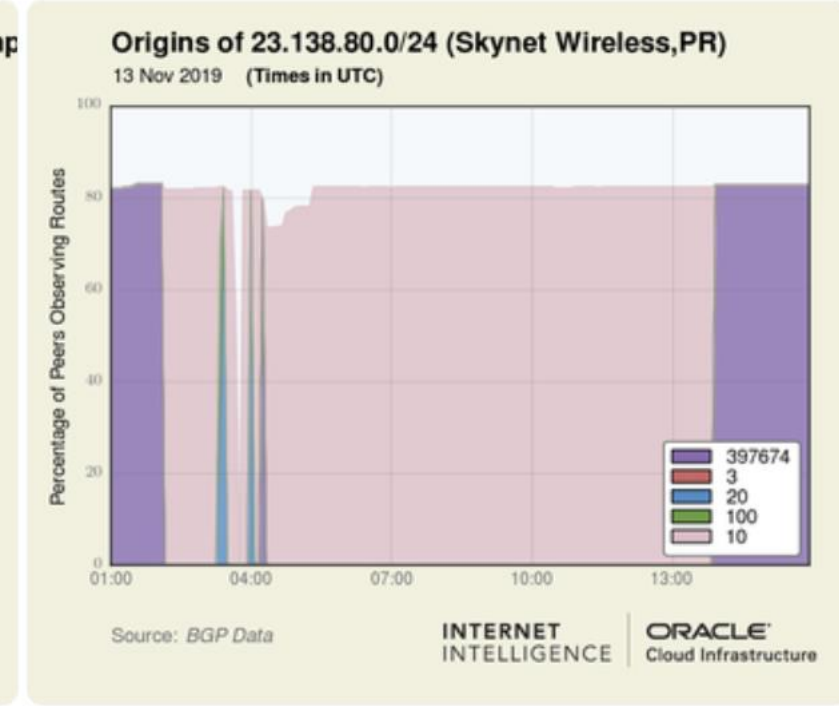


INTELLIGENCE | Cloud Infrastructure

2 1 2

Doug Madory (also on Bluesky) @DougMadory · Nov 14, 2019
Lots of BGP typos yesterday!





2 1

infoblox.



Doug Madory (also on Bluesky)
@DougMadory

#Typostream



6:32 AM · Dec 5, 2019

10 6 34

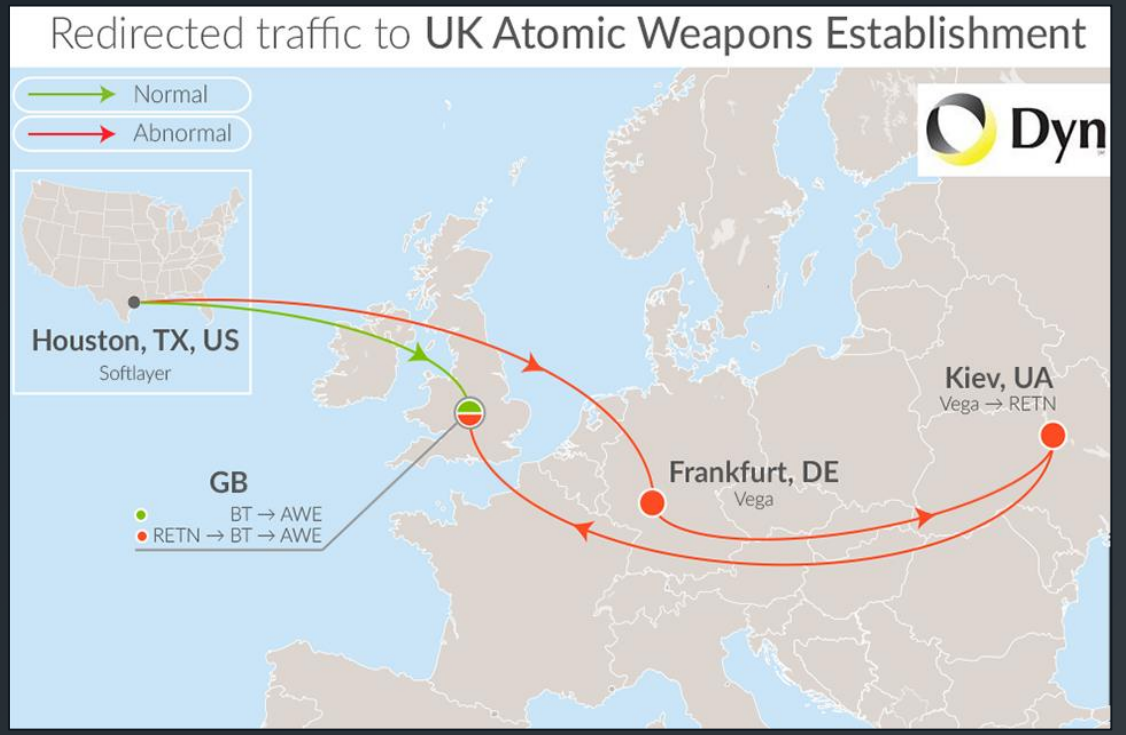
infoblox.

My analysis falls into two buckets

Geopolitical



BGP security



infoblox

My analysis falls into two buckets

Geopolitical



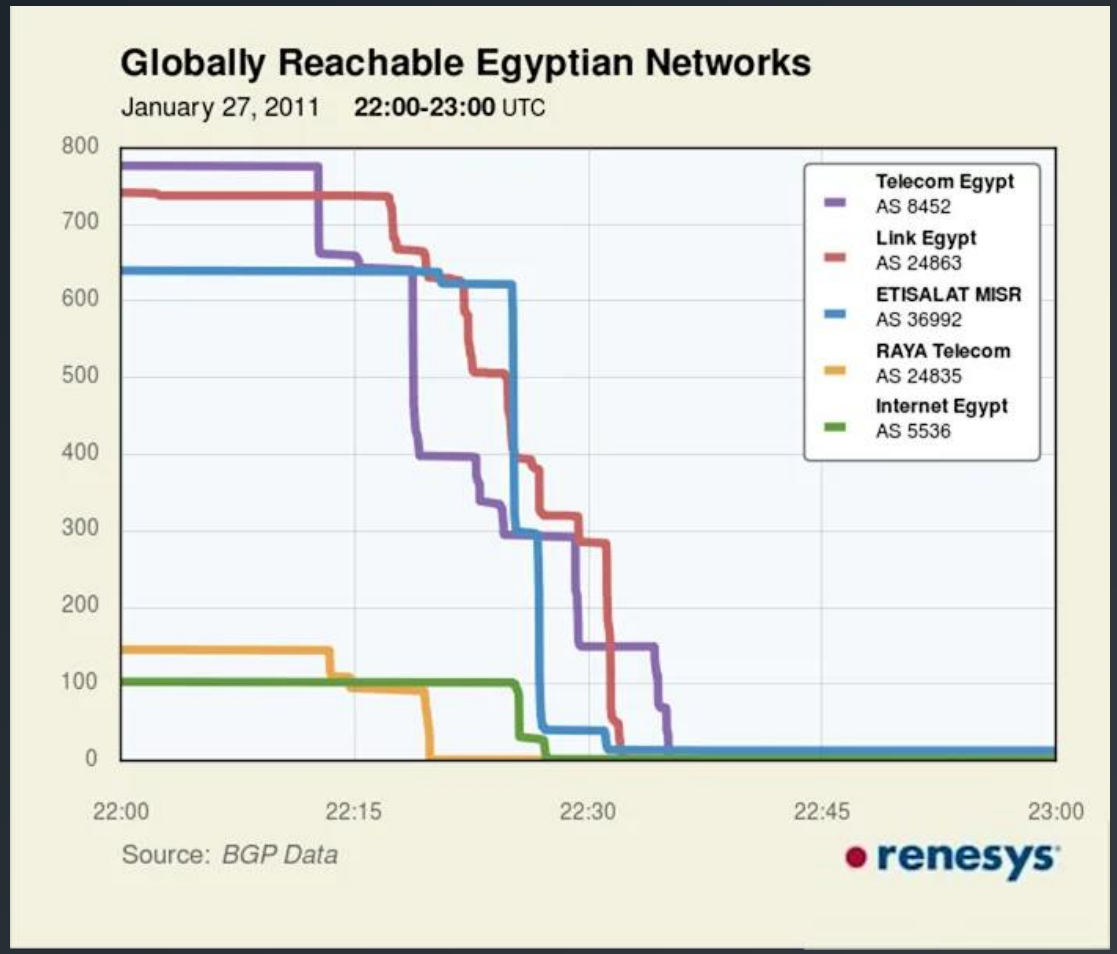
BGP security



infoblox

Geopolitical: Internet shutdowns

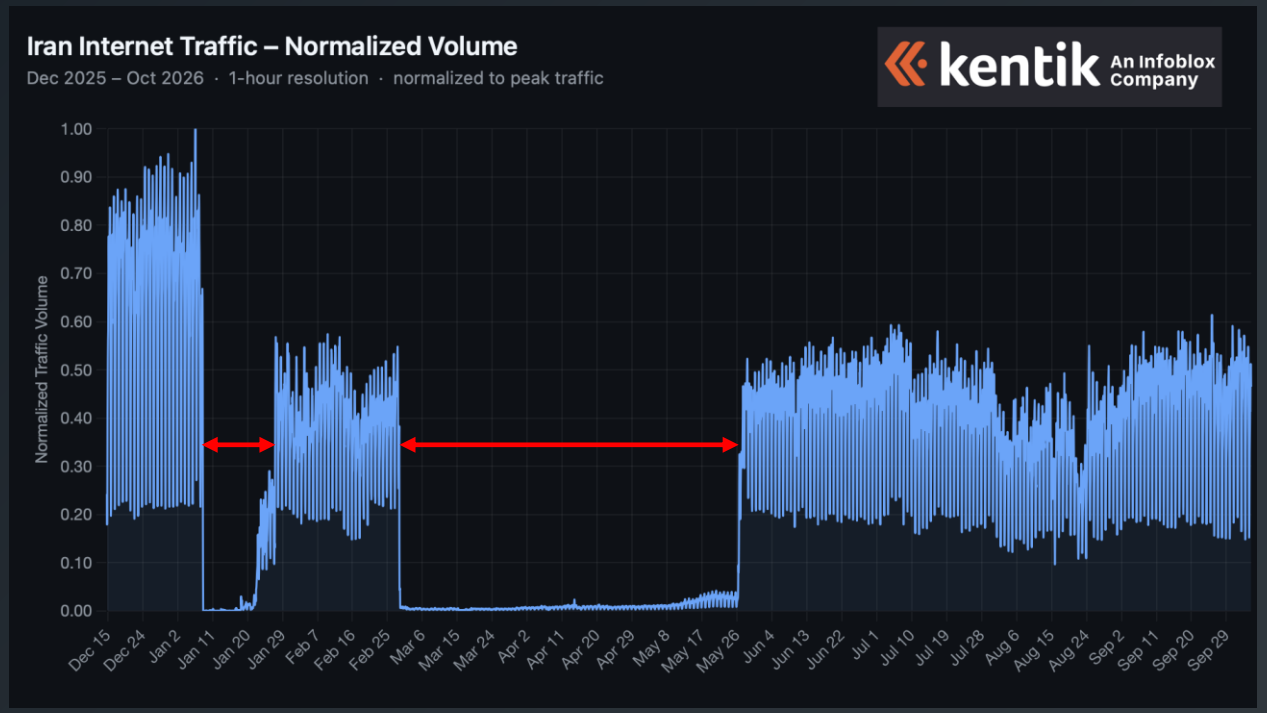
- Egyptian shutdown (Jan 2011)
  - Ushered in the era of “digital authoritarianism” still with us today.
- Initial techno-optimism was misplaced.
  - Costs of shutdowns irrelevant to dictator.
  - Diverse international links not a panacea.
  - Emergence of digital rights community and rapid innovation of circumvention tech.
- Numerous shutdowns since Egypt.
  - A problem that will unfortunately continue.



infoblox

Geopolitical: Internet shutdowns

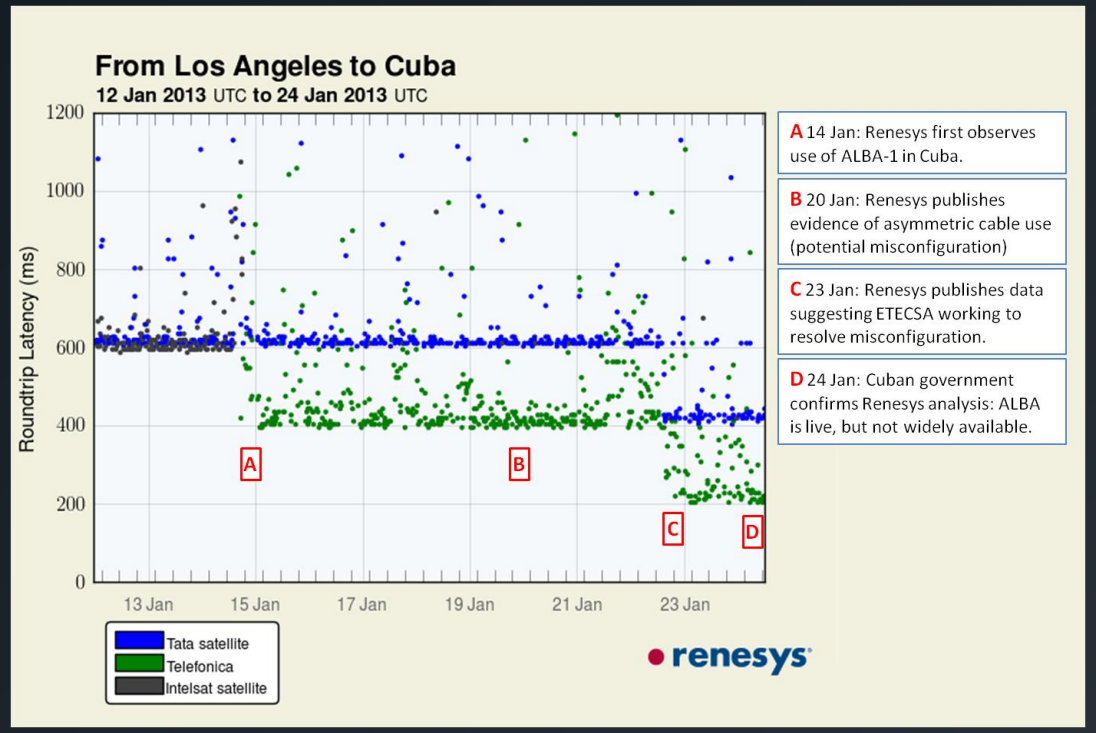
- Iran shutdowns of 2026
  - Most impactful shutdown in history.
  - BGP routes stayed up, country offline.
  - Filtering implemented through GFW-like capability.
- Various attempts to mitigate costs.
  - Nightly Internet curfews (2022)
  - National domestic Internet (NIN)
  - Allowlisting (2026)

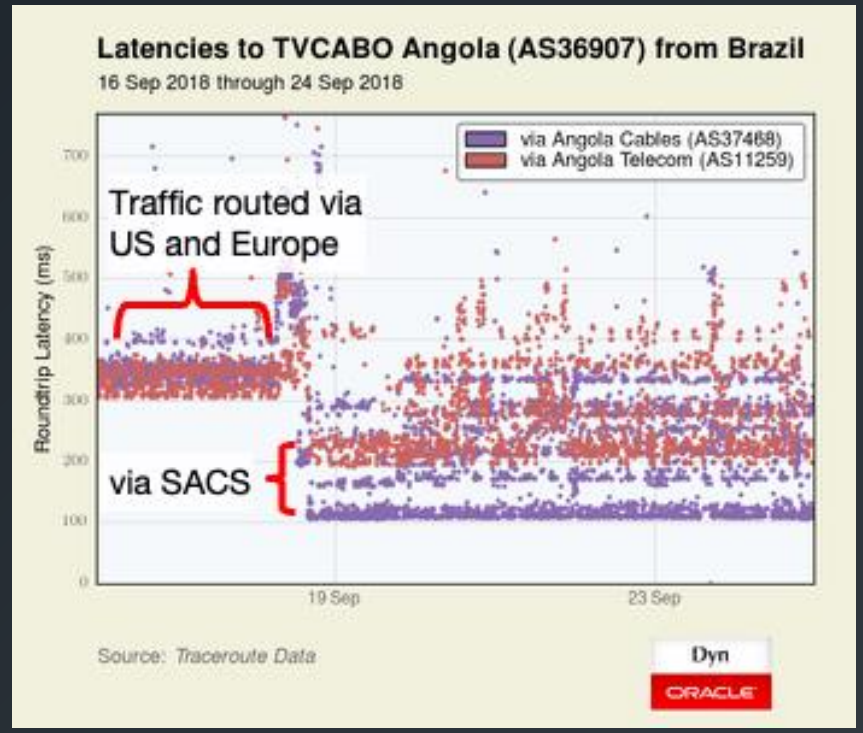


infoblox

Geopolitical: ALBA-1 submarine cable activation

- Published the first evidence of the activation of the first subsea cable connecting Cuba to the Internet. (Jan 2013)
  - Spotted a new BGP adjacency for ETECSA (AS11960), confirmed with traceroutes.
- At LACNIC 30 in Rosario, I presented the first evidence of the activation of SACS, the first operational submarine cable across the South Atlantic.

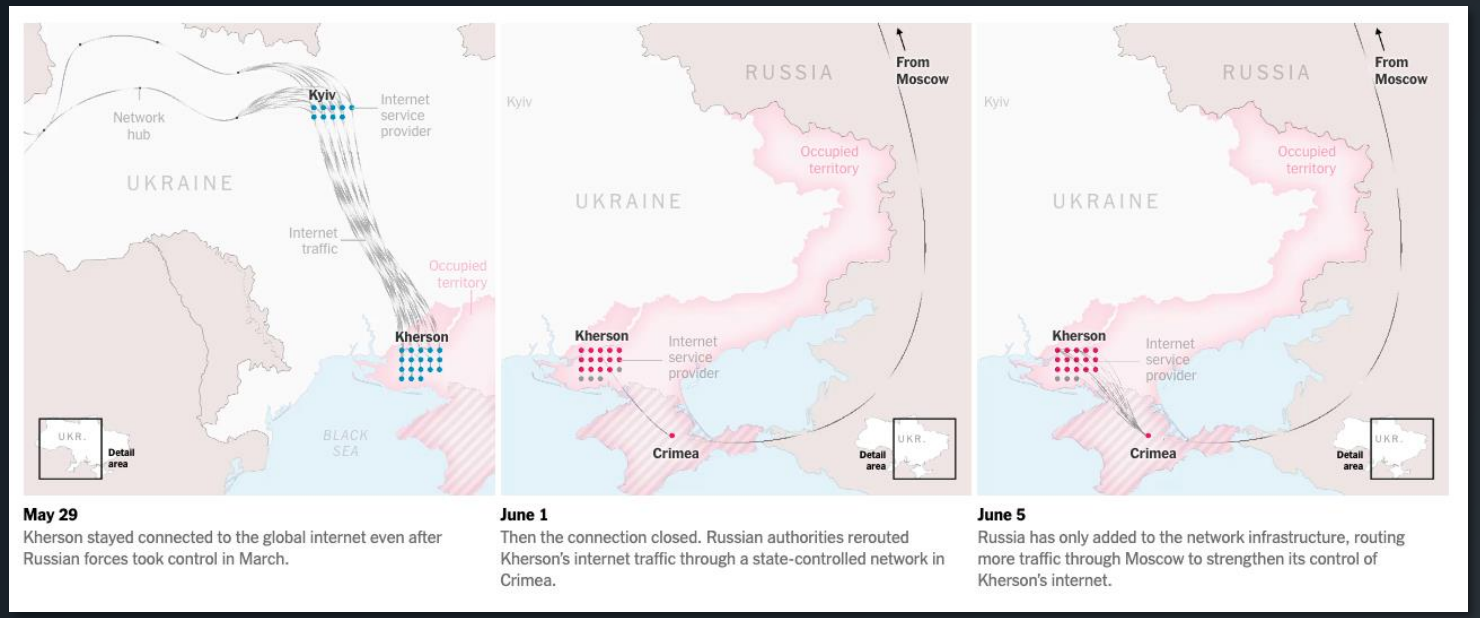




Geopolitical: Kherson switchover to Russian transit

- March 2014: Russia annexed Crimean Peninsula from Ukraine
- Crimea Internet re-routed via Miranda Media (AS201776) in July 2014.
- Kherson Internet re-routed via AS201776 in June 2022.

How Russia Took Over Ukraine's Internet in Occupied Territories
(New York Times, Aug 9)



May 29
Kherson stayed connected to the global internet even after Russian forces took control in March.

June 1
Then the connection closed. Russian authorities rerouted Kherson's internet traffic through a state-controlled network in Crimea.

June 5
Russia has only added to the network infrastructure, routing more traffic through Moscow to strengthen its control of Kherson's internet.

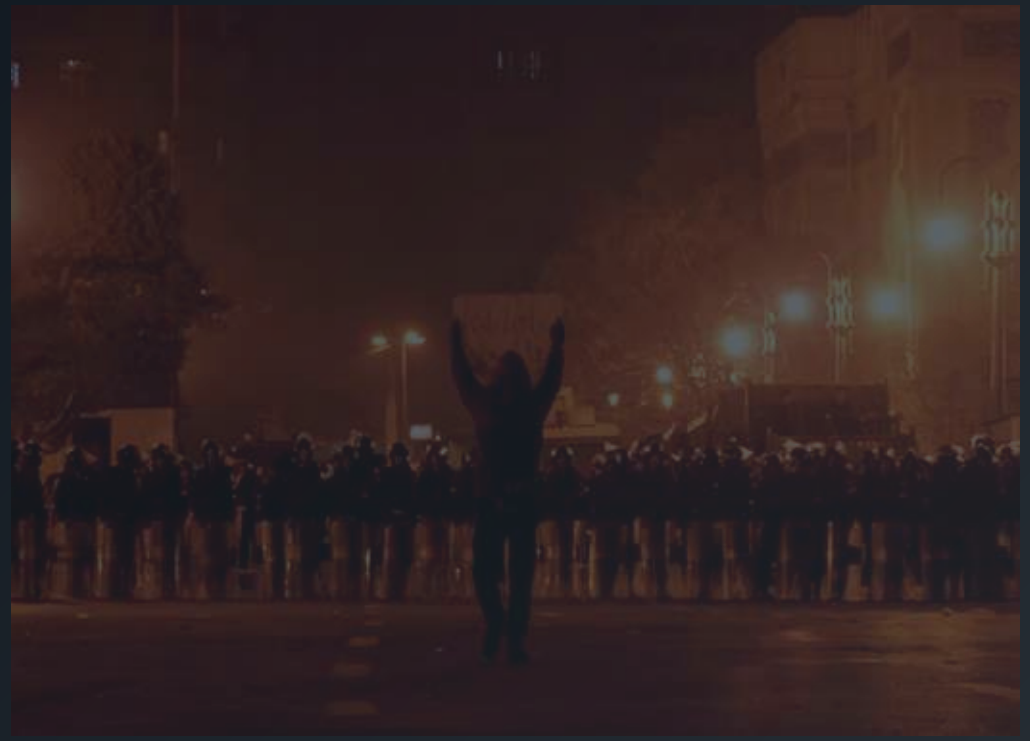
All Kherson ISPs switch to Russian transit beginning June 1, 2022.



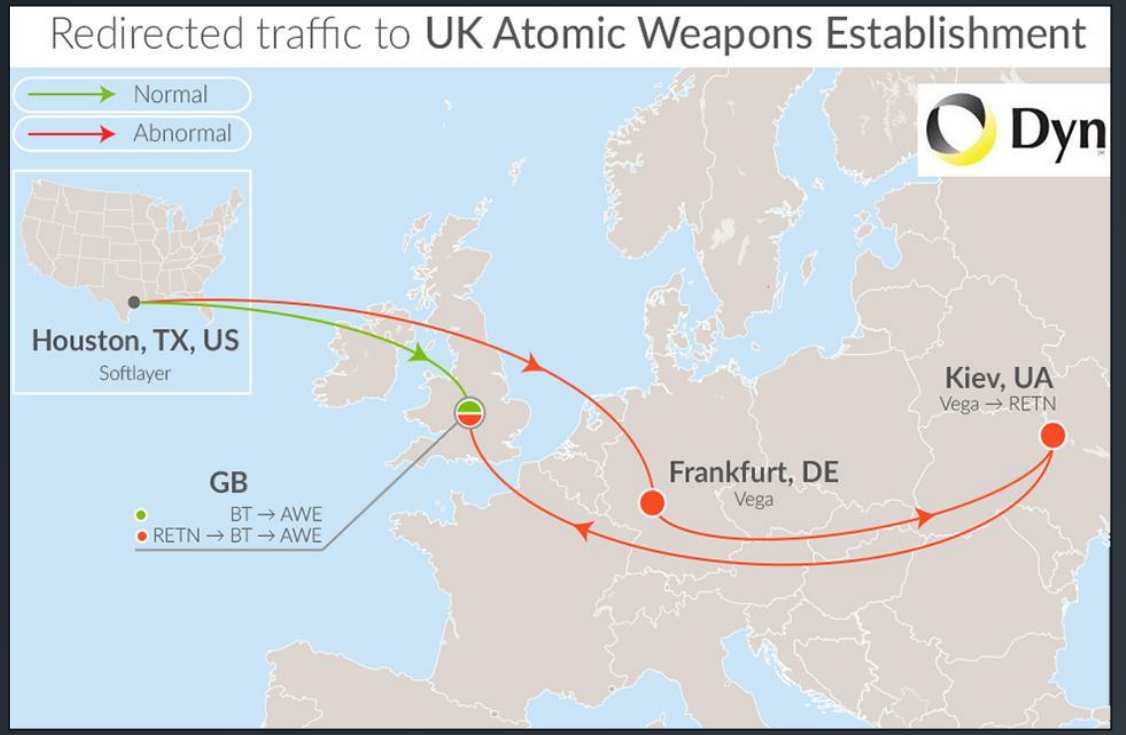
https://www.nytimes.com/interactive/2022/08/09/technology/ukraine-internet-russia-censorship.html
https://www.kentik.com/blog/rerouting-of-kherson-follows-familiar-gameplan/

My analysis falls into two buckets

Geopolitical



BGP security



infoblox

Real world attacks: BGP MITM hijacks

- First documented cases of BGP MITM attacks.
  - Belarus ASes hijacked many entities in Feb 2013
  - Targets included:
    - Visa & Mastercard
    - Numerous Foreign Ministries
- Motivated Renesys to build a system to detect all BGP hijacks in the routing table.
  - Discovered many more.



- Legacy of those early BGP attacks.
  - Today, RPKI ROV and other filtering mechanisms would have stopped these.
  - Public reporting tools (BGPstream, GRIP) caused hijackers to shift tactics.

infoblox

Real world attacks: Other BGP malfeasance

Disconnection of Bitcanal (AS197426)

- Platform for bad actors performing BGP hijacks.
- Disconnected from Internet by coordinated action.

- Legacy of this incident:
  - Unfortunately, residential proxies and IPv4 leasing have obviated the need for such a service.
  - After takedown, bad actors moved to US telecoms.



Intentional, but also accidental.

- Local block leaks out
- Most famous incident: YouTube/Pakistan
- Most recent: Telegram/India

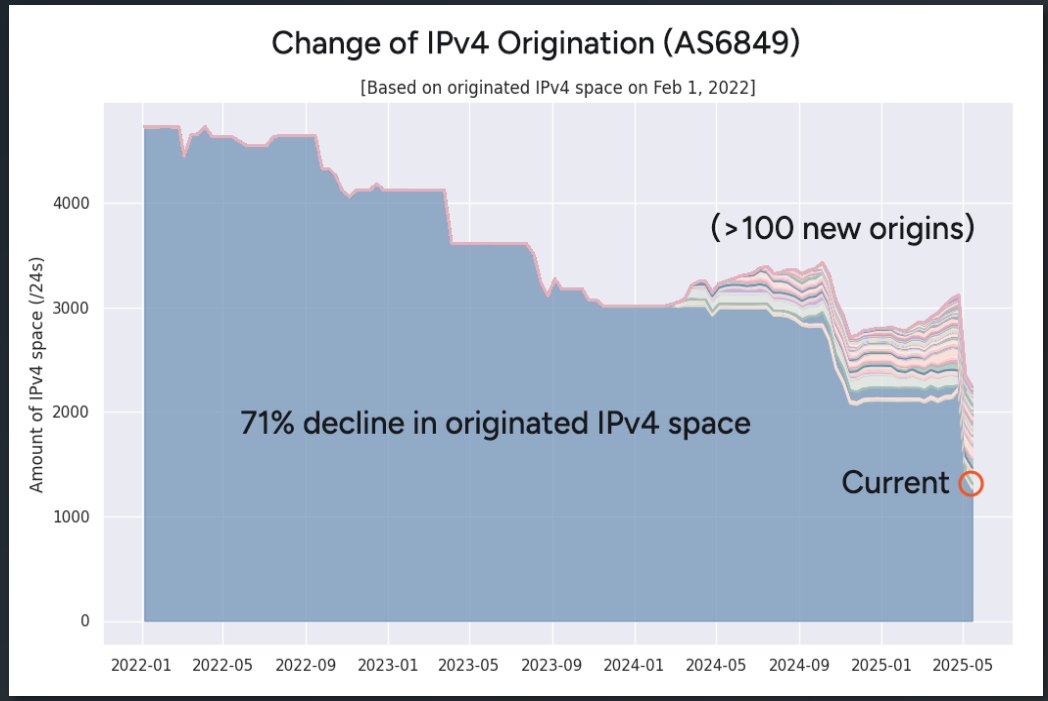
Legacy: the times have changed!

- RPKI ROV has (mostly) contained these events.

infoblox

Real world attacks: IPv4 leasing and residential proxies

- IPv4 private transfer market took off in 2014.
  - Introduced a new player in the Internet ecosystem: the IPv4 broker.
- IPv4 leasing came a few years later.
  - Added the flexibility of quick, temporary usage.
  - Didn't require an RIR-mediated transfer of ownership.
- Ukraine's footprint in the global routing table shrank by 18.5% in the years following the invasion by Russia.
- Ukrainian providers leasing their IPv4 for needed revenue, only to be abused by residential proxies.
  - Subject of an analysis by Brian Krebs.

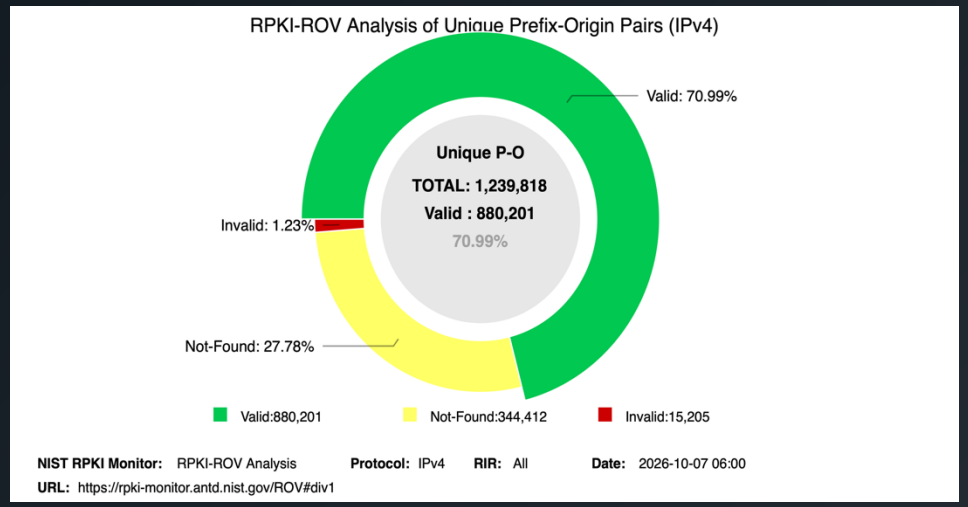


https://www.kentik.com/blog/from-ukraine-to-the-cloud-stories-of-ipv4-migration/

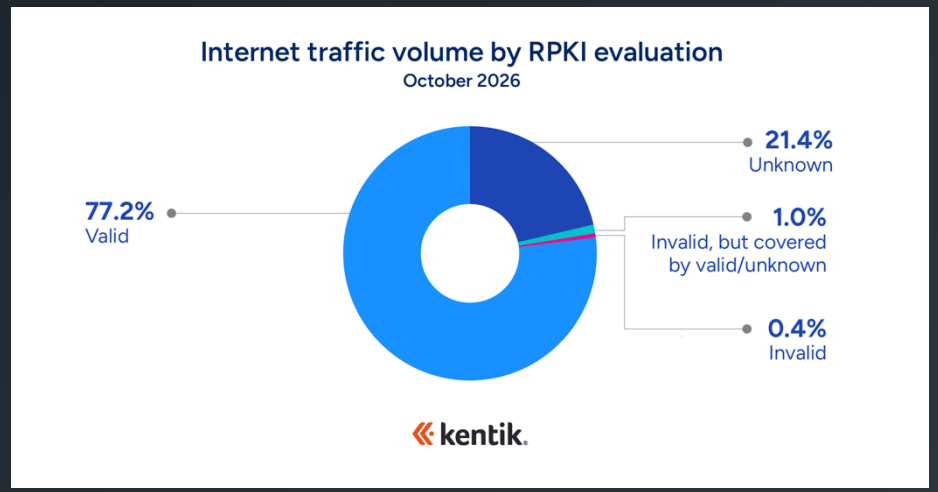
infoblox

Quick Review of RPKI ROV

- A ROA authorizes an origin AS (and optional maxLength) for a prefix.
- ROV checks routes against ROAs and rejects invalids.



Routes with ROAs
71% of IPv4
79% of IPv6
Source NIST RPKI Monitor

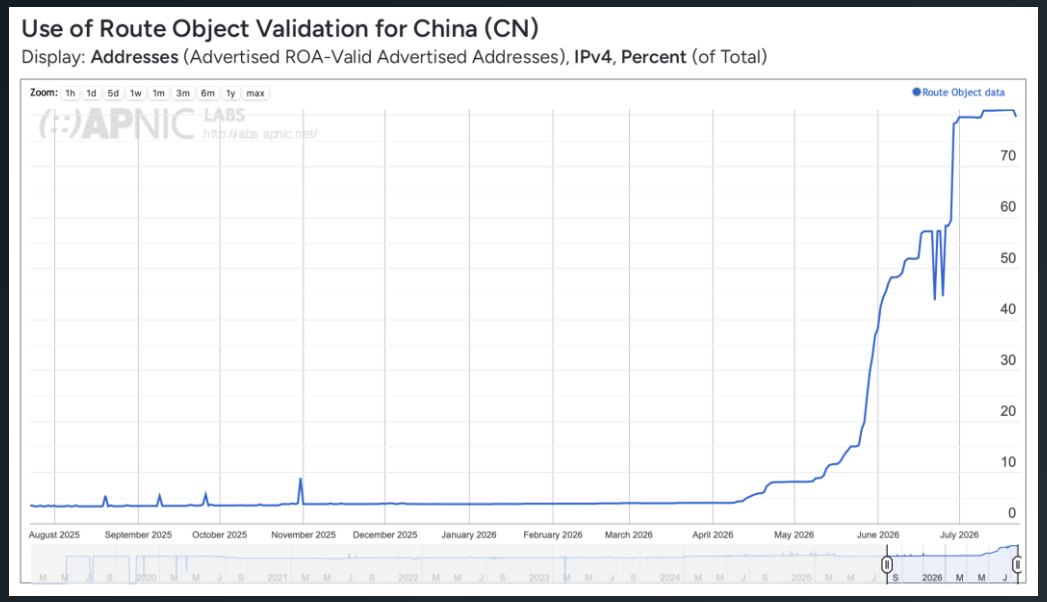


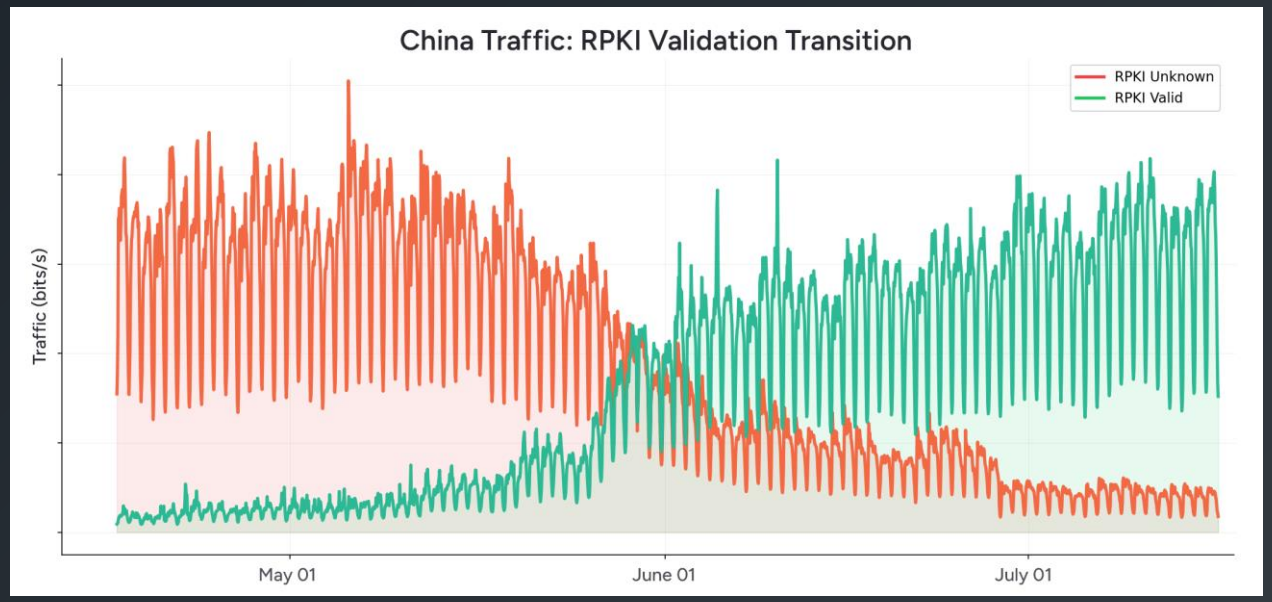
Traffic to Routes with ROAs
78% bits/sec
Source: Kentik aggregate traffic data

infoblox

RPKI ROV: China rolls out the ROAs

- China's embrace of ROAs caused an uptick in global coverage stats.
- Since April 2026, ROA coverage in China increased from 4% to 81%.
- Increased ROA coverage in the APNIC region from 55% to 77%





https://www.kentik.com/blog/china-rolls-out-the-roas/

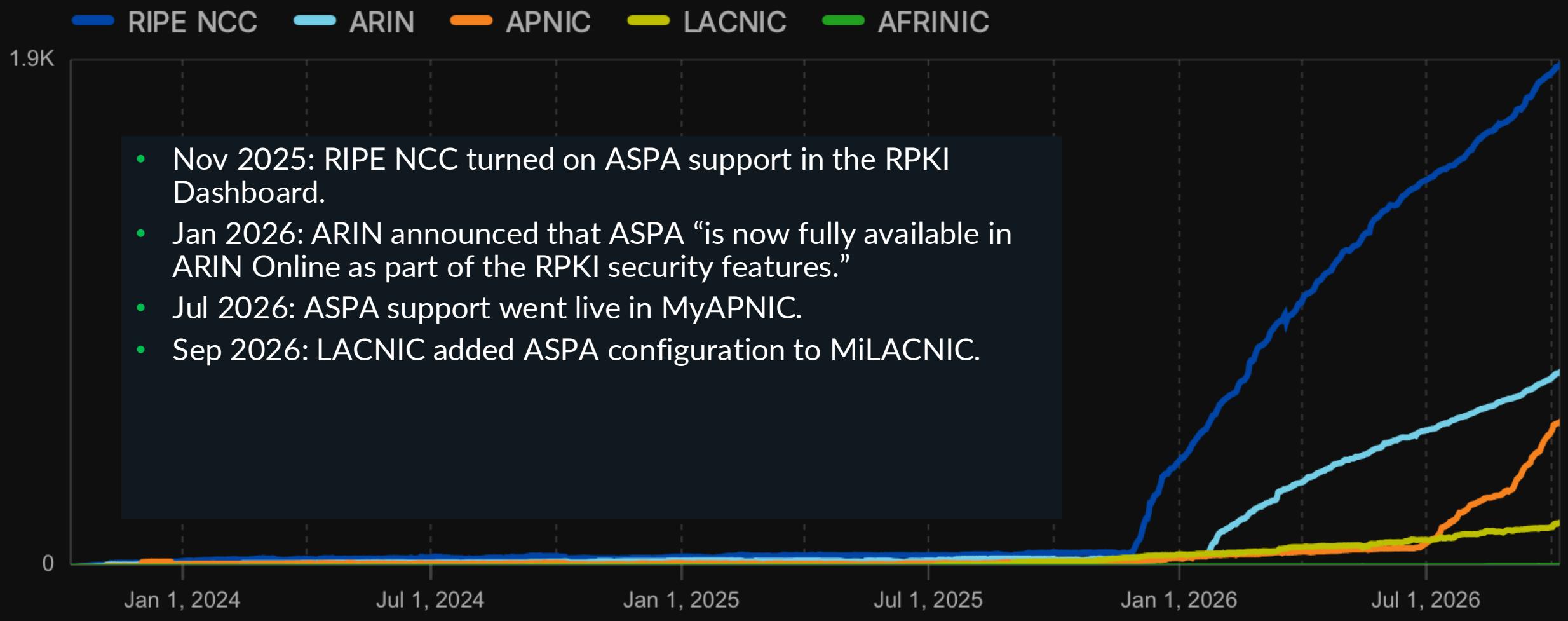
infoblox

ASPA: Validating the Path, Beyond the Origin

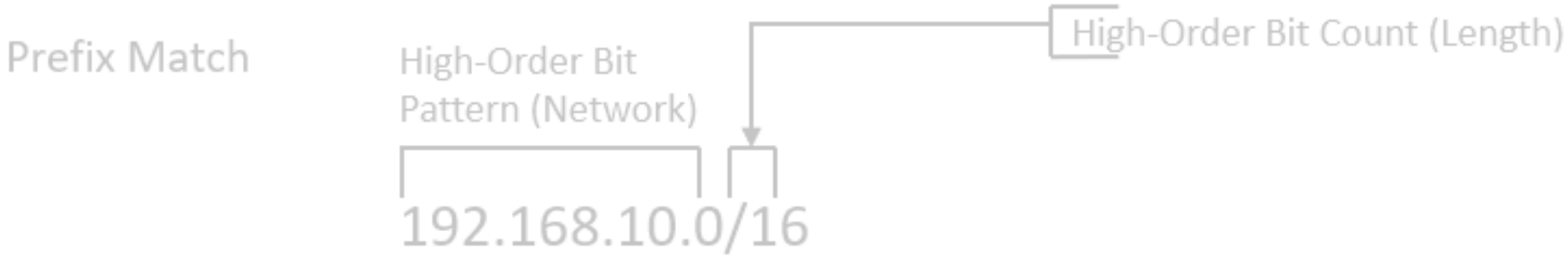
- ROV asks: is this AS allowed to originate this prefix?
- ASPA asks the next question: does this AS path follow real business relationships?
- Each network signs one ASPA object listing its upstream transit providers.
- Routers check that a path climbs up through providers and comes back down only once (valley-free).
- It catches two threats ROV misses:
  - Route leaks (e.g., Verizon/DQE, 2019)
  - Forged-origin hijacks

RPKI ASPA deployment worldwide

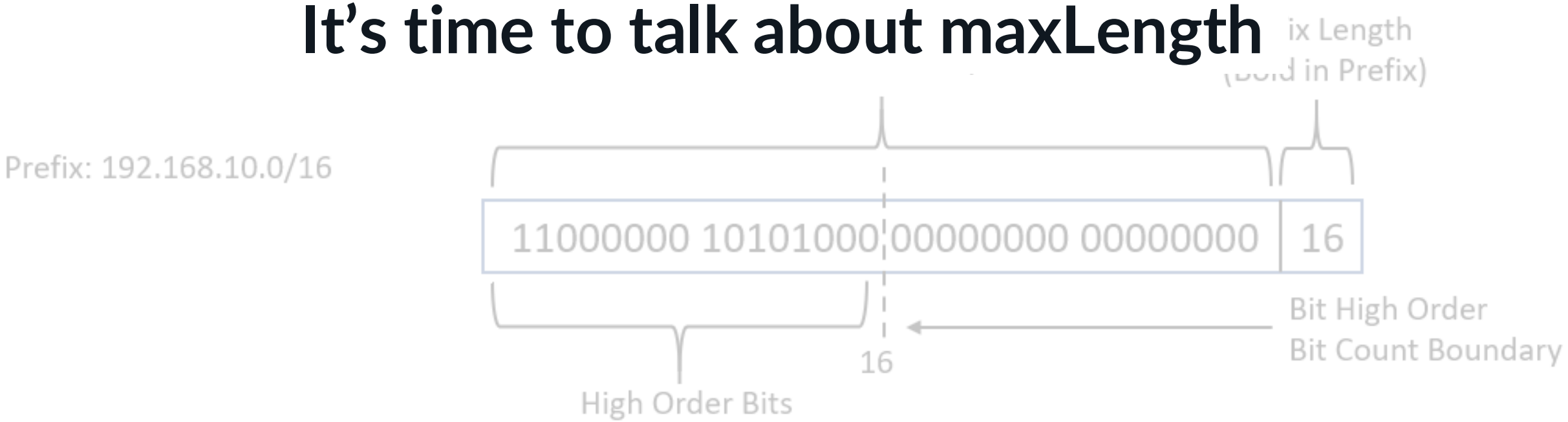
Number of RPKI ASPA entries over time



- Nov 2025: RIPE NCC turned on ASPA support in the RPKI Dashboard.
- Jan 2026: ARIN announced that ASPA “is now fully available in ARIN Online as part of the RPKI security features.”
- Jul 2026: ASPA support went live in MyAPNIC.
- Sep 2026: LACNIC added ASPA configuration to MiLACNIC.



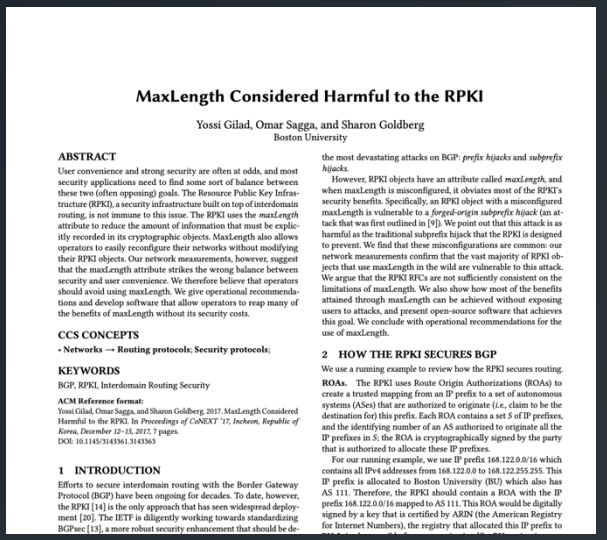
It's time to talk about maxLength



Early warnings on maxLength

- 2017 paper by Gilad, Sagga, and Goldberg outlined risks of overly permissive maxLength values in ROAs.
- RPKI ROV could be undermined by a hijack with:
  - Unannounced more-specific (subprefix) within the maxLength limit
  - Forged AS path ending in the ROA's authorized origin

- In 2018, Birge-Lee et al. showed how an attacker could obtain a valid TLS certificate using a BGP hijack.
  - Domain validation runs over unauthenticated connections and assumes the routing system is correct.
- Led to the development of Multi-Perspective Issuance Corroboration (MPIC), now required of all public CAs.
  - Validates from multiple geographically and topologically diverse locations.
  - A quorum must agree before a certificate is issued.



MaxLength Considered Harmful to the RPKI

Yossi Gilad, Omar Sagga, and Sharon Goldberg
Boston University

ABSTRACT

User convenience and strong security are often at odds, and most security applications need to find some sort of balance between these two (often opposing) goals. The Resource Public Key Infrastructure (RPKI), a security infrastructure built on top of interdomain routing, is not immune to this issue. The RPKI uses the *maxLength* attribute to reduce the amount of information that must be explicitly recorded in its cryptographic objects. MaxLength also allows operators to easily reconfigure their networks without modifying their RPKI objects. Our network measurements, however, suggest that the maxLength attribute strikes the wrong balance between security and user convenience. We therefore believe that operators should avoid using maxLength. We give operational recommendations and develop software that allow operators to reap many of the benefits of maxLength without its security costs.

CCS CONCEPTS

• **Networks → Routing protocols**; **Security protocols**;

KEYWORDS

BGP, RPKI, Interdomain Routing Security

ACM Reference format:
Yossi Gilad, Omar Sagga, and Sharon Goldberg. 2017. MaxLength Considered Harmful to the RPKI. In *Proceedings of CoNEXT '17, Incheon, Republic of Korea, Deamber 12–15, 2017.* 7 pages.
DOI: 10.1145/3143361.3143363

1 INTRODUCTION

Efforts to secure interdomain routing with the Border Gateway Protocol (BGP) have been ongoing for decades. To date, however, the RPKI [14] is the only approach that has seen widespread deployment [20]. The IETF is diligently working towards standardizing BGPsec [13], a more robust security enhancement that should be de-

the most devastating attacks on BGP: *prefix hijacks* and *subprefix hijacks*.

However, RPKI objects have an attribute called *maxLength*, and when maxLength is misconfigured, it obviates most of the RPKI's security benefits. Specifically, an RPKI object with a misconfigured maxLength is vulnerable to a *forged-origin subprefix hijack* (an attack that was first outlined in [9]). We point out that this attack is as harmful as the traditional subprefix hijack that the RPKI is designed to prevent. We find that these misconfigurations are common: our network measurements confirm that the vast majority of RPKI objects that use maxLength in the wild are vulnerable to this attack. We argue that the RPKI RFCs are not sufficiently consistent on the limitations of maxLength. We also show how most of the benefits attained through maxLength can be achieved without exposing users to attacks, and present open-source software that achieves this goal. We conclude with operational recommendations for the use of maxLength.

2 HOW THE RPKI SECURES BGP

We use a running example to review how the RPKI secures routing.

ROAs. The RPKI uses Route Origin Authorizations (ROAs) to create a trusted mapping from an IP prefix to a set of autonomous systems (ASes) that are authorized to originate (i.e., claim to be the destination for) this prefix. Each ROA contains a set S of IP prefixes, and the identifying number of an AS authorized to originate all the IP prefixes in S; the ROA is cryptographically signed by the party that is authorized to allocate these IP prefixes.

For our running example, we use IP prefix 168.122.0.0/16 which contains all IPv4 addresses from 168.122.0.0 to 168.122.255.255. This IP prefix is allocated to Boston University (BU) which also has AS 111. Therefore, the RPKI should contain a ROA with the IP prefix 168.122.0.0/16 mapped to AS 111. This ROA would be digitally signed by a key that is certified by ARIN (the American Registry for Internet Numbers), the registry that allocated this IP prefix to



usenix
THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

Bamboozling Certificate Authorities with BGP

Henry Birge-Lee, Yixin Sun, Anne Edmundson, Jennifer Rexford, and Prateek Mittal, *Princeton University*

https://www.usenix.org/conference/usenixsecurity18/presentation/birge-lee

This paper is included in the Proceedings of the 27th USENIX Security Symposium.

August 15–17, 2018 • Baltimore, MD, USA

ISBN 978-1-931971-46-1

infoblox

Real world attacks: Softaculous (Aug 2026)

- On August 28, a BGP hijack was used as part of an attack on hosting software vendor Softaculous.
  - The attacker was able to deliver a “malicious Virtualizor update package” to a “small number of installations.”
  - Able to do so by obtaining a ***technically valid TLS certificate*** using a successful BGP hijack.
- Attacker used more-specific forged-origin hijack to defeat RPKI ROV and Multi-Perspective Issuance Corroboration (MPIC).
- Similar techniques used in 2022 attacks on cryptocurrency services KLAYswap and Celer Bridge.



https://www.kentik.com/blog/latest-bgp-hijack-targets-hosting-software-vendor/

Real world attacks: Softaculous (Aug 2026)

- Hijack included an AS path with a forged origin.
  - The attacker appended 24940 as the rightmost ASN in the path
- It was considered RPKI-valid for two reasons:
  1. ROA required the origin to be 24940
  2. *ROA allowed prefix length to be anywhere from /16 to /24.*
- Because there was no existing route for 162.55.80.0/24, it propagated as far as other route filtering mechanisms would allow.
- Because it was a more-specific route, any traffic destined for this IP range would prefer it over the legitimate route (162.55.0.0/16) due to routers' preference for longest-prefix-match.

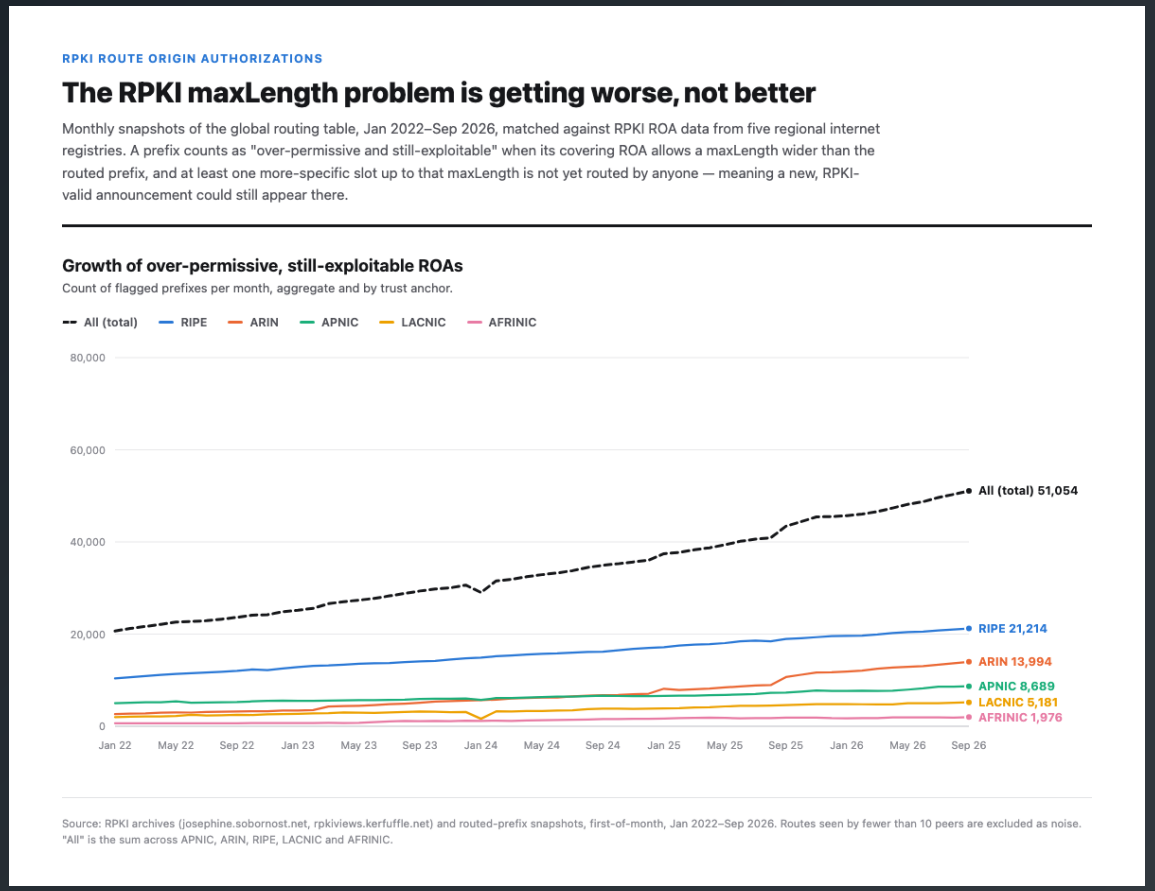


https://www.kentik.com/blog/latest-bgp-hijack-targets-hosting-software-vendor/

infoblox

Real world attacks: Softaculous (Aug 2026)

- Solution to non-minimal ROAs is outlined in RFC9319 (2022).
- Primary fix:
  - **Avoid using the maxLength field in ROAs (it's optional).**
- Main challenges are:
  - Quick traffic engineering
  - BGP-based DDoS mitigation
- For those scenarios, limit the maxLength field to only prefix lengths that might ever be announced (typically one level beyond the routed prefix length).
- ~50,000 routes on the Internet are currently subject to a similar style of attack.



https://www.kentik.com/blog/latest-bgp-hijack-targets-hosting-software-vendor/

infoblox

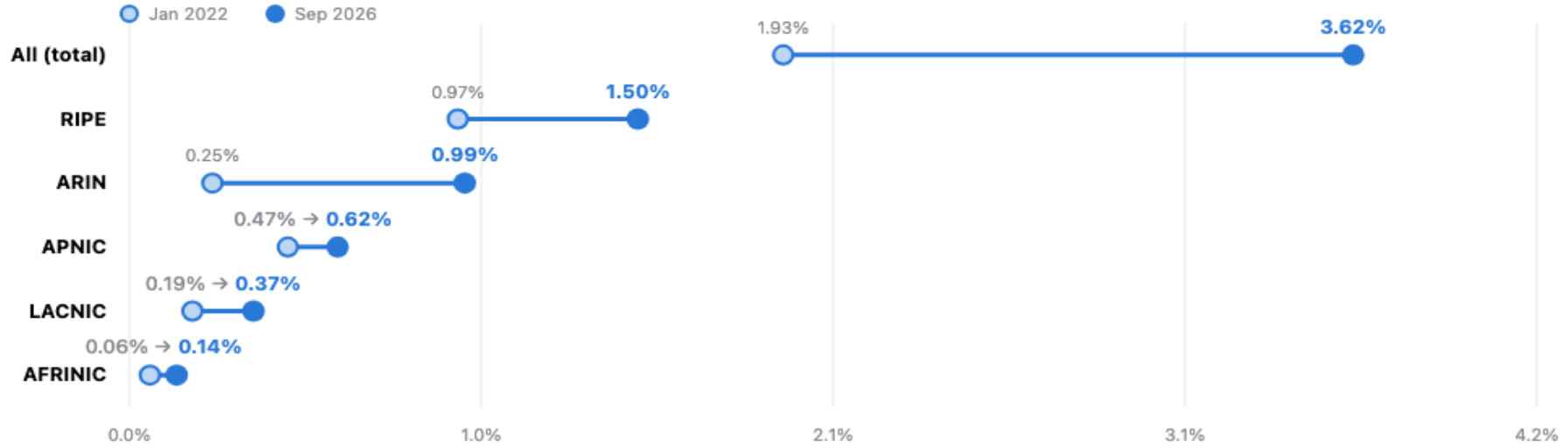
RPKI ROUTE ORIGIN AUTHORIZATIONS

The RPKI maxLength problem is getting worse, not better

Monthly snapshots of the global routing table, Jan 2022–Sep 2026, matched against RPKI ROA data from five regional internet registries. A prefix counts as "over-permissive and still-exploitable" when its covering ROA allows a maxLength wider than the routed prefix, and at least one more-specific slot up to that maxLength is not yet routed by anyone — meaning a new, RPKI-valid announcement could still appear there.

Share of the global routing table

Still-exploitable prefixes as a percentage of all routed prefixes, start vs. end of the analysis period.



Source: RPKI archives (josephine.sobornost.net, rpkiviews.kerfuffle.net) and routed-prefix snapshots, first-of-month, Jan 2022–Sep 2026. Routes seen by fewer than 10 peers are excluded as noise. "All" is the sum across APNIC, ARIN, RIPE, LACNIC and AFRINIC.

RPKI ROUTE ORIGIN AUTHORIZATIONS

Top ASNs by number of BGP routes with non-minimal ROAs

Top 10 origin ASNs within each RIR trust anchor

RIPE		ARIN		APNIC		LACNIC		AFRINIC	
21,422 routes in total		14,944 routes in total		8,645 routes in total		5,288 routes in total		2,103 routes in total	
AS51167	502	AS16509	1,932	AS9829	348	AS28343	119	AS11404	116
AS47583	302	AS31898	1,493	AS4694	186	AS52580	62	AS11427	110
AS203020	273	AS62904	465	AS9583	165	AS28006	57	AS29975	101
AS3215	257	AS54253	425	AS53813	156	AS3816	51	AS138915	61
AS16509	224	AS22616	243	AS55836	143	AS7418	48	AS20011	59
AS200845	223	AS398101	225	AS45271	135	AS13489	46	AS32043	46
AS9009	174	AS30103	204	AS10010	121	AS262907	39	AS36916	46
AS62044	165	AS6079	191	AS9299	120	AS14754	38	AS214143	41
AS212238	136	AS63949	184	AS16509	119	AS14080	36	AS36924	36
AS61157	135	AS3257	156	AS7713	114	AS22927	34	AS328608	34

A route is counted when its covering ROA's maxLength is longer than the routed prefix and at least one more-specific slot up to that maxLength is not yet routed by anyone, so a new RPKI-valid announcement could still appear. Routes seen by fewer than 10 peers are excluded. Data: routing snapshot 8 Oct 2026 12:00 UTC, RPKI snapshot 12:07 UTC. Bars are scaled within each trust anchor, so lengths are not comparable across panels.


THE ROAD AHEAD

What 17 years of watching BGP taught me

Geopolitical

- Internet shutdowns and blockages aren’t ending anytime soon.
  - As they become more sophisticated, they are becoming harder to measure.
  - Iran 2026: routes stayed up while the country went offline. Only traffic data showed it.
- Politics often shapes the paths that Internet traffic takes.
  - From Cuba to Kherson, BGP followed politics.
- Digital authoritarianism will continue to innovate.
  - Other countries may adopt Iran’s allowlist system.
  - The digital rights community needs support and resources.

What 17 years of watching BGP taught me

BGP security

- We've made tremendous improvements!
  - Large-scale, debilitating route leaks are largely a thing of the past.
  - Most famous incidents couldn't happen today.
- The determined adversary finally gets its due.
  - ROV, ASPA, and one day BGPSEC.
  - The fight never stops. It's a multi-year project.

To-do list:

1. Create ROAs (without maxLength) & reject invalids.
2. Create ASPA records (while at LACNIC 46)
3. Periodically review AS-SETs, routing policy, prepending.

People overestimate what can be done in a year and underestimate what can be done in ten.

(attributed to Bill Gates)

infoblox

Siempre para adelante

- The Internet is the defining technology of modern civilization.
  - It is also a beautiful, remarkable, resilient thing.
- How will we survive this time of AI adolescence?
  - AI traffic volumes won't break the Internet, but the pace of novel exploits could.
- We can fix things collectively, and **communities like LACNIC matter**.



infoblox

THANK YOU!

Doug Madory
dmadory@infoblox.com

