

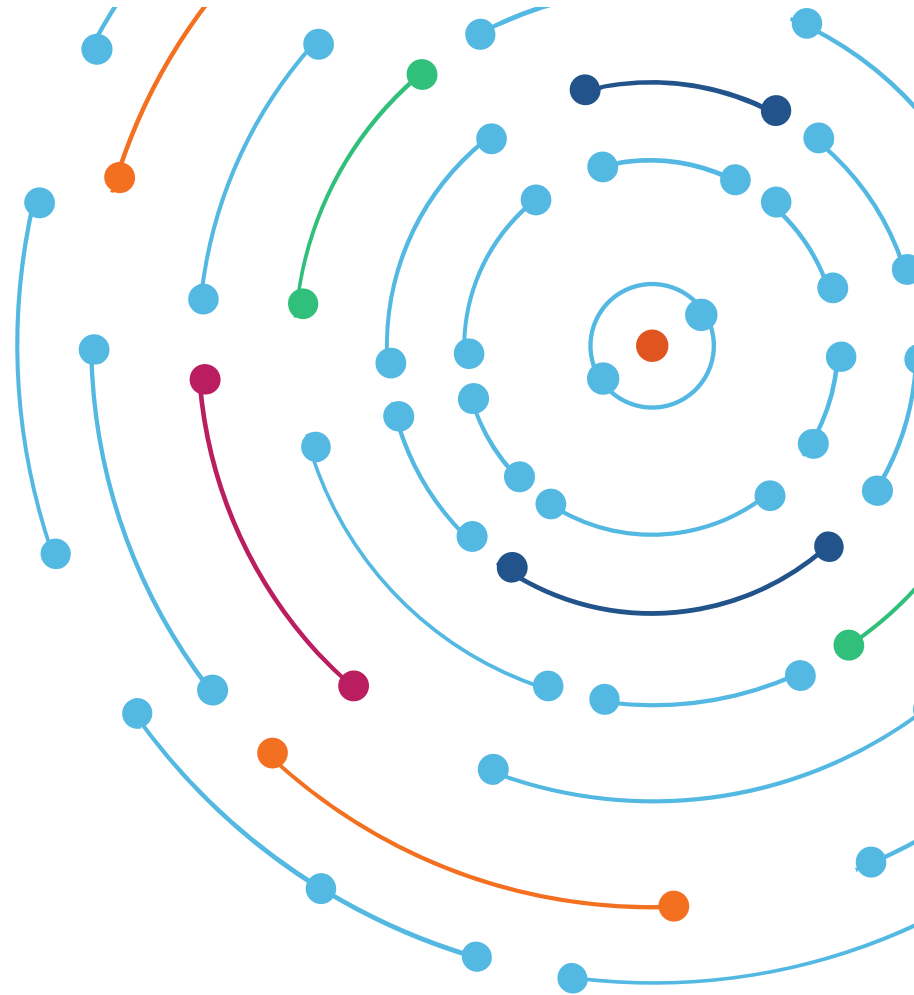


Turning a corner on BGP security?

Doug Madory

AUSNOG

2 September 2022



# Let's stroll through the history of BGP incidents

What's the problem with BGP incidents?

BGP routing incidents can be problematic because:

1. **Disruption** of flow of legitimate Internet traffic
2. **Misdirection** of communications, posing a security risk from interception or manipulation



# Let's stroll through the history of BGP incidents

Consider the spectrum of BGP incidents...

Bonehead errors



Determined adversary



*Degree of difficulty of mitigation*

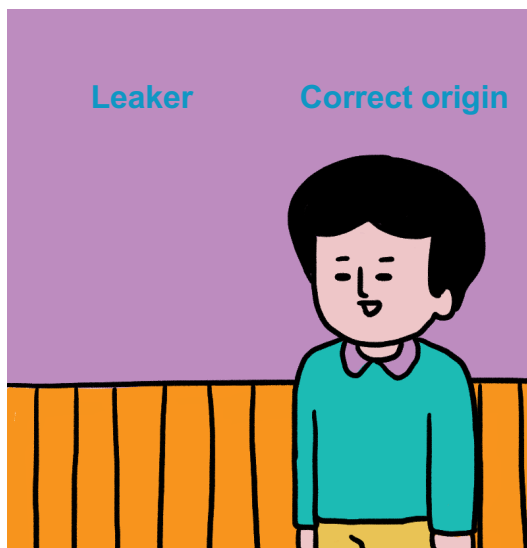
Until recently, we really couldn't prevent anything along this line.

# Strolling through the history of BGP incidents

## 1. Disruptions due to leaks

“A route leak is the propagation of routing announcement(s) beyond their intended scope.” - RFC7908 (Problem Definition and Classification of BGP Route Leaks)

### Origination



### Adjacency

Wrong export

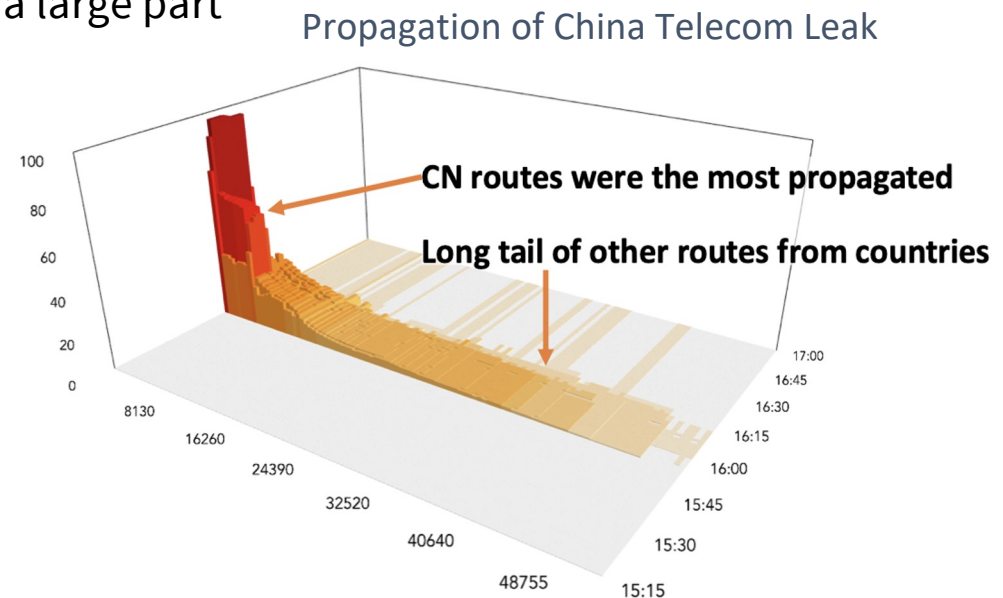


BGP announcements

# Strolling through the history of BGP incidents

## 1. Disruptions due to leaks - *Origin leaks*

- AS7007 leak (April 1997)
  - 1st major Internet disruption caused by a routing leak
  - Software bug caused a router to originate a large part of the global routing table
- Numerous large origination leaks since AS7007:
  - Turk Telecom leak (Dec 2004)
  - China Telecom leak (Apr 2010)
  - Telecom Malaysia leak (Jun 2015)
  - And more...

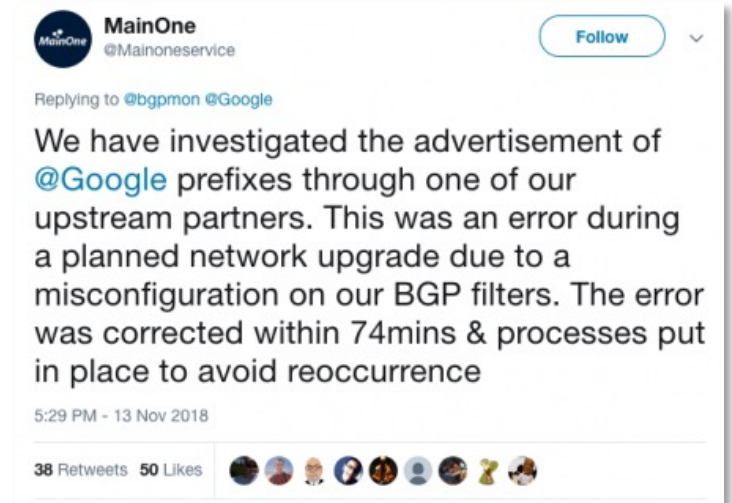


Visualizing Routing Incidents in 3D (NANOG 78)

# Strolling through the history of BGP incidents

## 1. Disruptions due to leaks - *Adjacency leaks*

- MainOne (AS37282) leak (Nov 2018)
  - Passed peer routes to transit providers.
  - China Telecom carried routes to Internet
  - Google, Cloudflare among disrupted networks.
- Allegheny Technologies (AS396531) leak (Jun 2019)
  - ~29k routes passed from one provider to another.
  - Route-optimizer generated many more-specifics.
  - Cloudflare experienced largest disruption as a result.
- Origins *were intact* in these leaks.
  - Ex leaked Google path: ... 4809 37282 15169
  - Ex leaked Cloudflare path: ... 701 396531 33154 13335



Strolling through the history of BGP incidents  
**2. Misdirection of communications (hijacks!)**

**Global routing system can be (*and has been*)  
manipulated to redirect Internet traffic**



# Strolling through the history of BGP incidents

## 2. Misdirection of communications (hijacks!)

- 2008: Pilosov-Kapela theorizes use of BGP in MITM attack
- 2013: Renesys identifies MITM BGP hijacks coming from Belarus
  - Used BGP communities to shape route propagation
  - Targeted US financial institutions and foreign ministries of numerous governments



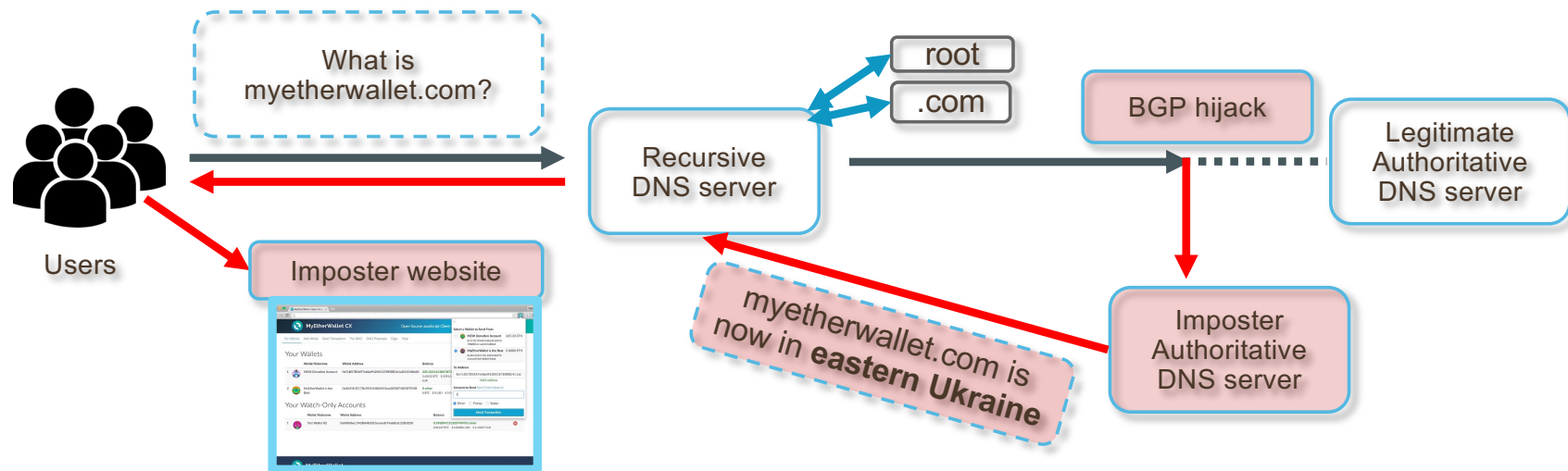
<https://www.wired.com/2013/12/bgp-hijacking-belarus-iceland/>



# Strolling through the history of BGP incidents

## 2. Misdirection of communications (hijacks!)

- BGP Hijack of Amazon DNS to Steal Crypto Currency (April 2018)

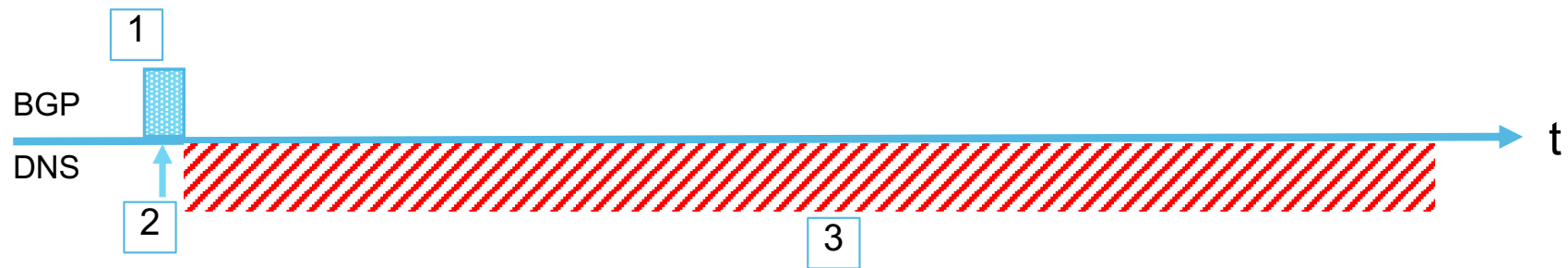


- When queried for myetherwallet.com, an imposter authoritative DNS service returned an IP in eastern Ukraine (Lugansk People's Republic).
- Hosted on this IP was a fake copy of the myetherwallet.com site ready to steal their currency as soon as they login.

# Strolling through the history of BGP incidents

## 2. Misdirection of communications (hijacks!)

- Just 3 Months after the Route53 hijack, another BGP/DNS hijack
- This time Digital Wireless Indonesia (AS38146) briefly hijacked prefixes hosting the nameservers of major payment processors (Vantiv, Worldpay, Datawire, etc)



1. Brief BGP hijack: As long as a major public DNS service accepted the route, affected population could be very large.
2. Attackers could time queries to public DNS service to ensure bogus record was cached.
3. TTLs of forged responses were ~1 week (normally 600 sec).  
*Needed to be flushed to stop the misdirection.*

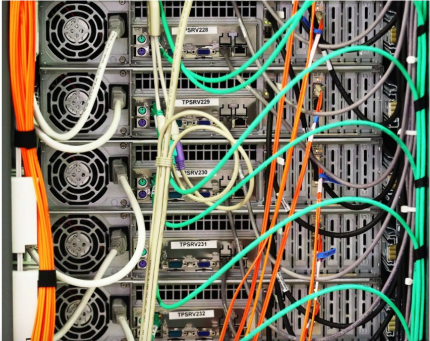
🐱 *Bridging gap protocol is hopeless!* 🐱

WIRED BACKCHANNEL BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY MY ACCOUNT

LILY HAY NEWMAN SECURITY JUN 28, 2019 12:38 PM

## The Infrastructure Mess Causing Countless Internet Outages

You may not have heard of the Border Gateway Protocol, but you definitely know when it goes wrong.



FACEBOOK OUTAGE

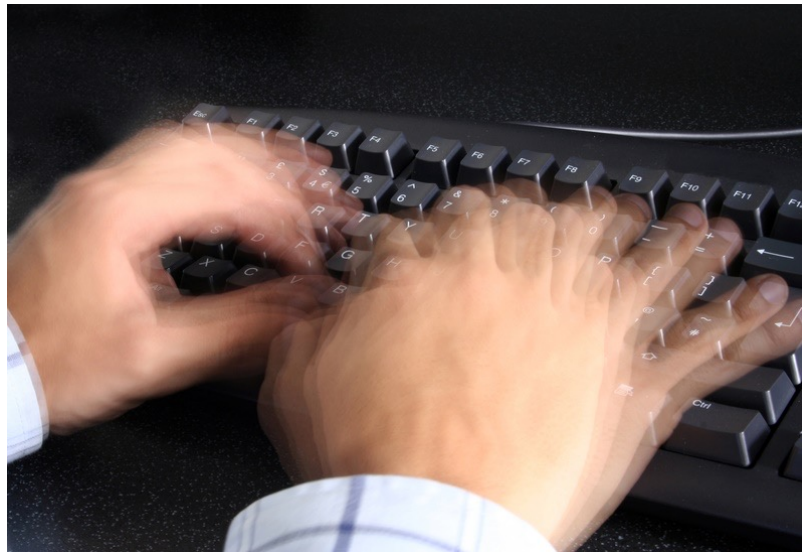
Hello. Fancy a coffee?

Bridging Gap Protocol

sly news .com ing young people's mental health **BREAKING NEWS** Facebook's Director of Polic

*But wait ... is it though?*

Ask yourself:  
When was the last debilitating BGP routing leak?

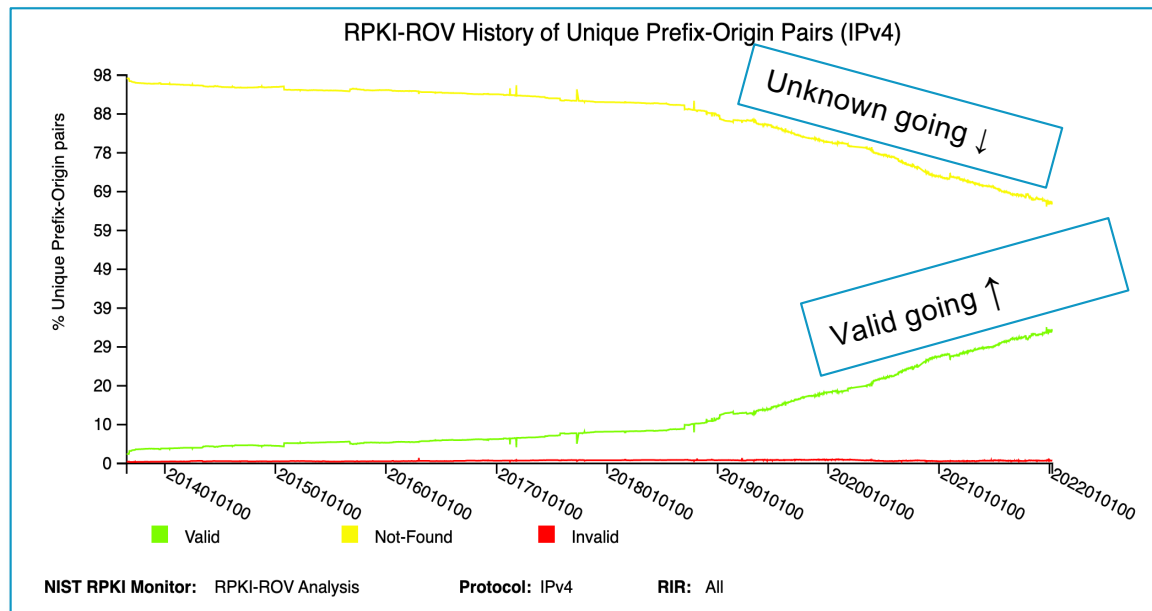


*Are our fingers getting less fat? Definitely not.*

# Strolling through the history of BGP incidents

## 4. We're making progress ... no really!

- Enormous progress in recent years as Tier-1 NSPs agreed to reject RPKI-Invalids.
  - NTT, GTT, Arelion (Telia), Cogent, Telstra, PCCW, Lumen, and more!
- According to NIST RPKI Monitor, the trend line is going in the right direction!

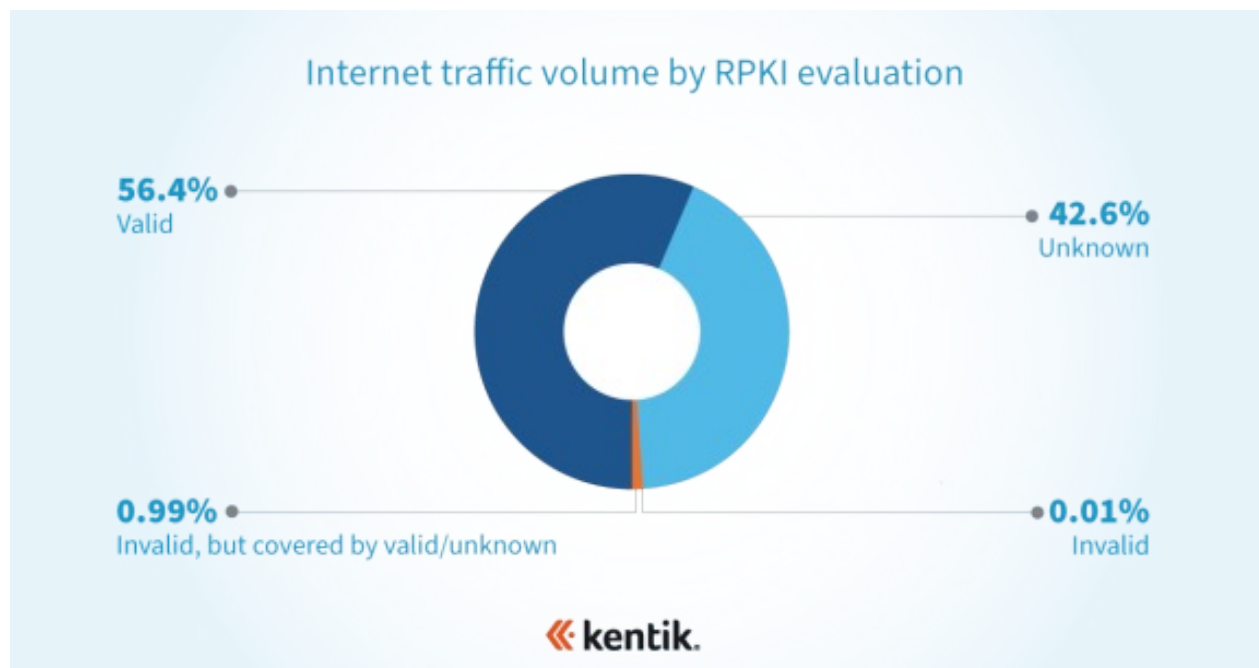


<https://rpki-monitor.antd.nist.gov>

# Strolling through the history of BGP incidents

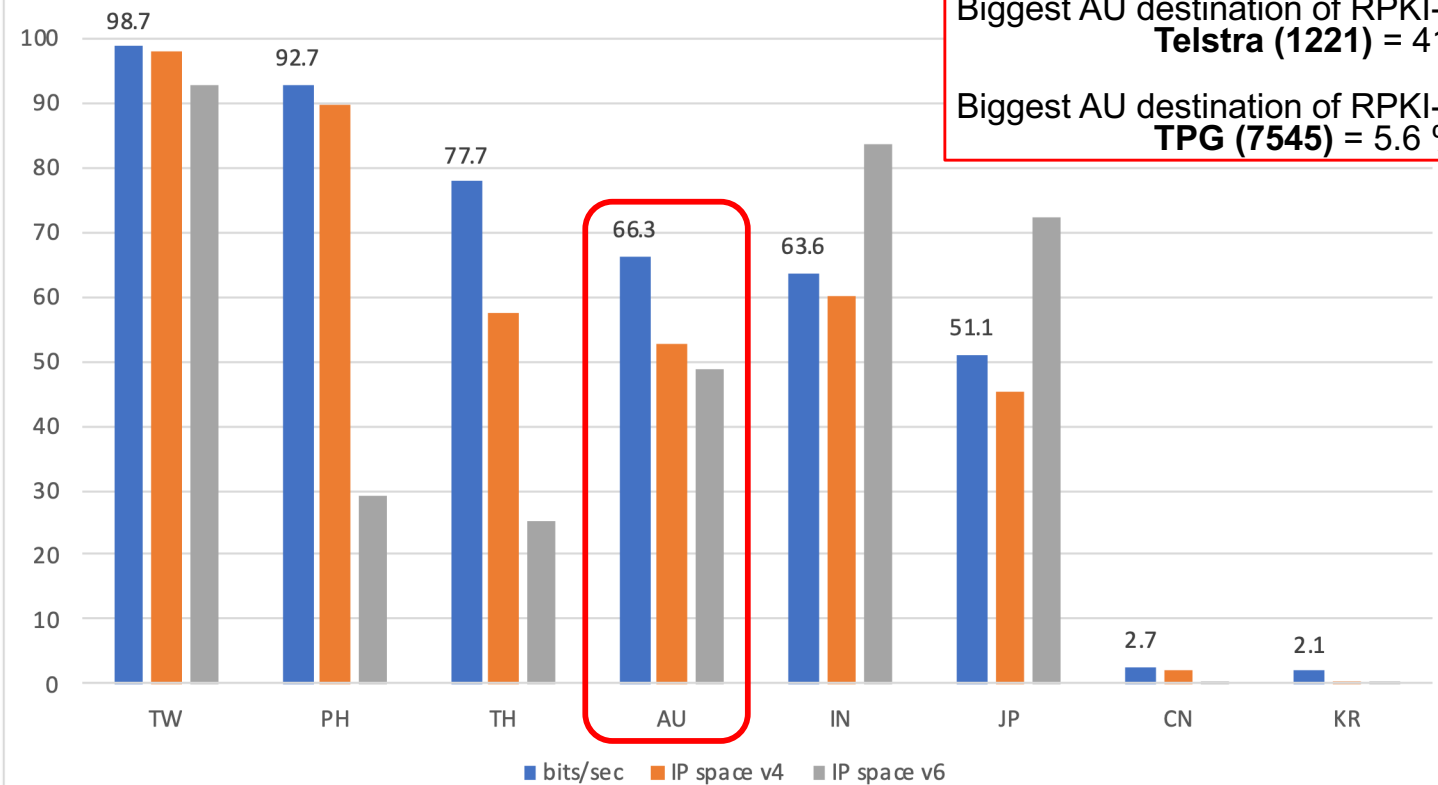
## 4. We're making progress ... no really!

Only ~1/3 of BGP routes have ROAs - but how much traffic? The **majority** of it.



Measuring RPKI ROV adoption in NetFlow (NANOG 85)

### ROA Measurement (%) Asia & Australia

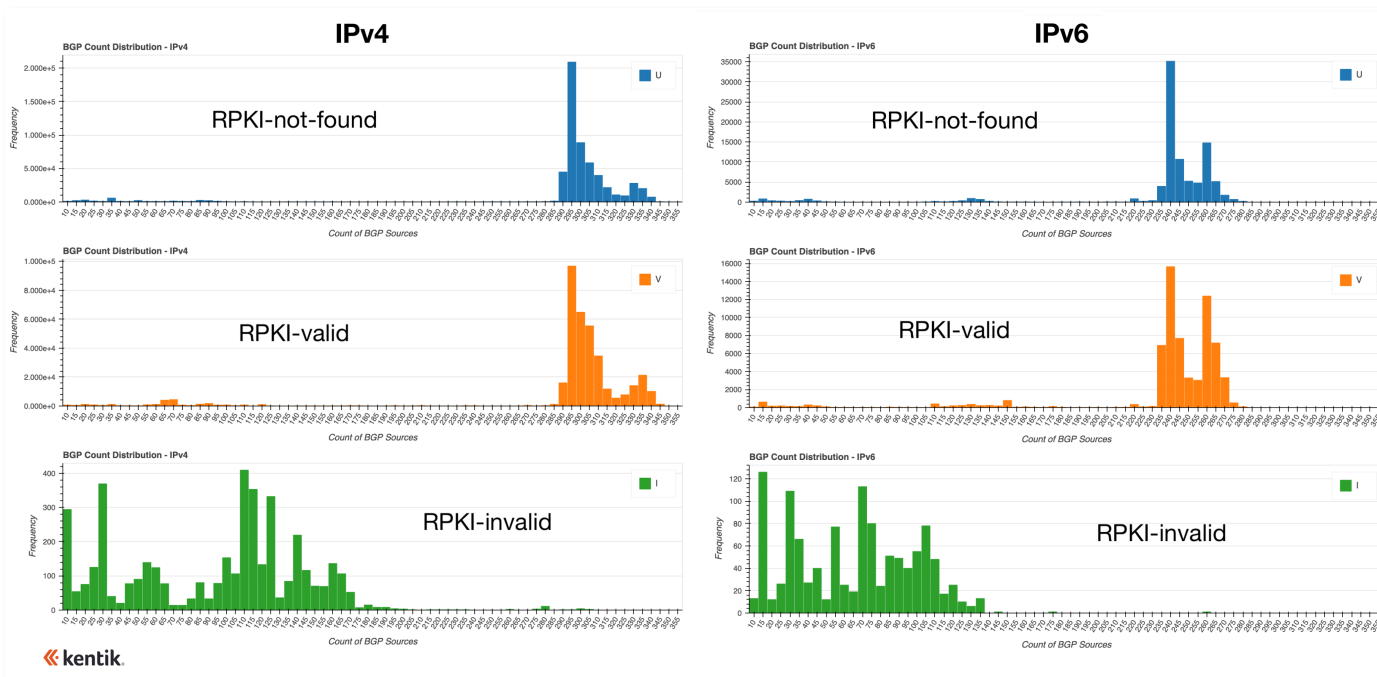


Biggest AU destination of RPKI-valid traffic:  
**Telstra (1221) = 41.6%**

Biggest AU destination of RPKI-not-found traffic:  
**TPG (7545) = 5.6 %**

# Is RPKI ROV reducing the propagation of RPKI-invalid routes?

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



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



Facts I'd like to become common knowledge in networking:

- 1) The majority of internet traffic is directed to RPKI-valid routes,**
- 2) Route propagation is cut in half when evaluated as RPKI-invalid.**

Many engineers at many companies have worked very hard to get us here.

# Strolling through the history of BGP incidents

## 5. More progress to come

Expect to hear from a certain routing security evangelist soon!

- Peerlock ✓
- Using RPKI to cleanup IRR ✓
- RPKI ✓
  - To reduce impacts of fat-fingers.
- BGPSEC
  - To eliminate origin impersonation.
- ASPA (IEFT draft)
  - To reduce impacts of adjacency leaks.



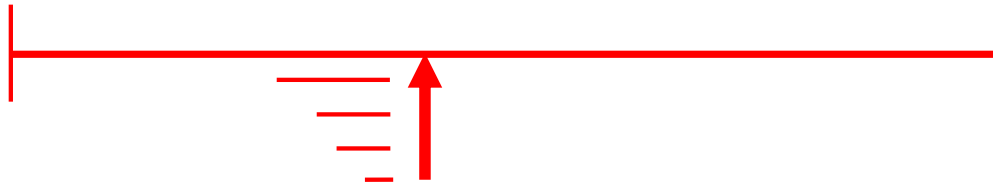
We're "moving the needle" on routing security!

Things are improving and it isn't by accident.

Bonehead errors



Determined adversary



Let's go!



Thank you!

Doug Madory  
@dougmadory  
dmadory@Kentik.com

Copyright © 2021 Kentik. All rights reserved.

