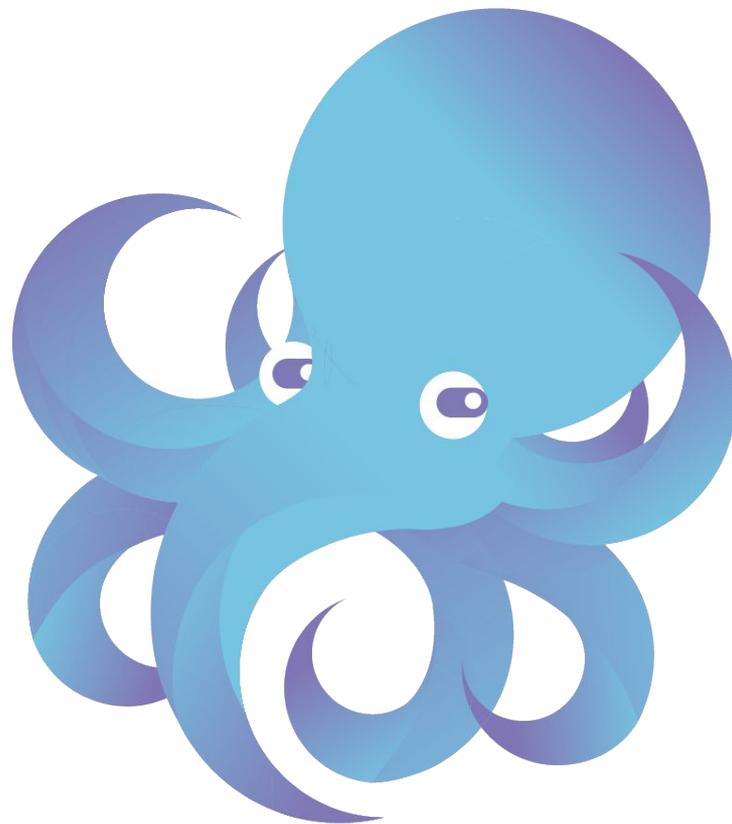




RPKI, Real World Examples

Louis Poinsignon



Introduction

Network Engineer at Cloudflare in San Francisco

Open-source projects including flows and RPKI

Network data collection (BGP, flows, peering-portal)

Talk is short, feel free to ask questions!



<https://blog.cloudflare.com/rpki-details/>
<https://blog.cloudflare.com/rpki/>

RPKI Today

Statistics

22907 ROA files

12905 Certificates

9 rsync paths (5 root, 4 subroots)

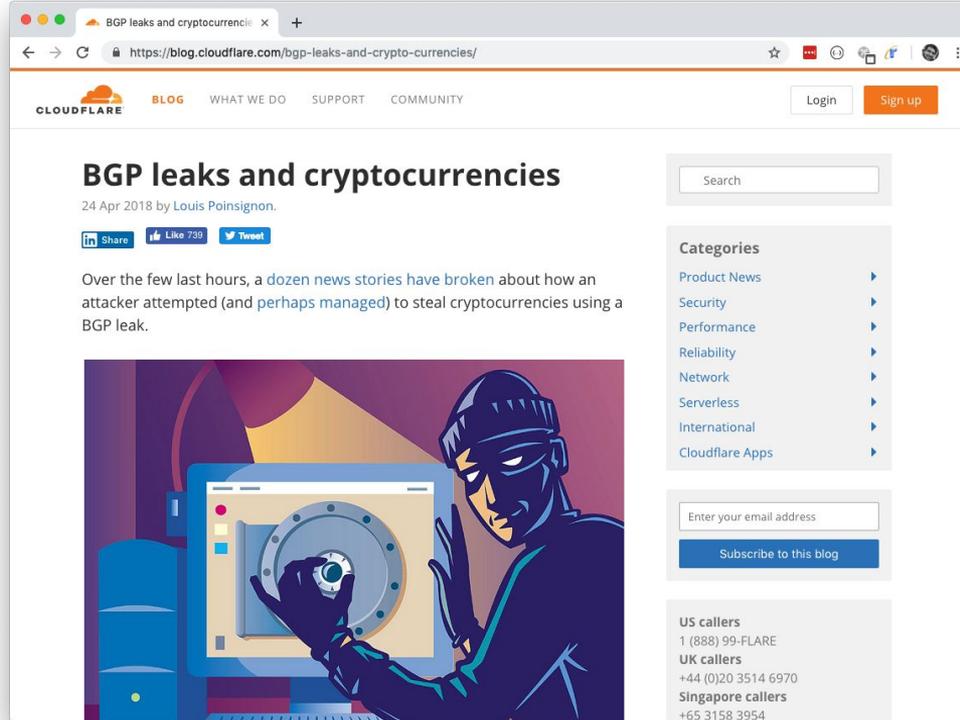
10021 unique ASN

89262 unique prefixes

⇒ 29885 aggregates signed

⇒ 508 millions signed IPv4

How did it start?



The screenshot shows a web browser window displaying a blog post on the Cloudflare website. The browser's address bar shows the URL <https://blog.cloudflare.com/bgp-leaks-and-crypto-currencies/>. The page header includes the Cloudflare logo, navigation links for 'BLOG', 'WHAT WE DO', 'SUPPORT', and 'COMMUNITY', and buttons for 'Login' and 'Sign up'. The main content area features the article title 'BGP leaks and cryptocurrencies' by Louis Poinignon, dated 24 Apr 2018. Below the title are social sharing buttons for LinkedIn, Facebook (739 likes), and Twitter. The introductory text states: 'Over the few last hours, a dozen news stories have broken about how an attacker attempted (and perhaps managed) to steal cryptocurrencies using a BGP leak.' An illustration of a hacker in a dark hood and mask working at a computer with a glowing screen is positioned below the text. To the right of the main content, there is a search bar, a 'Categories' sidebar with links to Product News, Security, Performance, Reliability, Network, Serverless, International, and Cloudflare Apps, an email subscription form with a 'Subscribe to this blog' button, and contact information for US, UK, and Singapore callers.

BGP leaks and cryptocurrencies

24 Apr 2018 by Louis Poinignon.

[Share](#) [Like 739](#) [Tweet](#)

Over the few last hours, a dozen news stories have broken about how an attacker attempted (and perhaps managed) to steal cryptocurrencies using a BGP leak.

Categories

- Product News
- Security
- Performance
- Reliability
- Network
- Serverless
- International
- Cloudflare Apps

Enter your email address

Subscribe to this blog

US callers
1 (888) 99-FLARE
UK callers
+44 (0)20 3514 6970
Singapore callers
+65 3158 3954

The Initial Story

Authority DNS route hijack in April 2018.

This affected our DNS Resolver.

The route was sent to us on a Chicago peering session.

What should we do?

The Initial Story

At the time...

150+ unique cities, 26000 BGP sessions, IP space in 5 RIRs

Just the RIPE Validator^[1]

How to distribute a prefix list efficiently?

The Initial Story

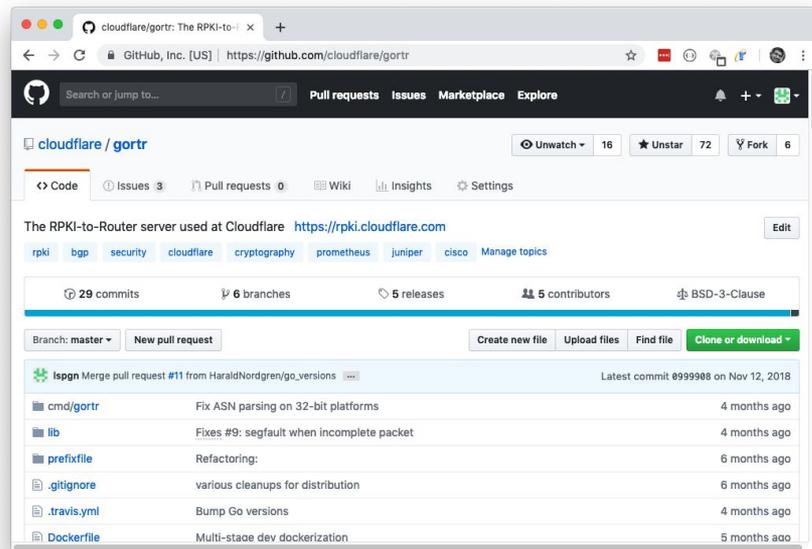
July: started deploying internally GoRTR.

August: open-source release.

<https://github.com/cloudflare/gotr>

September → December:

- Turn up RTR sessions
- Signing prefixes



Effects

The question everyone asked us.

How much traffic was affected?

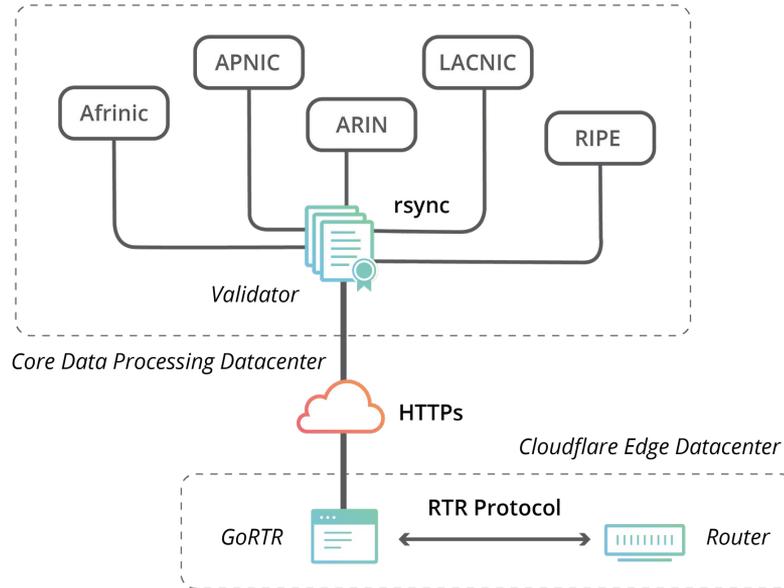
Many invalids. Little traffic in practice (default or valid less specific).

Except in one place. Few gigabits per seconds displaced due to geographical more specific.



<https://www.flickr.com/photos/thure/6287816628/>

Diagram



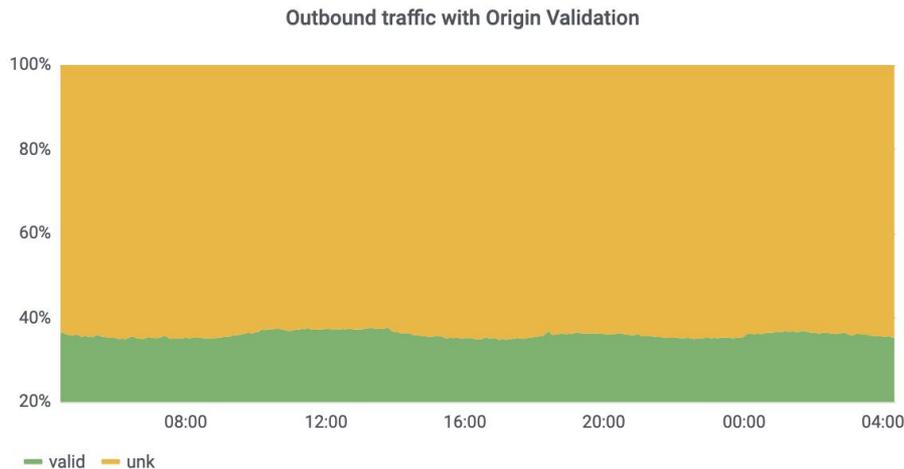
Accounting

Using flows, we see **at least 30%** of the traffic being **valid**. Very **little/none invalid**.

We use **GoFlow** for accounting.

Other tools compatible with flows:

pmacct and Kentik



Cloudflare's Validator

Sets of libraries and tools written in Go.

Including, a validator ***OctoRPKI*** 

<https://github.com/cloudflare/cfrpki>

GoRTR

OctoRPKI does not embed a RTR server. Modular and independence!

Fully compatible with **GoRTR**

<https://github.com/cloudflare/gortr>

Signs the prefix list to ensure a safe distribution of the file.

Can run natively on Juniper!

```
$ docker run -ti \  
  -p 8082:8082 \  
  -v $PWD/example.pub:/example.pub \  
  cloudflare/gortr \  
  -verify.key /example.pub \  
  -cache https://YOUR_ROA_URL
```

RPKI without installing anything

GoRTR without OctoRPKI will fetch Cloudflare's public list of prefixes

or

SSH: `rtr.rpki.cloudflare.com:8283` (user: rpki/pass: rpki)

and

Plaintext: `rtr.rpki.cloudflare.com:8282`



Just configure your router

Cloudflare's RPKI Portal

rpki.cloudflare.com

The screenshot shows the 'Route Validator' section of the RPKI Portal. It features a green box indicating that the route 1.1.1.0/24 is valid, originating from AS13335, and is covered by one RPA. Below this, a table lists the covering ROAs.

Validating route **1.1.1.0/24**
from origin **AS13335**
Valid
1 covering RPA found

Covering ROAs:

Trust Anchor	Prefix	Max Length	ASN	Expiration	Match
APNIC	1.1.1.0/24	24	13335	in 2 years	✓

The screenshot shows the 'Resource List' view of the RPKI Portal. It displays search filters and a table of ROAs. The first row in the table is for AS13335, covering prefix 1.0.0.0/24. Below the table, detailed information for this ROA is provided, including its name, trust anchor, key, parent key, path, validity, and emission dates.

Found 2 ROAs and 9 certificates

ROAs

ASN	Prefix	Max Length	IP Family	Trust Anchor	Emitted	Expiration
AS13335	1.0.0.0/24	/24	IPv4	APNIC	3/16/2018	in 2 years

Name: 5aabf815-9744
Trust Anchor: APNIC
Key: aa24090e86c3bc39ee7ac345b3bf9a38cd9ff3ad
Parent Key: 68faf9dace19768cac3d4ed7bb24372bffa6d018
Path: rsync://rpki.apnic.net/member_repository/A91872ED/ED8C96901D6C11E28A38A3AD08B02CD2/797B4DEC29B11E8B187196DC4F9AE02.roa
Validity: Fri, 16 Mar 2018 17:00:05 GMT - Wed, 31 Mar 2021 00:00:00 GMT
Emitted: Fri, 16 Mar 2018 17:00:05 GMT
ASN: 13335
Prefix: 1.0.0.0/24
Max Length: /24

Recent Leaks And Conclusions

Summary of Amazon Route Hijack

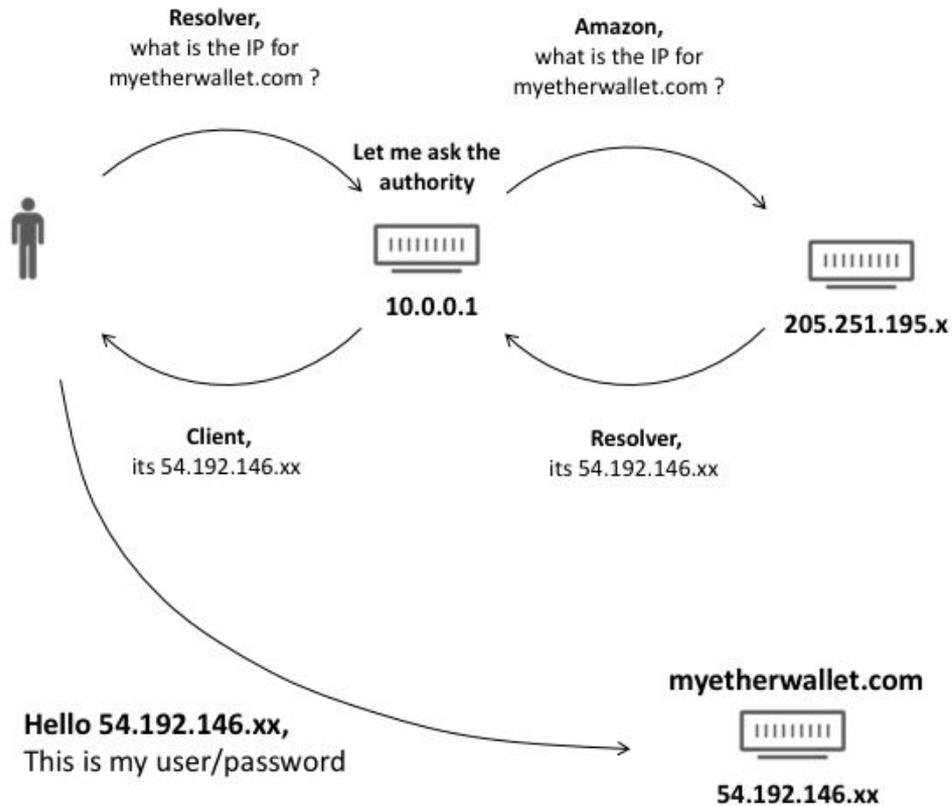
An attacker announces Amazon Authority DNS prefixes.

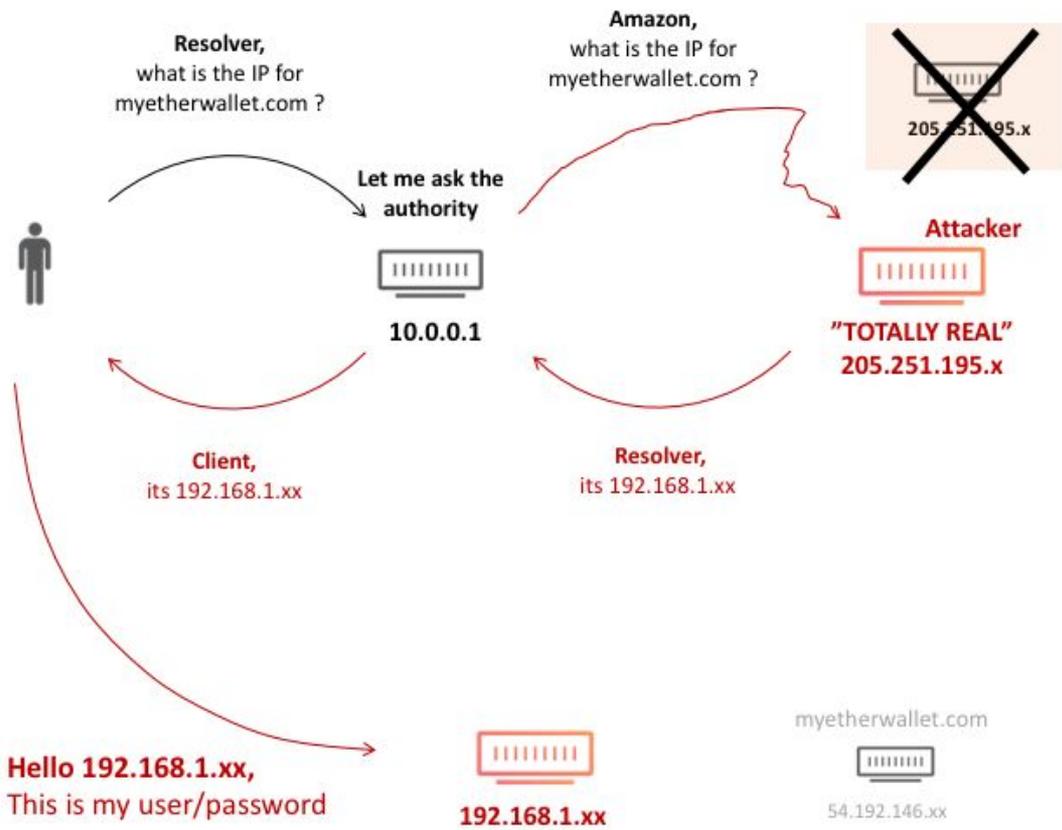
Cloudflare and Google accept them in specific locations.

Cloudflare and Google DNS resolvers use this route when clients request the website, the attacker's server is returned.

The server has a phishing website for the client.

Attacker gather credentials and steals Bitcoins.





Summary of Amazon Route Hijack

Amazon did not have signed routes.

Cloudflare did not do RPKI validation + route filtering

If RPKI was deployed:

Route would have been rejected because wrong origin.

Summary of Verizon Route Leak

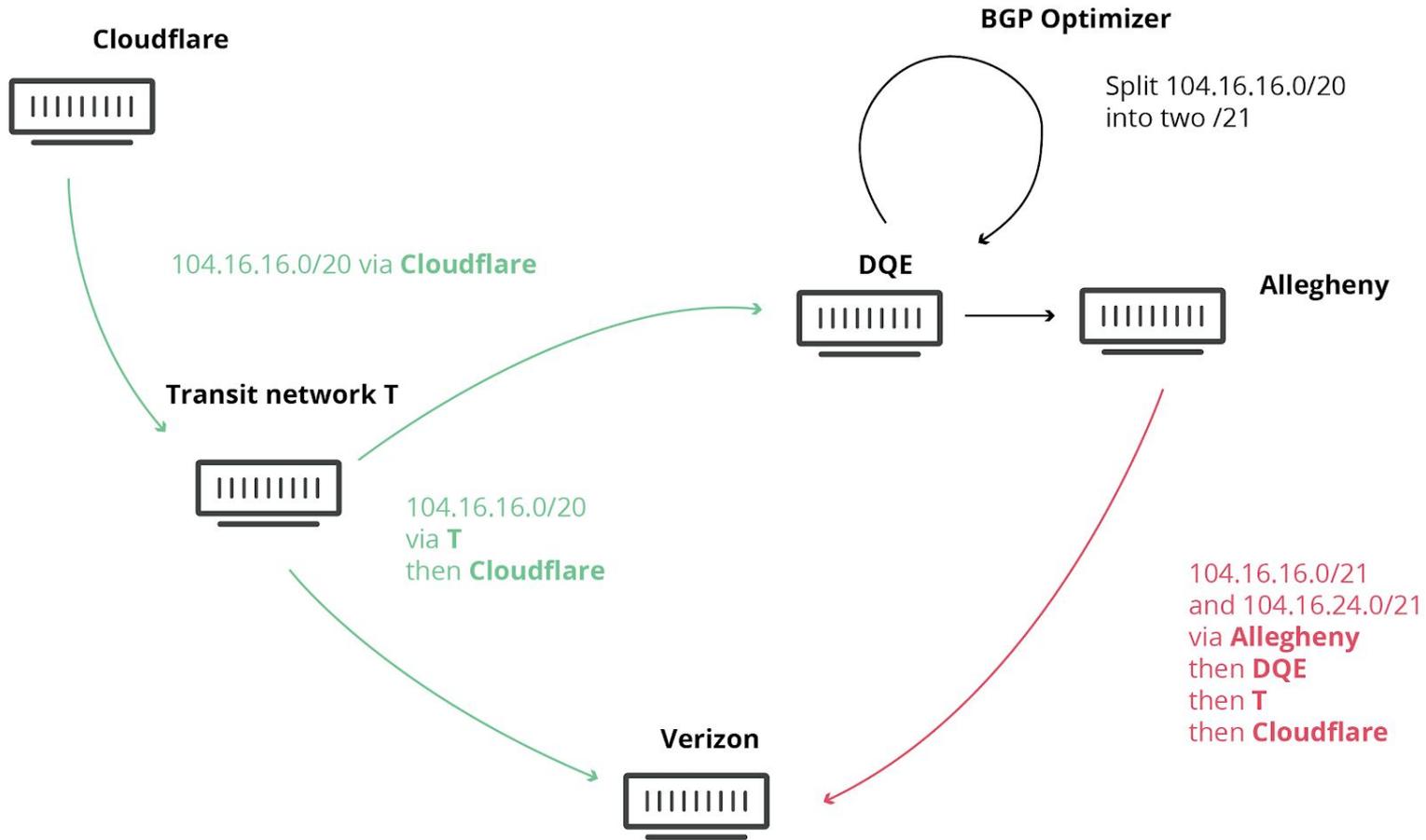
A company has two Internet accesses: Verizon and another ISP.

The ISP has a BGP optimizer which feeds more-specific routes.

Unfortunately, the ISP sends the routes to the company which end up being sent to Verizon.

Verizon did not filter them and re-announces them to its peers and clients.

Cloudflare loses traffic.



Summary of Verizon Route leak

Cloudflare had signed routes.

Verizon did not filter. Many networks accepted the leak.

Cloudflare filtering routes did not matter here.

If basic filtering was deployed:

Peering sessions would have been removed when going above prefix threshold.

AS-Path filtering could have avoided accepting routes.

If RPKI was deployed:

Routes would have been rejected because wrong length.

What we learned

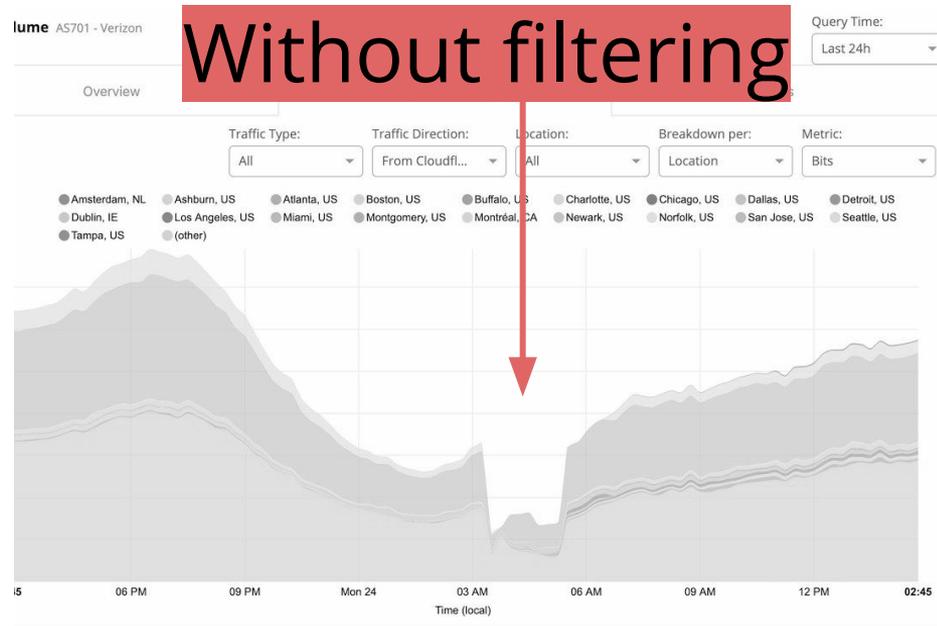
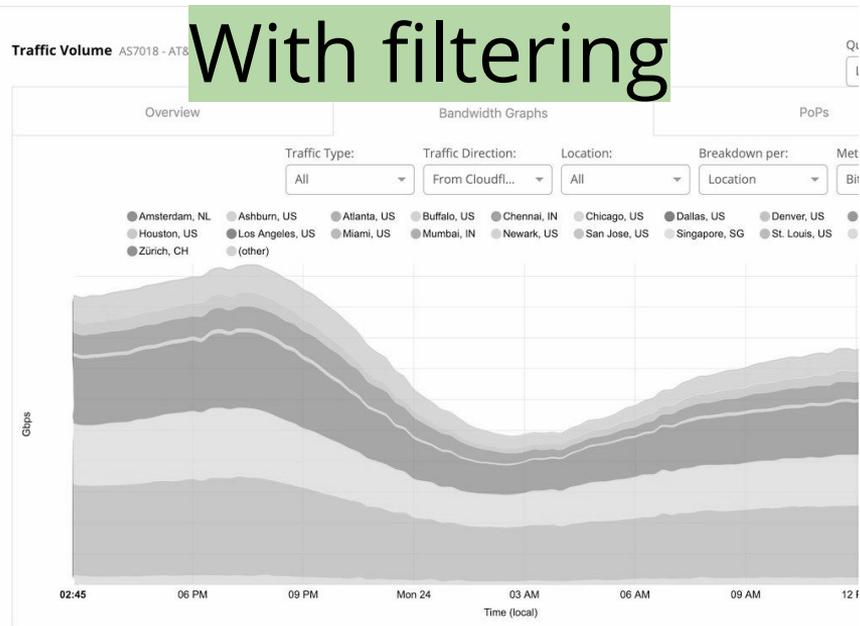
RPKI will not be the solution to everything. But in our stories...

Filtering solves Amazon being hijacked

Signing helps your network not being leaked

Deploy RPKI now

Because tomorrow is already too late



Thank you

Questions?

louis@cloudflare.com
[@lpoinsig](https://twitter.com/lpoinsig) (twitter)

