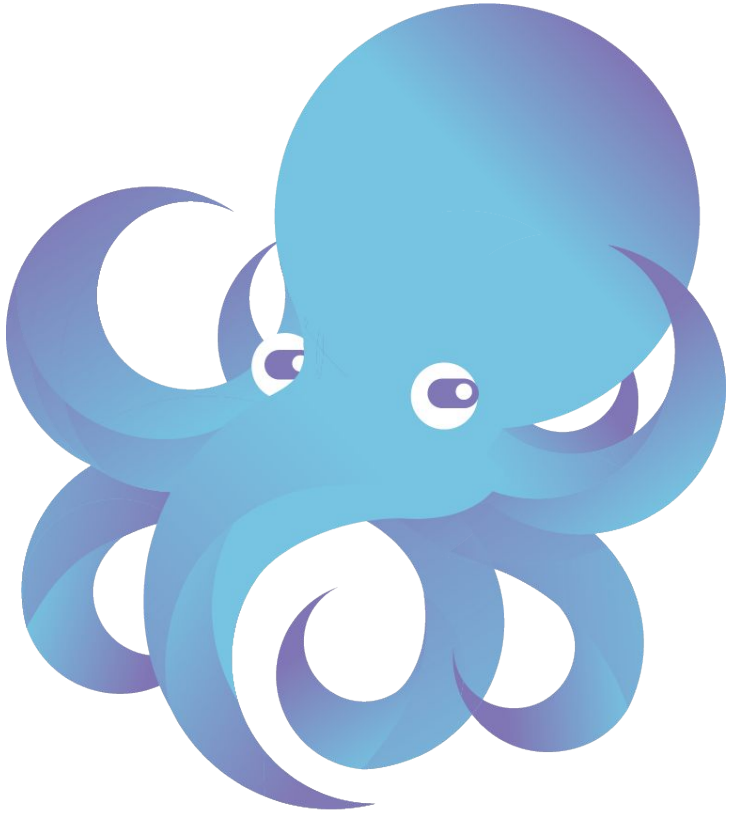
CLOUDFLARE



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!

CLOUDFLARE

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

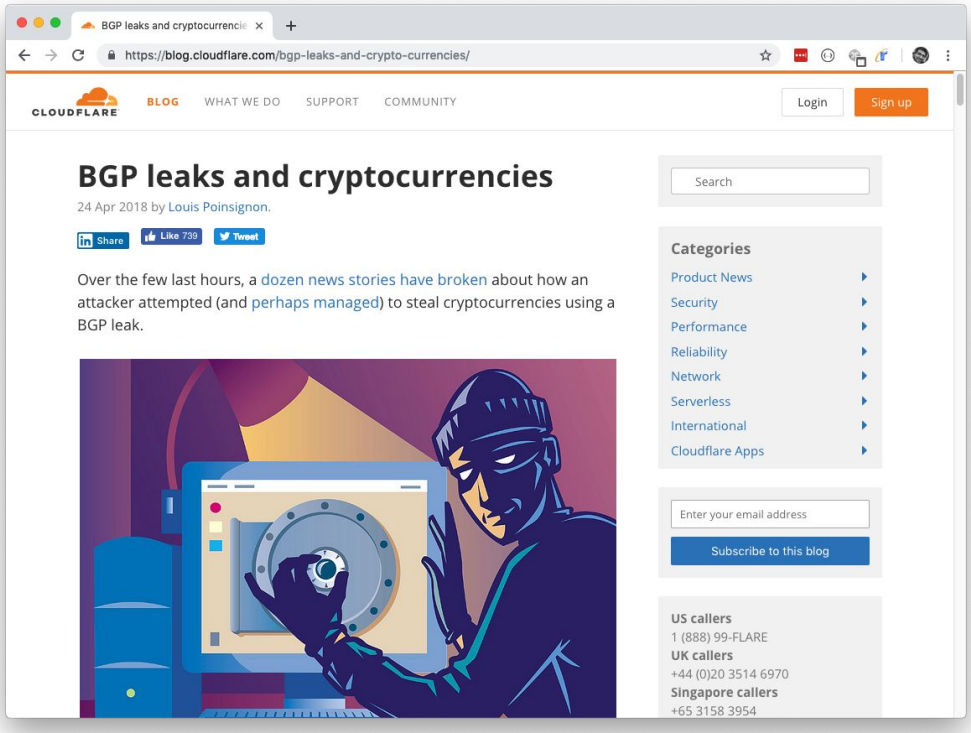
89262 unique prefixes

⇒ 29885 aggregates signed

⇒ 508 millions signed IPv4

CLOUDFLARE

How did it start?



CLOUDFLARE

https://blog.cloudflare.com/bgp-leaks-and-crypto-currencies/

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?

CLOUDFLARE

[1] Cloudflare is very grateful for the RIPE Validator s/w

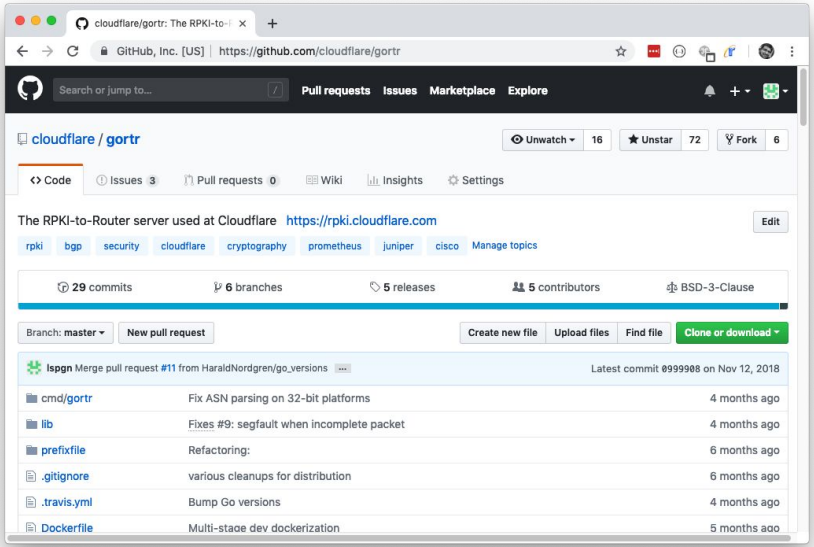
The Initial Story

July: started deploying internally GoRTR.

August: open-source release.
https://github.com/cloudflare/gortr

September → December:

- Turn up RTR sessions
- Signing prefixes



CLOUDFLARE

Effects

The question everyone asked us.

How much traffic was affected?

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

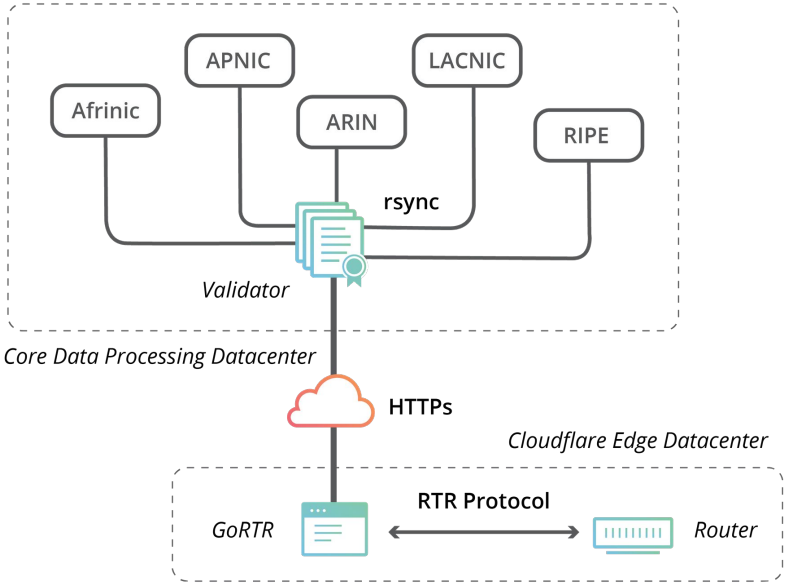
https://www.flickr.com/photos/thure/6287816628/

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

CLOUDFLARE

Tooling

Diagram



CLOUDFLARE

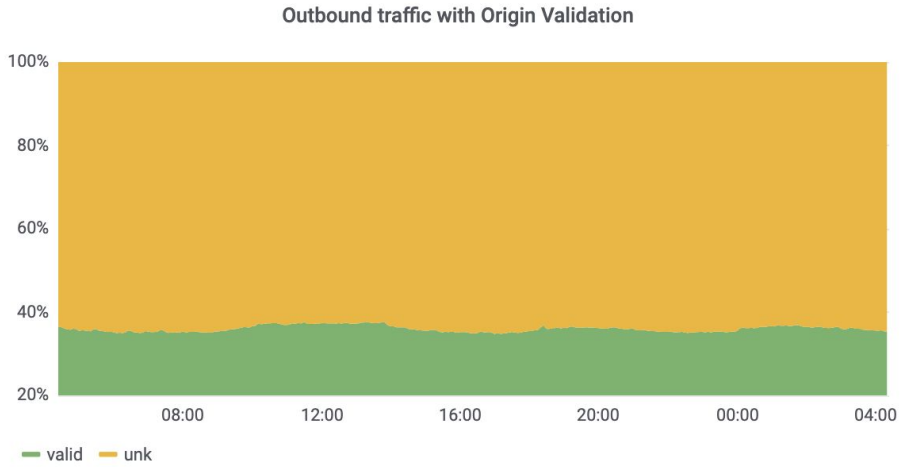
Accouting

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

Cloudflare's Validator

Sets of libraries and tools written in Go.

Including, a validator ***OctoRPKI*** 

https://github.com/cloudflare/cfrpki

CLOUDFLARE

https://blog.cloudflare.com/cloudflares-rpki-toolkit/

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
```

CLOUDFLARE

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

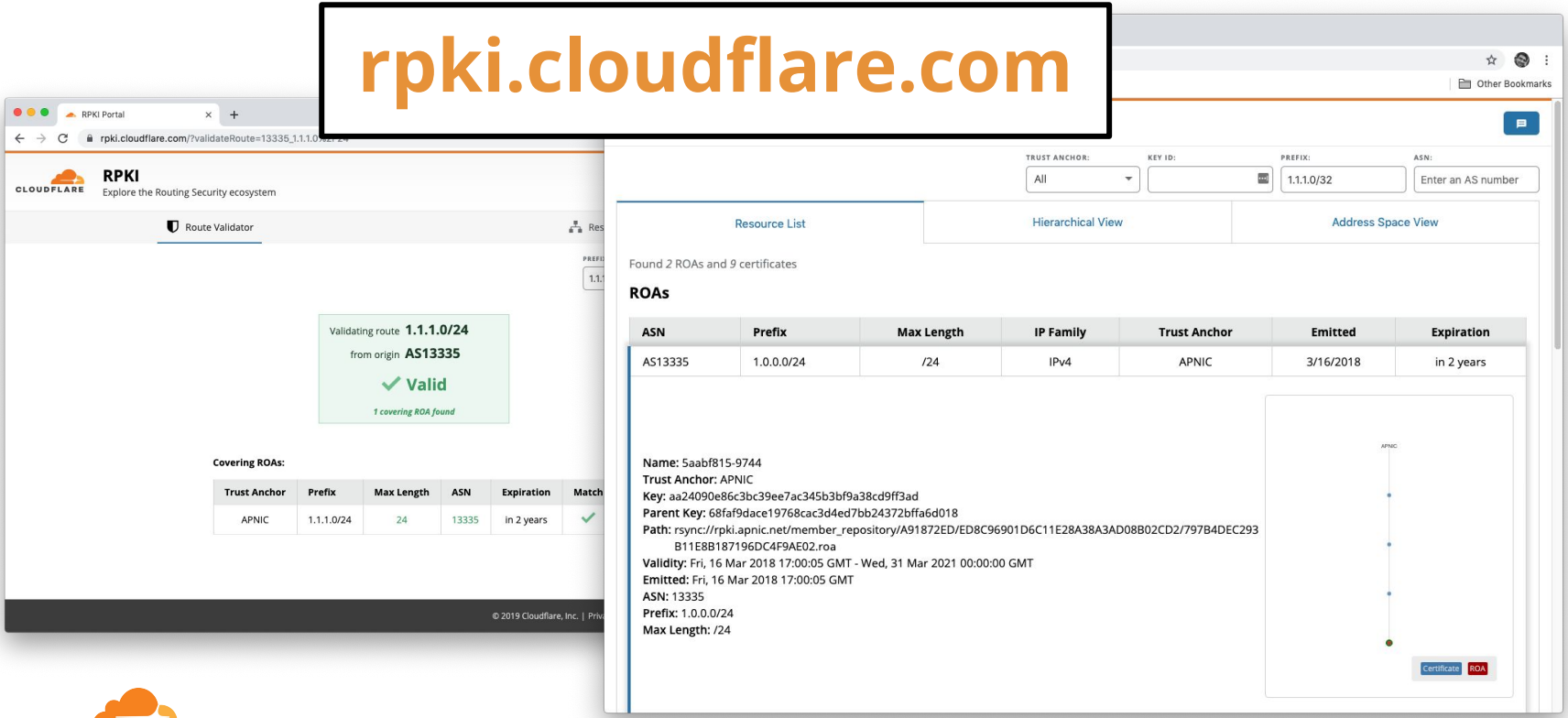
Plaintext: `rtr.rpki.cloudflare.com:8282`

Just configure your router

CLOUDFLARE

Cloudflare's RPKI Portal

rpki.cloudflare.com



CLOUDFLARE

Recent Leaks And Conclusions

Summary of Amazon Route Hijack

An attacker announces Amazon Authority DNS prefixes.

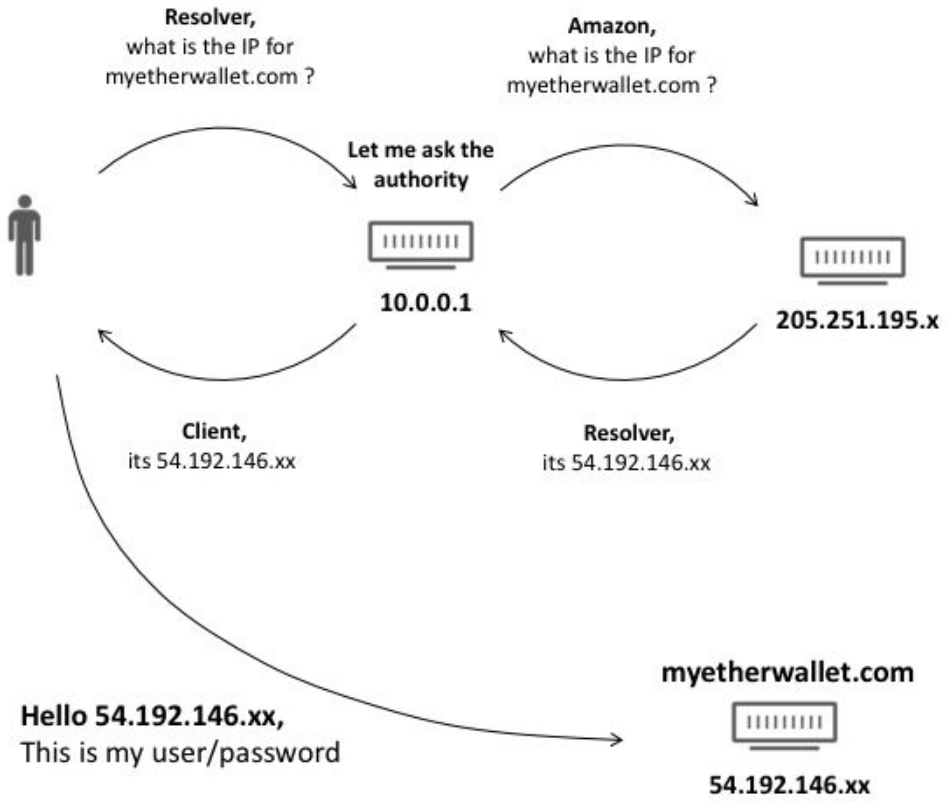
Cloudflare and Google accept them in specific locations.

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

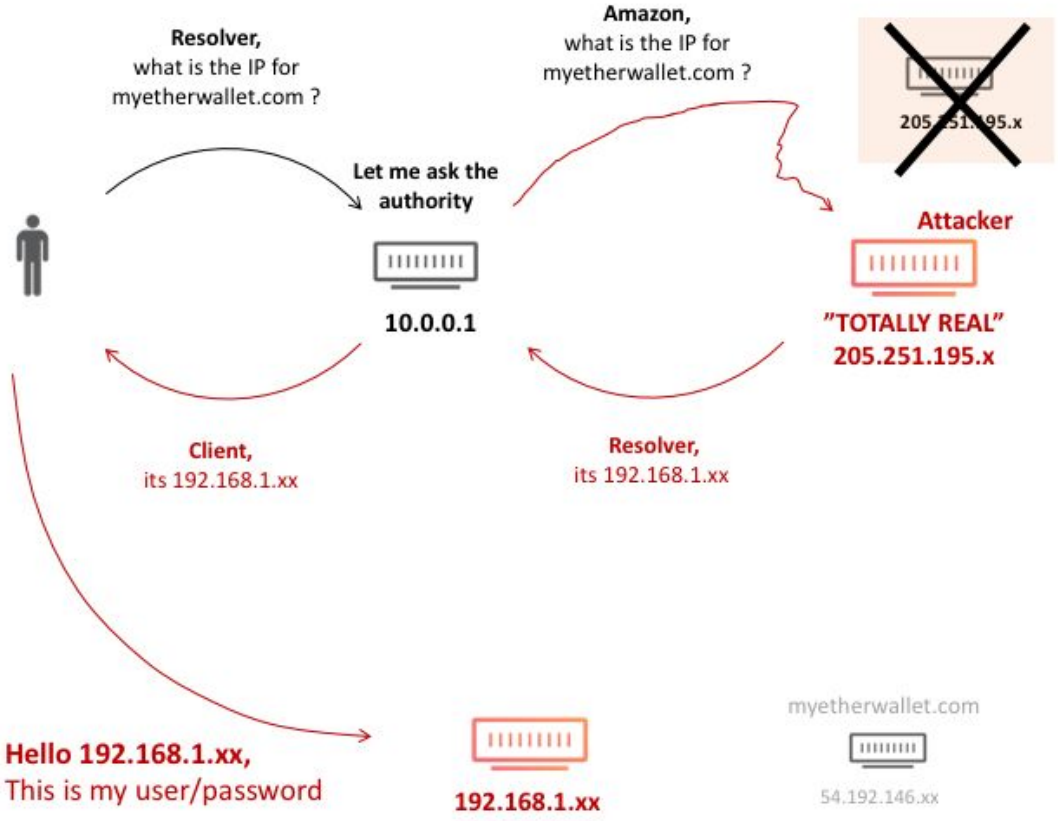
The server has a phishing website for the client.

Attacker gather credentials and steals Bitcoins.

CLOUDFLARE


Resolver,
what is the IP for
myetherwallet.com ?
Amazon,
what is the IP for
myetherwallet.com ?
Let me ask the
authority
10.0.0.1
205.251.195.x
Client,
its 54.192.146.xx
Resolver,
its 54.192.146.xx
Hello 54.192.146.xx,
This is my user/password
myetherwallet.com
54.192.146.xx

CLOUDFLARE


Resolver,
what is the IP for
myetherwallet.com ?
Amazon,
what is the IP for
myetherwallet.com ?
205.251.195.x
Let me ask the
authority
Attacker
10.0.0.1
"TOTALLY REAL"
205.251.195.x
Client,
its 192.168.1.xx
Resolver,
its 192.168.1.xx
Hello 192.168.1.xx,
This is my user/password
192.168.1.xx
myetherwallet.com
54.192.146.xx

CLOUDFLARE

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.

CLOUDFLARE

Summary of Verizon Route Leak

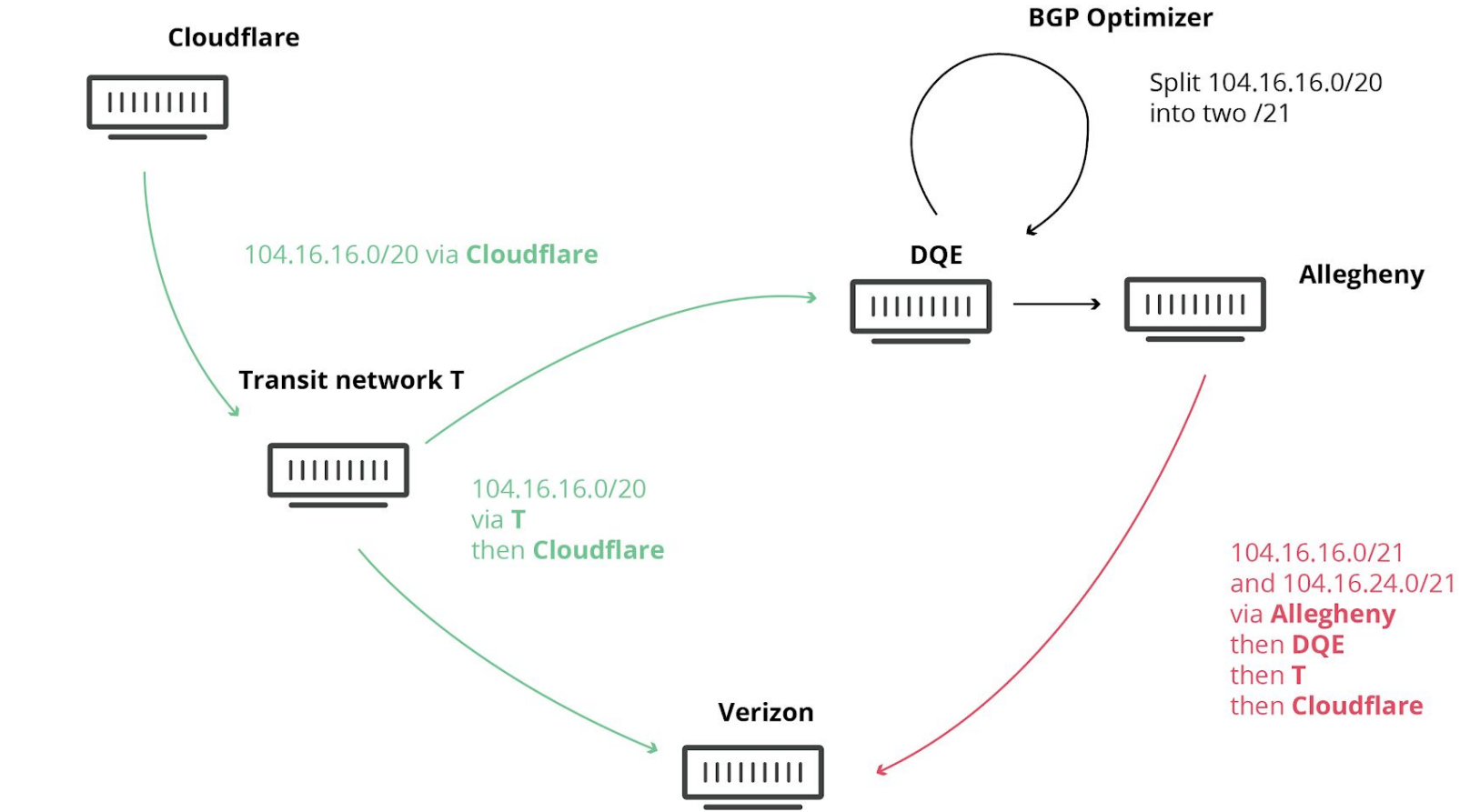
A company has two Internet accesses: Verizon and another ISP.

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.


Cloudflare
BGP Optimizer
Split 104.16.16.0/20
into two /21
104.16.16.0/20 via Cloudflare
DQE
Allegheny
Transit network T
104.16.16.0/20
via T
then Cloudflare
104.16.16.0/21
and 104.16.24.0/21
via Allegheny
then DQE
then T
then Cloudflare
Verizon

CLOUDFLARE

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…

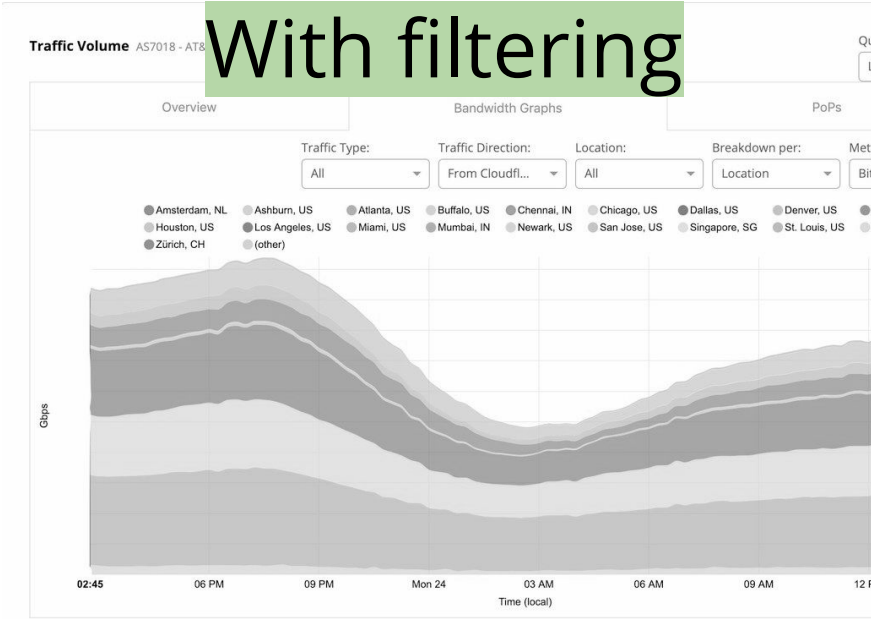
Filtering solves Amazon being hijacked

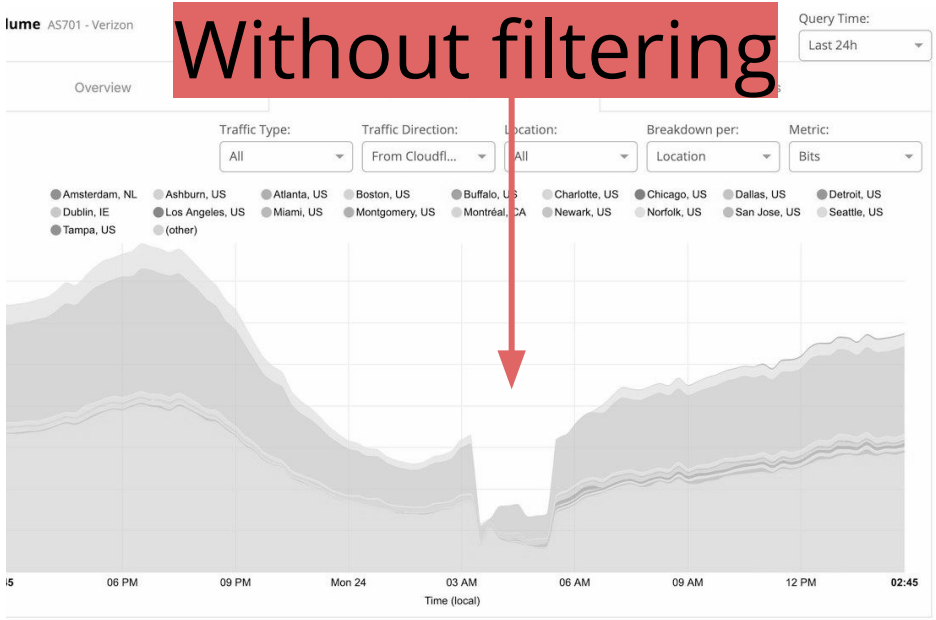
Signing helps your network not being leaked

CLOUDFLARE

Deploy RPKI now

Because tomorrow is already too late



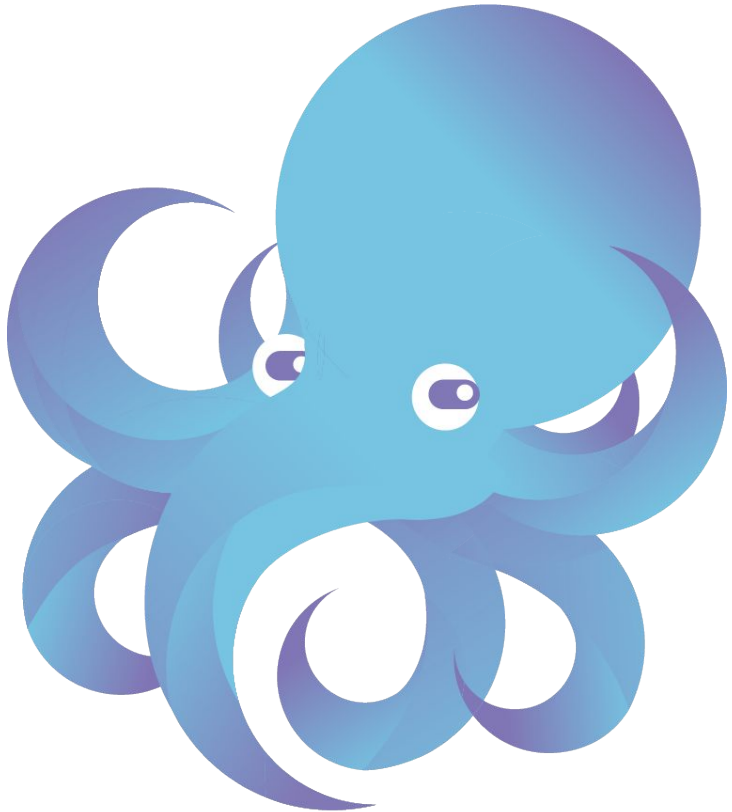


CLOUDFLARE

Thank you

Questions?

louis@cloudflare.com
@lpoinsig (twitter)



CLOUDFLARE