How we leaked a prefix

TL;DR: AS-SETs are dangerous

OPENFACTORY

Better - Connected - Faster

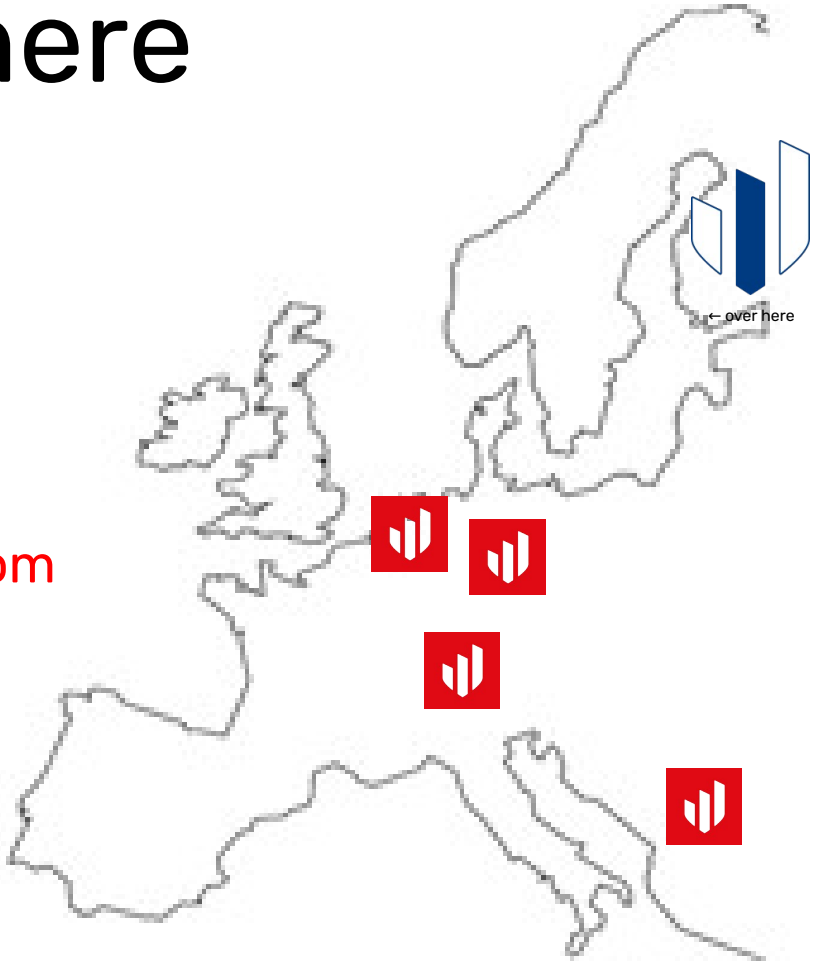
Who

- Funded in 2009, Openfactory GmbH (CH)
- Expanded in 2010, Openfactory Services UG
- Serbian developing since 2011 – with the openfactory novi sad d.o.o.
- Finnish team since 2020 (Pandemic) and registred 2021 as openfactory nordic oy
- 7 Permanent, 11 Freelancers (Project-by-Project up to 16)
- Speaking English, Azerbaijan, Dutch, German, Swiss German, French, Afrikaans, Turkish, Serbian and Kroatian, Xhosa, ja opiskelen suomi

Where

- Europe wide (and a little further)
- Physical team locations:

  - Switzerland
  - Germany
  - Netherlands
  - Belgium
  - United Kingdom
  - Finland
  - Serbia



Backstory

- 2014: LIR
- First: some own servers
- Then colo
- DSL Customers
- Transit customers
- sponsorships

Sponsorships

- Why? Educate people
- How many? Too many
- ASN (we only have like 5-10 16bit, almost everyone got 32bit)
- Exploded when HE stopped giving out bgp tunnels

AS-SET

AS-SET: AS58299:AS-ALL

Includes paying customers

Includes free customers

Things to prevent stuff to go wrong

- Not accepting AS-SETs from free customers
- Legacy still remained
- Prefix limits
- Export limits are very high
- Filter by community only

The incident

- Customer complains about packetloss/bad voice calls
- Cpu load high on vyos router.
- Looks like the sflow daemon ran wild. Consumes lot of cpu.
- After killing it, customer reports stuff is okay again
- Then we get a ticket from salesforce.com

— SFDC CC Cloudflare 35688352 || Open Factory AS 58299 subnet leak out of DE-CIX Munich

So what went wrong?

- Salesforce says, we announce them a route to cloudflare
- We don’t have a session with them
- We are not upstream of salesforce or cloudflare
- Should not the routeserver then filter this?
- So we raise a ticket

Investigation / Fuckup 1

- Running a query on the AS-SET says: cloudflare is in there
- Irrexplorer to investigate
- Find it >4 levels down.
  - Us
    - Downstream (paid customer)
      - Their Customer (A competing tunnelbroker, funny enough)
        - One of their customers put all peerings into the AS-SET

Investigation

- Okay, fair enough. But we have an export filter. Routemap is:
  - Static Filterlist of our own RIPE Blocks with maxlenght
  - Customer-Community for customer routes only
  - We wouldn’t tag cloudflare this way
  - We only install new generated customer filters by hand*. No update was done that day.

    * guess why….

Investigation

- Further fuckup:
  - VYOS configuration handling of the 1.2.X Branch is limited
  - Our commits took 20-30 minutes already
  - Sometimes config on disk and in memory goes out of sync
  - Has to be fixed manually
  - Apparently the route map wasn’t copied fully once

Fuckup 2

- Routemaps on FRR
  - Apprently no default reject/deny
  - We lost the deny statement
  - Nobody noticed since well, it worked, and the repair was done by a junior overnight (I don’t blame him, everyone does mistakes like this)

Investigation / Fuckup 3?

- Never via RS?
- HE peers on RS
- We announced: Salesforce => OF => HE => Cloudflare
- Plausiblity at RS?
- Max Prefix limit should have resulted in sh(i)ut? (we leaked full table)

How to prevent?

- On our end? “Do not fuck up” is not a prevention
- Plausbility
- Fix Concept of AS-SETs and involve plausiblity
- Combine AS-SET with RPSL and plausiblity? Historical data?
- Planned master thesis for coworker to bring up proposals

Q&A

- +358 2 480 933 93
- contact@fi.openfactory.net

OPENFACTORY