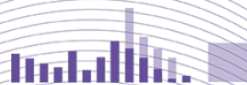


CSNOG 2023
2023-05-16

QRATOR
LABS

Roleplay v BGP

Alexander Zubkov
green@qrator.net



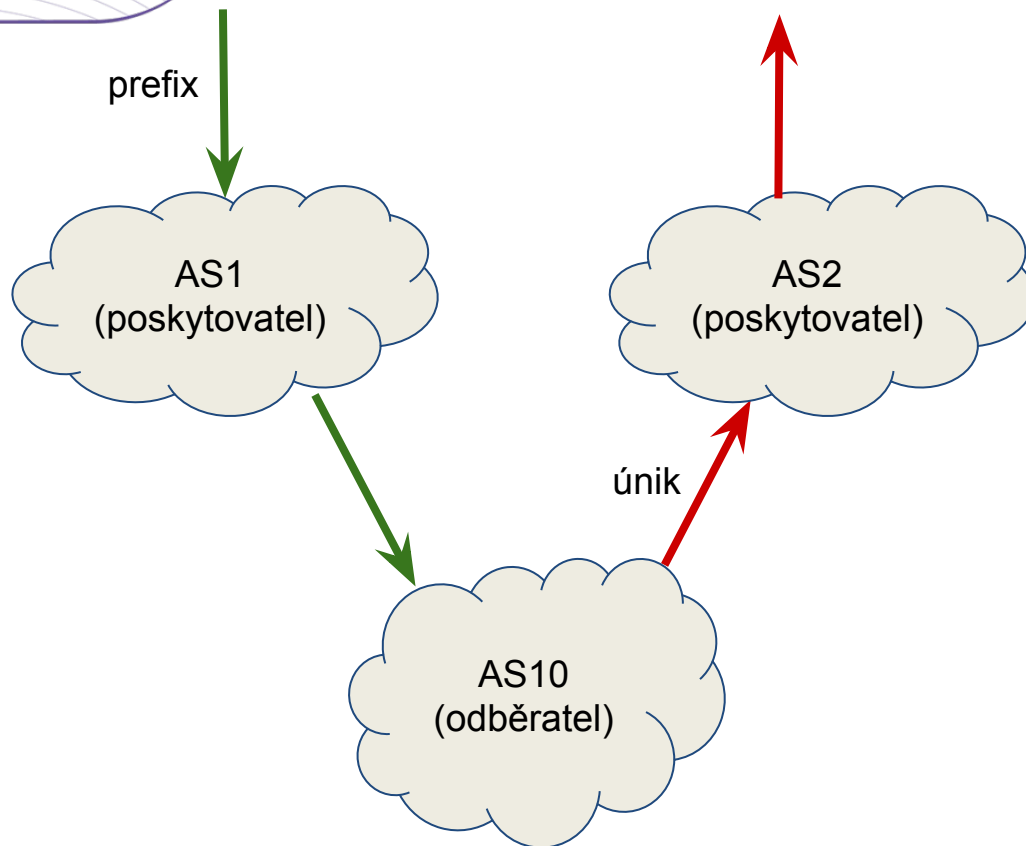
- **únik (leak)**

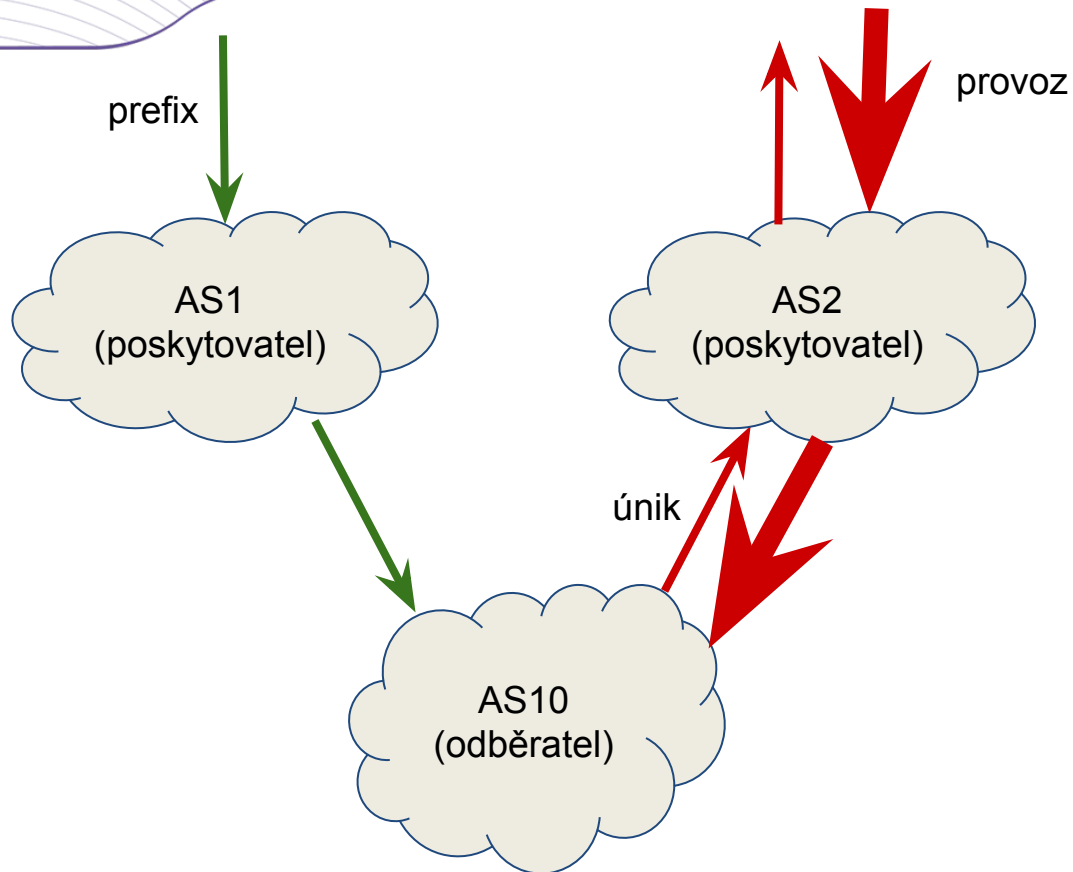
- cesta směřuje k oprávněnému cíli
- šíření skutečných záznamů o sítích mimo určených cest

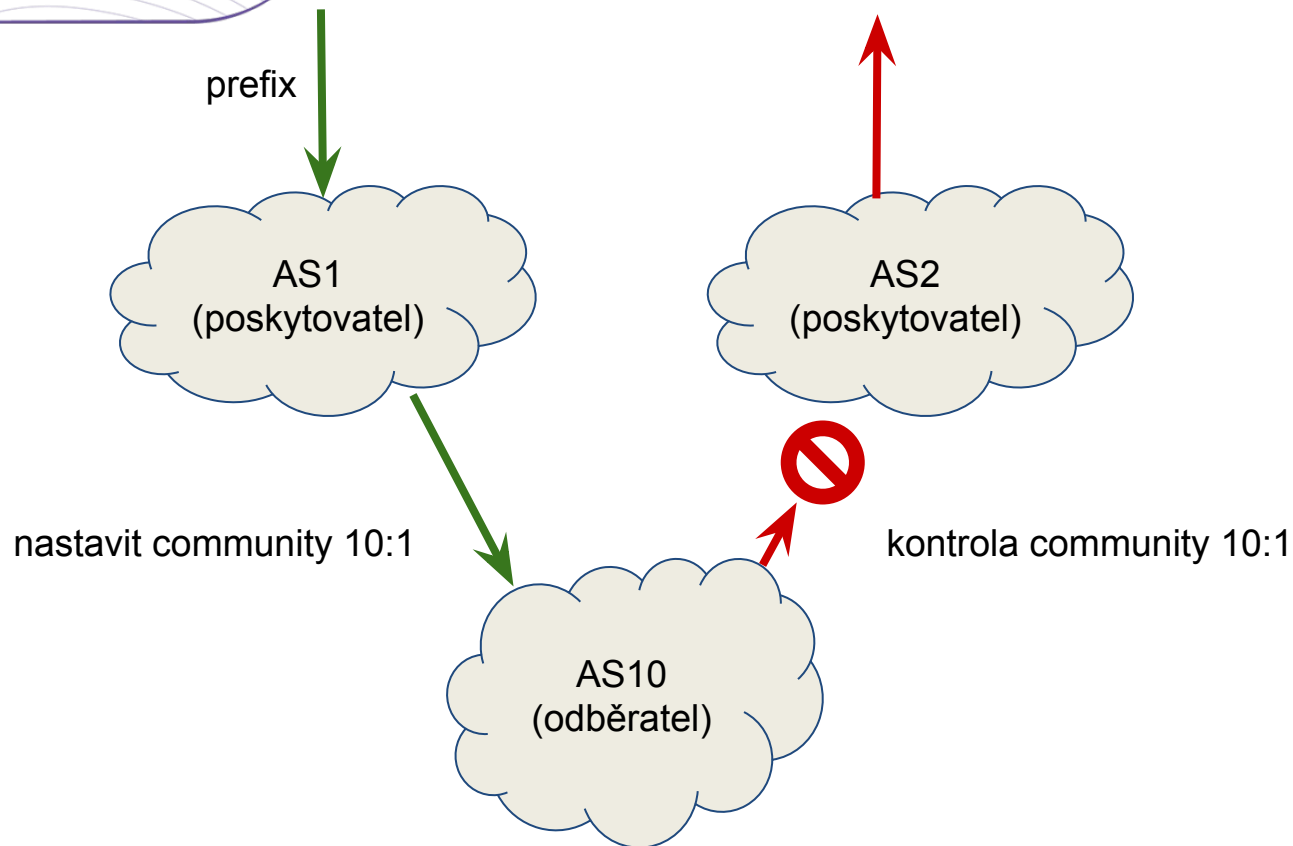
- **únos (hijack)**

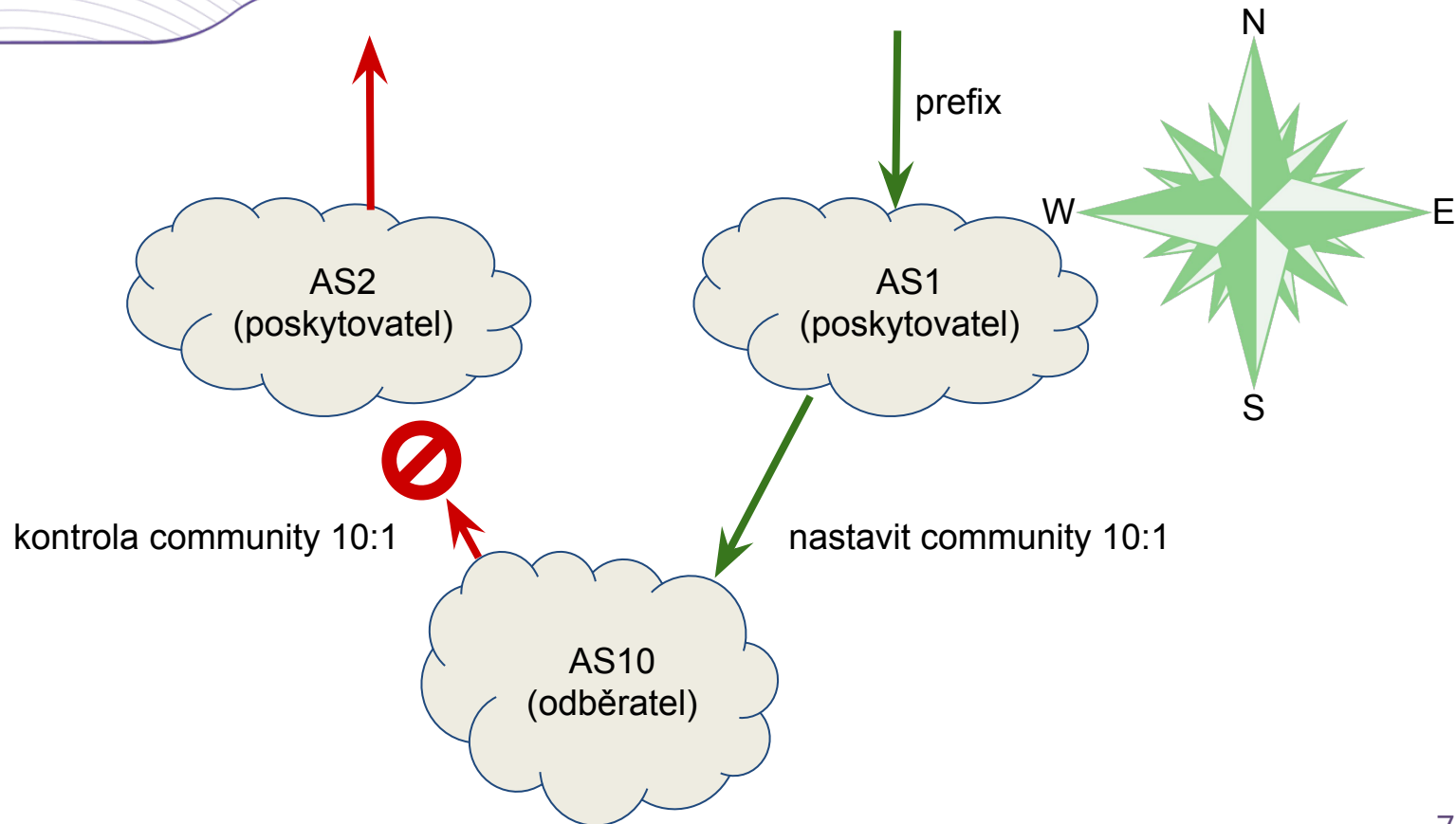
- cesta směřuje někam jinam
- vytvoření protiprávní informace

- ustálený model vztahu mezi sítěmi
 - “Stable Internet Routing Without Global Coordination” [[Gao-Rexford](#)]
 - hierarchické vztahy
 - customer - provider (odběratel - poskytovatel)
 - peer-peer (soused - soused)
 - Route Server - RS-client

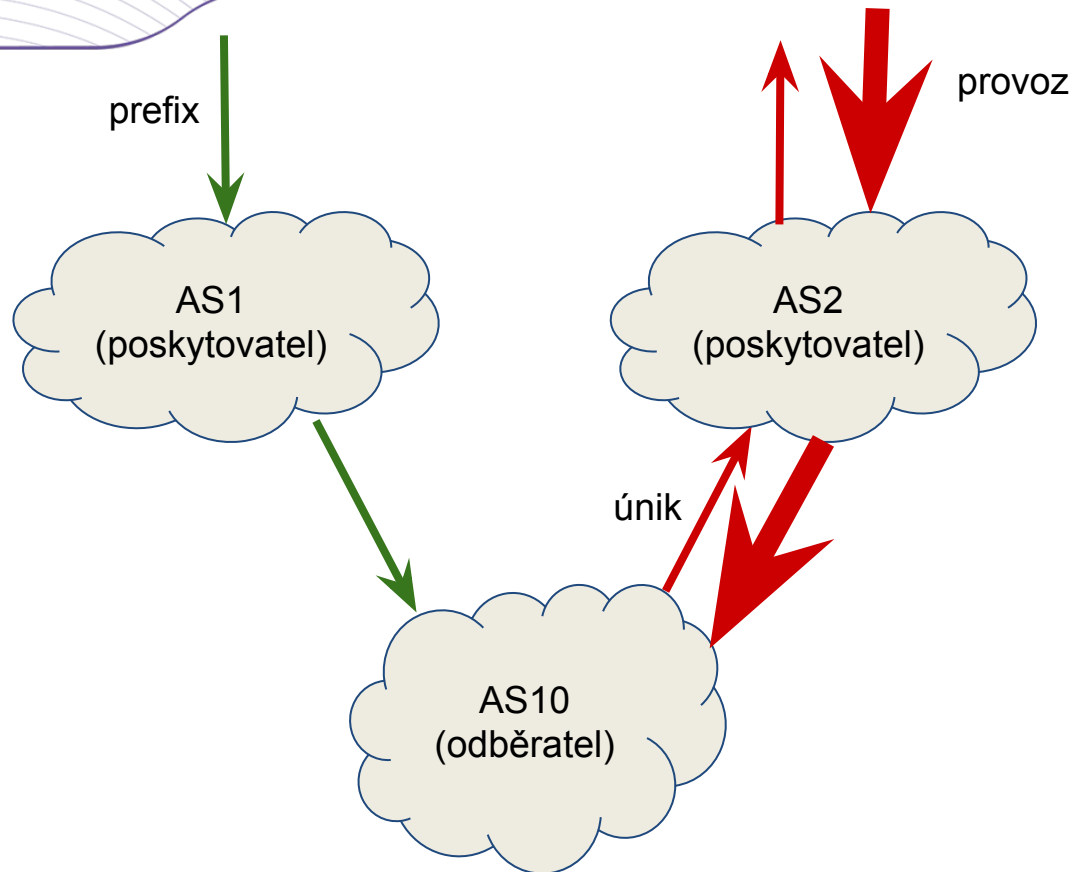








- může to být nenápadné
 - filtrace bez označení
 - například jen pomocí seznamu prefixů
- vlastní metoda a community
- musí být součástí vašeho filtru
- nesmíte udělat žádnou chybu



- <https://datatracker.ietf.org/doc/rfc9234/>
 - “Route Leak Prevention and Detection Using Roles in UPDATE and OPEN Messages”
 - “Prevence a detekce úniků pomocí rolí v zprávách UPDATE a OPEN”
 - březen 2016 — 1. pracovní verze
 - květen 2022 — RFC 9234
 - cca. 6 let

- jen “běžný” BGP

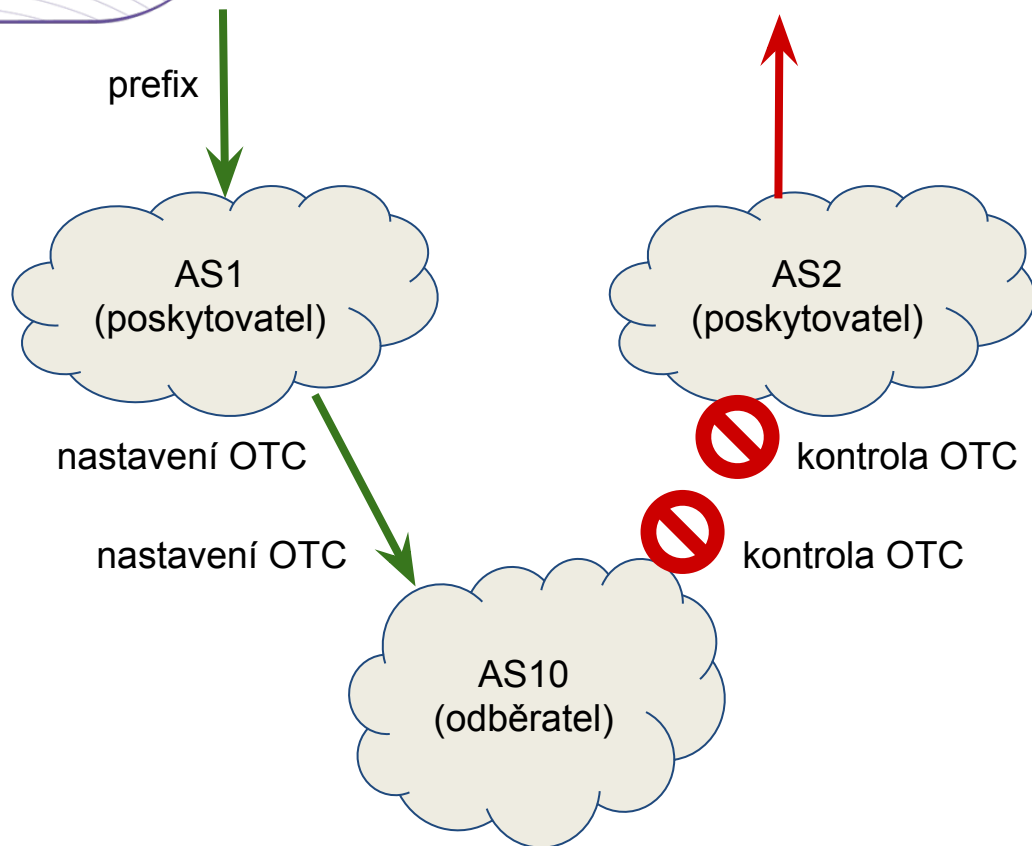
- ~~multicast, vpn~~
- ~~confederation~~

- role

- při zřizování BGP relaci (OPEN zpráva)
- vzájemná kontrola
- přísný (strict) režim

● OTC atribut

- “only to customer” — jen k odběrateli
 - poskytovatel, peer, route server
- informace o cestě (UPDATE zpráva)
- přechodný (transitive) atribut
- funguje automaticky
- dvojitá kontrola (import, export)
- dvojitě nastavení



OpenBGPD	7.5 (25. července 2022)
FRRouting	8.4 (7. listopadu 2022)
BIRD	2.0.11 (12. listopadu 2022)
freeRtr	28. dubna 2023
VyOS	frr uvnitř, ale šablony jsou ve vývoji
MikroTik	~7 verze, ale jen v konfigurace

tcpdump	vývojová větev od 8. prosince 2022 ale verze 4.99.4 od 7. dubna 2023 zatím nemá podporu
Wireshark	vývojová větev od 1. května 2023 asi bude ve verzi 4.1

- další nástroje
 - Vývojáři, komunita tě potřebuje!
- síťová zařízení
 - výrobci chtějí více požadavků

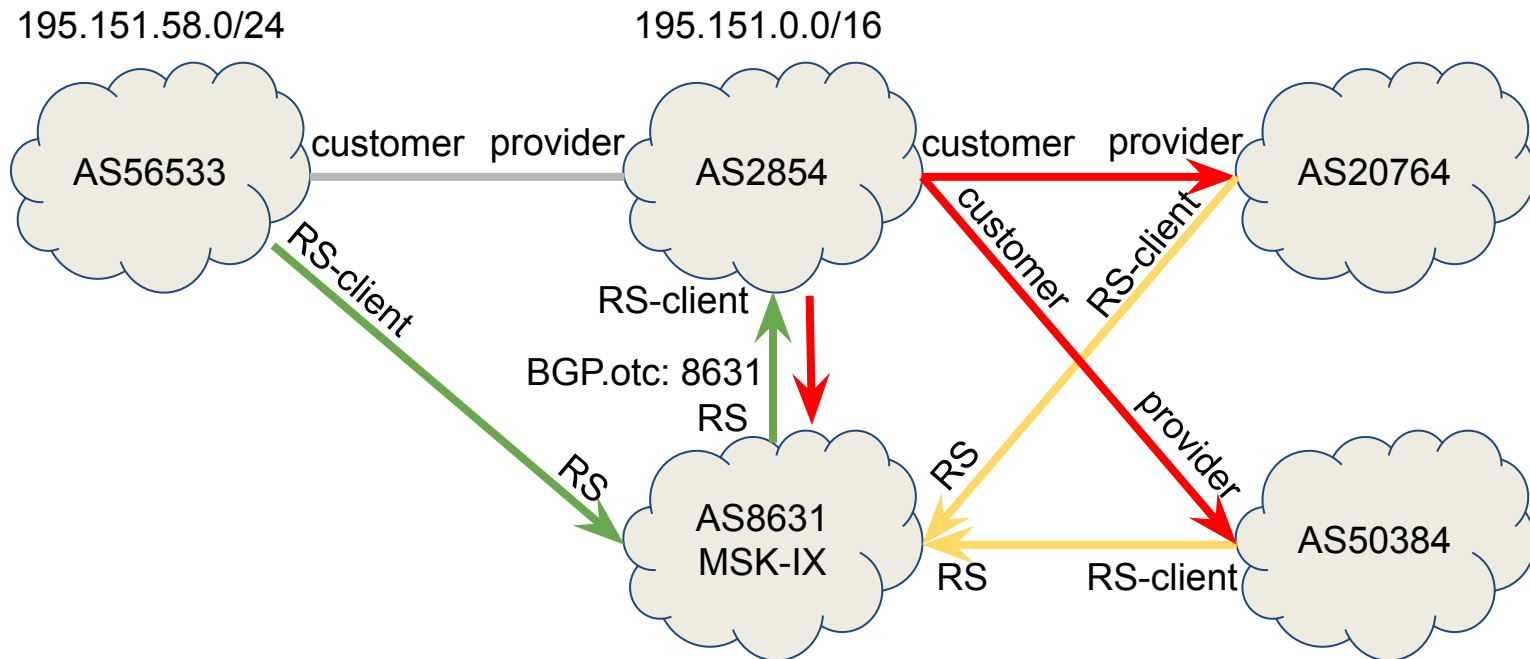


● RIS MRT dump

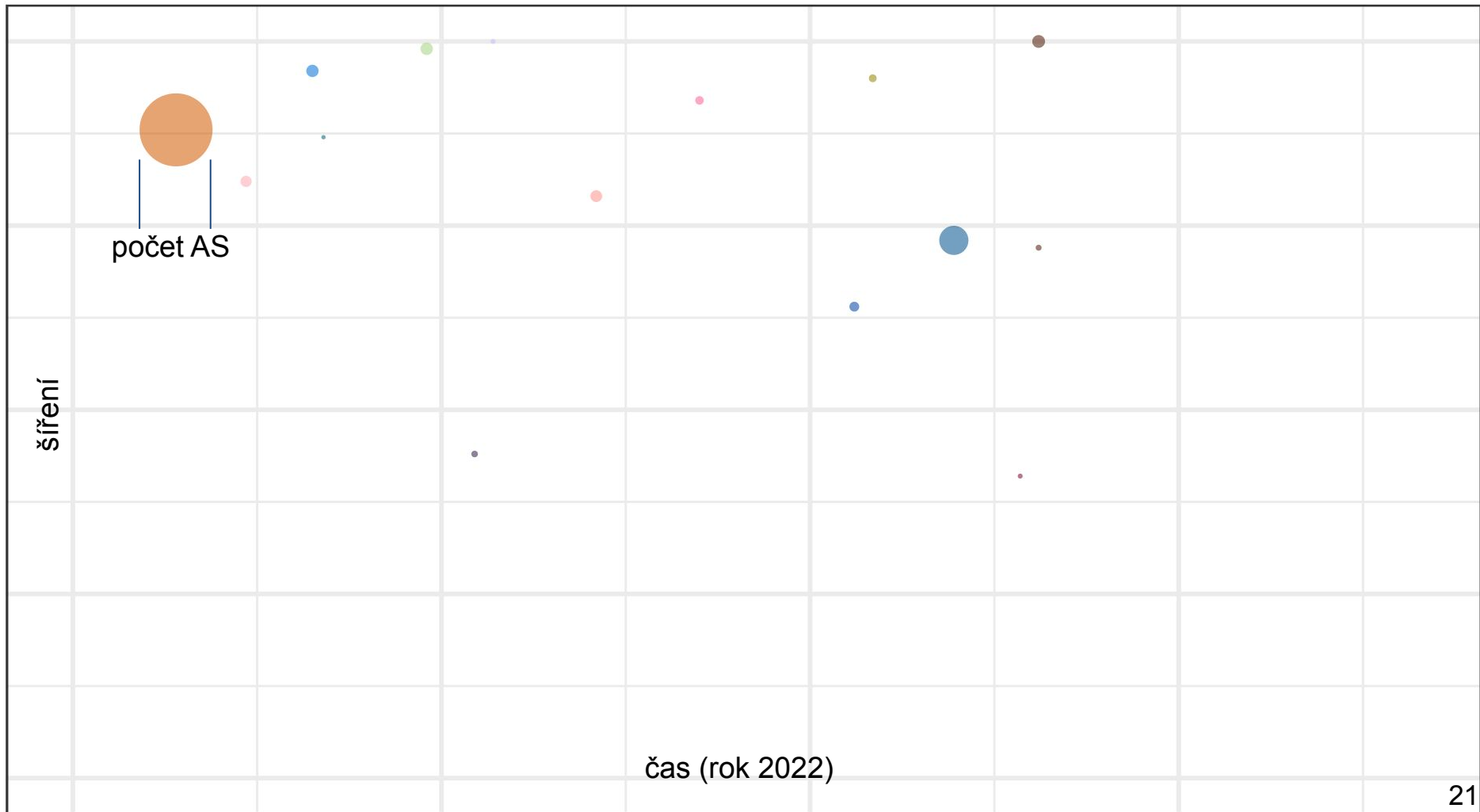
- 1 097 657 / 53 147 435 ~ 2%
- AS204092 GRIFON (FR): 1 092 519
- AS8631 MSK-IX: 4 802
 - a další: EKT, NSK, VLV, RND, SMR, SPB
- zbývá 336
- možná AS6939 Hurricane Electric

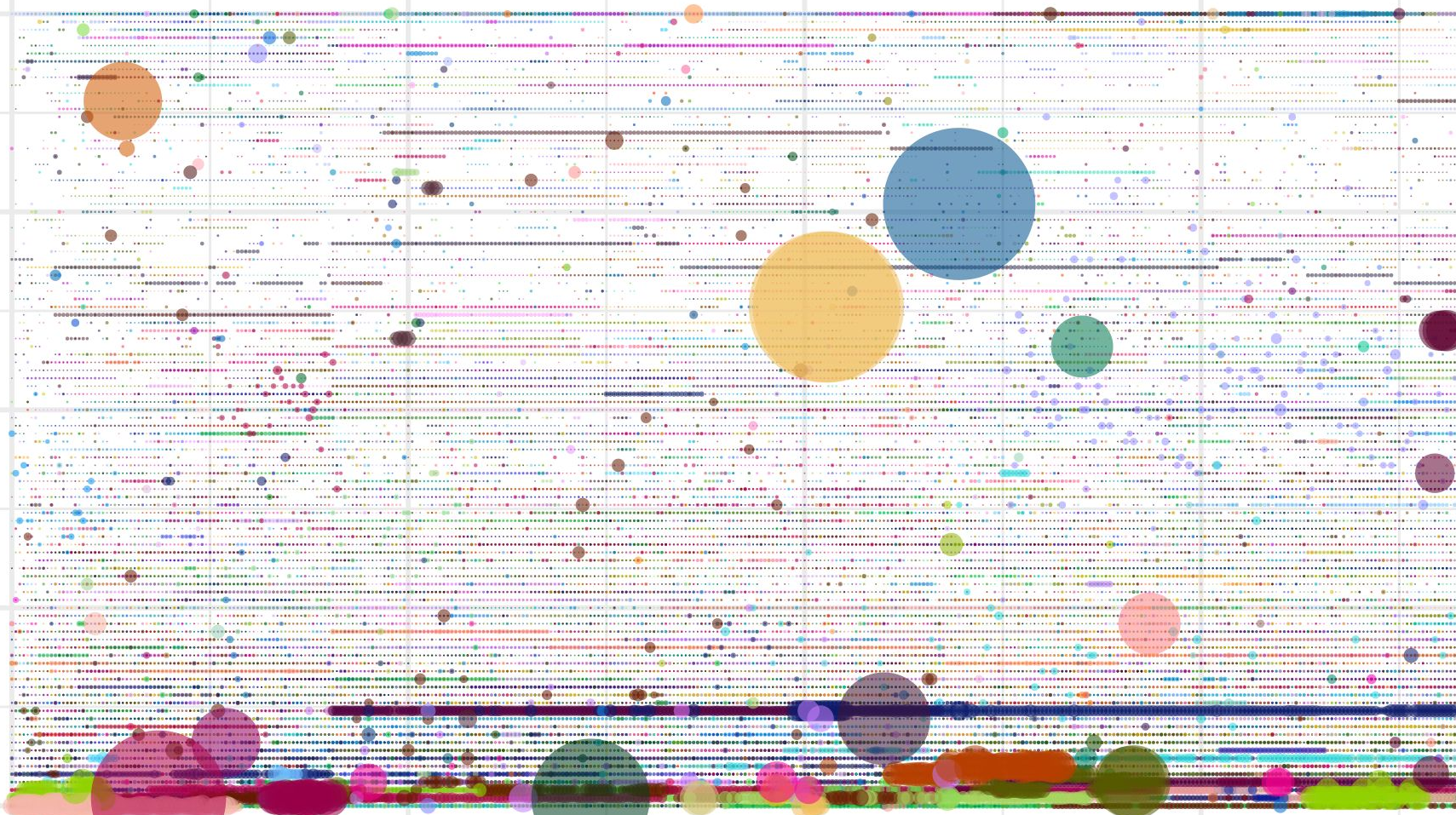
● full view

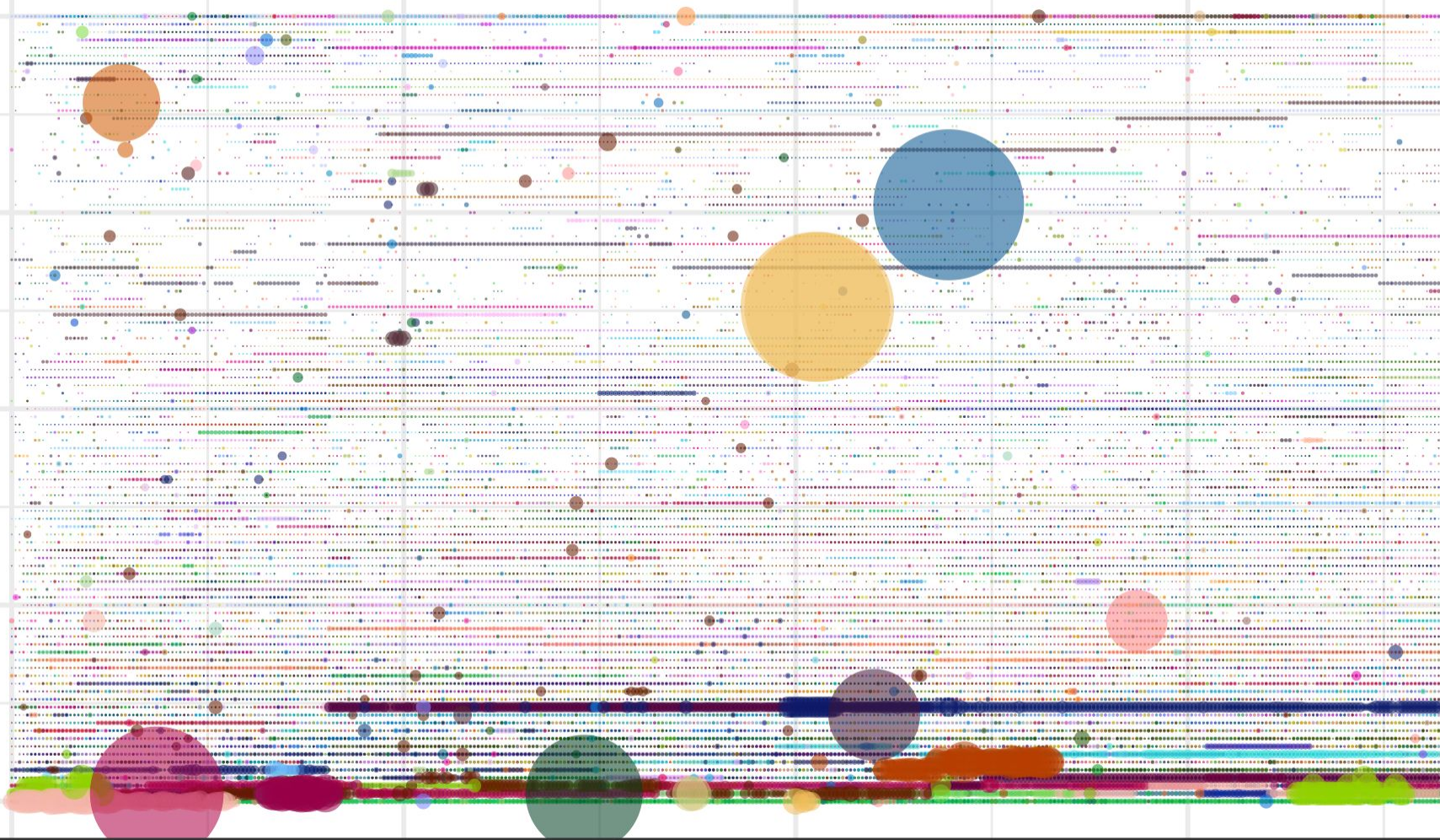
- AS200950 Tom Funken (DE)
- AS207024 Cloudcell (TR)
- AS8631 MSK-IX
 - 195.151.58.0/24
 - BGP.as_path: 5511 2854 8631 29470 56533
 - BGP.otc: 8631
 - 195.151.0.0/16
 - origin: AS2854

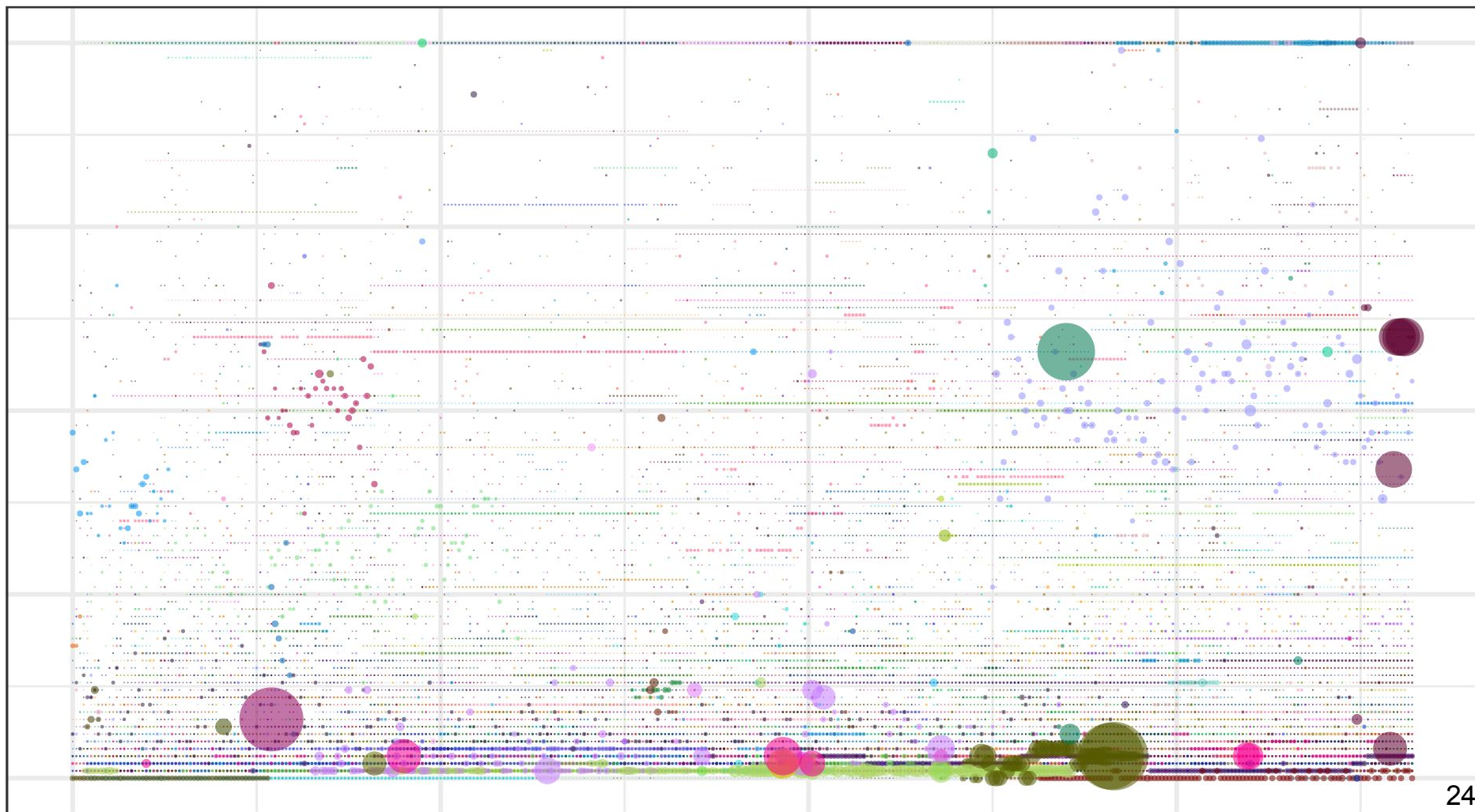


- Alexander Zubkov
 - Qrator Labs
 - green@qrator.net
- Qrator.Radar
 - <https://radar.qrator.net>
 - https://twitter.com/Qrator_radar
 - radar@qrator.net









	Únik (leak)	Únos (hijack)	Potřebuje RPKI	Všichni musí	Dostupné
Role	neúmyslný	ne	ne	ne	slabá podpora
ROA	ne	neúmyslný	ano	ne	ano
ASPA	ano	ano	ano	ne	pracovní
BGPsec	ne	ne	ano	ano	ve vývoji