(APNIC ISIF Project)

Developing a Collaborative BGP Routing Analyzing and Diagnosing Platform

8 June 2023
TNC 23

Outline

- Project Overview
- Project Progress
- Future Work Plan
- Comments/Suggestions

Project Information

- Name: Developing a Collaborative BGP Routing Analyzing and Diagnosing Platform

- Co-PI: Jilong Wang, (Tsinghua University, CERNET, China)
  Co-PI: Chalermpol Charnsripinyo (ThaiREN, Thailand)
  Co-PI: Simon Peter Green (SingAREN, Singapore)

- Date: 2022.2.24 - 2023.8.24 (tbc with APNIC Foundation)
- APNIC ISIF Grants : US$150,000.00
- Tsinghua University In-Kind Contribution: US$69,660.00

清華大學 Tsinghua University

APNIC FOUNDATION

Objectives & Deliverables

- Build a collaborative BGP routing analyzing and diagnosing platform
  - Looking Glass platform
  - BGP routing sharing platform
  - BGP monitoring and diagnosing platform, focusing on routing hijacking detection and mitigation system
  - BGP analysis platform, focusing on invulnerability analysis of regional routing
- Set up a website for sharing knowledge
- Enhance the NREN capacity of network operation and measurement in Asia Pacific area and promote international collaborations

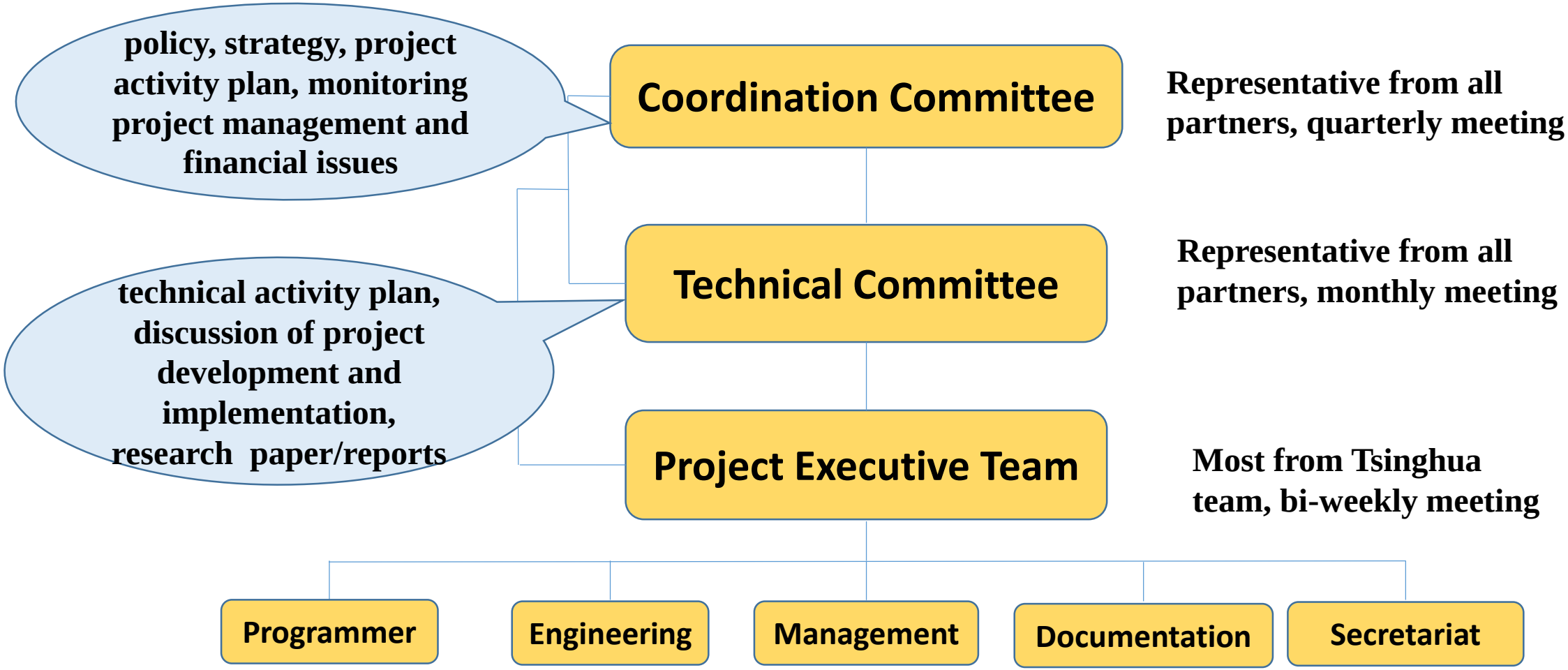
Partnership

- **19 Partner Organizations (listed alphabetically)**
  - AARNET(AU)
  - APAN-JP(JP)
  - BdREN(BD)
  - CERNET(CN)
  - DOST-ASTI(PREGINET)(PH)
  - ERNET(IN)
  - Gottingen University(DE)
  - HARNET(JUCC, HK)
  - ITB(ID)
  - KREONET(KR)
  - LEARN(LK)
  - MYREN(MY)
  - NREN(NP)
  - PERN(PK)
  - REANNZ(NZ)
  - SingAREN(SG)
  - Surrey University(UK)
  - ThaiREN(TH)
  - TransPAC(US, APAN/GNA-G Routing WG)
- **Keep open till June, 2023**

清華大學 Tsinghua University

APNIC FOUNDATION

Project Governance



清華大學 Tsinghua University

APNIC FOUNDATION

Project Progress

- **Project Web Site**
- **Build a collaborative BGP routing analyzing and diagnosing platform**

  -Looking Glass platform:

  Connected with 7 Education & Research network & linked to 3 partner's Looking Glass

  -BGP routing sharing platform

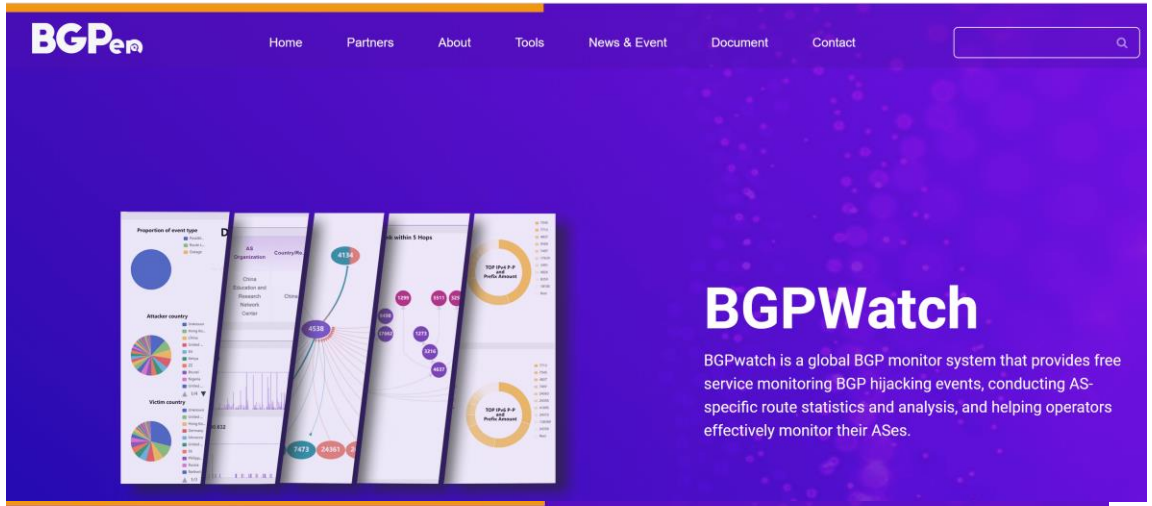
  Established BGP session with 15 partners

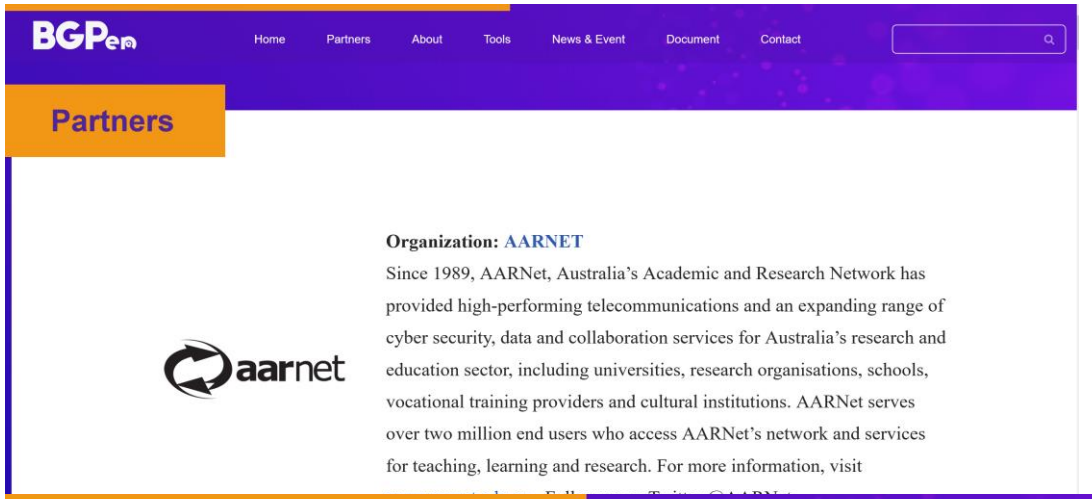
  -BGPWatch: Analyzing and Diagnosing Platform

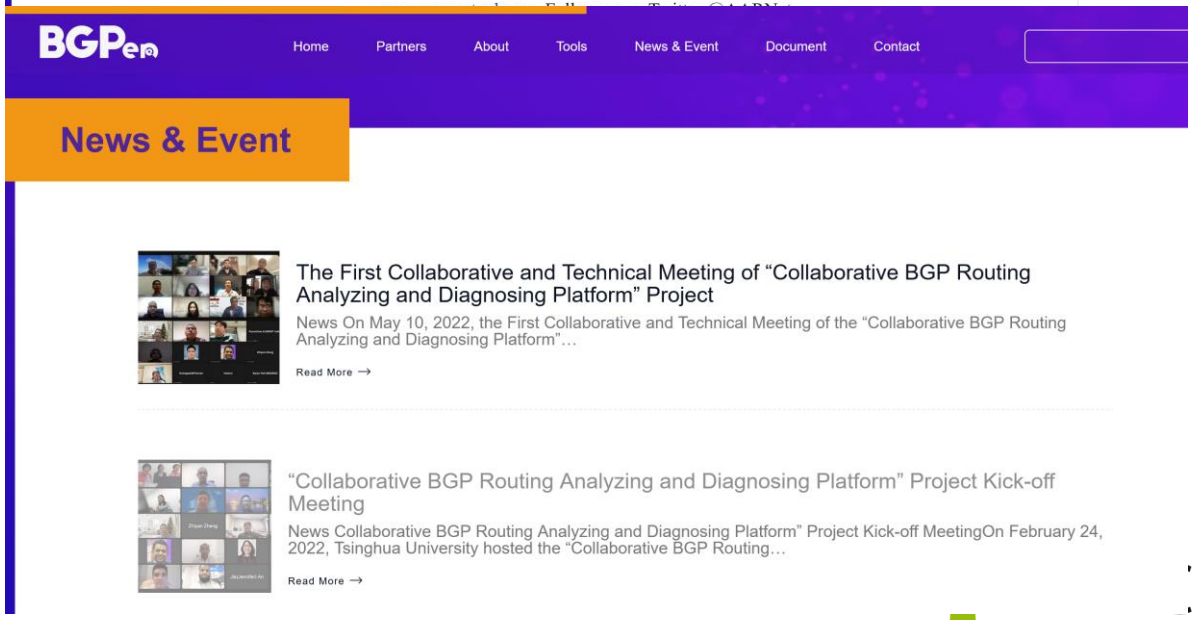
- **Knowledge Sharing & Community Building**

Project Web Site

https://bgper.net



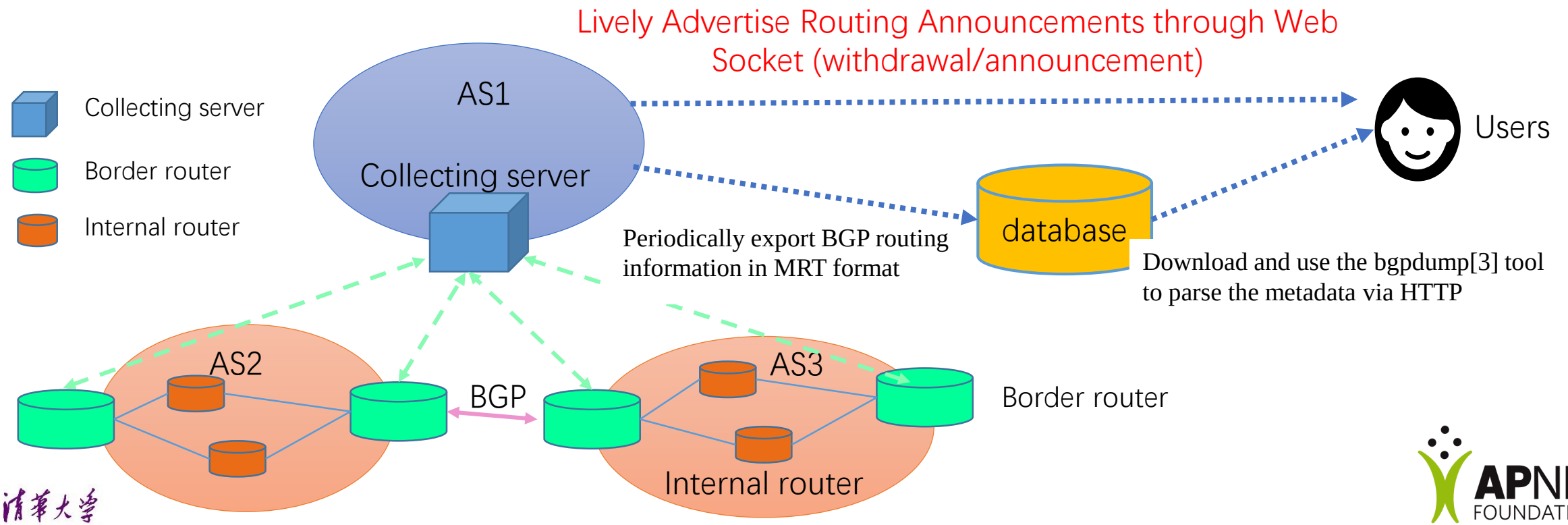




BGP Routing Sharing: CGTF RIS

https://bgp.cgtf.net

- Collecting server： Use routing FRR[2] to simulate a real BGP router
- Border routers: Connect with the collecting server by BGP peering
- Feature: Lively Advertise Routing Announcements



清華大學 Tsinghua University

APNIC FOUNDATION

CGTF RIS

https://bgp.cgtf.net

We have established BGP session with 15 partners.
Configuration manual can be accessed at
https://www.bgper.net/index.php/document/

No.	Partner	No.	Partner
1	APAN-JP	9	MYREN
2	AARNET	10	PERN
3	BDREN	11	REANNZ
4	CERNET	12	SINGAREN
5	HARNET	13	ThaiSARN
6	ITB	14	TransPAC
7	KREONET	15	NREN
8	LEARN		

Index of /ribs/2022/07

Name	Last modified	Size	Description
rib.20220730.0600.mrt.bz2	2022-07-30 06:00	13M	
rib.20220730.0800.mrt.bz2	2022-07-30 08:00	13M	
rib.20220730.1000.mrt.bz2	2022-07-30 10:00	13M	
rib.20220730.1200.mrt.bz2	2022-07-30 12:00	13M	
rib.20220730.1400.mrt.bz2	2022-07-30 14:00	13M	
rib.20220730.1600.mrt.bz2	2022-07-30 16:00	13M	
rib.20220730.1800.mrt.bz2	2022-07-30 18:00	13M	
rib.20220730.2000.mrt.bz2	2022-07-30 20:00	13M	
rib.20220730.2200.mrt.bz2	2022-07-30 22:00	13M	
rib.20220731.0000.mrt.bz2	2022-07-31 00:00	13M	
rib.20220731.0200.mrt.bz2	2022-07-31 02:00	13M	
rib.20220731.0400.mrt.bz2	2022-07-31 04:00	13M	
rib.20220731.0600.mrt.bz2	2022-07-31 06:00	13M	
rib.20220731.0800.mrt.bz2	2022-07-31 08:00	13M	
rib.20220731.1000.mrt.bz2	2022-07-31 10:00	13M	

APNIC FOUNDATION

清華大學 Tsinghua University

CGTF RIS Collector

- Just have your border router **establish an eBGP session** with our collector:
- Our Collector ASN： 65534

- Our Collector1 IPv4 address： 47.241.43.108
- Our Collector1 IPv6 address: 240b:4000:b:db00:8106:7413:738f:e9ed

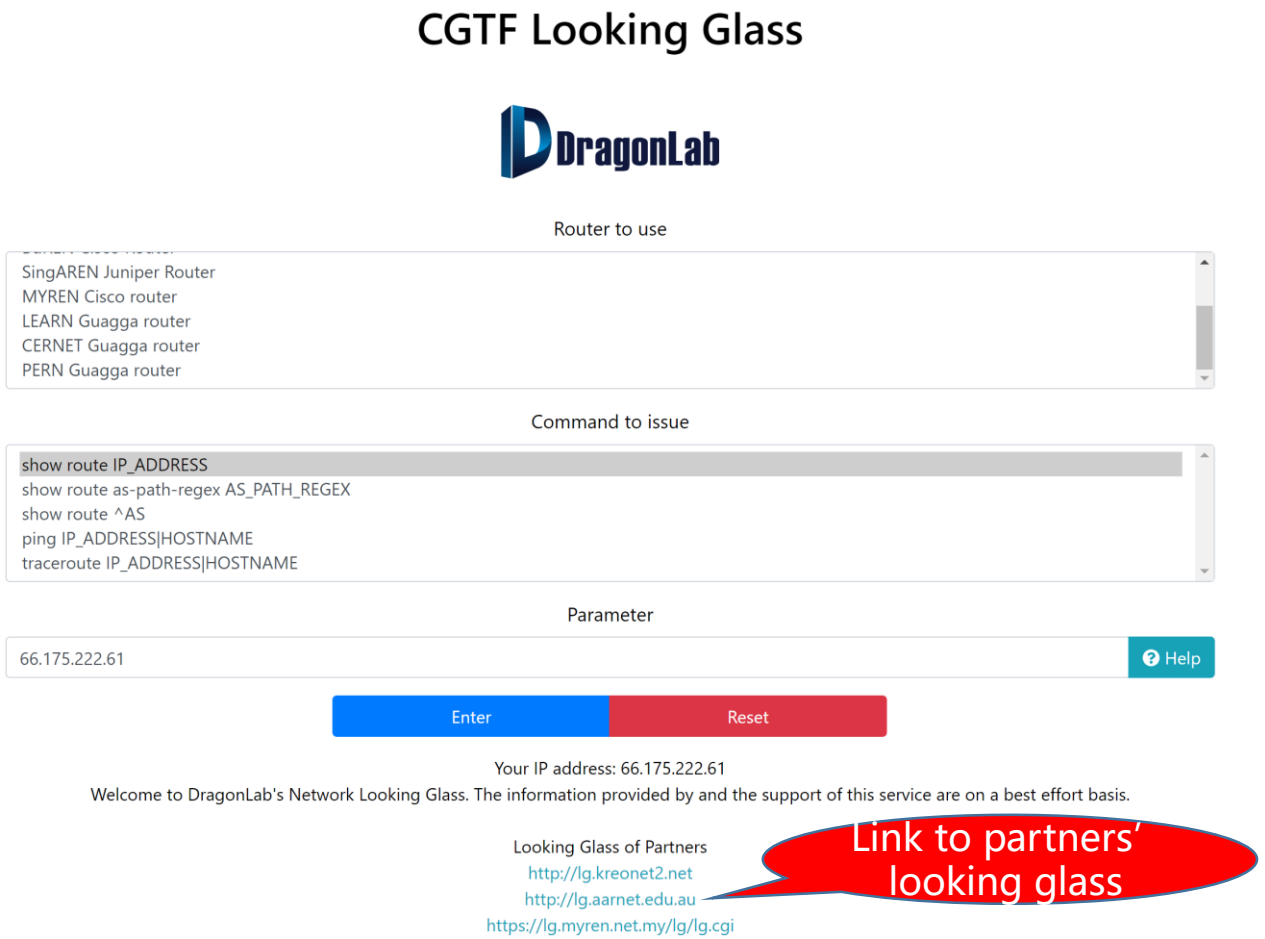
- Our Collector2 IPv4 address： 203.91.121.227
- Our Collector2 IPv6 address： 2001:da8:217:1213::227

APNIC FOUNDATION

Tsinghua University

CGTF Looking Glass

- https://lg.cgtf.net
- Open Source:
  - https://github.com/gmazoyer/looking-glass
- 5 commands
- Query speed limit for security
- More partners is welcomed



7 Education & Research network joined

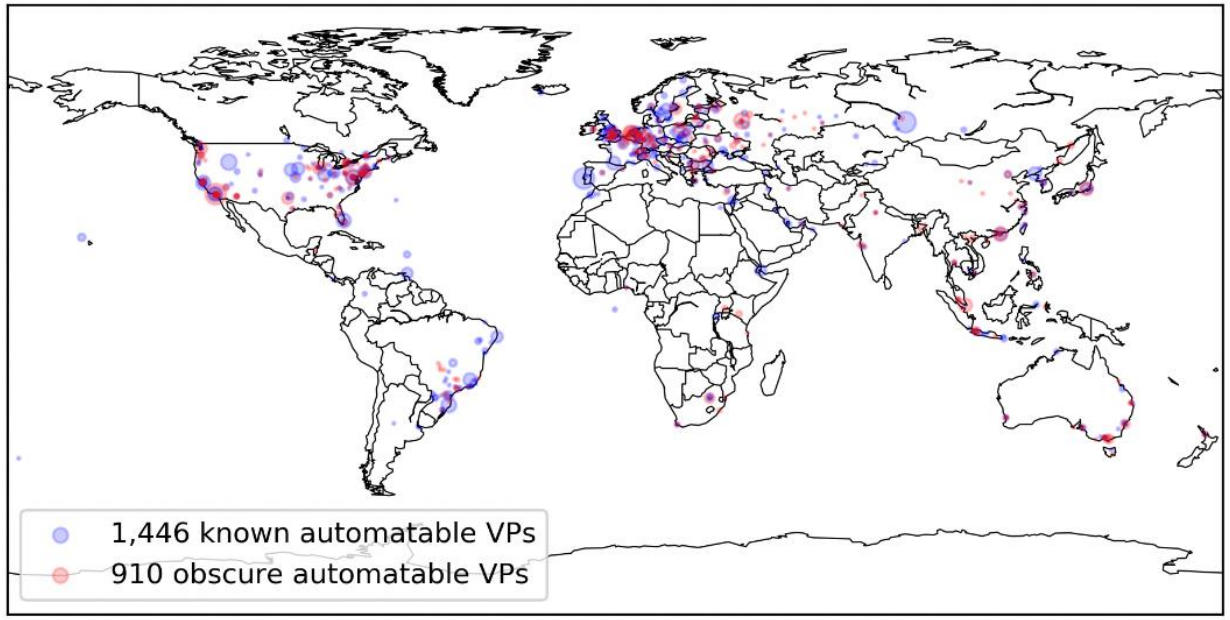
Add links to partners' looking glass

APNIC FOUNDATION

清華大學 Tsinghua University

Open Looking Glass Vantage Point

- **Paper: “Discovering obscure looking glass sites on the web to facilitate internet measurement research”——CoNEXT’21**



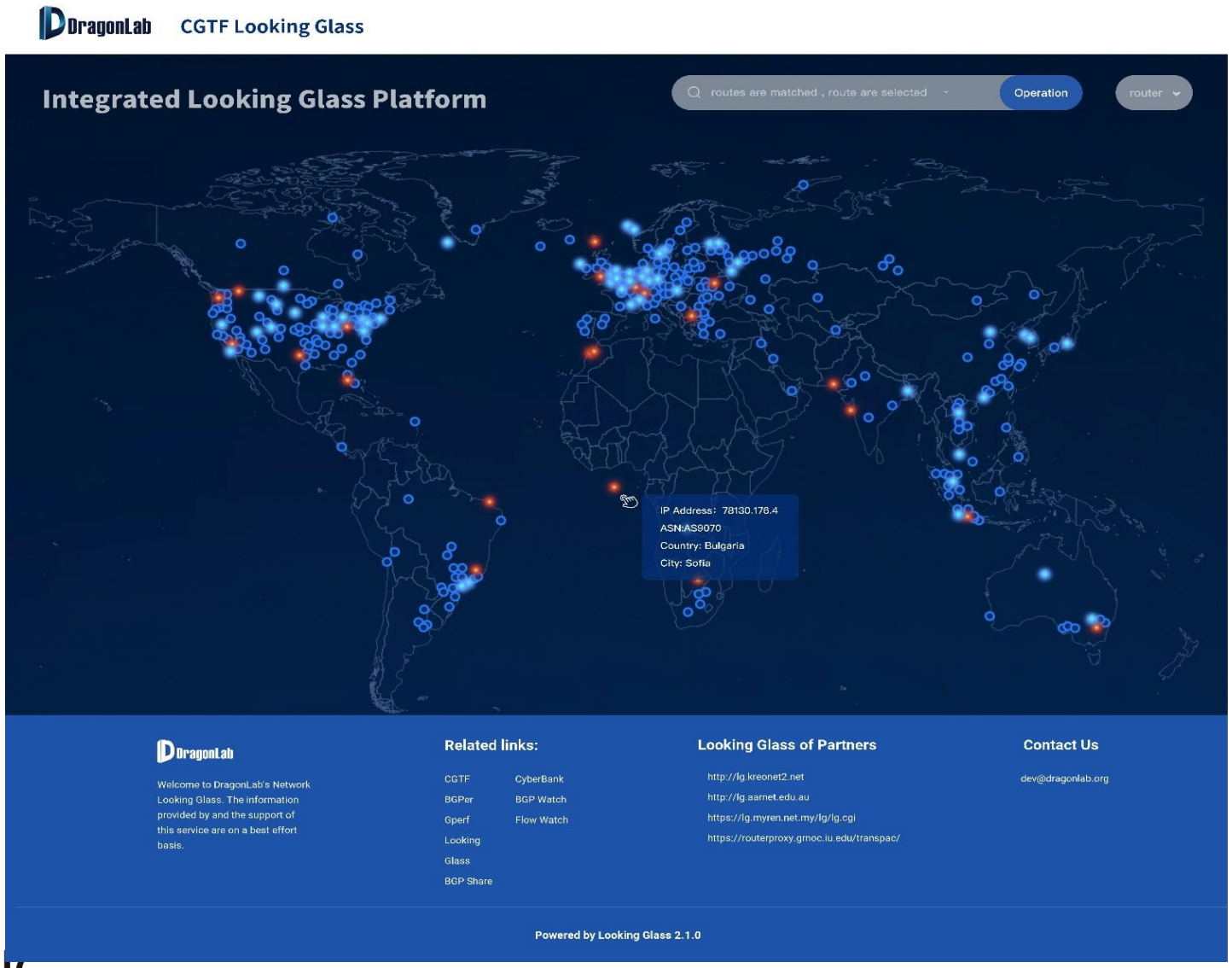
1,446 known LG VPs in 386 cities of 75 countries
910 obscure LG VPs in 282 cities in 55 countries

✓ The 910 obscure VPs cover **8 exclusive countries** and **160 exclusive cities,** where no known LG VPs have been found before

✓ The 8 countries are mainly distributed in **East Africa** and **South Asia**

Periscope has found several hundred VPs (364)

An Integrated Looking Glass and Open API



Based on the found VP
Open API,
Open source,
Open Platform

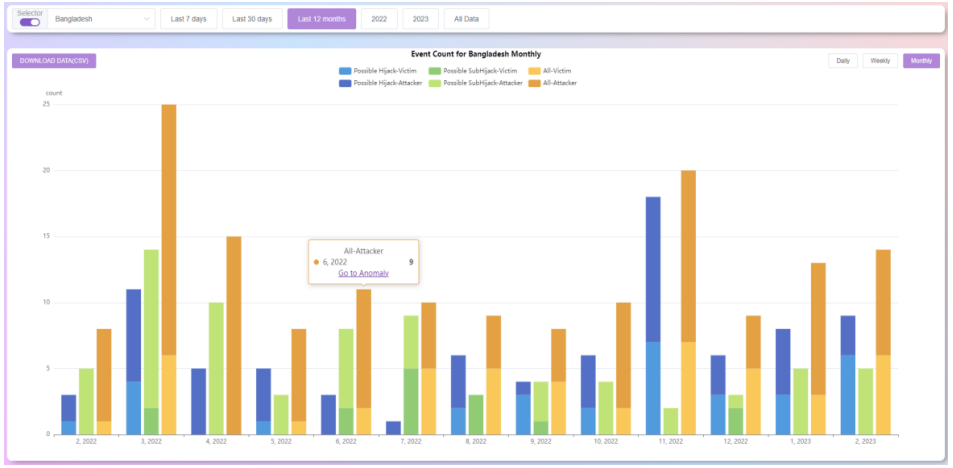
APNIC FOUNDATION

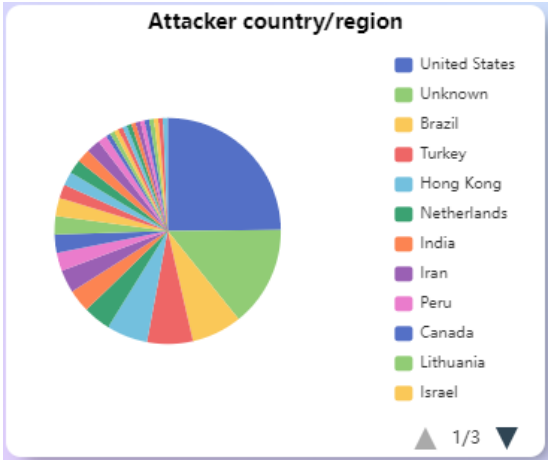
清華大學 Tsinghua University

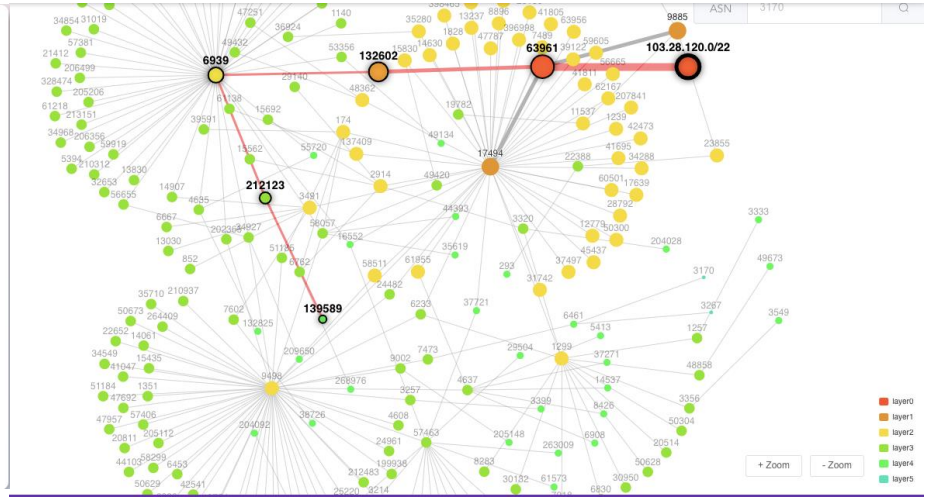
BGP Routing Monitoring and Analysis: BGPWatch

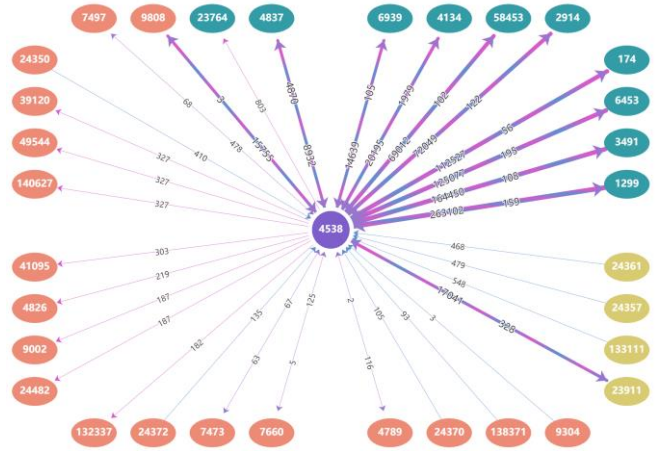
https://bgpwatch.cgtf.net

- Hijacking Detection
- Hijacking Statistics
- Dashboard:AS info
- Routing Search：
  - forward, reverse, bi-direction
- Subscribe, Alarming







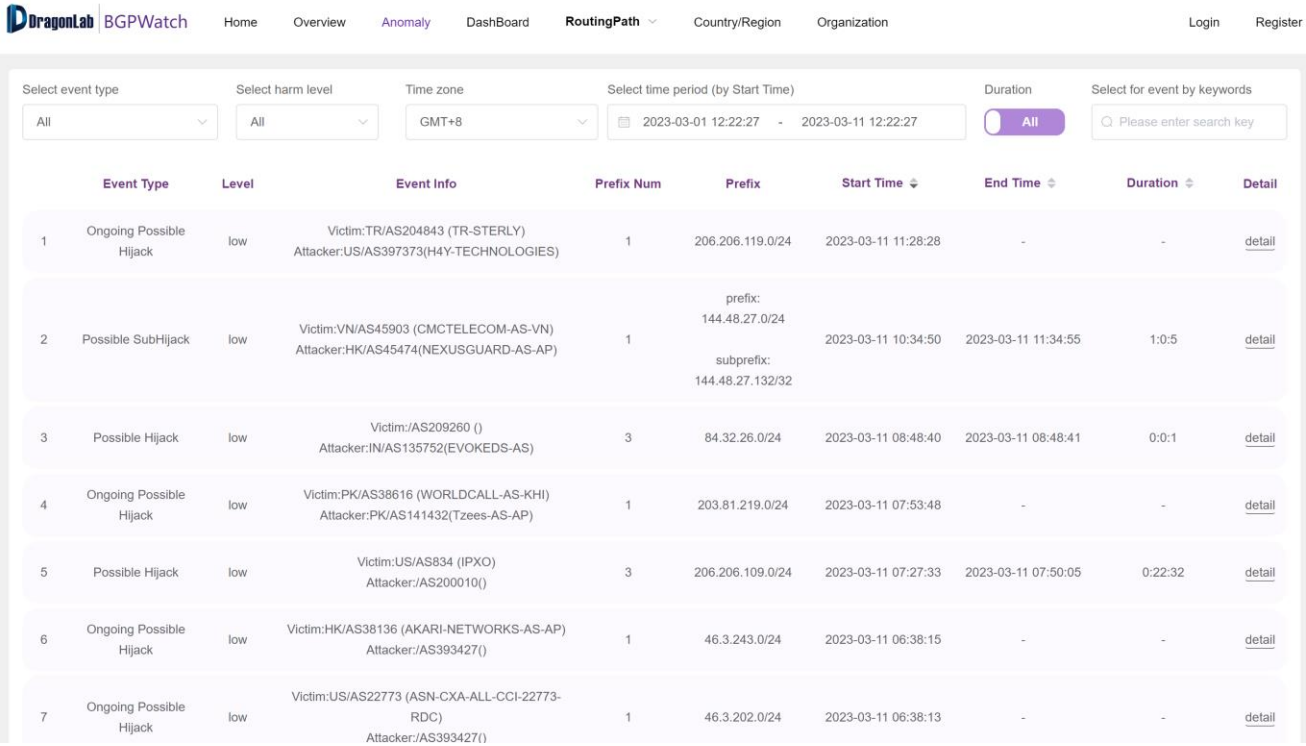


APNIC FOUNDATION

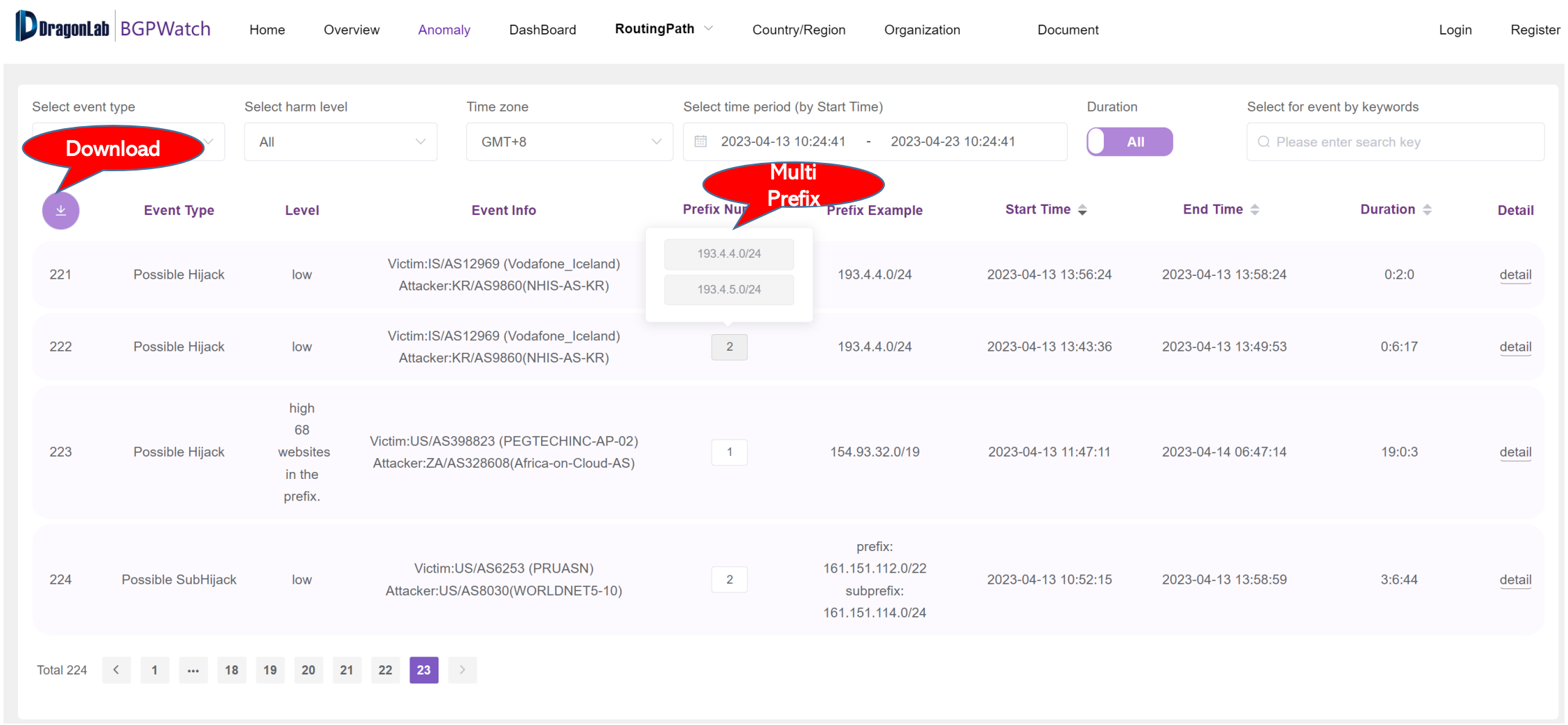
Tsinghua University

Hijacking Detection

- Knowledge-based real-tIme BGP hIjacking Detection System
- Public BGP event reporting servcie
- Based on MOAS(subMOAS)
- Rely on Domain Knowledge （ROA，IRR，AS relationship etc)
- URL: https://bgpwatch.cgtf.net



Hijacking Detection



- Support download and show multi prefix
- Sync ROA & RIR data daily

APNIC FOUNDATION

清華大學 Tsinghua University

Features --- Event Level Evaluation

- **Evaluate event impact based on importance of AS and prefix.**

high level

Ongoing Possible Hijack Events

103.242.2.0/23-hijack1685952502 Ongoing Possible Hijack Events

Victim AS：140096

Victim Country：CN (China)

Victim Description：JINX-AS-AP

Start Time：2023-06-05 08:08:22

During Time：no data

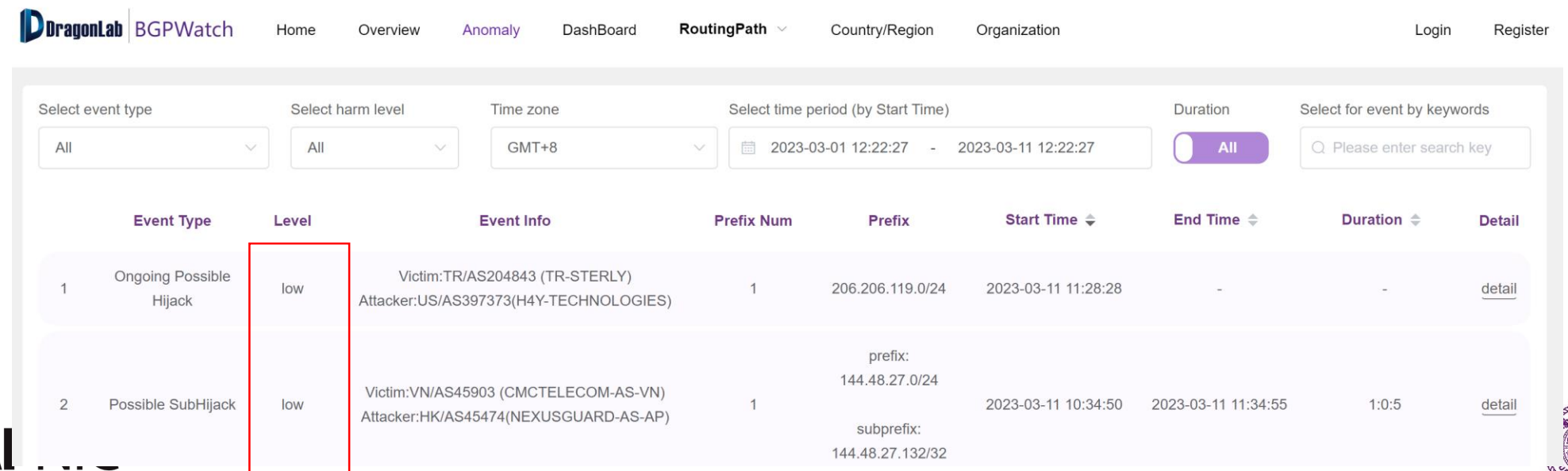
Hijacker AS：32519

Hijacker Country：US (United States)

Hijacker Description：DMIT-SERVICES

End Time：-

Time Zone：UTC

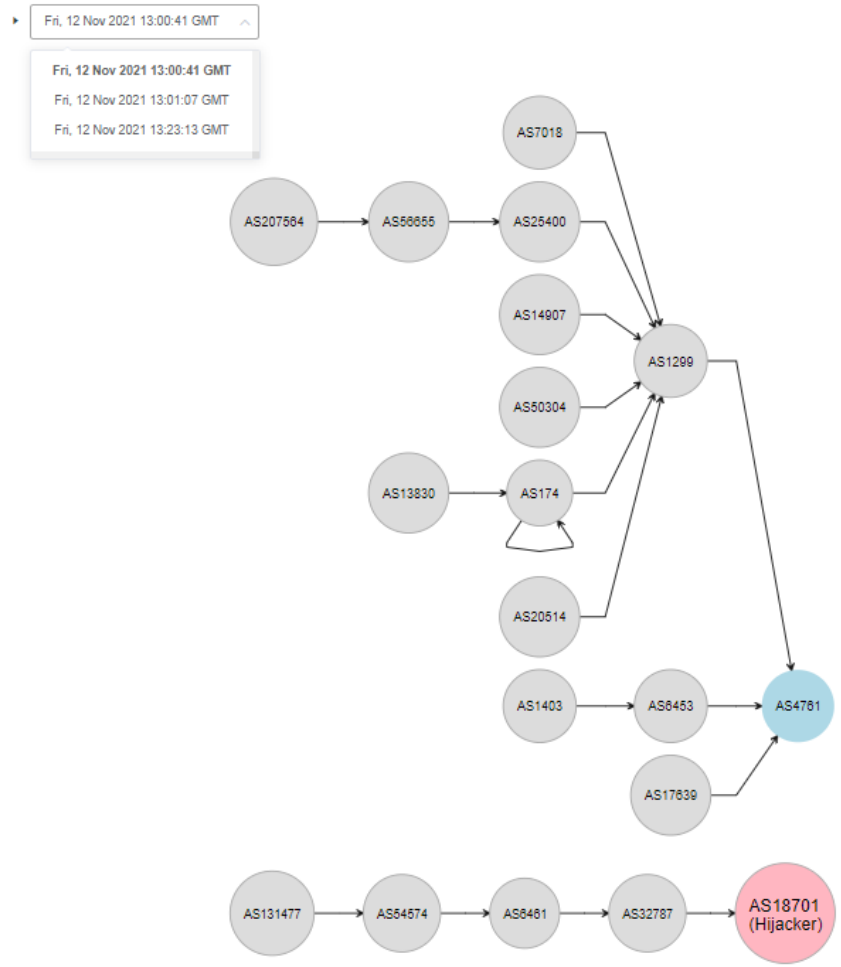


AI FOUNDATION

Tsinghua University

Features --- Quick Response, Event replay

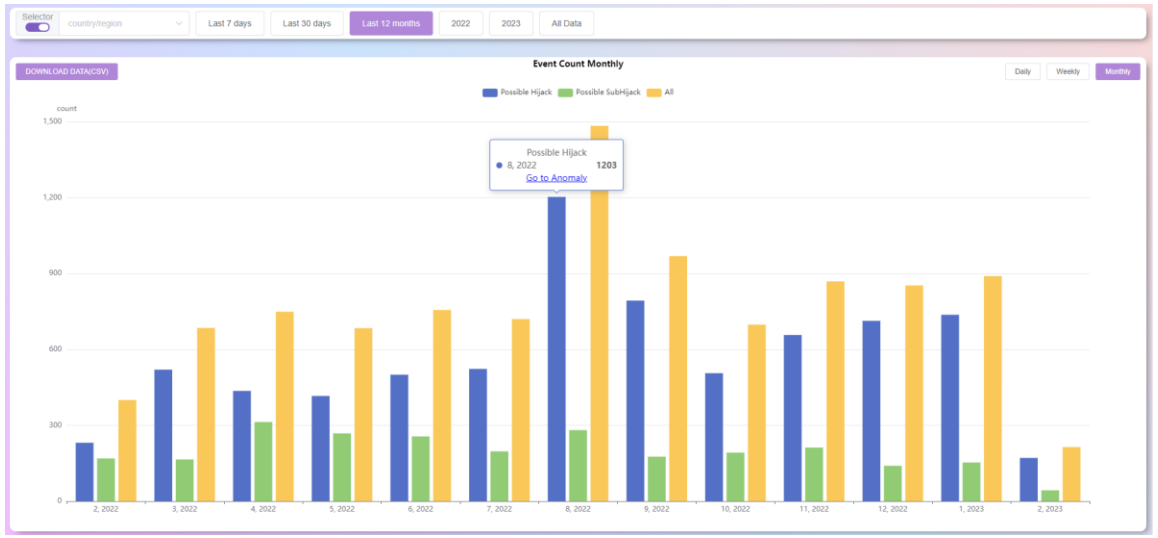
- About 5 mins delay, much better than most systems
- Notify immediately when an event is detected, minimizing damage from hijackings
- Understanding how the BGP routing changes
- Analyze the extent of the impact of the event

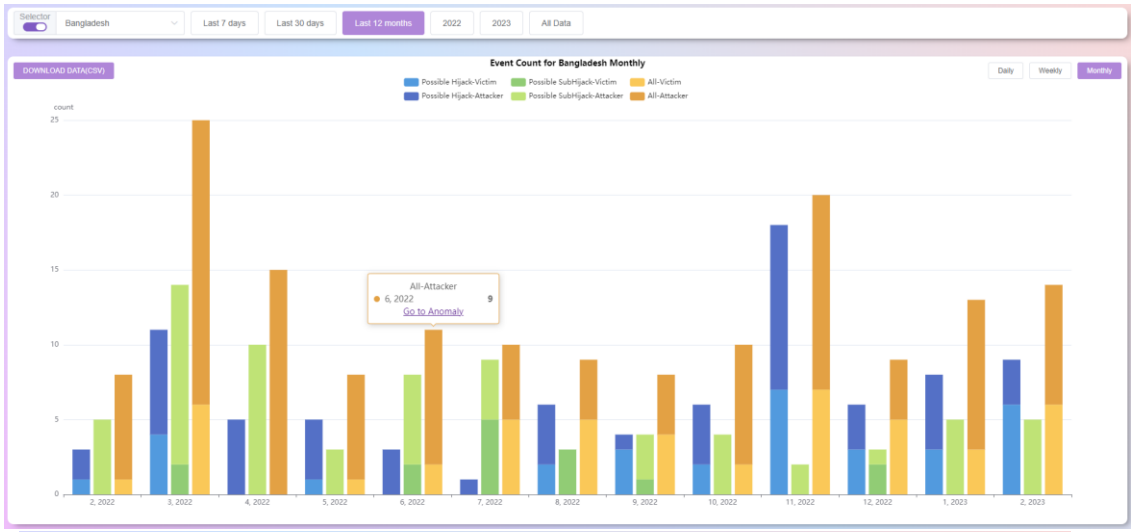


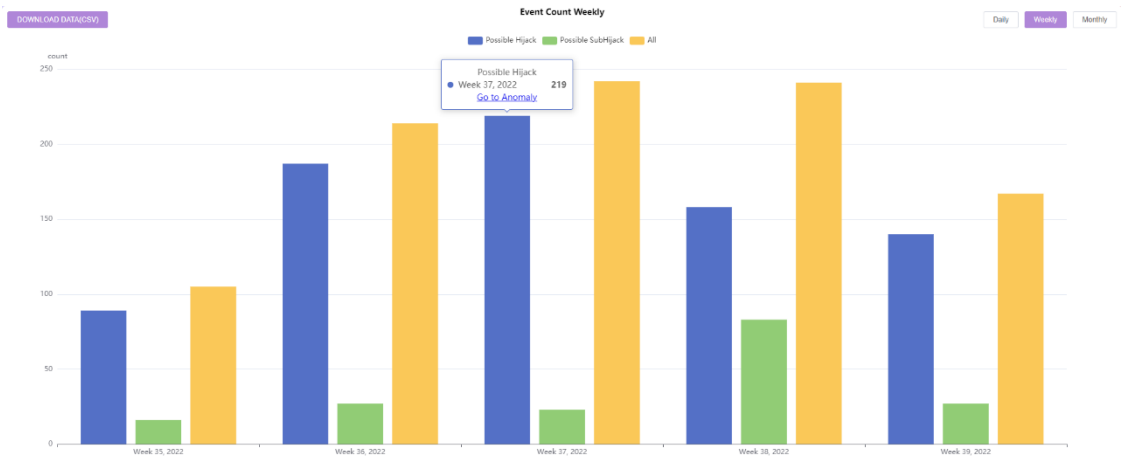
APNIC FOUNDATION

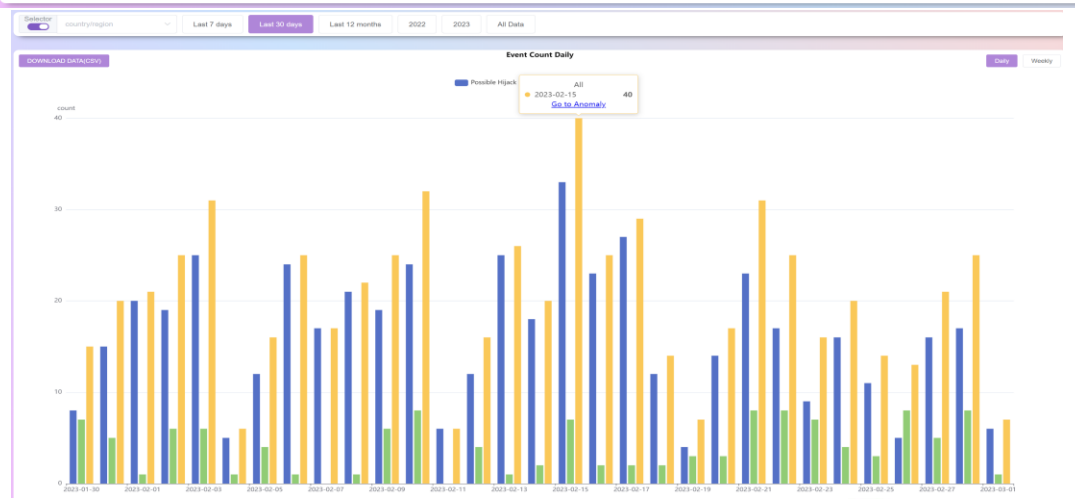
Tsinghua University

Overview--Statistics for Anomaly Events



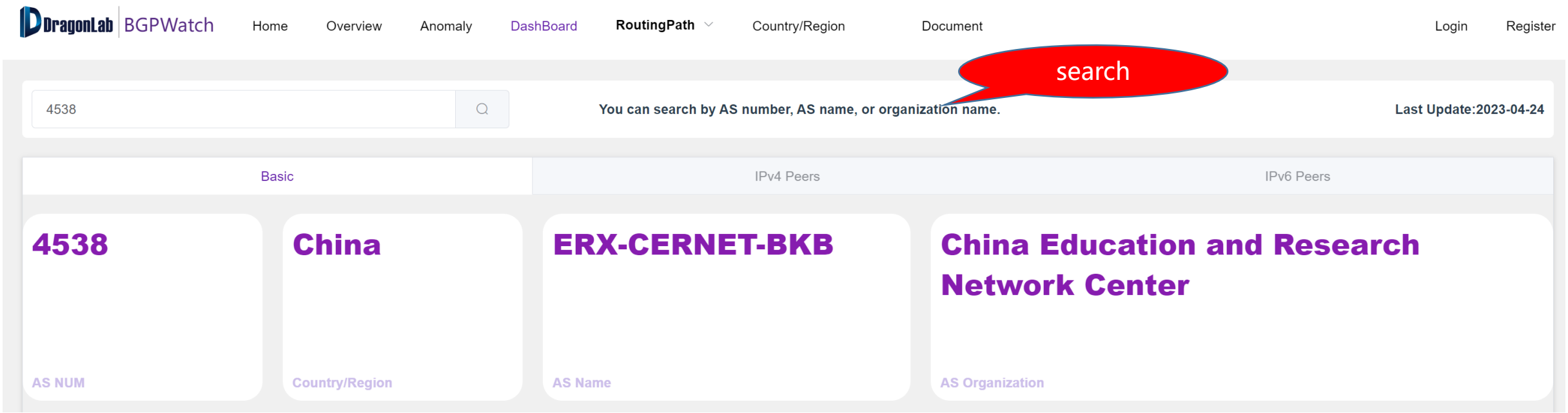






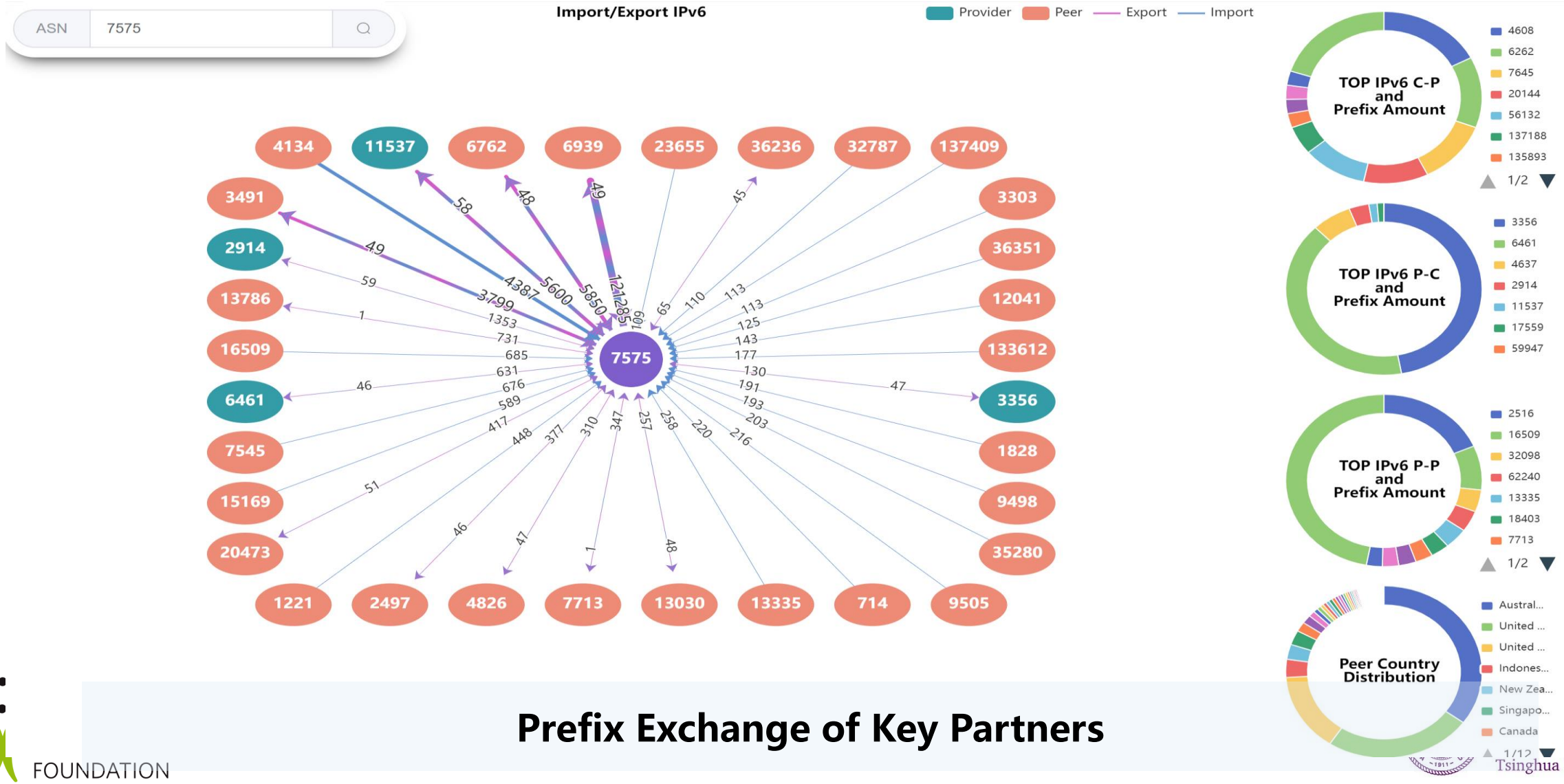
Do statistics by country/region, AS, and by yearly, monthly, weekly, and daily

DashBoard



- Subnet and Super-Net of Prefix are searched

IPv4/IPv6 Key Peers Information

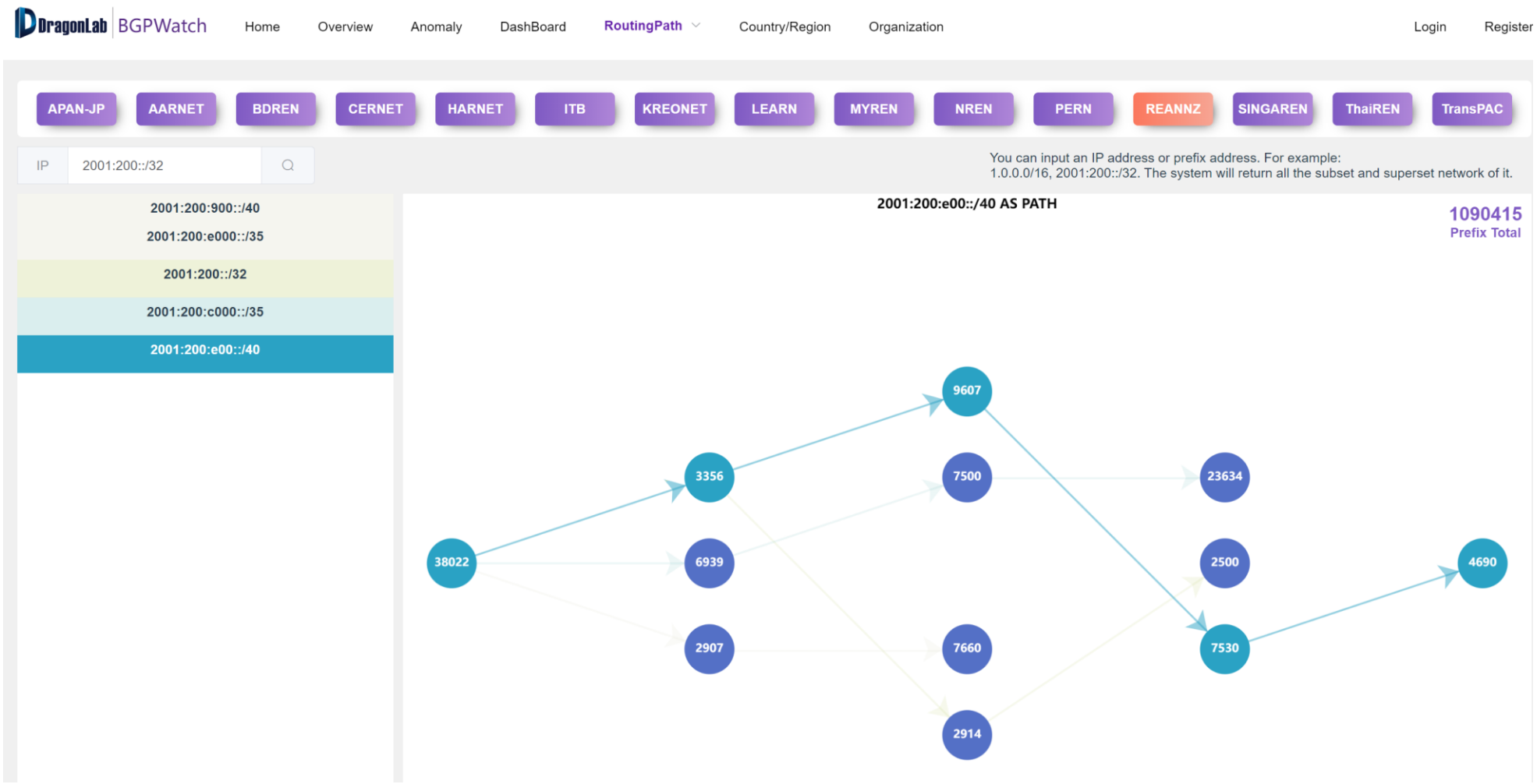


Prefix Exchange of Key Partners

FOUNDATION

Tsinghua University

Routing Path Search

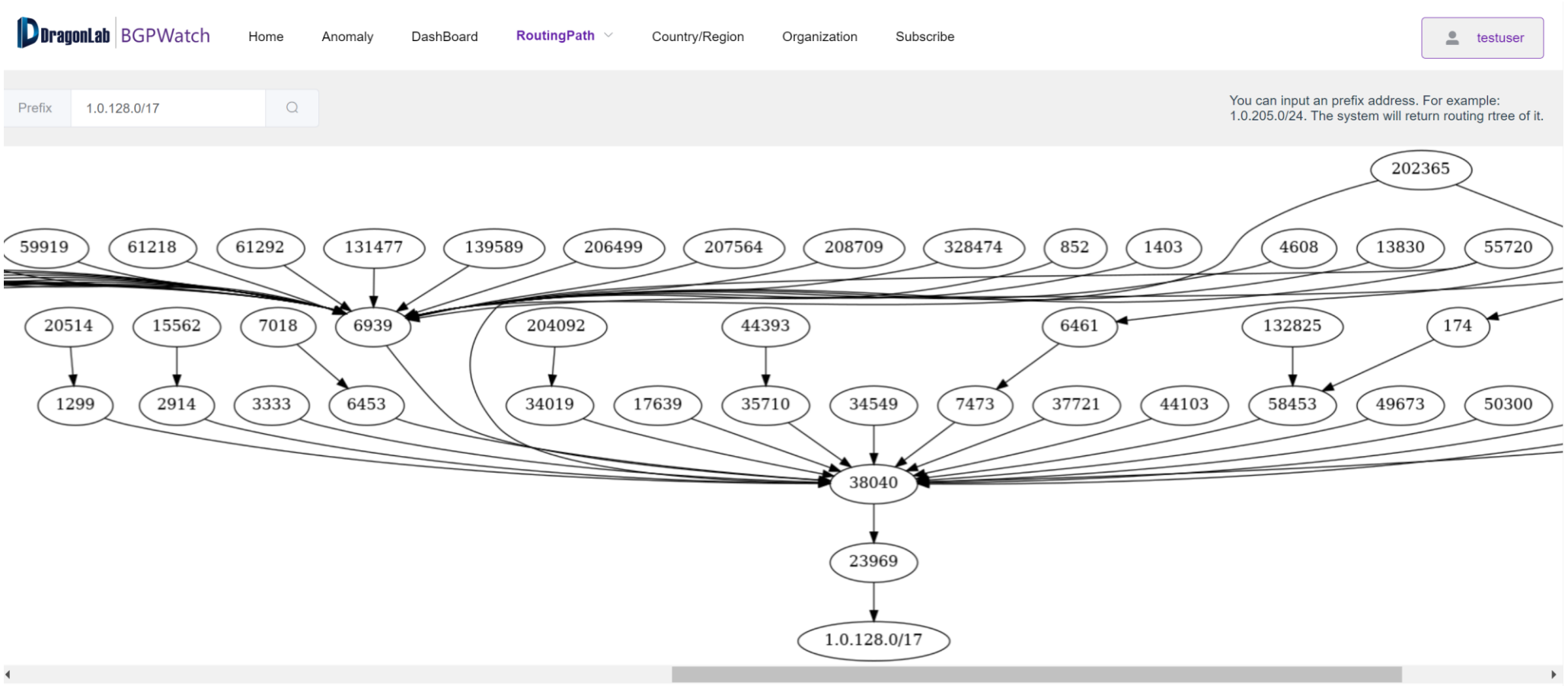


Support Prefix /IP, IPv4 / IPv6.

Return paths of all sub networks and super networks of the input prefix.

Group Prefixes with the same routing path.

Reverse Routing Path

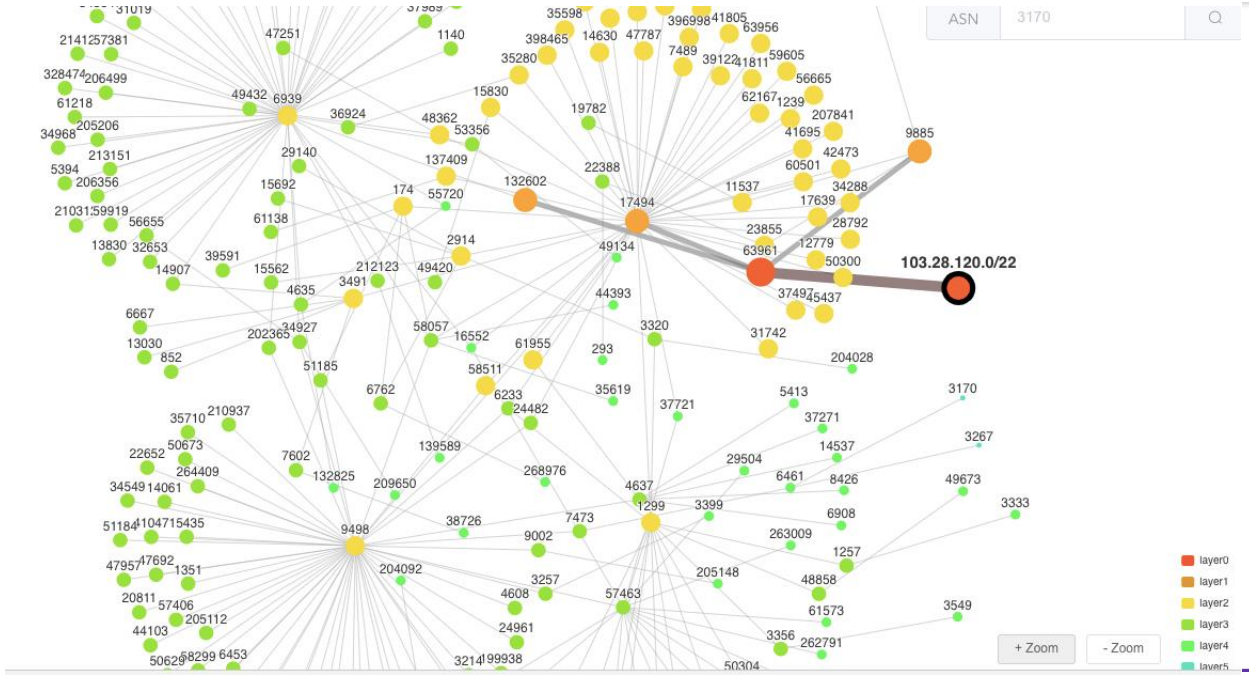


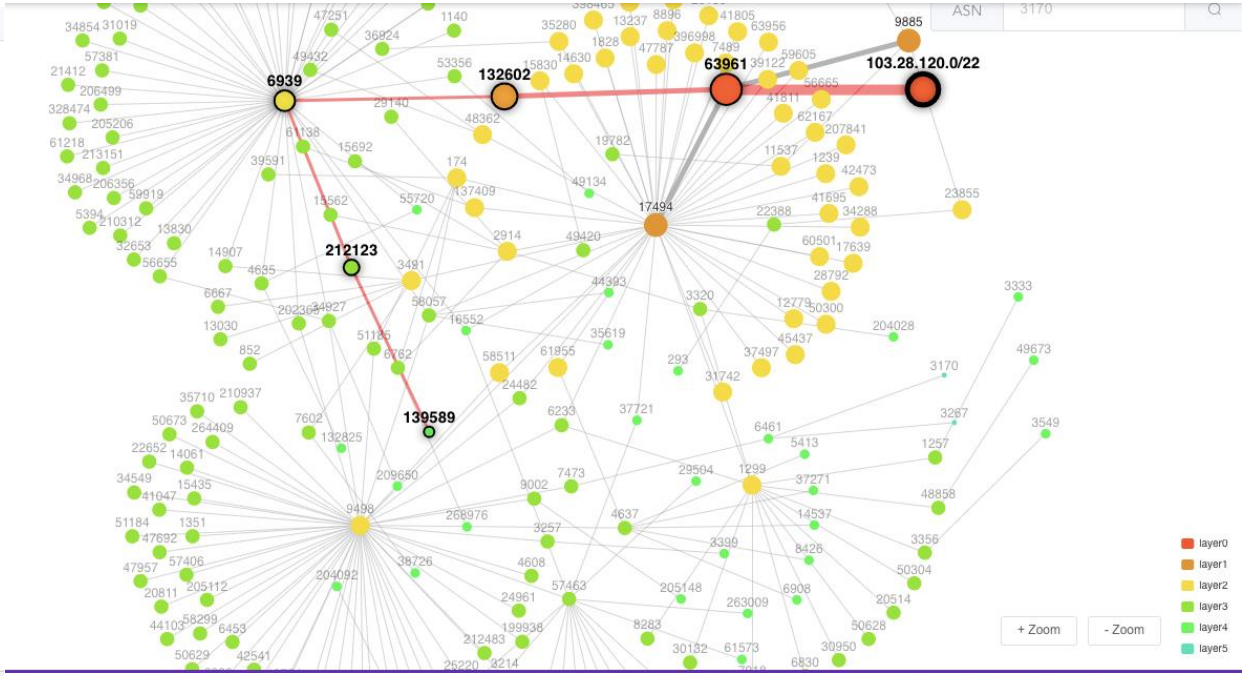
Support Prefix /IP, IPv4 / IPv6.
The system will search the best matched prefix and return the reverse routing tree.

APNIC FOUNDATION

清華大學 Tsinghua University

Reverse Routing Path (TOPO)



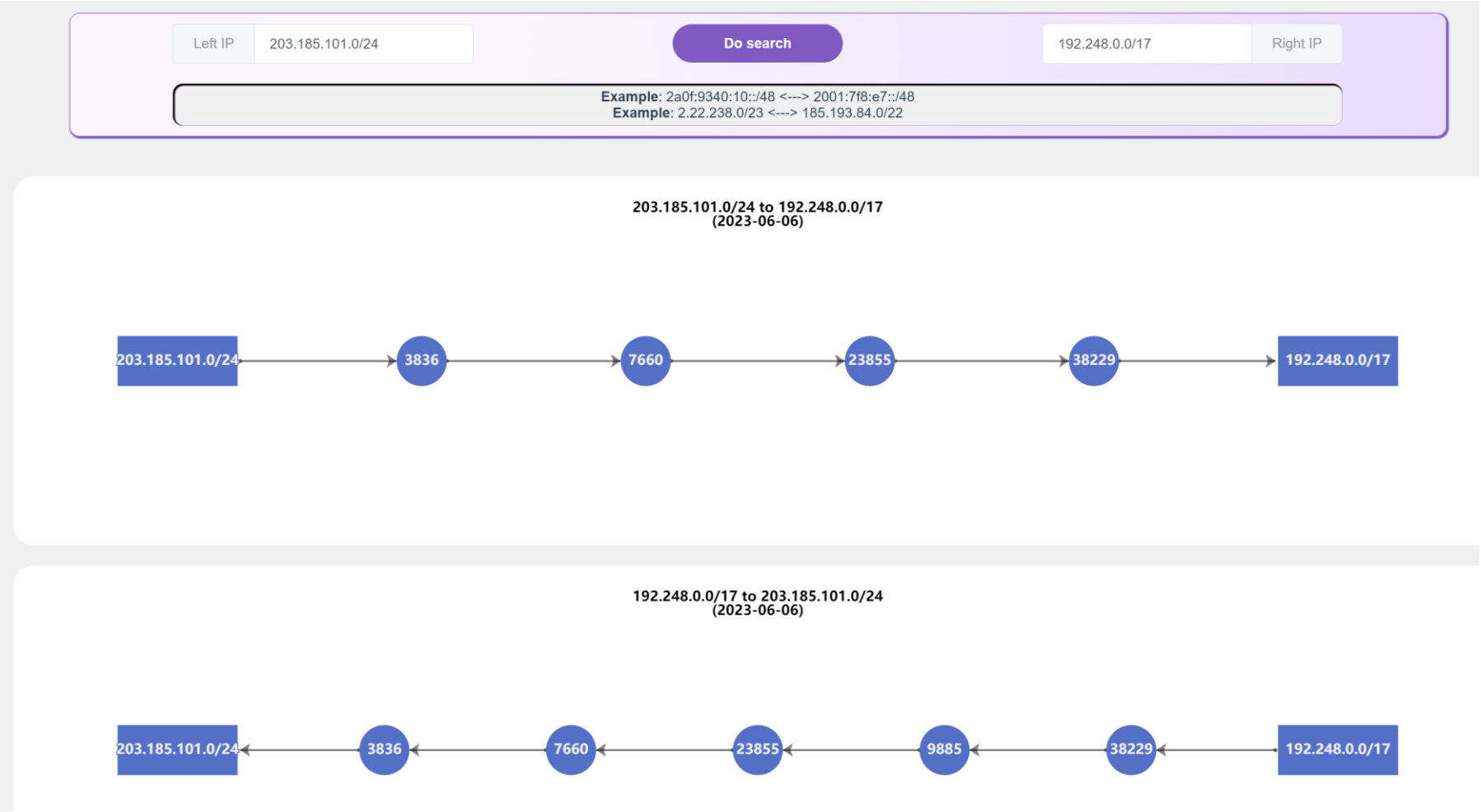


- **Support Prefix /IP, IPv4 / IPv6.**
- **The system will search the best matched prefix and return the reverse routing tree.**
- **With better interactivity**
- **Can select an AS or input AS number, the system will highlight the path to the AS**
- **The number of layers to display can be selected**

APNIC FOUNDATION

清華大學 Tsinghua University

Bi-Routing Path



- Left : 203.185.101.0/24 , from ThaiREN
- Right: 192.248.0.0/17 , from LEARN

Support Prefix /IP, IPv4 / IPv6.
The system will search the best matched prefix.

APNIC FOUNDATION

清華大學 Tsinghua University

Subscribe and Send Alarm Email

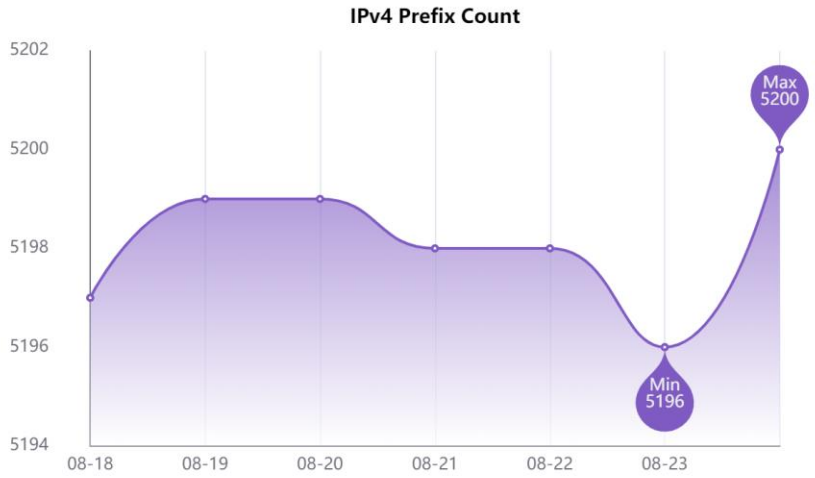
ASN **4538**

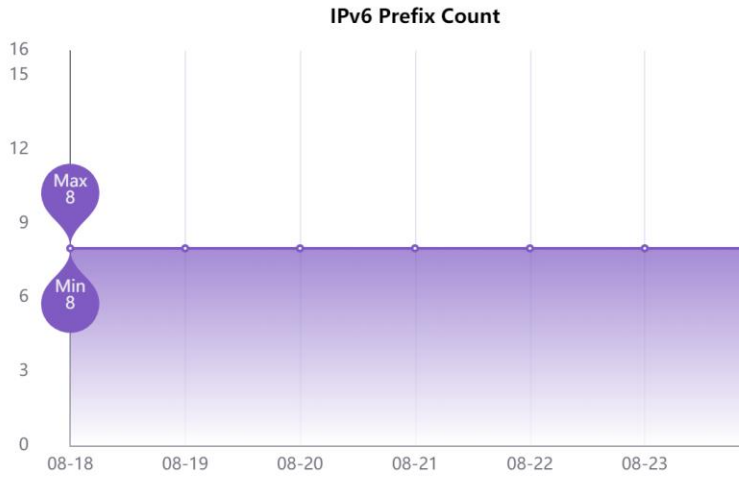
Country/Region **CN**

Name **ERX-CERNET-BKB**

Organization **China Education and Research Network Center**

Prefixes Changed **+ 4 - 0**





Prefix Change

+59.64.64.0/20

+121.194.32.0/20

+211.68.32.0/20

+211.82.96.0/20

Announced prefixes changes between 2022-08-24 00:00:00 (GMT) and 2022-08-23 00:00:00 (GMT)

ASN 7575
+ 203.6.255.0/24

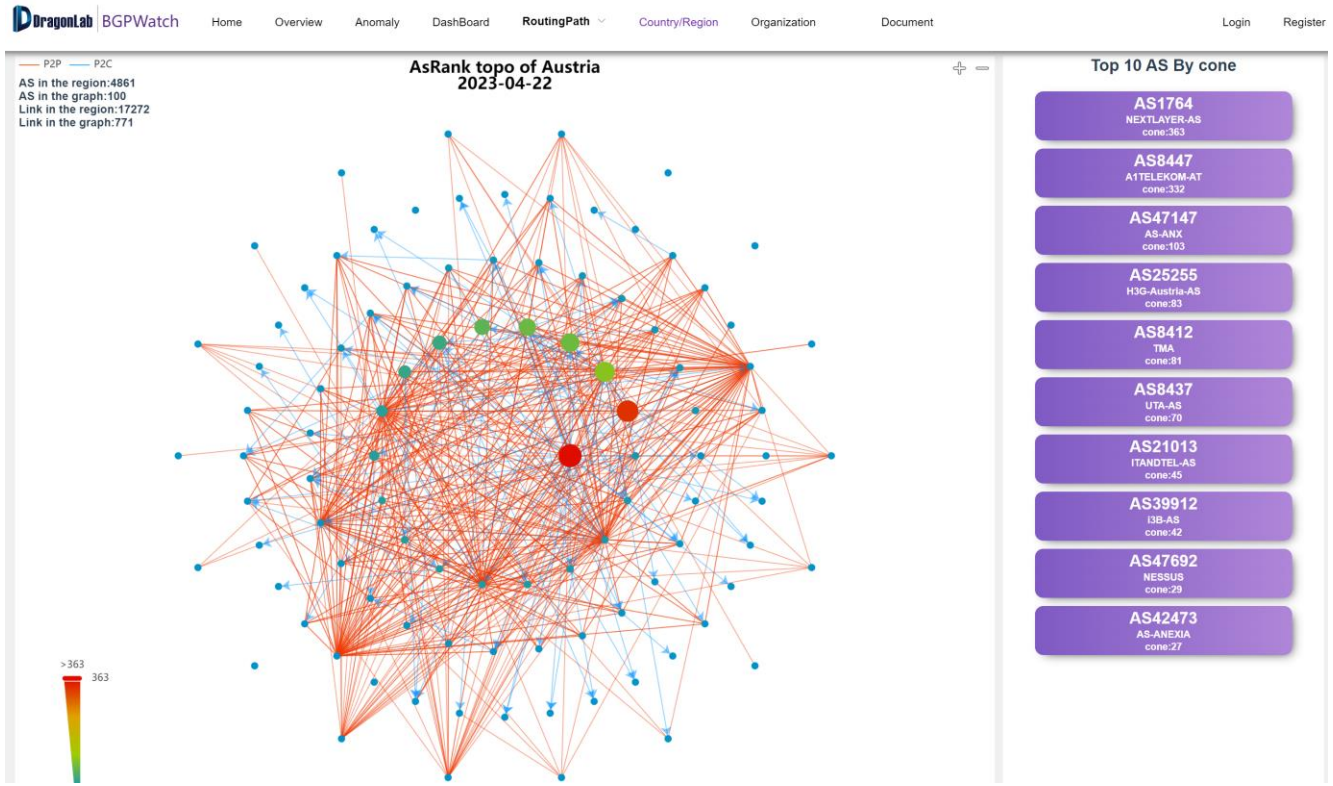
ASN 4538
+ 59.64.64.0/20
+ 121.194.32.0/20
+ 211.68.32.0/20
+ 211.82.96.0/20

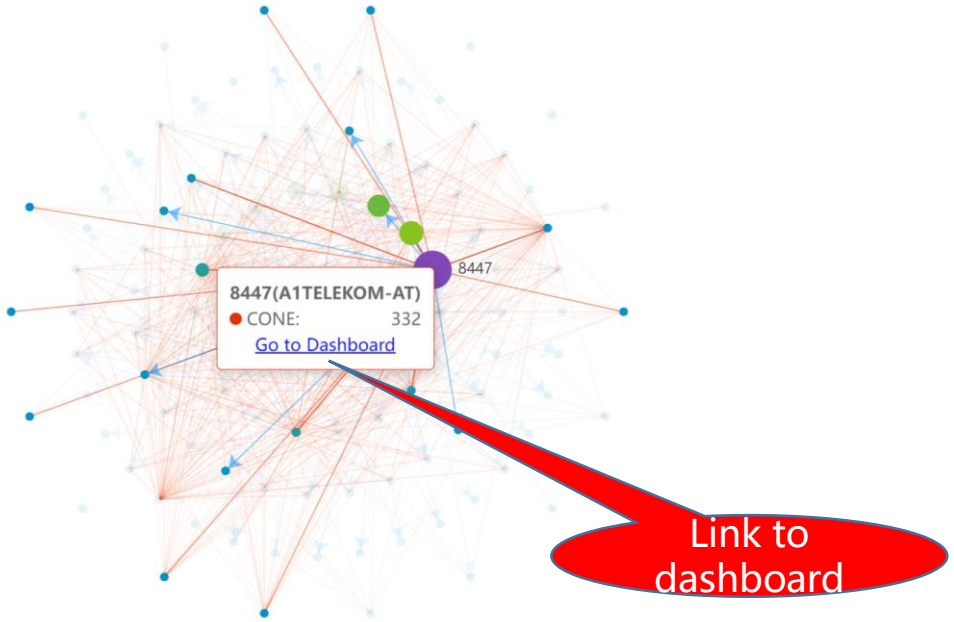
We are testing sending alarm by Slack

APNIC FOUNDATION

清華大學 Tsinghua University

Topo of Country/Region





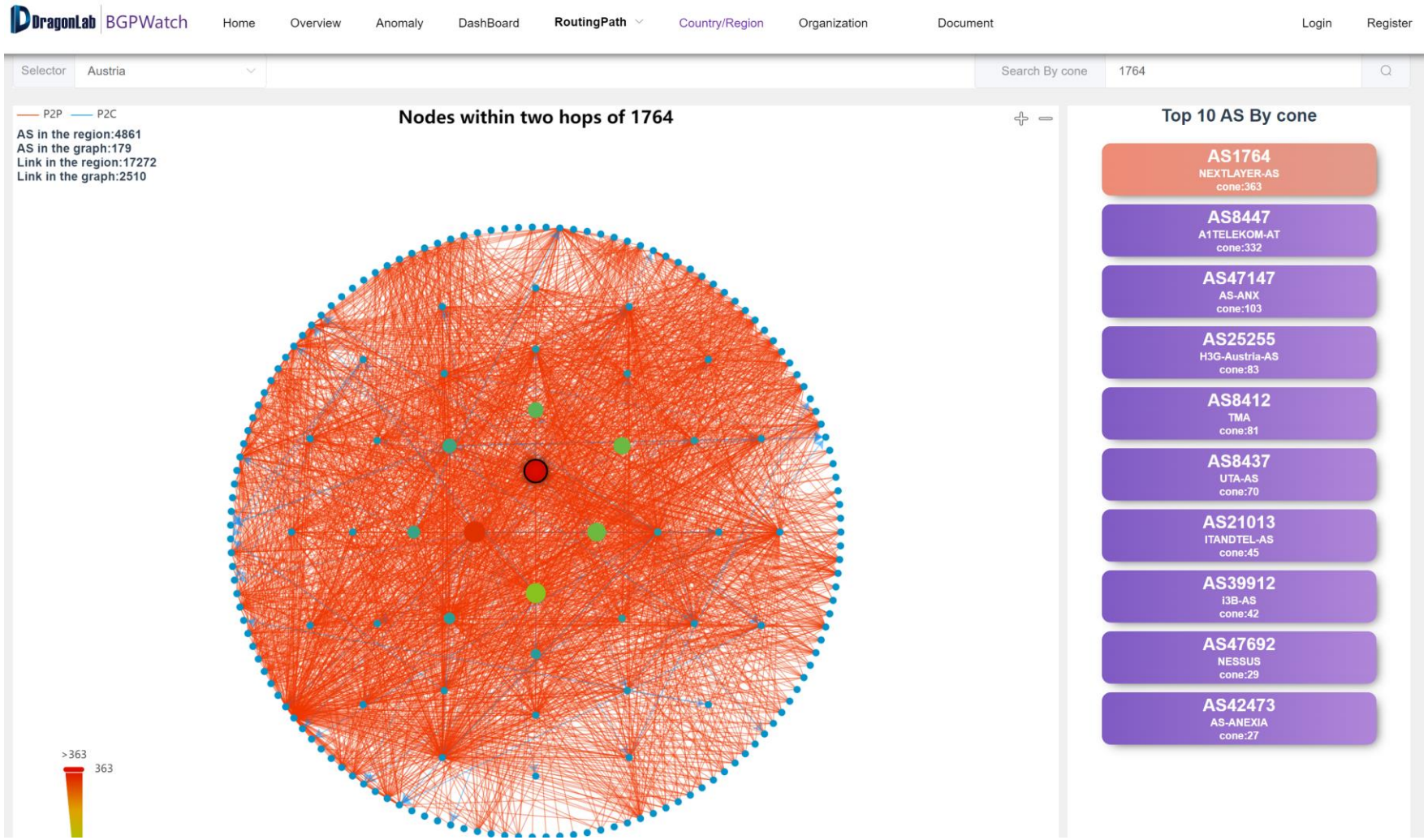
Show TOP 10 AS

Link to Dashboard

APNIC FOUNDATION

Tsinghua University

Topo of Country/Region



Click the AS button, show nodes within two hops of it

The Online Training in February

RPKI Basic Knowledge		
Date/Time	Length	Trainer/APNIC
1st Feb. 2023 (Wednesday) 0500-0700 GMT	2 hours	Warren Finch(trainer), Awal Haolader(assistant)
RPKI Hands-on		
3rd Feb. 2023 (Friday) 0500-0730 GMT	2.5 hours	Warren Finch, Awal Haolader(assistant)
Remarks		

Open Links via APNIC Academy:

https://academy.apnic.net/en/events?id=a0B2e000000cg1jEAA

https://academy.apnic.net/en/events?id=a0B2e000000cg3BEAQ

80 Engineers and Technicians take part in

清華大學 Tsinghua University

APNIC FOUNDATION

Knowledge Sharing at APAN55

- Knowledge Sharing Events at APAN55 were very successful
  - 4 sessions for RPKI Theory and Hands-on
  - 1 session for RPKI User Cases and Experience Sharing
  - 2 sessions for MANRS: What, Why and How, and User Cases and Experience Sharing
  - About 170 training opportunities were provided with very good feedback
  - A small complain is that the meeting room seemed too small because of more participants
- Acknowledgement
  - Tsinghua team, APNIC, APAN, NREN (NP), and the support from other NREN partners
  - Warrick Mitchell (AARNET)
    - Gave a lots of advice on these events organization
    - Chair of one MANRS session
    - Trainer of MANRS
    - Speaker of two sessions: RPKI and MANRS Experience Sharing
  - Other trainers/speakers from APNIC and NREN partners
    - Jamie Gillespie (APNIC), Dibya Khatiwada (APNIC Community Trainer)
    - Aaron Murrihy (REANNZ), Christopher Bruton (CENIC), Jiang Zhu (China Telecom), Yanbiao Li (CSTNET), Zhonghui Li (CERNET)
    - Two NREN assistant trainers from Nepal NREN: Binita Kusum Dhamala, Milan Adhikari

清華大學 Tsinghua University

APNIC FOUNDATION

Physical Meeting in Beijing (May 24-25)

- **Two Research Topic:**

- Topic: Detecting Fake AS-PATHs Based on Link Prediction
  Speaker: Chengwan Zhang, Tsinghua University
- Topic: Outsourcing Mitigation against BGP Prefix Hijacking
  Speaker: Man Zeng, Beijing University of Posts and Telecommunications

- **Bilateral meeting with 6 partner organizations:**

  - Thairen
  - Bdren
  - LEARN
  - DOST – ASTI
  - NREN
  - PERN

- **DNSSEC Training**

Over 50 Engineers and Technicians take part in

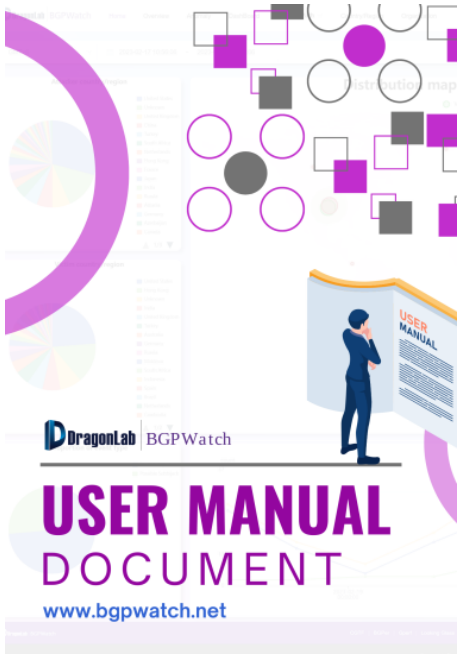
APNIC FOUNDATION

清華大學 Tsinghua University

Manual and Video

- User Manual for BGPWatch
- User Manual for BGPWatch(Video)

  --Joint efforts of BdREN and Tsinghua University



- CGTF BGP RIS Platform Manual
- CGTF Looking Glass Platform Manual
- Analysis of Suspected Hijacking Events in 2022

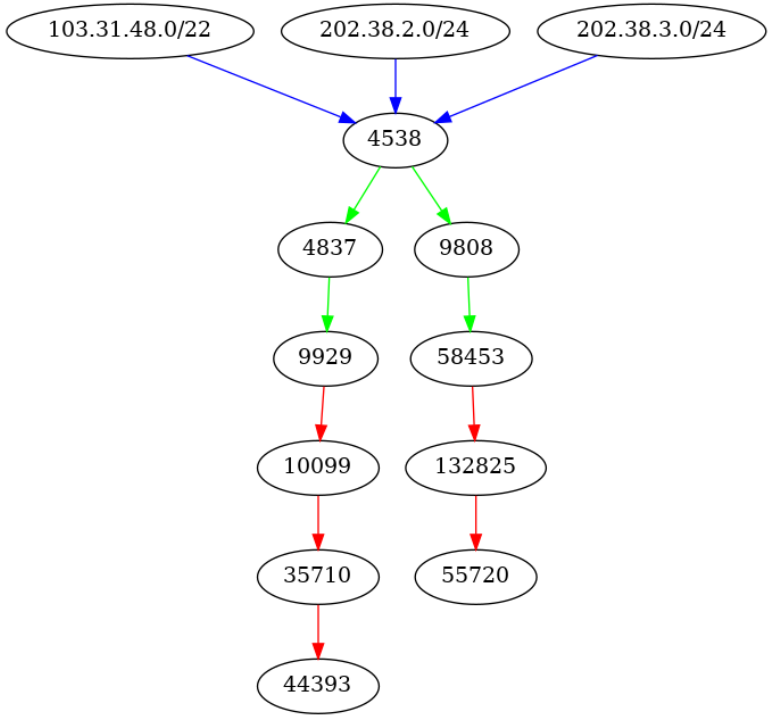
https://www.bgper.net/index.php/document/

清華大學 Tsinghua University

APNIC FOUNDATION

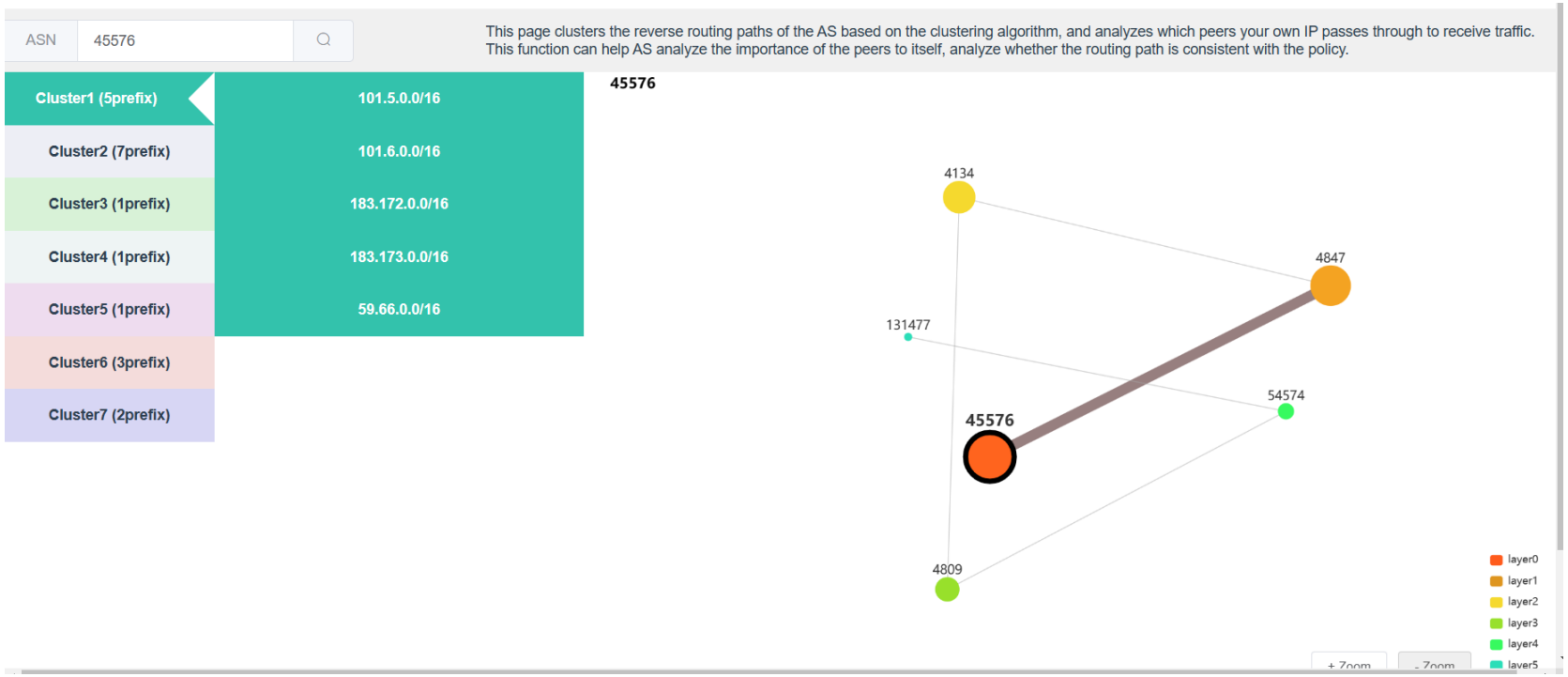
Research Work: Routing tree Clustering

- Routing tree: All AS-PATHs from BGP monitors to target prefix.
- Observation: AS will set different routing policies for different groups of prefixes. Different policy lead to different routing trees.
- Routing tree clustering: grouping of identical or similar routing trees.



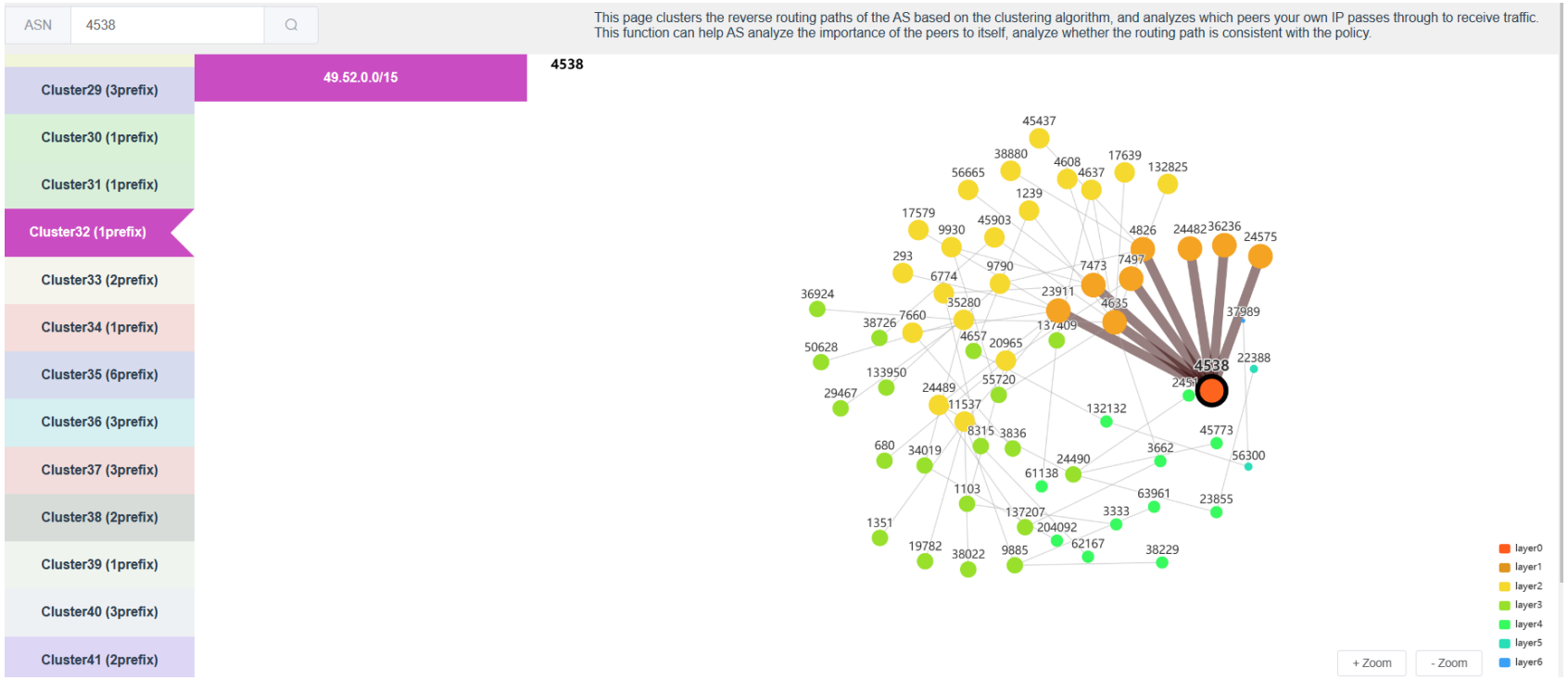
Application of Routing tree clustering

- Routing policy configuration consistency check
  - Administrators can check the consistency of external observations and internal routing policy configuration with the clustering result.



Application of Routing tree clustering

- Important prefix/special prefix discovery
  - Some AS configure separate routing policies for a small number of prefixes, which may be some important prefixes or special prefixes.

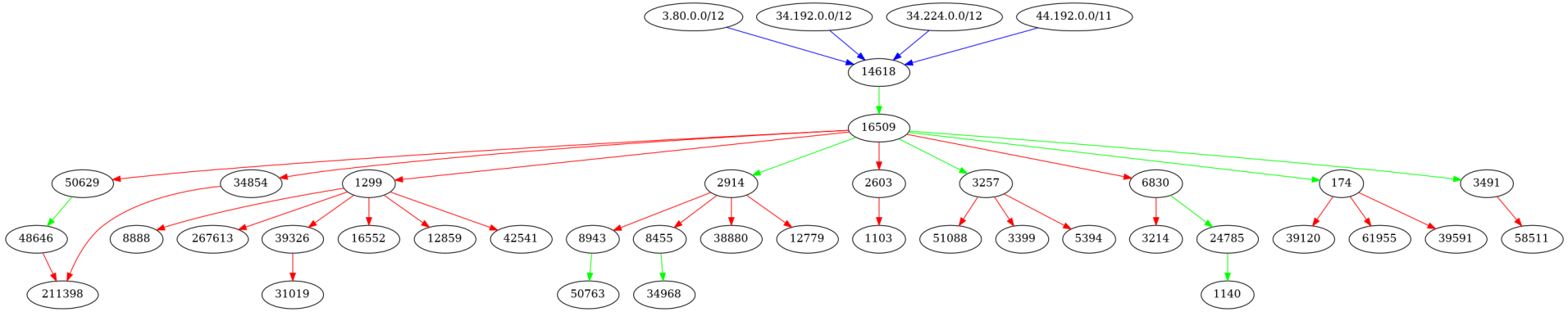


Application of Routing Tree Clustering

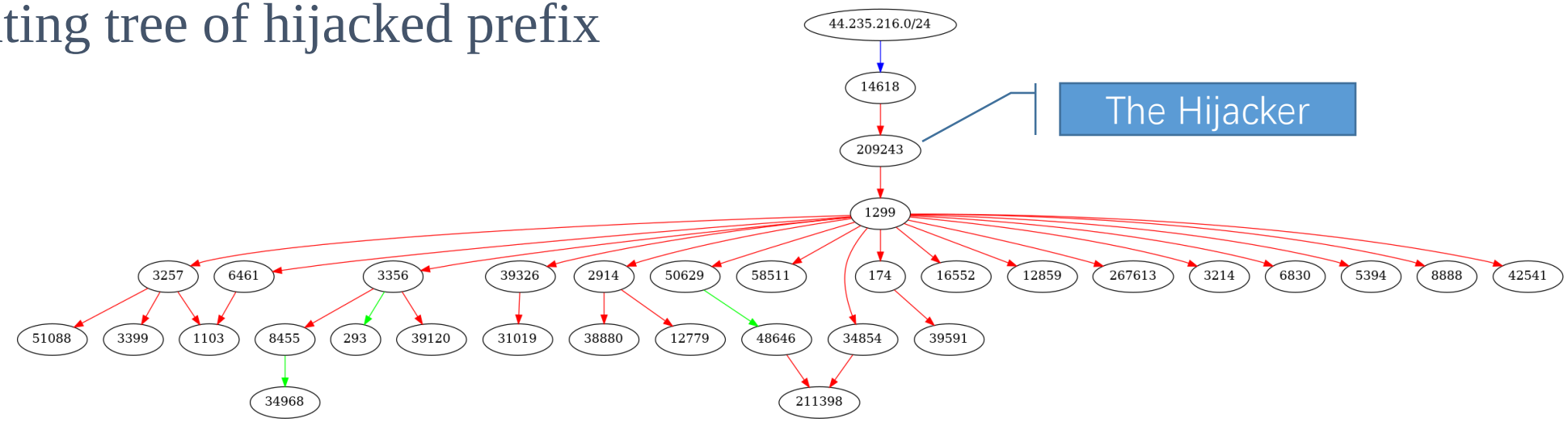
- Anomaly detection or Event review
  - Prefix hijacking or link failure, etc. can cause changes in clustering results, which can be used to detect anomalies.
  - For example, On August 17, 2022, 44.235.216.0/24 （belong to Amazon） was maliciously hijacked by attacker AS209243.
  - The results of clustering all prefixes of AS14618 by next-hop AS before and after hijacking.
  - 18:00 (before hijacking): 1 cluster, all paths go through AS16059 before arriving at AS14618.
  - 20:00 (during hijacking): 2 clusters， the hijacked prefixes form a separate cluster.
  - 24:00 (after hijacking recovery): 1 cluster.

Application of Routing Tree Clustering

- Routing tree of normal prefixes



- Routing tree of hijacked prefix



Work Plan for the Next Four Months

- Continue working on feedback from partners
- Parallel Computing and Clusters to handle big routing data
  - There are huge amount routing data from RouteViews, RIS, PCH, CGTF. Now we only use part of there data. We'll try to process all the data by Parallel Computing and Clusters. Even though, no one can get all the path information, so it's a best effort system.
  - Consider to analyze data by user request, not all path change, but the specific prefix user subscribed.

Proposal of the Next APNIC ISIF Funding (Draft)

- Deadline: 30 April
- Project name: An Extension of the Ongoing Project ‘Developing a Collaborative BGP Routing Analyzing and Diagnosing Platform’ Project
- Funds: USD85,000
- Duration: 18 months
- Objectives:
  - Develop an integrated looking glass platform and api, which can leverage many looking glasses and return data to users
  - Use looking glass to further check routing hijacking at the data plan, and to improve detection accuracy
  - Develop path hijacking detection and routing leak detection
  - Continue to maintain and fix bugs of BGPWatch platform
  - Continue the community development and international collaboration

清華大學 Tsinghua University

APNIC FOUNDATION

Comments and Suggestions?

Contact us at: sec@cgtf.net