

(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**

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**

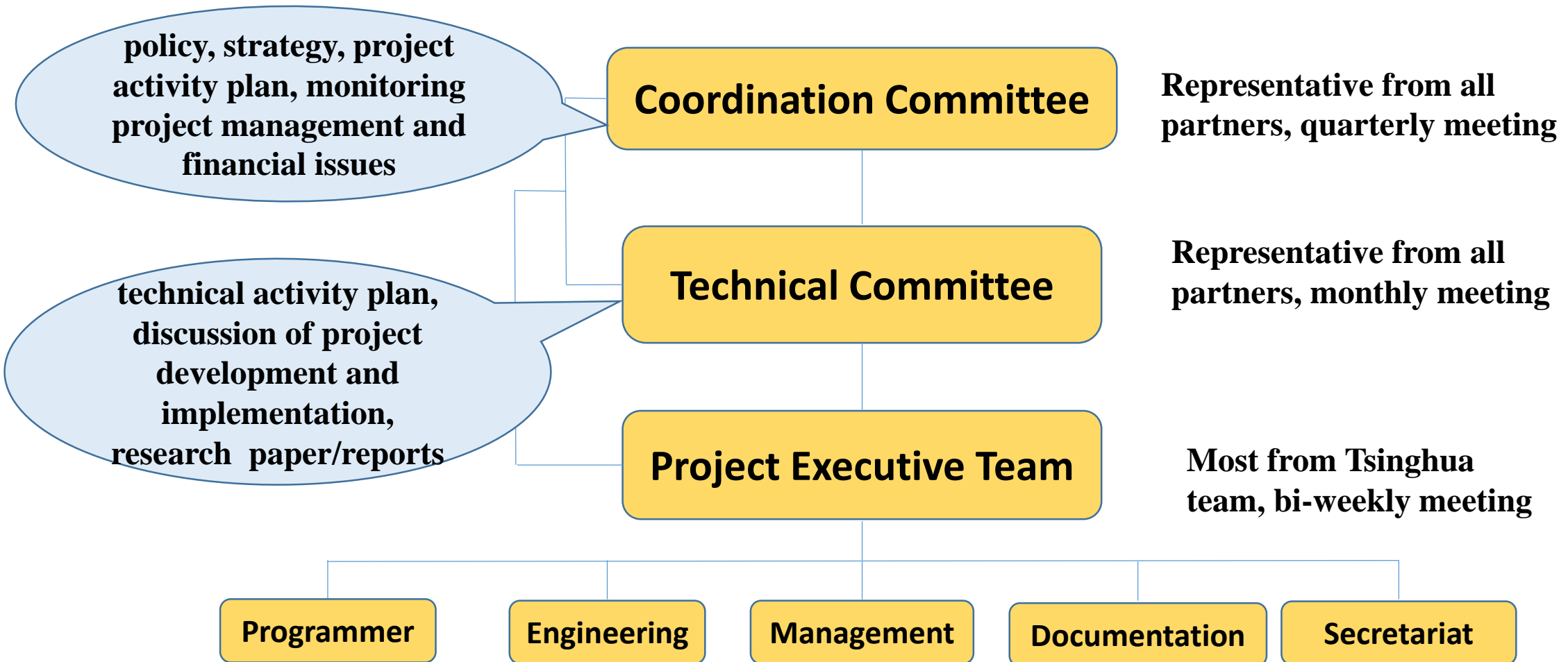
Partnership

- **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**

Project Governance



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

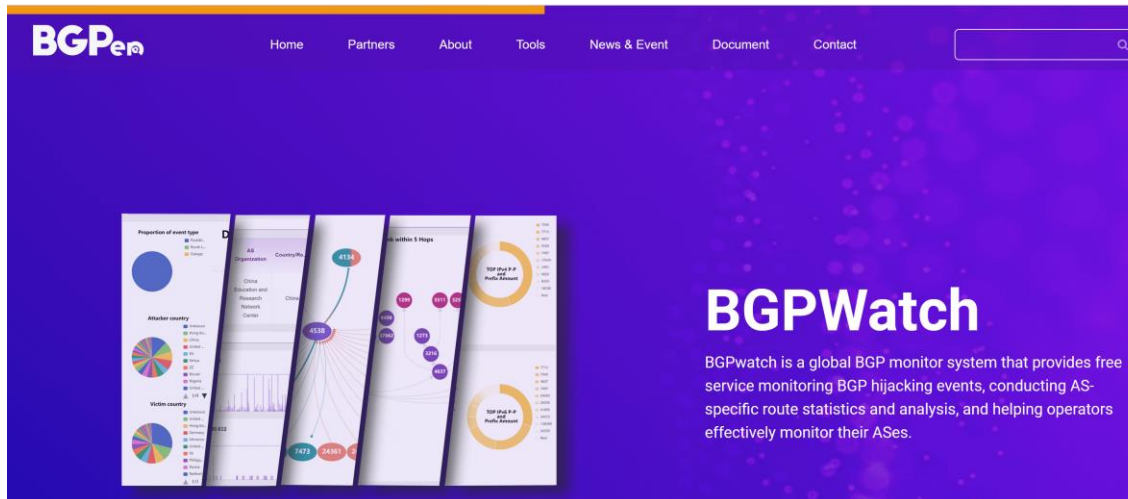
Established BGP session with **15 partners**

-BGPWatch: Analyzing and Diagnosing Platform

- **Knowledge Sharing & Community Building**

Project Web Site

<https://bgper.net>



Documents		
Meeting Materials		
• Meeting Materials	[APNIC Project] 5th Technical Committee Report	2023-01-19
• Other Presentations	[APNIC Project] Third Coordination Committee Report	2023-01-19
• Technical Documents	[APNIC Project] Second Coordination Committee Report	2022-09-29
	[APNIC Project] Fourth Technical Committee Report	2022-09-29
	[APNIC Project] Third Technical Committee Report	2022-08-03
	[APNIC Project] Second Technical Committee Report	2022-06-20
	[APNIC Project] First Coordination Committee Report	2022-05-10
	[APNIC Project] First Technical Committee Report	2022-05-10
Other Presentations		
	APNIC ISIF Presentation at APAN53	2022-03-08
	APNIC ISIF Presentation at APAN54	2022-08-24

Partners

Organization: AARNET

Since 1989, AARNET, Australia's Academic and Research Network has provided high-performing telecommunications and an expanding range of cyber security, data and collaboration services for Australia's research and education sector, including universities, research organisations, schools, vocational training providers and cultural institutions. AARNET serves over two million end users who access AARNET's network and services for teaching, learning and research. For more information, visit aarnet.edu.au

News & Event

The First Collaborative and Technical Meeting of "Collaborative BGP Routing Analyzing and Diagnosing Platform" Project

News On May 10, 2022, the First Collaborative and Technical Meeting of the "Collaborative BGP Routing Analyzing and Diagnosing Platform"...

[Read More →](#)

"Collaborative BGP Routing Analyzing and Diagnosing Platform" Project Kick-off Meeting

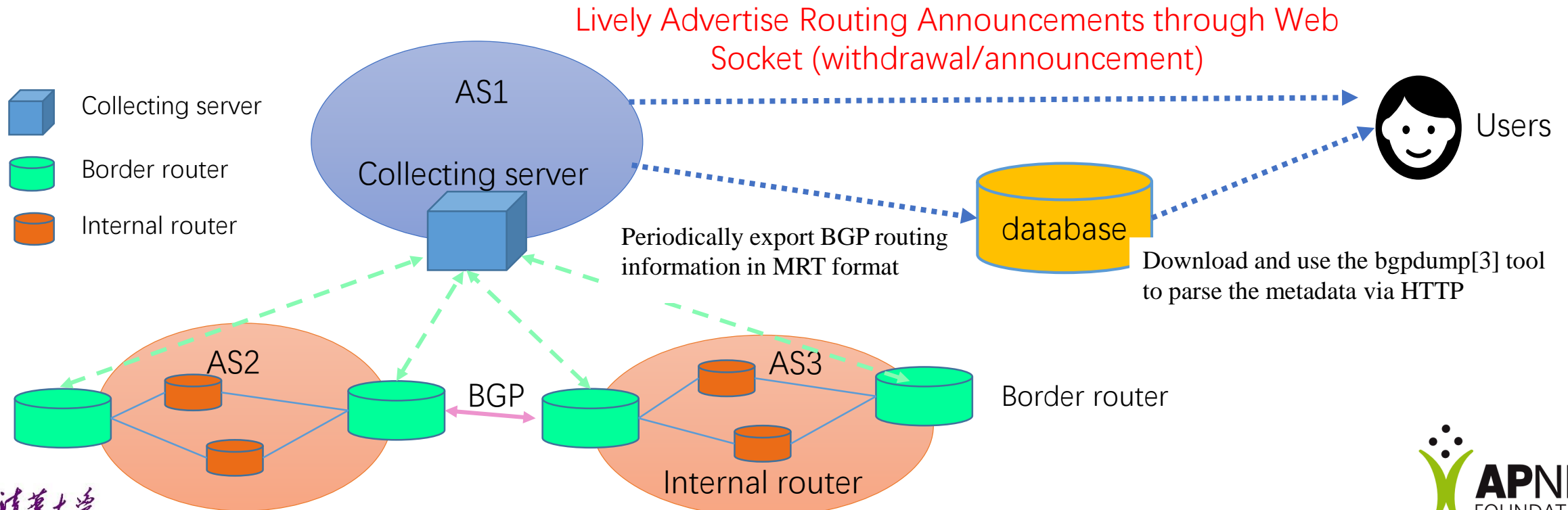
News Collaborative BGP Routing Analyzing and Diagnosing Platform" Project Kick-off MeetingOn February 24, 2022, Tsinghua University hosted the "Collaborative BGP Routing..."

[Read More →](#)

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



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/>

Index of /ribs/2022/07

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		

	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	

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

CGTF Looking Glass

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



Router to use

SingAREN Juniper Router
MYREN Cisco router
LEARN Guagga router
CERNET Guagga router
PERN Guagga router

Command to issue

show route IP_ADDRESS
show route as-path-regex AS_PATH_REGEX
show route ^AS
ping IP_ADDRESS|HOSTNAME
traceroute IP_ADDRESS|HOSTNAME

Parameter

66.175.222.61

Enter Reset

Your IP address: 66.175.222.61

Welcome to DragonLab's Network Looking Glass. The information provided by and the support of this service are on a best effort basis.

Looking Glass of Partners
<http://lg.kreonet2.net>
<http://lg.aarnet.edu.au>
<https://lg.myren.net.my/lg/lg.cgi>

Link to partners' looking glass

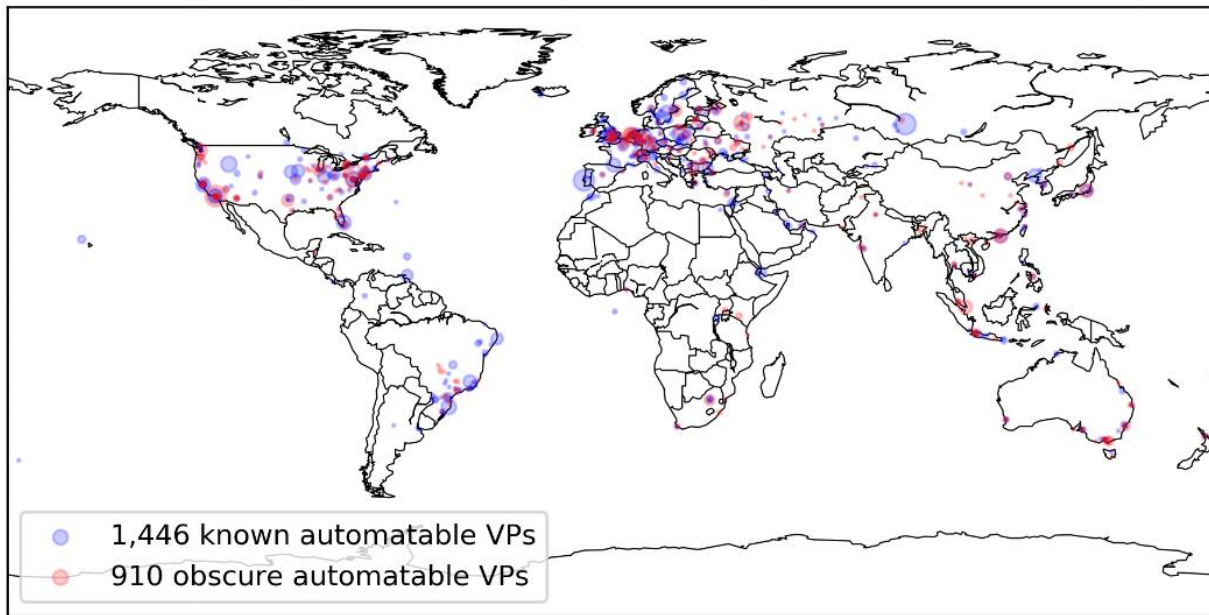


7 Education & Research network joined
Add links to partners' looking glass



Open Looking Glass Vantage Point

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



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

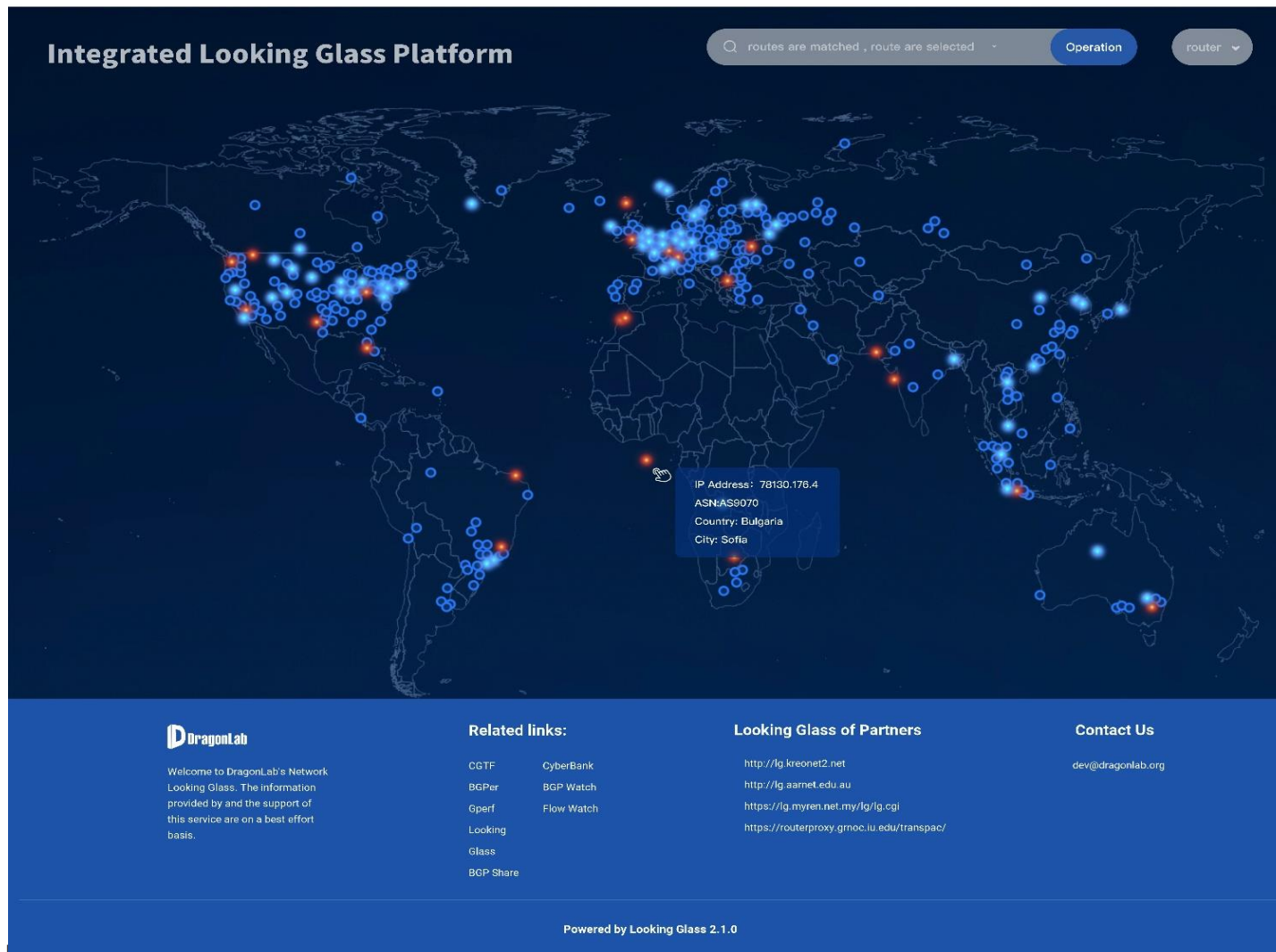
- ✓ The 8 countries are mainly distributed in **East Africa** and **South Asia**

Periscope has found several hundred VPs (364)

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

An Integrated Looking Glass and Open API

DragonLab CGTF Looking Glass

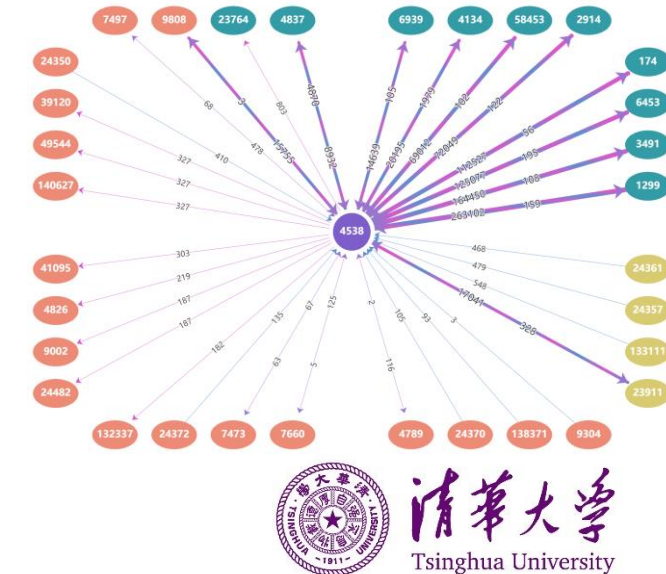
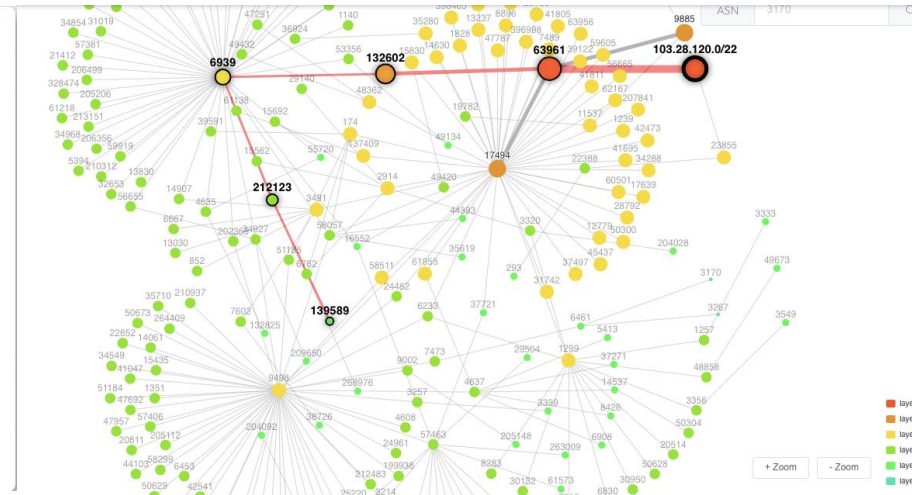
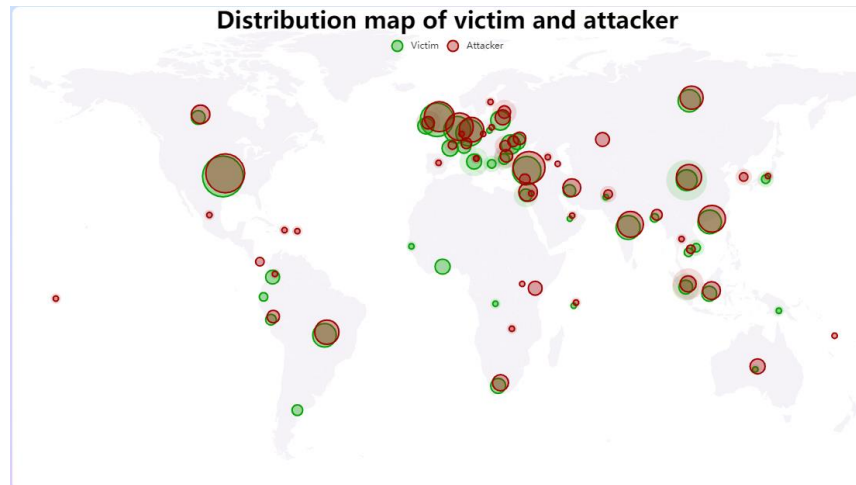
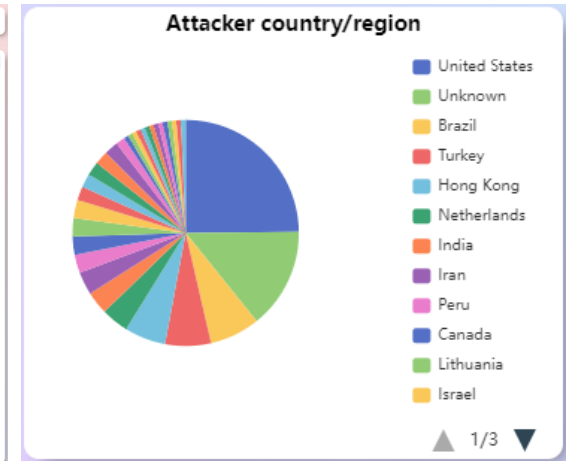
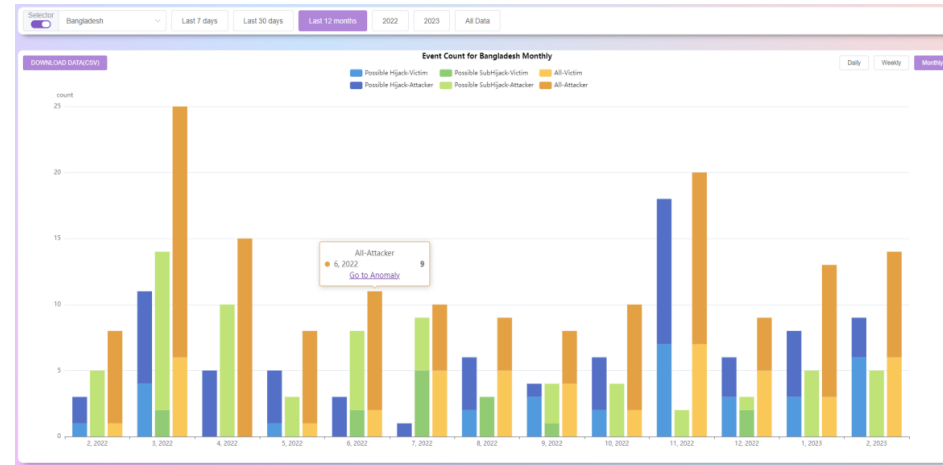


Based on the found VP
Open API,
Open source,
Open Platform

BGP Routing Monitoring and Analysis: BGPWatch

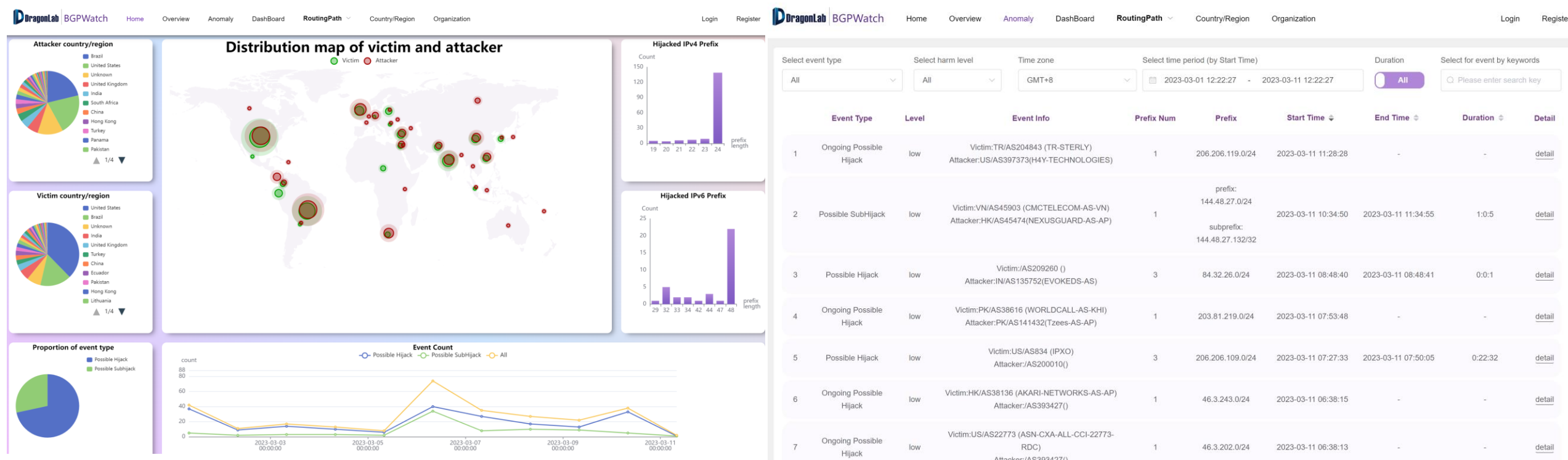
<https://bgpwatch.cgtf.net>

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



Hijacking Detection

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



Hijacking Detection

Select event type

Select harm level

Time zone

Select time period (by Start Time)

Duration

Select for event by keywords

Download

All

GMT+8

2023-04-13 10:24:41 - 2023-04-23 10:24:41

All

Please enter search key

	Event Type	Level	Event Info	Prefix Num	Prefix Example	Start Time	End Time	Duration	Detail
221	Possible Hijack	low	Victim:IS/AS12969 (Vodafone_Iceland) Attacker:KR/AS9860(NHIS-AS-KR)	<div>193.4.4.0/24</div> <div>193.4.5.0/24</div>	193.4.4.0/24	2023-04-13 13:56:24	2023-04-13 13:58:24	0:2:0	detail
222	Possible Hijack	low	Victim:IS/AS12969 (Vodafone_Iceland) Attacker:KR/AS9860(NHIS-AS-KR)	2	193.4.4.0/24	2023-04-13 13:43:36	2023-04-13 13:49:53	0:6:17	detail
223	Possible Hijack	high 68 websites in the prefix.	Victim:US/AS398823 (PEGTECHINC-AP-02) Attacker:ZA/AS328608(Africa-on-Cloud-AS)	1	154.93.32.0/19	2023-04-13 11:47:11	2023-04-14 06:47:14	19:0:3	detail
224	Possible SubHijack	low	Victim:US/AS6253 (PRUASN) Attacker:US/AS8030(WORLDDNET5-10)	2	prefix: 161.151.112.0/22 subprefix: 161.151.114.0/24	2023-04-13 10:52:15	2023-04-13 13:58:59	3:6:44	detail

Total 224 < 1 ... 18 19 20 21 22 23 >

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

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

DragonLab | BGPWatch

Home Overview Anomaly DashBoard RoutingPath Country/Region Organization Login Register

Select event type

All

Select harm level

All

Time zone

GMT+8

Select time period (by Start Time)

2023-03-01 12:22:27 - 2023-03-11 12:22:27

Duration

All

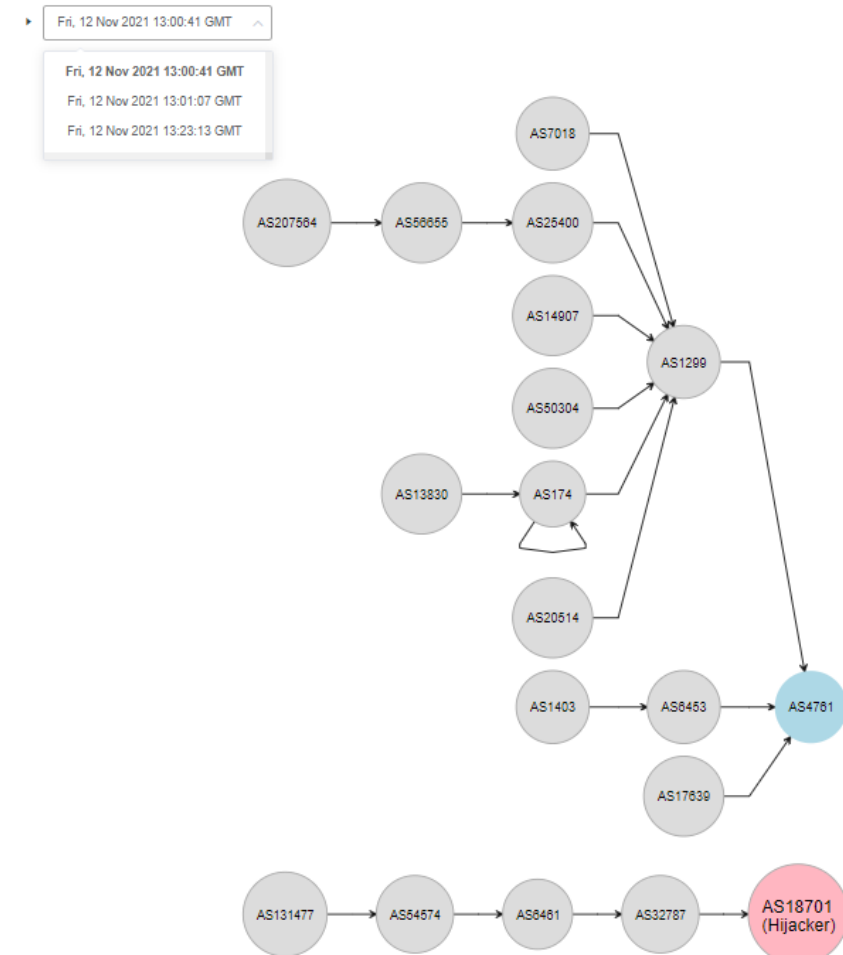
Select for event by keywords

Please enter search key

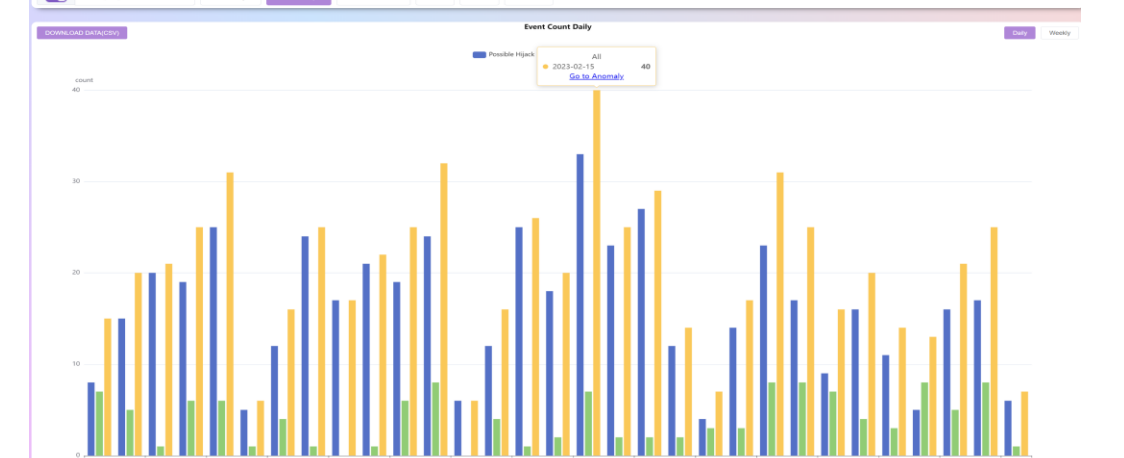
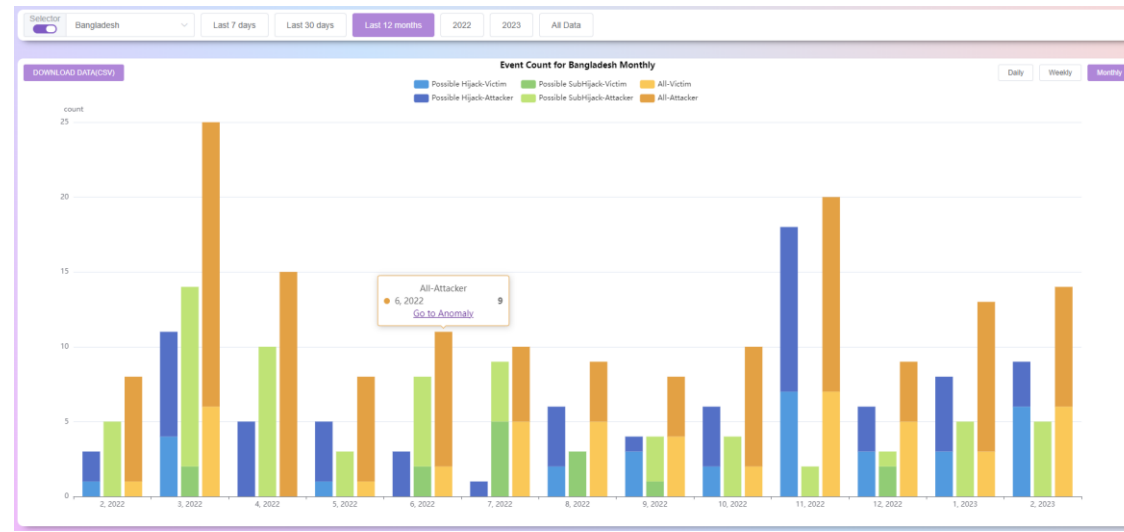
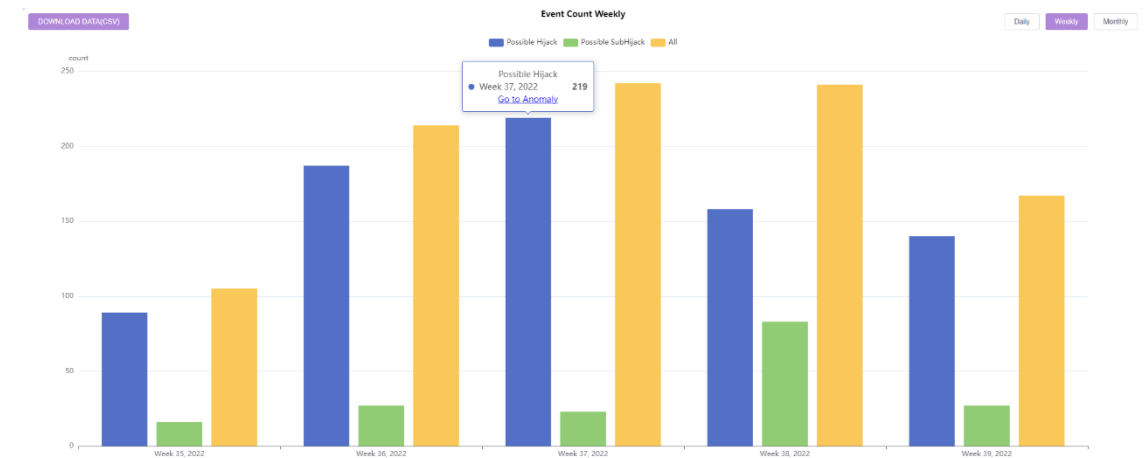
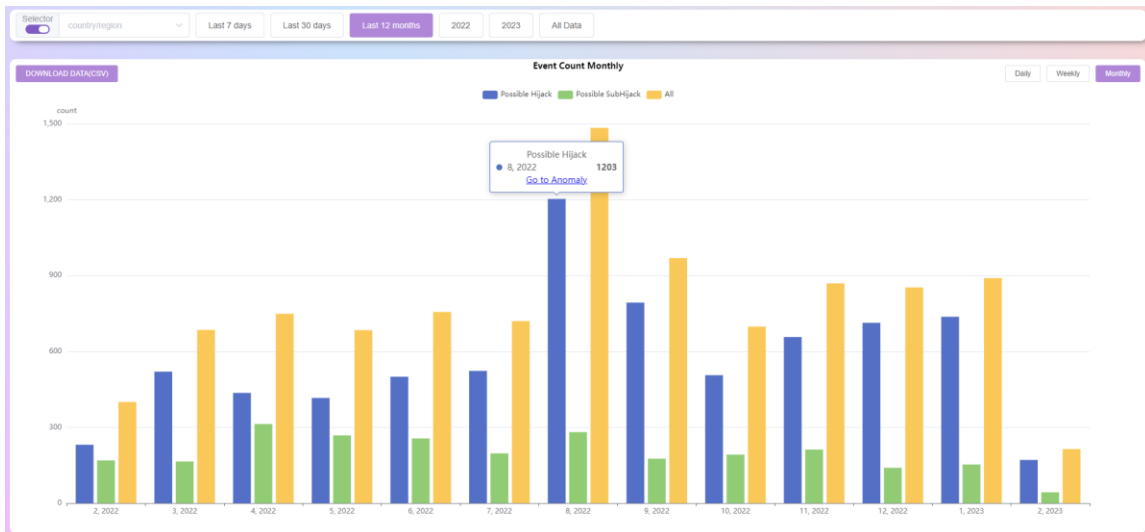
	Event Type	Level	Event Info	Prefix Num	Prefix	Start Time	End Time	Duration	Detail
1	Ongoing Possible Hijack	low	Victim:TR/AS204843 (TR-STERLY) Attacker:US/AS397373(H4Y-TECHNOLOGIES)	1	206.206.119.0/24	2023-03-11 11:28:28	-	-	detail
2	Possible SubHijack	low	Victim:VN/AS45903 (CMCTELECOM-AS-VN) Attacker:HK/AS45474(NEXUSGUARD-AS-AP)	1	prefix: 144.48.27.0/24 subprefix: 144.48.27.132/32	2023-03-11 10:34:50	2023-03-11 11:34:55	1:0:5	detail

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



Overview--Statistics for Anomaly Events



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



DashBoard

4538



You can search by AS number, AS name, or organization name.

search

Last Update:2023-04-24

Basic

IPv4 Peers

IPv6 Peers

4538

AS NUM

China

Country/Region

ERX-CERNET-BKB

AS Name

China Education and Research
Network Center

AS Organization

input

All



103.28.121.0/24

result

Prefix

1

103.28.120.0/22

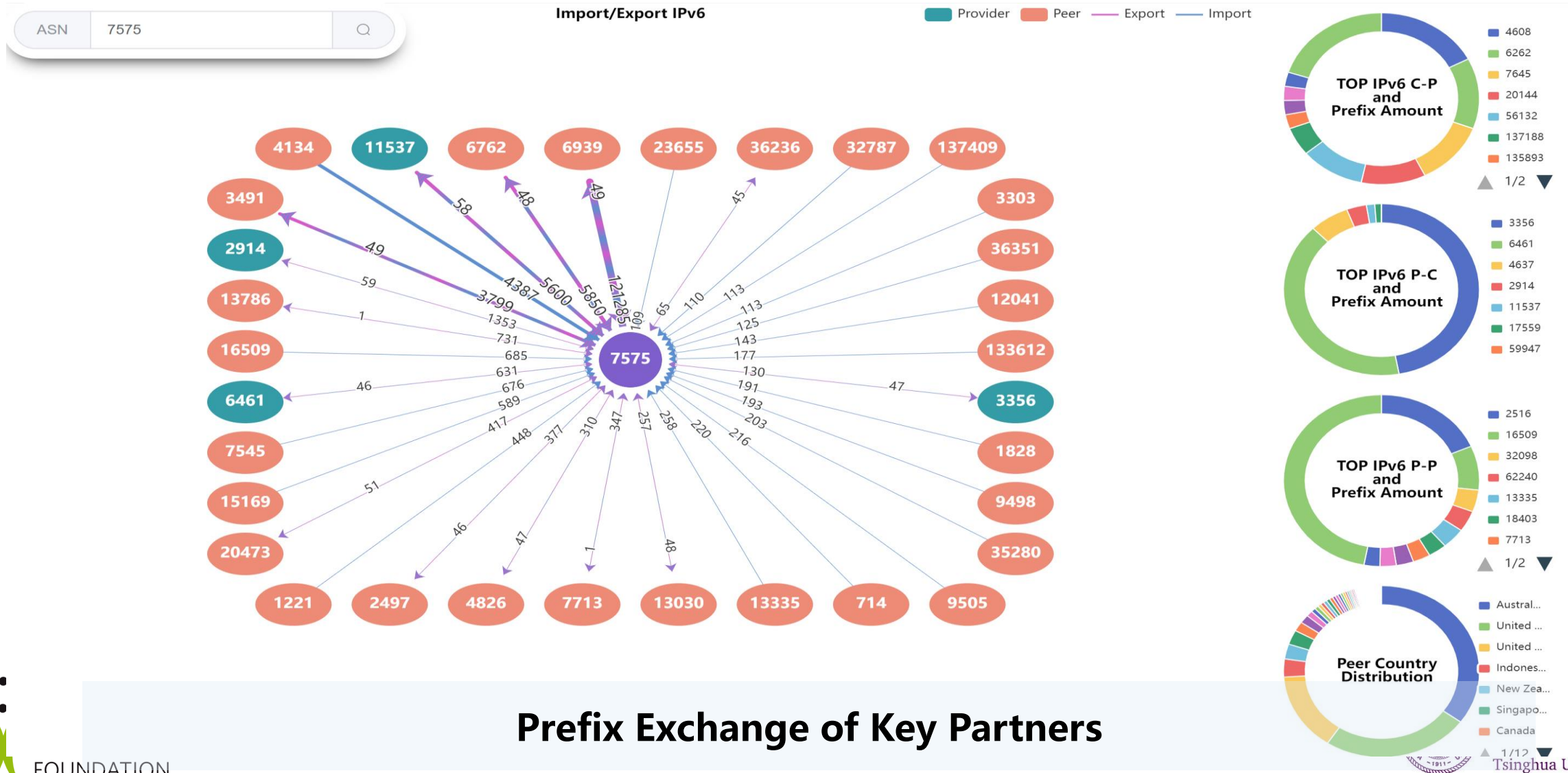


1

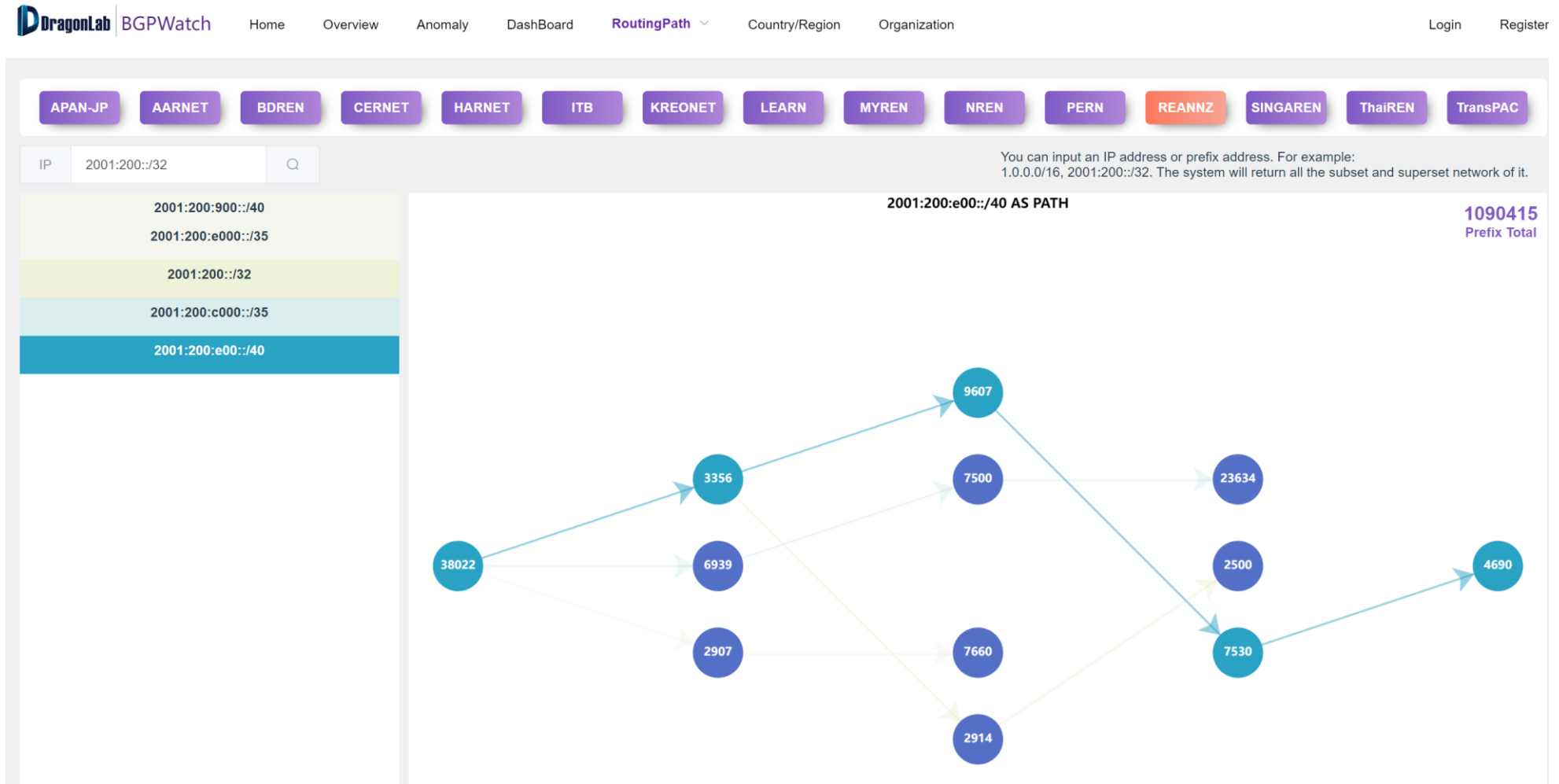


- Subnet and Super-Net of Prefix are searched

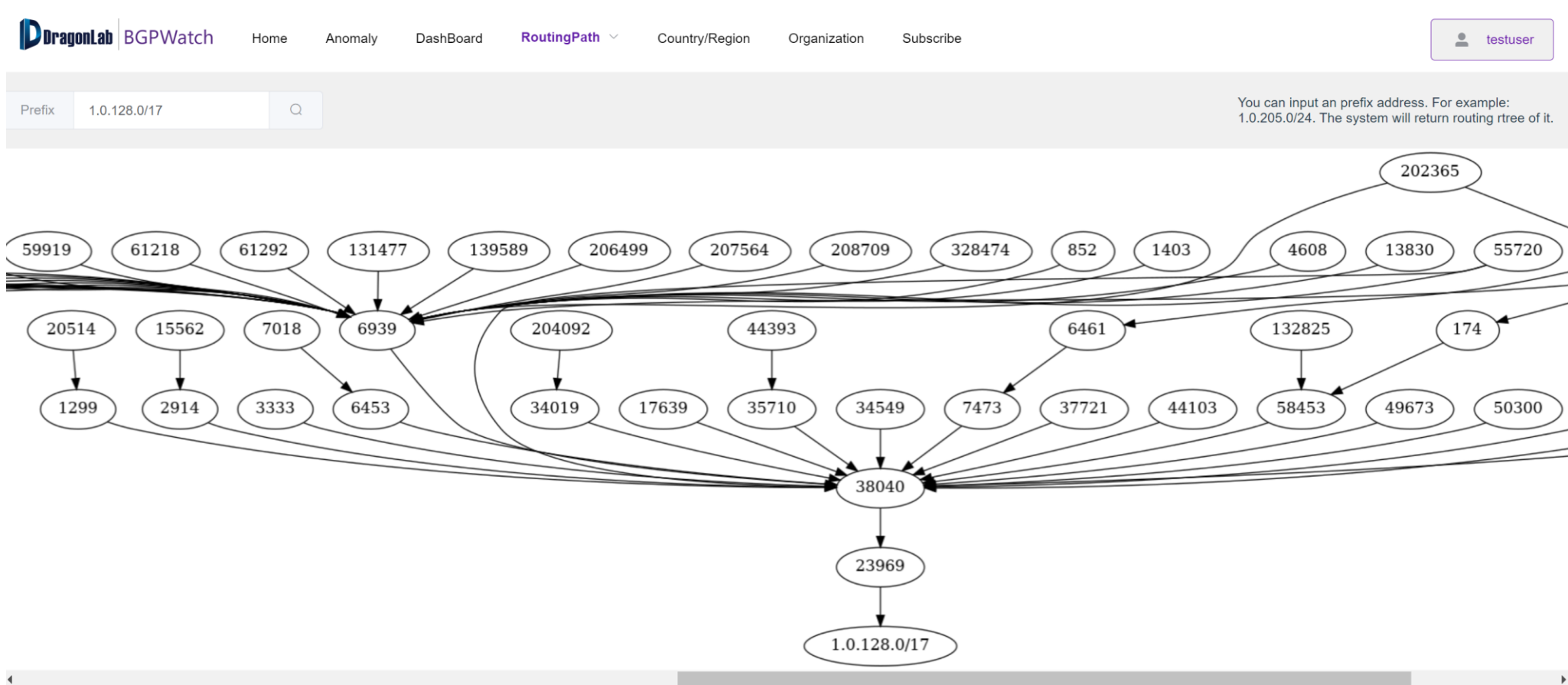
IPv4/IPv6 Key Peers Information



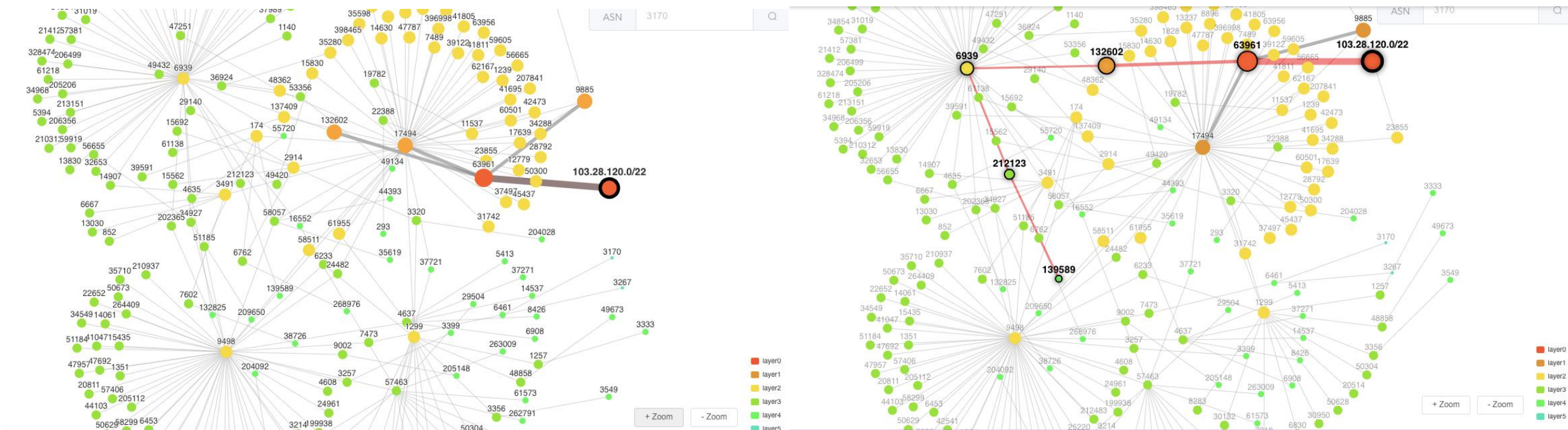
Routing Path Search



Reverse Routing Path

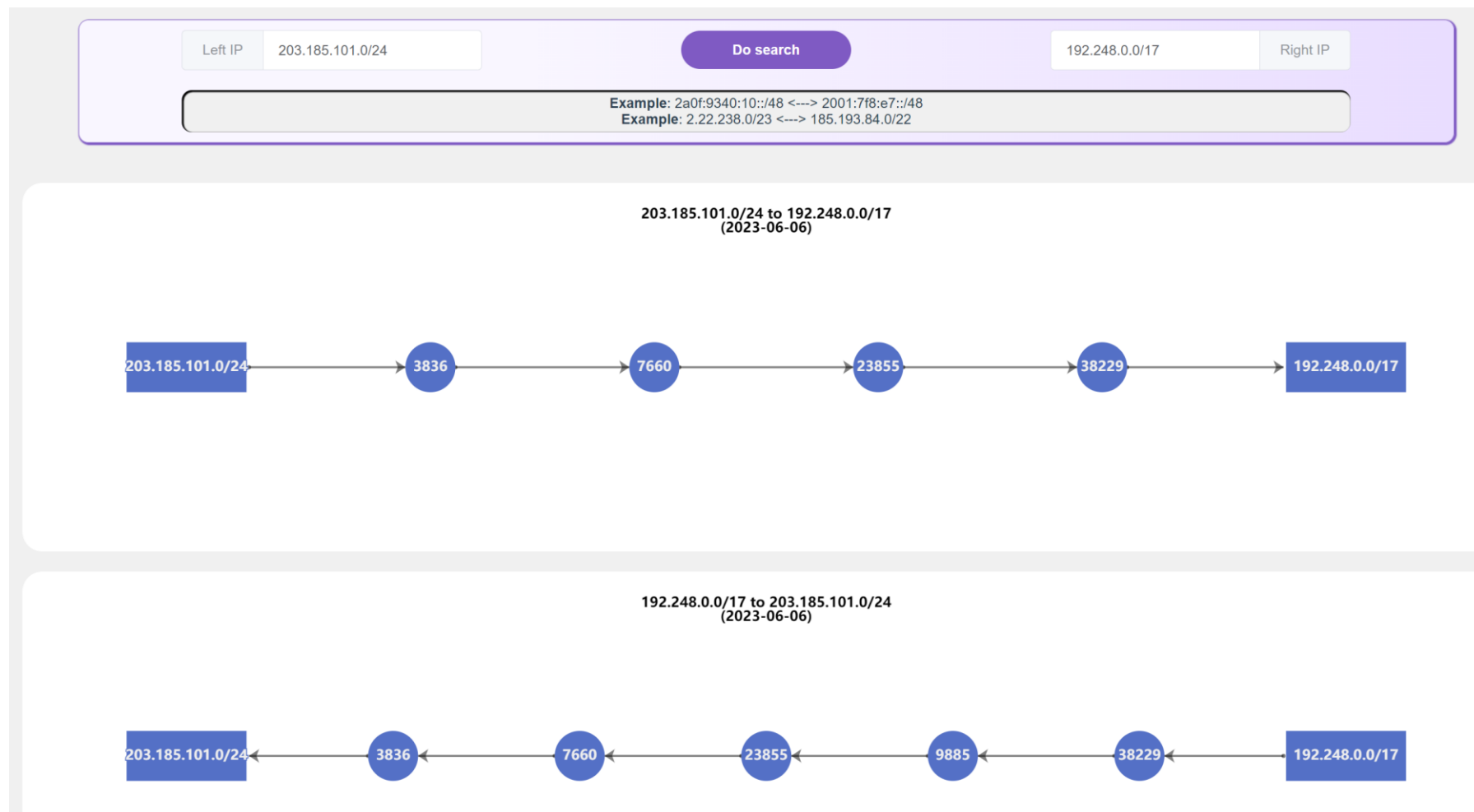


Reverse Routing Path (TOPO)



- 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

Bi-Routing Path



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

Subscribe and Send Alarm Email

ASN
4538

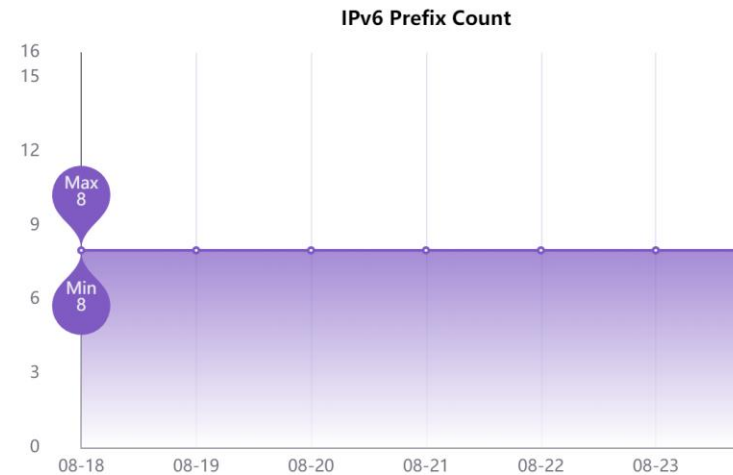
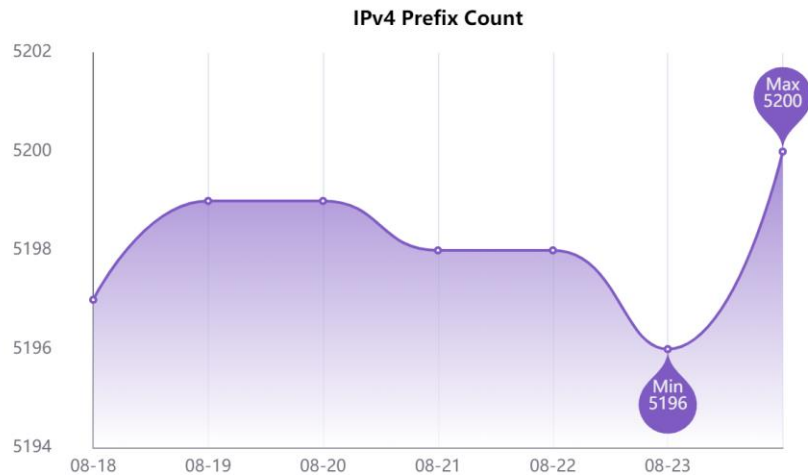
Country/Region
CN

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

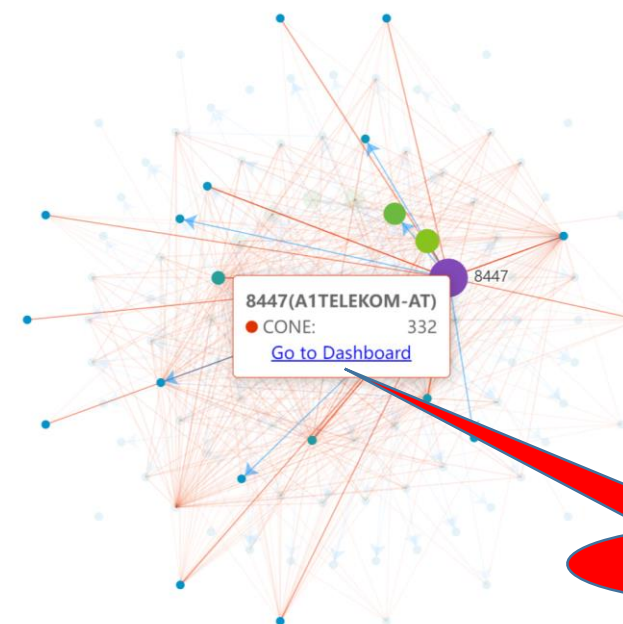
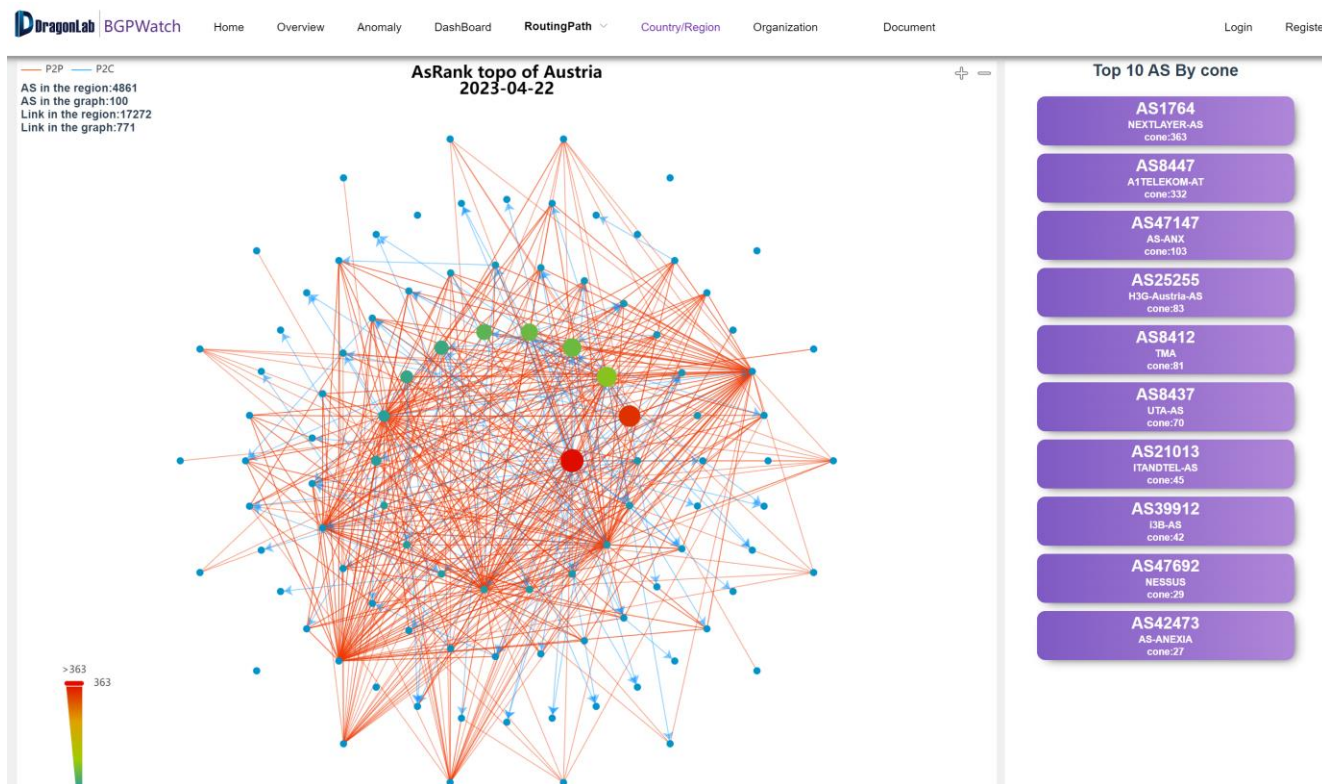
Announced prefixes changes between 2022-08-24 00:00:00 (GMT) and 2022-08-23 00:00:00 (GMT)

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

Topo of Country/Region

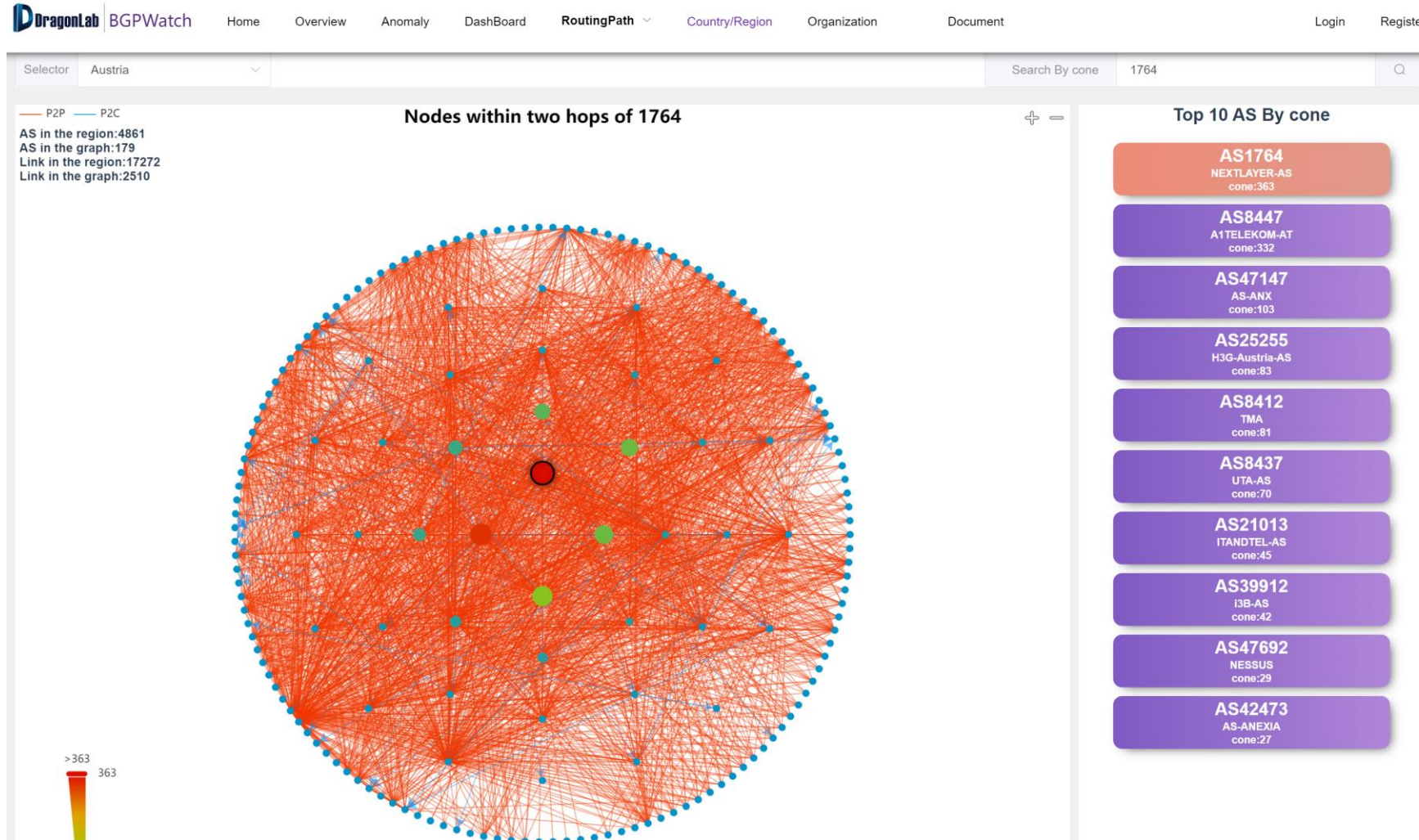


Link to
dashboard

Show TOP 10 AS

Link to Dashboard

Topo of Country/Region





JOIN US

- The RPKI Online Basic Knowledge Training
Time: 05:00-07:00(GMT) February 1, 2023
- The RPKI Online Hands-on Training
Time: 05:00-07:30(GMT) February 3, 2023

RPKI Training

APNIC ISIF Project  

www.bgper.net

The Online Training in February

RPKI Basic Knowledge

Date/Time	Length	Trainer/APNIC
1 st Feb. 2023 (Wednesday) 0500-0700 GMT	2 hours	Warren Finch(trainer), Awal Haolader(assistant)

RPKI Hands-on

3 rd 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

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

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

Manual and Video

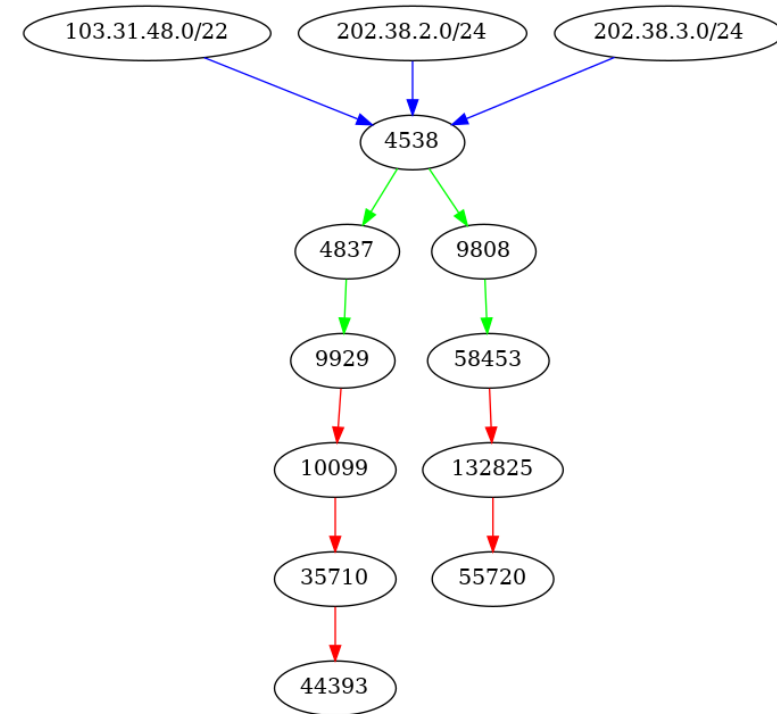
- [User Manual for BGPWatch](#)
- [User Manual for BGPWatch\(Video\)](#)
--Joint efforts of BdREN and Tsinghua University
- [CGTF BGP RIS Platform Manual](#)
- [CGTF Looking Glass Platform Manual](#)
- [Analysis of Suspected Hijacking Events in 2022](#)



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

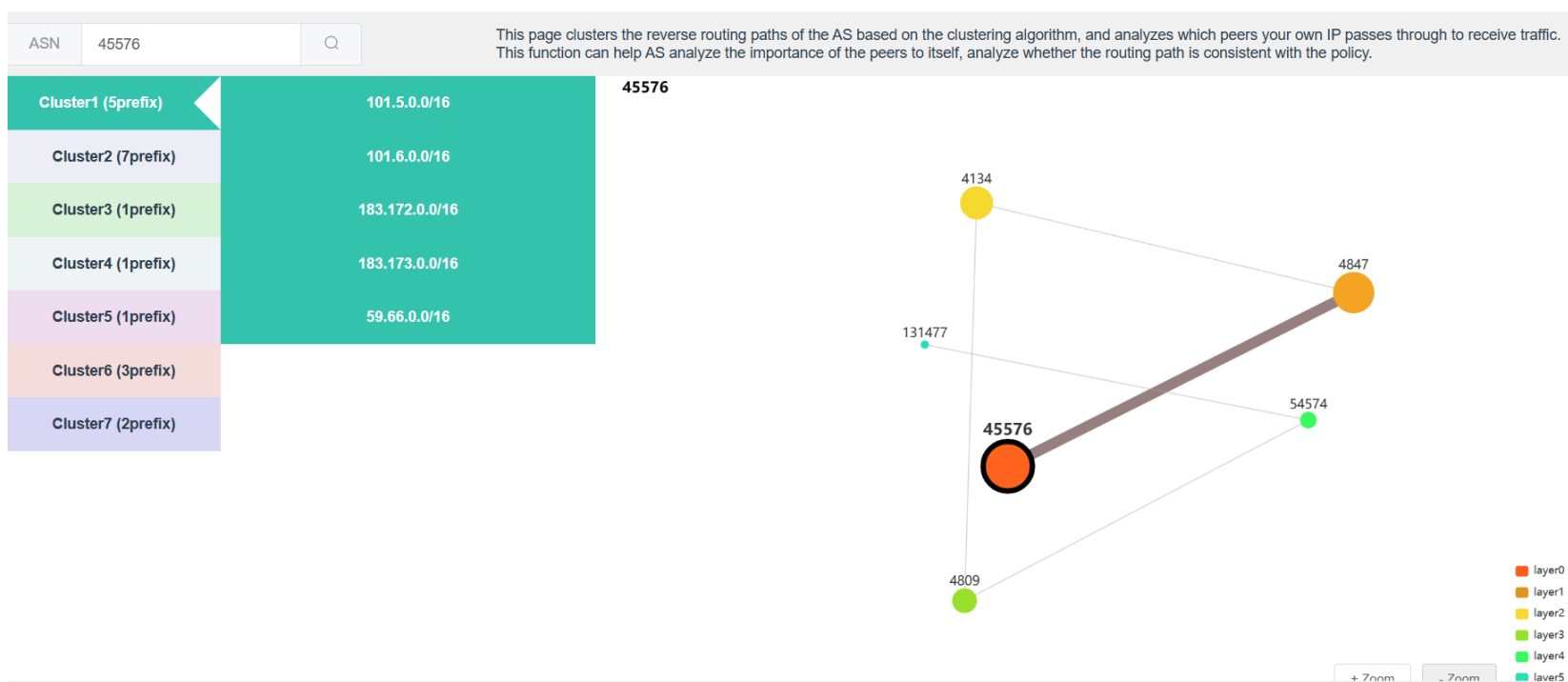
Research Work: Routing tree Clustering

- 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.



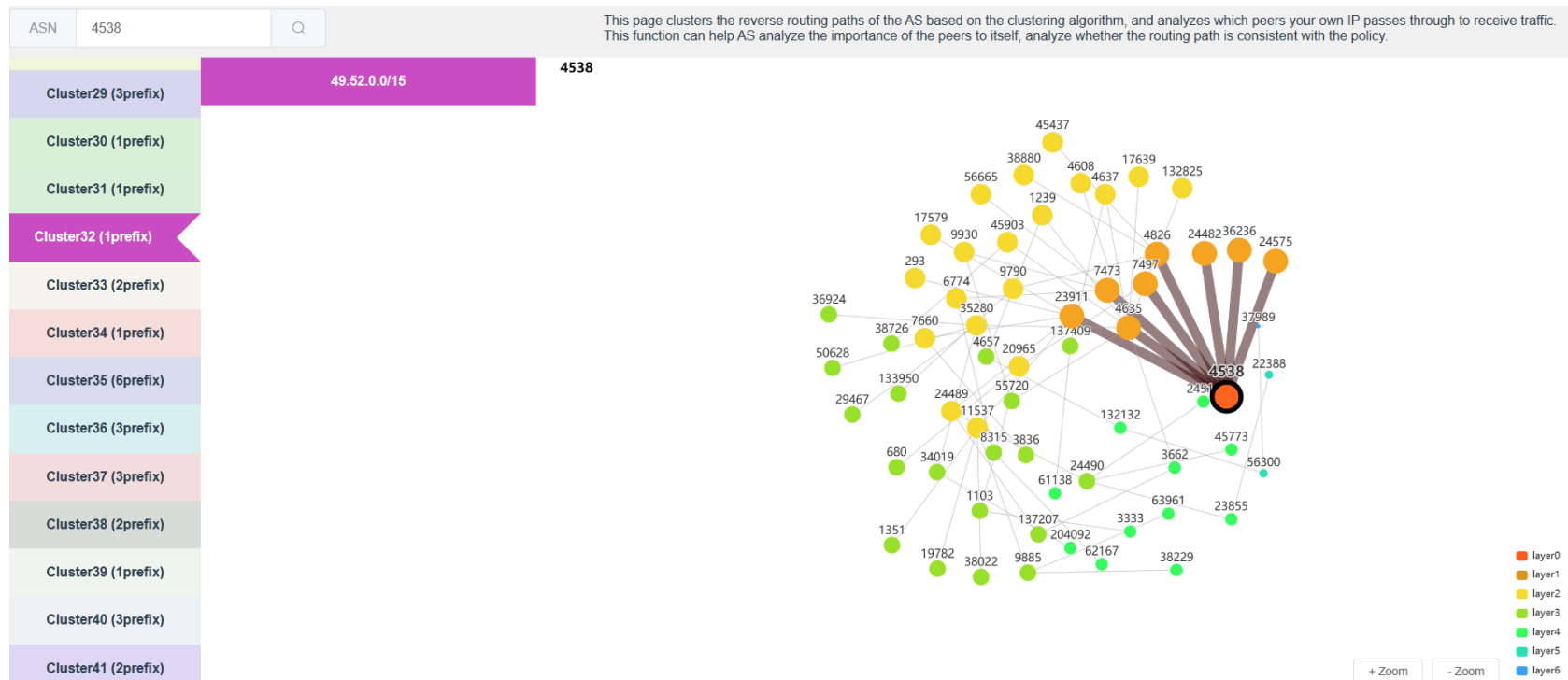
Application of Routing tree clustering

- 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.

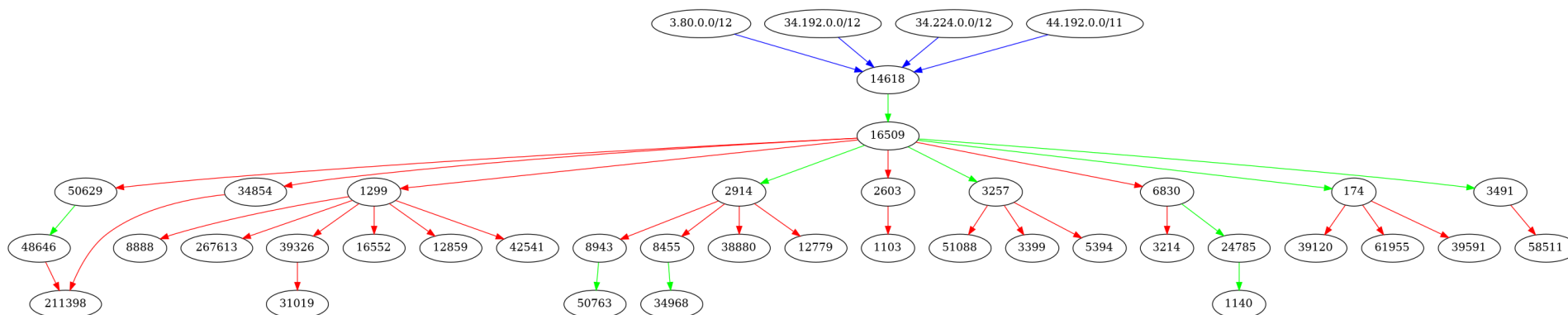


Application of Routing Tree Clustering

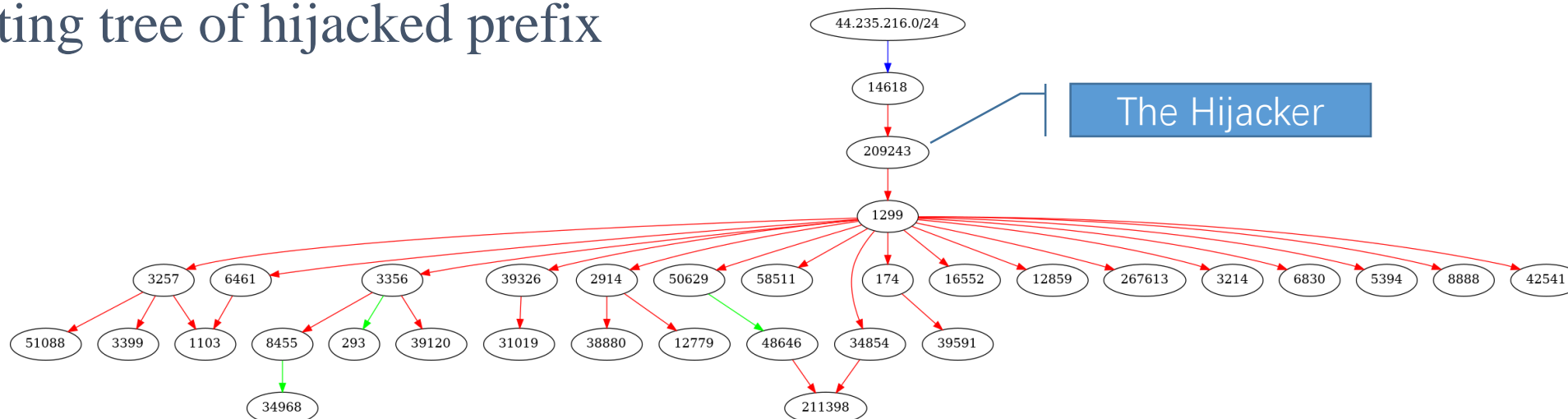
- Anomaly detection or Event review
 - Prefix hijacking or link failure, etc. can cause changes in clustering results, which can be used to detect anomalies.
 - For example, On August 17, 2022, 44.235.216.0/24 (belong to Amazon) was maliciously hijacked by attacker AS209243.
 - The results of clustering 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

Comments and Suggestions?

Contact us at: sec@cgtf.net
