The Report of the Technical Committee
- APNIC ISIF Project

24 August, 2023

APNIC FOUNDATION

Tsinghua University

APAN56 Colombo Sri Lanka 21- 25 August, 2023

Collaborative Community

- **Work of 19 Team members (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)

APNIC FOUNDATION

清華大學 Tsinghua University

Outline

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

APNIC FOUNDATION

Background

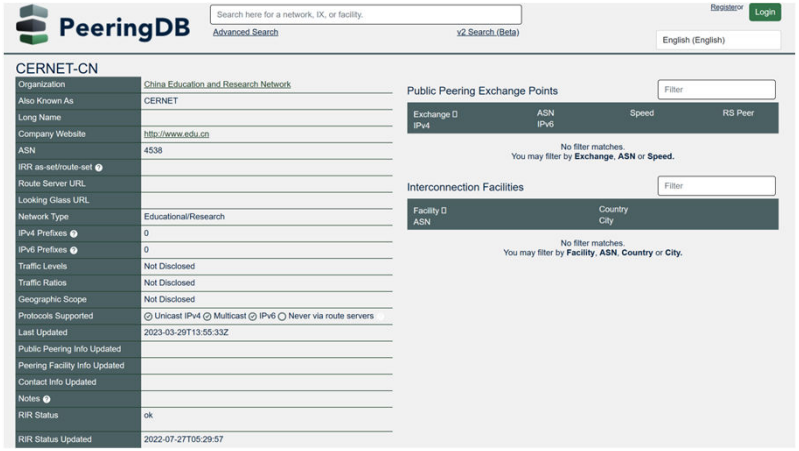
Data Collecting	Data Mining	Application
✓ Registration: WHOIS, RIR, PeeringDB, Radb, ROA ✓ Looking Glass ✓ Routing information ✓ Active Probing ✓ Passive measurement	✓ Statistics ✓ Machine learning ✓ Deep learning	✓ Hijacking, leaking, outage detection ✓ Inter-domain topology discovery ✓ Monitoring peering and path changing ✓ Performance monitoring ✓ Link-level congestion detection ✓ Cyber-attack detection

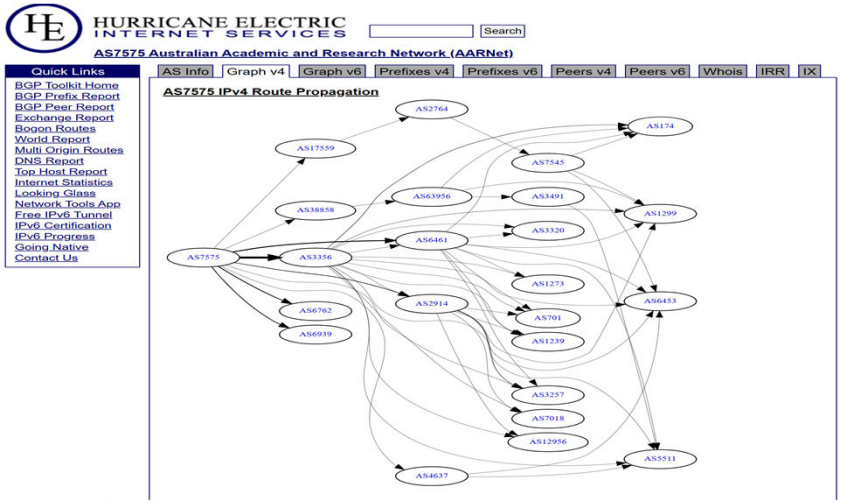
Objectives: Improve internet security, availability and provide tools for operators

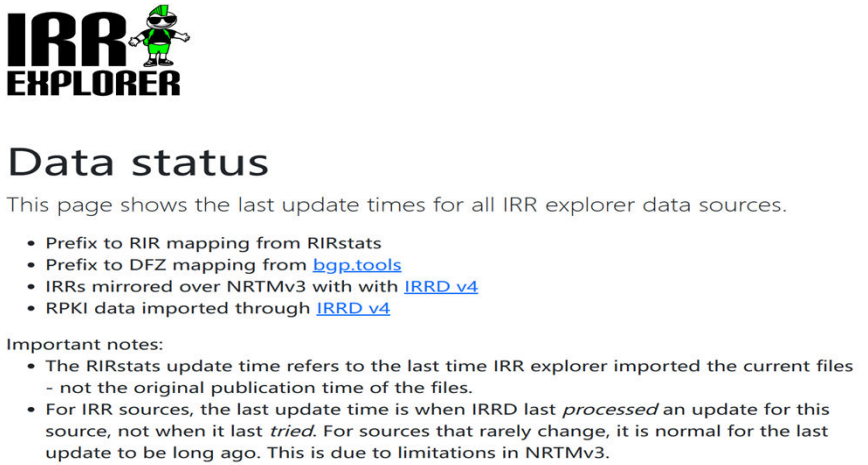
APNIC FOUNDATION

清華大學 Tsinghua University

Registration Data







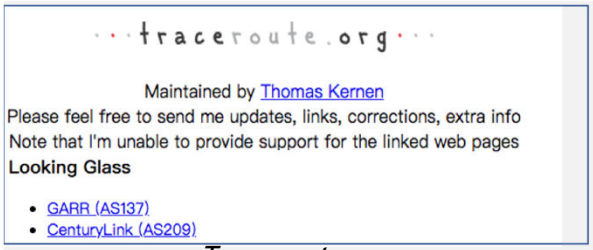
APNIC FOUNDATION

Tsinghua University

Looking Glass VPs

Researchers usually find and use LG pages from several well-known portal pages

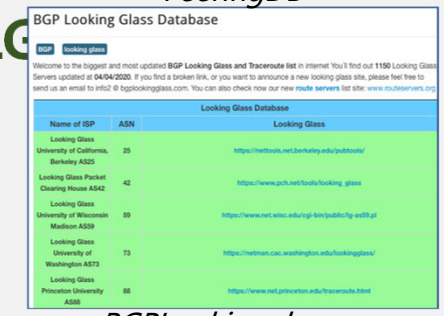
Many other available LG pages cannot be found and exploited easily !



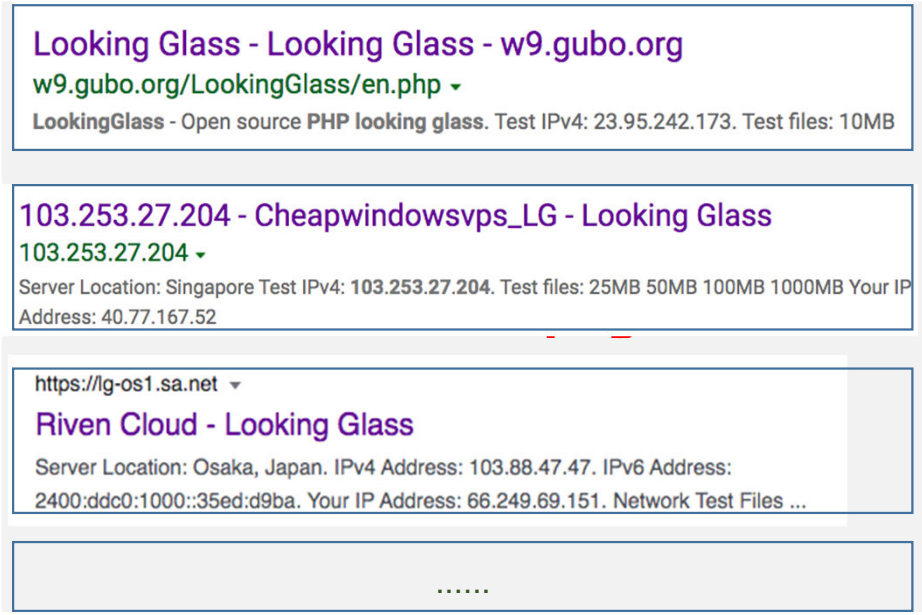
Traceroute.org

PeeringDB

BGP4.as



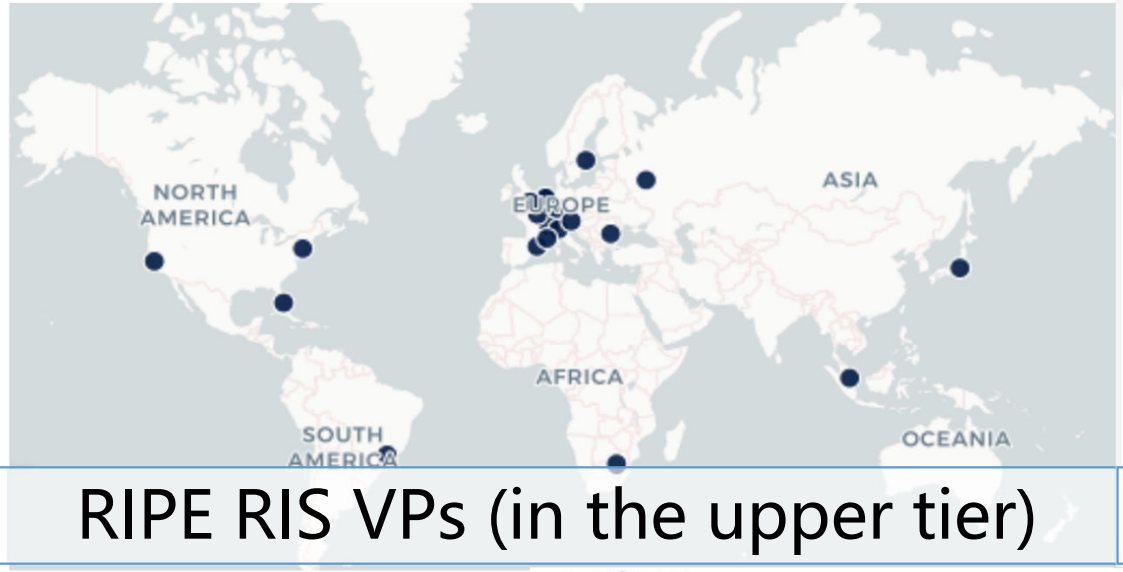
BGPLookingglass.com



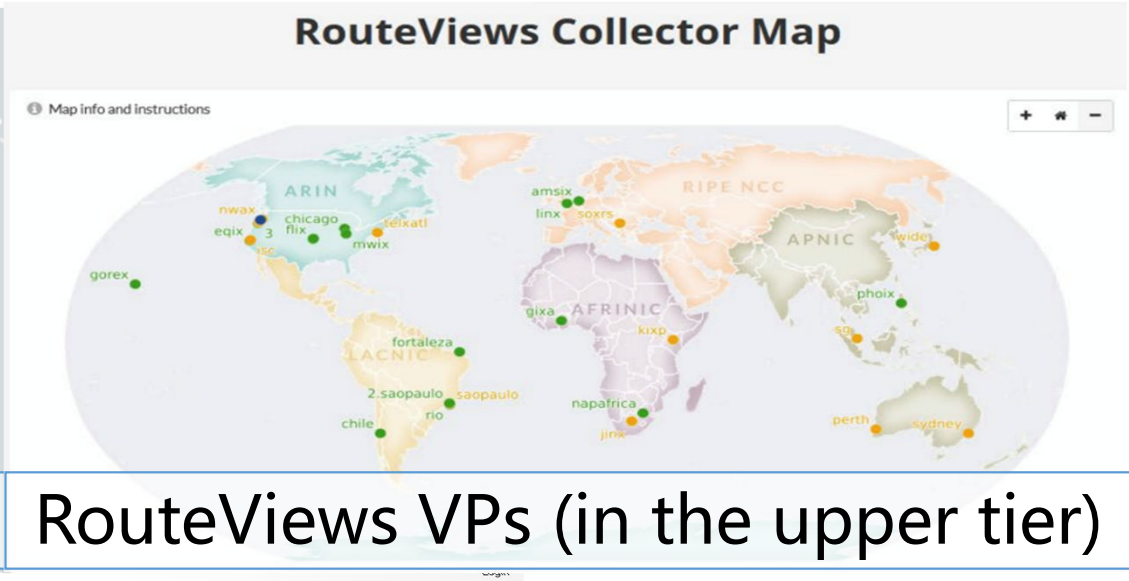
APNIC FOUNDATION

清華大學 Tsinghua University

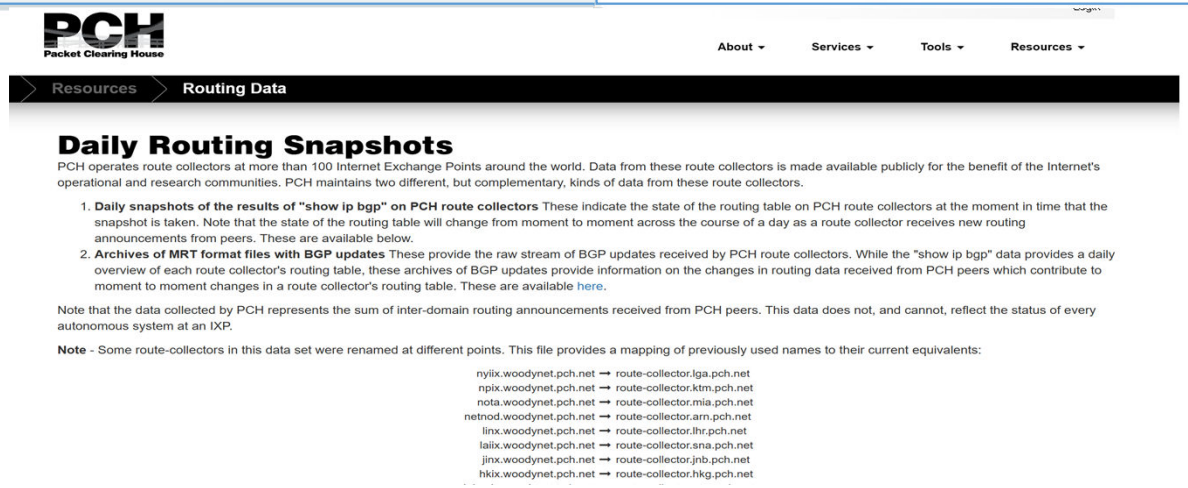
Routing Collection VPs



RIPE RIS VPs (in the upper tier)



RouteViews VPs (in the upper tier)



PCH Packet Clearing House

About ▾ Services ▾ Tools ▾ Resources ▾

Resources › Routing Data

Daily Routing Snapshots

PCH operates route collectors at more than 100 Internet Exchange Points around the world. Data from these route collectors is made available publicly for the benefit of the Internet's operational and research communities. PCH maintains two different, but complementary, kinds of data from these route collectors.

1. **Daily snapshots of the results of "show ip bgp" on PCH route collectors** These indicate the state of the routing table on PCH route collectors at the moment in time that the snapshot is taken. Note that the state of the routing table will change from moment to moment across the course of a day as a route collector receives new routing announcements from peers. These are available below.
2. **Archives of MRT format files with BGP updates** These provide the raw stream of BGP updates received by PCH route collectors. While the "show ip bgp" data provides a daily overview of each route collector's routing table, these archives of BGP updates provide information on the changes in routing data received from PCH peers which contribute to moment to moment changes in a route collector's routing table. These are available here.

Note that the data collected by PCH represents the sum of inter-domain routing announcements received from PCH peers. This data does not, and cannot, reflect the status of every autonomous system at an IXP.

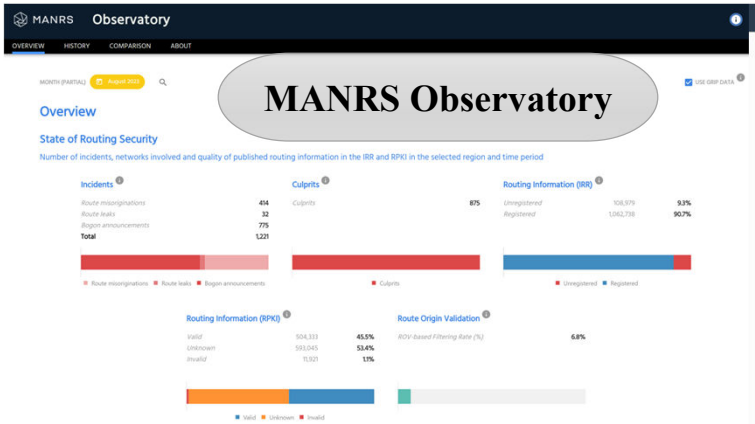
Note - Some route-collectors in this data set were renamed at different points. This file provides a mapping of previously used names to their current equivalents:

nyiix.woodynet.pch.net → route-collector.lga.pch.net
npix.woodynet.pch.net → route-collector.ktm.pch.net
nota.woodynet.pch.net → route-collector.mia.pch.net
netnod.woodynet.pch.net → route-collector.arn.pch.net
linx.woodynet.pch.net → route-collector.lhr.pch.net
laiix.woodynet.pch.net → route-collector.sna.pch.net
jinx.woodynet.pch.net → route-collector.jnb.pch.net
hkix.woodynet.pch.net → route-collector.hkg.pch.net

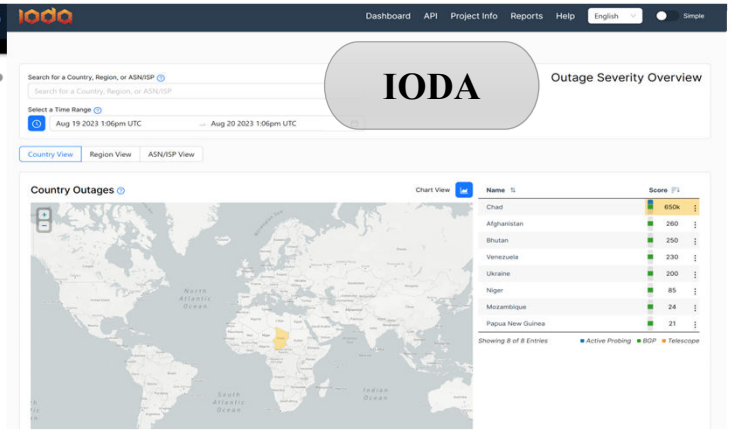
APNIC FOUNDATION

清華大學 Tsinghua University

Application Platforms



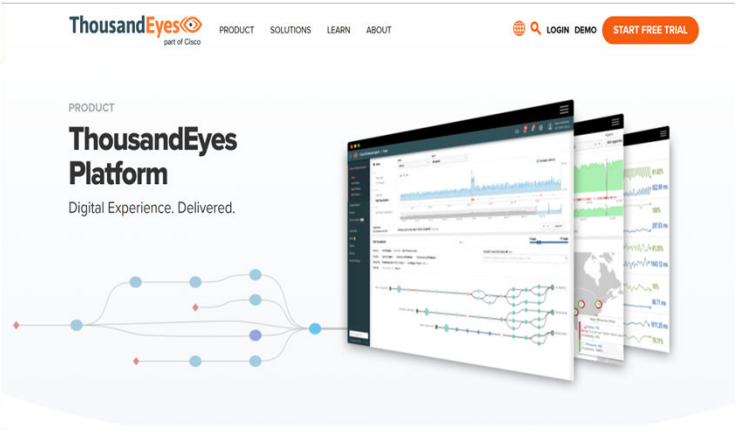
MANRS Observatory



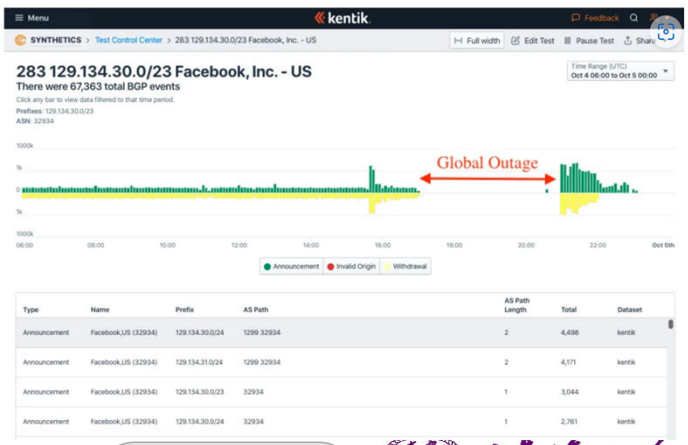
IODA

CISCO BGPSTREAM

CATCHPOINT



ThousandEyes

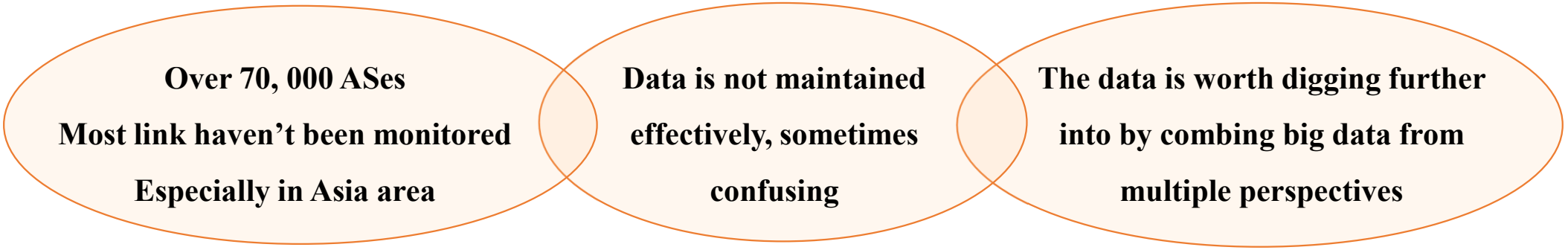


KENTIK

APNIC FOUNDATION

Tsinghua University

Is it enough?
What's the meaning of the project



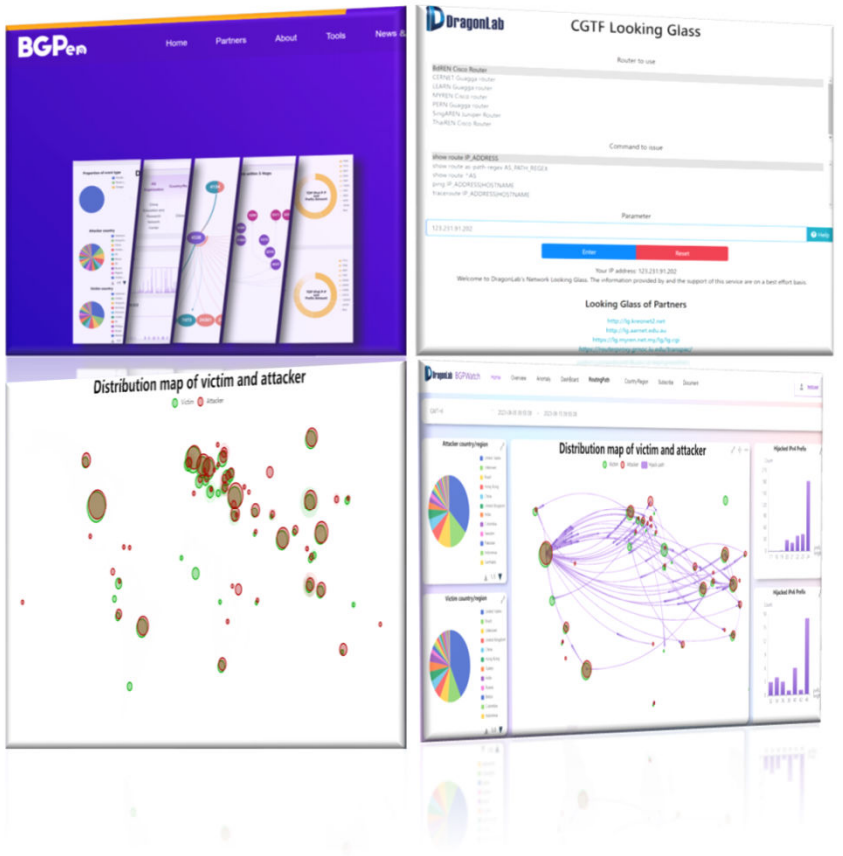
- **Hope to contribute to the community**
- **Hope do something from a different perspective**
- **Hope do something others haven't done**

APNIC FOUNDATION

清華大學 Tsinghua University

Objectives

- Looking Glass platform
- BGP routing sharing platform
- BGP hijacking detection
- BGP monitoring tools for operators



APNIC FOUNDATION

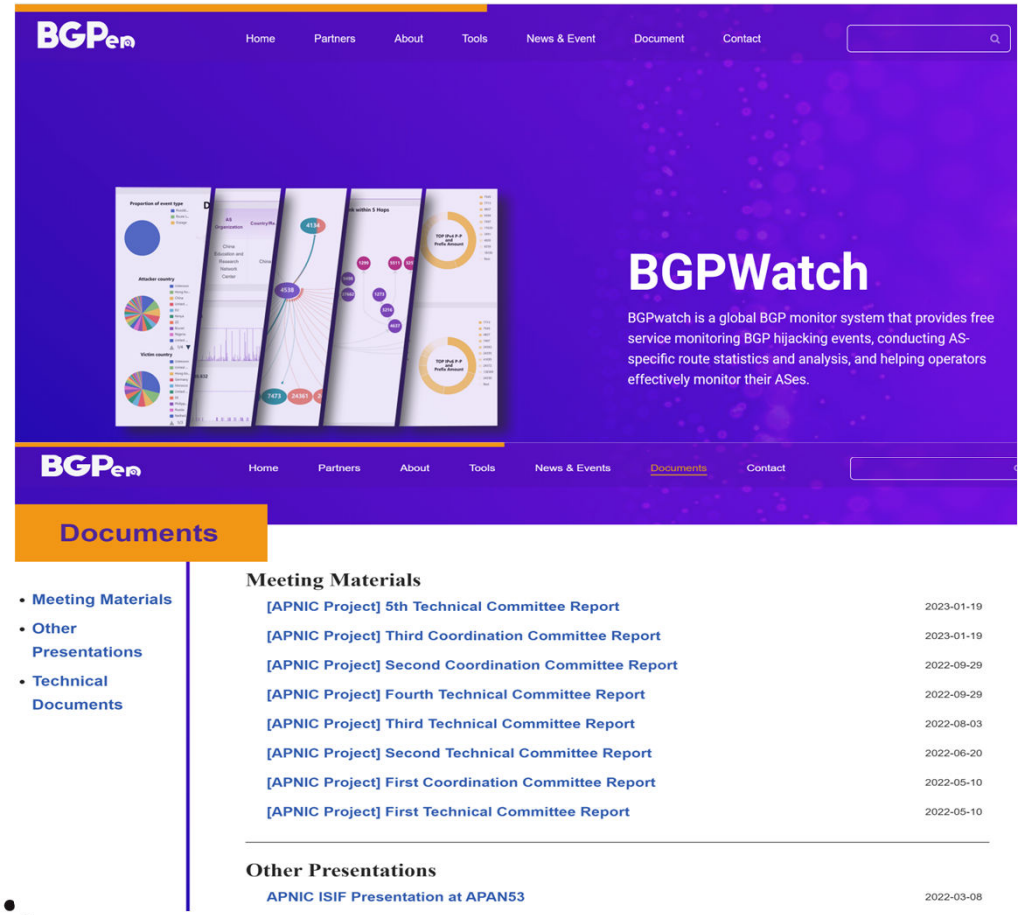
清華大學 Tsinghua University

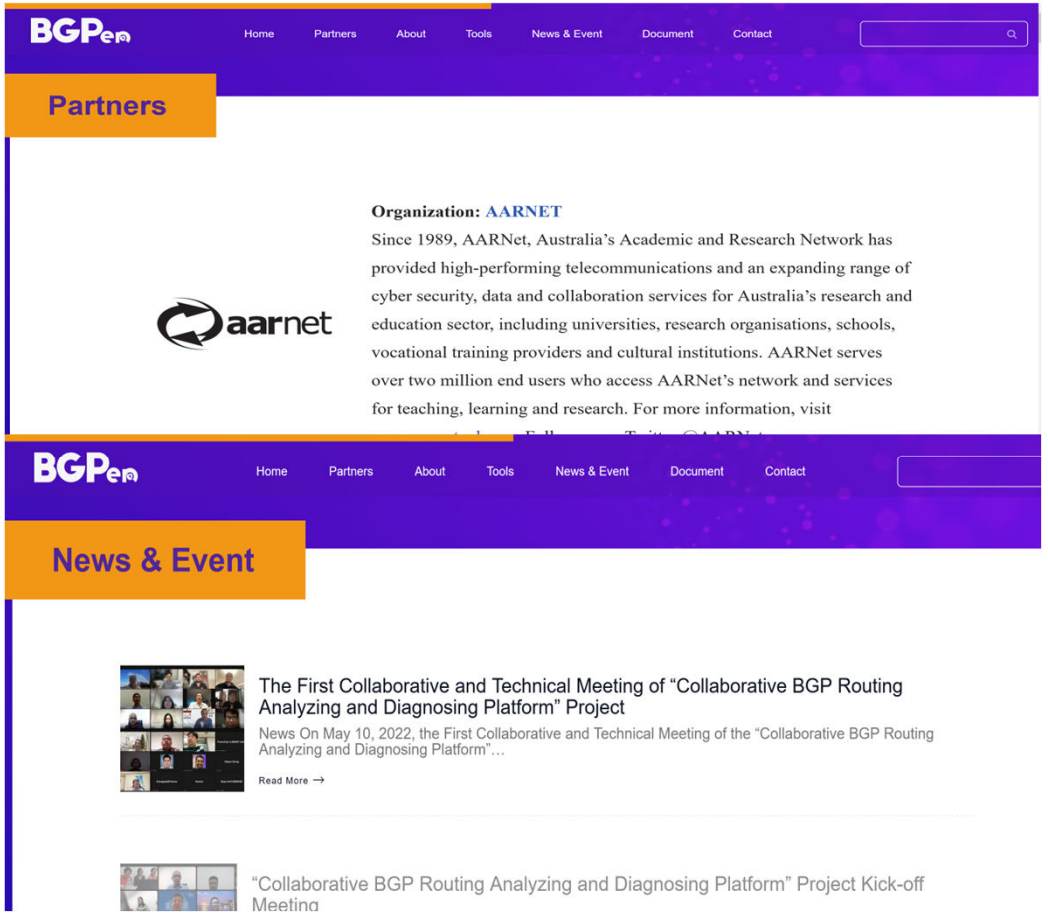
Activities

Objectives	Detail work	Status
Build a collaborative community for enhancing the capacity of NRENs' network operation and measurement	Setting up project website	Finished by May 2022
	Collaborative Work: Knowledge sharing, training, manual, video	Done
	Platform development and deployment	See below
Establish a distributed BGP routing monitoring platform and a looking glass platform in the Asia-Pacific region	BGP Routing Information Sharing	15 partners
	Looking Glass Platform	Connect with 7 partners, link to 4 partners
	Tools for operator(dashboard, routing path search, register and alarm email)	Done by August 2023
Deploy a BGP hijacking detection and mitigation system and analyze the robustness of routing in the Asia-Pacific region	Development of prefix hijacking detection	Done by August 2023
	Research Paper: region resilience	Done by May 2023
	Research Paper: routing hijacking detection	Done by June 2023
Share knowledge and experience globally	RPKI, MANRS, BGPSEC, DNSSEC	Done by May 2023
	paper, technical document	Nearly Done

Project Web Site

https://bgper.net





APNIC FOUNDATION

清華大學 Tsinghua University

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

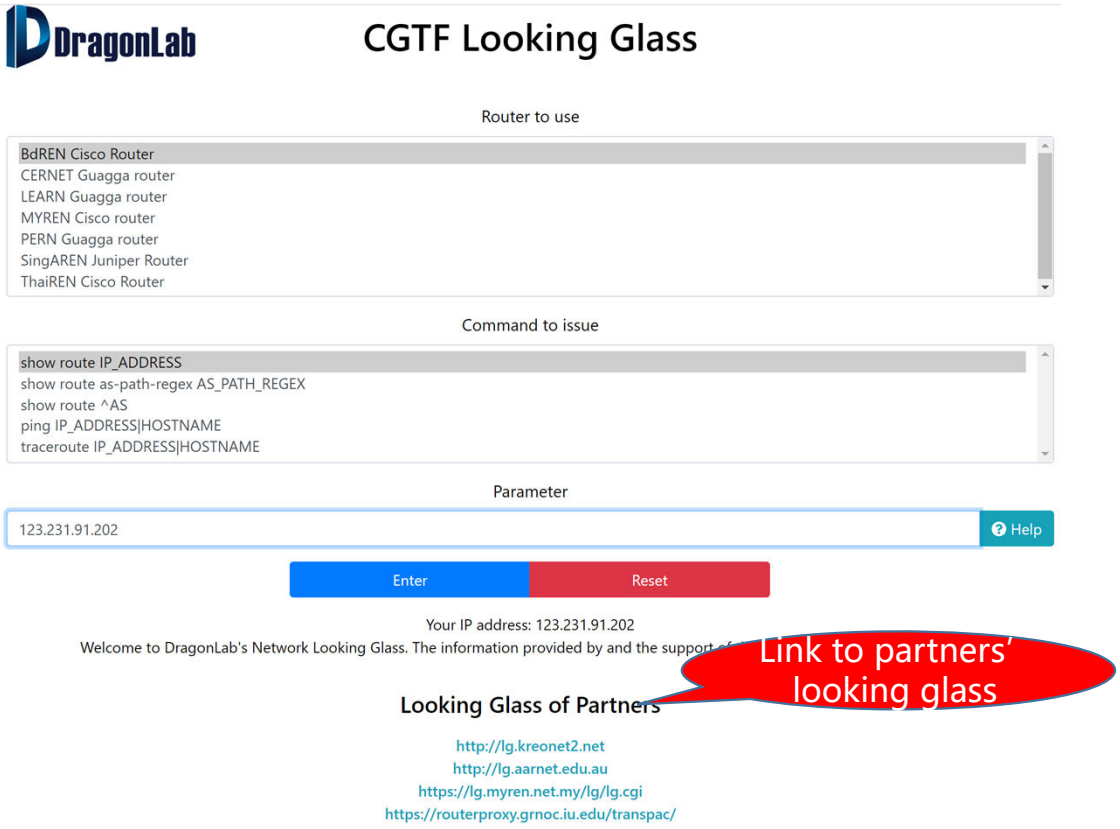
APNIC FOUNDATION

清華大學 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

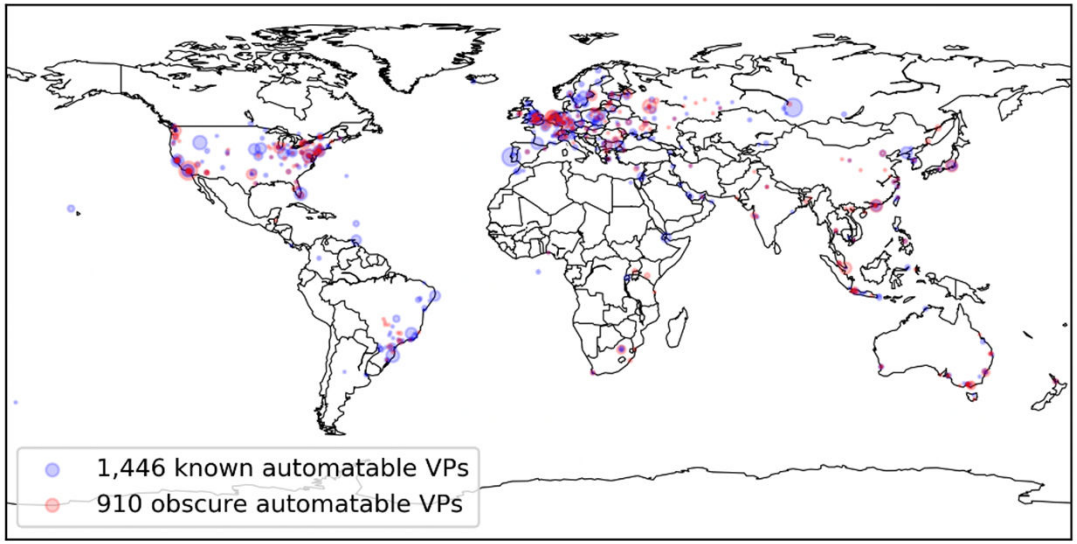
Add links to 4 partners' looking glass

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**

https://github.com/zhuangshuying18/discover_obscure_LG

Periscope has found several hundred VPs (364)

Use obscure LG VPs to improve the completeness of AS-level topology

Collect AS paths from LG VPs

RUB Looking Glass - show bgp ipv4 unicast neighbors 10.12.1.163 advertised-routes

Router: RUB Border Router 2
Command: show bgp ipv4 unicast neighbors 10.12.1.163 advertised-routes

```
BGP table version is 36248632, local router ID is 10.12.0.14
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
              t secondary path, L long-lived-stale,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  1.0.0.0/24       188.1.245.93             0    100      0 680 13335 i
 *>  1.0.4.0/24       188.1.245.93             0    100      0 680 6939 4826 38803 i
 *>  1.0.4.0/22       188.1.245.93             0    100      0 680 6939 4826 38803 i
 *>  1.0.5.0/24       188.1.245.93             0    100      0 680 6939 4826 38803 i
```

Automatically collect AS paths from 14 known LG VPs and **8 obscure VPs**

Improve AS-level topology completeness

		Known LG VPs	Obscure LG VPs	RIPE RIS	RouteViews	ALL
ASes	Observed	44,955	44,355	44,952	**45,339**	**45,635**
	Exclusive	247	10	12	271	-
AS links	Observed	100,356	76,907	154,828	204,889	253,719
	Exclusive	8,318	1,428	37,383	85,450	-

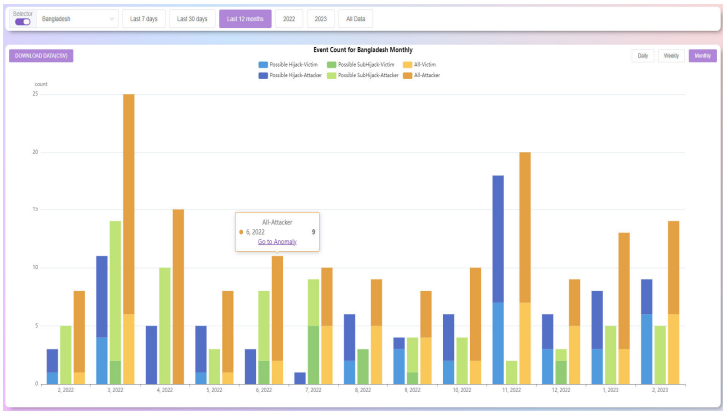
Table 6: The number of observed and exclusive ASes, AS links extracted from each dataset.

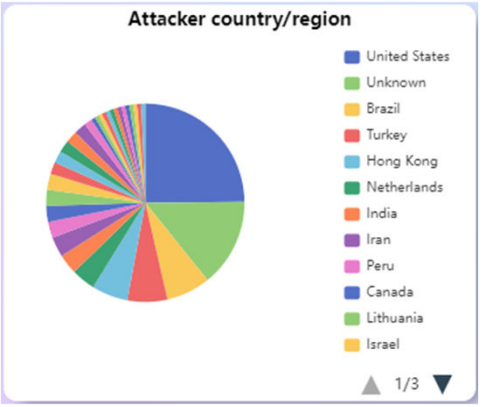
Compare with AS topologies collected from known LG VPs, RIPE RIS and RouteViews

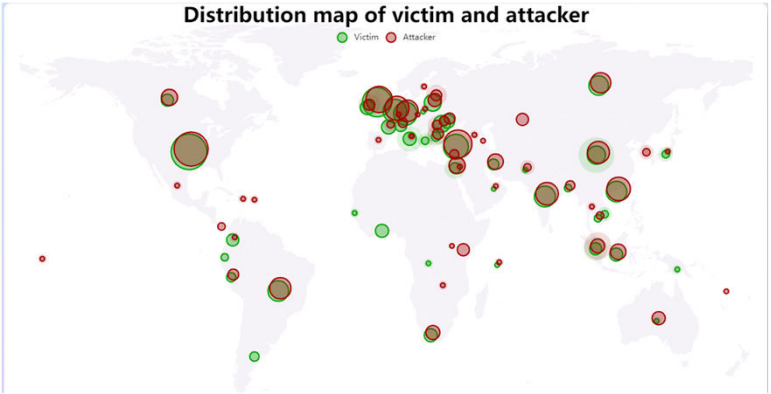
10 new ASes, and 1428 new links

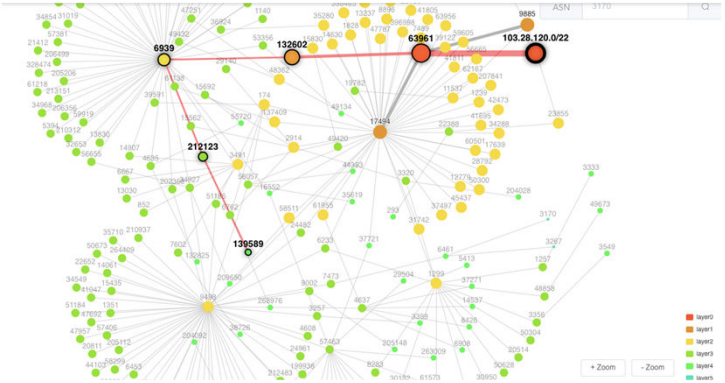
BGP Routing Monitoring and Analysis: BGPWatch

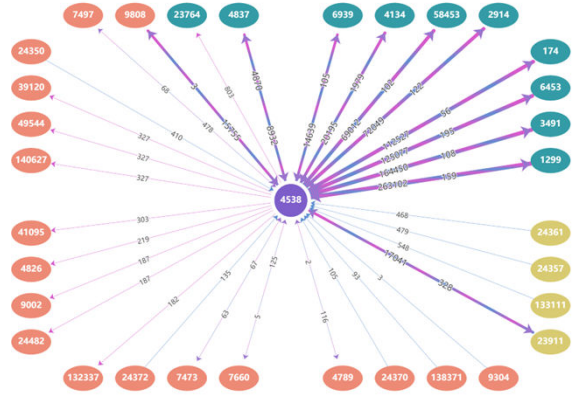
- Hijacking Detection
- Hijacking Statistics
- Dashboard: AS info, prefix, peers
- Routing Search：
  - forward, reverse, bi-direction
- Subscribe, Alarming







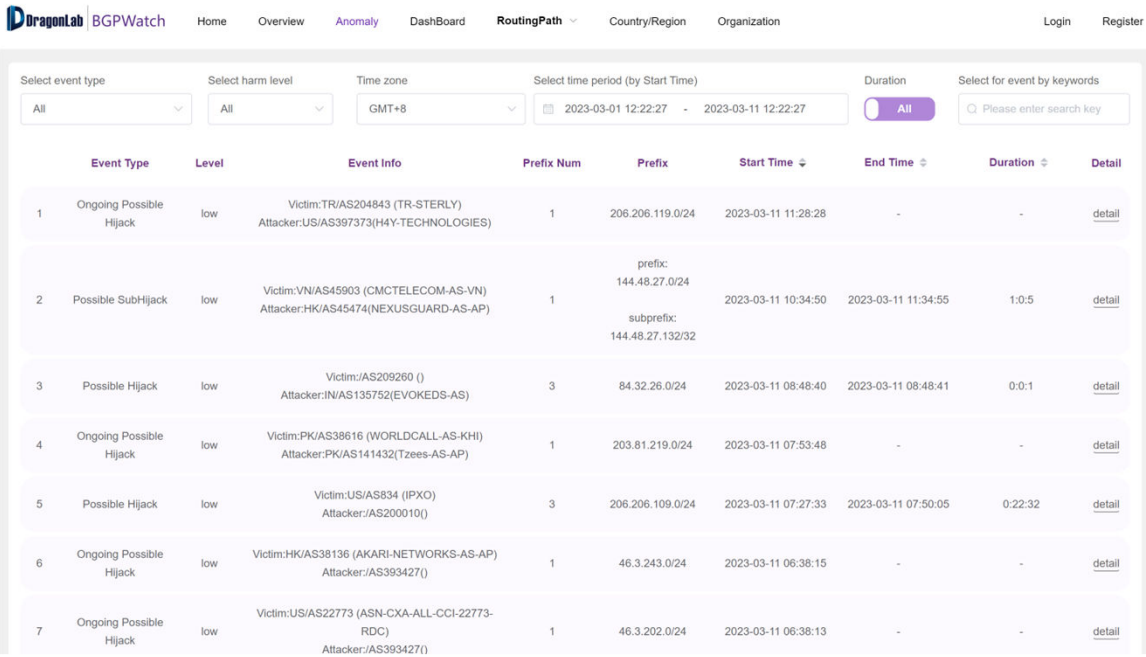




https://bgpwatch.cgtf.net

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)



APNIC FOUNDATION

https://bgpwatch.cgtf.net

清華大學 Tsinghua University

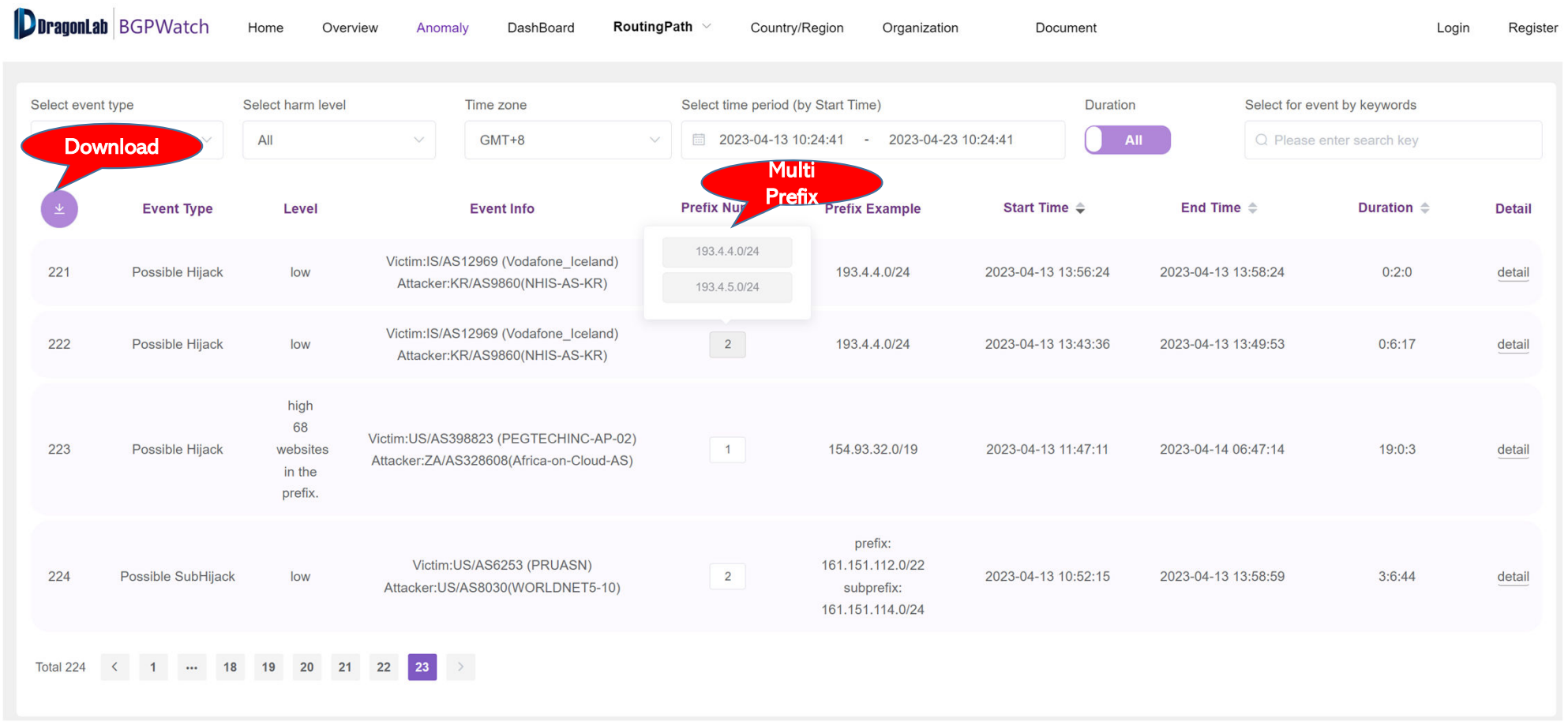
BGP Routing Monitoring and Analysis: BGPWatch

Home Page Statistic Info

APNIC FOUNDATION

清華大學 Tsinghua University

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

45.58.36.0/23-hijack1692553572 Ongoing Possible Hijack Events

Victim AS: 13768

Victim Country: CA (Canada)

Victim Description: COGECO-PEER1

Normal Prefix: 45.58.36.0/23

Start Time: 2023-08-20 17:46:12

During Time: no data

Hijacker AS: 6364

Hijacker Country: US (United States)

Hijacker Description: ATLANTIC-NET-1

End Time: -

Time Zone: UTC

Website:

easteuropeanbrides.com | theloop21.com | dnscalifornia.net | bigonsports.com | riversideclinictrail.ca | trackword.net | mqisolutions.net

swarovski-crystal.co | royaltytheme.com | thestreethockeyshop.com | renewablelogic.com.au | gamefocus.ca | essay-writer.ca | jimcrowhistory.org

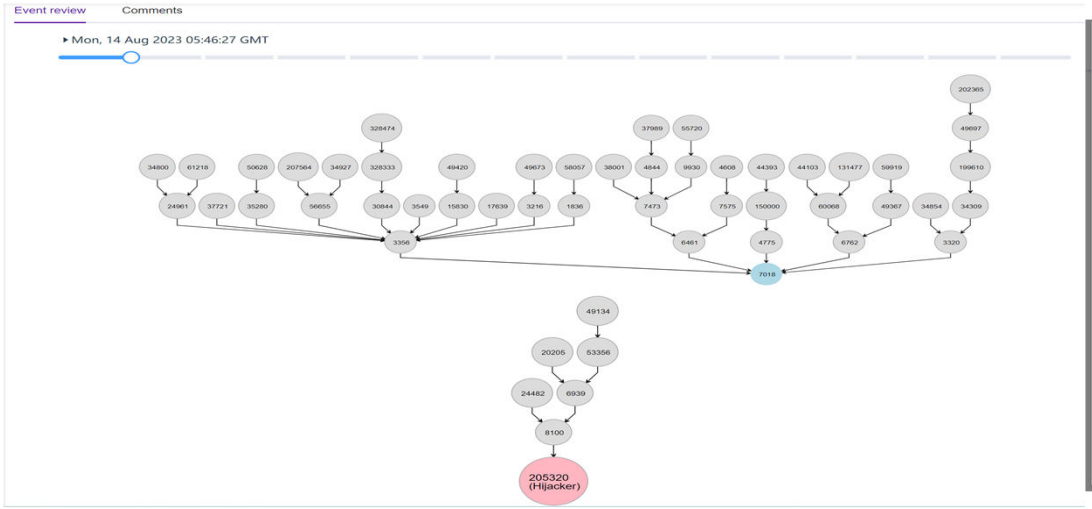
formalium.com | sstenligne.com | tobyspeople.com | the-northface.com.co | benitezmodernconstruction.com | triofertility.com

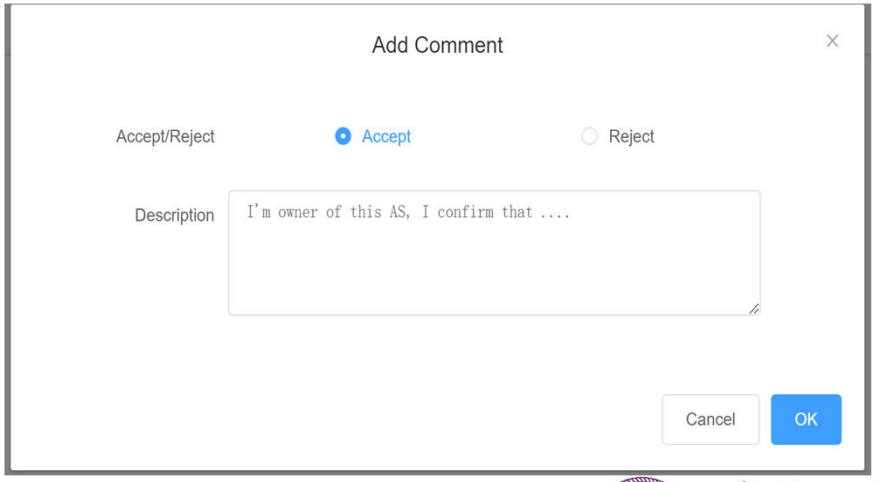
APNIC FOUNDATION

清華大學 Tsinghua University

Features --- Quick Response, Event replay, Comments

- 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

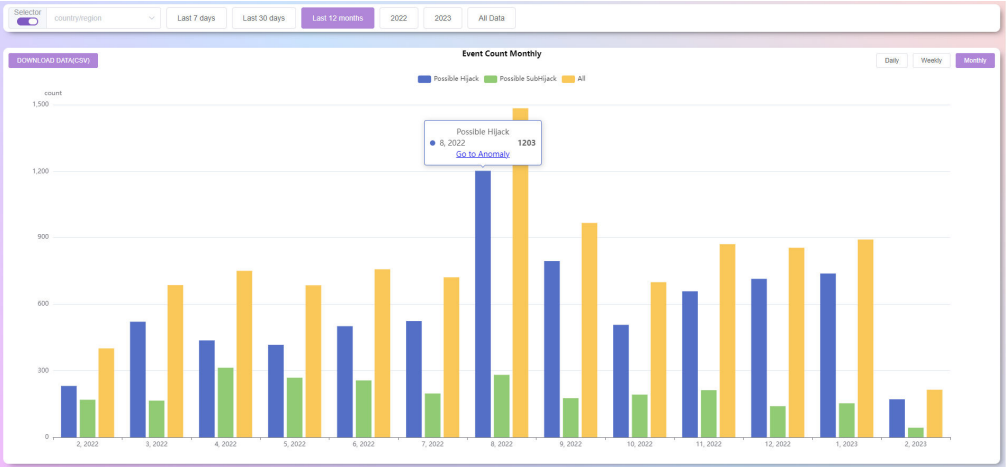


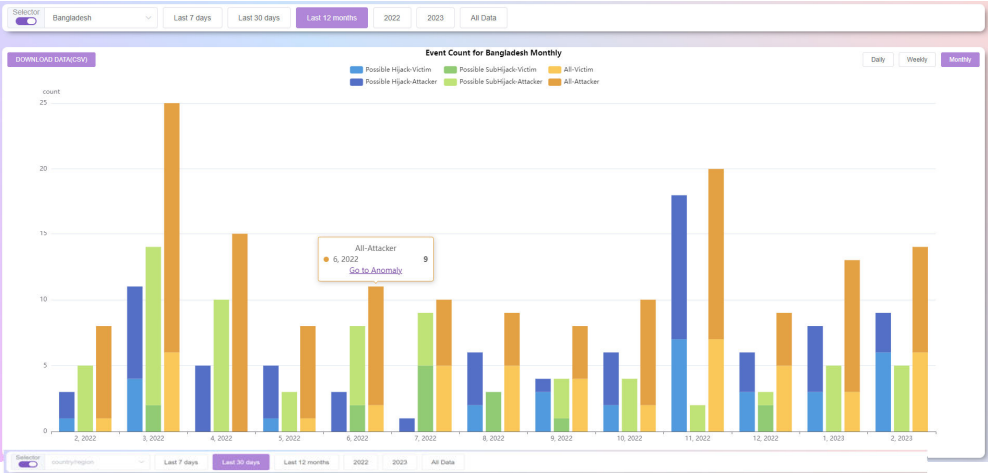


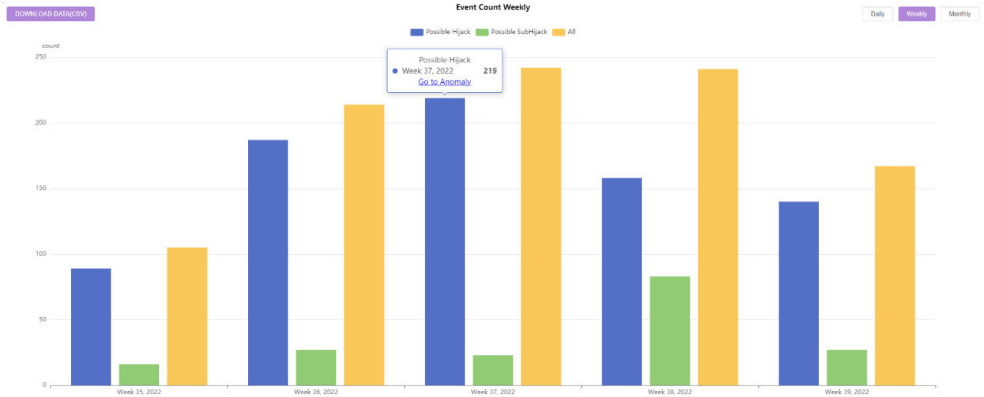
APNIC FOUNDATION

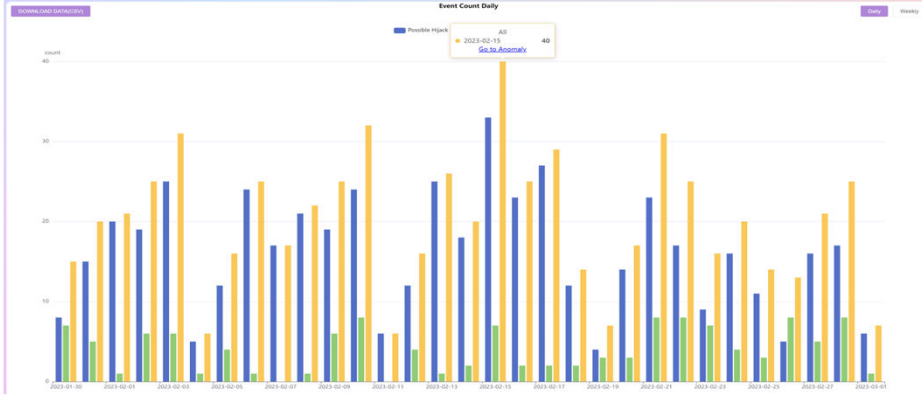
Tsinghua University

Overview--Statistics for Anomaly Events







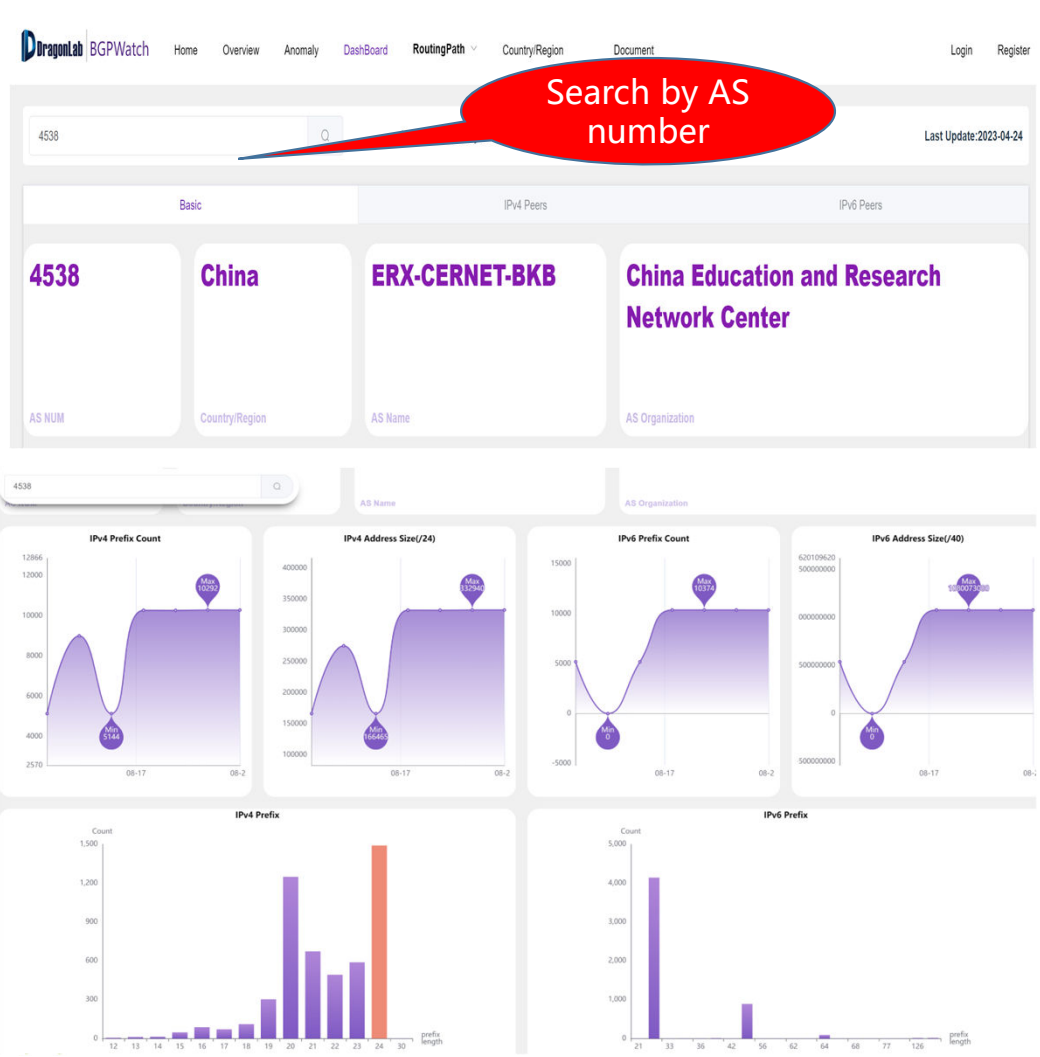


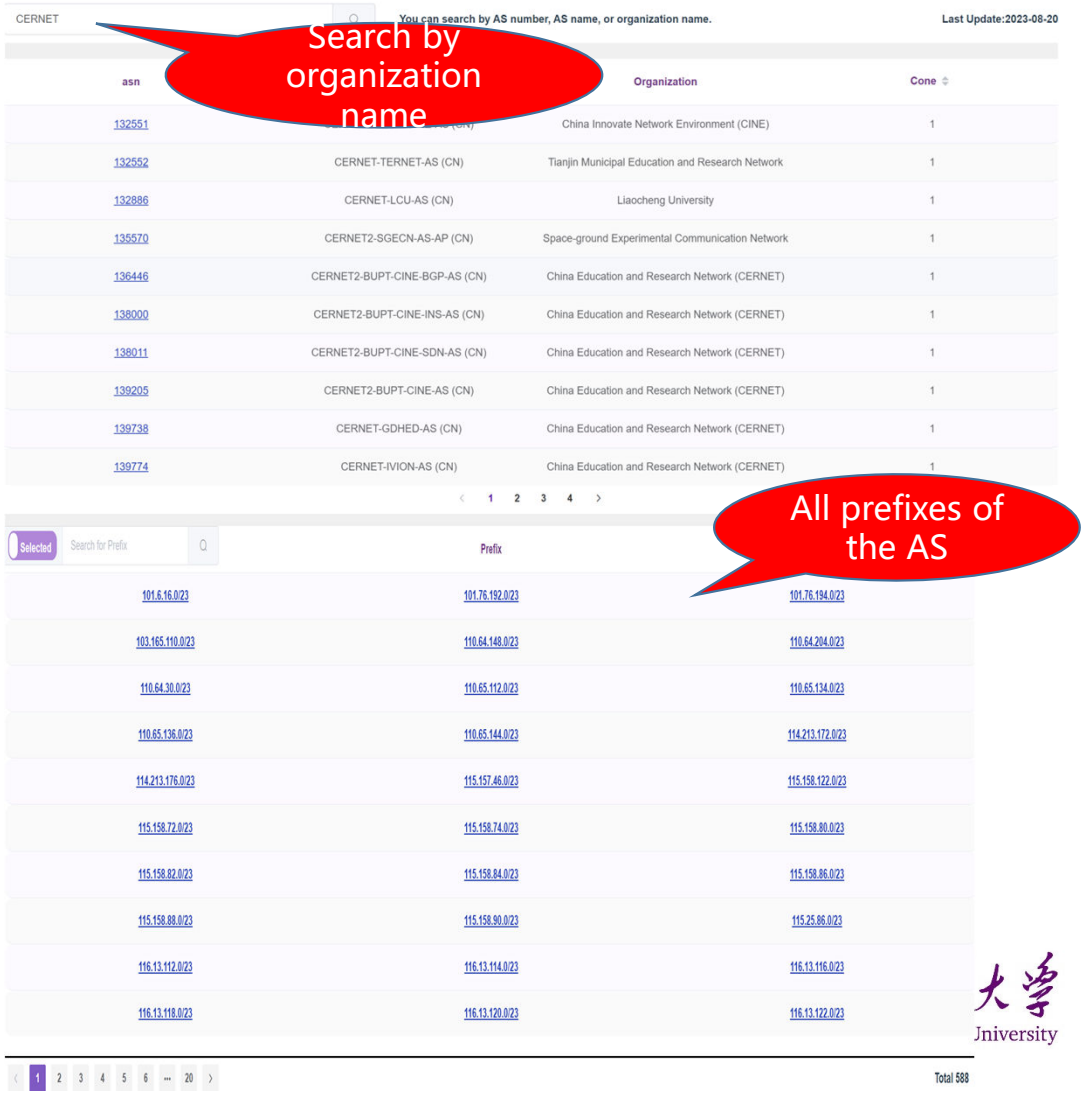
Do statistics by country/region, AS, and by yearly, monthly, weekly, and daily

FOUNDATION

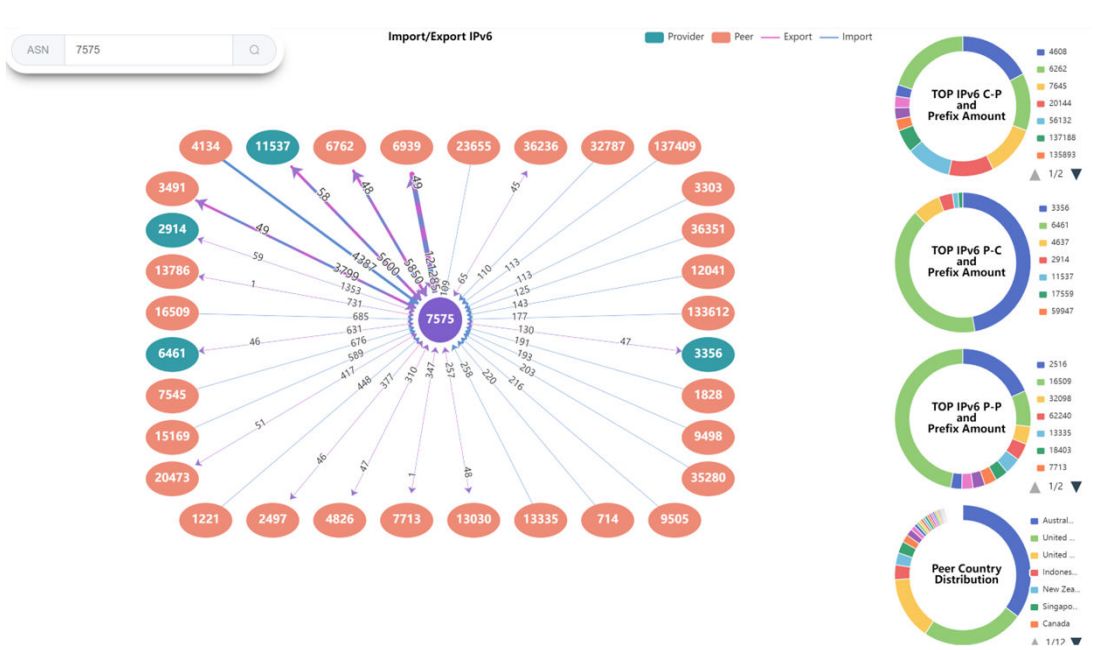
Tsinghua University

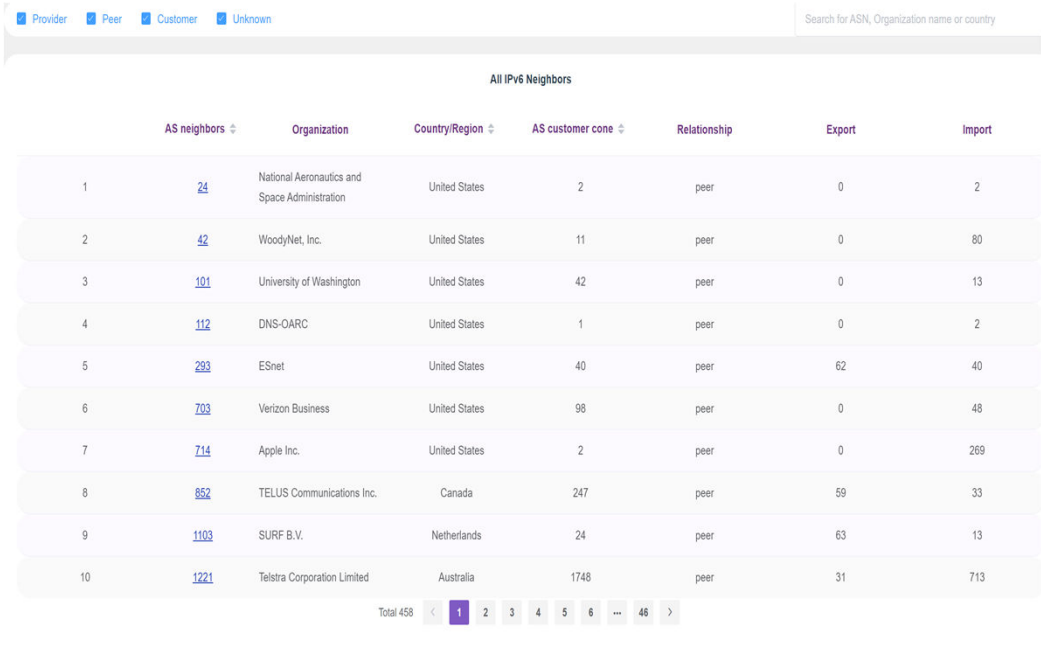
DashBoard


DragonLab BGPWatch
Home
Overview
Anomaly
DashBoard
RoutingPath
Country/Region
Document
Login
Register
Search by AS number
4538
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
IPv4 Prefix Count
IPv4 Address Size(/24)
IPv6 Prefix Count
IPv6 Address Size(/40)
IPv4 Prefix
IPv6 Prefix


CERNET
You can search by AS number, AS name, or organization name.
Last Update:2023-08-20
Search by organization name
asn
Organization
Cone
132551 China Innovate Network Environment (CINE) 1
132552 CERNET-TERNET-AS (CN) Tianjin Municipal Education and Research Network 1
132886 CERNET-LCU-AS (CN) Liaocheng University 1
135570 CERNET2-SGECN-AS-AP (CN) Space-ground Experimental Communication Network 1
136446 CERNET2-BUPT-CINE-BGP-AS (CN) China Education and Research Network (CERNET) 1
138000 CERNET2-BUPT-CINE-INS-AS (CN) China Education and Research Network (CERNET) 1
138011 CERNET2-BUPT-CINE-SDN-AS (CN) China Education and Research Network (CERNET) 1
139205 CERNET2-BUPT-CINE-AS (CN) China Education and Research Network (CERNET) 1
139738 CERNET-GDHED-AS (CN) China Education and Research Network (CERNET) 1
139774 CERNET-IVION-AS (CN) China Education and Research Network (CERNET) 1
All prefixes of the AS
Selected
Search for Prefix
Prefix
101.6.16.0/23 101.76.192.0/23 101.76.194.0/23
103.165.110.0/23 110.64.148.0/23 110.64.204.0/23
110.64.30.0/23 110.65.112.0/23 110.65.134.0/23
110.65.136.0/23 110.65.144.0/23 114.213.172.0/23
114.213.176.0/23 115.157.46.0/23 115.158.122.0/23
115.158.72.0/23 115.158.74.0/23 115.158.80.0/23
115.158.82.0/23 115.158.84.0/23 115.158.86.0/23
115.158.88.0/23 115.158.90.0/23 115.25.86.0/23
116.13.112.0/23 116.13.114.0/23 116.13.116.0/23
116.13.118.0/23 116.13.120.0/23 116.13.122.0/23
Total 588

Dashboard: IPv4/IPv6 Key Peers and All neighbors Information





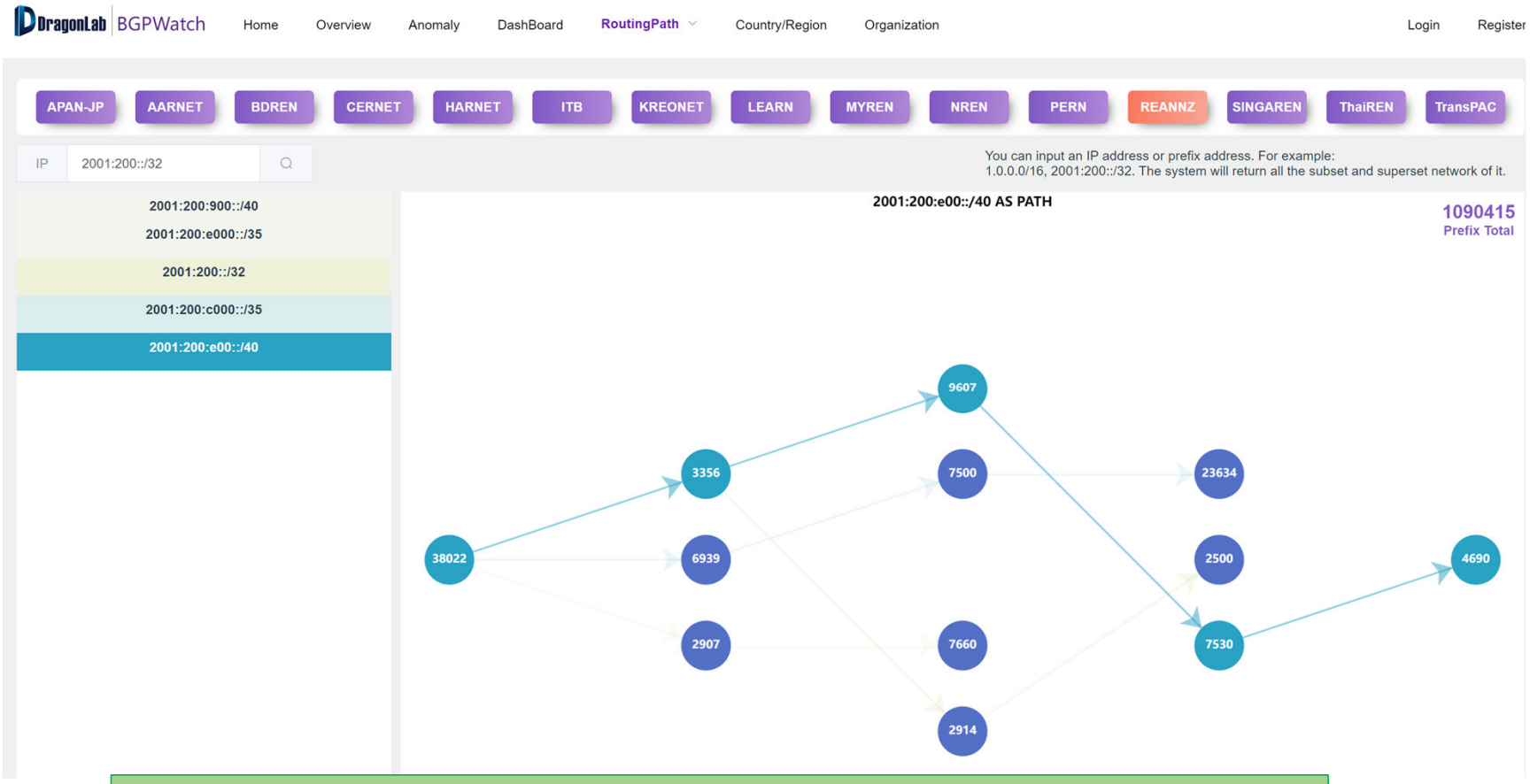
Key Peers

All neighbors

APNIC FOUNDATION

Tsinghua University

Routing Path Search

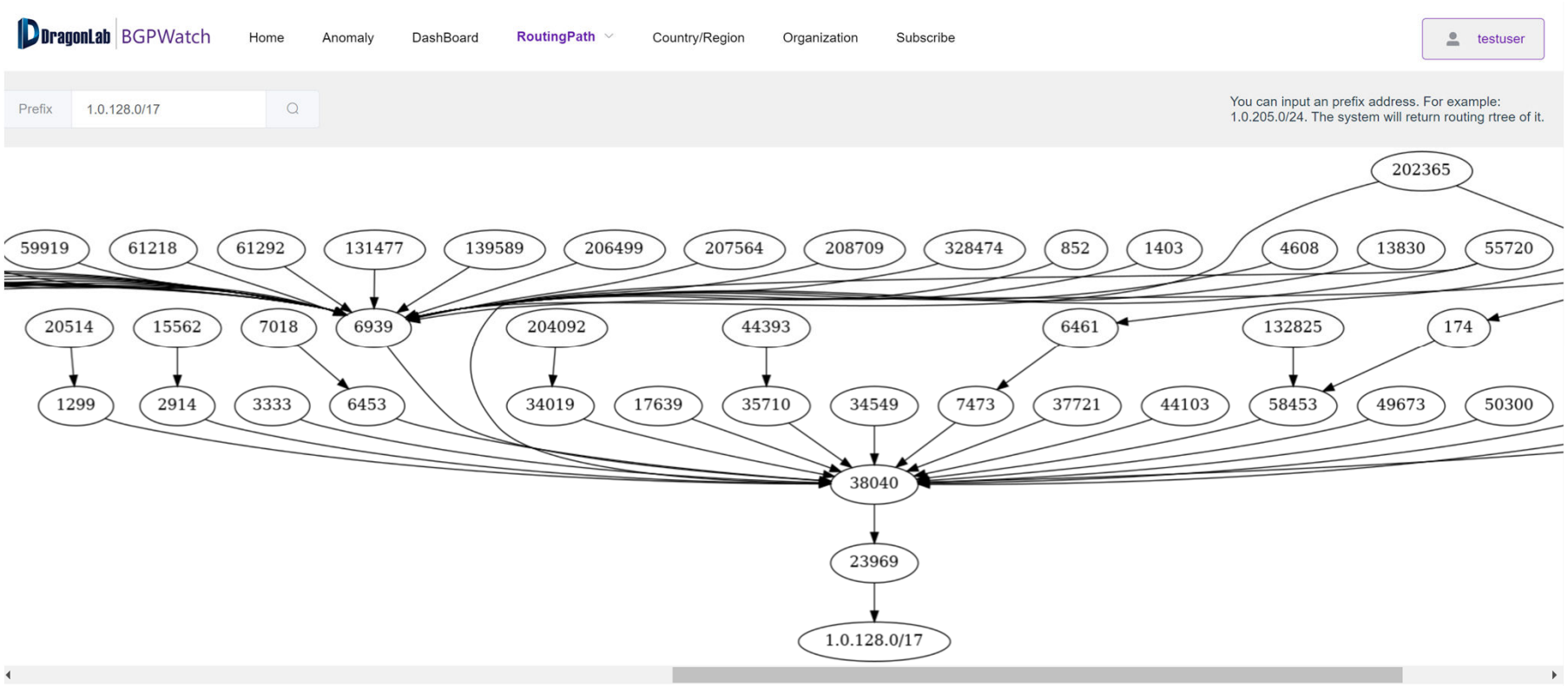


Support Prefix /IP, IPv4 / IPv6.
Return paths of all sub networks and super networks of the input prefix.
Group Prefixes with the same routing path.

APNIC FOUNDATION

Tsinghua University

Reverse Routing Path

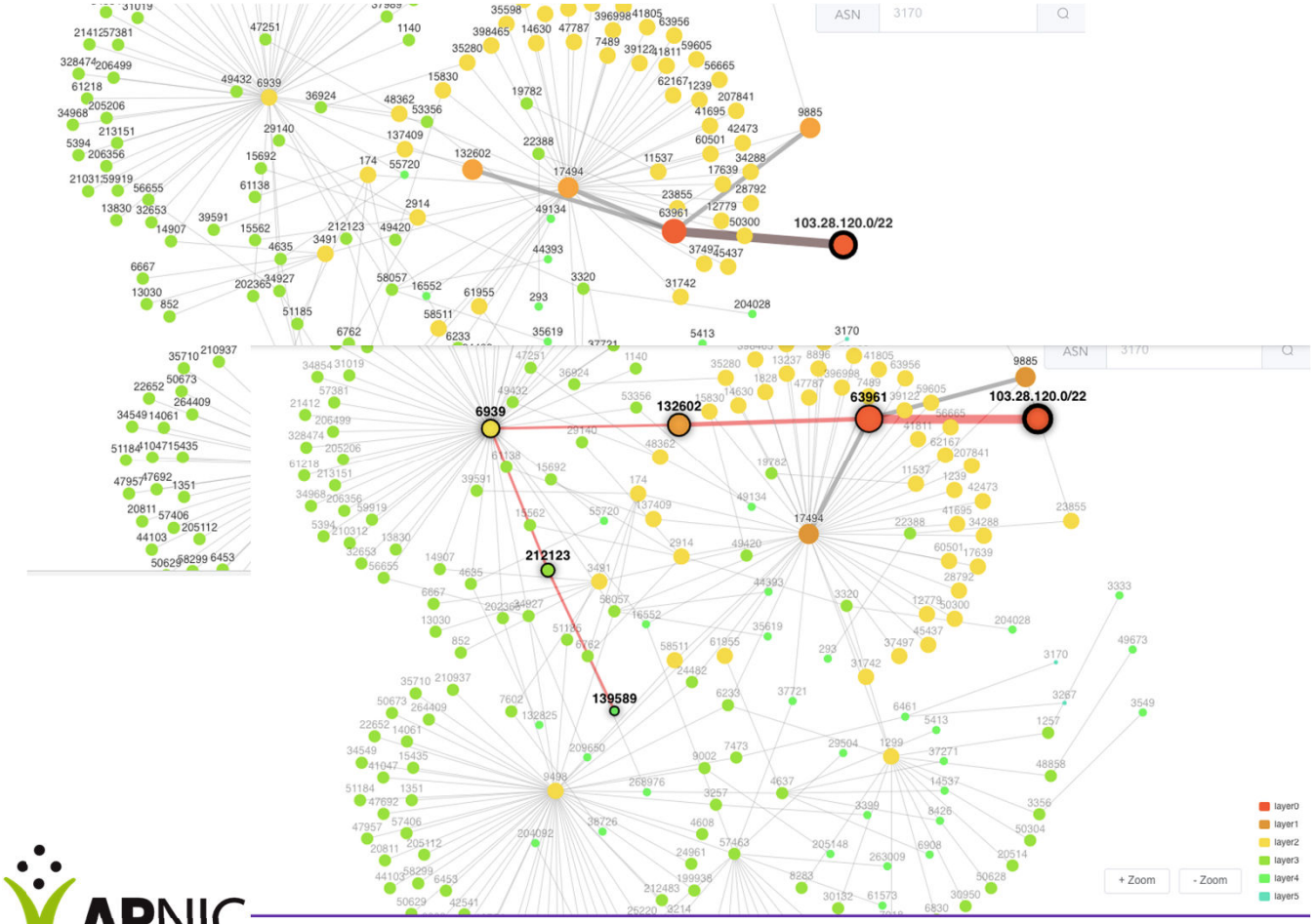


Support Prefix /IP, IPv4 / IPv6.
The system will search the best matched prefix and return the reverse routing tree.

APNIC FOUNDATION

清華大學 Tsinghua University

Reverse Routing Path (TOPO)

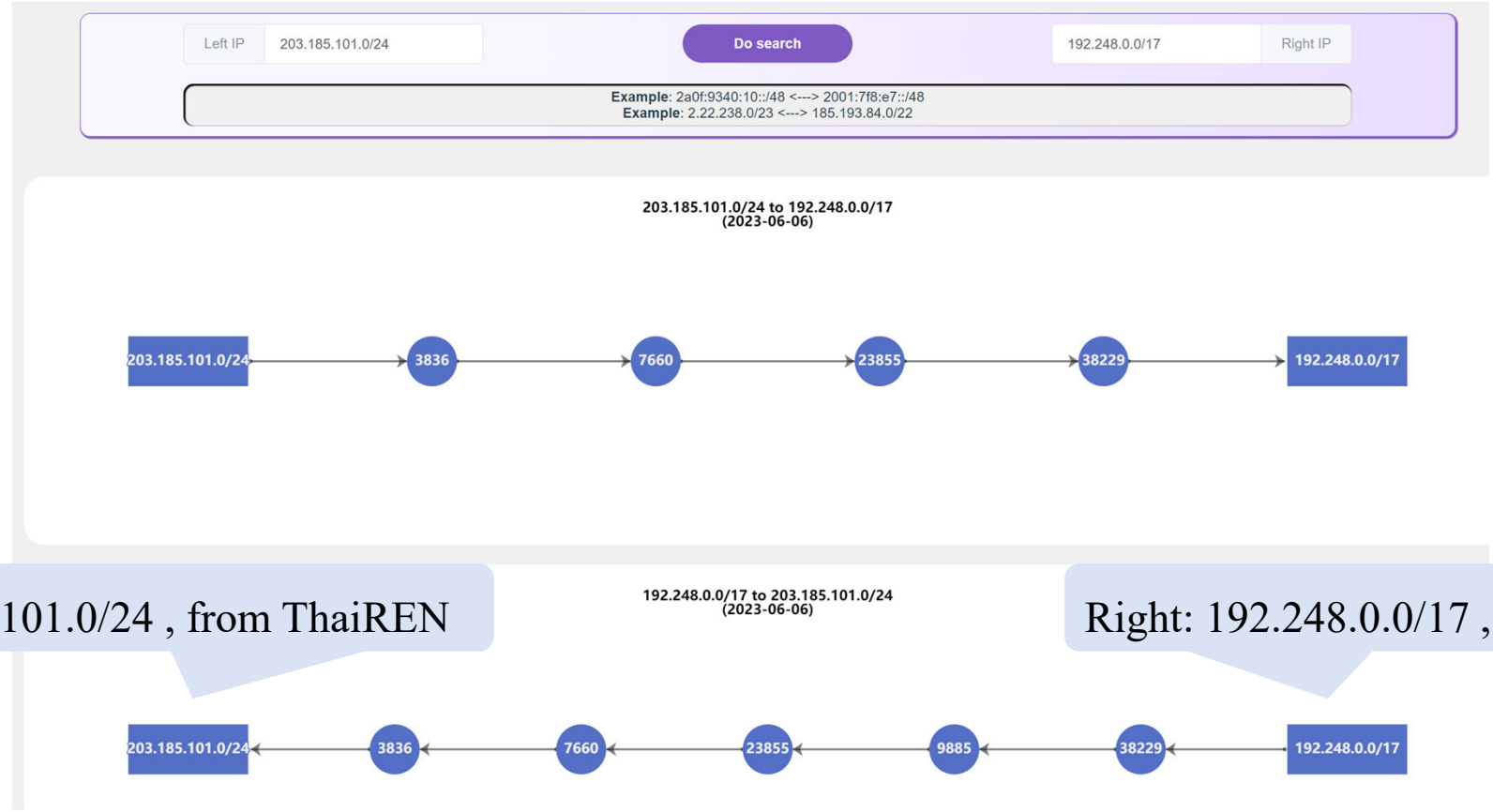


- Support Prefix /IP, IPv4 / IPv6.
- The system will search the best matched prefix and return the reverse routing tree.
- With better interactivity
- Can select an AS or input AS number, the system will highlight the path to the AS
- The number of layers to display can be selected

APNIC FOUNDATION

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 when Prefix Change

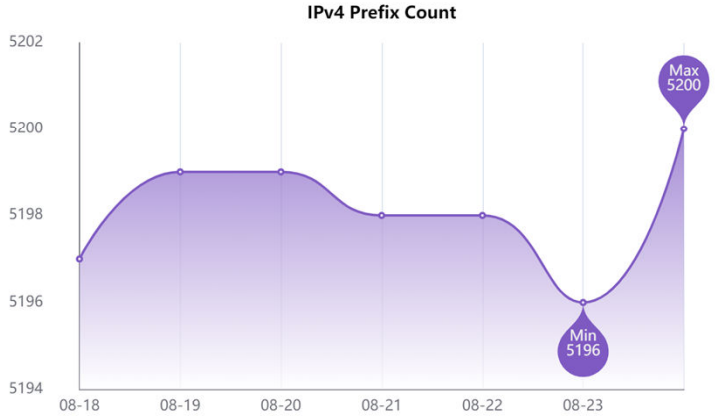
ASN **4538**

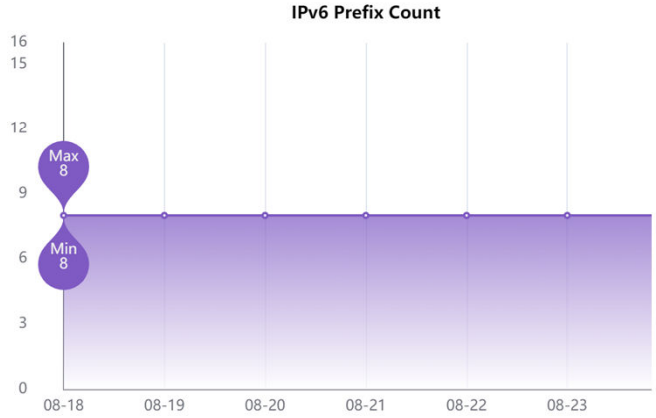
Country/Region **CN**

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

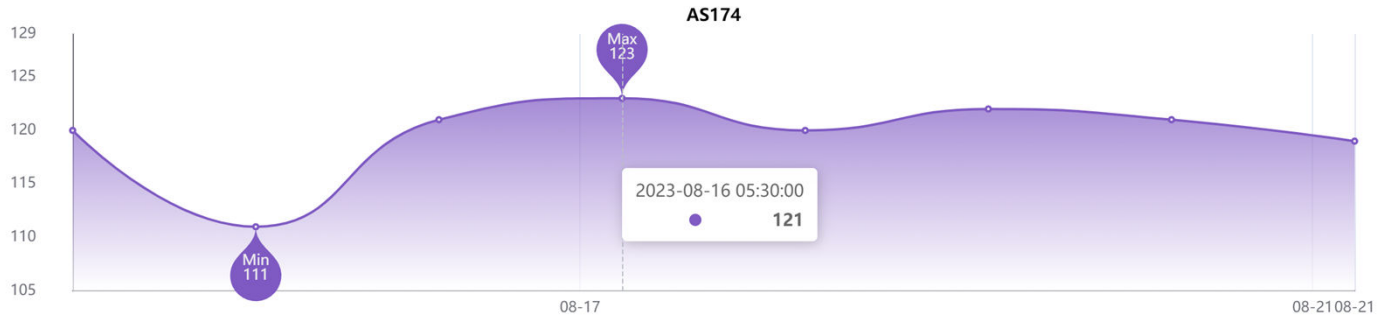
subscribe ASN [4538,4630]

You can input an ASN expression , one or more ASN. For example:
[1,100]: will subscribe to ASes which ASN range from 1 to 100;
4538: will subscribe to AS which ASN is 4538;
4538,4134: will subscribe to ASes which ASN are 4538 and 4134

APNIC FOUNDATION

Tsinghua University

Peer Change

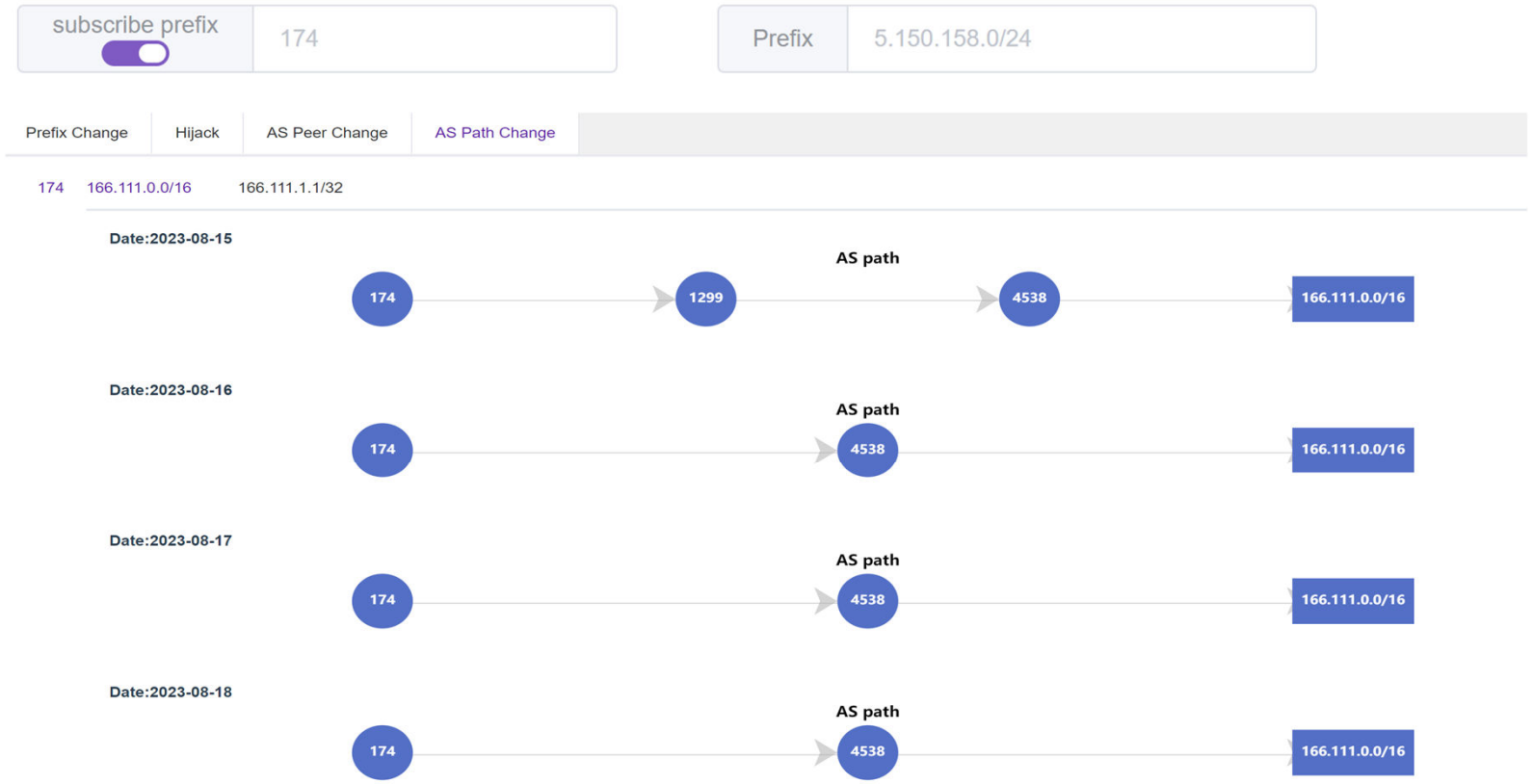


-263009	-62663	18106	38880	835	3741	38193	49788	61595	39591	1031	23673	47787	701	63927	136557
14315	34927	8529	6762	6461	3491	56987	6057	7195	2914	271253	37468	4788	13786	6327	11686
40934	1299	6830	2497	34288	3303	4775	18747	6082	3356	4764	1351	395348	20485	3320	398465
56665	8966	31133	3257	267613	17557	46887	7713	38195	19151	58453	137409	37271	24516	19754	52694
2518	9297	49544	22652	4657	1403	12779	14259	1239	132337	5650	36236	61568	199524	55222	208594
37100	7018	45352	5511	852	53732	58299	39120	16735	37662	23473	264409	1798	4538	52320	63956
12956	5713	53013	1273	53427	30600	6453	61955	60068	33185	28329	4230	55081	20764	20912	23352
50673	34465	7303	7162	5580	23033	34549	270868	2516							

APNIC FOUNDATION

清華大學 Tsinghua University

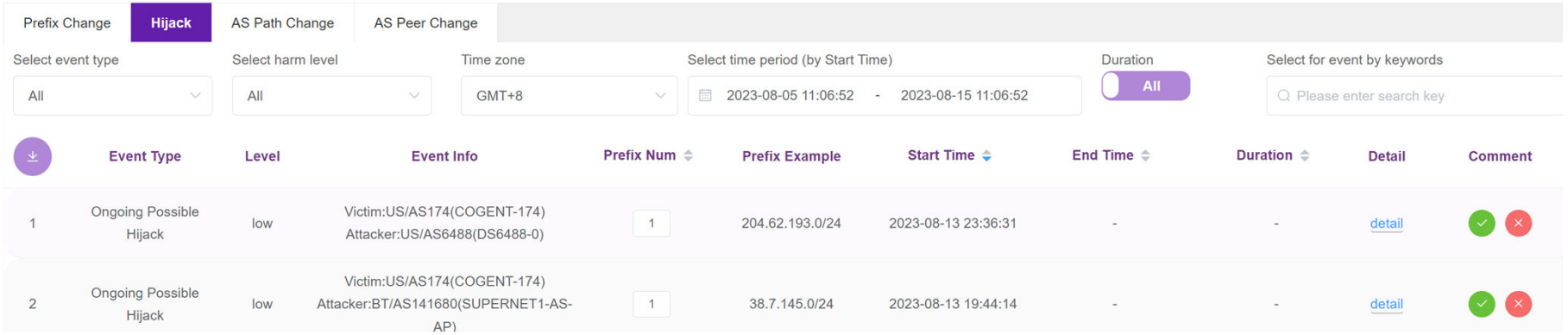
Path Change

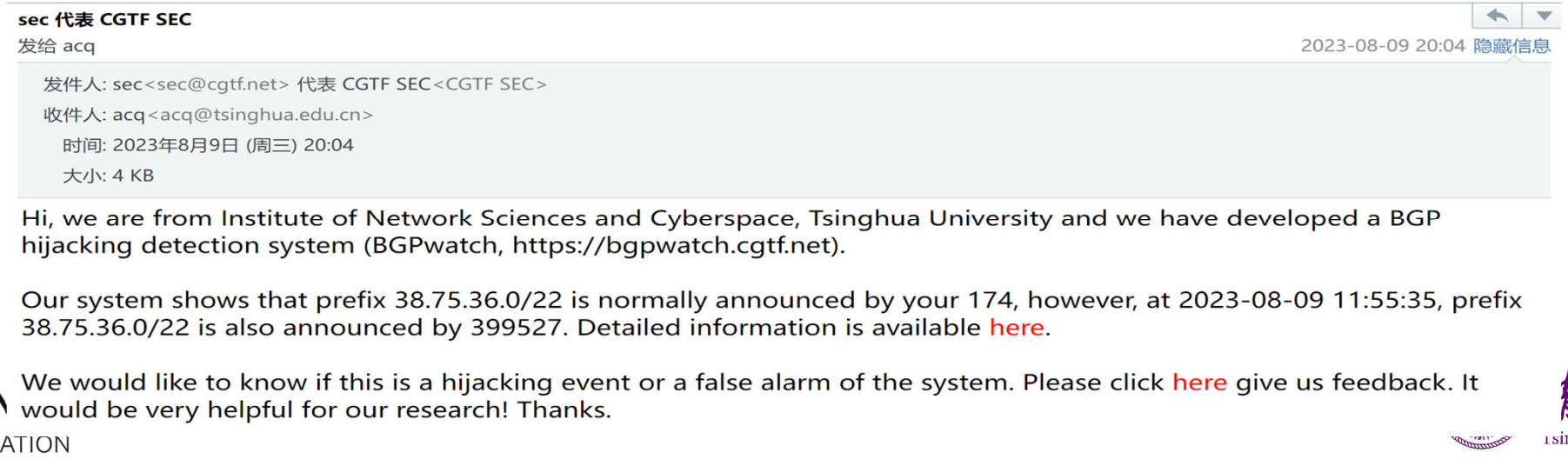


APNIC FOUNDATION

清華大學 Tsinghua University

Subscribe Hijacking Events for AS and Send Alarm

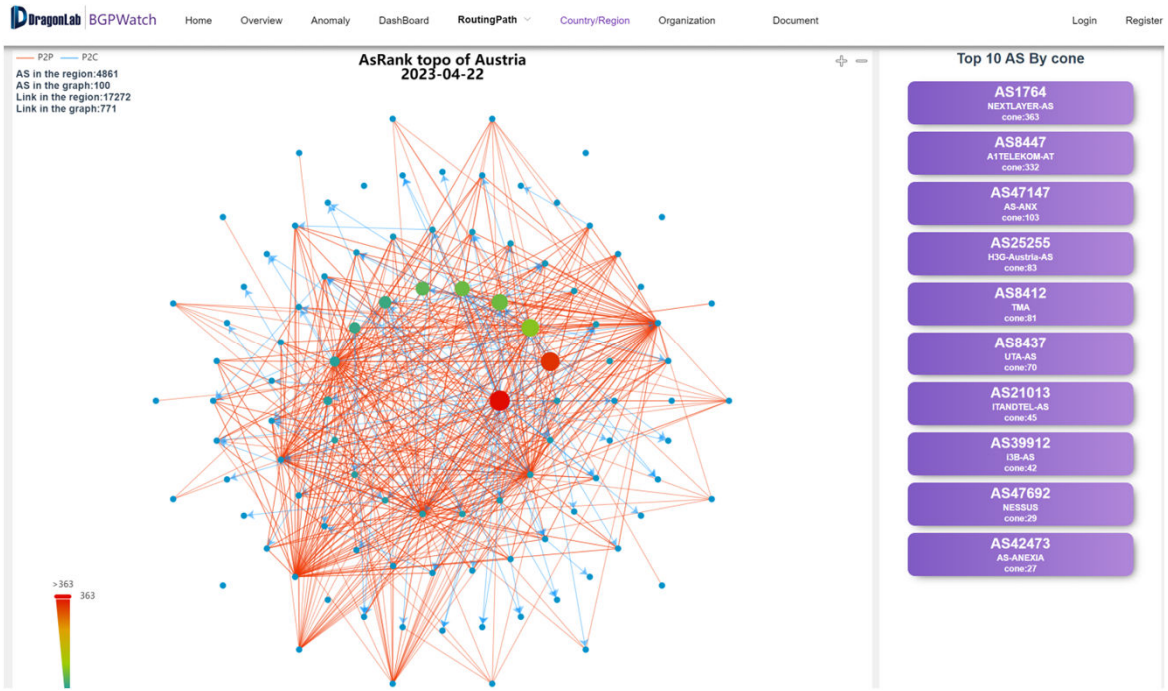


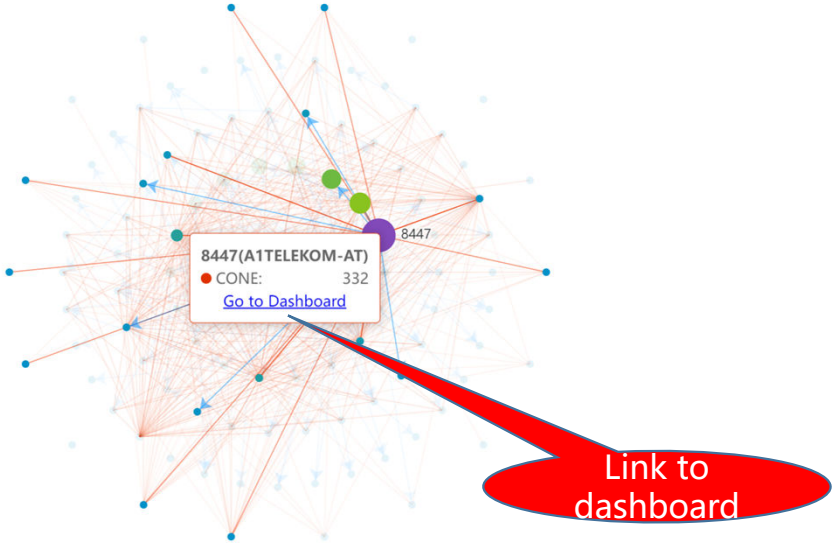


APNIC FOUNDATION

清華大學 Tsinghua University

Topo of Country/Region





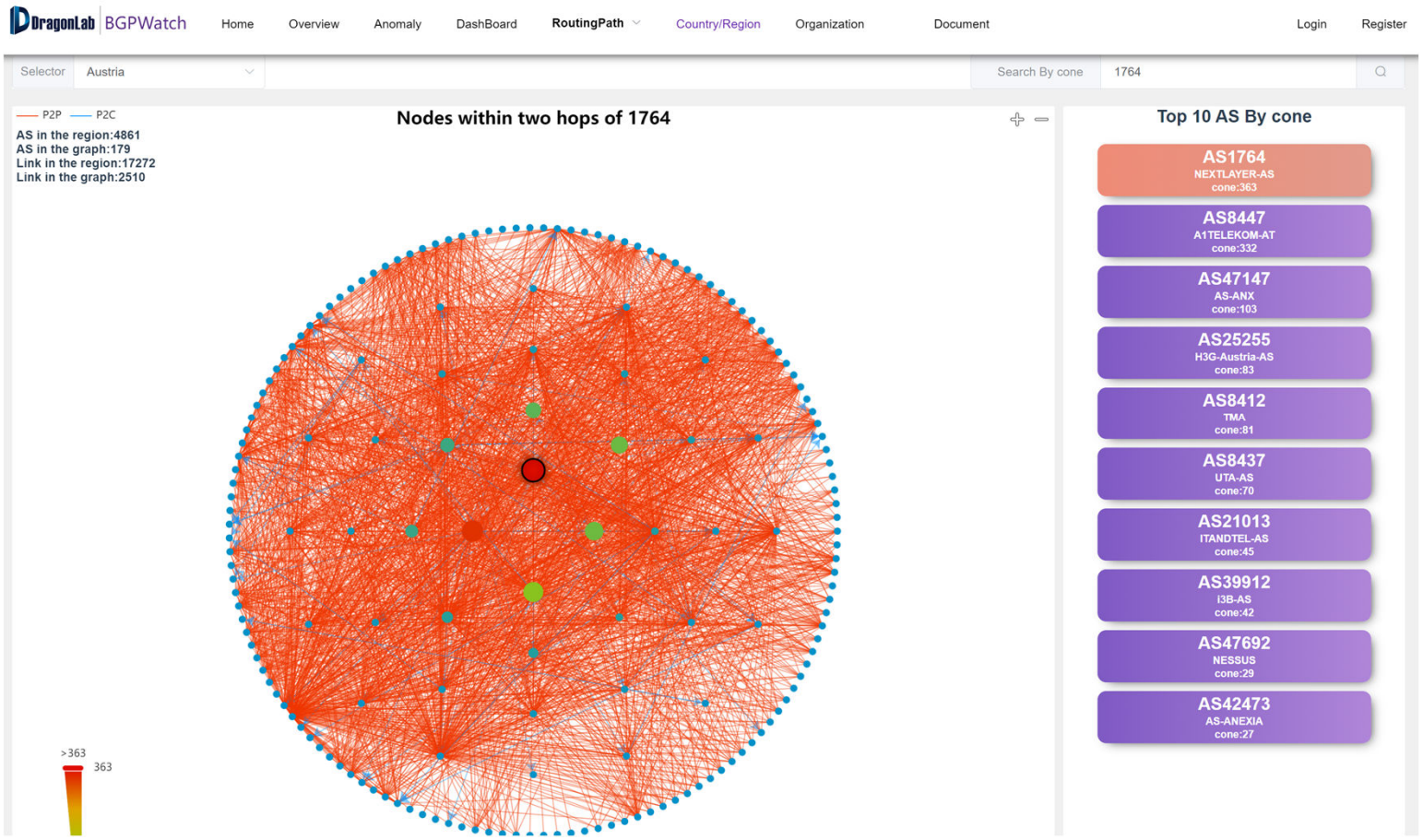
Show Topology and TOP 10 ASes

Show connection of a node, and can go to Dashboard

APNIC FOUNDATION

清華大學 Tsinghua University

Topo of Country/Region



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

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/

APNIC FOUNDATION

清華大學 Tsinghua University

Feedback from Partners I

- Screen Resolution Auto Adaption (done)
- Error when search IPv6 address routing(done)
- Statistics error on Home page(done)
- Configure interested prefix/AS, and send alert when anomaly/hijacking
- More BGP related alert, such as peer change/path change
- Send message by slack channel
- Bi direction routing path(done)
- Reverse routing path(done)
- Monthly /weekly summary(done)
- Show alternative routing path/track multi path
- Path performance

APNIC FOUNDATION

Been Fixed **Been Fixed Lately**

清華大學 Tsinghua University

Feedback from Partners II

- If you want to search an “Organization” using name, AS-name or AS-number you have to go to the “Organization” menu
  - Organization Name is “Case sensitive”, better if it is made “Case insensitive”
- The prefixes in “Dashboard=>IPv4 Peers” and that of “Routing Path” should match.
- Needs to put the “last date of update” for the records which will be periodically updated.
- Remedial Measures： Once the “Hijacker” is suspected, can we warn the suspected entity AS20853 along with its upstream provider AS 1299 with emails. The process may be automatized if we can collect the administrative contacts of each AS from APNIC.

APNIC FOUNDATION

Been Fixed **Been Fixed Lately**

清華大學 Tsinghua University

Feedback from Partners III

- Reporting Anomaly： Incomplete information, Timezone undefined
- Fault alarm (Must sync ROA & RIR data timely)
- Bidirectional Routing Path: some paths are missing
- Can we mention the name of the Top-10 organizations and their cone size next to the diagram? That will give an idea about the top service providers in each country.

- In the “Dashboard”, it searches advertised prefixes but there is no subnet-wise search. Suppose, it will find out 103.28.120.0/22 under BdREN but cannot locate 103.28.121.0/24.

- There is not much usage of “Reverse Route Path”. It generates a file in “image” format which also doesn’t provide a legible view when enlarged. Better if it could be made available in pdf format.

APNIC FOUNDATION

Been Fixed

清華大學 Tsinghua University

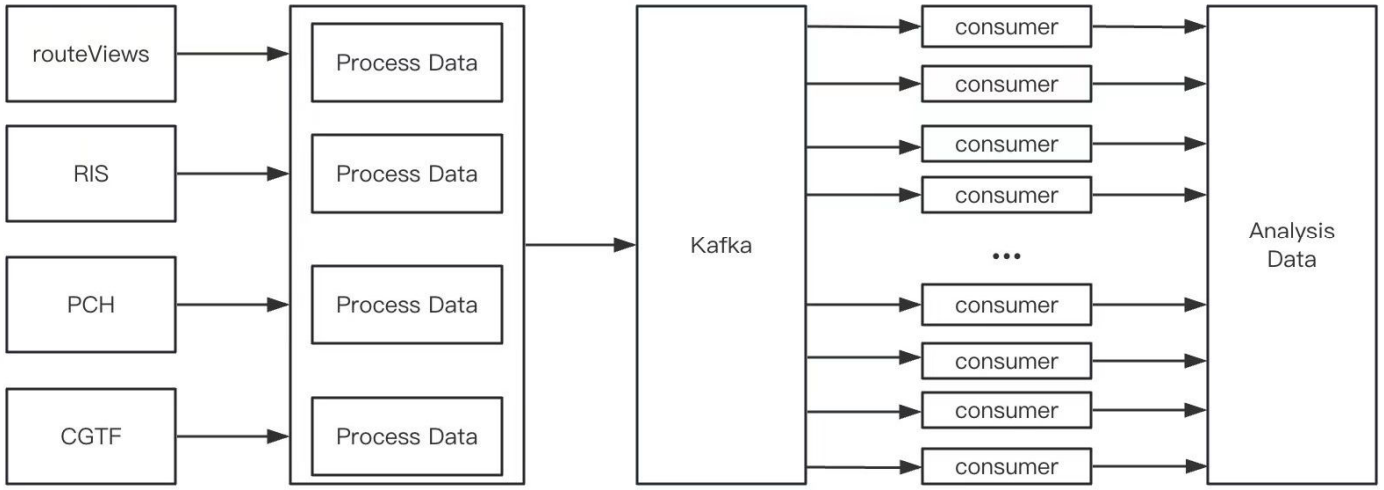
Feedback from Partners IV

- Suggestion on Visual improvements
  - Visual directional relationship from attacker to victim
  - Zooming of Map
  - Larger view/pop-out view of other surrounding windows
- Prefix information should be updated regularly
- Wrong direction in Bi-Routing Path
- Mitigation feature support is highly required
- Monitoring or alerting system for AS path change to a selected destination
- API for receiving data to display on partner customized applications and monitoring systems
- Some topologies does not show ASN details when hovering over the ASN nodes
- Open source the project

Been Fixed Been Fixed Lately

Parallel Computing and Clusters to handle big routing data

- Parallel Computing and Clusters to handle big routing data
  - There are huge amount routing data from RouteViews, RIS, PCH, CGTF.
  - We improved the system a by Parallel Computing and Clusters.



APNIC FOUNDATION

清華大學 Tsinghua University

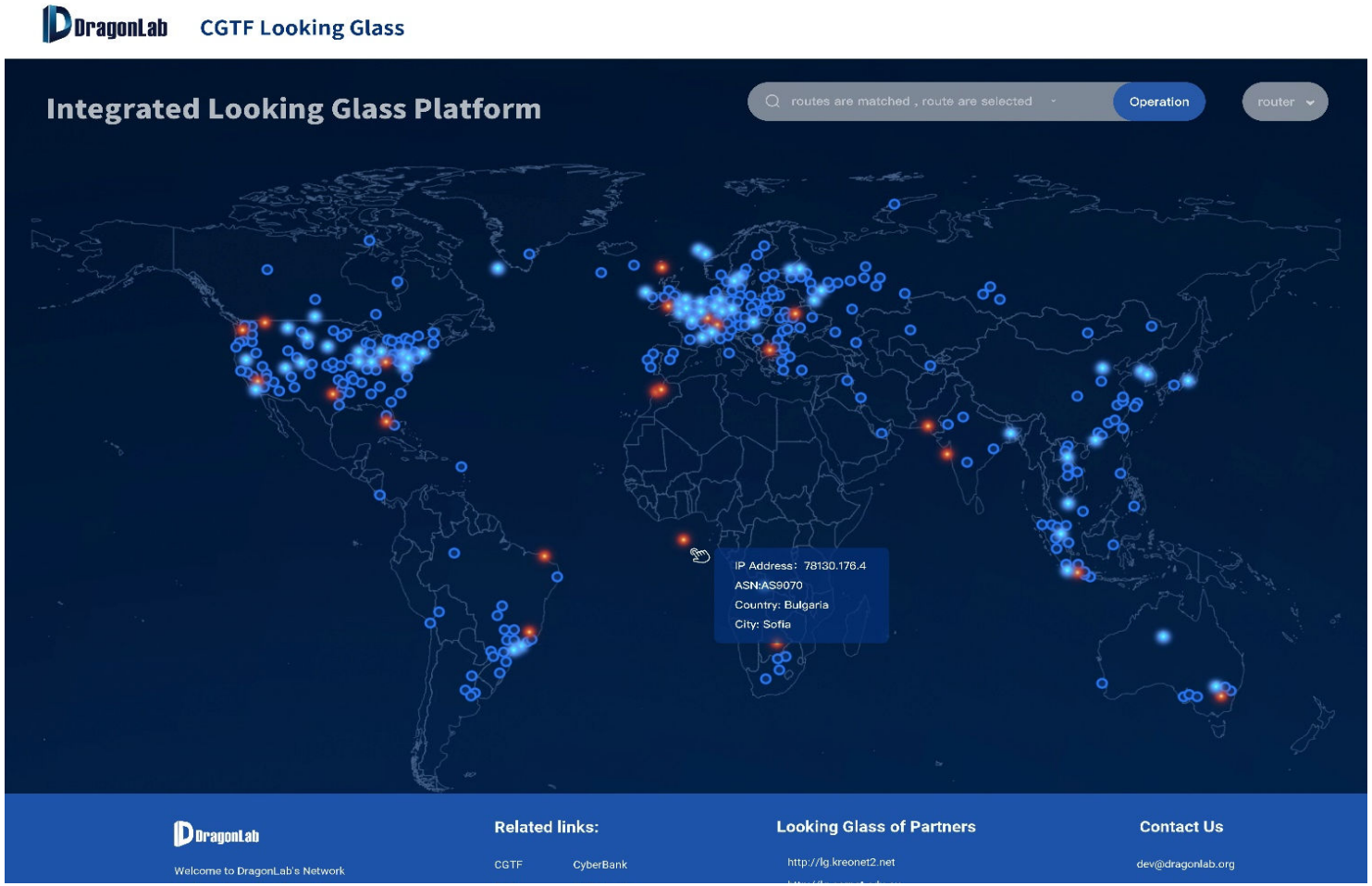
Future Work: Proposal of the Next APNIC ISIF Funding (Approved)

- 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 (Draft):
  - 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

APNIC FOUNDATION

清華大學 Tsinghua University

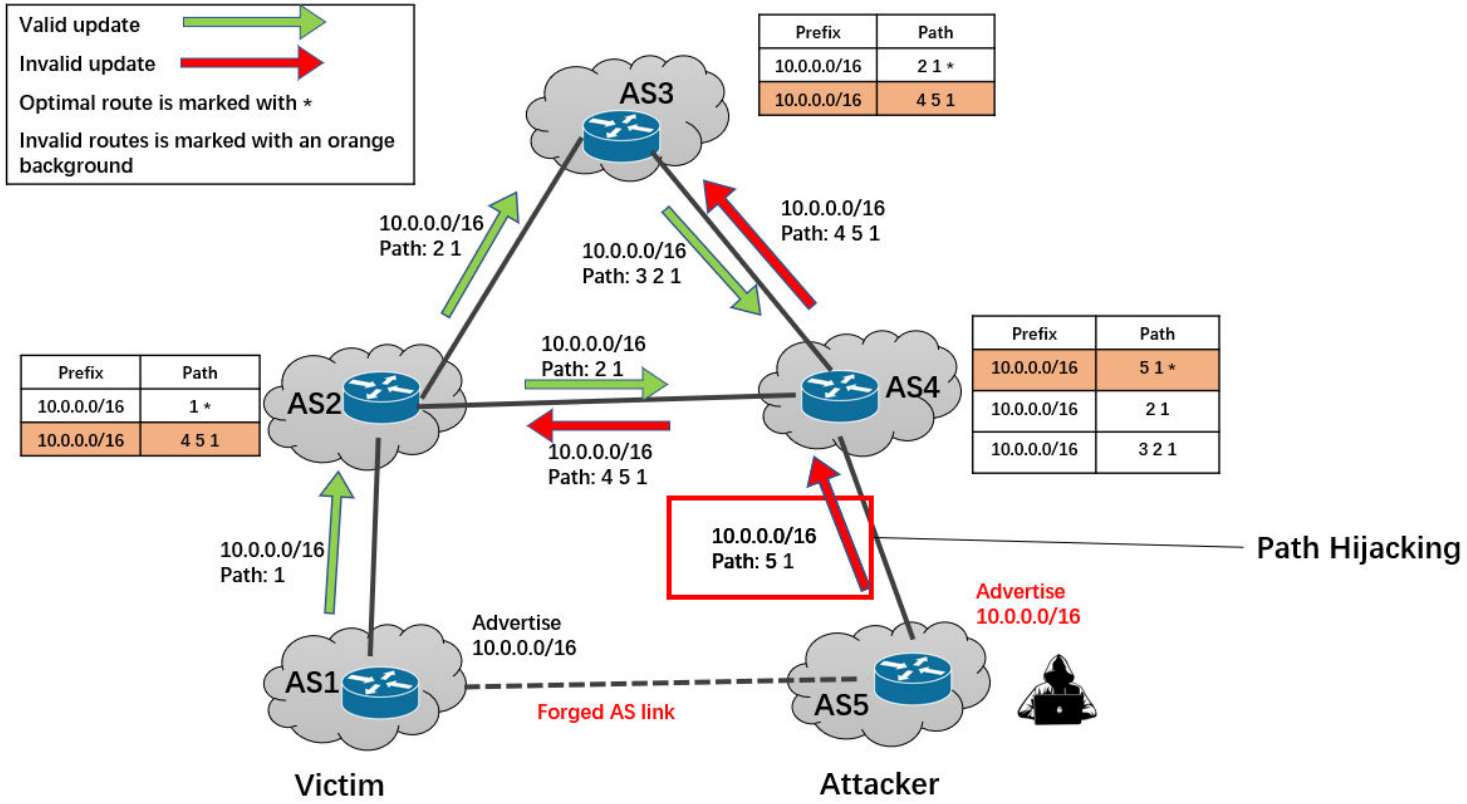
An Integrated Looking Glass and Open API



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

Detecting Fake AS-PATHs based on Link Prediction --Paper published at ISCC2023

- Path hijacking can evade MOAS ,but usually cause unseen AS link.

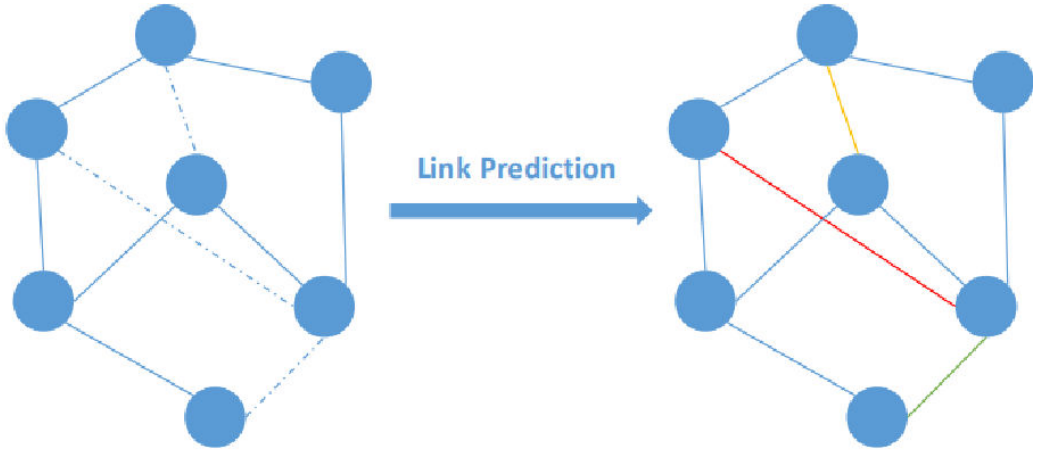


State-of-the-art for path hijacking detection

- Hybrid-plane detection technique（Argus、Fingerprints etc）
  - Treat all unseen links appearing in the control plane as suspicious event, then validate the event through the data-plane probing.
- Limitation
  - Unseen links are very common（New peering establishment, Backup links. Route policy changes, etc）， and only a few of them are due to path hijacking.
  - Existing methods encounter severe data-plane overhead waste, making them Inefficient and difficult to guarantee real-time.

Idea

- Evaluating the authenticity of unseen links with link prediction and filtering the benign unseen links.
- Link prediction: a technique for inferring whether a link is likely to exist between two nodes from an existing observable portion of the network.



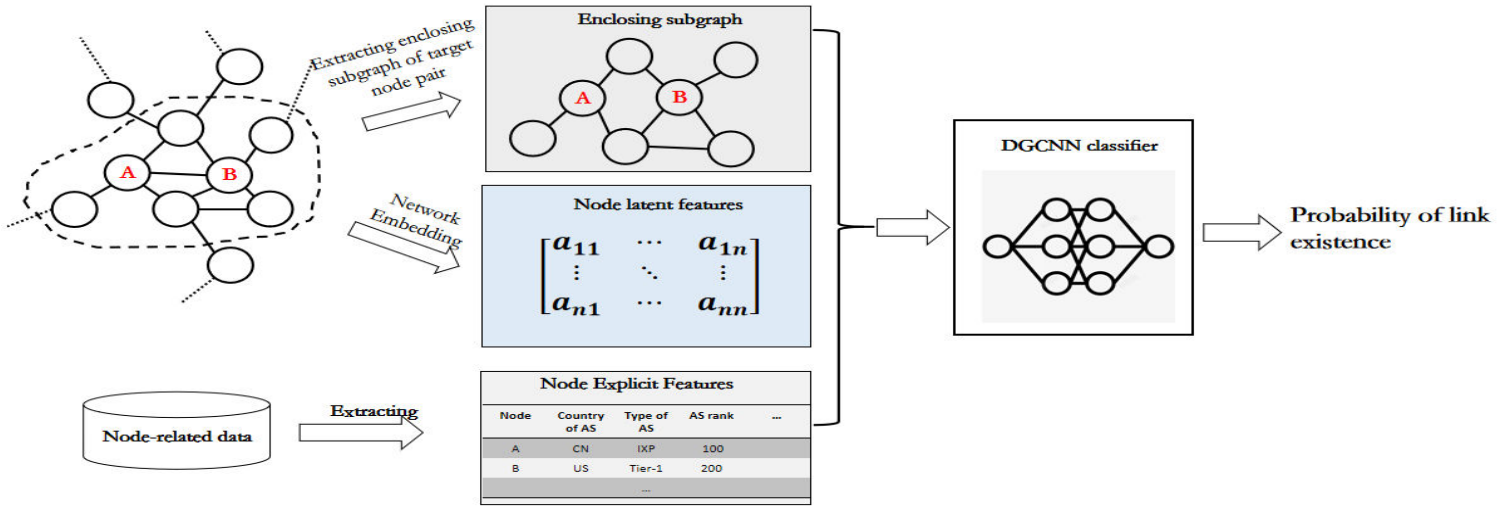
Is AS link predictable?

- Zhuang et al recently formulate the link prediction as a matrix completion task. Their work explain the predictability of AS link.

- Graph characteristics of AS-level topology
  - power-law distribution
  - negative degree-degree correlation
  - Hierarchical
  - AS links usually connect two ASes with the same properties.

Unseen link classification

- We select SEAL as the link prediction algorithm
- CAIDA AS relationship 2021 & AS location、 type and size
- Training with positive and negative samples
- The accuracy reached 0.95 and the AUC reached 0.98



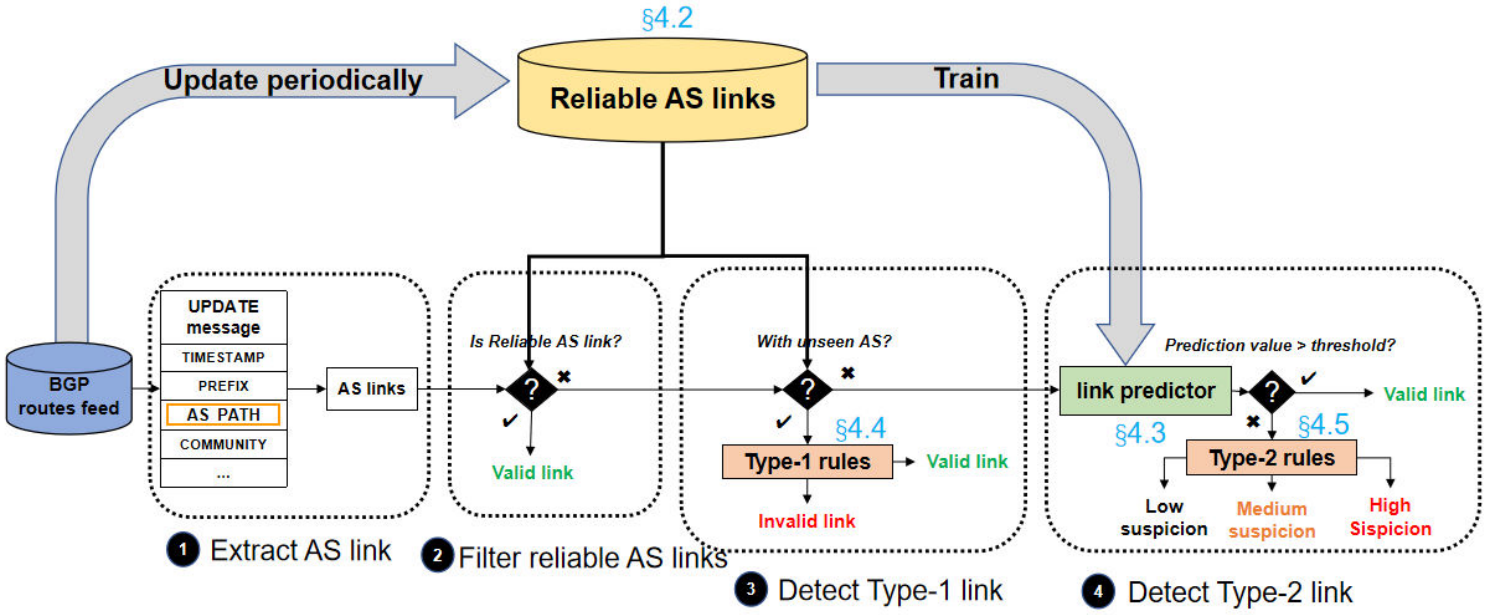
Workflow of SEAL

APNIC FOUNDATION

清華大學 Tsinghua University

Metis: a fake AS-PATHs detection framework

- Still based on unseen links
- Combine link prediction and rules
- Link prediction is used to find suspicious unseen links, and rules are used to improve the confidence level

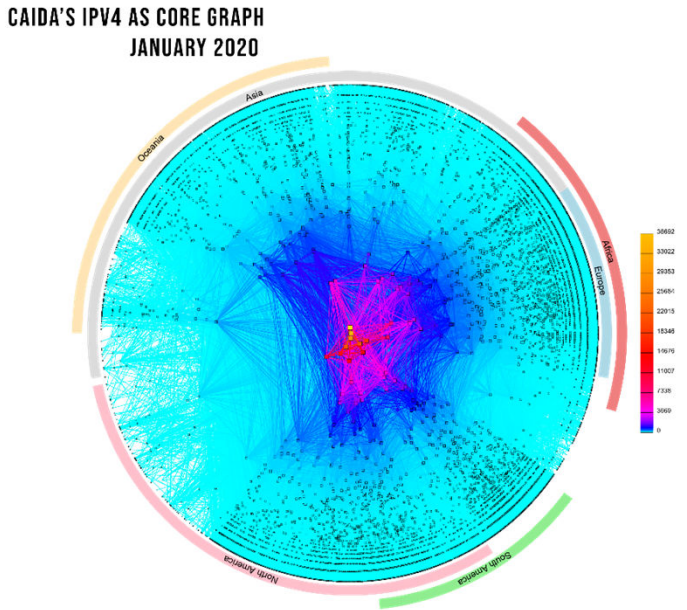


APNIC FOUNDATION

清華大學 Tsinghua University

Reliable links

- Links are believed to be real links on the current AS topology
- Goal: more historical seen links but few obsolete links
- Our method: union of the past 6 months of the CAIDA AS relationship dataset



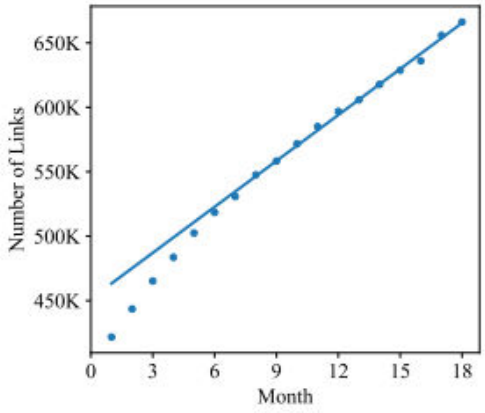


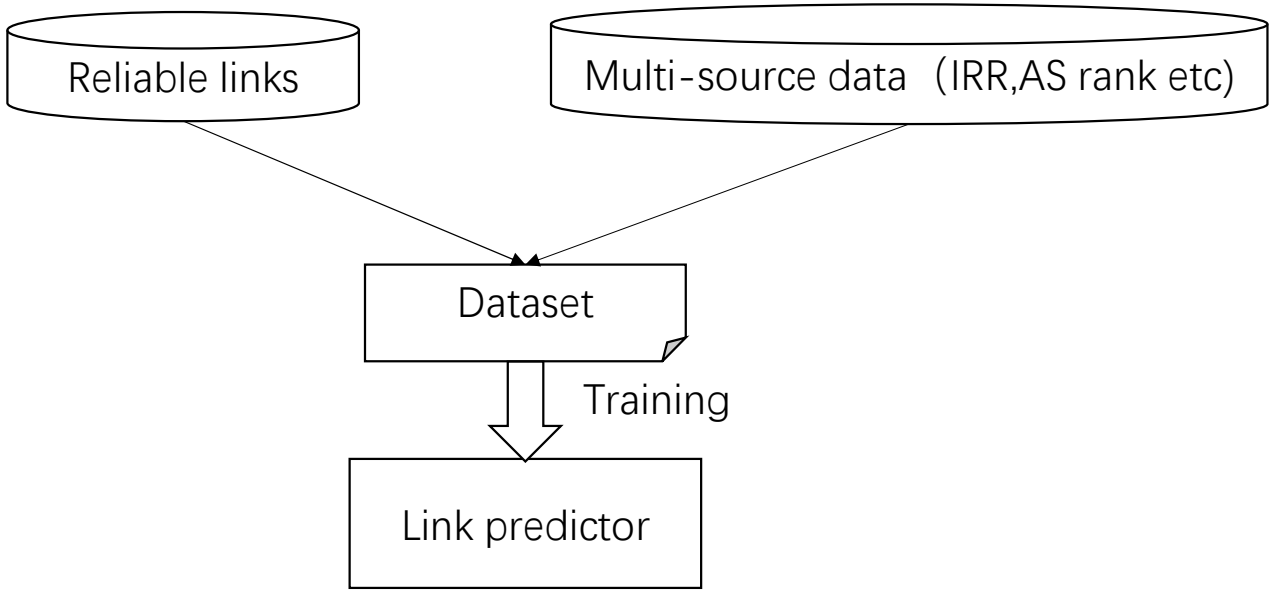
Fig. 7: The number of union AS links in CAIDA AS relationship data of the past N months of November 2021

APNIC FOUNDATION

清華大學 Tsinghua University

Link predictor

- To evaluating the authenticity of unseen links
- Trained with reliable links and side information of ASes
- In the framework, it can use any link prediction algorithm



APNIC FOUNDATION

清華大學 Tsinghua University

Type-1 unseen link detection

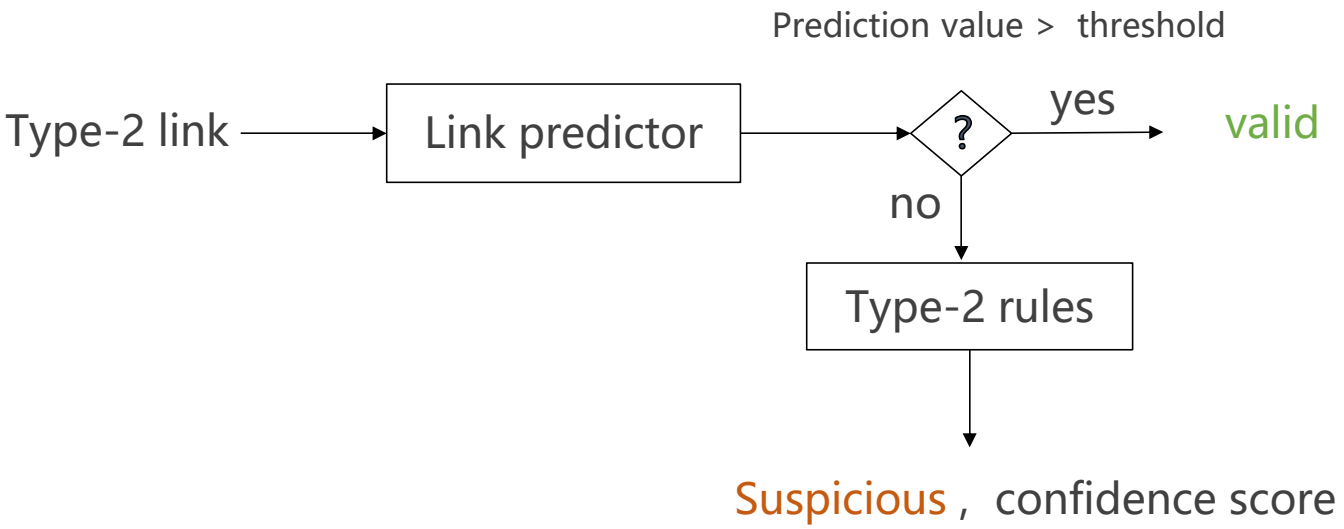
- Type-1 link with unseen new AS, cannot be evaluated by link predictor
- account for a relatively small percentage
- 3 simple rules:
  - The new AS is a reserved ASN
    - 24514 24490 24489 23911 4538 65534
  - The new AS is not registered in the whois data of the 5 RIRs
    - 24514 24490 24489 23911 4538 66666
  - The new AS is not the last hop in the AS-PATH（Our measurement show more than 97% of newly used ASes appear on the Internet as a stub AS.）
    - 24514 24490 24489 23911 4537 4538

APNIC FOUNDATION

清華大學 Tsinghua University

Type-2 unseen link detection

- Input into link predictor, and then determine the confidence level with Type-2 rules.



APNIC FOUNDATION

清華大學 Tsinghua University

Type-2 rules

- Initial confidence score is 0
- The score increases 1 when:
  - AS-PATH is longer than the pre-set length threshold
  - The link with single digit ASN in the right side
  - The edit distance of the ASes is 1
  - Loop in AS-PATH, and the link is in the loop
  - AS-PATH violate valley-free rule
  - Traffic detour in the AS-PATH
- The score reduced by 2 when:
  - The suspicious link is at the end of the AS-PATH and the link is a domestic link

Evaluation

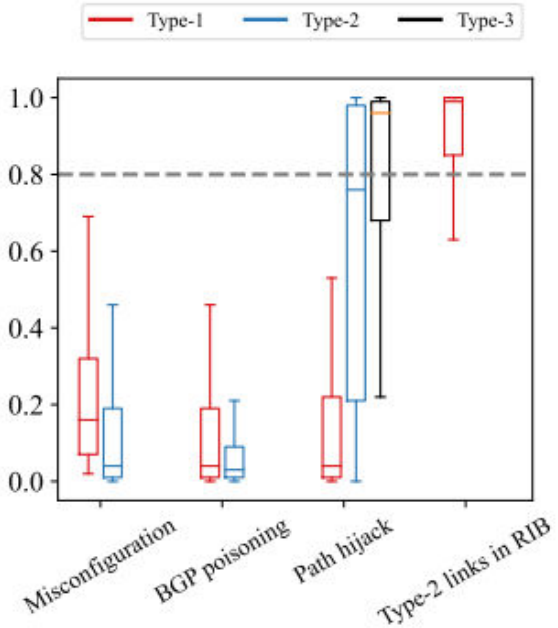
- Dataset
  - 7000 AS-PATHs in the RIB of RIPE RRC00 at 00:00 UTC on November 1, 2021
  - Misconfiguration
    - 24514 24490 24489 23911 4538 3 (Type-1 Misconfiguration)
    - 24514 24490 24489 23911 4538 4528 (Type-2 Misconfiguration)
  - BGP Poisoning
    - 24514 24490 24489 23911 4538 123 4538 (Type-1 Poisoning)
    - 24514 24490 24489 23911 4538 123 456 4538 (Type-2 Poisoning)
  - Path hijacking
    - 24514 24490 24489 23911 4538 16509 (Type-1 Path hijacking)
    - 24514 24490 24489 23911 4538 3356 16509 (Type-2 Path hijacking)
    - 24514 24490 24489 23911 4538 3356 16509 xxxx (Type-3 Path hijacking)

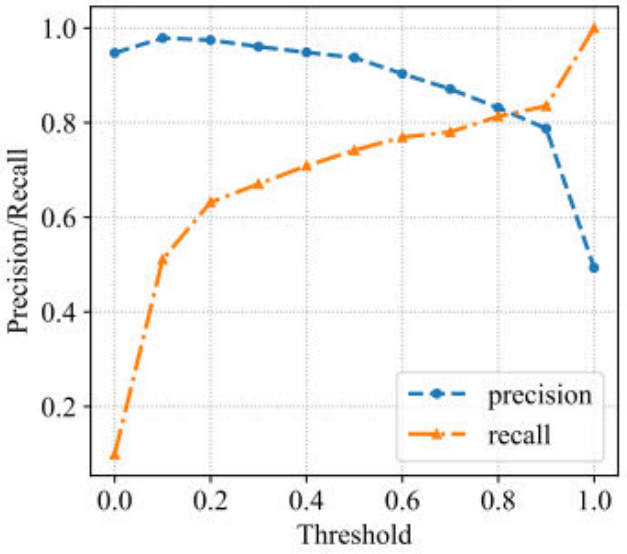
APNIC FOUNDATION

清華大學 Tsinghua University

Evaluation

- Prediction values of crafted Type-2 links are significantly lower than that of the normal links in the RIB
- When the threshold is 0.8, the classification accuracy and recall are around 80%





Evaluation

- The accuracy of positive AS-PATHs is about 99.5%, and the accuracy of Type-1 path hijacking is 87.5%.

TABLE III: Result of crafted AS-PATHs

Type of AS-PATH	Number	Reliable link	Type-1 link	Type-2 link	valid AS-PATH	Suspicious AS-PATH				Accuracy
						Type-1	high	medium	low	
GREEN AS-PATHs	7000	11181	358	187	6966	5	3	6	**20**	**99.5%**
Type-1 Misconfiguration	1000	2231	108	985	167	0	924	0	0	92.4%
Type-2 Misconfiguration	1000	2174	496	582	256	247	528	0	0	77.5%
Type-1 hijacking	1000	2213	163	940	125	3	345	481	46	**87.5%**
Type-2 hijacking	1000	3018	153	984	493	2	322	176	7	50.7 %
Type-3 hijacking	1000	3706	160	935	700	0	250	50	0	30.0%
Type-1 BGP poisoning	1000	2237	236	940	107	14	879	0	0	89.3%
Type-2 BGP poisoning	1000	2241	372	2731	11	15	974	0	0	98.9%

APNIC FOUNDATION

清華大學 Tsinghua University

Evaluation

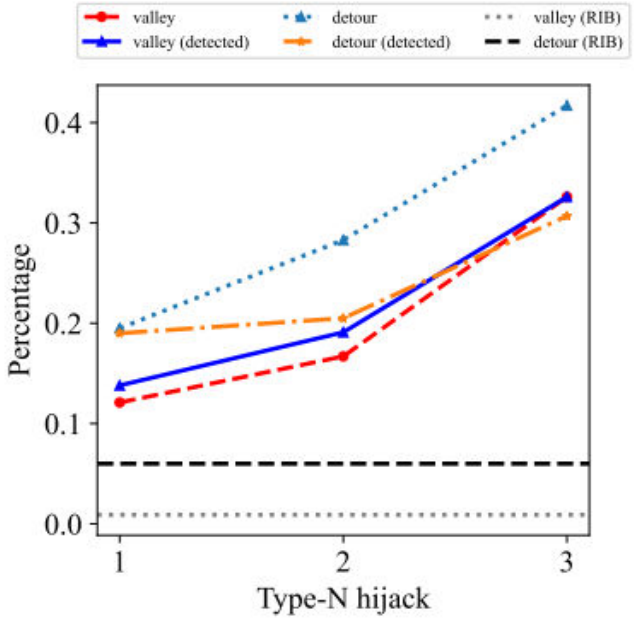
- Type-N hijacking： N is the **length of fake segment** in the AS-PATH.
- Normal AS-PATH:
  - 24514 24490 24489 23911 4538
- AS4538(CERNET) is attempt to hijack AS16509(AMAZON)
- Type-1 hijacking:
  - 24514 24490 24489 23911 4538 16509
  - Fake link : 4538-16059
- Type-2 hijacking:
  - 24514 24490 24489 23911 4538 3356 16509
  - Fake link : 4538-3356

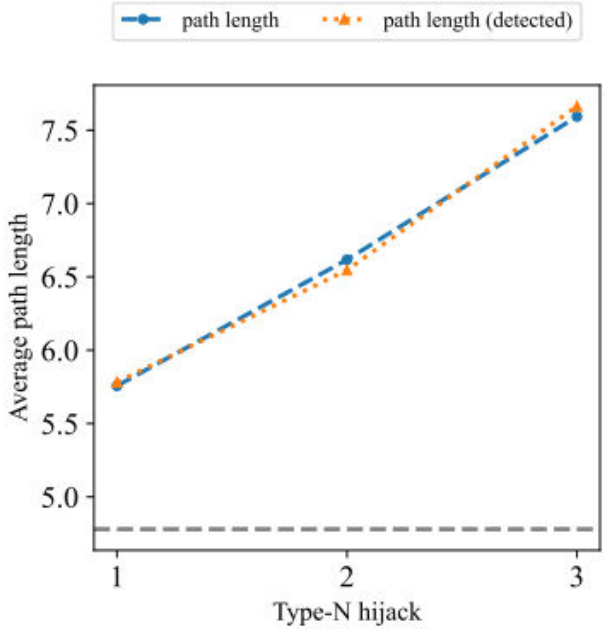
APNIC FOUNDATION

清華大學 Tsinghua University

Evaluation

- Type-N hijacking： N is the **length of fake segment** in the AS-PATH.
- Path hijacking
  - AS the N grows, the fake AS-PATHs will more likely to cause valley, traffic detour and longer AS-PATH.





APNIC FOUNDATION

清華大學 Tsinghua University

Evaluation

- Historical path hijacking detection
- 7 of 18 detected
- false negative reason:
  - 1. some hijackings (bitcanal, etc.) insert ASNs registered in the RIR but not used, thus bypassing Metis' Type-1 detection.
  - 2. Some hijackings insert real unseen links.

Event title	Hijack type	Type-1 link Number	Type-2 link Number	(sub)MOAS	Origin AS set Format	Alarm
bitcanal_3	subprefix	1	0	✓	{V,N}	✗
bitcanal_4	subprefix	1	0	✓	{V,N}	✗
petersburg_unused_1	unused	1	0	✗	{N}	✗
petersburg_unused_2	unused	1	0	✗	{N}	✗
petersburg_1	subprefix	1	0	✓	{V,N}	✗
petersburg_2	subprefix	1	0	✓	{V,N}	✗
Torg_1	prefix	0	2	✓	{V,O}	✗
Torg_2	prefix	0	2	✓	{V,O}	✗
Torg_3	prefix	0	2	✓	{V,O}	✗
backconnect_3	subprefix	2	5	✓	{V,H,O}	✓
backconnect_5	subprefix	0	2	✓	{V,O}	✓
backconnect_6	subprefix	0	2	✓	{V,H,O}	✓
france_1	subprefix	0	1	✓	{V,O}	✓
enzu_1	subprefix	0	3	✗	{V}	✓
facebook_1	subprefix	0	2	✗	{V}	✗
calson_1	subprefix	1	0	✓	{V,O,N}	✓
Defcon_1	subprefix	0	1	✓	{V,H}	✗
amazon_1	prefix	0	1	✗	{V1,V2}	✓

APNIC FOUNDATION

清華大學 Tsinghua University

Comments and Suggestions?

Contact us at: sec@cgtf.net

APNIC FOUNDATION

清華大學 Tsinghua University