APRICOT 2024
APNIC 57

BANGKOK, THAILAND
21 February – 1 March 2024

Developing a Collaborative BGP Routing Analyzing and Diagnosing Platform

Tsinghua University

APRICOT 2024

APNIC 57

March 1, 2024

APNIC FOUNDATION

清華大學 Tsinghua University

Outline

- Background
- BGP Hijacking Detection Algorithm
- Functionality of the BGPWatch Platform
- Future Work

#apricot2024
BANGKOK, THAILAND
21 February – 1 March 2024

APNIC FOUNDATION

清華大學
Tsinghua University

Collaborative Community

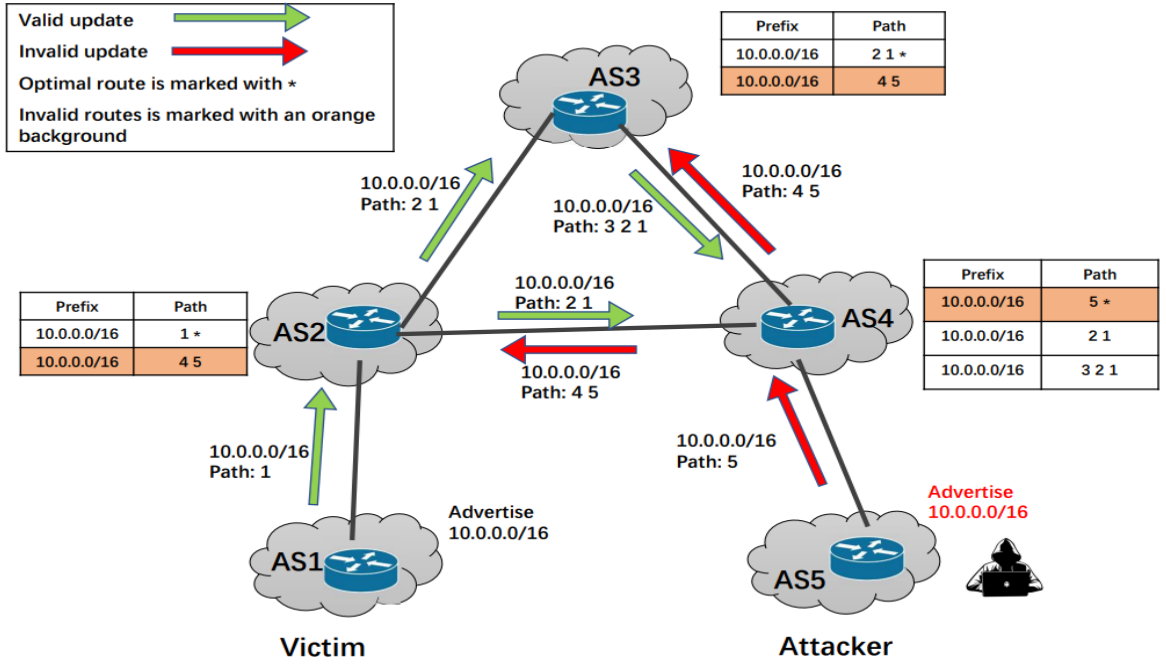
- **Work of 19 organizations (listed alphabetically)**
  - AARNET (AU)
  - APAN-JP (JP)
  - BdREN (BD)
  - CERNET (CN)
  - DOST-ASTI (PREGINET, PH)
  - ERNET (IN)
  - Gottingen University (DE)
  - HARNET (JUCC, HK)
  - ITB (ID)
  - KREONET (KR)
  - LEARN (LK)
  - MYREN (MY)
  - NREN (NP)
  - PERN (PK)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

APNIC FOUNDATION

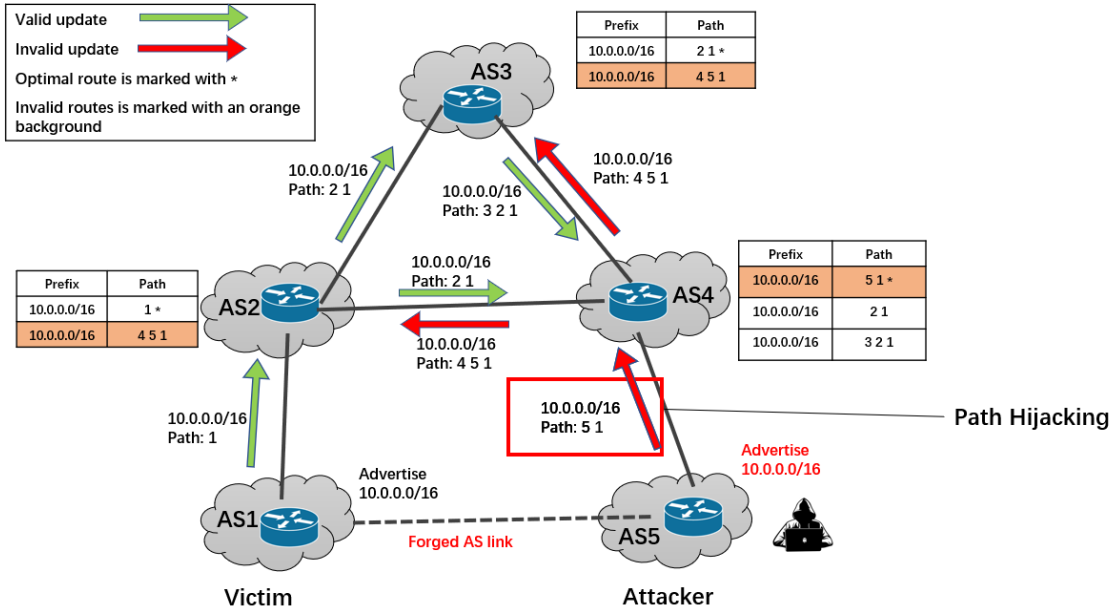
清華大學 Tsinghua University

BGP Hijacking

BGP hijacking often leads to catastrophic consequences



Prefix Hijacking



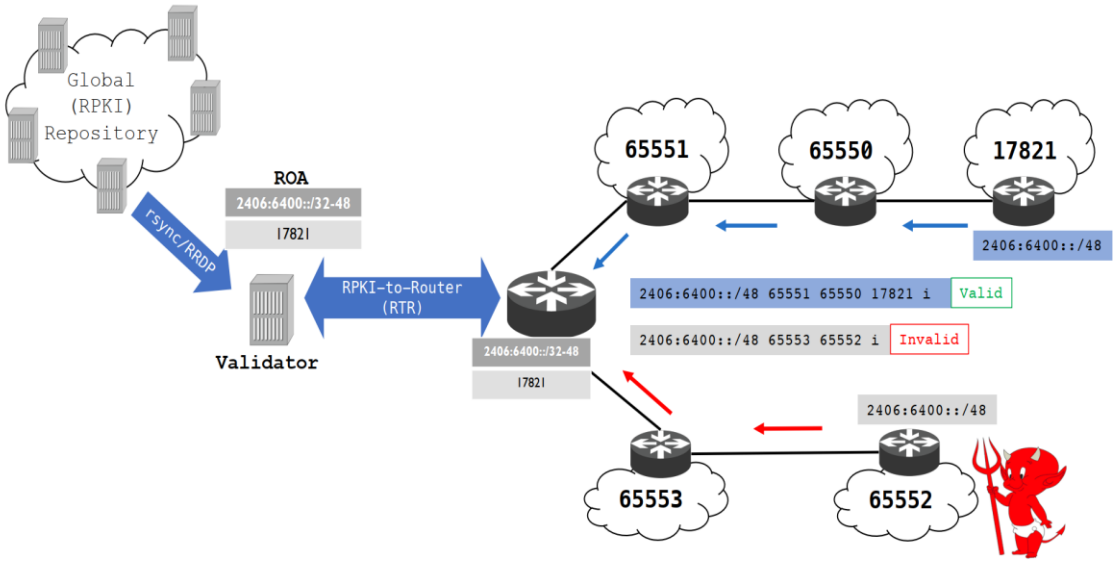
Path Hijacking

APNIC FOUNDATION

清華大學 Tsinghua University

Solutions to BGP Hijacking

- Preventing the hijacking before it happens
  - RPKI (Resource Public Key Infrastructure)
  - ASPA(Autonomous System Provider Authorization)
- Monitoring to detect the hijacking
  - Route Views
  - RIPE RIS
  - BGPstream
  - GRIP
- Mitigating the hijacking
  - Announcing a more specific prefix
  - Contact other networks to filter routes



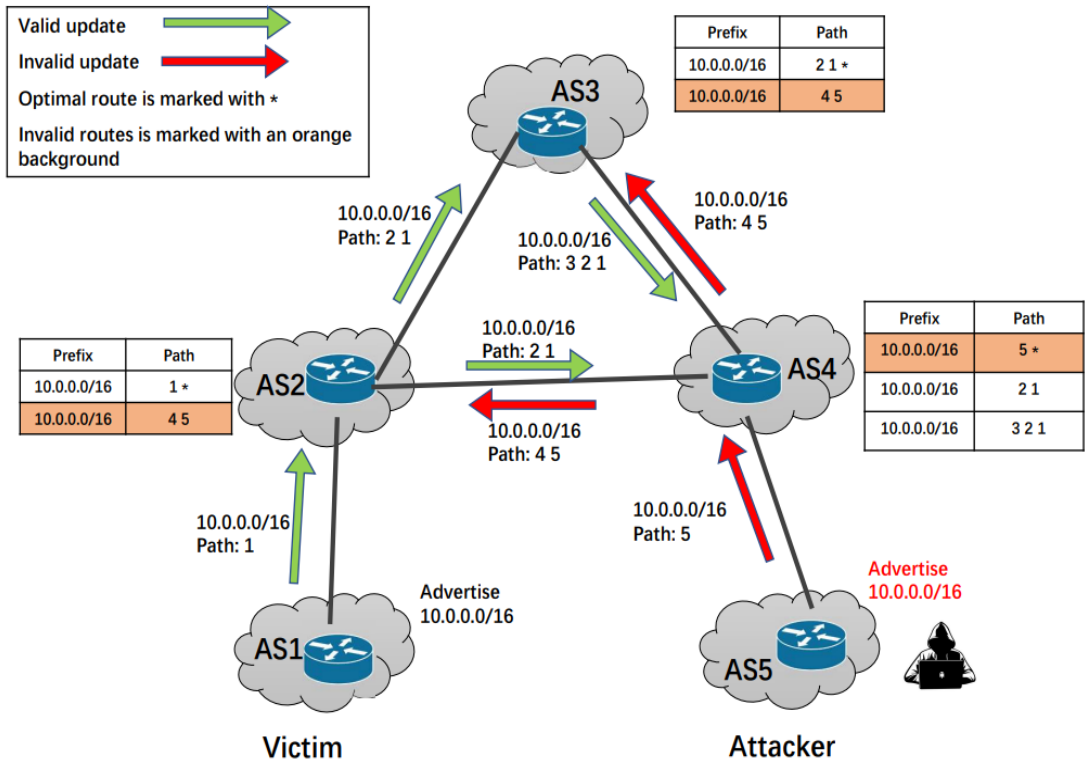
RPKI is very useful, but it's still in the process of deployment

APNIC FOUNDATION

清華大學 Tsinghua University

MOAS and BGP Prefix Hijacking

- MOAS (Multiple Origin AS) : A single IP prefix has multiple AS numbers claiming to be the origin for that prefix
- MOAS is a critical characteristic of source hijacking
- MOAS is not solely caused by hijacking
  - Multihoming
  - Traffic Engineering
  - DDOS Mitigating
  - Anycast Address

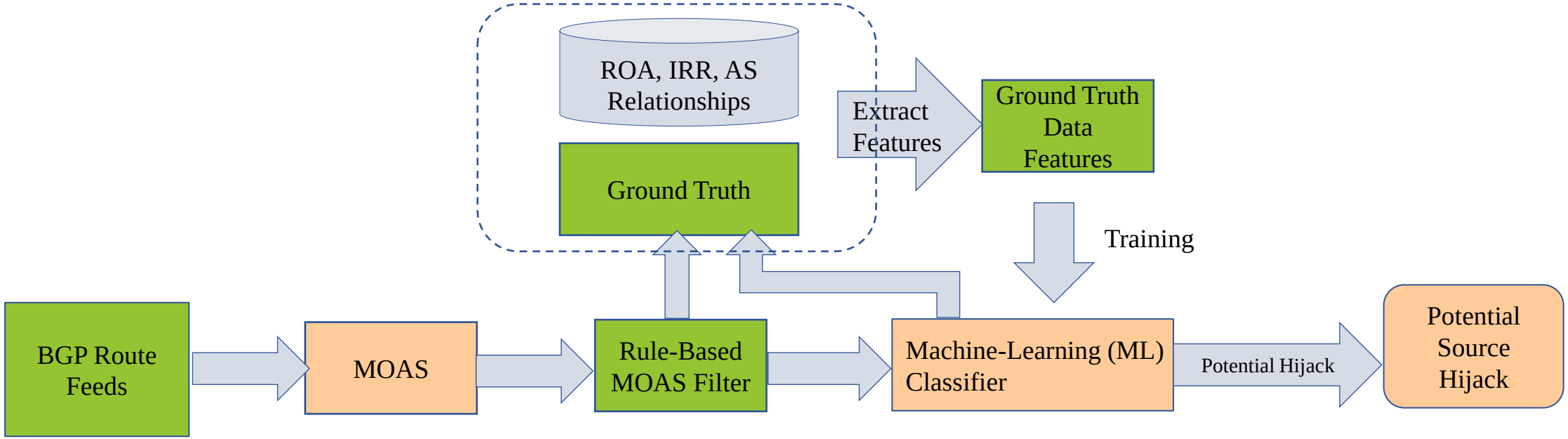


Determining the legitimacy of MOAS is a major challenge

APNIC FOUNDATION

清華大學 Tsinghua University

A Rules and Machine Learning Combined Method



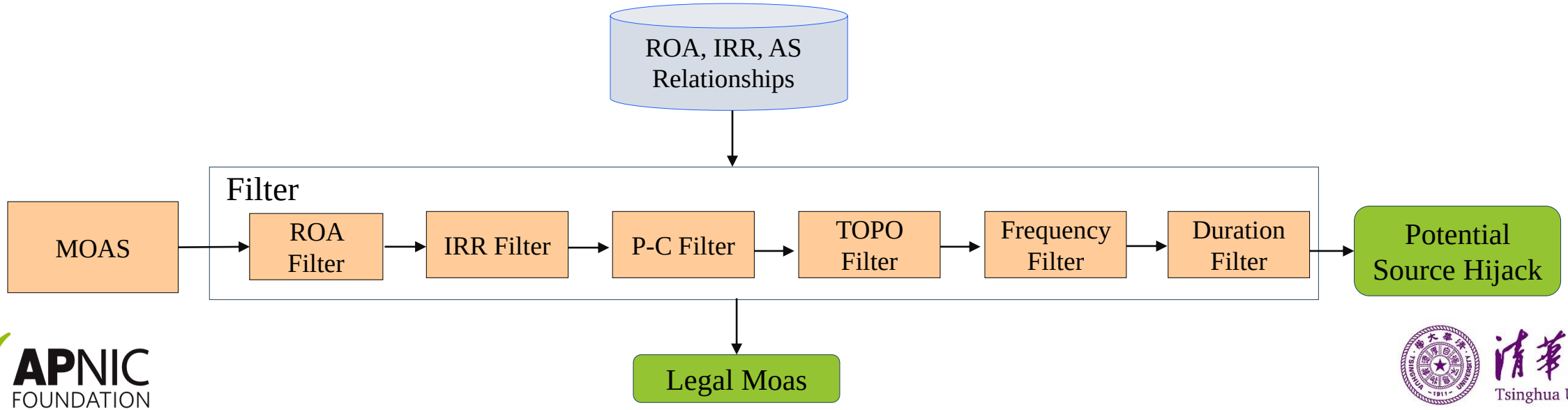
- Initially, train the machine learning classifier.
- During operation, the platform fetches BGP ROUTE feeds, extracts MOAS.
- Rule-based filters are used to sift through a large volume of legitimate MOAS.
- Then, the machine learning classifier is utilized to categorize the remaining MOAS.

APNIC FOUNDATION

Tsinghua University

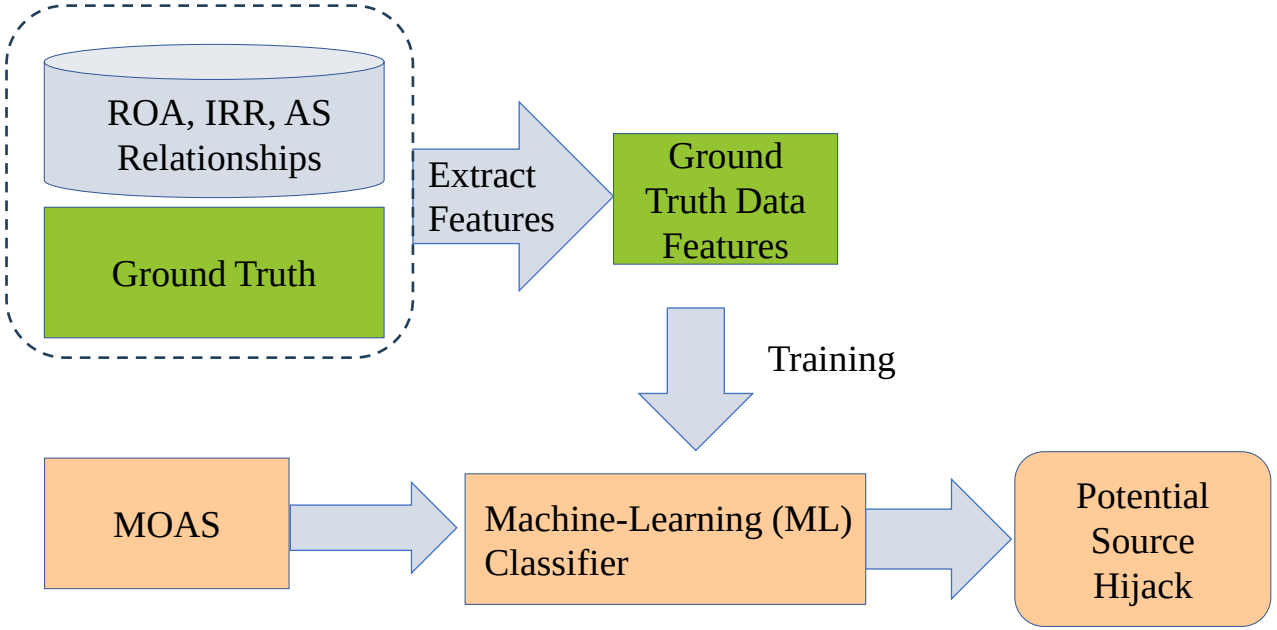
Rule based Filtering

- ROA Filter: Sync with public repository using Routinator, every minute
- IRR Filter: use Internet Routing Registries to assist in filtering, sync every day
- Provider-Customer Filter: CAIDA as relationship database
- TOPO Filter: Hijacker and Victim in the same AS-PATH
- Admin Filter: Same administrator etc., sync with WHOIS every day
- Frequency/Duration Filter: Frequency/Duration longer than a threshold



Machine Learning based Filtering

- Features
  - MOAS TYPE, AS Rank Difference, Business Relationship, Geographical Relationship,
  - Announcement Activity, Hijacking Activity,
  - Edit Distance of AS name, org, desc,
  - AS type, Degree and Coreness of AS,
  - Prefix type
- Classifier
  - Extreme Randomized Trees



Result:

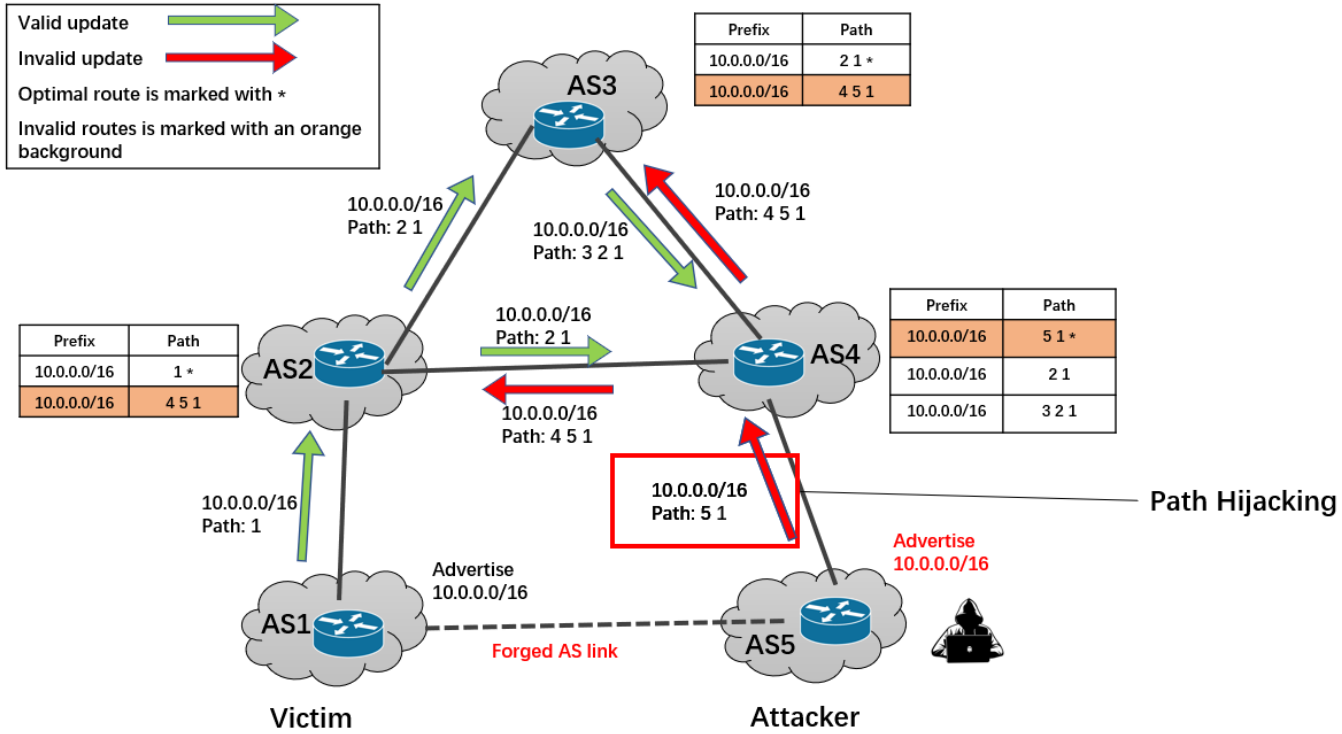
Precision	Recall	Accuracy
0.9410	0.9570	0.9622

APNIC FOUNDATION

清華大學 Tsinghua University

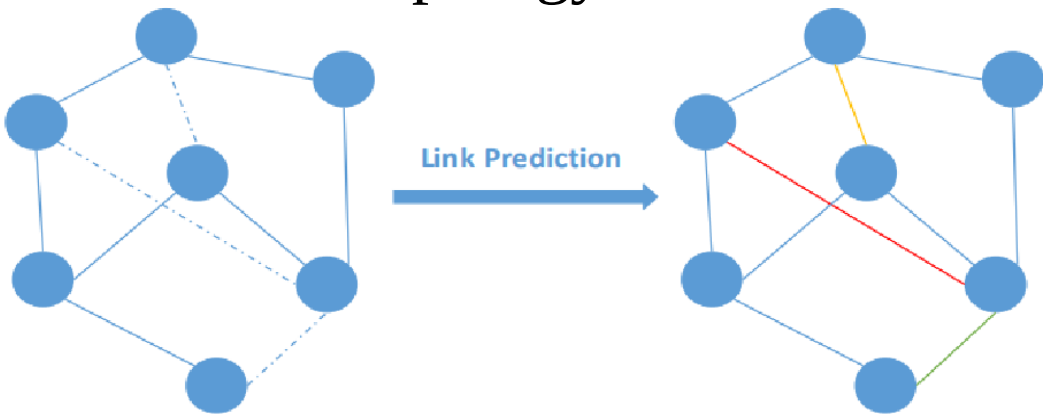
Path Hijacking Detection

- Path hijacking can evade MOAS, but usually cause unseen AS link
- State of the art detection technique
  - 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
  - Intense data-plane workload
  - Inefficient and difficult to guarantee real-time



Detecting Fake AS-PATHs based on Link Prediction

- Evaluate the authenticity of unseen links with link prediction and filter 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? Graph characteristics of AS-level topology
  - Power-law distribution
  - Negative degree-degree correlation
  - Hierarchical structure
  - AS links usually connect two ASes with the same properties

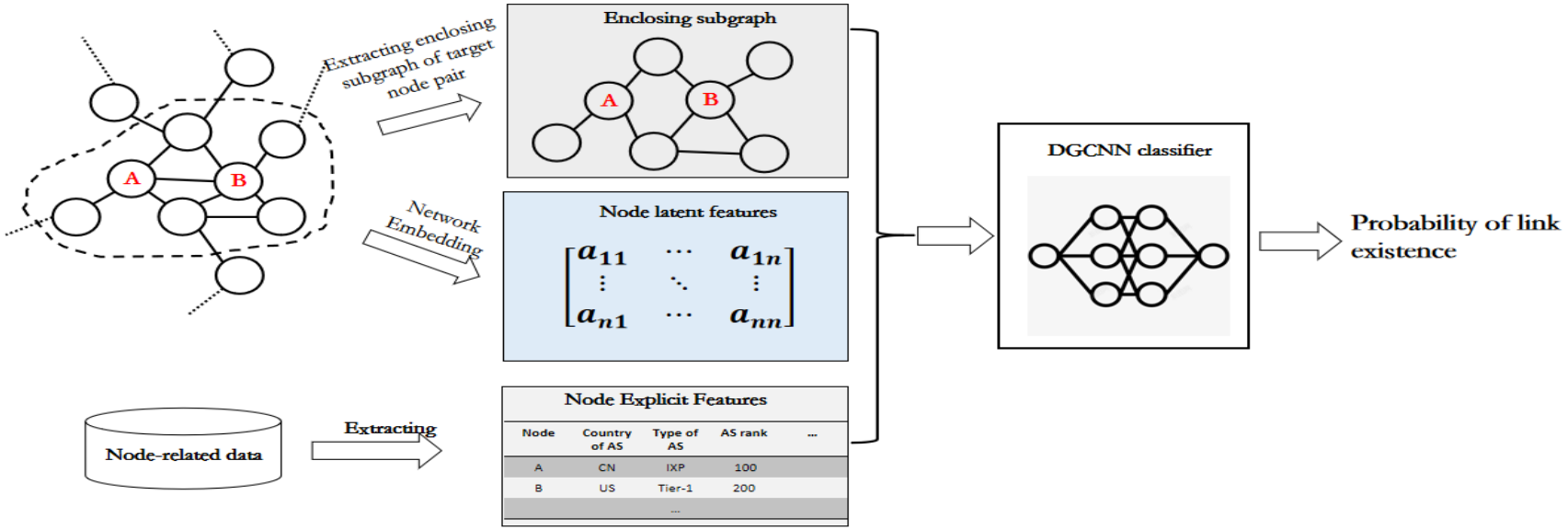


APNIC FOUNDATION

清華大學 Tsinghua University

Unseen Link Prediction

- Select Deep Graph Convolutional Neural Network (DGCNN) as the link prediction algorithm
- CAIDA AS relationship & AS location、 type and rank
- Training with positive and negative samples
- The accuracy reached 0.95 and the AUC reached 0.98

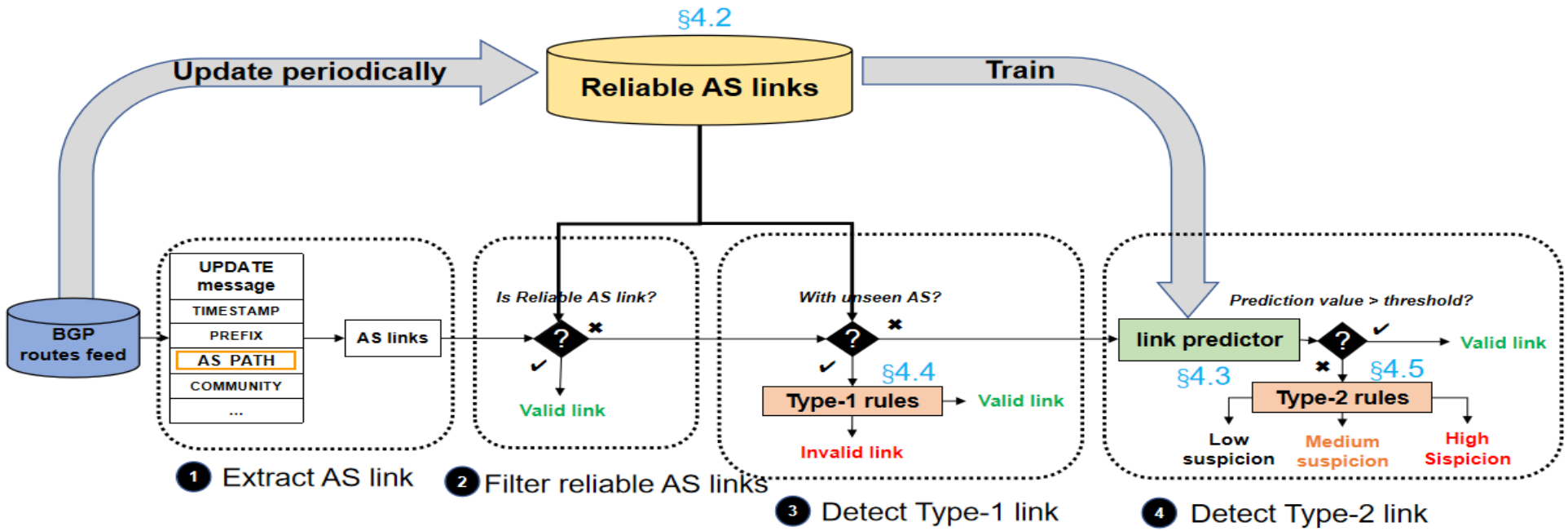


APNIC FOUNDATION

清華大學 Tsinghua University

Framework: Combining Link Prediction and Rules

- Link prediction is used to find suspicious unseen links, and rules are used to improve the confidence level
- The accuracy of positive AS-PATHs is about 99.5%
- The accuracy of Type-1 path hijacking is 87.5%



APN FOUNDA

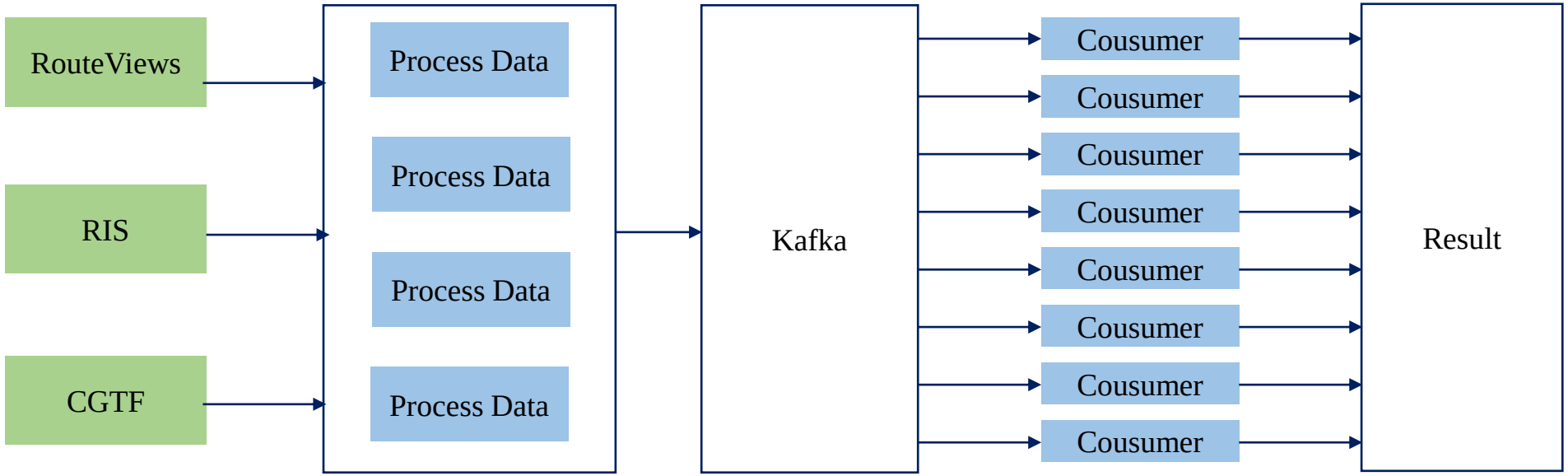
清華大學 Tsinghua University

Rules

- If any rules are successfully matched, the suspicious score is increasd by 1.
  - The number of unique ASes in AS-PATH is greater than the pre-set threshold.
  - The suspicious link with a single-digit ASN at the end of the AS-PATH.
  - The Damerau-Levenshtein edit distance of the two ASNs of the suspicious link is no more than 1.
  - The AS-PATH has AS loop, and the link is in the loop.
  - The AS-PATH violates the valley-free rule.
  - The AS-PATH causes traffic detour.
- When a path score reaches a threshold, it is judged as hijacking.

Parallel Computing and Clusters to Handle Big Routing Data

- There is a huge amount of routing data from RouteViews, RIS, CGTF.
- We improved the system by Parallel Computing and Clusters.



APNIC FOUNDATION

清華大學 Tsinghua University

Evaluate Harm Level

- Use Prefix information and AS information to evaluate Harm Level

high level

Ongoing Possible Hijack Events

103.120.14.0/24-hijack1708563695 Ongoing Possible Hijack Events

Victim AS: 397423
Victim Country: US (United States)
Victim AS Name: TIER-NET
Start Time: 2024-02-22 01:01:35
During Time: no data

Hijacker AS: 147287
Hijacker Country: IN (India)
Hijacker AS Name: DATAPARA1-AS-IN
End Time: no data
Time Zone: UTC

Reason:

- (397423, 103.120.14.0/24) aligns in ROA
- (147287, 103.120.14.0/24) doesn't align in ROA
- (397423, 103.120.14.0/24) doesn't align in WHOIS
- (147287, 103.120.14.0/24) doesn't align in WHOIS

Prefix Info: 103.120.14.0/24

Website:

mirrorworld.space	fitnesshub.shop	vrbaseball.xyz	voteit2020.online	podologe.online	healthpro.store	vinsabienesraices.website
fritolay.store	twinkletwinkle.website	waterlevel.online	mailout.xyz	opencompute.life	seniorservices.website	theneo.shop
cdao.website	compareit.online	vimax.space	tomate.store	adera.store	t-app.xyz	mediabuzz.xyz

Domains in Prefix and AS TYPE

- TOP 1M domain:
  - Tranco: https://tranco-list.eu/
  - Cloudflare: https://radar.cloudflare.com/domains
- Convert domain name to IP Prefix

- Get AS type from ASdb:
  - https://asdb.stanford.edu/
  - ASdb is a research dataset that maps ASN to organizations and industry types using data from business intelligence databases, website classifiers, and a machine learning algorithm.
  - Hosting and Cloud Provider

APNIC FOUNDATION

清華大學 Tsinghua University

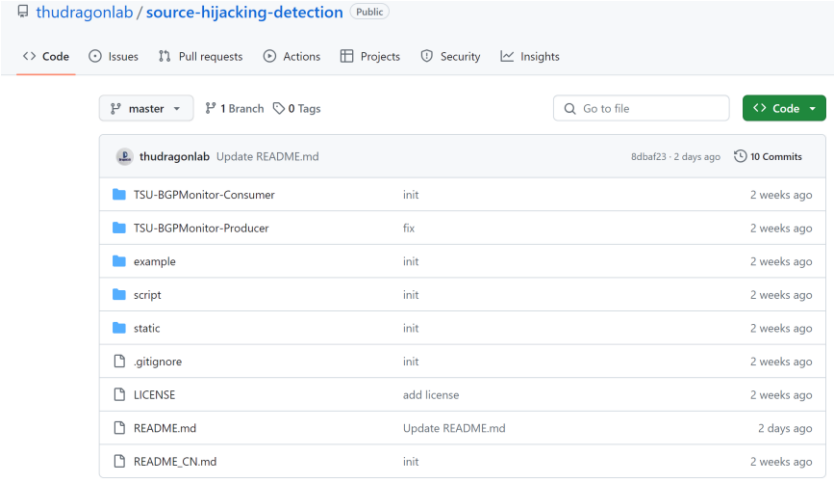
Open Source

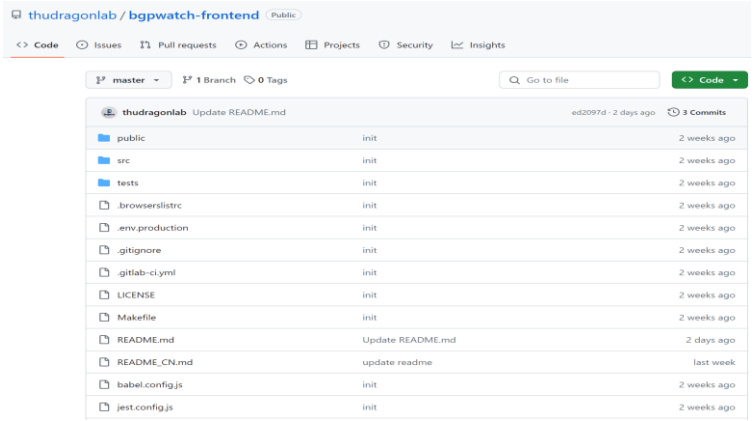
https://github.com/thudragonlab/source-hijacking-detection

https://github.com/thudragonlab/bgpwatch-frontend

https://github.com/thudragonlab/bgpwatch-backend

https://github.com/thudragonlab/bgp-analysis





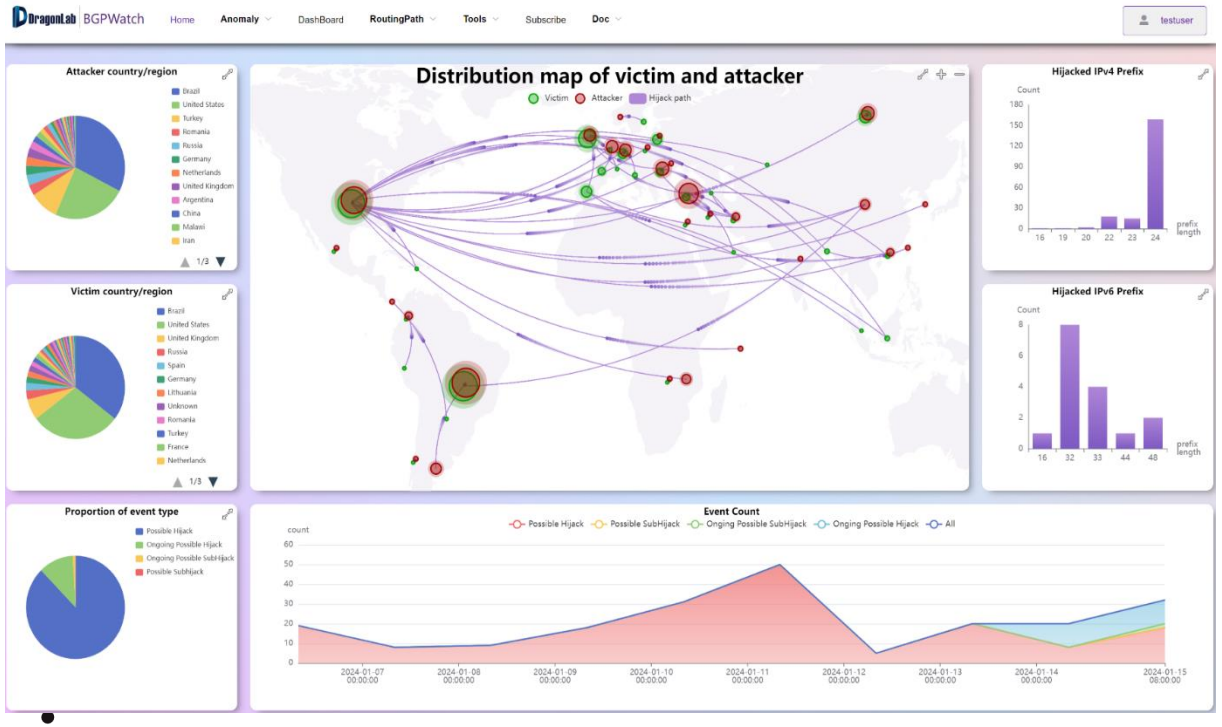
APNIC FOUNDATION

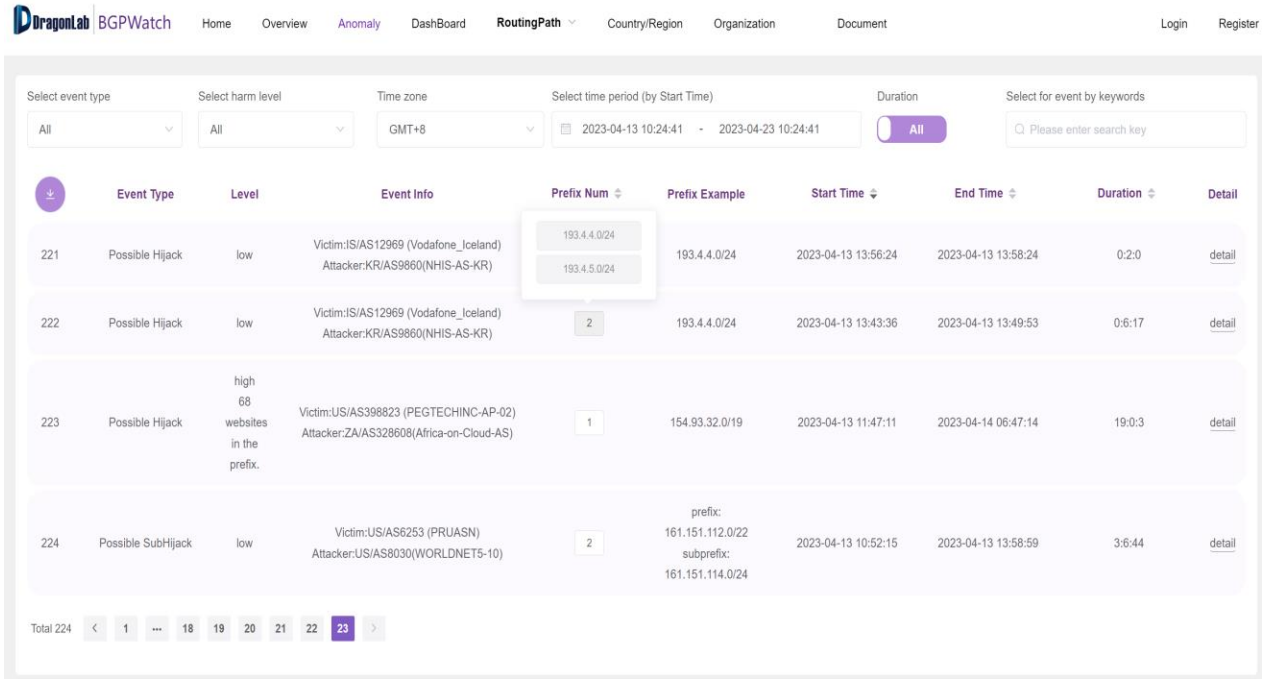
清華大學 Tsinghua University

BGPWatch: Prefix Hijacking Detection Platform

- 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, routing path, accumulated information, etc.)





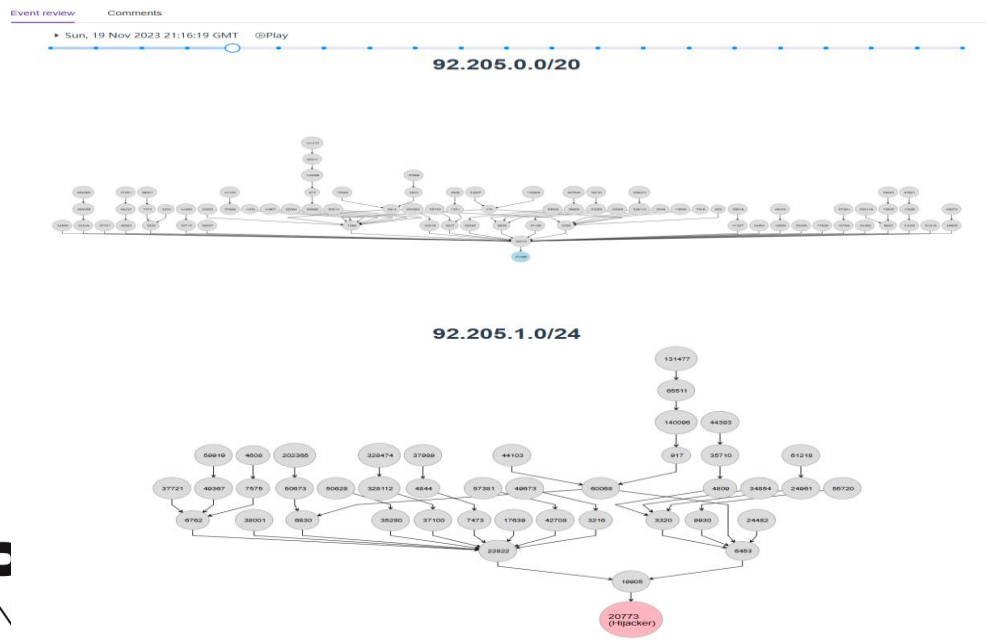
APNIC FOUNDATION

https://bgpwatch.cgtf.net

清華大學 Tsinghua University

Quick Response, Event replay, Comments

- About 5 mins delay
- Notify users immediately when an event is detected, minimizing damage from hijackings
- Event replay can help users understand the procedure, and analyze the extent of the impact of the event
- Comments from users can help improve the platform



Tsinghua University

Subscribe Hijacking Events for AS and Send Alarm

Prefix Change | Hijack | AS Peer Change | AS Path Change

Select event type: All
Select harm level: All
Time zone: GMT+8
Select time period (by Start Time): 2023-11-10 10:22:41 - 2023-11-20 10:22:41
Duration: All
Select for event by keywords: 945

	Event Type	Level	Event Info	Prefix Num	Prefix Example	Start Time	End Time	Duration	Detail	Comment
1	Possible Hijack	low	Victim:TW/AS945(8964) Attacker:US/AS200827(VV-NETWORK)	1	23.150.11.0/24	2023-11-19 11:01:13	2023-11-19 11:15:16	0:14:3	detail	
2	Possible Hijack	low	Victim:TW/AS945(8964) Attacker:US/AS200827(VV-NETWORK)	1	23.150.11.0/24	2023-11-19 09:00:47	2023-11-19 09:15:20	0:14:33	detail	
3	Possible Hijack	low	Victim:TW/AS945(8964) Attacker:US/AS200827(VV-NETWORK)	1	23.150.11.0/24	2023-11-18 19:00:46	2023-11-18 19:15:19	0:14:33	detail	

Hi,

Hope this message finds you well. Greetings from the Institute for Network Sciences and Cyberspace at Tsinghua University. We have developed a BGP hijacking detection system (BGPWatch, https://bgpwatch.cgtf.net).

Our system shows that prefix 23.150.11.0/24 is normally announced by your 945; however, at 2023-11-18 11:00:46 (UTC), prefix 23.150.11.0/24 is also announced by 200827 Detailed information is available here.

We would like to confirm with you whether this is a hijacking event or a false alarm of the system. Please click here to provide us with your feedback. Your time and response are greatly appreciated and will be very helpful for our research.

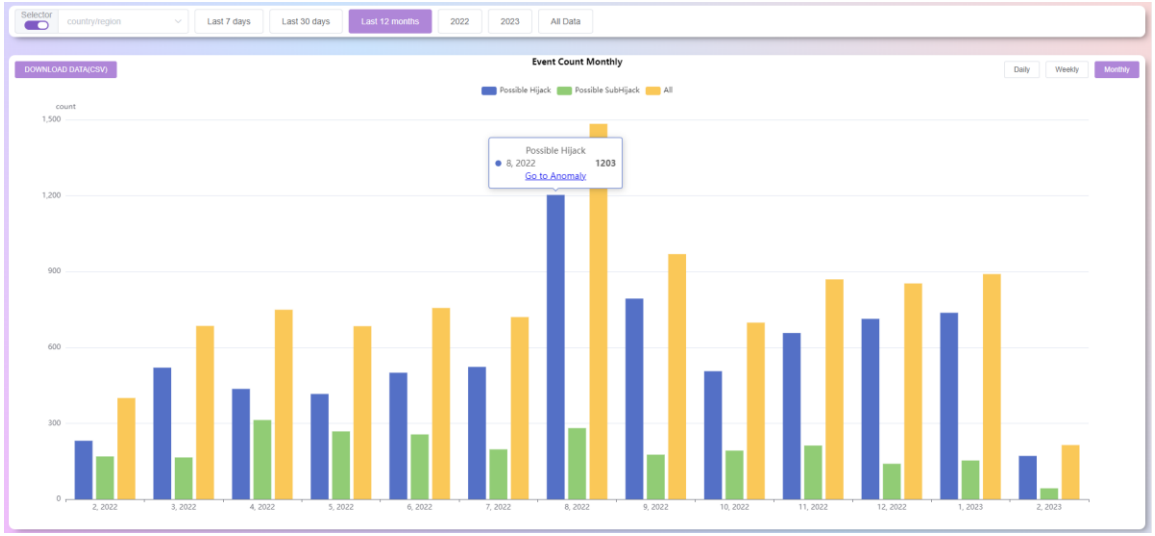
Have a good day!

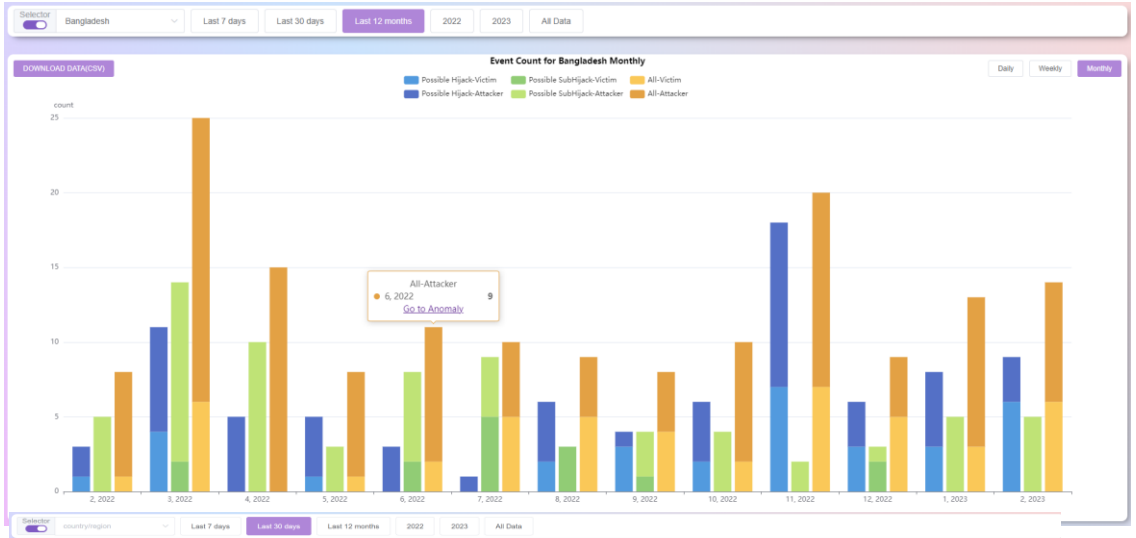
Best regards,
Institute for Network Sciences and Cyberspace
Tsinghua University

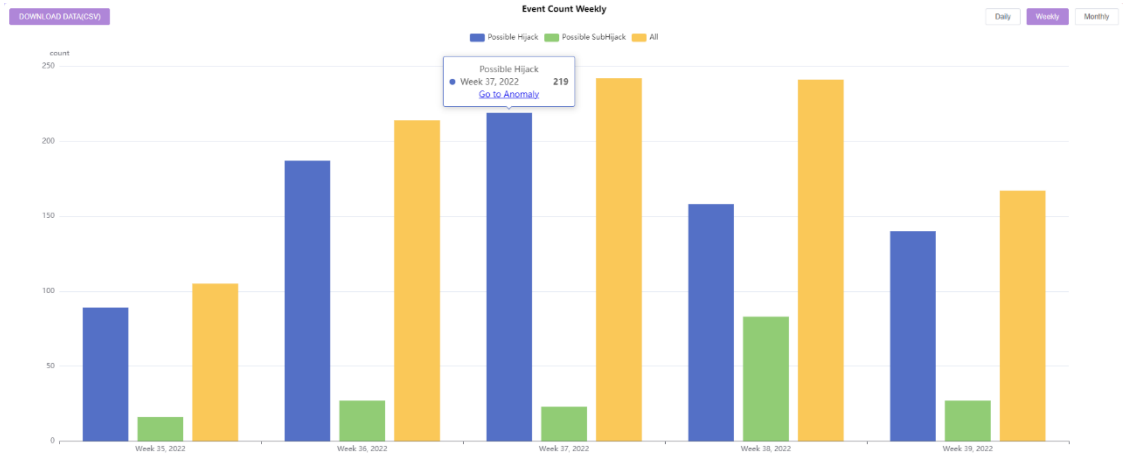
APNIC FOUNDATION

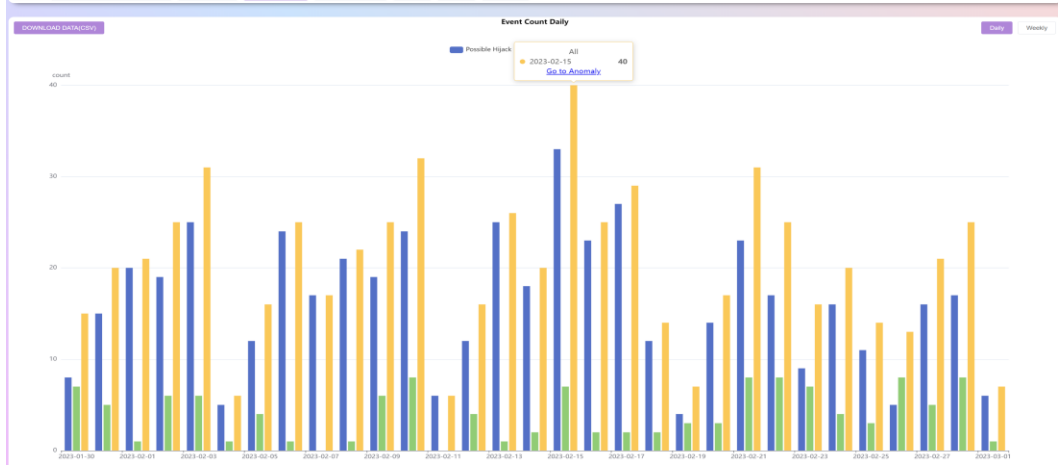
華大學 ua University

Overview--Statistics for Anomaly Events









Do statistics by economy, AS,

and by yearly, monthly, weekly, and daily

Compare with other Platforms

GRIP: Violate ROA

Potential Victims	Potential Attackers	Largest (Sub)Prefix	# Prefix Events	Start Time	Duration	Suspicion	Category	Type
USAS834 NLAS49981	PTAS24768	185.206.250.0/24	1	2023-11-15 15:15	5 hour	High	Default Tr Worthy	moas

BGPWatch: Compliant with ROA

Possible Hijack	low	Victim:PT/AS24768(ALMOUROLTEC) Attacker:US/AS834(IPXO)	1	185.206.250.0/24	2023-11-15 23:18:07	2023-11-16 04:25:30	5:7:23	deta

ROA

ASN	Prefix	Max Length
AS24768	185.206.250.0/24	24

APNIC FOUNDATION

清華大學 Tsinghua University

Compare with other Platforms

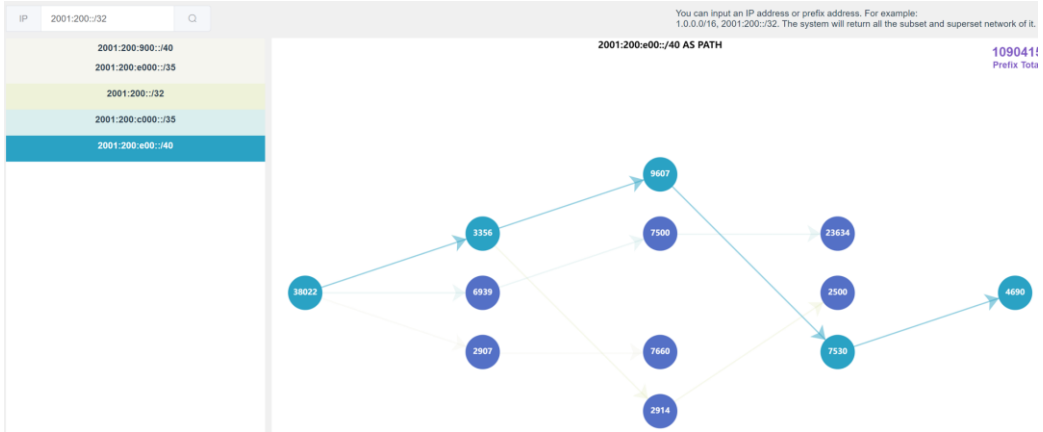
	BGPWatch	GRIP	BGPStream
Delay	5mins delay	5mins delay	More than 2 hours
Event replay	√	×	√
Event statistical analysis	√	×	×
Event level evaluation	√	×	×
Benign MOAS report	√	√	×
Email Alarm	√	×	×
Accuracy	High	Medium to High	Low

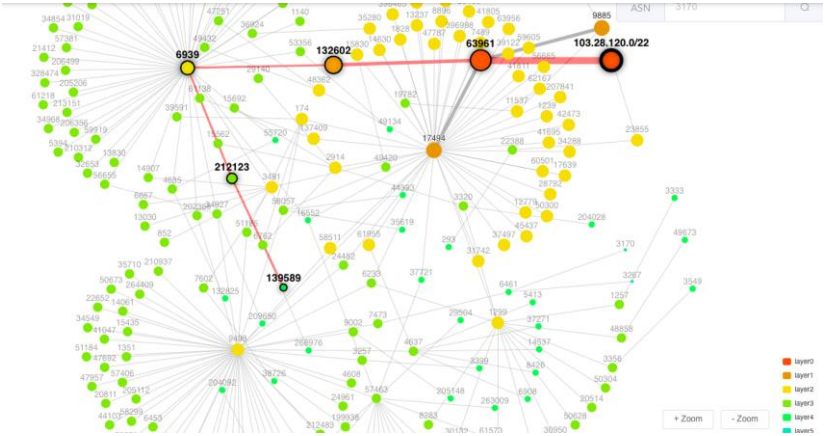
APNIC FOUNDATION

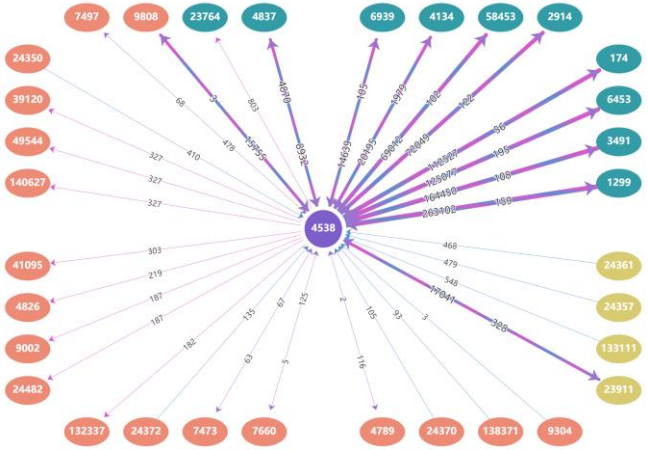
清華大學 Tsinghua University

Tools for Network Operator

- Dashboard: AS info, prefix, peers
- Routing Search：
  - Aggregated forward routing path
  - Reverse routing path
  - Bi-direction routing path
- Subscribing, Alarming

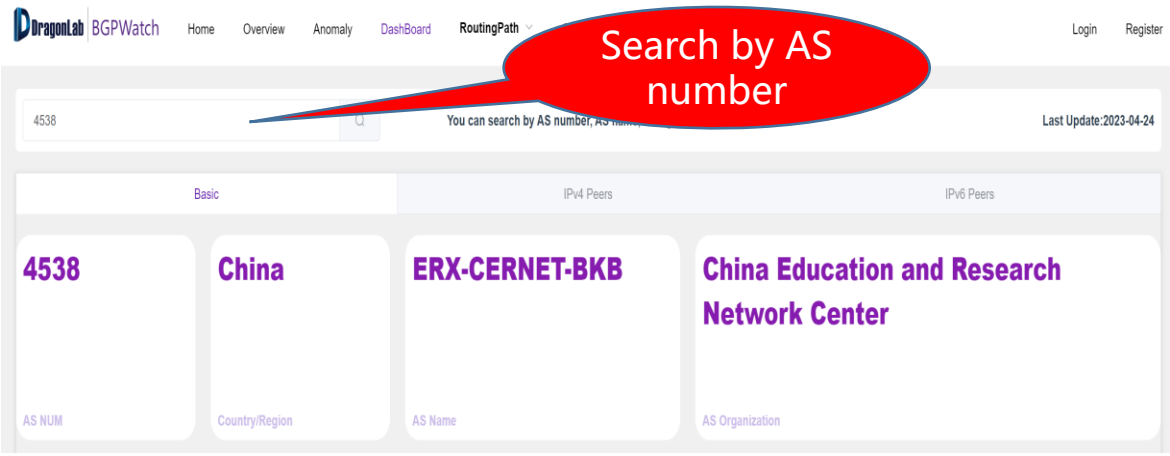


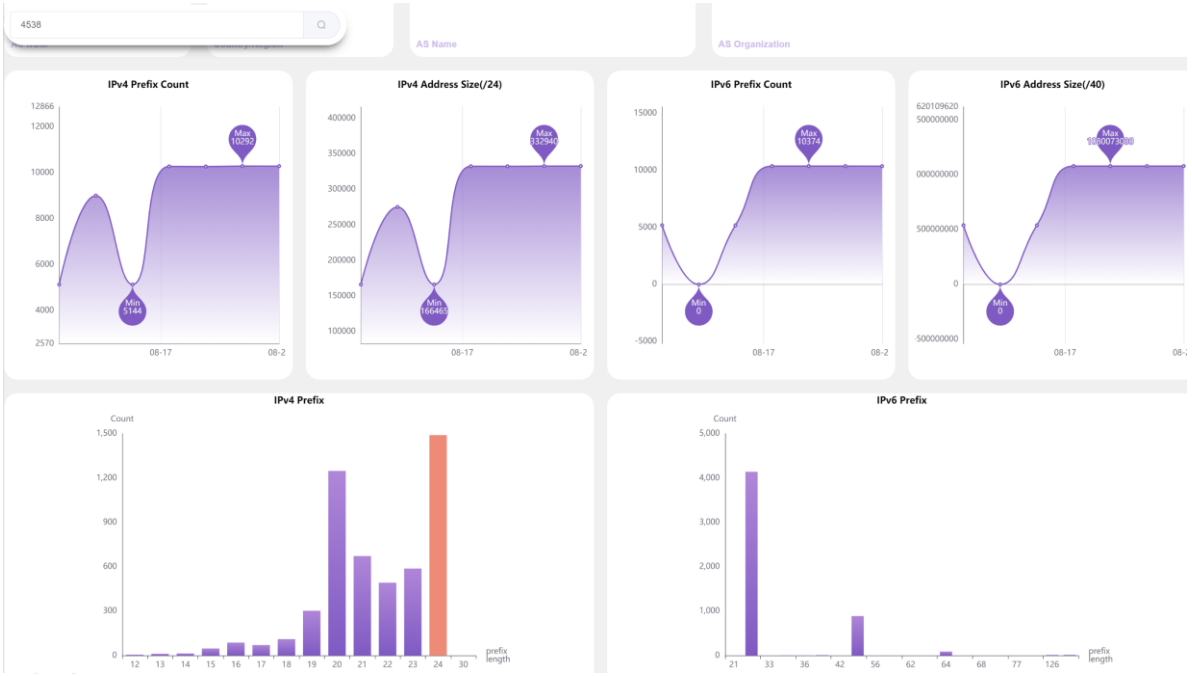


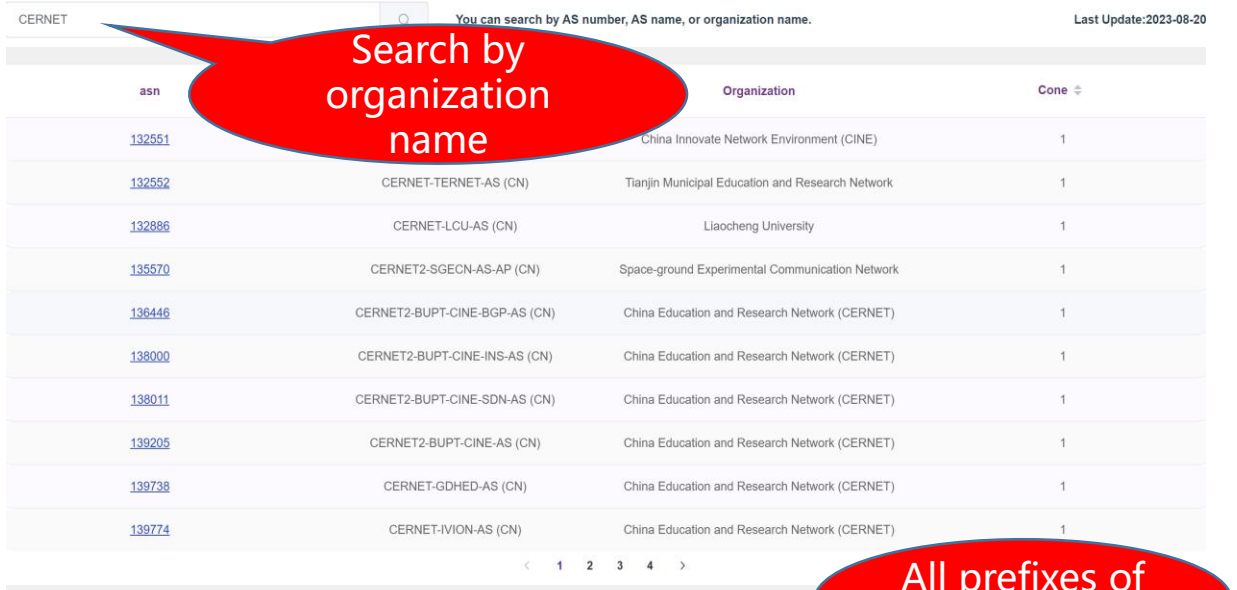


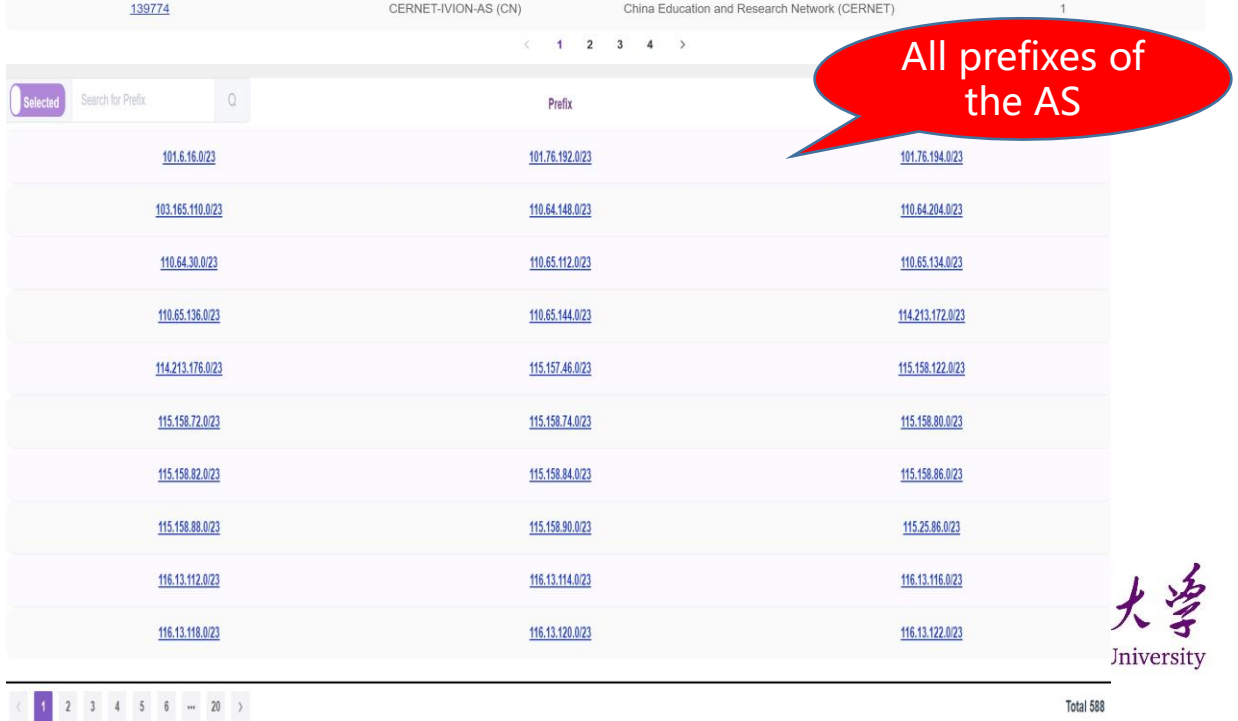
https://bgpwatch.cgtf.net

Dashboard

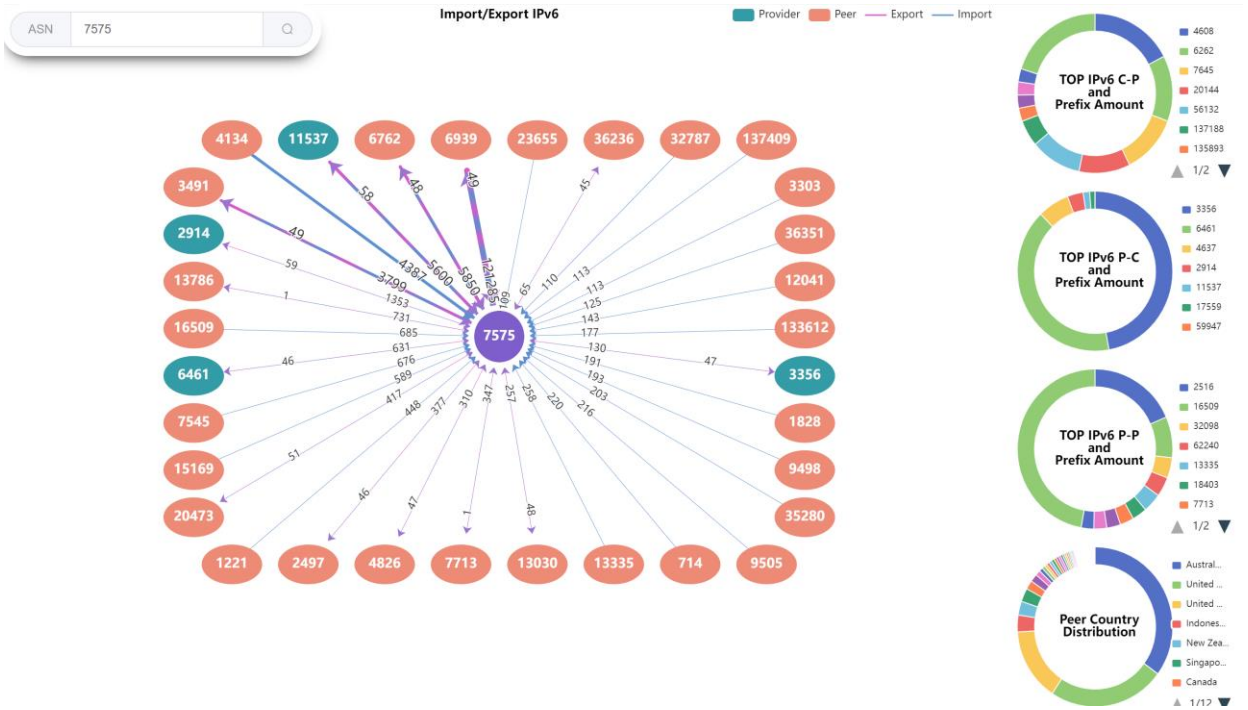

DragonLab BGPWatch
Home
Overview
Anomaly
DashBoard
RoutingPath
Login
Register
Search by AS number
4538
You can search by AS number, AS name, or organization name.
Last Update:2023-04-24
Basic
IPv4 Peers
IPv6 Peers
4538
AS NUM
China
Country/Region
ERX-CERNET-BKB
AS Name
China Education and Research Network Center
AS Organization


IPv4 Prefix Count
IPv4 Address Size(/24)
IPv6 Prefix Count
IPv6 Address Size(/40)
IPv4 Prefix
IPv6 Prefix

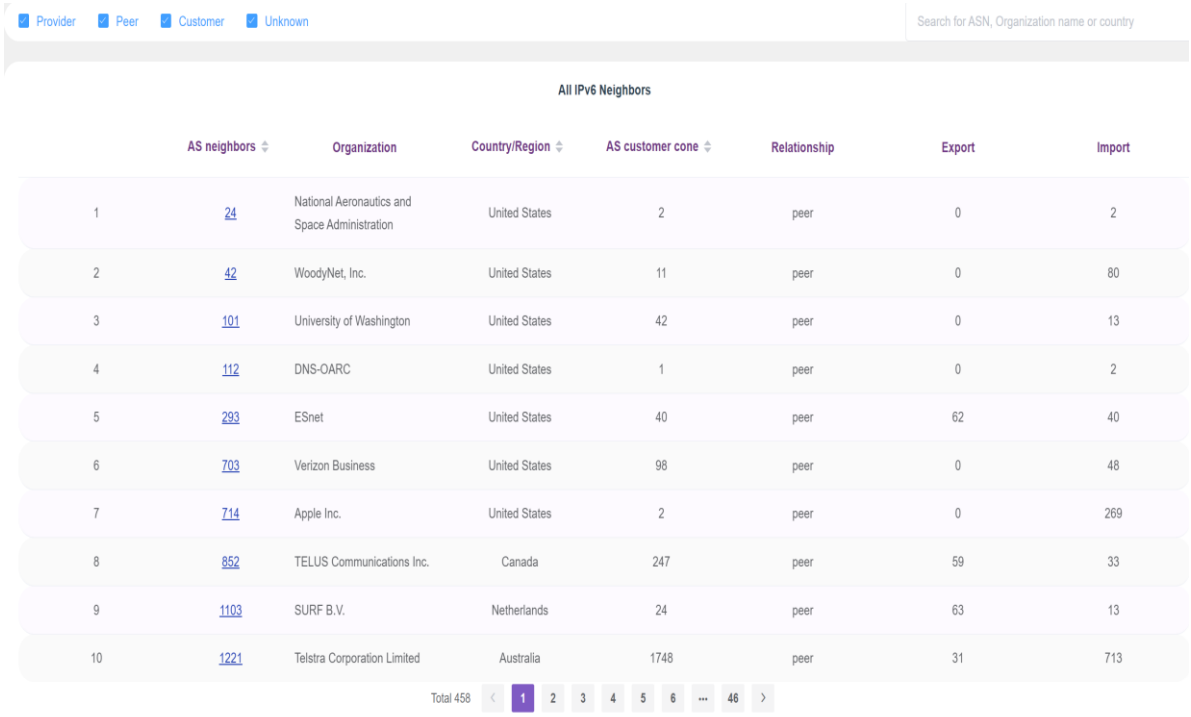

CERNET
You can search by AS number, AS name, or organization name.
Last Update:2023-08-20
Search by organization name
asn
Organization
Cone
132551
China Innovate Network Environment (CINE)
132552
CERNET-TERNET-AS (CN)
Tianjin Municipal Education and Research Network
132886
CERNET-LCU-AS (CN)
Liaocheng University
135570
CERNET2-SGECN-AS-AP (CN)
Space-ground Experimental Communication Network
136446
CERNET2-BUPT-CINE-BGP-AS (CN)
China Education and Research Network (CERNET)
138000
CERNET2-BUPT-CINE-INS-AS (CN)
138011
CERNET2-BUPT-CINE-SDN-AS (CN)
139205
CERNET2-BUPT-CINE-AS (CN)
139738
CERNET-GDHED-AS (CN)
139774
CERNET-IVION-AS (CN)


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 Neighbors



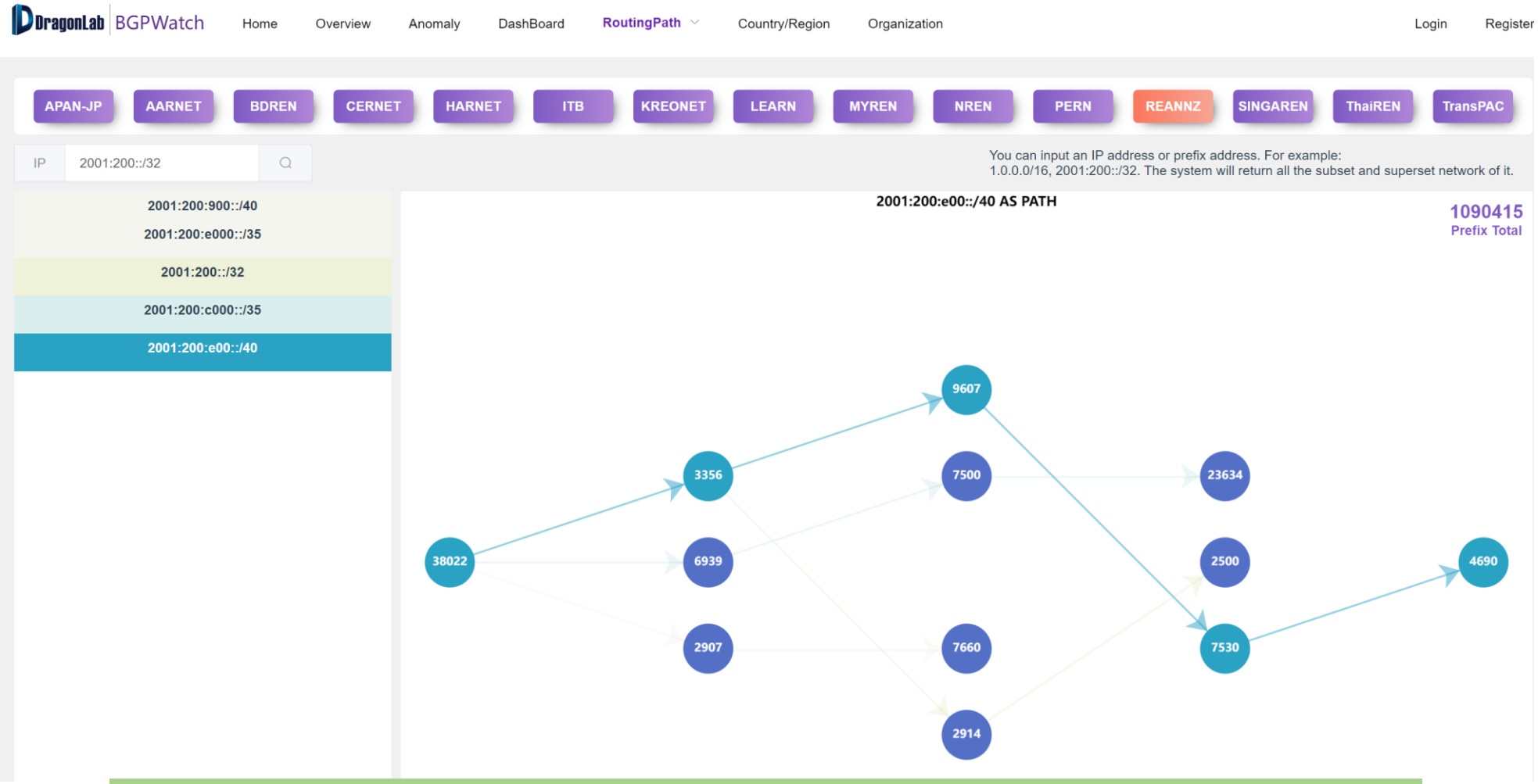
	AS neighbors	Organization	Country/Region	AS customer cone	Relationship	Export	Import
1	24	National Aeronautics and Space Administration	United States	2	peer	0	2
2	42	WoodyNet, Inc.	United States	11	peer	0	80
3	101	University of Washington	United States	42	peer	0	13
4	112	DNS-OARC	United States	1	peer	0	2
5	293	ESnet	United States	40	peer	62	40
6	703	Verizon Business	United States	98	peer	0	48
7	714	Apple Inc.	United States	2	peer	0	269
8	852	TELUS Communications Inc.	Canada	247	peer	59	33
9	1103	SURF B.V.	Netherlands	24	peer	63	13
10	1221	Telstra Corporation Limited	Australia	1748	peer	31	713

All Neighbors

APNIC FOUNDATION

清華大學 Tsinghua University

Multiple Routing Path Search

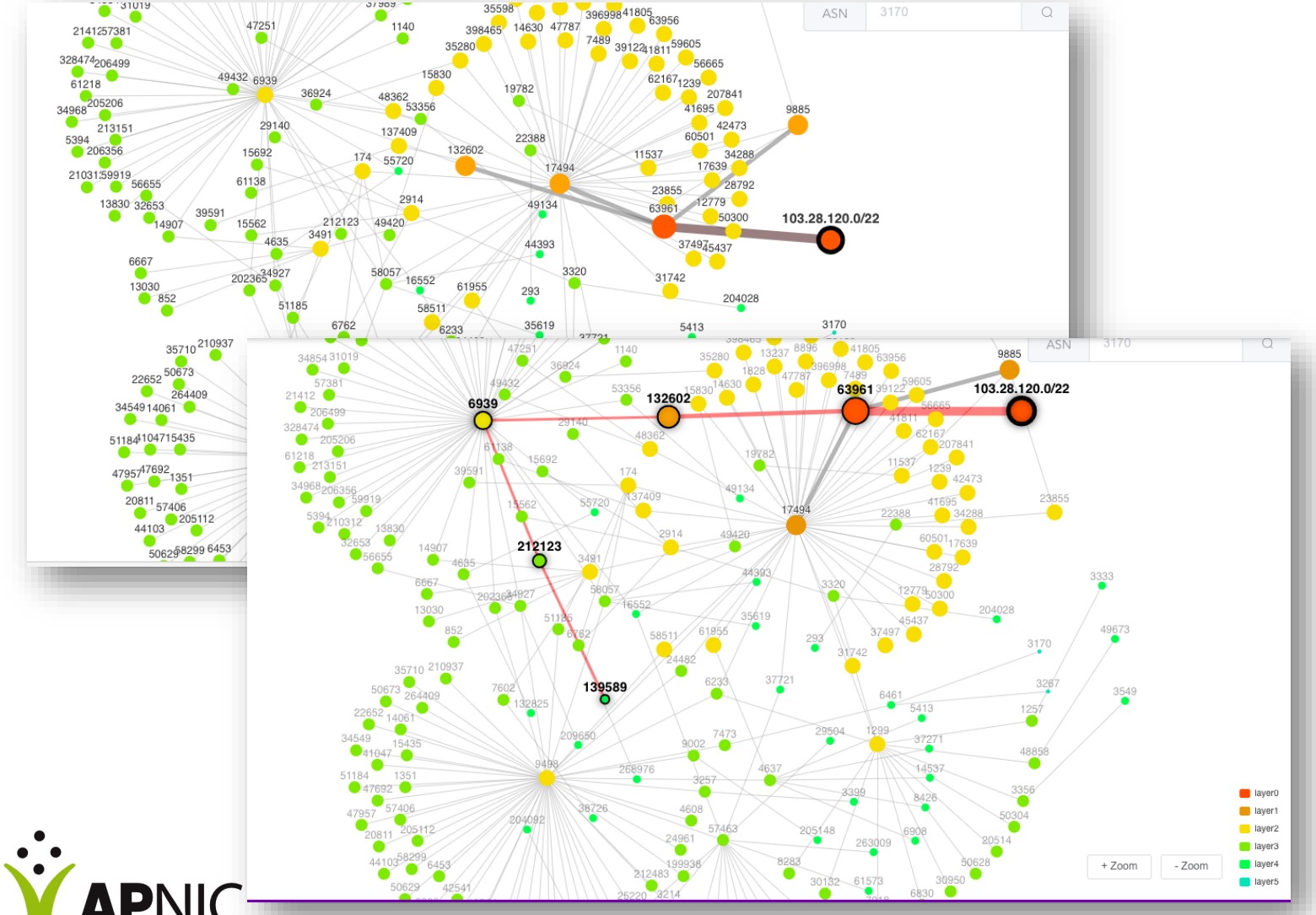


Support Prefix / IP, IPv4 / IPv6
Return paths of all sub networks and super networks of the input prefix
Group prefixes with the same routing path

APNIC FOUNDATION

清華大學 Tsinghua University

Reverse Routing Path (TOPO)

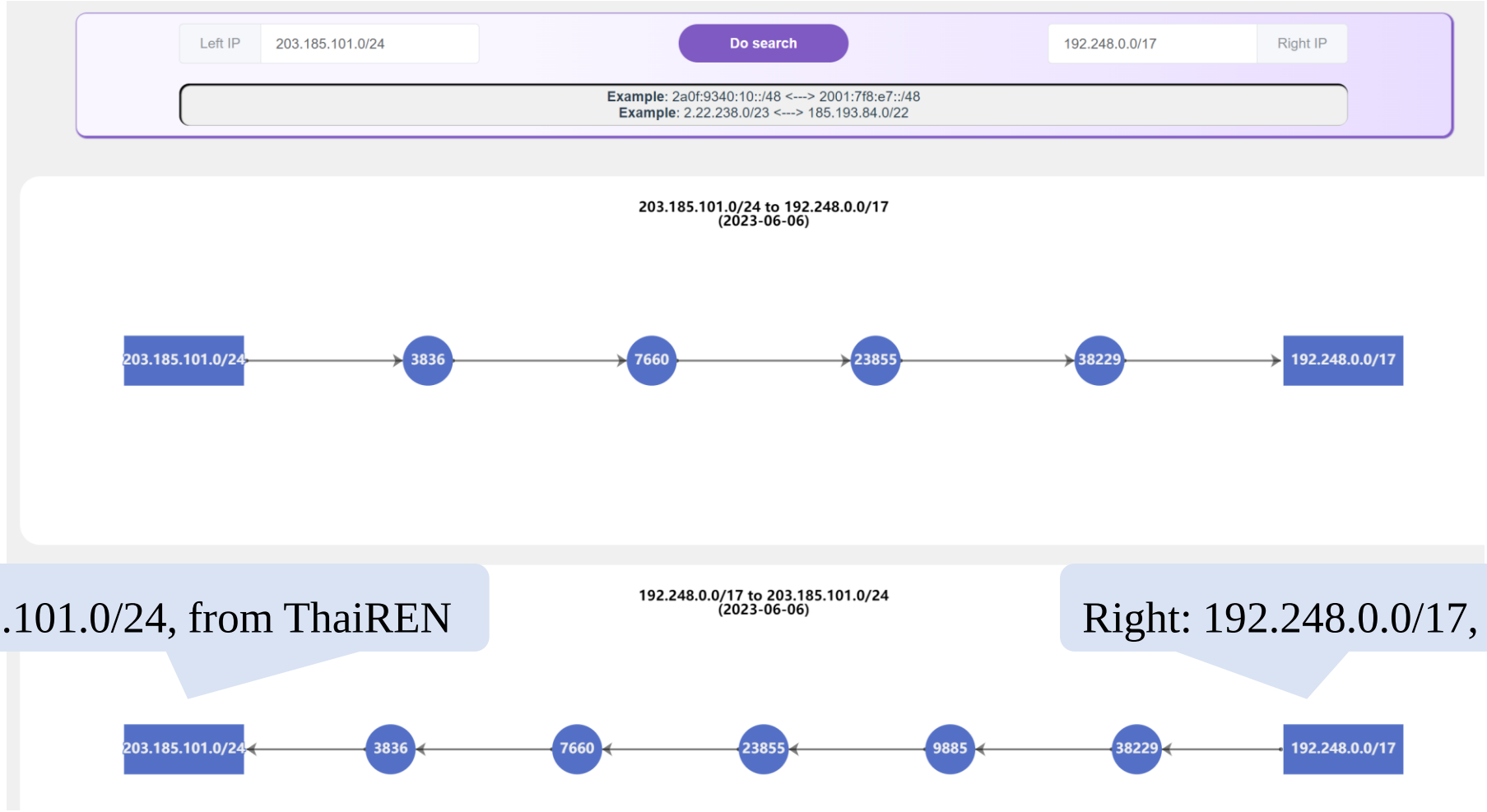


- Support Prefix / IP, IPv4 / IPv6
- The system will search the best matched prefix and return the reverse routing tree
- With better interactivity
- Click an AS or input AS number, the system will highlight the path to the AS
- The number of layers to display can be selected

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

Path Change

113.21.208.0/24 × | 170.114.134.0/23 | 66.175.208.0/21

Date:2024-02-15
Prefix:113.21.208.0/24

AS path

3662 → 4635 → 45474 → 17824 → 3491 → 3257 → 45474 → 6453 → 45474 → 113.21.208.0/24

Date:2024-02-16
Prefix:113.21.208.0/24

AS path

3662 → 4635 → 45474 → 17824 → 3491 → 6453 → 45474 → 3257 → 45474 → 113.21.208.0/24

Date:2024-02-17
Prefix:113.21.208.0/24

AS path

3662 → 4635 → 45474 → 17824 → 3491 → 6453 → 45474 → 3257 → 45474 → 113.21.208.0/24

APNIC FOUNDATION

清華大學 Tsinghua University

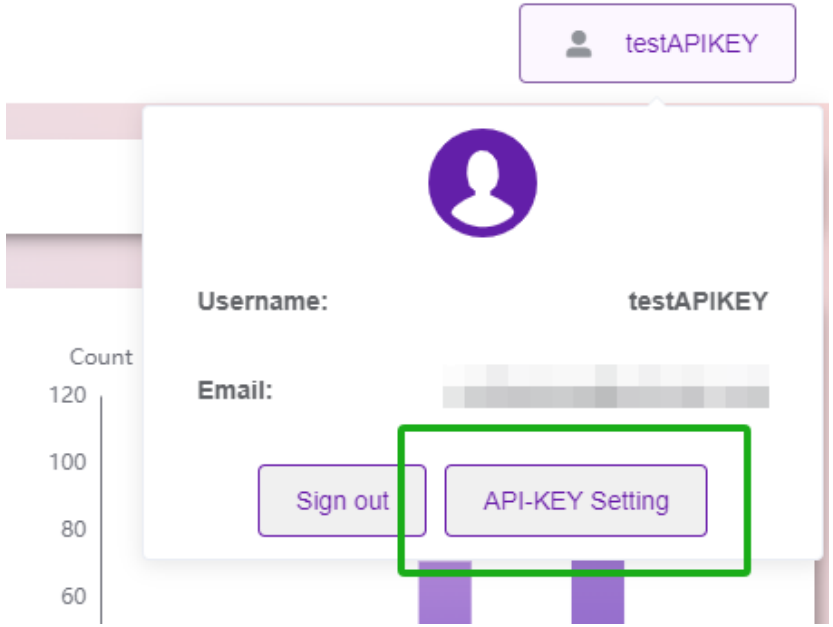
Router Jitter

APNIC FOUNDATION

清華大學 Tsinghua University

OPEN API

- /get_event_by_condition
- /get_event_detail



Body Params (application/json) | Code Generate | Example

type string required

Event Type

Allowed values: `Possible Hijack` `Possible SubHijack` `Ongoing Possible Hijack` `Ongoing Possible SubHijack`

Example: `Ongoing Possible SubHijack`

condition object {9} required

Find Condition (Support mongo scripts)

- start_timestamp anyOf {2} anyOf, must be valid against any of the subschemas optional
- hijack_as anyOf {2} anyOf, must be valid against any of the subschemas optional
- hijack_as_country anyOf {2} anyOf, must be valid against any of the subschemas optional
- level anyOf {2} anyOf, must be valid against any of the subschemas optional
- prefix anyOf {2} anyOf, must be valid against any of the subschemas optional
- subprefix anyOf {2} anyOf, must be valid against any of the subschemas optional
- victim_as anyOf {2} anyOf, must be valid against any of the subschemas optional
- victim_as_country anyOf {2} anyOf, must be valid against any of the subschemas optional
- end_timestamp anyOf {2} anyOf, must be valid against any of the subschemas optional

```
{
  "type": "Possible Hijack",
  "condition": {}
}
```

APNIC FOUNDATION

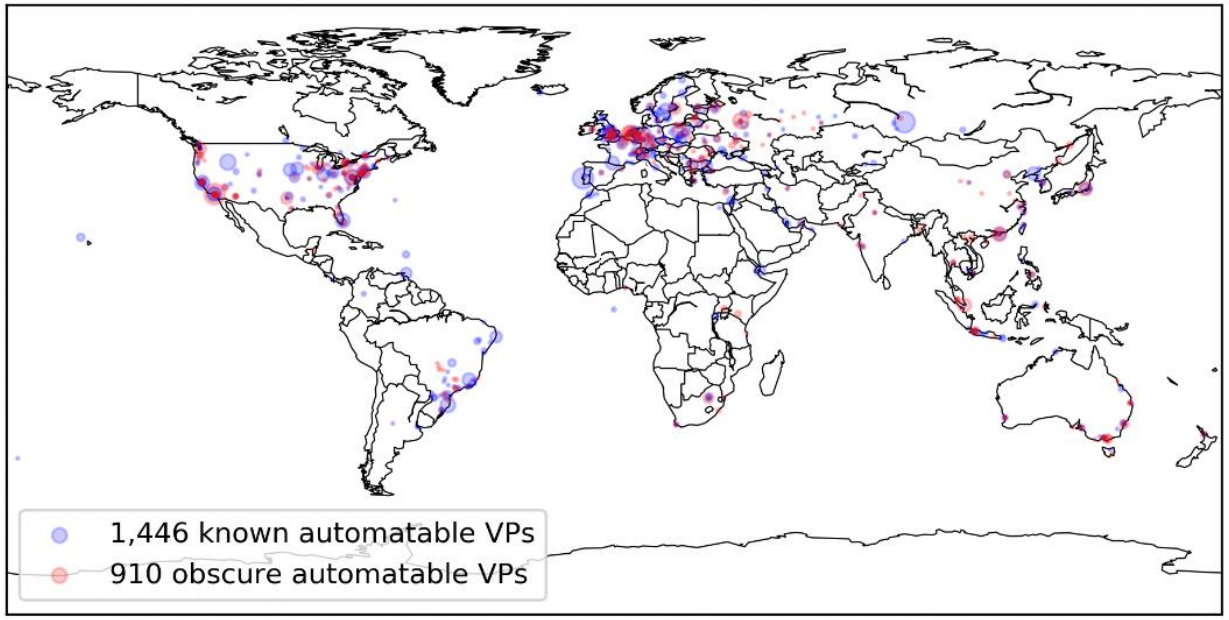
Tsinghua University

Future Work Plan

Objectives	Work Plan	Tentative Timeline
Develop an integrated Looking Glass platform	Find obscure Looking Glass VP regularly	Dec. 2023
	Develop integrated Looking Glass platform	Feb. 2024
	Develop Looking Glass API	Mar. 2024
Use Looking Glass to further check routing hijacking at the data plan	Develop data plan detection method and decision algorithm	June 2024
	Integrate the algorithm to the system	Aug. 2024
Implement path hijacking detection and routing leak detection methods	Develop path hijacking detection method	Nov. 2024
	Develop routing leak detection method	Jan. 2025
Continue to maintain and fix bugs in the BGPWatch platform	Continually test and get suggestions from user	Throughout the entire project duration
Continue community development and engagement, and international collaboration	The second phase of the project funded by APNIC Foundation (**Dec.06, 2023 – June 06, 2025 (18 months))** **Welcome new partners to join!**	Throughout the entire project duration

Open Looking Glass Vantage Point

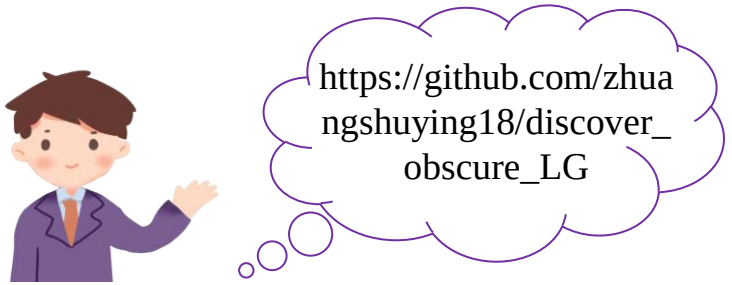
- **Paper: "Discovering obscure looking glass sites on the web to facilitate internet measurement research"——CoNEXT'21**



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**

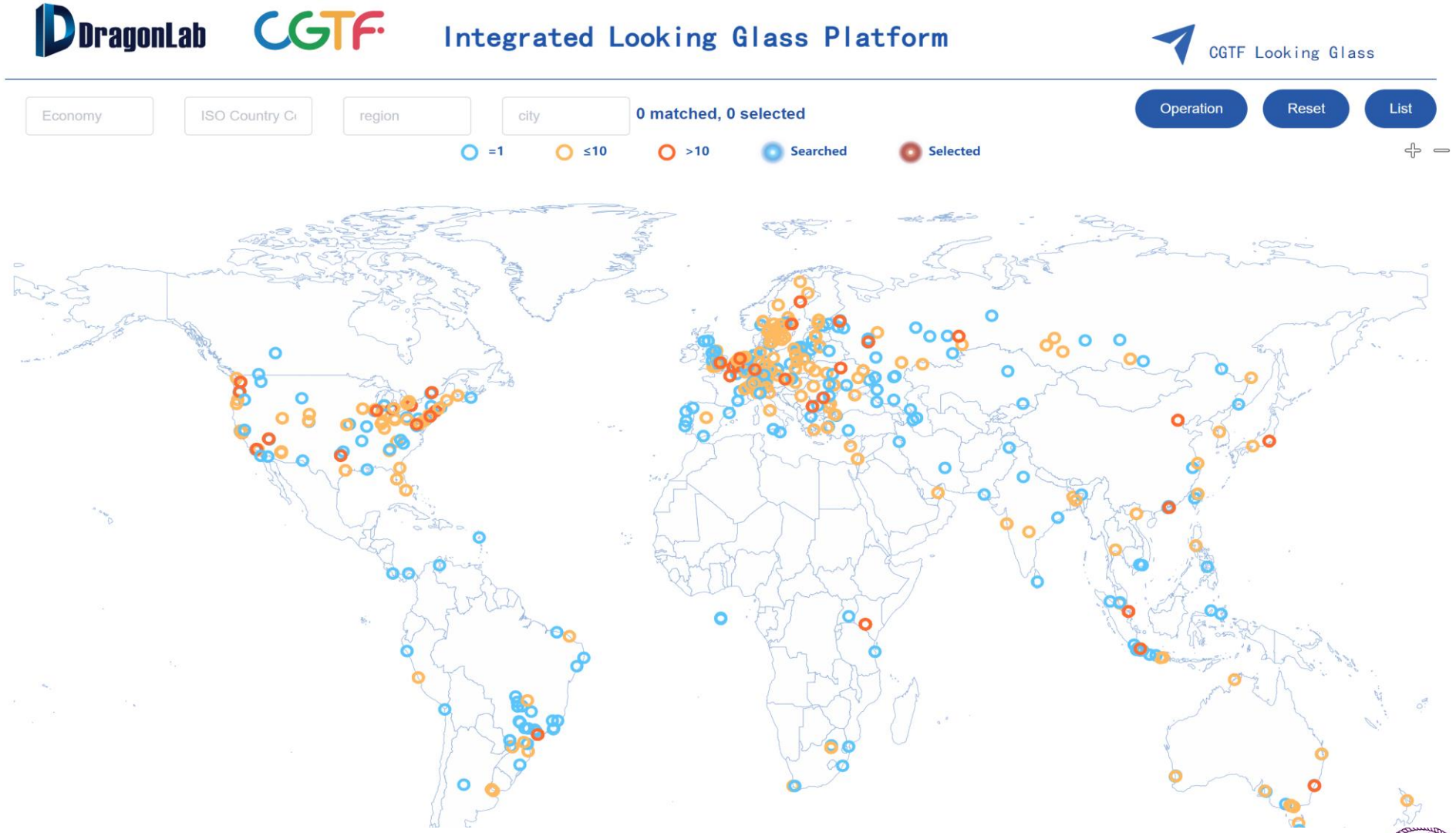


Periscope has found several hundred VPs (364)

APNIC FOUNDATION

清華大學 Tsinghua University

An Integrated Looking Glass and Open API

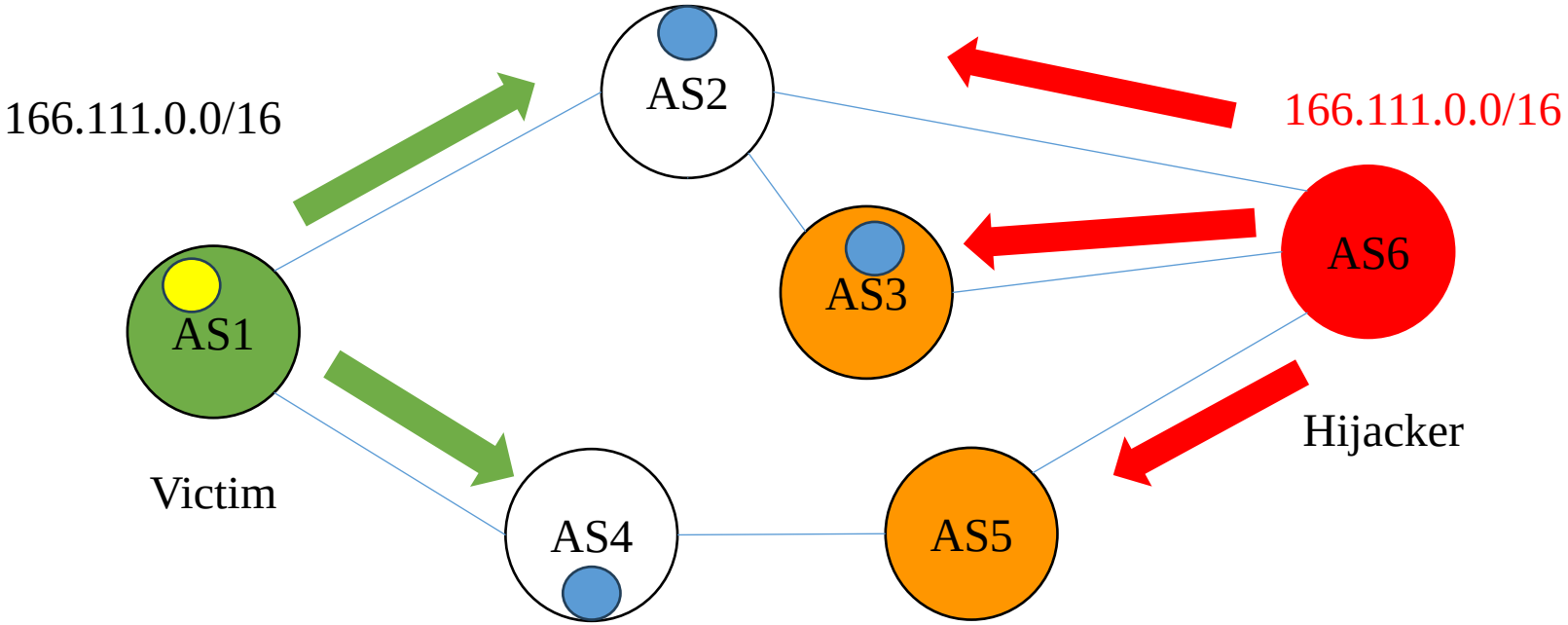


https://gperf.cgtf.net/#/outsidemap

APNIC FOUNDATION

清華大學 Tsinghua University

Data Plane Detection



Looking Glass vantage point

Representative services

- Possible Hijacking?

  1. Multi Home, Proxy
  2. Prefix Migration
  3. Hijacking

- When a hijacking occurs, it will affect the service
- Approach: Test representative service from VPs

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