(APNIC ISIF Project)

An Extension of the Ongoing Project "Developing a Collaborative BGP Routing Analyzing and Diagnosing Platform" Project

Technical Report

Project Review

Tsinghua University

May 27, 2025

APNIC FOUNDATION

清華大學 Tsinghua University

Contents

- Project Overview
- Technical Work
- Future Work Plan

APNIC FOUNDATION

清華大學 Tsinghua University

Project Overview

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

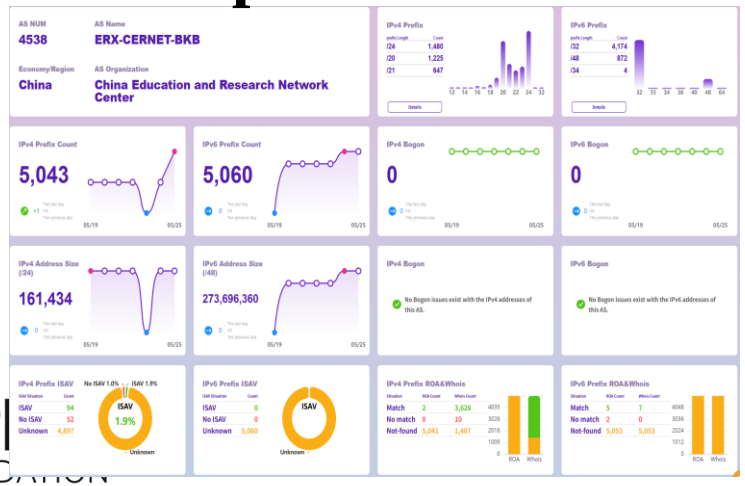
清華大學 Tsinghua University

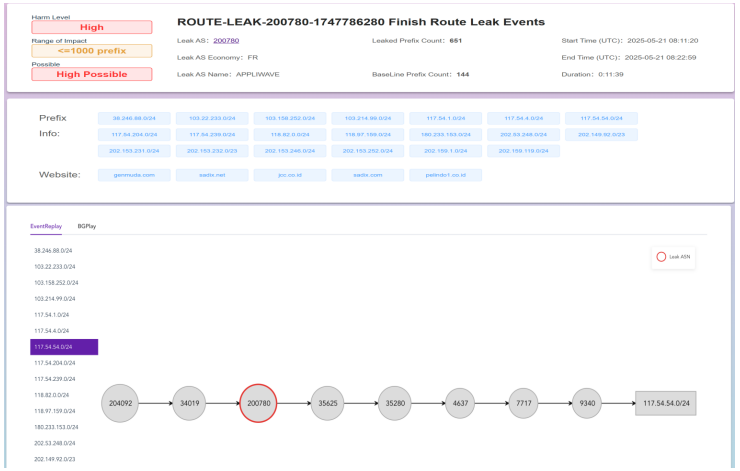
Activities of the 2nd Phase

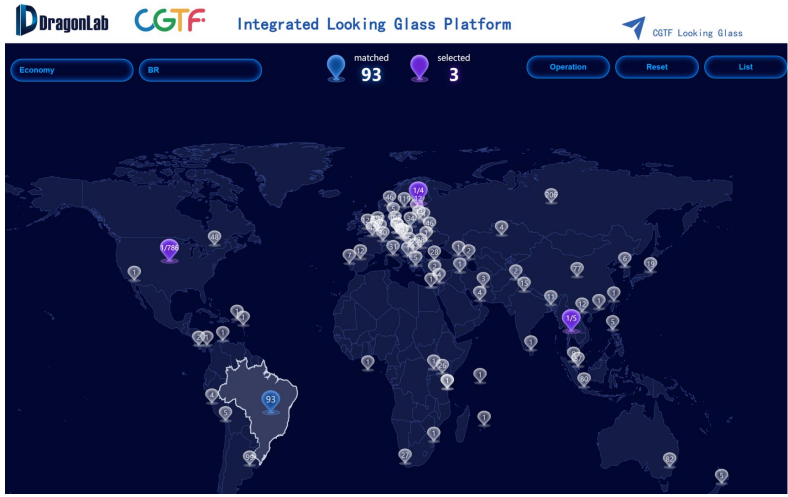
Objectives	Work Plan	Tentative Timeline
Develop an integrated Looking Glass platform	Find obscure Looking Glass VP regularly	Dec. 2023 Done
	Develop integrated Looking Glass platform	Feb. 2024 Done
	Develop Looking Glass API	Mar. 2024 Done
Use Looking Glass to further check routing hijacking at the data plan	Develop data plan detection method and decision algorithm	June 2024 Done
	Integrate the algorithm to the system	Aug. 2024 Done
Implement path hijacking detection and routing leak detection methods	Develop path hijacking detection method	Nov. 2024 Done
	Develop routing leak detection method	May. 2025 Done
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 (**Dec.06, 2023 – June 06, 2025 (18 months))** **Welcome new partners to join!**	Throughout the entire project duration

Technical Work

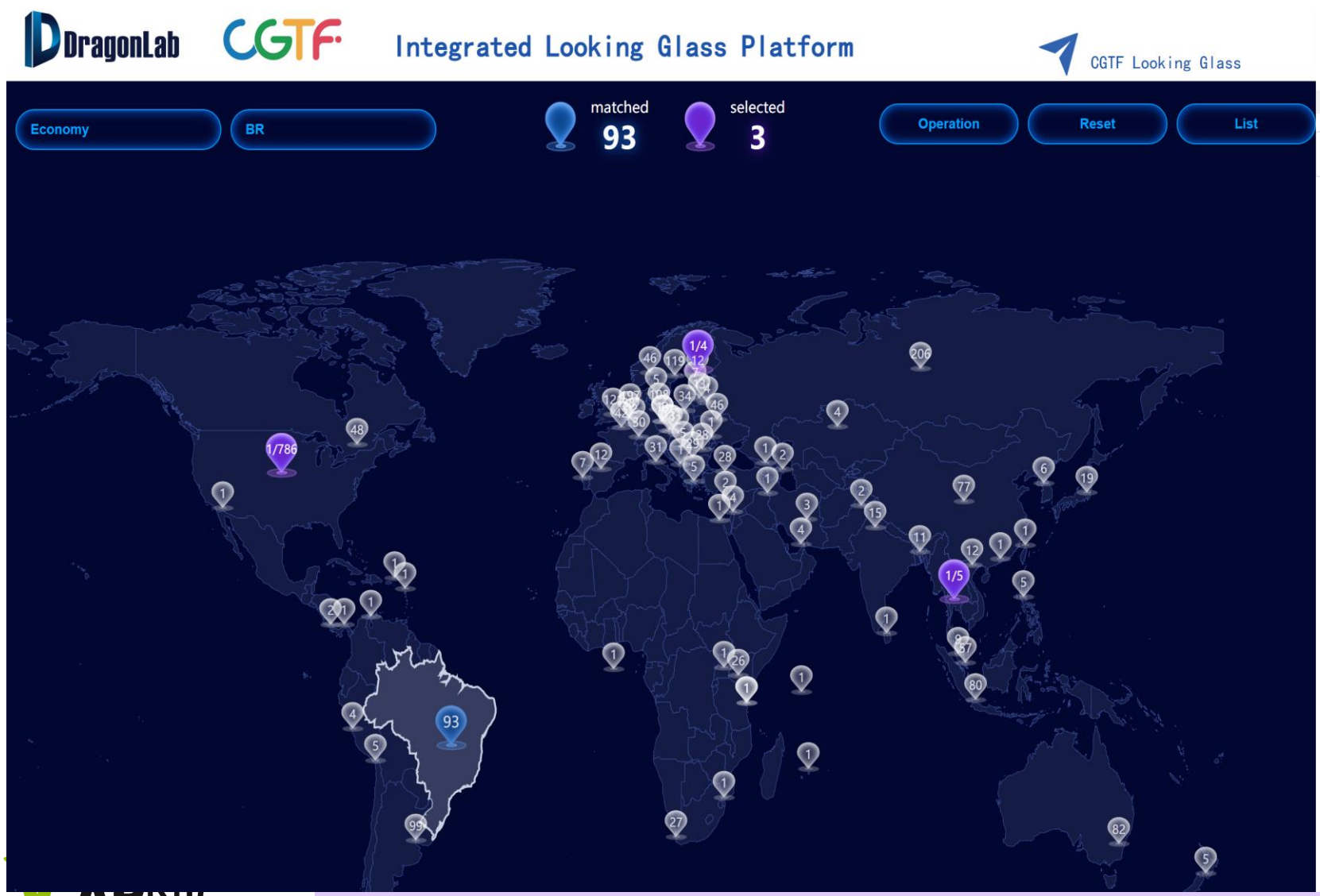
- An Integrated Looking Glass Platform
- Enhanced Anomaly Detection via Data Plane Probing
- Path Hijacking Detection
- Routing Leak Detection
- Tools for Operators

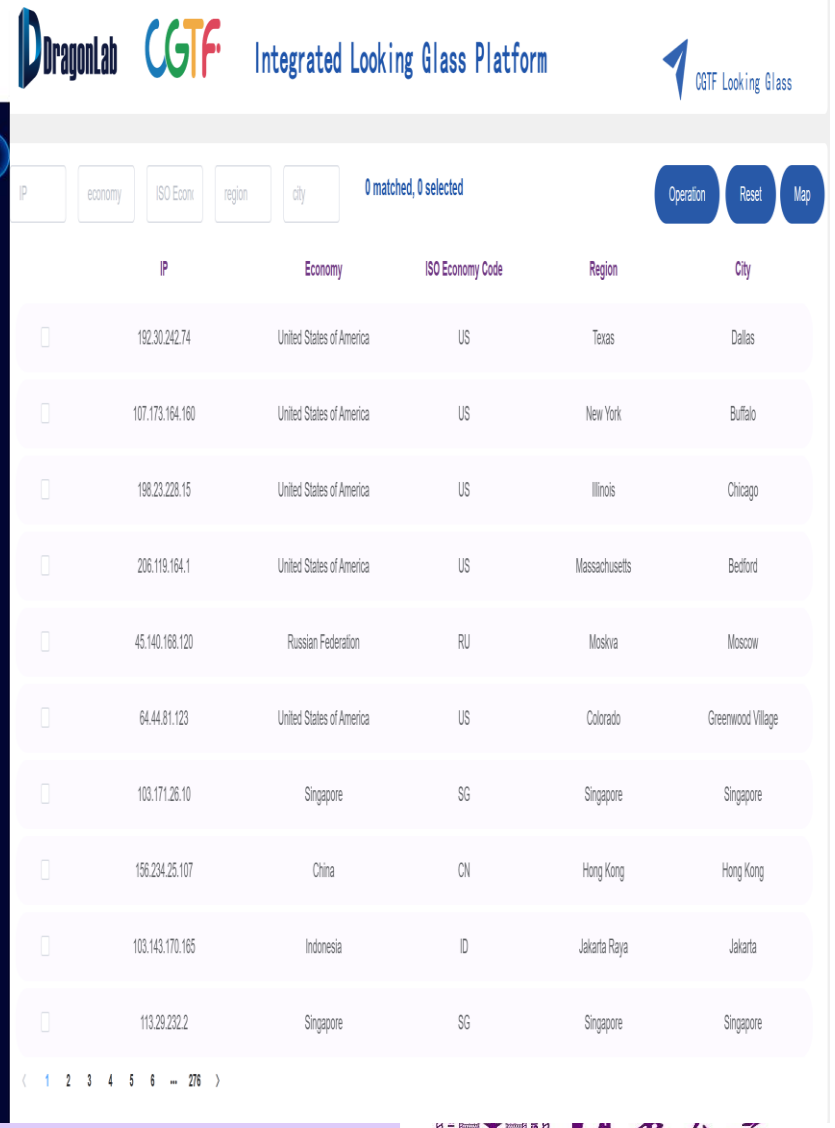






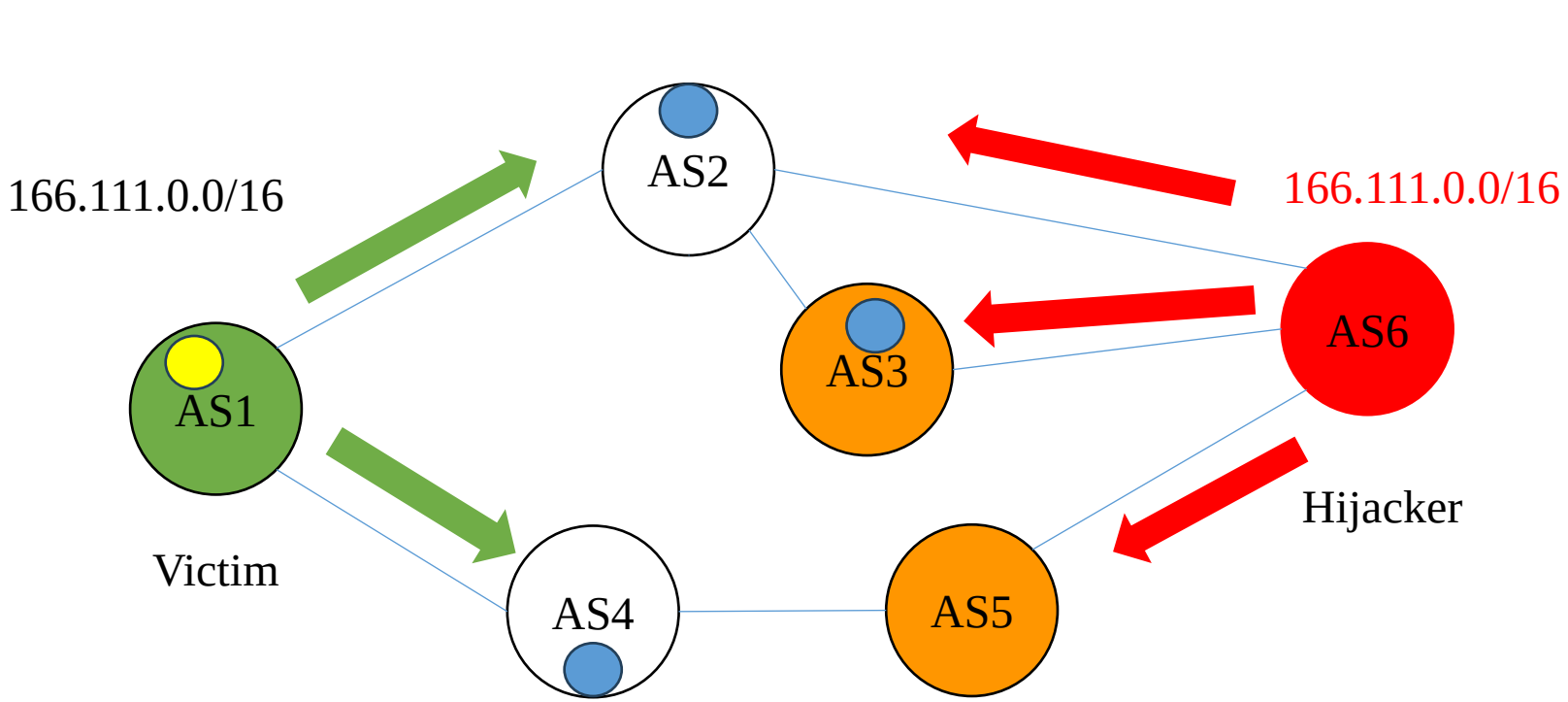
An Integrated Looking Glass Platform





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

Enhancing Anomaly Detection via Data Plane Probing



Looking Glass vantage point

Representative services

- Possible Hijacking?

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

Approach: Test representative services from VPs

Enhancing Anomaly Detection via Data Plane Detection

- Choose probes in certain ASes
- Choose destinations from the hijacked prefixes
- Do Probing
- Calculate Correlation Coefficient

Correlation Coefficient:

$$r(X,Y) = \frac{Cov(X,Y)}{\sqrt{Var[X]\,Var[Y]}}$$

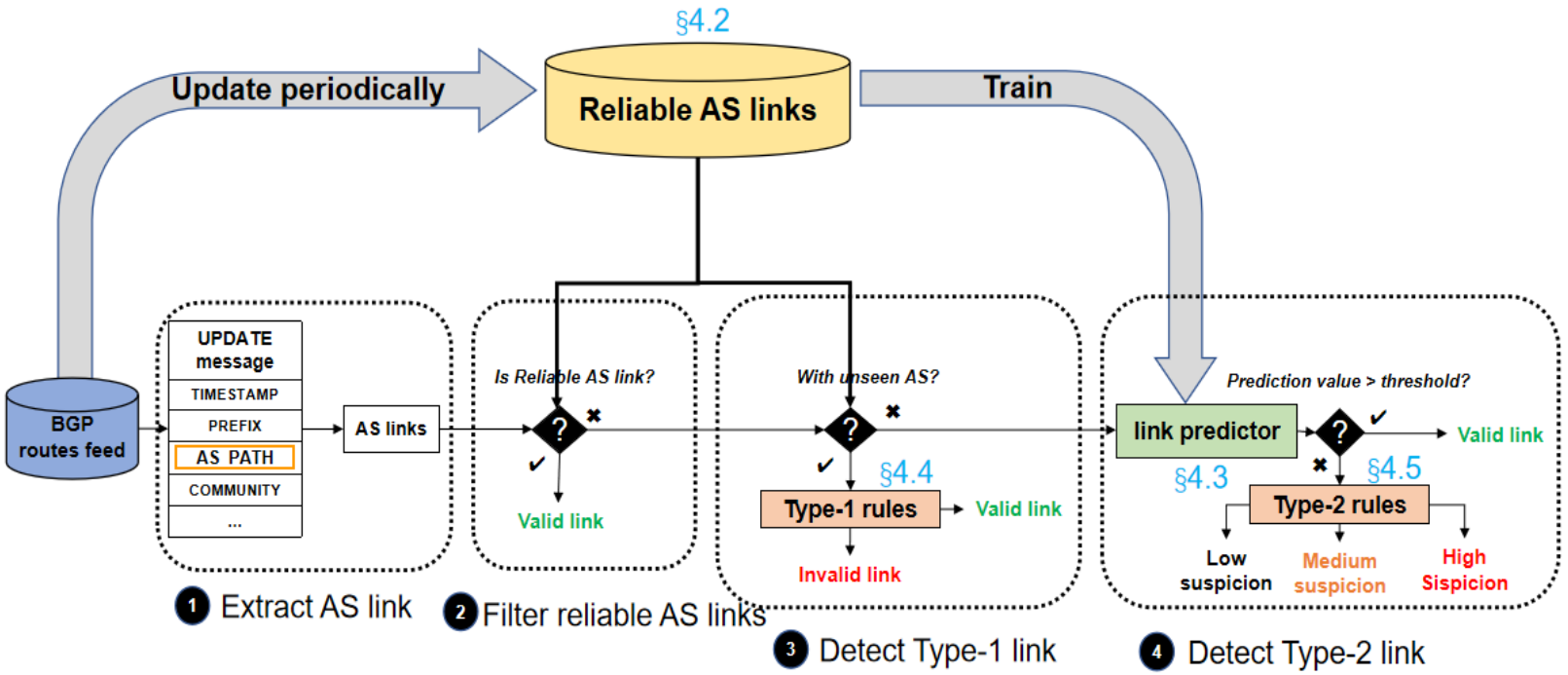
- Vector X:

For each prober, set to 0 if located in the affected AS; otherwise, set to 1.

- Vector Y:

For probe result from each prober, set to 1 if reachable; otherwise, set to 0.

BGP Anomaly Detection：Hybrid Rule-ML Approach

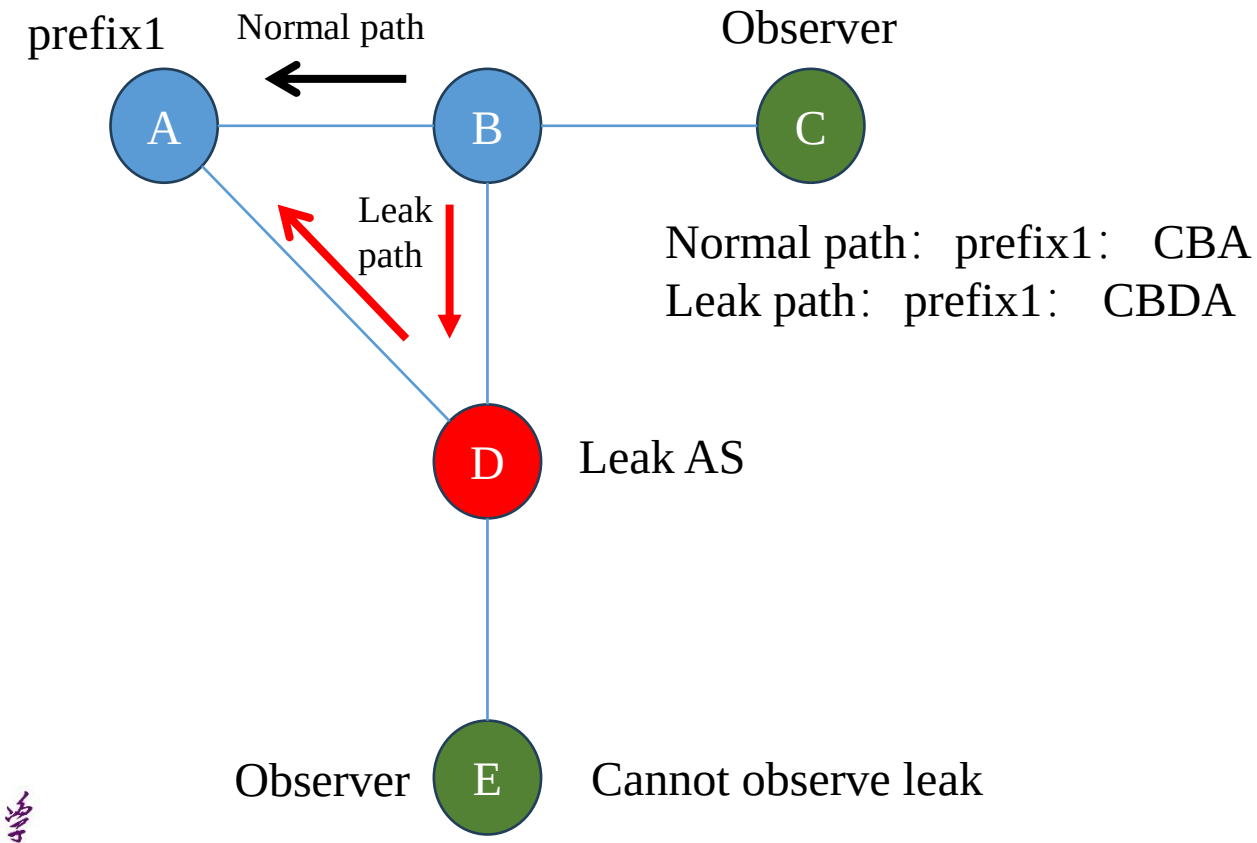


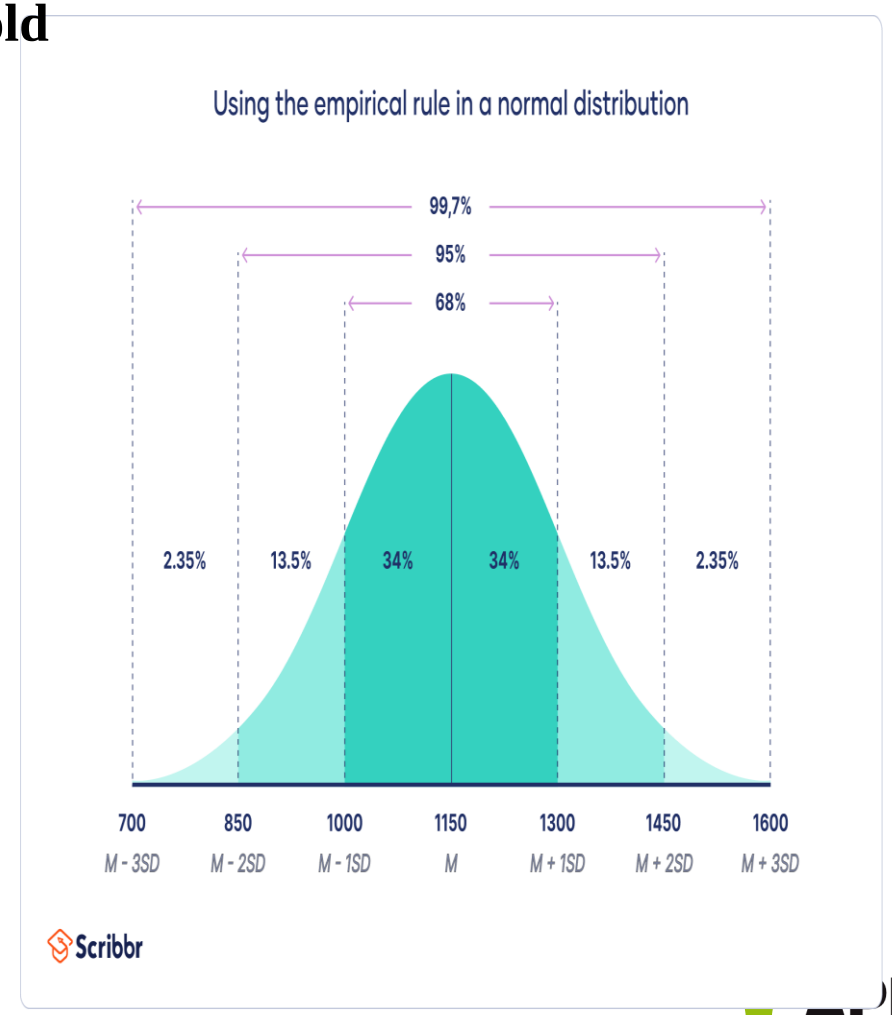
- Initially, train the machine learning classifier.
- During operation, the platform fetches BGP ROUTE feeds, extracts MOAS and new Links and ASes.
- ML Classifier is used to find suspicious hijack, and rules are used to improve the confidence level.

Route Leak Detection: A Baseline and Credibility-Driven Approach

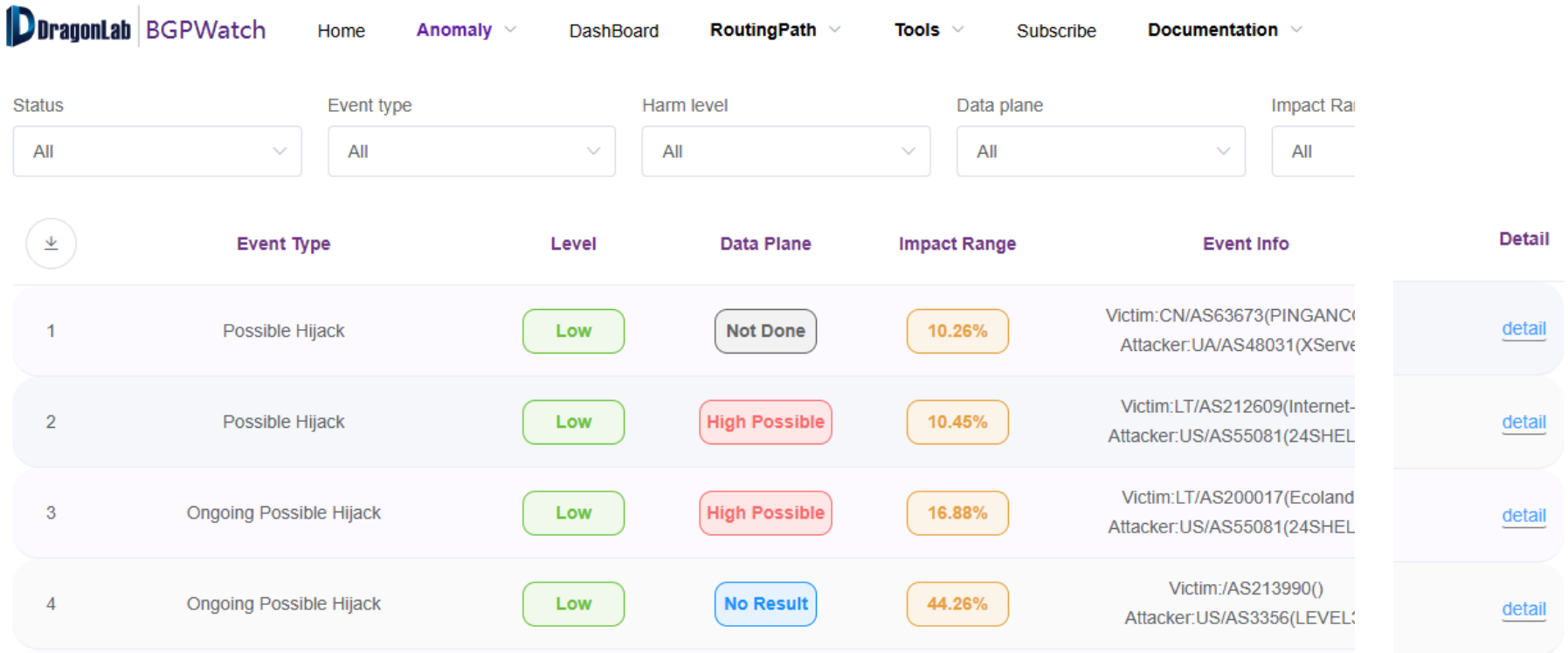
AS leak possibility: dynamic baseline, dynamic upper threshold

Path credibility: new path with low credibility



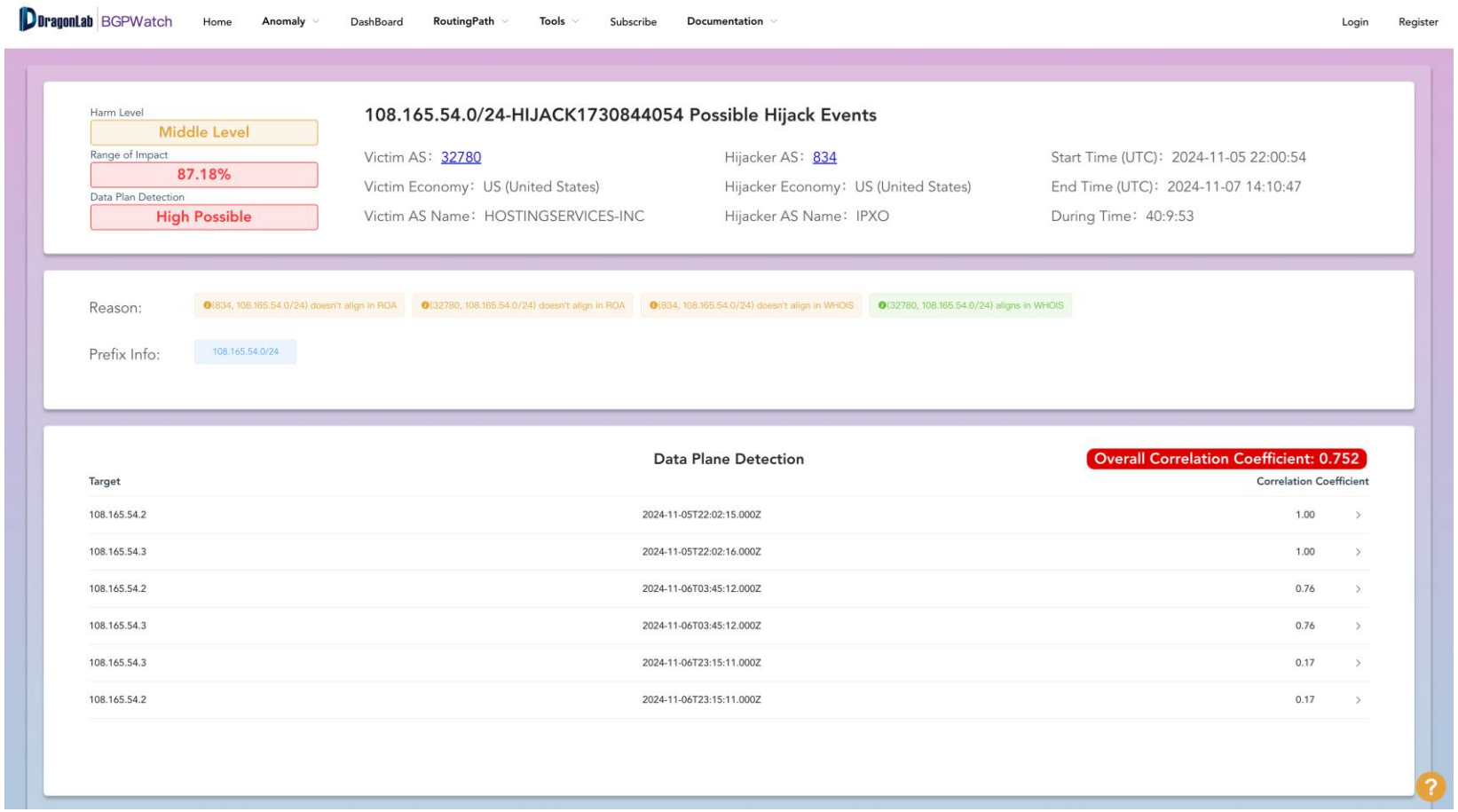


Prefix Anomaly



- **Impact Range**
  - <10%: Fewer than 10% of ASNs in the replay path are affected.
  - >=10%: More than 10% of ASNs in the replay path are affected.
  - >=50%: More than 10% of ASNs in the replay path are affected.

Prefix Anomaly – Detail



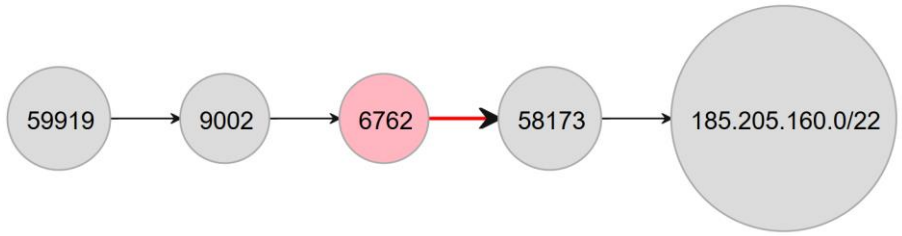
- **Data Plane Detection**
  - Not Done:
    No measurable target found
  - No Result:
    Probed, but received no results
  - Not Hijack:
    Correlation Coefficient = 0
  - Low Possible:
    Correlation Coefficient < 0.6
  - High Possible:
    Correlation Coefficient >= 0.6

Path Anomaly

	Event Type	Level	Possible	Impact Range	Event Info	Prefix Num	Example Prefix	Start Time
61	Ongoing New Link	Low	Low Possible	<=1 path	New Link: 11014(AR) -> 269818(AR) Reason:The suspicious link is at the end of the AS-PATH and is a domestic link (AR)	1	45.184.152.0/24	2024-11-13 15:05:30
62	Ongoing New AS	Low	High Possible	>5 path	New AS: 31196 Reason:ASN31196 is not the last hop	1	202.36.221.0/24	2024-11-13 14:40:48
63	Ongoing New Link	Low	Low Possible	<=1 path	New Link: 32307(US) -> 400707(US) Reason:The suspicious link is at the end of the AS-PATH and is a domestic link (US)	1	38.109.250.0/24	2024-11-13 14:29:20
64	Ongoing New Link	Low	High Possible	<=1 path	New Link: 58212(DE) -> 214309(GB) Reason:Detour of domestic traffic (34854,GB) (1299,SE) (199524,LU) (58212,DE) (214309,GB)	1	45.151.91.0/24	2024-11-13 14:14:44
65	Finish New Link	Low	Low Possible	<=1 path	New Link: 52863(BR) -> 264485(BR) Reason:The suspicious link is at the end of the AS-PATH and is a domestic link (BR)	1	189.91.147.0/24	2024-11-13 14:10:47

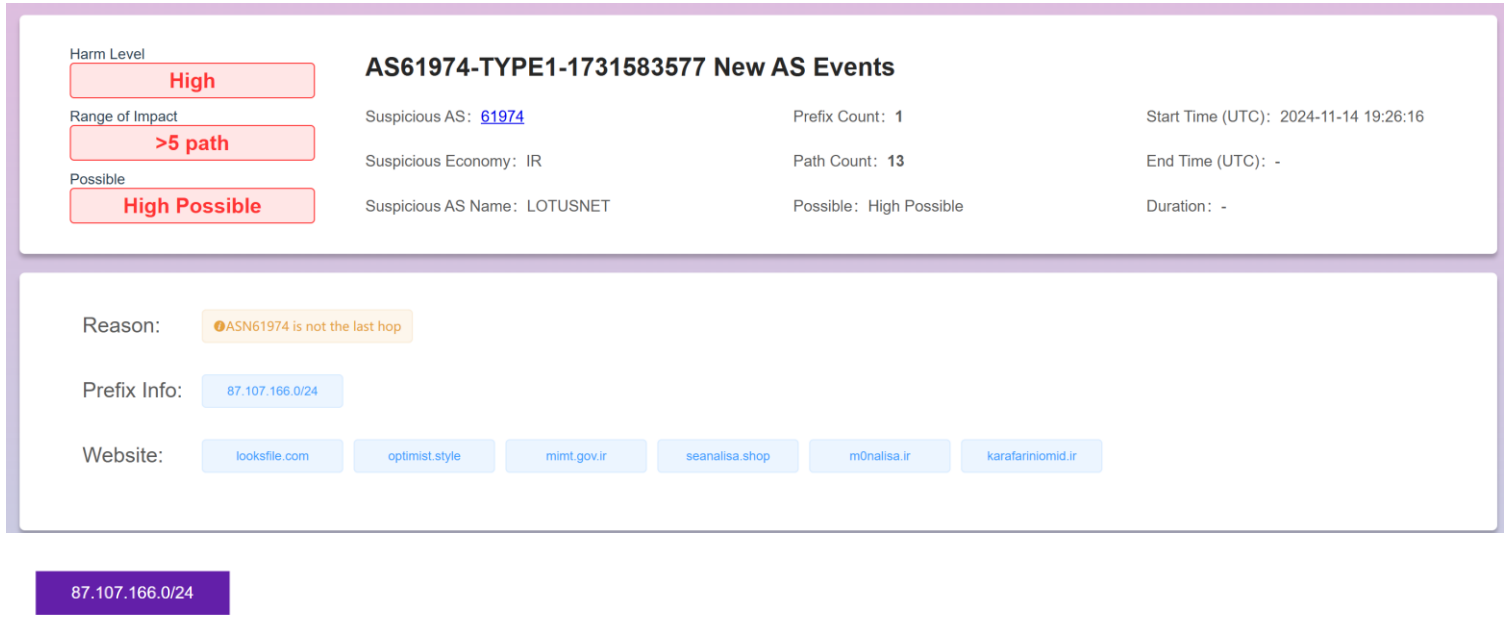
Path Anomaly Detail – Suspicious New Link

Reason:
Detour of domestic traffic (58173,GB) (6762,IT) (9002,GB)



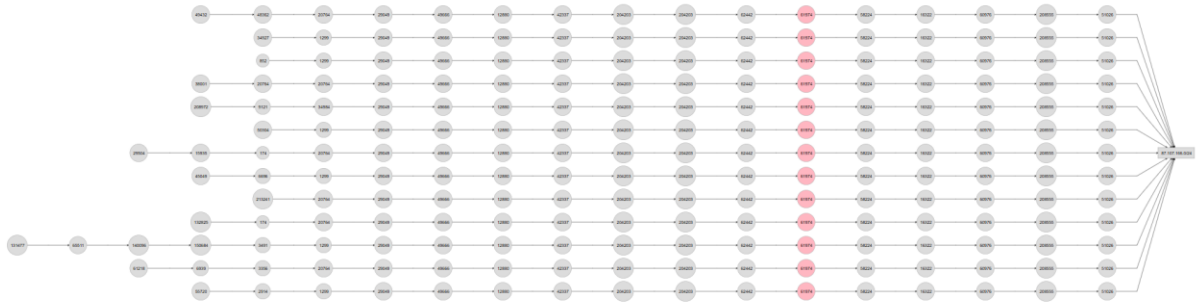
The suspicious AS and link are marked red.

Path Anomaly Detail – Suspicious New AS



87.107.166.0/24

Reason:
ASN61974 is not the last hop.

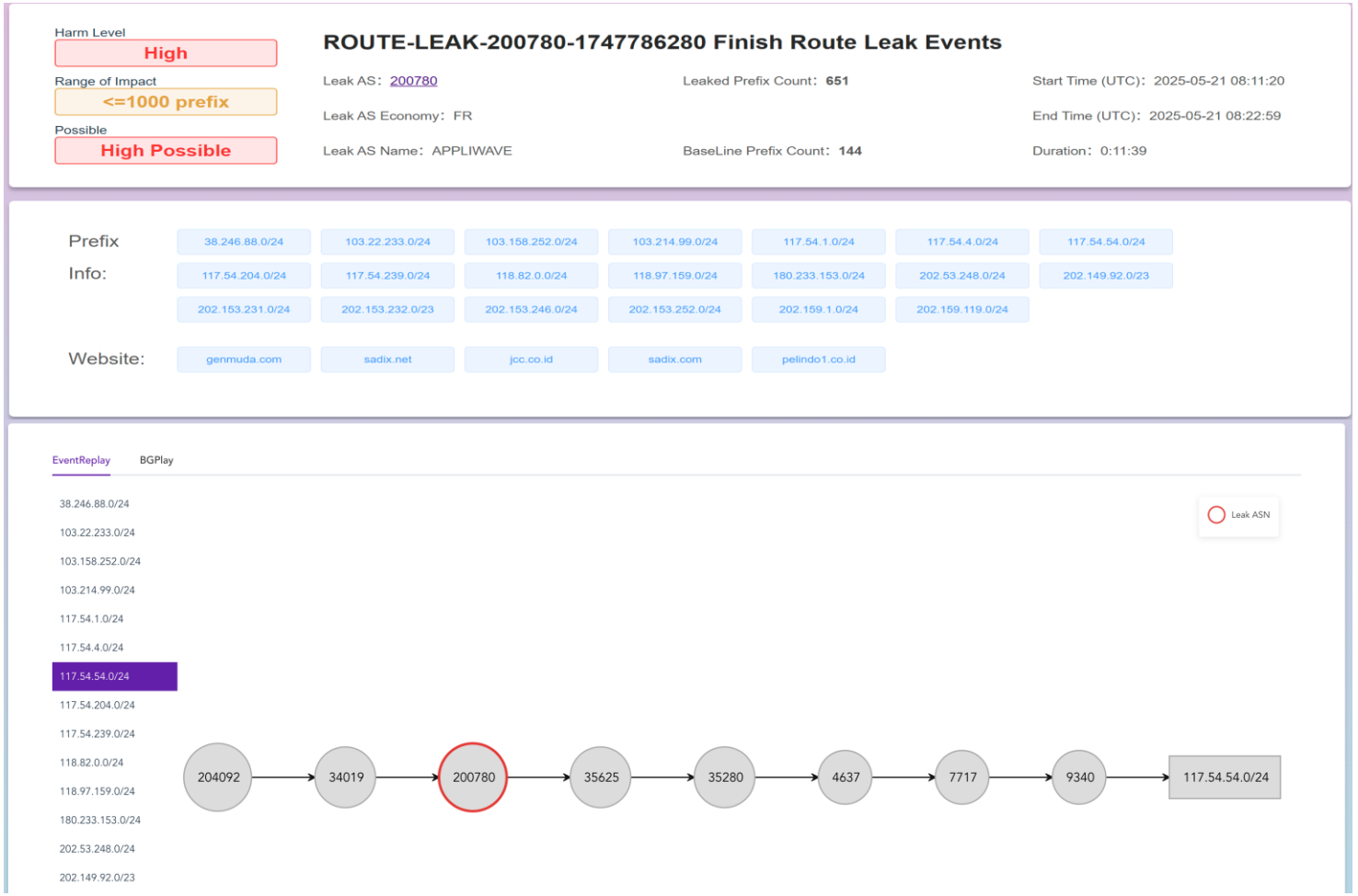


All the paths affected.

Route Leak Anomaly

	Event Type	Level	Impact Range	Possible	Leak ASN	Prefixes	Start Time	End Time	Duration	Detail
1	Finish Route Leak	High	<100 prefix	Middle Possible	AS150215	83	2025-05-24 21:19:36	2025-05-25 05:20:06	0:0:30	detail
2	Ongoing Route Leak	High	>1000 prefix	High Possible	AS20473	22566	2025-05-24 18:00:04	-	-	detail
3	Ongoing Route Leak	High	>1000 prefix	High Possible	AS13030	32671	2025-05-24 18:00:03	-	-	detail
4	Finish Route Leak	High	<100 prefix	Low Possible	AS150215	37	2025-05-24 13:44:21	2025-05-24 21:55:24	0:11:3	detail
5	Finish Route Leak	High	<100 prefix	Low Possible	AS150215	41	2025-05-24 11:25:51	2025-05-24 19:26:21	0:0:30	detail
6	Finish Route Leak	Low	>1000 prefix	High Possible	AS29390	5060	2025-05-23 19:30:42	2025-05-24 03:30:45	0:0:3	detail
7	Finish Route Leak	High	<100 prefix	Low Possible	AS150215	28	2025-05-23 19:29:17	2025-05-24 03:29:47	0:0:30	detail
8	Finish Route Leak	Low	>1000 prefix	Low Possible	AS211288	1564	2025-05-23 19:17:26	2025-05-24 03:30:40	0:13:14	detail
9	Finish Route Leak	High	<100 prefix	Low Possible	AS22677	48	2025-05-23 19:13:31	2025-05-24 03:30:45	0:17:14	detail
10	Finish Route Leak	High	<100 prefix	Low Possible	AS150215	15	2025-05-22 15:48:30	2025-05-22 23:49:00	0:0:30	detail

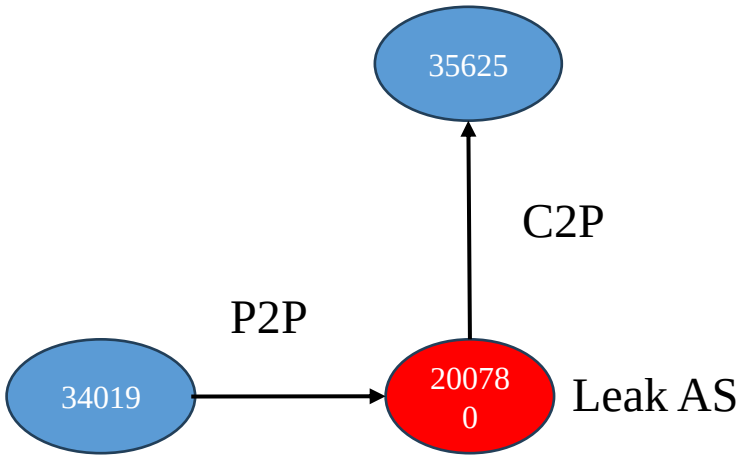
Route Leak Detail



From 00:11:20 to 00:22:58 UTC on May 21, 2025.

A total of 651 prefixes were leaked, with 20 sample prefixes listed in the prefix information.

AS34019←→AS200780 (p2p)
AS200780 → AS35625 (c2p)

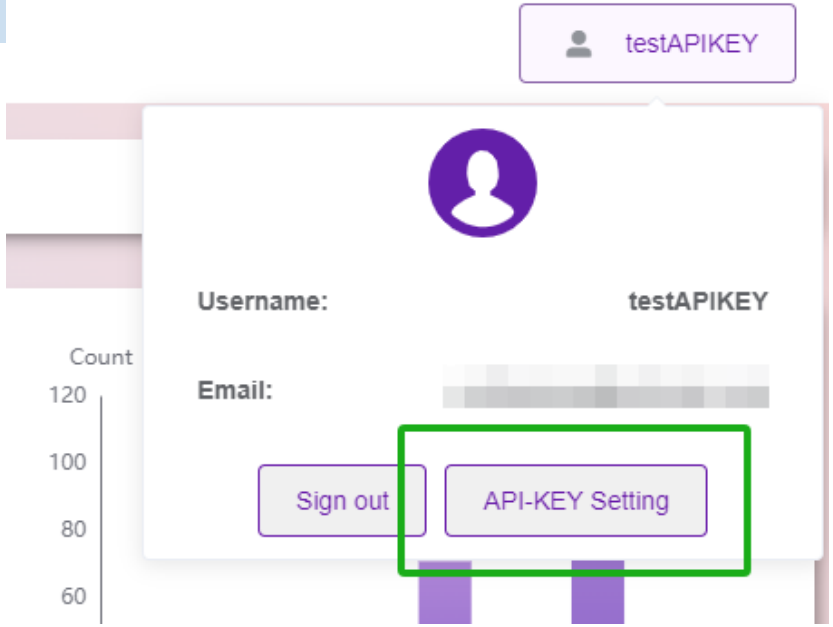


APNIC FOUNDATION

Tsinghua University

OPEN API

- /get_event_by_condition
- /get_event_detail
- /get_events_by_type



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

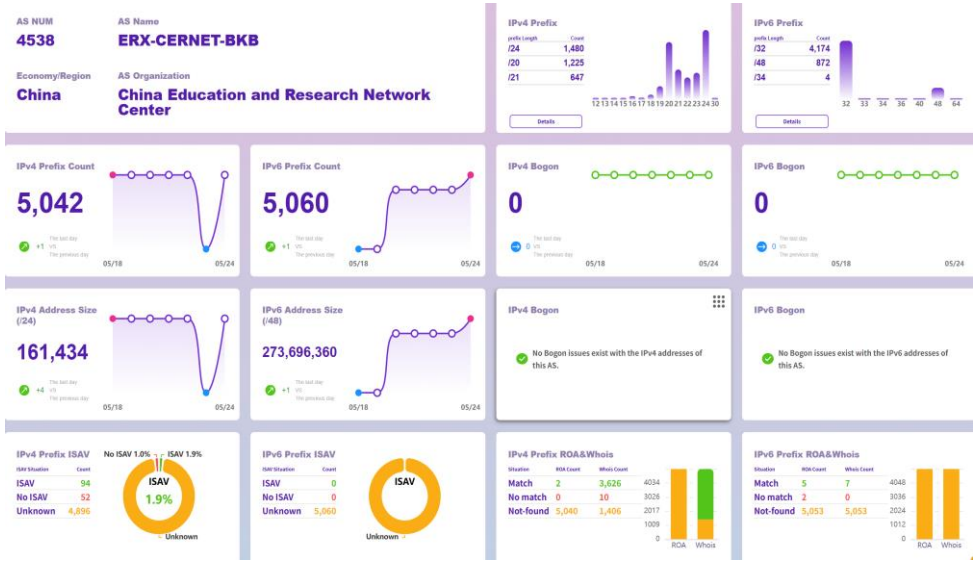
Find Condition (Support mongo scripts)

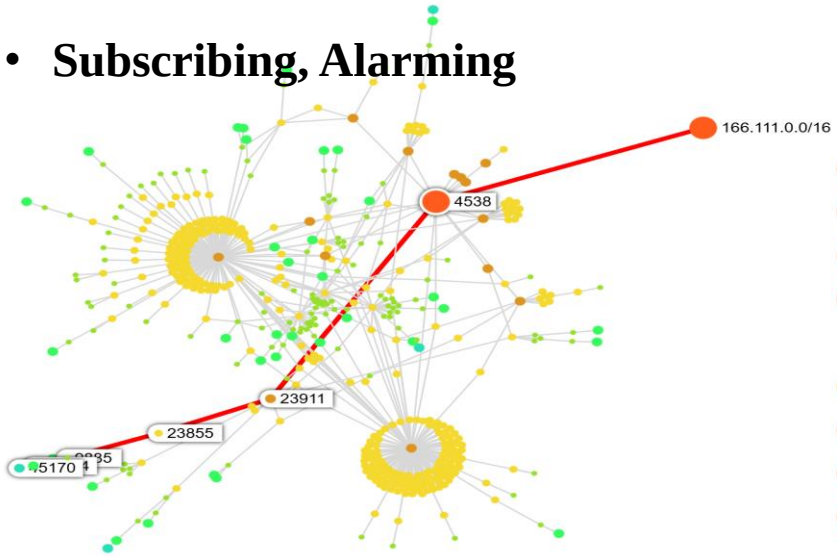
- start_timestamp anyOf {2} anyOf, must be valid against any of the subschemas optional
- hijack_as anyOf {2} anyOf, must be valid against any of the subschemas optional
- hijack_as_country anyOf {2} anyOf, must be valid against any of the subschemas optional
- level anyOf {2} anyOf, must be valid against 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

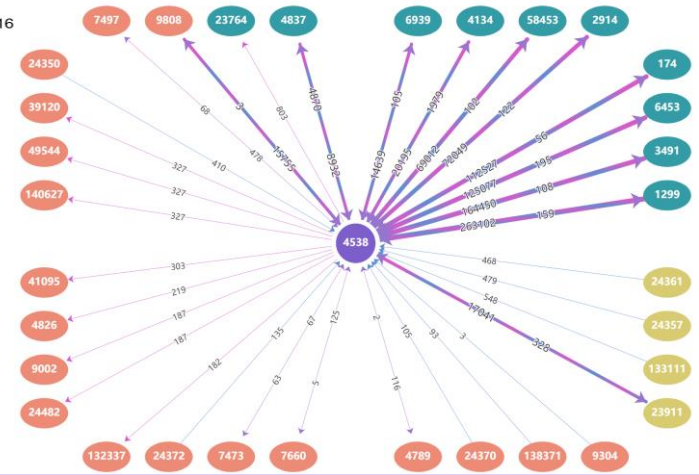
```
{
  "type": "Possible Hijack",
  "condition": {}
}
```

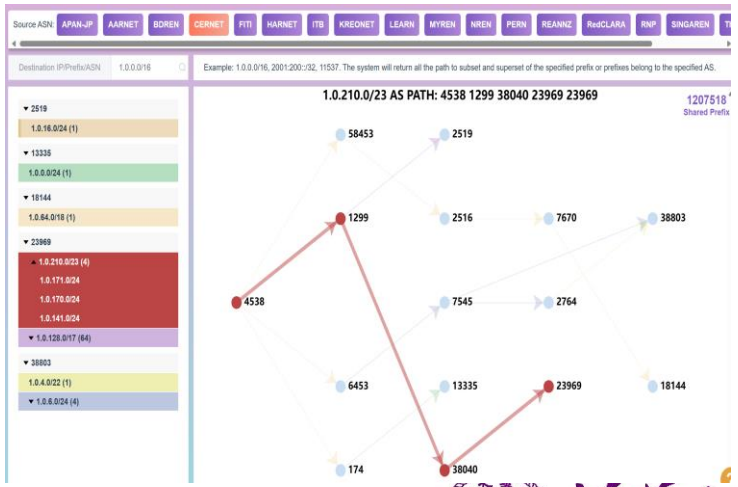
Tools for Network Operators

- **Dashboard: AS info, prefix, peers, Peering DB info**
- **Routing Search:**
  - **Aggregated forward routing path**
  - **Reverse routing path**
  - **Bi-direction routing path**
- **Bogon IP monitoring**
- **Subscribing, Alarming**



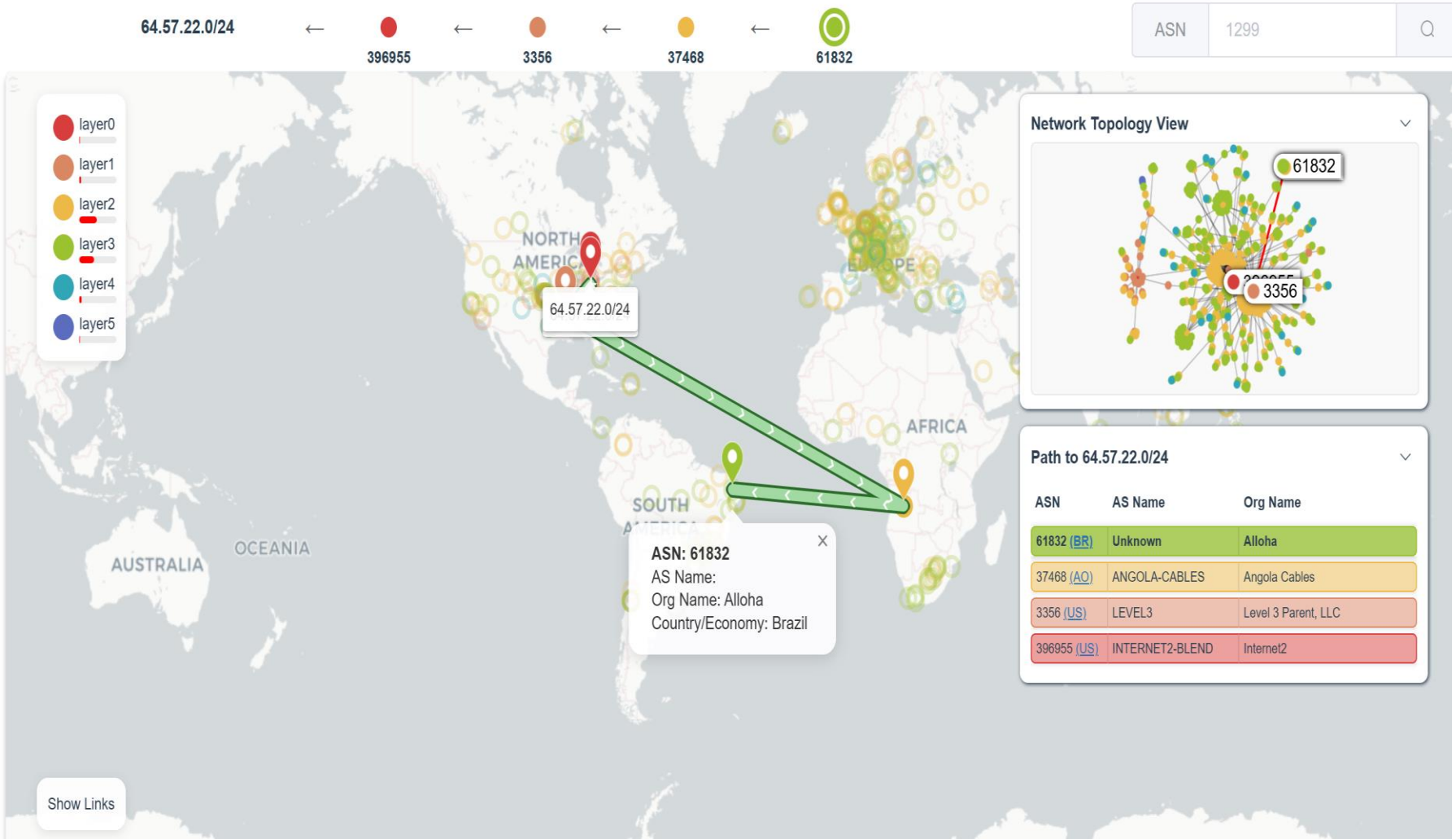






https://bgpwatch.cgtf.net

Reverse Routing Path (Map)

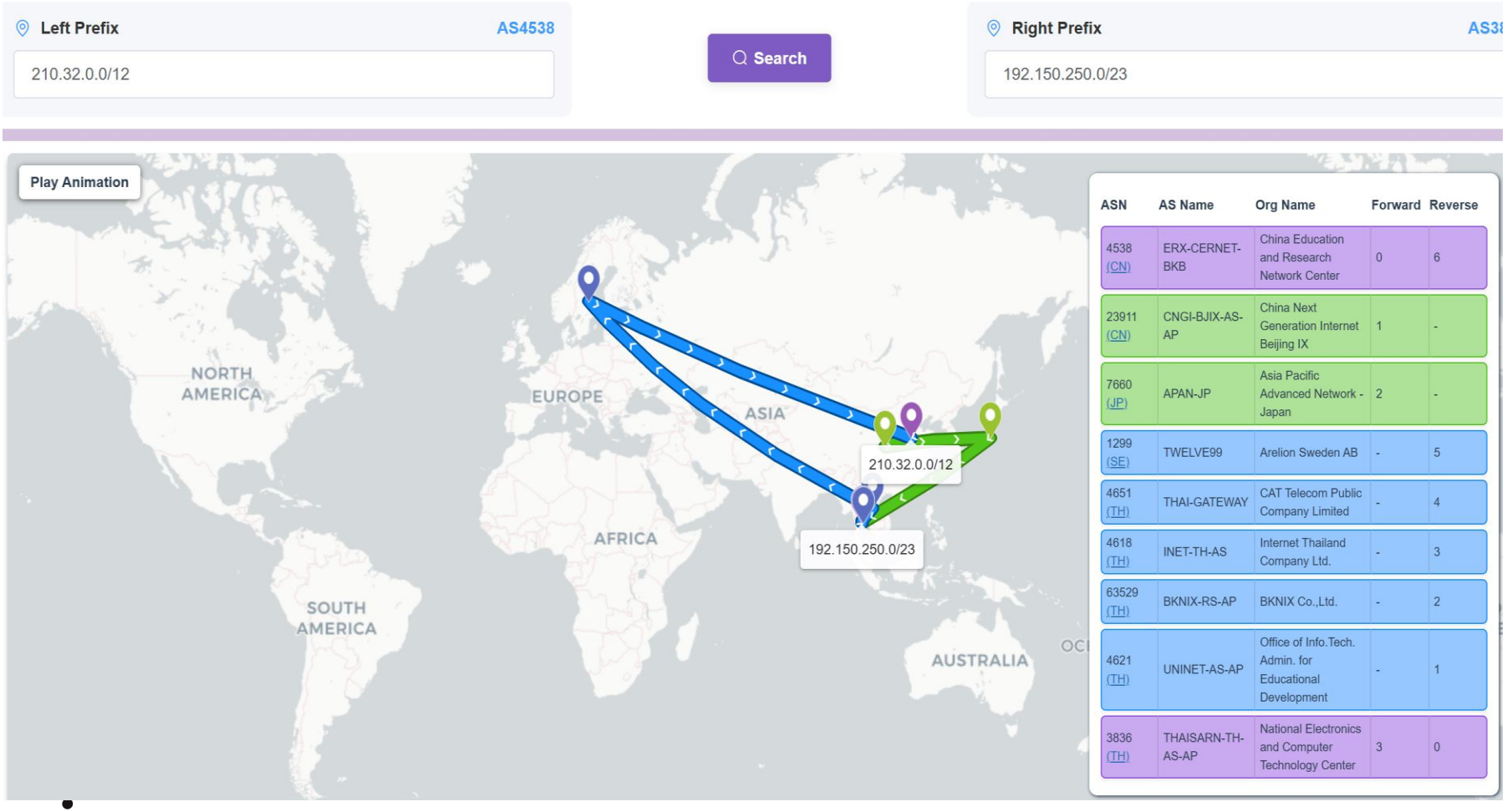


- Display the routing tree leading to a specific prefix on the map.
- Users can click on any AS node within this tree or enter an AS number in the input box located on the right side.
- The corresponding routing path will be highlighted.
- Each node infomation will be listed in the right table.

APNIC FOUNDATION

清華大學 Tsinghua University

Bi Routing Path (Map)



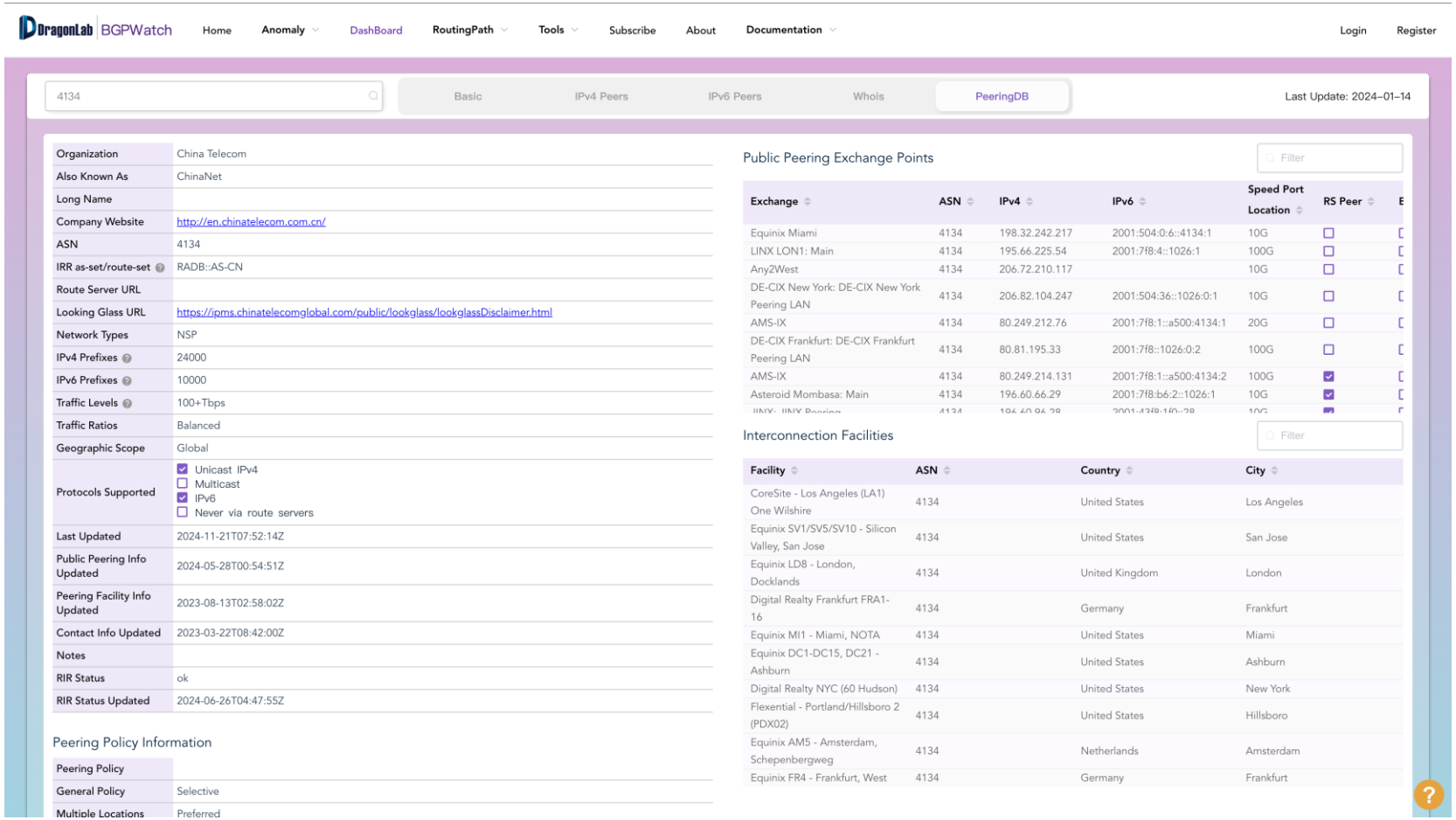
ASN	AS Name	Org Name	Forward	Reverse
4538 (CN)	ERX-CERNET-BKB	China Education and Research Network Center	0	6
23911 (CN)	CNGI-BJIX-AS-AP	China Next Generation Internet Beijing IX	1	-
7660 (JP)	APAN-JP	Asia Pacific Advanced Network - Japan	2	-
1299 (SE)	TWELVE99	Arelion Sweden AB	-	5
4651 (TH)	THAI-GATEWAY	CAT Telecom Public Company Limited	-	4
4618 (TH)	INET-TH-AS	Internet Thailand Company Ltd.	-	3
63529 (TH)	BKNIX-RS-AP	BKNIX Co.,Ltd.	-	2
4621 (TH)	UNINET-AS-AP	Office of Info.Tech. Admin. for Educational Development	-	1
3836 (TH)	THAISARN-TH-AS-AP	National Electronics and Computer Technology Center	3	0

- Show routes between two IP prefixes (IPv4/IPv6): green indicates the forward path, and blue indicates the reverse path.
- Each node information is listed in the right table with corresponding hops in the routing table.Green indicates nodes in the forward path, blue indicates nodes in the reverse path, and purple indicates nodes in both paths.
- Click each node on the map, and the corresponding row in the table will be highlighted.

APNIC FOUNDATION

Tsinghua University

Peering DB Info



Core Features:

- PeeringDB-integrated data visualization
- IXP and facility mapping
- Policy and contact management

Data Sources:

- Real-time PeeringDB public data
- Comprehensive ASN information
- Global IXP database

APNIC FOUNDATION

Tsinghua University

Future Work

- Conduct development and project review
  - Collect feedback and insights from partners and users
  - Review the project and submit the final report
- Explore more international collaborations
- Continue to secure new funds
  - Conduct fine-grained routing policy learning through AI methods
  - Infer the unobservable routing paths
  - Predict accident consequence. If some network incidents occur and cause network outages, what impacts will their routing paths be subject to and which backup links will be used

Thank you!

Contact us at: sec@cgtf.net

APNIC FOUNDATION

清華大學 Tsinghua University