

(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**

Contents

- **Project Overview**
- **Technical Work**
- **Future Work Plan**

Project Overview

Data Collecting

- ✓ Registration: WHOIS, RIR, PeeringDB, Radb, ROA
- ✓ Looking Glass
- ✓ Routing information
- ✓ Active Probing
- ✓ Passive measurement

Data Mining

- ✓ Statistics
- ✓ Machine learning
- ✓ Deep learning

Application

- ✓ Hijacking, leaking, outage detection
- ✓ Inter-domain topology discovery
- ✓ Monitoring peering and path changing
- ✓ Performance monitoring
- ✓ Link-level congestion detection
- ✓ Cyber-attack detection

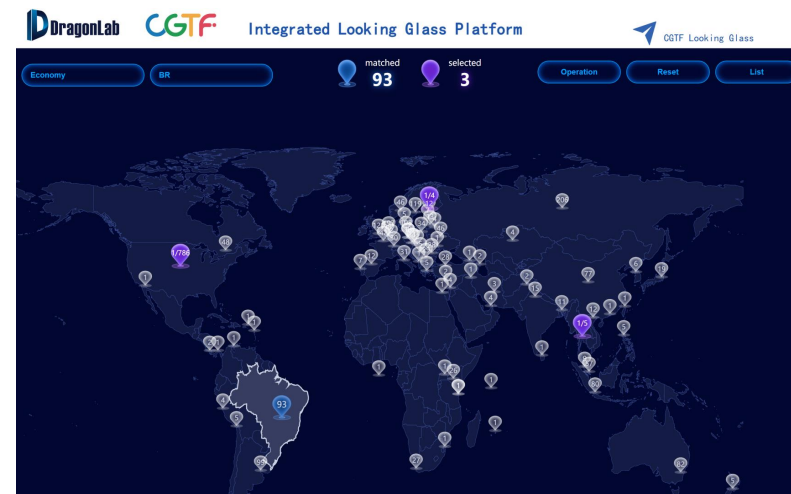
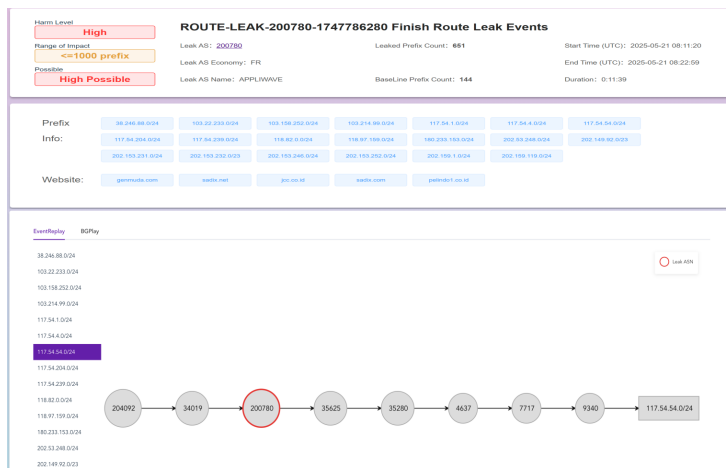
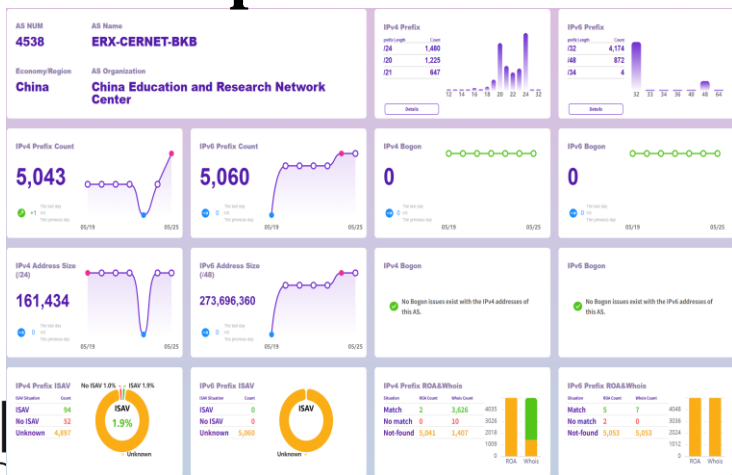
**Objectives: Improve internet security, availability
and provide tools for operators**

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



Integrated Looking Glass Platform



CGTF Looking Glass



Integrated Looking Glass Platform

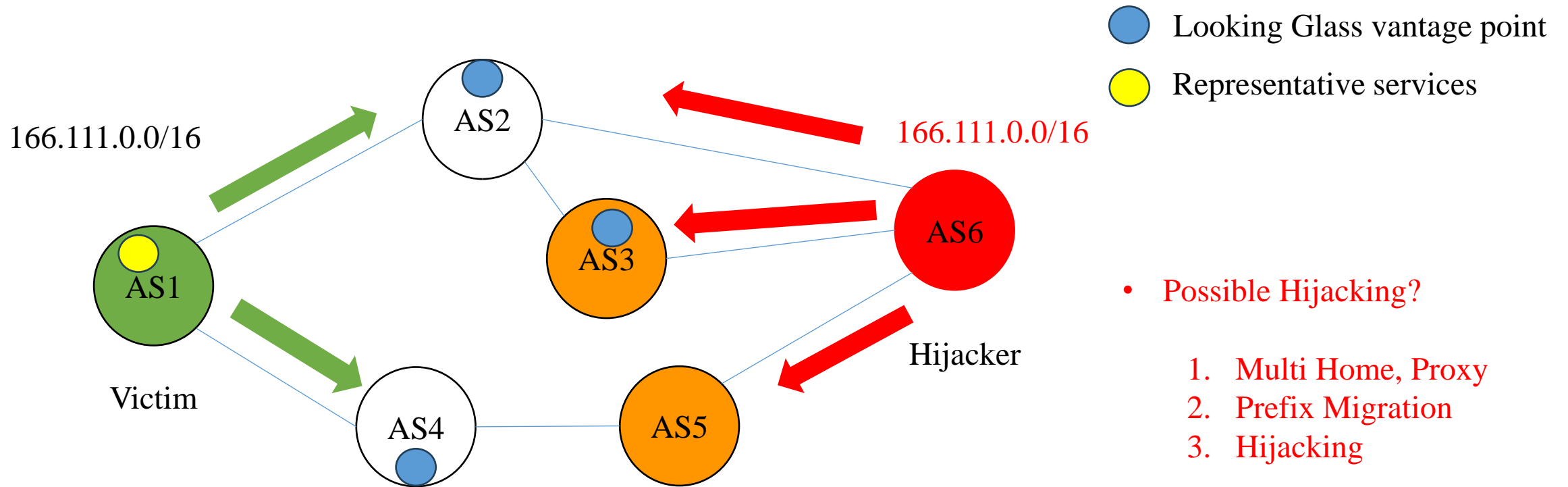


CGTF Looking Glass



IP	economy	ISO Econ	region	city	0 matched, 0 selected	Operation	Reset	Map
IP	Economy	ISO Economy Code	Region	City				
<input type="checkbox"/>	192.30.242.74	United States of America	US	Texas	Dallas			
<input type="checkbox"/>	107.173.164.160	United States of America	US	New York	Buffalo			
<input type="checkbox"/>	198.23.228.15	United States of America	US	Illinois	Chicago			
<input type="checkbox"/>	206.119.164.1	United States of America	US	Massachusetts	Bedford			
<input type="checkbox"/>	45.140.168.120	Russian Federation	RU	Moskva	Moscow			
<input type="checkbox"/>	64.44.81.123	United States of America	US	Colorado	Greenwood Village			
<input type="checkbox"/>	103.171.26.10	Singapore	SG	Singapore	Singapore			
<input type="checkbox"/>	156.234.25.107	China	CN	Hong Kong	Hong Kong			
<input type="checkbox"/>	103.143.170.165	Indonesia	ID	Jakarta Raya	Jakarta			
<input type="checkbox"/>	113.29.232.2	Singapore	SG	Singapore	Singapore			

Enhancing Anomaly Detection via Data Plane Probing



Approach: Test representative services from VPs

Enhancing Anomaly Detection via Data Plane Detection

108.165.54.3

Probe AS	Economy	Time(UTC)	From	Min RTT	Packet Loss
AS34549 		2024-11-06T03:45:12.000Z	185.150.98.36	No reply	100.00%
AS49420 		2024-11-06T03:45:12.000Z	91.212.242.241	No reply	100.00%
AS17639 		2024-11-06T03:45:14.000Z	161.49.13.234	No reply	100.00%
AS3333 		2024-11-06T03:45:12.000Z	193.0.0.165	No reply	100.00%
AS48362 		2024-11-06T03:45:12.000Z	94.199.170.201	No reply	100.00%
AS204092 		2024-11-06T03:45:13.000Z	80.67.190.218	No reply	100.00%
AS49673 		2024-11-06T03:45:12.000Z	94.247.111.19	No reply	100.00%
AS34800 		2024-11-06T03:45:12.000Z	194.50.99.201	No reply	100.00%
AS1403 		2024-11-06T03:45:12.000Z	198.16.163.75	13.81ms	0.00%
AS20205 		2024-11-06T03:45:12.000Z	38.67.212.178	16.77ms	0.00%
AS7018 		2024-11-06T03:45:14.000Z	162.225.60.96	22.56ms	0.00%
AS3549 		2024-11-06T03:45:13.000Z	66.162.17.4	23.65ms	0.00%
AS1299 		2024-11-06T03:45:12.000Z	62.115.192.103	27.96ms	0.00%
AS13830 		2024-11-06T03:45:12.000Z	161.129.155.179	41.25ms	0.00%
AS3356 		2024-11-06T03:45:13.000Z	4.8.13.234	42.41ms	0.00%

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

Correlation Coefficient:

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

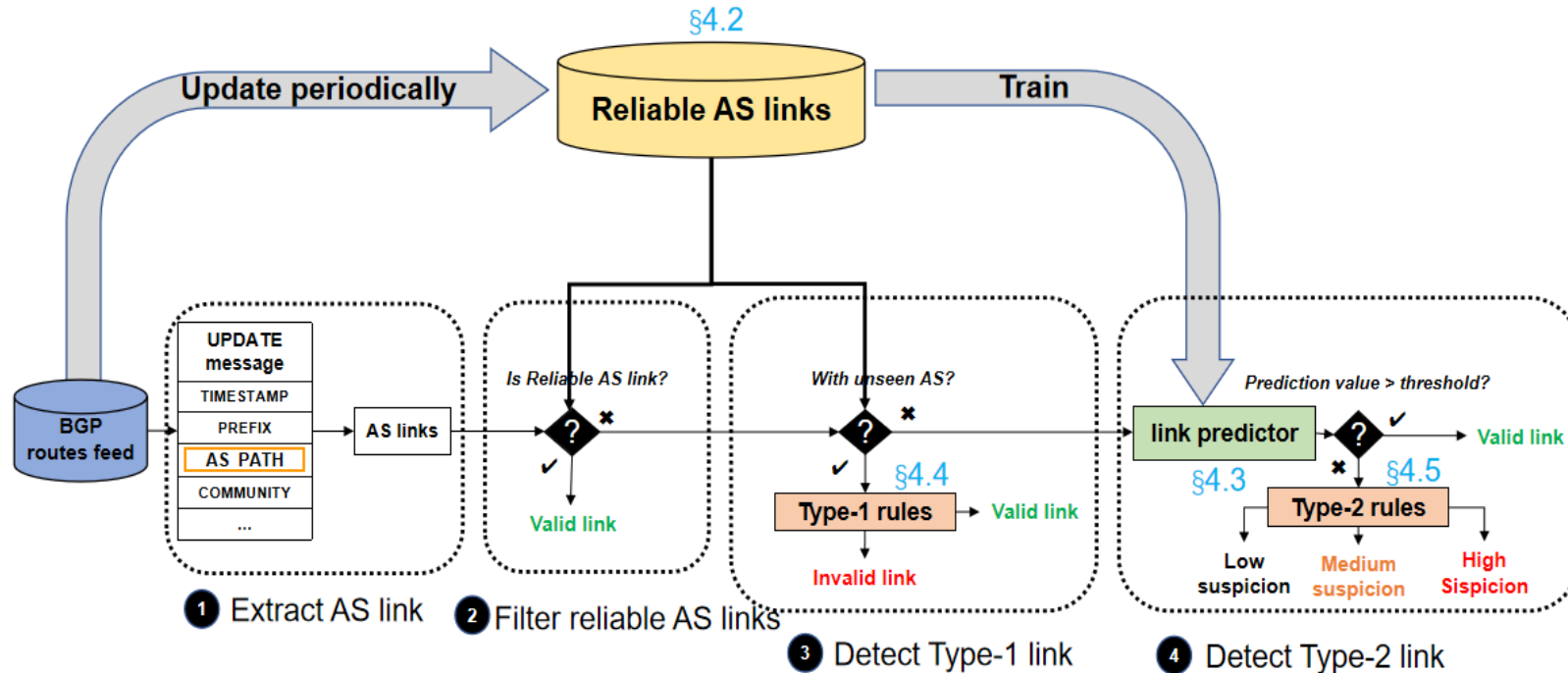
- Vector X:

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

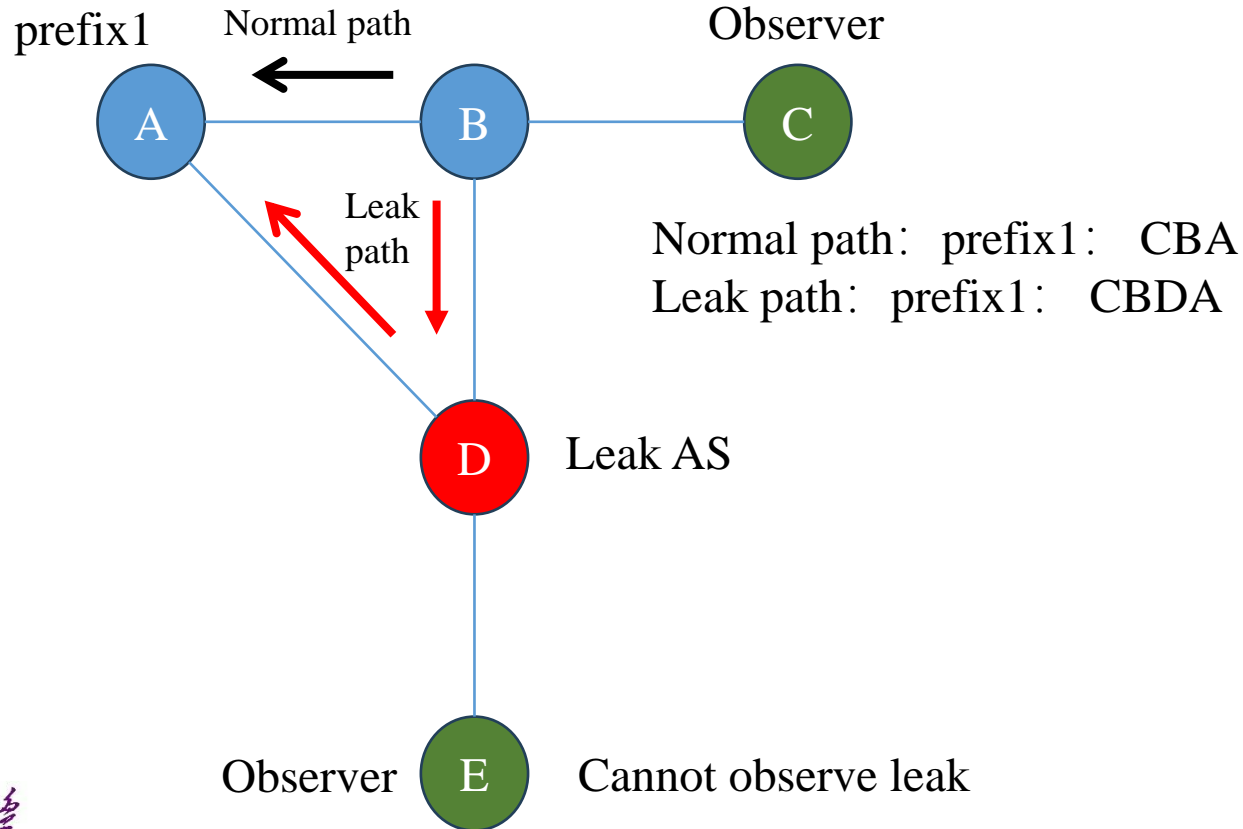


- Initially, train the machine learning classifier.
- During operation, the platform fetches BGP ROUTE feeds, extracts MOAS and new Links and ASes.
- ML Classifier is used to find suspicious hijack, and rules are used to improve the confidence level.

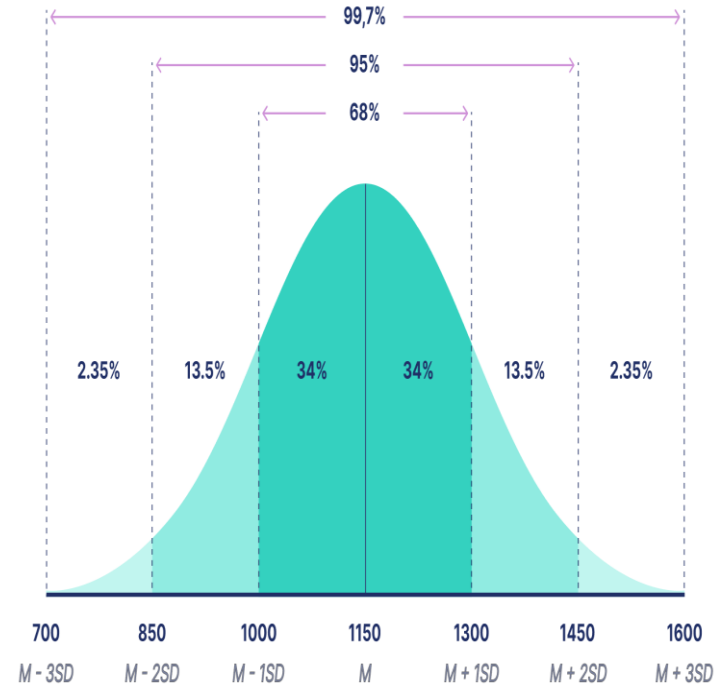
Route Leak Detection: A Baseline and Credibility-Driven Approach

AS leak possibility: dynamic baseline, dynamic upper threshold

Path credibility: new path with low credibility



Using the empirical rule in a normal distribution



Prefix Anomaly

DragonLab | BGPWatch

Home Anomaly ▾ DashBoard RoutingPath ▾ Tools ▾ Subscribe Documentation ▾

Status: All ▾ Event type: All ▾ Harm level: All ▾ Data plane: All ▾ Impact Range: All ▾

	Event Type	Level	Data Plane	Impact Range	Event Info	Detail
1	Possible Hijack	Low	Not Done	10.26%	Victim: CN/AS63673(PINGANCI) Attacker: UA/AS48031(XServe	detail
2	Possible Hijack	Low	High Possible	10.45%	Victim: LT/AS212609(Internet- Attacker: US/AS55081(24SHEL	detail
3	Ongoing Possible Hijack	Low	High Possible	16.88%	Victim: LT/AS200017(Ecoland Attacker: US/AS55081(24SHEL	detail
4	Ongoing Possible Hijack	Low	No Result	44.26%	Victim: /AS213990() Attacker: US/AS3356(LEVEL:	detail

- **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

DragonLab BGPWatch Home Anomaly DashBoard RoutingPath Tools Subscribe Documentation Login Register

Harm Level: **Middle Level**

Range of Impact: **87.18%**

Data Plan Detection: **High Possible**

108.165.54.0/24-HIJACK1730844054 Possible Hijack Events

Victim AS: [32780](#) Hijacker AS: [834](#) Start Time (UTC): 2024-11-05 22:00:54
Victim Economy: US (United States) Hijacker Economy: US (United States) End Time (UTC): 2024-11-07 14:10:47
Victim AS Name: HOSTINGSERVICES-INC Hijacker AS Name: IPXO During Time: 40:9:53

Reason: ●(834, 108.165.54.0/24) doesn't align in ROA ●(32780, 108.165.54.0/24) doesn't align in ROA ●(834, 108.165.54.0/24) doesn't align in WHOIS ●(32780, 108.165.54.0/24) aligns in WHOIS

Prefix Info: [108.165.54.0/24](#)

Target	Data Plane Detection	Correlation Coefficient
108.165.54.2	2024-11-05T22:02:15.000Z	1.00 >
108.165.54.3	2024-11-05T22:02:16.000Z	1.00 >
108.165.54.2	2024-11-06T03:45:12.000Z	0.76 >
108.165.54.3	2024-11-06T03:45:12.000Z	0.76 >
108.165.54.3	2024-11-06T23:15:11.000Z	0.17 >
108.165.54.2	2024-11-06T23:15:11.000Z	0.17 >

Overall Correlation Coefficient: 0.752

- **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

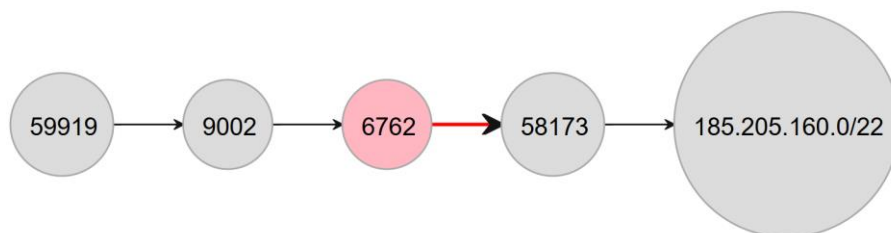
	Event Type	Level	Possible	Impact Range	Event Info	Prefix Num ⬆	Example Prefix	Start Time ⬇
61	Ongoing New Link	Low	Low Possible	≤ 1 path	New Link: 11014(AR) -> 269818(AR) Reason:The suspicious link is at the end of the AS-PATH and is a domestic link (AR)	1	45.184.152.0/24	2024-11-13 15:05:30
62	Ongoing 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

Harm Level

High

Range of Impact

>5 path

Possible

High Possible

AS61974-TYPE1-1731583577 New AS Events

Suspicious AS: [61974](#)

Prefix Count: 1

Start Time (UTC): 2024-11-14 19:26:16

Suspicious Economy: IR

Path Count: 13

End Time (UTC): -

Suspicious AS Name: LOTUSNET

Possible: High Possible

Duration: -

Reason:

●ASN61974 is not the last hop

Prefix Info:

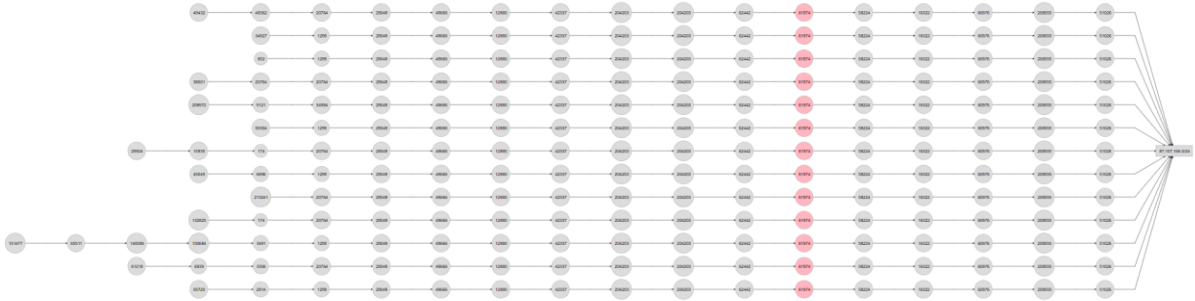
87.107.166.0/24

Website:

[looksfile.com](#)[optimist.style](#)[mimt.gov.ir](#)[seanalisa.shop](#)[m0nalisa.ir](#)[karafariniomid.ir](#)

Reason:
ASN61974 is not the last hop.

87.107.166.0/24

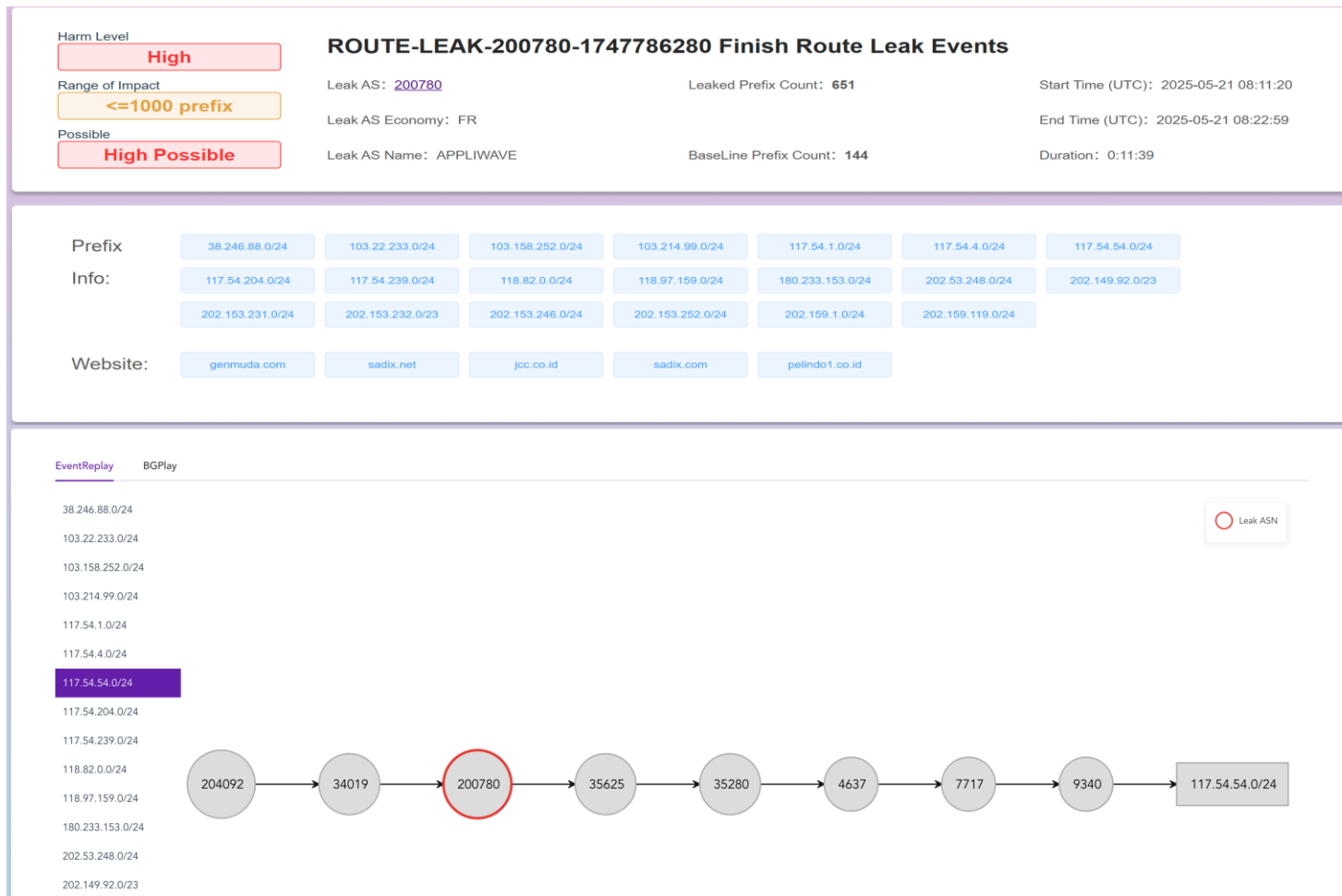


All the paths affected.

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

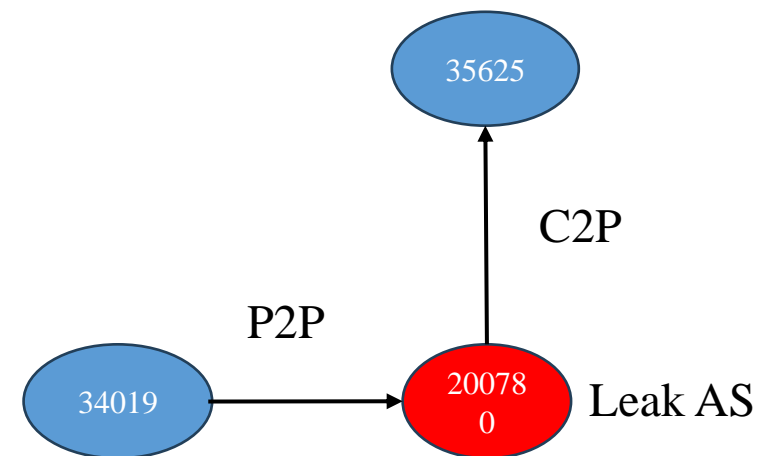
Route Leak Detail



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

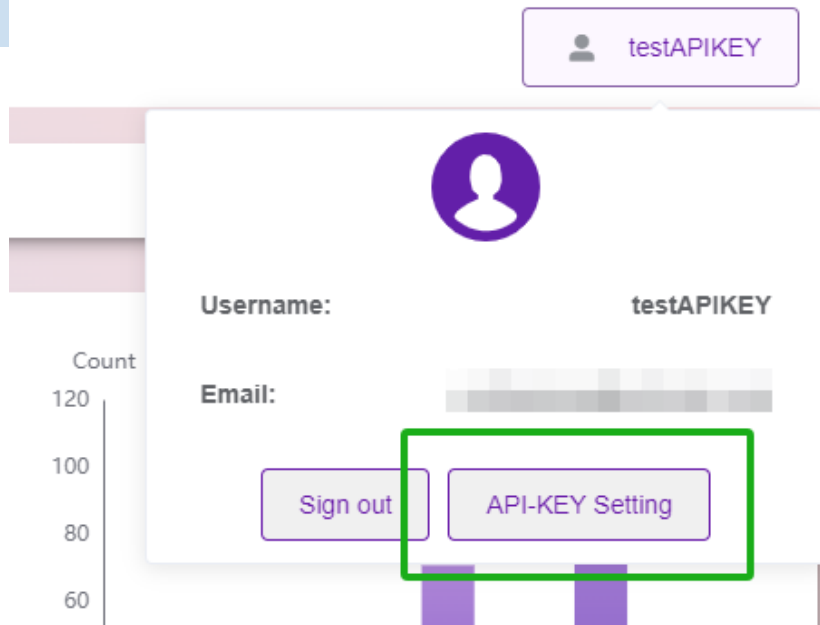
A total of 651 prefixes were leaked, with 20 sample prefixes listed in the prefix information.

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



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

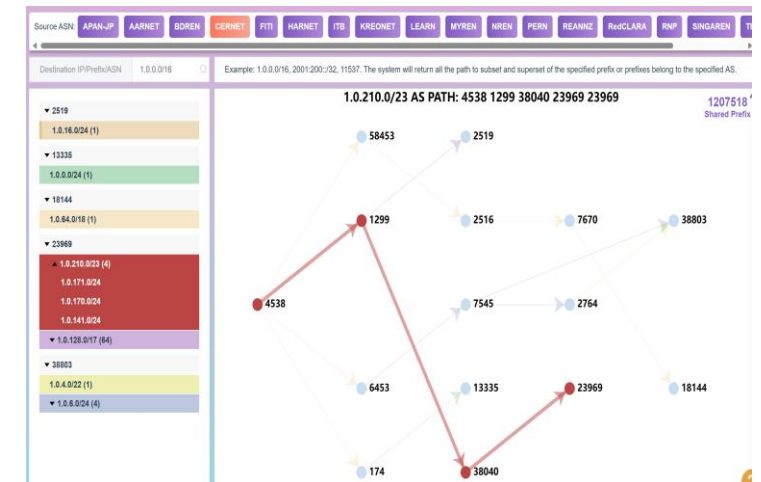
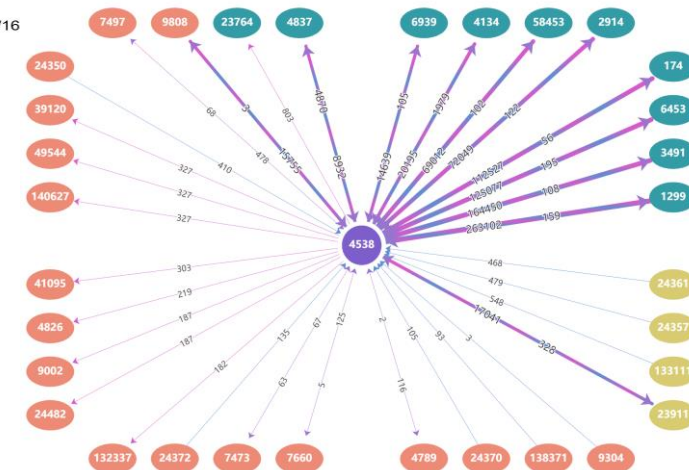
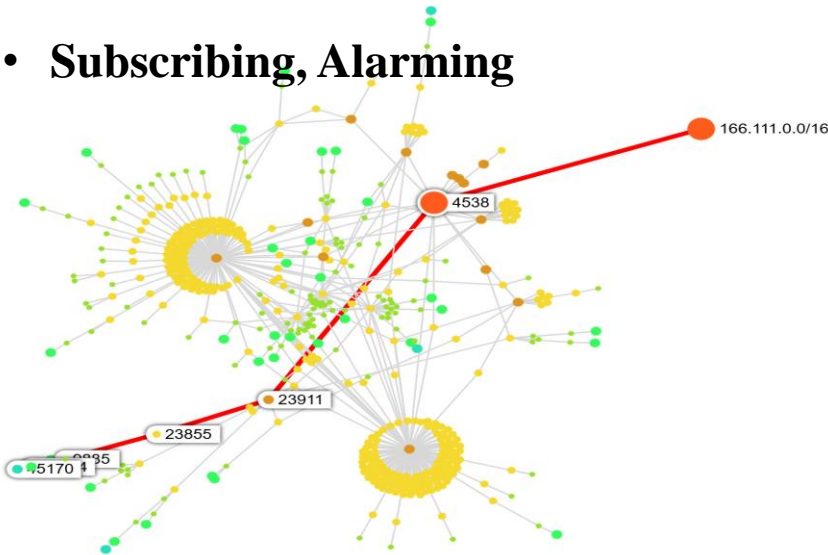
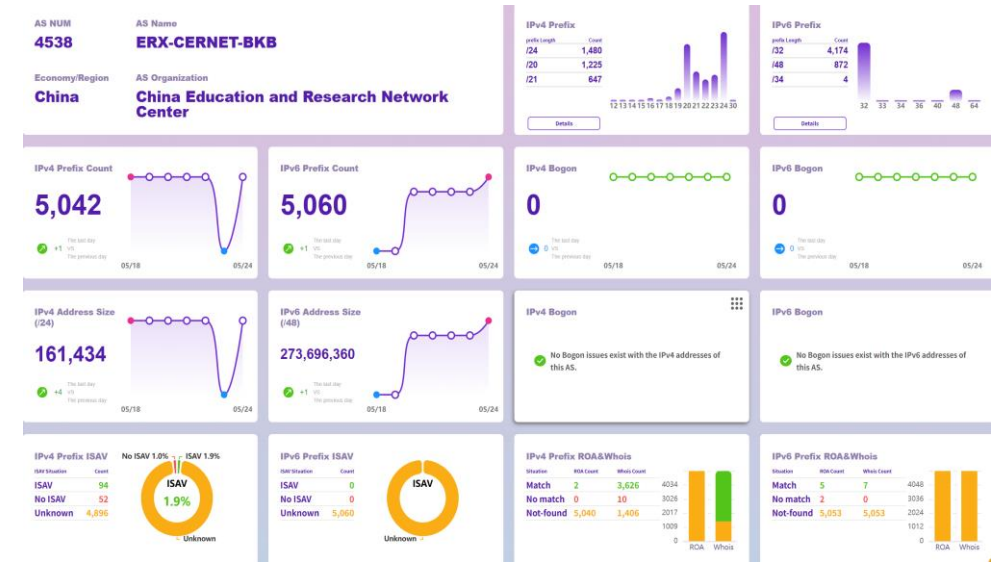
Find Condition (Support mongo scripts)

- > 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

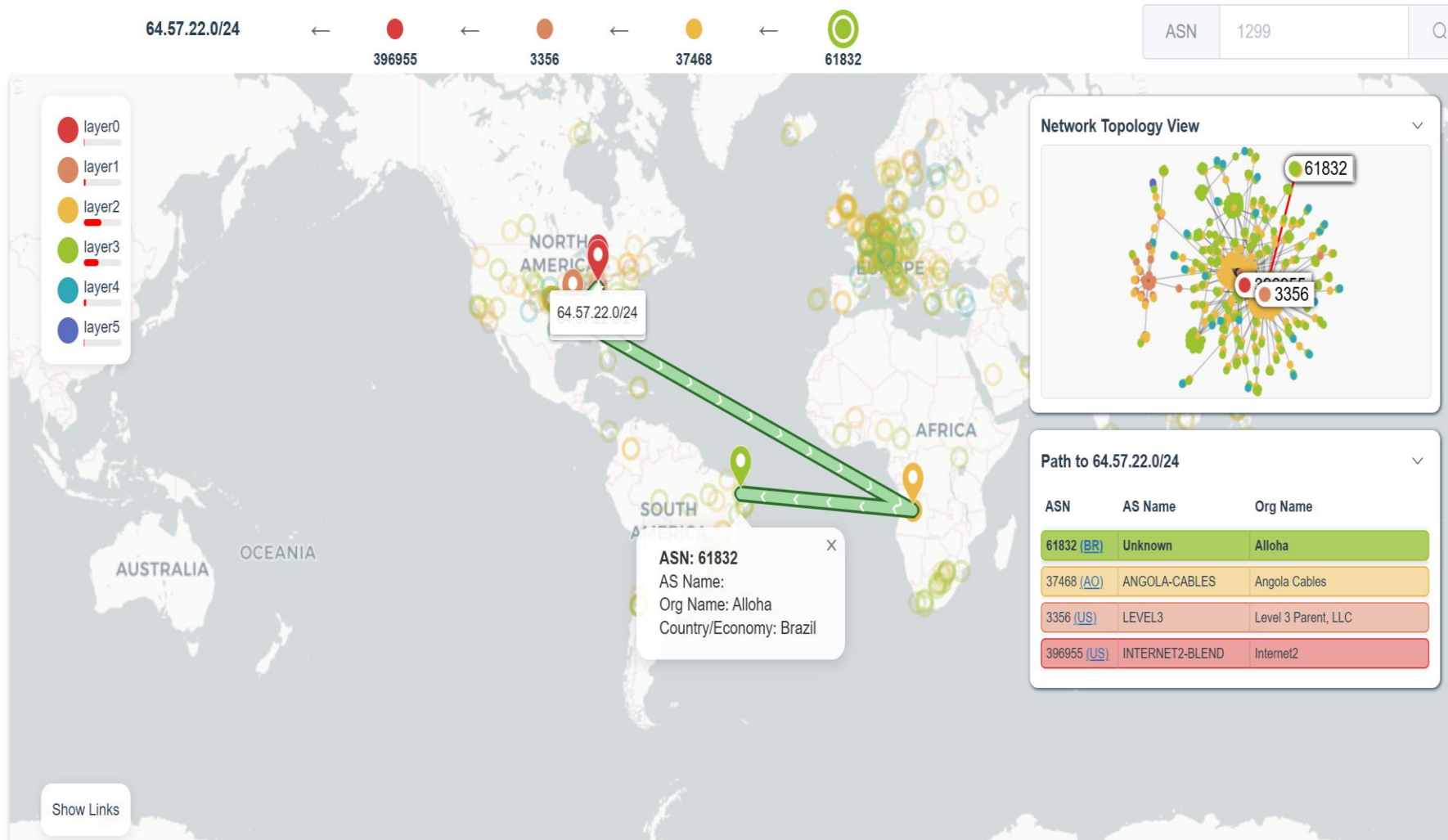
```
{
  "type": "Possible Hijack",
  "condition": {}
}
```

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

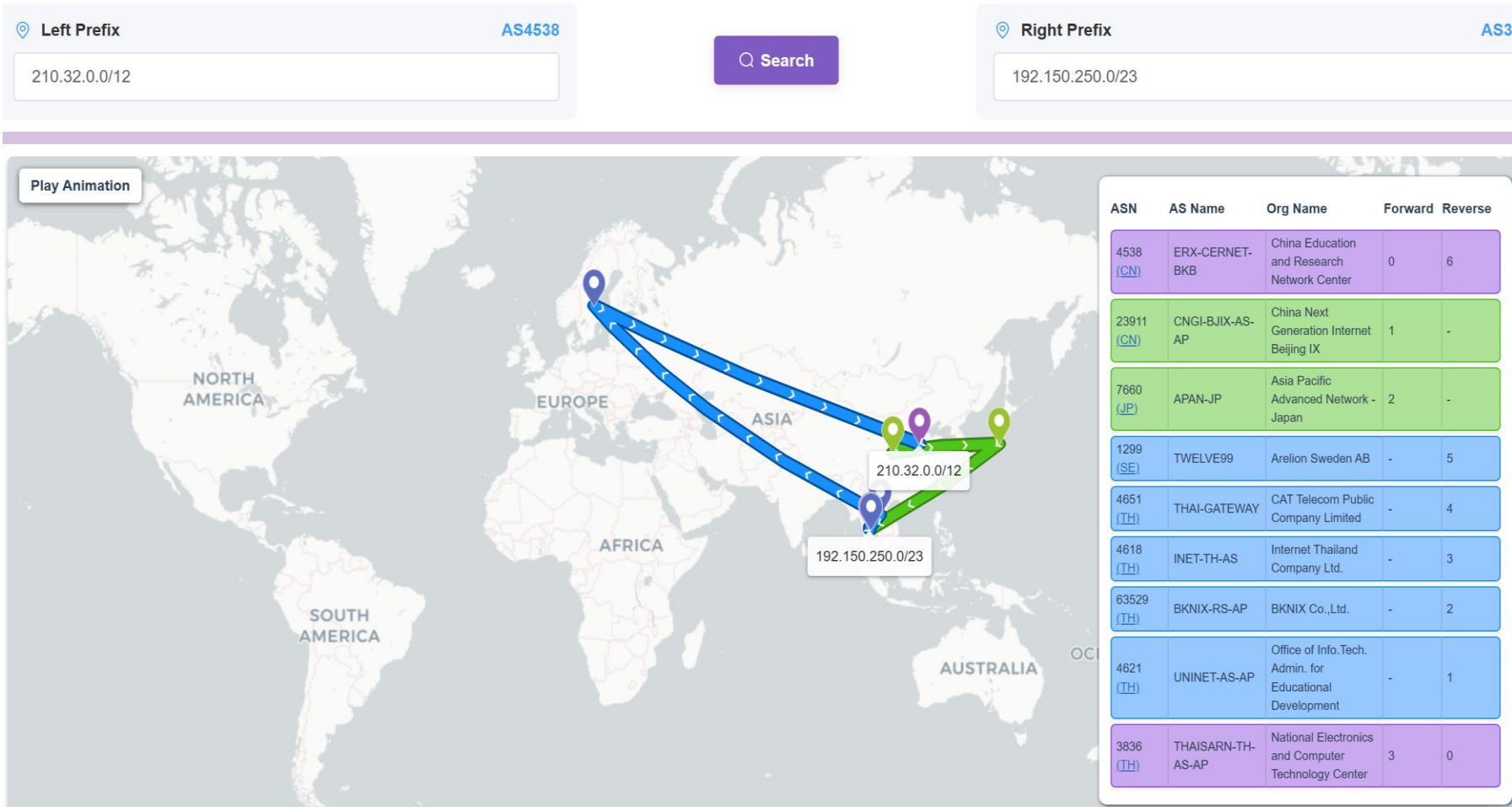


Reverse Routing Path (Map)



- 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 information will be listed in the right table.

Bi Routing Path (Map)



- 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.

Peering DB Info

DragonLab | BGPWatch

HomeAnomalyDashBoardRoutingPathToolsSubscribeAboutDocumentation

LoginRegister

4134

BasicIPv4 PeersIPv6 PeersWhoisPeeringDB

Last Update: 2024-01-14

OrganizationChina Telecom

Also Known AsChinaNet

Long Name

Company Website<http://en.chinatelecom.com.cn/>

ASN4134

IRR as-set/route-setRADB:AS-CN

Route Server URL

Looking Glass URL<https://ipms.chinatelecomglobal.com/public/lookglass/lookglassDisclaimer.html>

Network TypesNSP

IPv4 Prefixes24000

IPv6 Prefixes10000

Traffic Levels100+Tbps

Traffic RatiosBalanced

Geographic ScopeGlobal

Protocols Supported

- ☒ Unicast IPv4
- ☐ Multicast
- ☒ IPv6
- ☐ Never via route servers

Last Updated2024-11-21T07:52:14Z

Public Peering Info Updated2024-05-28T00:54:51Z

Peering Facility Info Updated2023-08-13T02:58:02Z

Contact Info Updated2023-03-22T08:42:00Z

Notes

RIR Statusok

RIR Status Updated2024-06-26T04:47:55Z

Public Peering Exchange Points

Exchange	ASN	IPv4	IPv6	Speed Port Location	RS Peer
Equinix Miami	4134	198.32.242.217	2001:504:0:6::4134:1	10G	<input type="checkbox"/>
LINX LON1: Main	4134	195.66.225.54	2001:7f8:4::1026:1	100G	<input type="checkbox"/>
Any2West	4134	206.72.210.117		10G	<input type="checkbox"/>
DE-CIX New York: DE-CIX New York Peering LAN	4134	206.82.104.247	2001:504:36::1026:0:1	10G	<input type="checkbox"/>
AMS-IX	4134	80.249.212.76	2001:7f8:1::a500:4134:1	20G	<input type="checkbox"/>
DE-CIX Frankfurt: DE-CIX Frankfurt Peering LAN	4134	80.81.195.33	2001:7f8::1026:0:2	100G	<input type="checkbox"/>
AMS-IX	4134	80.249.214.131	2001:7f8:1::a500:4134:2	100G	<input checked="" type="checkbox"/>
Asteroid Mombasa: Main	4134	196.60.66.29	2001:7f8:b6:2::1026:1	10G	<input checked="" type="checkbox"/>

Interconnection Facilities

Facility	ASN	Country	City
CoreSite - Los Angeles (LA1)	4134	United States	Los Angeles
One Wilshire			
Equinix SV1/SV5/SV10 - Silicon Valley, San Jose	4134	United States	San Jose
Equinix LD8 - London, Docklands	4134	United Kingdom	London
Digital Realty Frankfurt FRA1-16	4134	Germany	Frankfurt
Equinix MI1 - Miami, NOTA	4134	United States	Miami
Equinix DC1-DC15, DC21 - Ashburn	4134	United States	Ashburn
Digital Realty NYC (60 Hudson)	4134	United States	New York
Flexential - Portland/Hillsboro 2 (PDX02)	4134	United States	Hillsboro
Equinix AM5 - Amsterdam, Schepenbergweg	4134	Netherlands	Amsterdam
Equinix FR4 - Frankfurt, West	4134	Germany	Frankfurt

Peering Policy Information

Peering Policy

General PolicySelective

Multiole LocationsPreferred

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

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