Developing a Collaborative BGP Routing Analyzing and Diagnosing Platform

Changqing An, Jilong Wang

Rennes, France

12 JUNE, 2024

tnc24
RENDEZVOUS À RENNES
Rennes, France | 10-14 JUNE 2024

Co-funded by the European Union

GÉANT

Outline

- Background
- BGP Hijacking Detection Algorithm
- Functionality of the BGPWatch Platform
- BGP Route Sharing and Looking Glass Platform
- Future Work

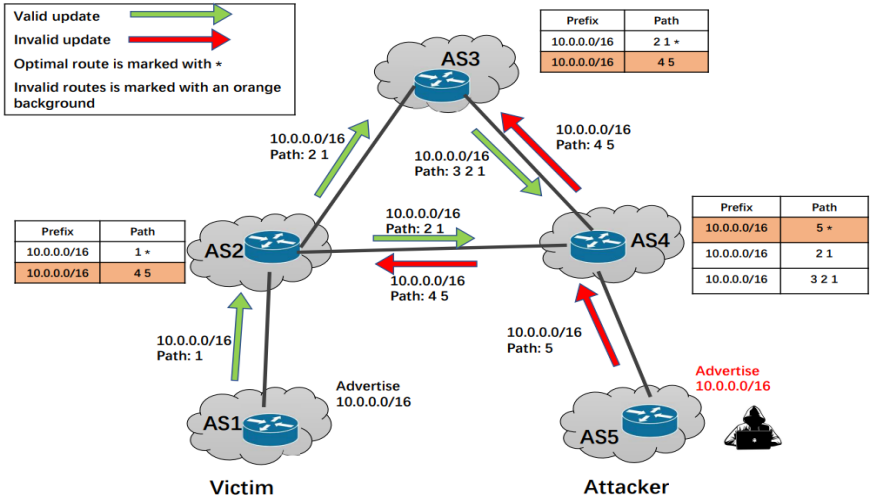
Collaborative Community

– **Work of 19 organizations (listed alphabetically)**

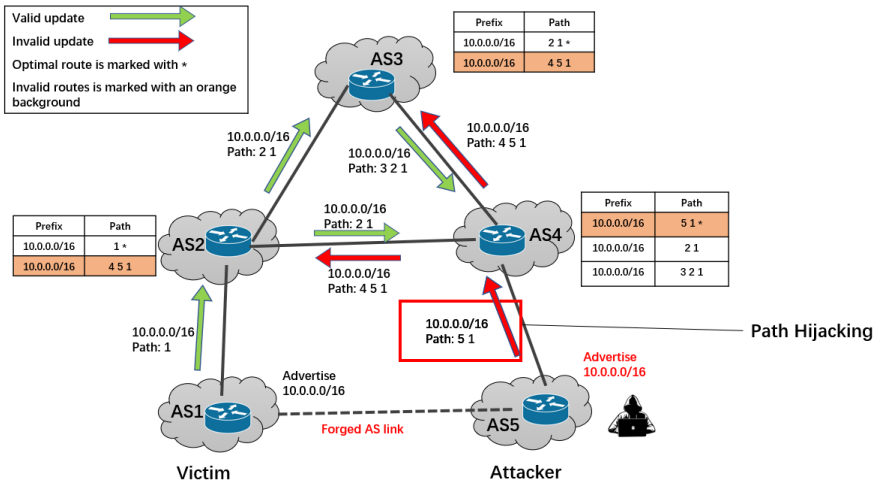
- AARNET (AU)
- APAN-JP (JP)
- BdREN (BD)
- CERNET (CN)
- DOST-ASTI (PREGINET, PH)
- ERNET (IN)
- Gottingen University (DE)
- HARNET (JUCC, HK)
- ITB (ID)
- KREONET (KR)
- LEARN (LK)
- MYREN (MY)
- NREN (NP)
- PERN (PK)
- REANNZ (NZ)
- SingAREN (SG)
- Surrey University (UK)
- ThaiREN (TH)
- TransPAC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

BGP Hijacking

BGP hijacking often leads to catastrophic consequences



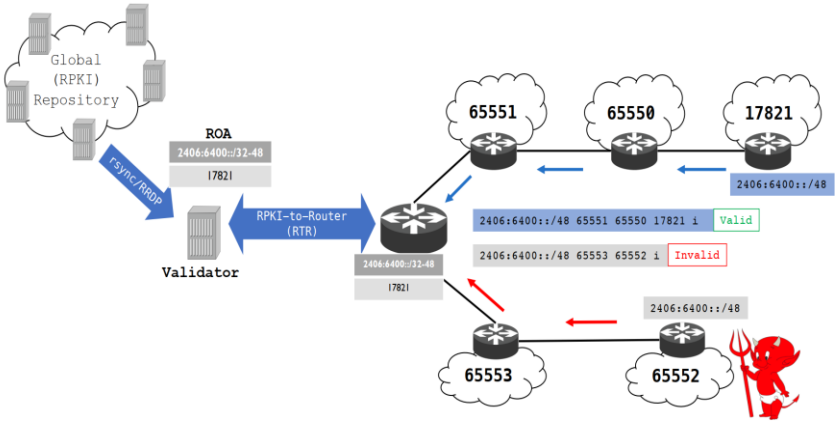
Prefix Hijacking



Path Hijacking

Solutions to BGP Hijacking

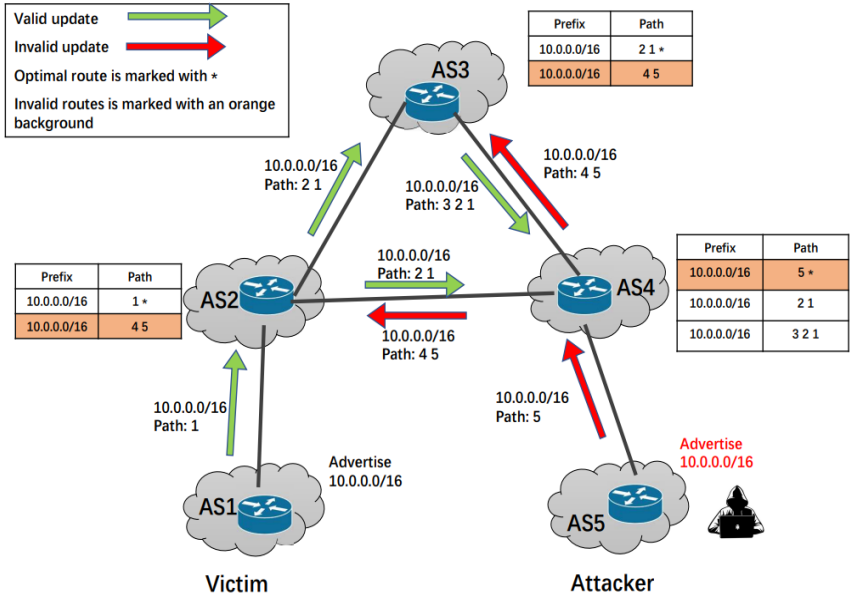
- Preventing the hijacking before it happens
  - RPKI (Resource Public Key Infrastructure)
  - ASPA(Autonomous System Provider Authorization)
- Monitoring to detect the hijacking
  - Route Views
  - RIPE RIS
  - BGPstream
  - GRIP
- Mitigating the hijacking
  - Announcing a more specific prefix
  - Contact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



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

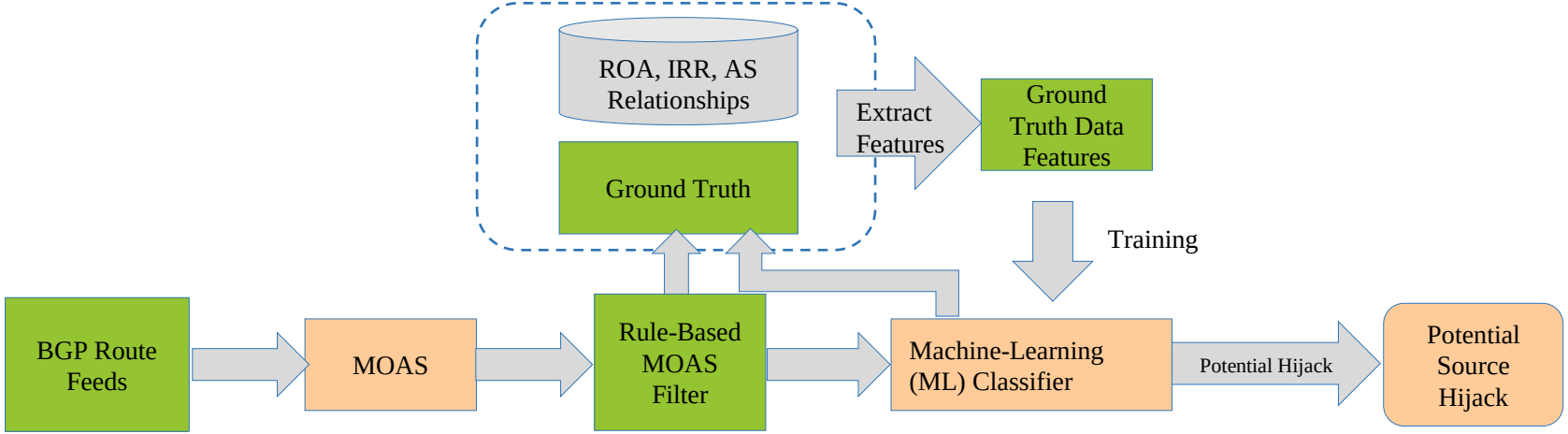
MOAS and BGP Prefix Hijacking

- MOAS (Multiple Origin AS) : multiple ASes originate the same 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

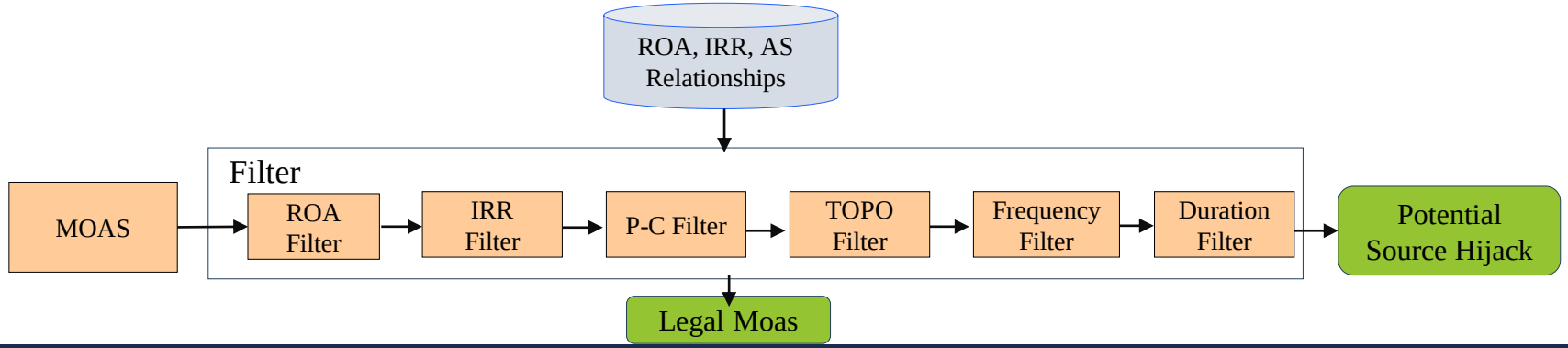
A Rules and Machine Learning Combined Method



- 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.

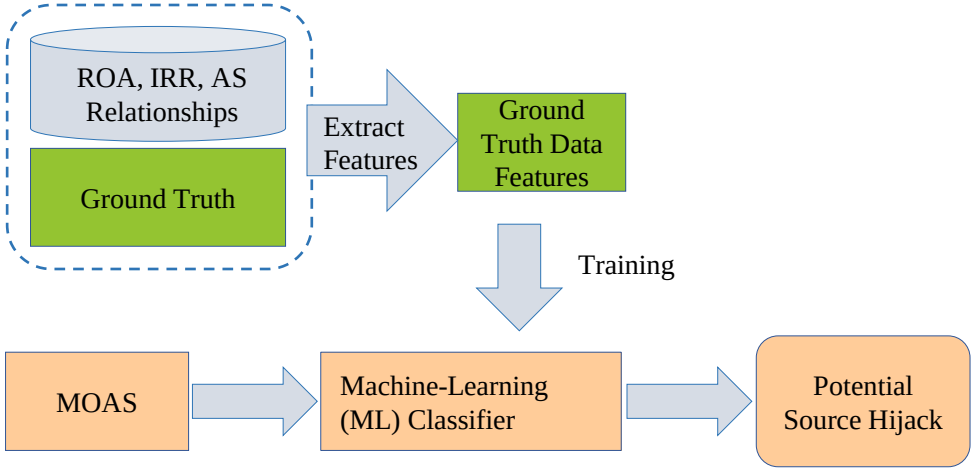
Rule based Filtering

- 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

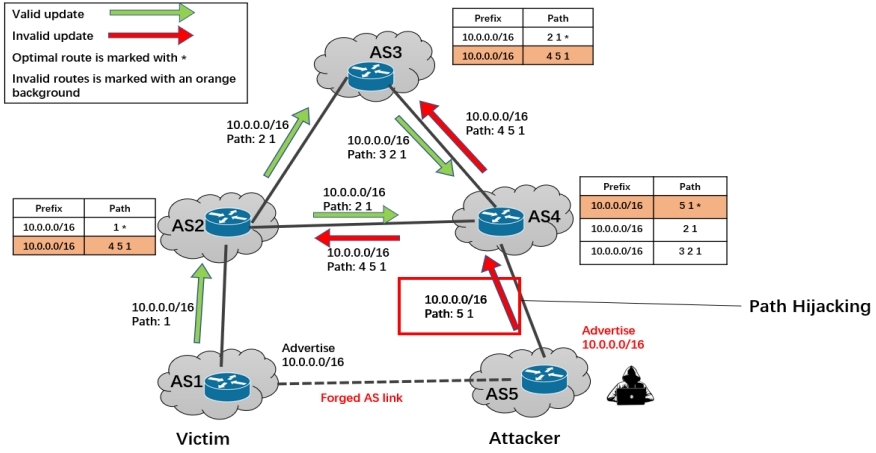


Result:

Precision	Recall	Accuracy
0.9410	0.9570	0.9622

Path Hijacking Detection

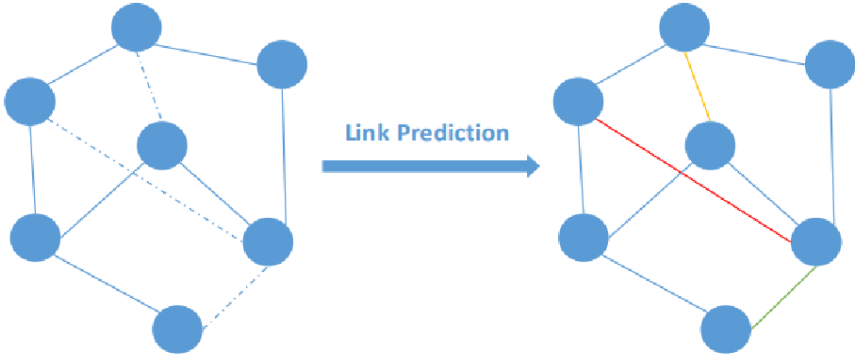
- Path hijacking can evade MOAS, but usually cause unseen AS link
- State of the art detection technique
  - Treat all unseen links appearing in the control plane as suspicious event
  - Then validate the event through the data-plane probing
- Limitation
  - Unseen links are very common
  - Intense data-plane workload
  - Inefficient and difficult to guarantee real-time



Detecting Fake AS-PATHs based on Link Prediction

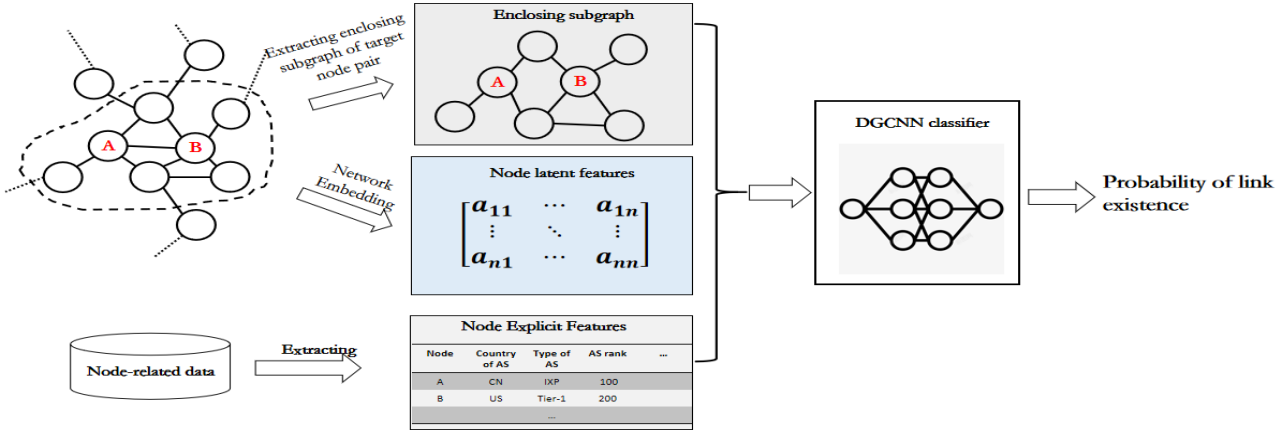
- Evaluate the authenticity of unseen links with link prediction and filter the benign unseen links
- Link prediction: a technique for inferring whether a link is likely to exist between two nodes from an existing observable portion of the network
- Is AS link predictable? Graph characteristics of AS-level topology
  - Power-law distribution
  - Negative degree-degree correlation
  - Hierarchical structure
  - AS links usually connect two ASes

  with the same properties.



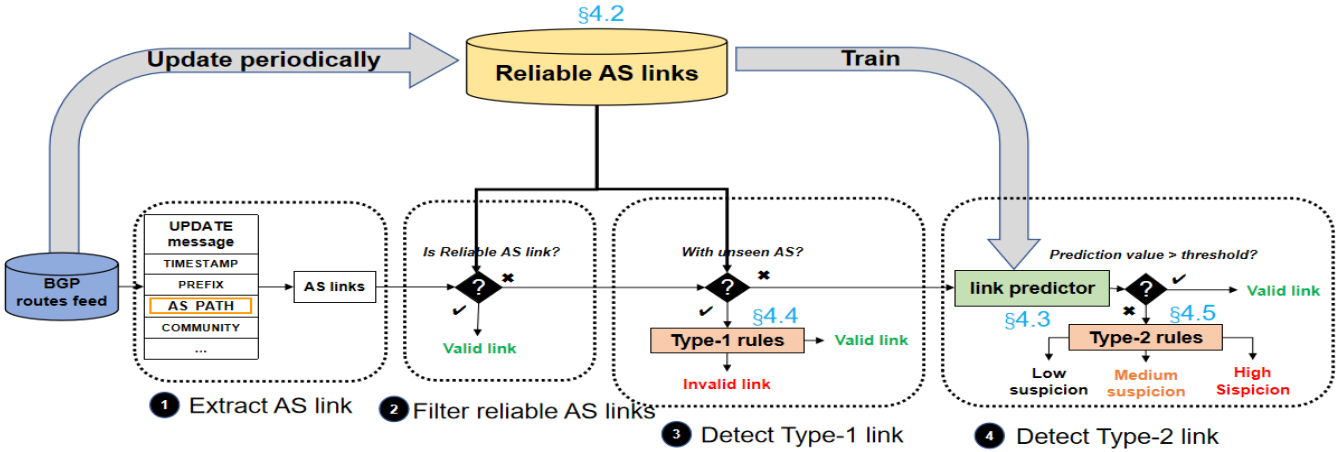
Unseen Link Prediction

- 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



Framework: Combining Link Prediction and Rules

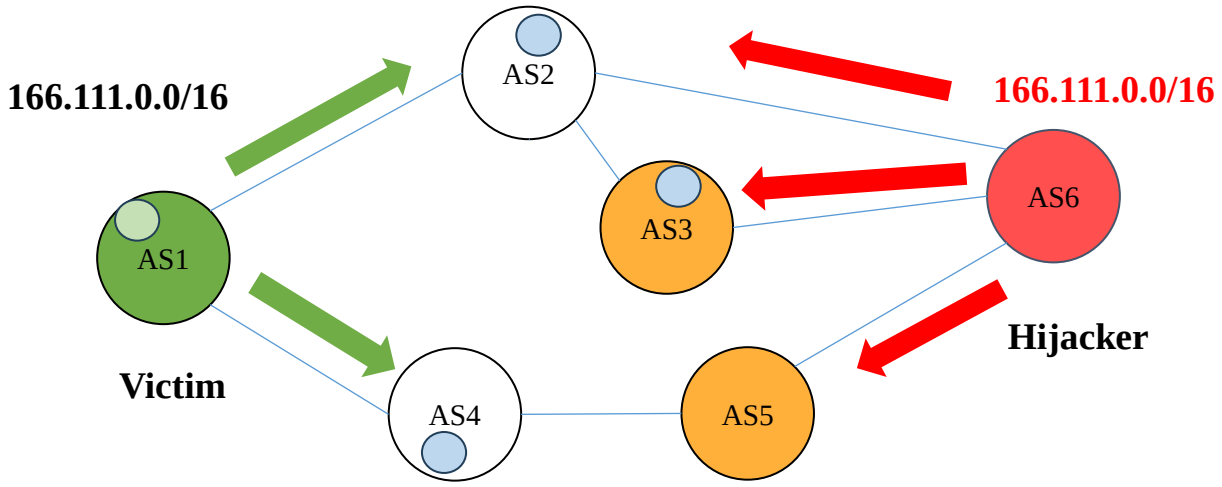
- Link prediction is used to find suspicious unseen links, and rules are used to improve the confidence level
- The accuracy of positive AS-PATHs is about 99.5%
- The accuracy of Type-1 path hijacking is 87.5%



Rules

- If any rules are successfully matched, the suspicious score is increased 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 editing distance between two ASN digits of a suspect link is not 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.

Further Data Plane Probing



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 reachability
- Approach: Test representative service from Looking Glass VPs

Further Data Plane Probing

1. Select anchor server for the prefix/subprefix from TOP 1M domain name.
2. Select looking glass vantage point from affected ASes and unaffected ASes.
3. Check reachability during attack and after attack. Ping? Tracert?
4. Evaluate the possibility of Hijacking.

45.174.10.11 gtecfibra.com.br

Probe AS	Probe IP	Ping During Attack	Ping After Attack
AS7489	210.16.120.5	✗ 2024-05-15 04:09:38	✓ 2024-05-15 04:14:21
AS29182	37.46.131.230	✗ 2024-05-15 04:09:38	✓ 2024-05-15 04:14:20
AS35297	91.204.213.202	✗ 2024-05-15 04:09:38	✓ 2024-05-15 04:14:20
AS36352	192.227.239.227	✗ 2024-05-15 04:09:38	✓ 2024-05-15 04:14:20
AS44066	212.224.76.52	✗ 2024-05-15 04:09:38	✓ 2024-05-15 04:14:20
AS53080	187.95.0.32	✓ 2024-05-15 04:09:38	✓ 2024-05-15 04:14:22
AS197071	91.217.251.2	✗ 2024-05-15 04:09:38	✓ 2024-05-15 04:14:20
AS200651	185.165.171.51	✗ 2024-05-15 04:09:38	✓ 2024-05-15 04:14:20
AS211211	193.42.112.3	✗ 2024-05-15 04:09:38	✓ 2024-05-15 04:14:20
AS267554	201.182.166.26	✓ 2024-05-15 04:09:38	✓ 2024-05-15 04:14:21

177.74.98.130 optimusnetwork.net.br

Probe AS	Probe IP	Ping During Attack
AS1653	193.10.220.163	✓ 2024-05-15 07:19:32
AS4739	203.16.215.13	✓ 2024-05-15 07:19:32
AS6762	195.22.210.237	✓ 2024-05-15 07:19:32
AS13830	161.129.152.2	✓ 2024-05-15 07:19:32
AS23855	203.30.39.80	✓ 2024-05-15 07:19:32
AS41108	91.228.52.157	✓ 2024-05-15 07:19:32
AS136088	103.87.228.9	✓ 2024-05-15 07:19:32
AS202015	79.141.162.45	✓ 2024-05-15 07:19:32
AS204957	82.118.21.55	✓ 2024-05-15 07:19:32
AS395092	45.155.37.12	✓ 2024-05-15 07:19:32

Example of a Hijacking Event

45.174.10.0/23-HIJACK1715746169 Possible Hijack Events

Victim AS: 268938

Victim Economy: BR (Brazil)

Victim AS Name: no data

Hijacker AS: 268342

Hijacker Economy: BR (Brazil)

Hijacker AS Name: no data

Start Time (UTC): 2024-05-15 04:09:29

End Time (UTC): 2024-05-15 04:14:15

During Time: 0:4:46

45.174.10.11 gtecfibra.com.br

Probe AS	Probe IP	Ping During Attack		Ping After Attack	
AS7489	210.16.120.5	✗	2024-05-15 04:09:38	✓	2024-05-15 04:14:21
AS29182	37.46.131.230	✗	2024-05-15 04:09:38	✓	2024-05-15 04:14:20
AS35297	91.204.213.202	✗	2024-05-15 04:09:38	✓	2024-05-15 04:14:20
AS36352	192.227.239.227	✗	2024-05-15 04:09:38	✓	2024-05-15 04:14:20
AS44066	212.224.76.52	✗	2024-05-15 04:09:38	✓	2024-05-15 04:14:20
AS53080	187.95.0.32	✓	2024-05-15 04:09:38	✓	2024-05-15 04:14:22
AS197071	91.217.251.2	✗	2024-05-15 04:09:38	✓	2024-05-15 04:14:20
AS200651	185.165.171.51	✗	2024-05-15 04:09:38	✓	2024-05-15 04:14:20
AS211211	193.42.112.3	✗	2024-05-15 04:09:38	✓	2024-05-15 04:14:20
AS267554	201.182.166.26	✓	2024-05-15 04:09:38	✓	2024-05-15 04:14:21

Example of a Non-hijacking Event

177.74.97.0/24-SUB-HIJACK1715757340 Ongoing Possible SubHijack Events

Victim AS: 270977

Victim Economy: BR (Brazil)

Victim AS Name: no data

Hijacker AS: 265467

Hijacker Economy: BR (Brazil)

Hijacker AS Name: no data

Start Time (UTC): 2024-05-15 07:15:40

End Time (UTC): no data

During Time: no data

177.74.98.130 optimusnetwork.net.br

Probe AS	Probe IP	Ping During Attack
AS1653	193.10.220.163	2024-05-15 07:19:32
AS4739	203.16.215.13	2024-05-15 07:19:32
AS6762	195.22.210.237	2024-05-15 07:19:32
AS13830	161.129.152.2	2024-05-15 07:19:32
AS23855	203.30.39.80	2024-05-15 07:19:32
AS41108	91.228.52.157	2024-05-15 07:19:32
AS136088	103.87.228.9	2024-05-15 07:19:32
AS202015	79.141.162.45	2024-05-15 07:19:32
AS204957	82.118.21.55	2024-05-15 07:19:32
AS395092	45.155.37.12	2024-05-15 07:19:32

Evaluate Harm Level

- Whether the prefix and AS provide critical services?

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

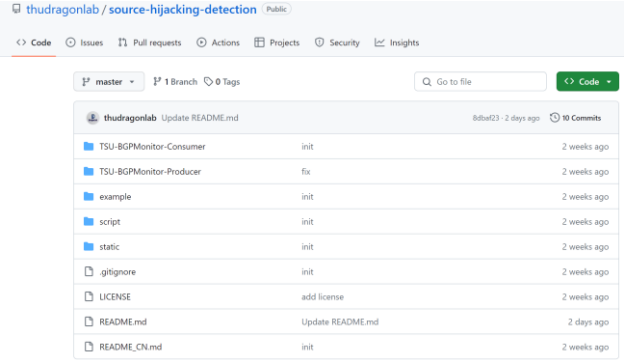
Open Source

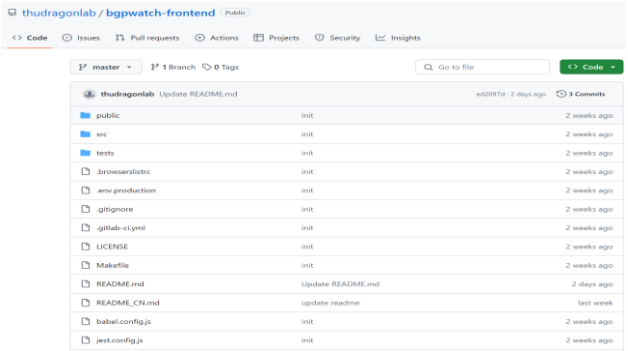
https://github.com/thudragonlab/source-hijacking-detection

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

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

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

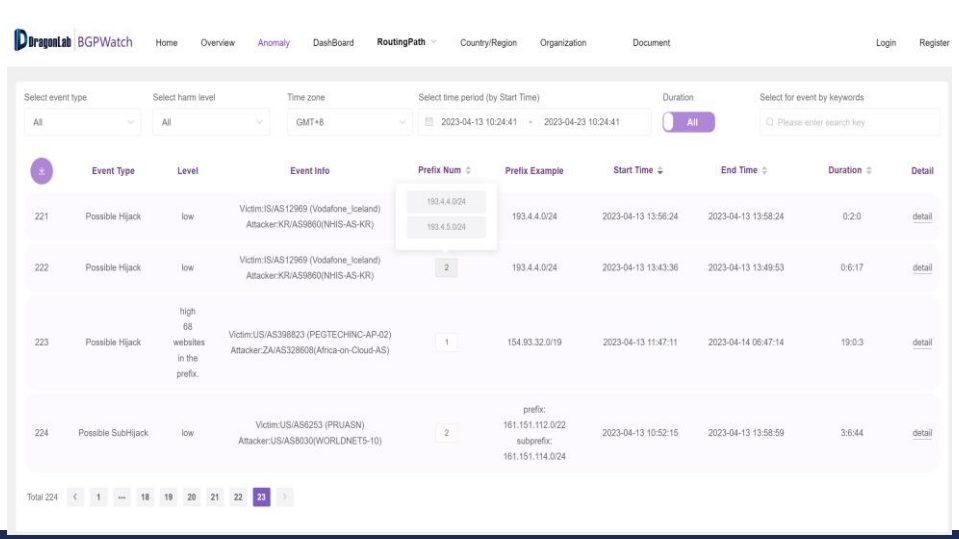




BGPWatch: Prefix Hijacking Detection Platform

- Knowledge-based real-time BGP hijacking Detection System
- Public BGP event reporting service

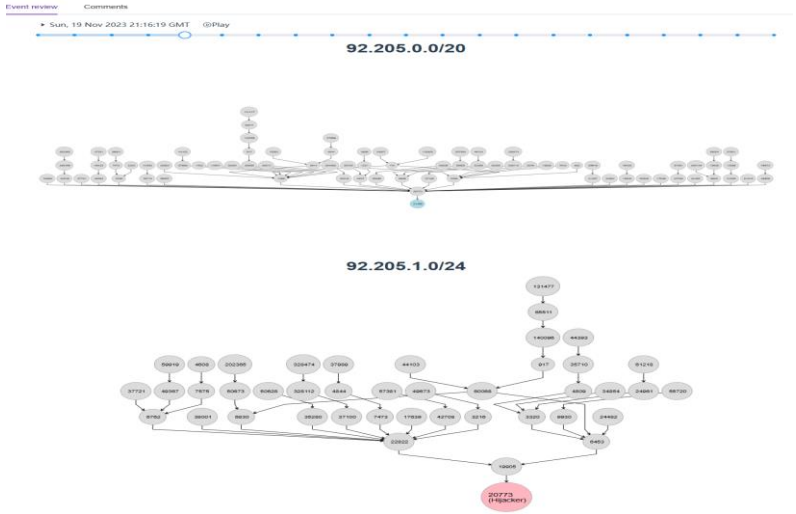
- Based on MOAS/subMOAS
- Rely on Domain Knowledge (ROA, IRR, AS relationship, routing path, accumulated information, etc.)



https://bgpwatch.cgtf.net

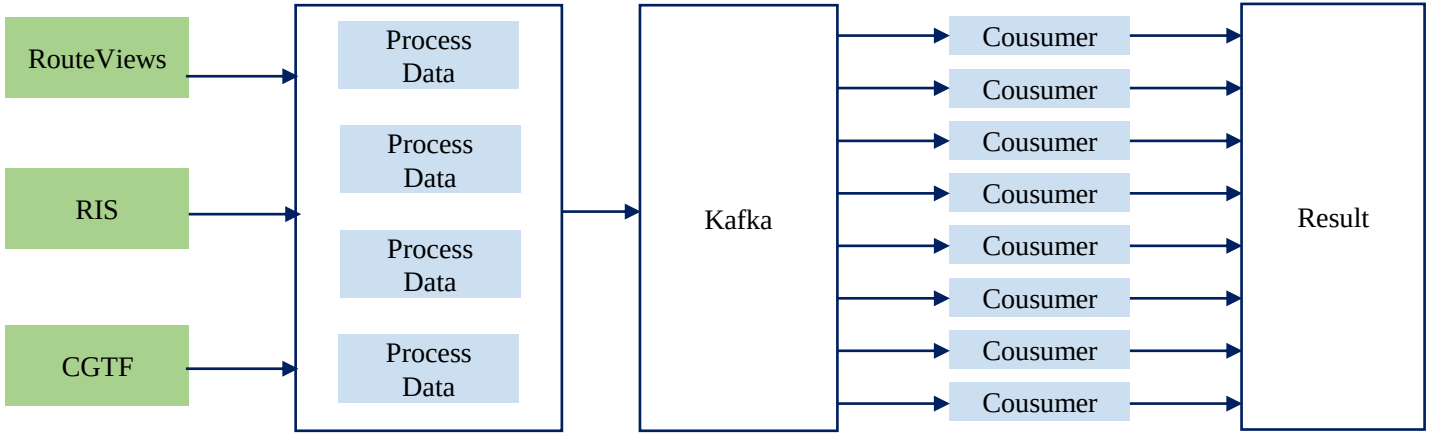
Quick Response, Event replay, Comments

- Use RIS LIVE data
- 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



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.



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).

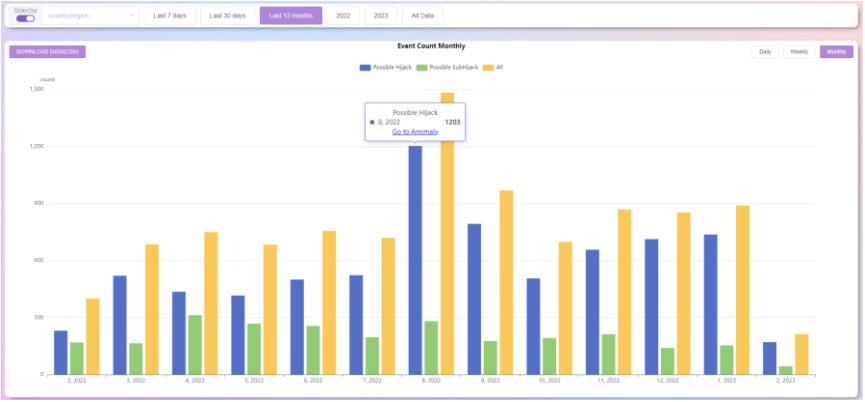
Our system shows that prefix 23.150.11.0/24 is normally announced by your 945; however, at 2023-11-18 11:00:46 (UTC), prefix 23.150.11.0/24 is also announced by 200827 Detailed information is available here.

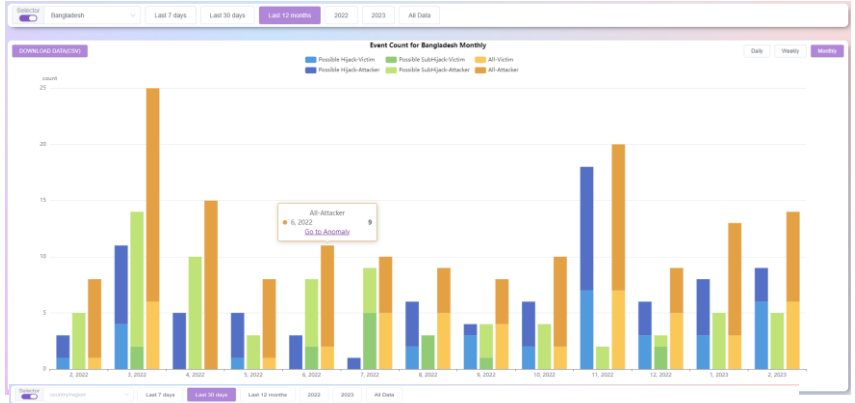
We would like to confirm with you whether this is a hijacking event or a false alarm of the system. Please click here to provide us with your feedback. Your time and response are greatly appreciated and will be very helpful for our research.

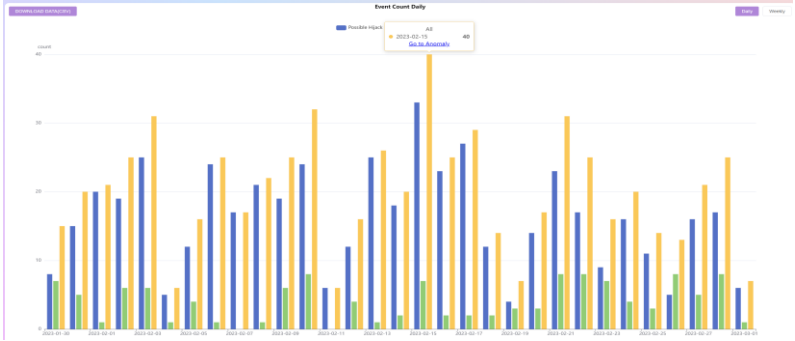
Have a good day!

Best regards,
Institute for Network Sciences and Cyberspace
Tsinghua University

Overview--Statistics for Anomaly Events







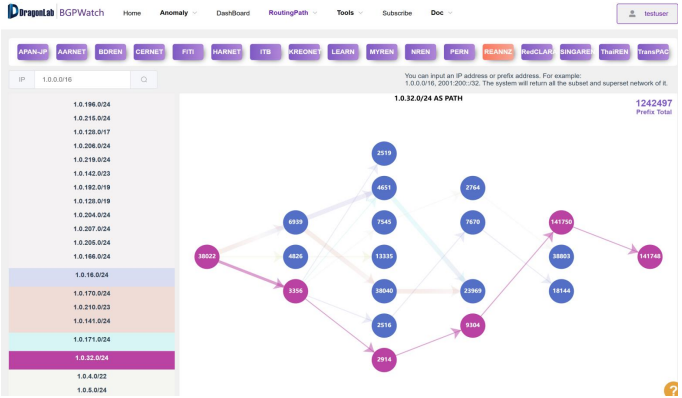
Do statistics by economy, AS,
and by yearly, monthly, weekly, and daily

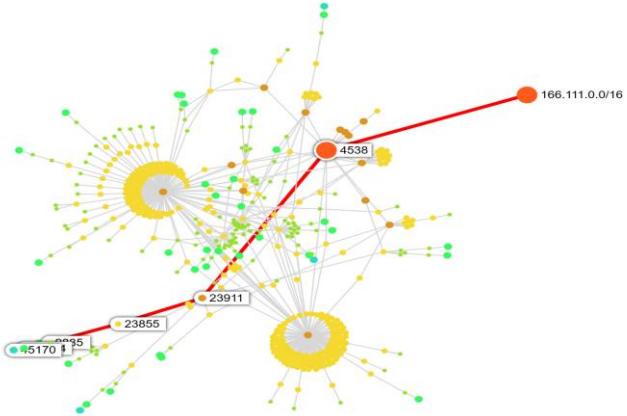
Compare with other Platforms

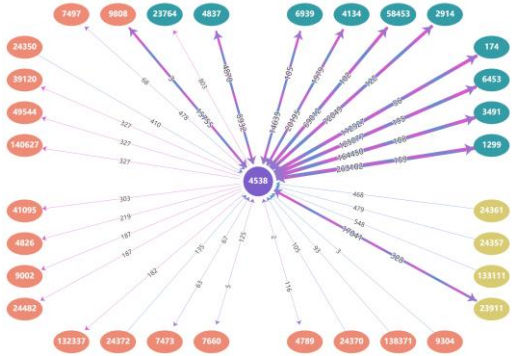
	BGPWatch	GRIP	BGPStream
Delay	2 mins delay	5 mins delay	More than 2 hours
Event replay	√	×	√
Event statistical analysis	√	×	×
Event level evaluation	√	×	×
Benign MOAS report	√	√	×
Email Alarm	√	×	×
Accuracy	High	Medium to High	Low

Tools for Network Operator

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

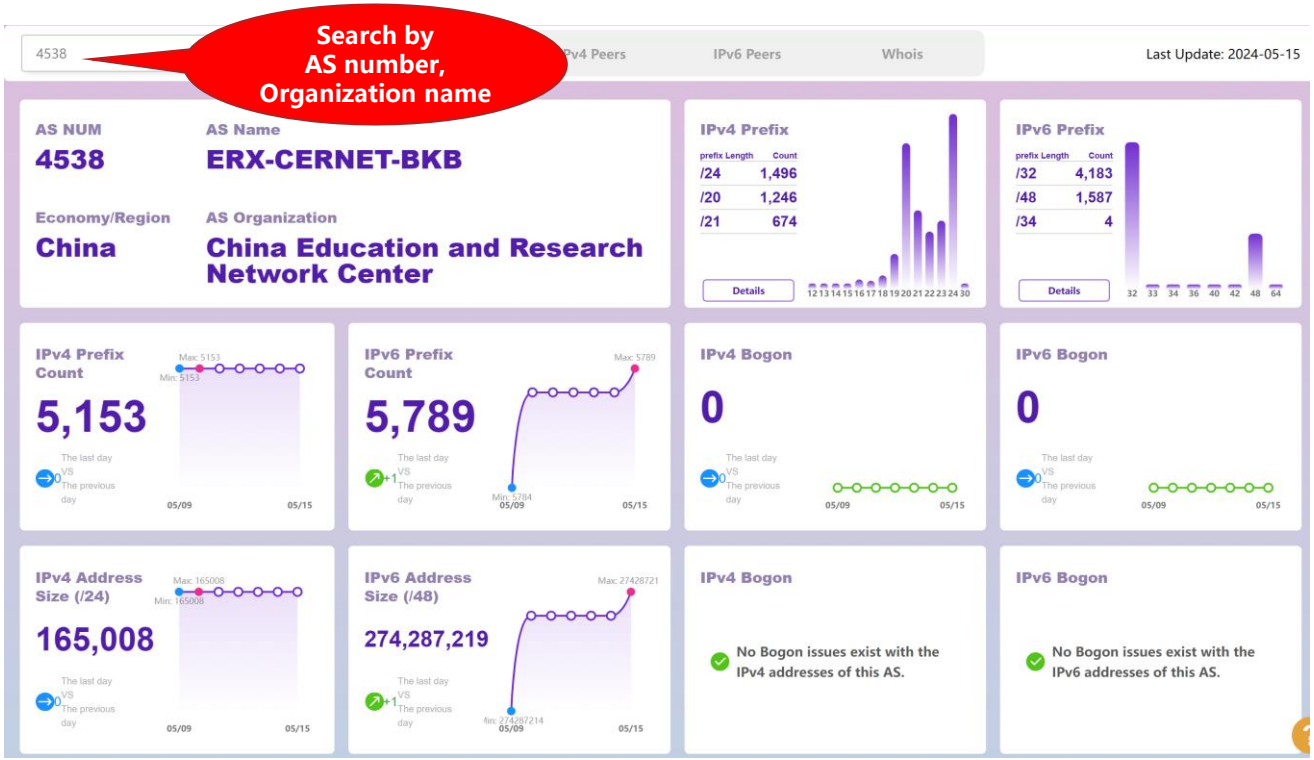




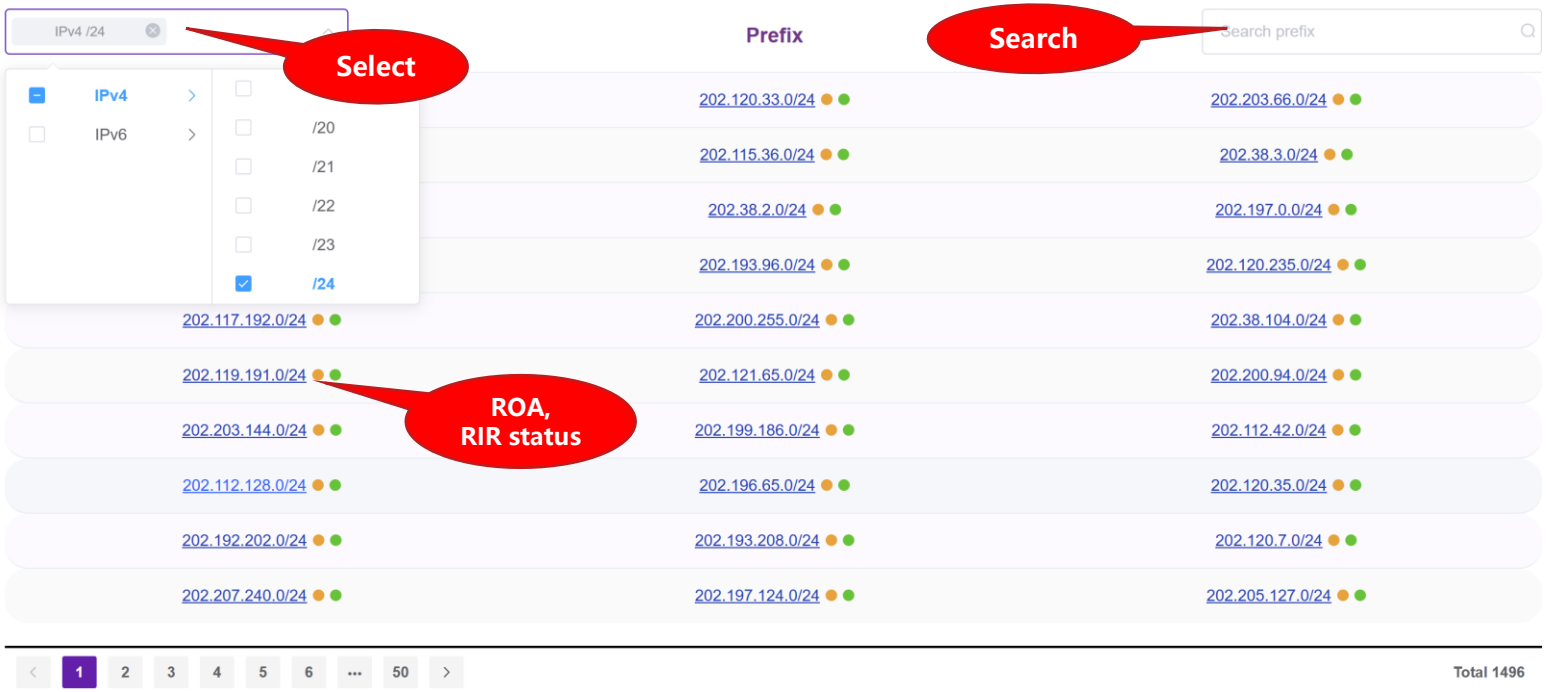


https://bgpwatch.cgtf.net

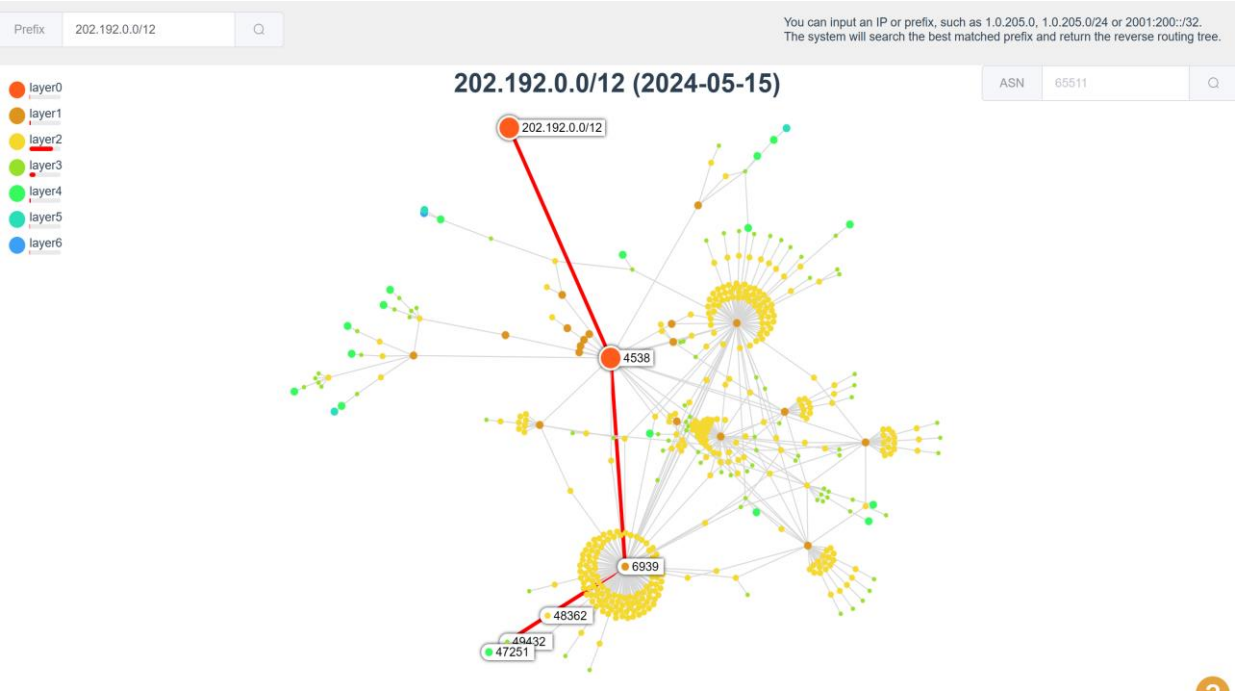
Dashboard


Search by
AS number,
Organization name
4538
Pv4 Peers
IPv6 Peers
Whois
Last Update: 2024-05-15
AS NUM
4538
AS Name
ERX-CERNET-BKB
Economy/Region
China
AS Organization
China Education and Research Network Center
IPv4 Prefix
prefix Length Count
/24 1,496
/20 1,246
/21 674
Details
IPv6 Prefix
prefix Length Count
/32 4,183
/48 1,587
/34 4
Details
IPv4 Prefix Count
5,153
IPv6 Prefix Count
5,789
IPv4 Bogon
0
IPv6 Bogon
0
IPv4 Address Size (/24)
165,008
IPv6 Address Size (/48)
274,287,219
IPv4 Bogon
No Bogon issues exist with the IPv4 addresses of this AS.
IPv6 Bogon
No Bogon issues exist with the IPv6 addresses of this AS.

Prefixes Originated from the AS

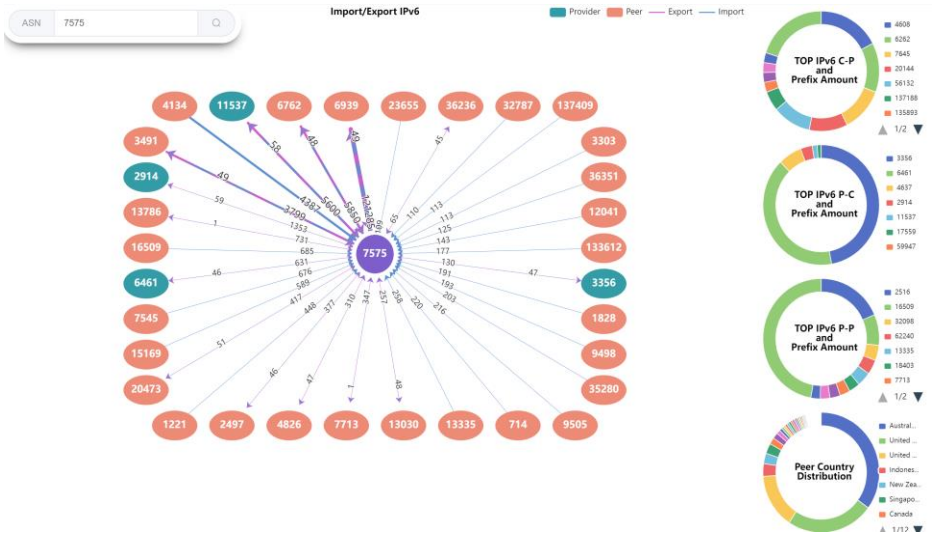


Reverse Routing Path

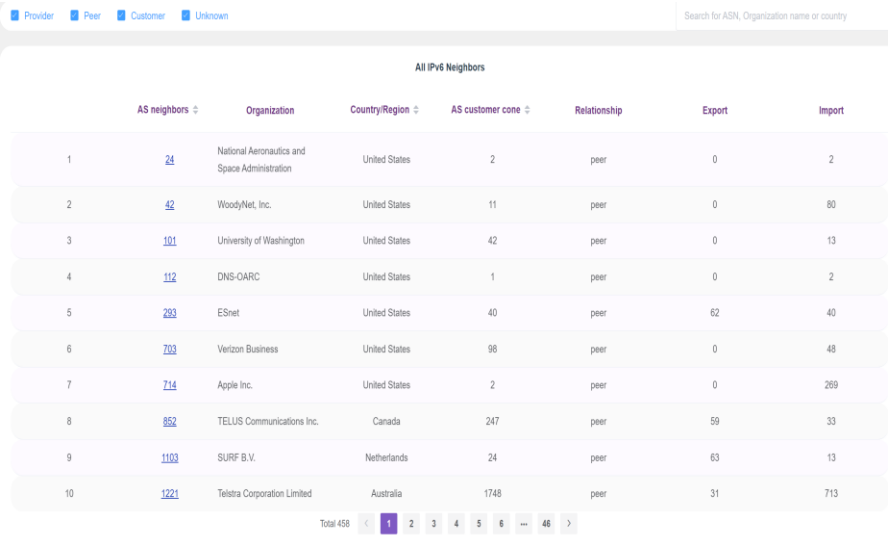


- Support Prefix / IP, IPv4 / IPv6
- The system will search the best matched prefix and return the reverse routing tree
- With better interactivity
- Click an AS or input AS number, the system will highlight the path to the AS
- The number of layers to display can be selected

Dashboard: IPv4/IPv6 Key Peers and All Neighbors Information



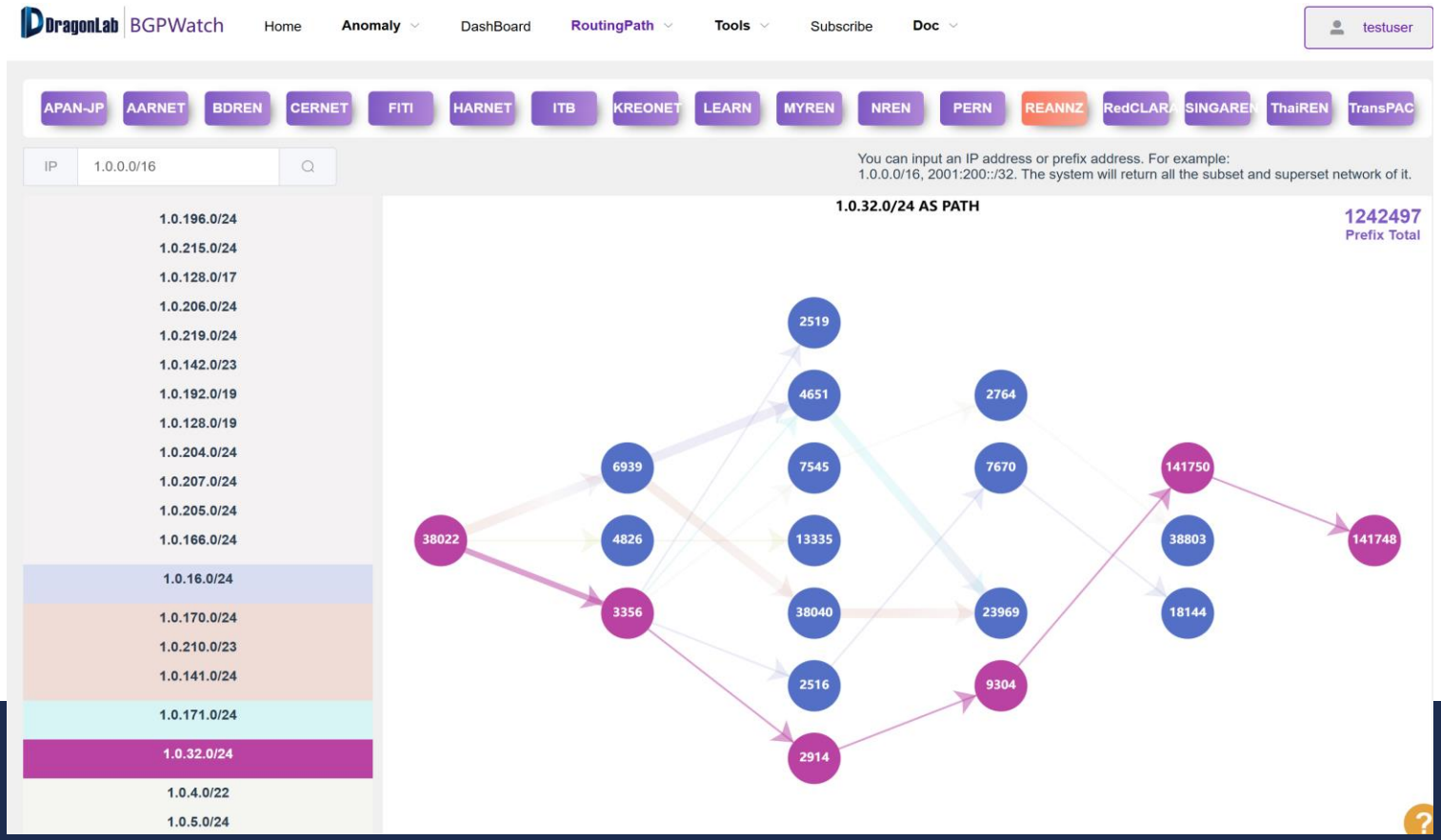
Key Neighbors



	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

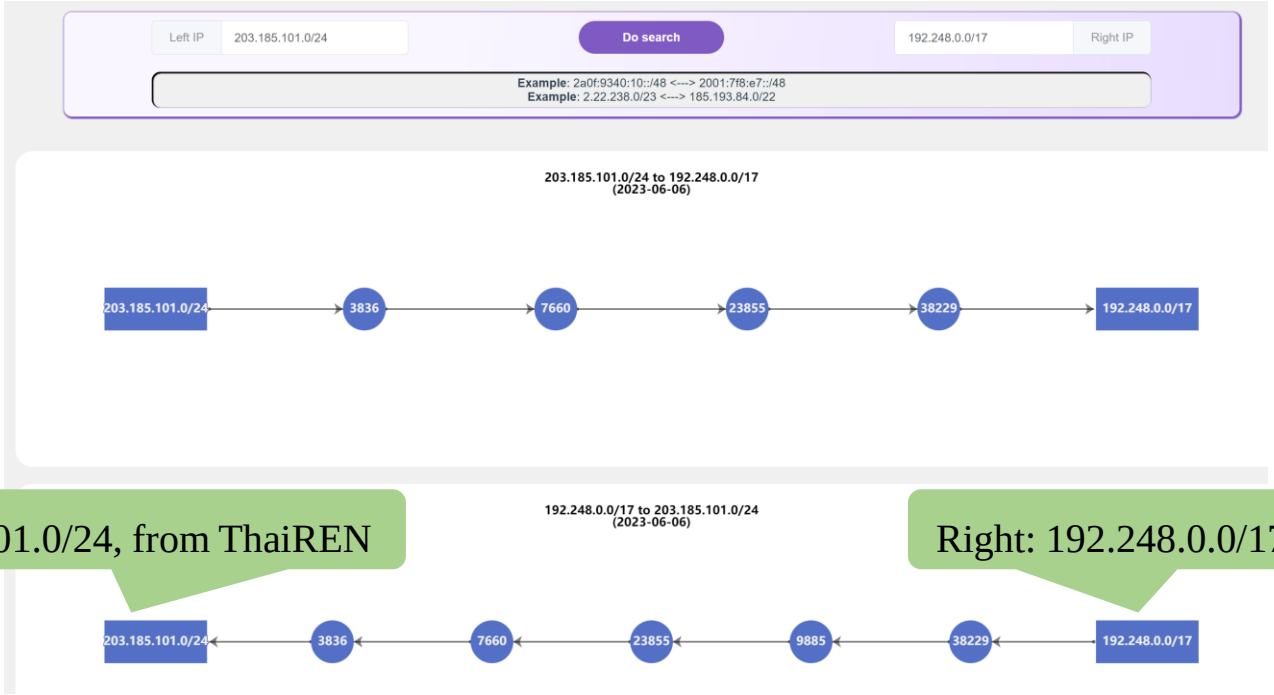
All Neighbors

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

Bi-Routing Path

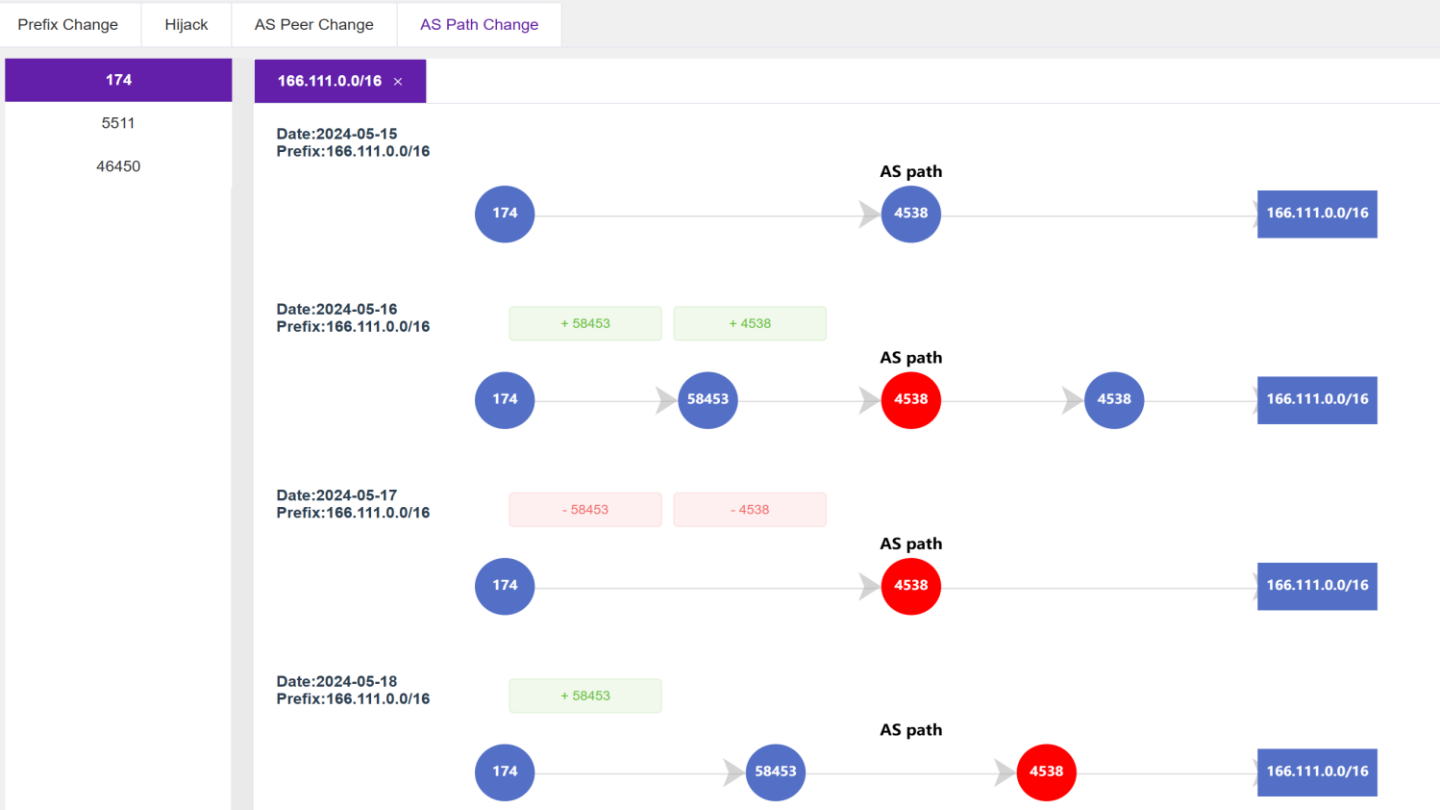


Left : 203.185.101.0/24, from ThaiREN

Right: 192.248.0.0/17, from LEARN

Support Prefix / IP, IPv4 / IPv6
Search the best matched prefix

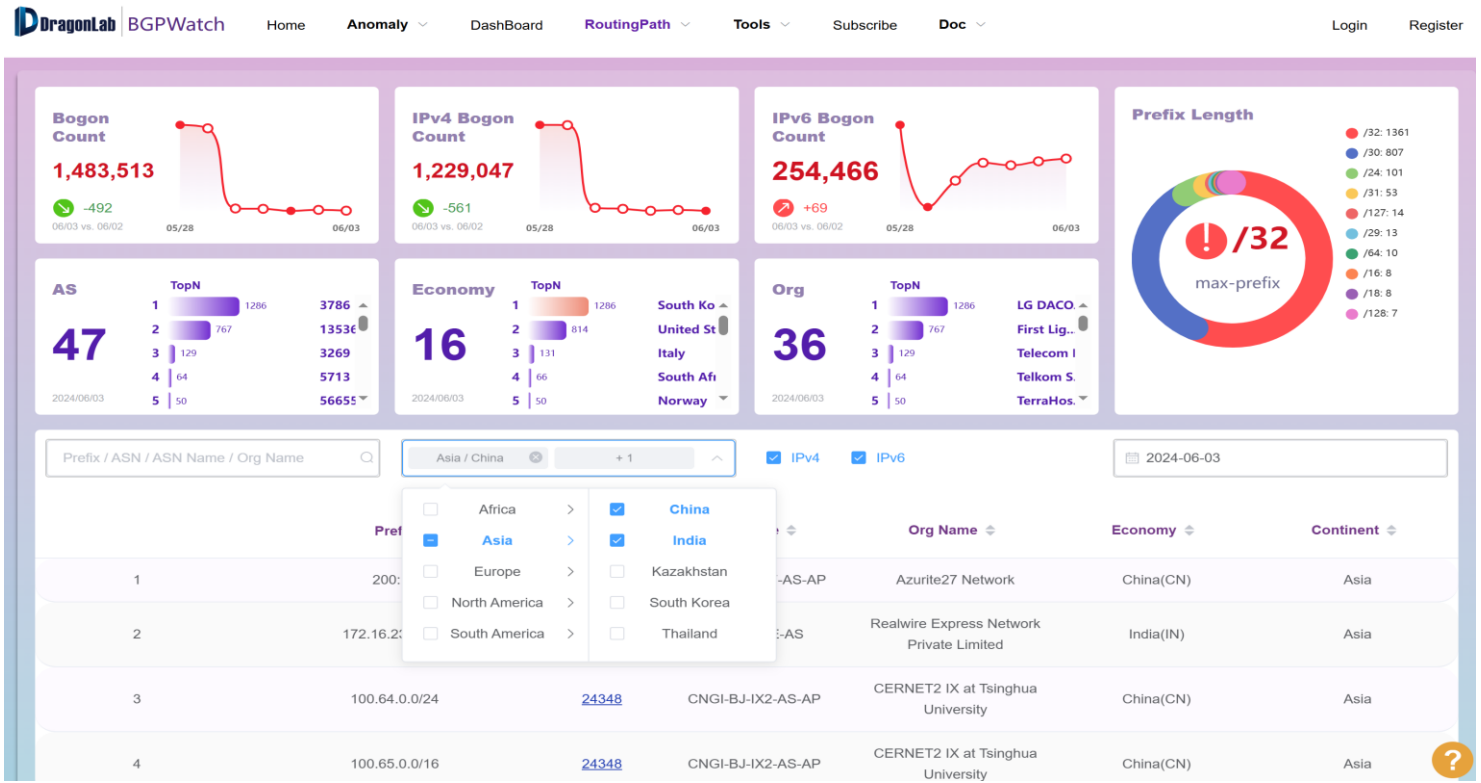
Path Change


Prefix Change
Hijack
AS Peer Change
AS Path Change
174
5511
46450
166.111.0.0/16 ×
Date:2024-05-15
Prefix:166.111.0.0/16
AS path
174
4538
166.111.0.0/16
Date:2024-05-16
Prefix:166.111.0.0/16
+ 58453
+ 4538
AS path
174
58453
4538
4538
166.111.0.0/16
Date:2024-05-17
Prefix:166.111.0.0/16
- 58453
- 4538
AS path
174
4538
166.111.0.0/16
Date:2024-05-18
Prefix:166.111.0.0/16
+ 58453
AS path
174
58453
4538
166.111.0.0/16

Router Jitter

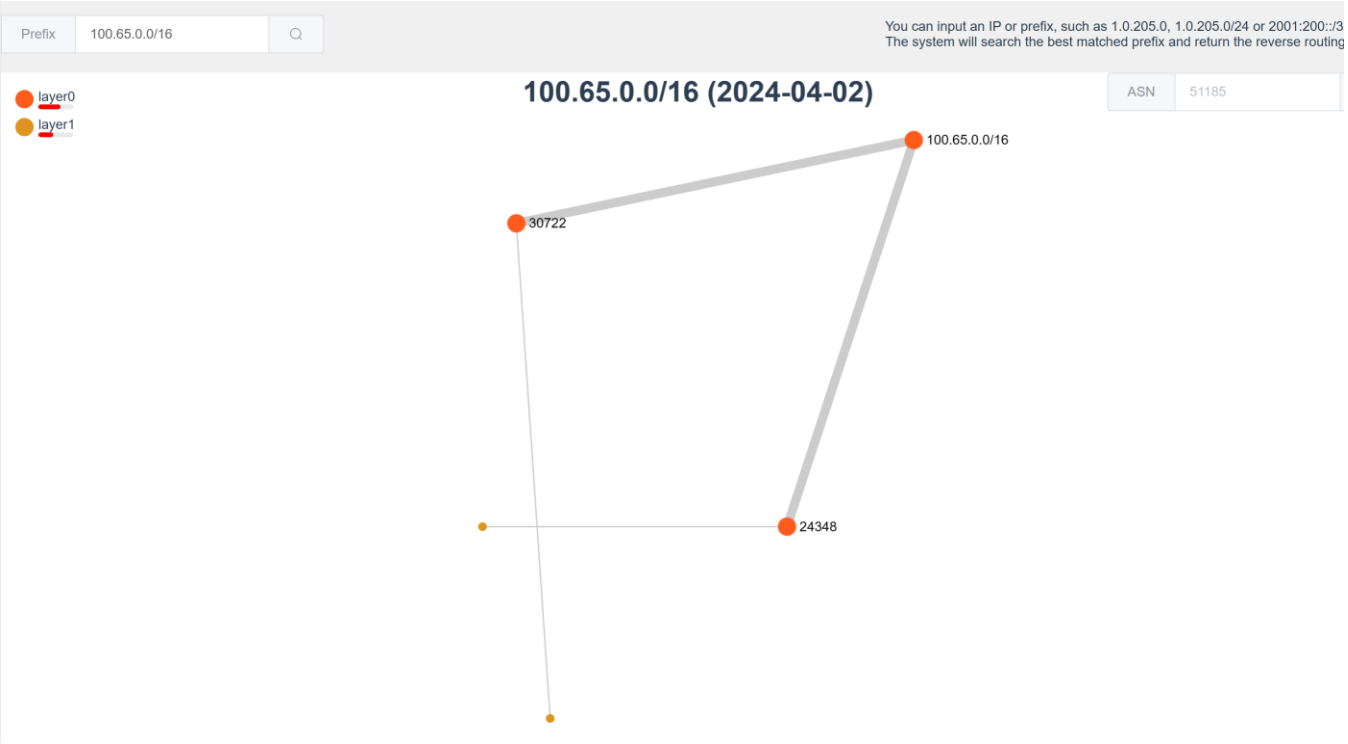
- The advertisement and withdraw messages are received frequently.
- If this will harm internet performance?
- We may conduct some data plane testing in the future.

Bogon IP Address Detection



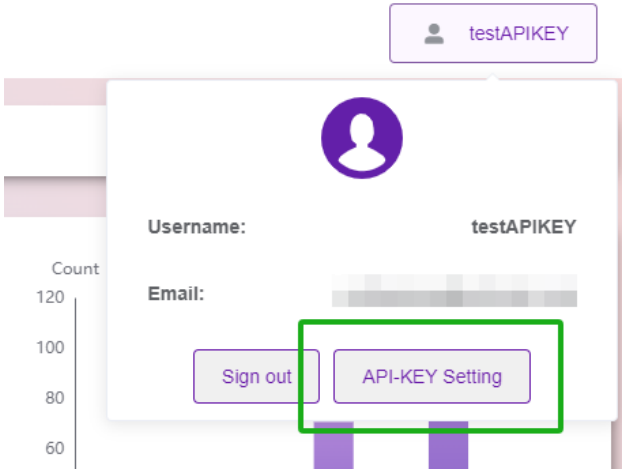
Support searching by continent, economy, AS

Propagation of the Bogon IP Address



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": {}
}
```

CGTF RIS

We have established BGP session with 16 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	16	RedCLARA

https://bgp.cgtf.net

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	

CGTF RIS Collector

- Just have your border router **establish an eBGP session with one of our collectors:**
- Our Collector ASN: 65534

- Our Collector1 IPv4 address: 47.241.43.108
- Our Collector1 IPv6 address: 240b:4000:b:db00:8106:7413:738f:e9ed

- Our Collector2 IPv4 address: 203.91.121.227
- Our Collector2 IPv6 address: 2001:da8:217:1213::227

CGTF Looking Glass

- Open Source:
  - https://github.com/gmazoyer/looking-glass
- 5 commands
- Query speed limit for security
- More partners is welcomed

https://lg.cgtf.net

- 7 Education & Research network joined
- Links to Integrated Looking Glass Platform

Configuration on Router Side

- Create a router account **only for LG**, and this account **only has privileges of executing the above command**.
- Use **IP filtering mechanism**. Add the **web server IP** to the **whitelist**.

- Juniper JUNOS:
  Define the login class with permissions:
  set system login class lookinglass permissions network
  set system login class lookinglass permissions routing
  set system login class lookinglass permissions view

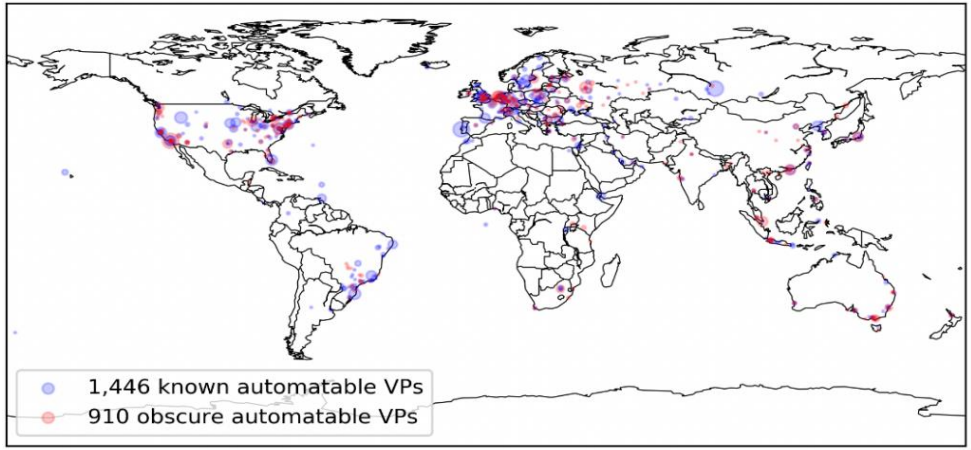
  Define the login user:
  set system login user lookinglass class lookinglass
  set system login user lookinglass authentication encrypted-password "encrypted-text"
  set system login user lookinglass authentication ssh-rsa "ssh-rsa rsa-pub-key-text"

BIRD
Cisco
Cisco IOS XR
FRRouting
Juniper
Quagga
Vyatta, VyOS, EdgeOS

https://www.bgper.net/index.php/document/
https://looking-glass.readthedocs.io/en/latest/

Open Looking Glass Vantage Point

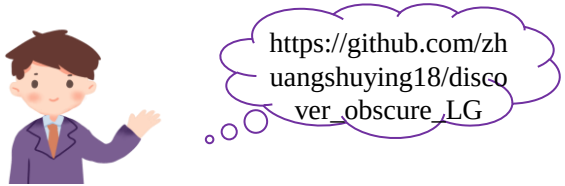
- **Paper: "Discovering obscure looking glass sites on the web to facilitate internet measurement research"——CoNEXT'21**



1,446 known LG VPs in 386 cities of 75 countries

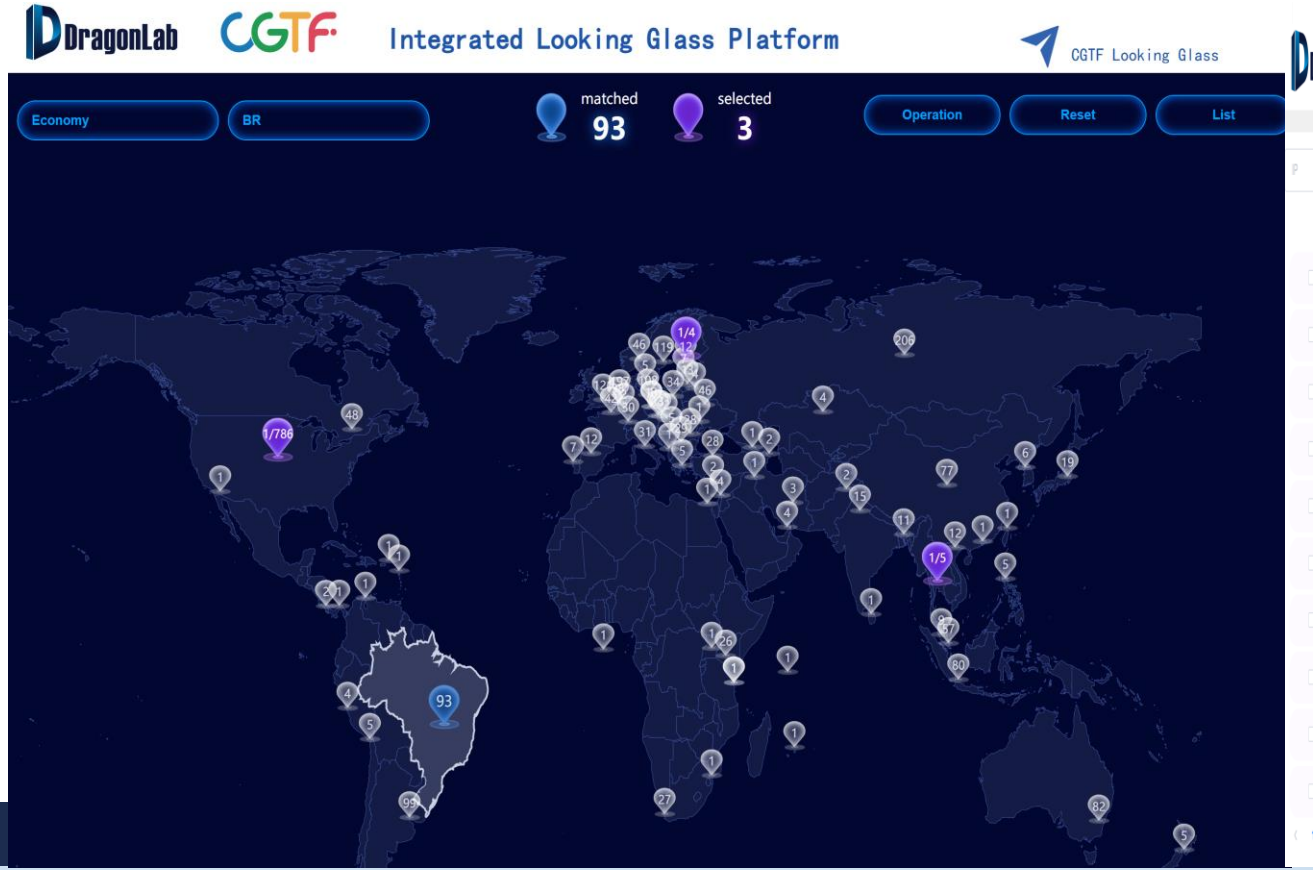
910 obscure LG VPs in 282 cities in 55 countries

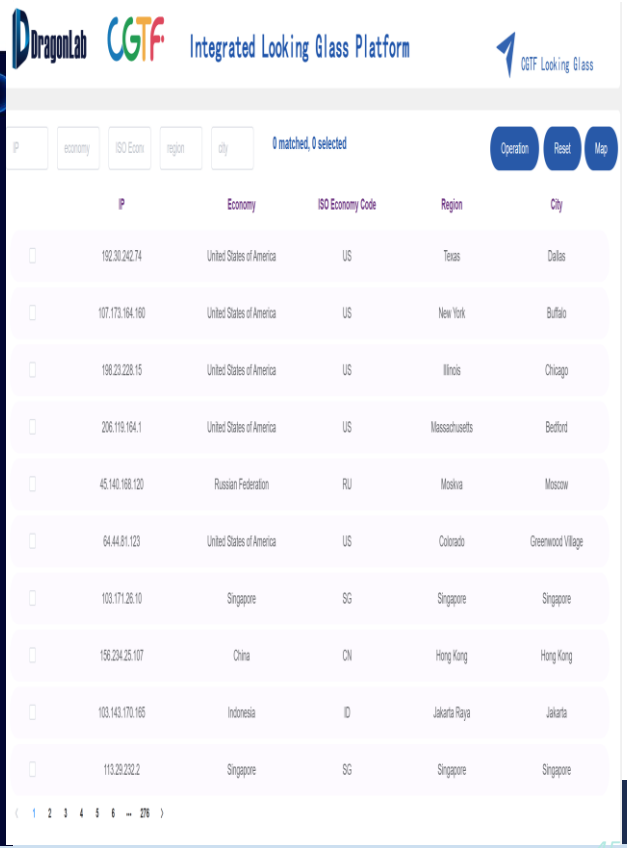
- ✓ The 910 obscure VPs cover **8 exclusive countries** and **160 exclusive cities,** where no known LG VPs have been found before
- ✓ The 8 countries are mainly distributed in **East Africa** and **South Asia**



Periscope has found several hundred VPs (364)

An Integrated Looking Glass Platform





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

Security Concerns

- Where are the data stored?
  - BGP sharing platform: Cloud server in Singapore
  - BGPWatch: Cloud server in Hongkong
  - Looking Glass: Cloud server in Hongkong
- Will peering harm my network?
  - We use routing FRR[2] to simulate a real BGP router and it won't send routing anouncement.
- Will sharing routing information harm my network?
  - No, it's common and useful. Routeviews and RIPE RIS are two most famous RIS sharing platform.
- Our security policy doesn't permit ssh/telnet access from other network
  - Such as SingAREN, they use a VM to simulate a router, and peer with their real router. Then our looking glass access to the VM.

Future Work Plan

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 Ongoing
	Integrate the algorithm to the system	Aug. 2024 Ongoing
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 (**Dec.06, 2023 – June 06, 2025 (18 months))** **Welcome new partners to join!**	Throughout the entire project duration

Thank you

Any questions?

Contact us at: sec@cgtf.net

Co-funded by the European Union

GÉANT