

The Report of the Technical Committee - APNIC ISIF Project

24 August, 2023



Collaborative Community

• Work of 19 Team members (listed alphabetically)

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

Outline

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



Background

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**

Registration Data

PeeringDB Search here for a network, IX, or facility. Register Login

Advanced Search v2 Search (Beta) English (English)

CERNET-CN

Organization: China Education and Research Network
 Also Known As: CERNET
 Long Name:
 Company Website: <http://www.edu.cn>
 ASN: 4538
 IRR as-set/route-set:
 Route Server URL:
 Looking Glass URL:
 Network Type: Educational/Research
 IPv4 Prefixes: 0
 IPv6 Prefixes: 0
 Traffic Levels: Not Disclosed
 Traffic Ratios: Not Disclosed
 Geographic Scope: Not Disclosed
 Protocols Supported: Unicast IPv4 Multicast IPv6 Never via route servers
 Last Updated: 2023-03-29T13:55:32Z
 Public Peering Info Updated:
 Peering Facility Info Updated:
 Contact Info Updated:
 Notes:
 RIR Status: ok
 RIR Status Updated: 2022-07-27T05:29:57

Public Peering Exchange Points

Exchange ID	ASN	Speed	RIS Peer
IPv4	IPv6		

No filter matches. You may filter by Exchange, ASN or Speed.

Interconnection Facilities

Facility ID	Country
ASN <td>City</td>	City

No filter matches. You may filter by Facility, ASN, Country or City.

RADb THE INTERNET ROUTING REALITY SUPPORT QUERY PRICING CONTACT SIGN IN REGISTER

RADB QUERY Query Help

AS33083 Advanced Options QUERY

```

aut-num: AS33083
as-name: AXCELX-NET
admin-c: DUMY-RIPE
tech-c: DUMY-RIPE
descr: AxcelX Technologies LLC
status: OTHER
mnt-by: MAINT-TOWARDEX
created: 2017-02-19T16:11:01Z
last-modified: 2018-09-04T15:30:39Z
source: RIPE-NONAUTH
remarks: *****
remarks: * THIS OBJECT IS MODIFIED
    
```

HURRICANE ELECTRIC INTERNET SERVICES Search

AS7575 Australian Academic and Research Network (AARNet)

Quick Links: BGP Toolkit Home, BGP Prefix Report, BGP Peer Report, Exchange Report, BGP Routes, World Report, Multi Origin Routes, DNS Report, Top Host Report, Internet Statistics, Looking Glass, Network Tools App, Free IPv6 Tunnel, IPv6 Certification, IPv6 Progress, Going Native, Contact Us

AS info | Graph v4 | Graph v6 | Prefixes v4 | Prefixes v6 | Peers v4 | Peers v6 | Whois | IRR | IX

AS7575 IPv4 Route Propagation

The graph shows route propagation from AS7575 to various other ASes. Key nodes include AS17559, AS18858, AS6762, AS6939, AS3356, AS2914, AS701, AS1239, AS1273, AS3257, AS7018, AS12956, AS2764, AS63956, AS3491, AS3320, AS7545, AS3491, AS3320, AS1273, AS3257, AS7018, AS12956, AS174, AS1299, AS6453, AS511.



Data status

This page shows the last update times for all IRR explorer data sources.

- Prefix to RIR mapping from RIRstats
- Prefix to DFZ mapping from bgp.tools
- IRRs mirrored over NRTMv3 with [IRRd v4](http://IRRd.v4)
- RPKI data imported through [IRRd v4](http://IRRd.v4)

Important notes:

- The RIRstats update time refers to the last time IRR explorer imported the current files - not the original publication time of the files.
- For IRR sources, the last update time is when IRRD last *processed* an update for this source, not when it last *tried*. For sources that rarely change, it is normal for the last update to be long ago. This is due to limitations in NRTMv3.



Looking Glass VPs

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

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

... traceroute.org ...

Maintained by [Thomas Kernen](#)

Please feel free to send me updates, links, corrections, extra info
Note that I'm unable to provide support for the linked web pages

Looking Glass

- [GARR \(AS137\)](#)
- [CenturyLink \(AS209\)](#)

Traceroute.org

PeeringDB 在此搜索网络、IX或设置。 高级搜索

UCOM AS8932

组织	UCOM LLC
别名	UCOM CJSC
长名称	
公司网站	http://www.ucom.am
ASN	8932
IRR as-set/route-set 对象	AS8932:AS-ALL
路由服务器 URL	
Looking Glass URL	http://lg.as8932.net

PeeringDB

CATEGORY 1 - IPv4 AND IPv6 BGP LOOKING GLASS SERVERS BY REGION

Please send LG additions and updates to webmaster@bgp4.as. Including NOC whitelist requests

ASN Whois Query Legend (RIRs) | A=ARIN | R=RIPE NCC | P=APNIC | L=LACNIC | F=AFRINIC

CC	Region	BGP Looking Glass website
GLOB	Global	BT Global Services Looking Glass
GLOB	Global	Cogent Communications Looking Glass
GLOB	Global	Deutsche Telekom Looking Glass
GLOB	Global	Easynet Global Services Looking Glass
GLOB	Global	GBLX Global Crossing (Level3) Looking Glass
GLOB	Global	GTT / Tinet Looking Glass
GLOB	Global	Hurricane Electric Looking Glass
GLOB	Global	Inteliquent / Tinet Looking Glass
GLOB	Global	Level3 Looking Glass
GLOB	Global	NTT Communications (NTT America) Looking Glass

BGP4.as

BGP Looking Glass Database

Looking Glass Database

Name of ISP	ASN	Looking Glass
Looking Glass		
University of California, Berkeley AS25	25	https://netbooks.net/lookingglass/public/
Looking Glass Packet Clearing House AS42	42	https://www.pch.net/lookingglass
Looking Glass	59	https://www.net.wisc.edu/cgi-bin/public/ig-ws9.pl
University of Wisconsin-Madison AS59	59	
Looking Glass	73	https://netman.cac.washington.edu/lookingglass/
University of Washington AS73	73	
Looking Glass	98	
Precision University AS98	98	https://www.net.precision.edu/Traceroute.html

BGPLookingglass.com

[Looking Glass - Looking Glass - w9.gubo.org](https://w9.gubo.org/LookingGlass/en.php)

w9.gubo.org/LookingGlass/en.php

LookingGlass - Open source PHP looking glass. Test IPv4: 23.95.242.173. Test files: 10MB

[103.253.27.204 - Cheapwindowsvps_LG - Looking Glass](https://103.253.27.204)

103.253.27.204

Server Location: Singapore Test IPv4: 103.253.27.204. Test files: 25MB 50MB 100MB 1000MB Your IP Address: 40.77.167.52

<https://lg-os1.sa.net>

[Riven Cloud - Looking Glass](https://lg-os1.sa.net)

Server Location: Osaka, Japan. IPv4 Address: 103.88.47.47. IPv6 Address: 2400:ddc0:1000::35ed:d9ba. Your IP Address: 66.249.69.151. Network Test Files ...

Routing Collection VPs



RIPE RIS VPs (in the upper tier)



RouteViews VPs (in the upper tier)



About Services Tools Resources

Resources Routing Data

Daily Routing Snapshots

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

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

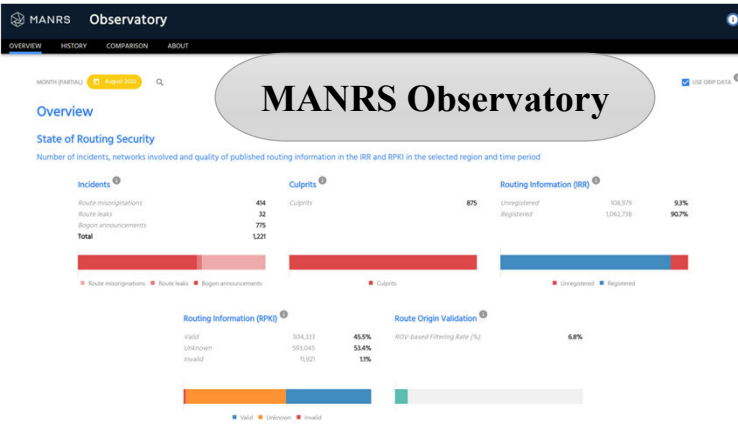
Note that the data collected by PCH represents the sum of inter-domain routing announcements received from PCH peers. This data does not, and cannot, reflect the status of every autonomous system at an IXP.

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

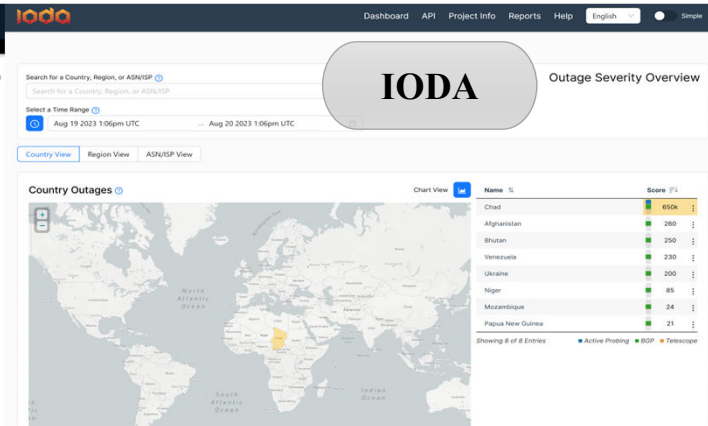
```
nyix.woodynet.pch.net → route-collector.lga.pch.net
npix.woodynet.pch.net → route-collector.ktm.pch.net
nota.woodynet.pch.net → route-collector.mia.pch.net
netnod.woodynet.pch.net → route-collector.arn.pch.net
linx.woodynet.pch.net → route-collector.lhr.pch.net
laiix.woodynet.pch.net → route-collector.sna.pch.net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



Application Platforms



MANRS Observatory



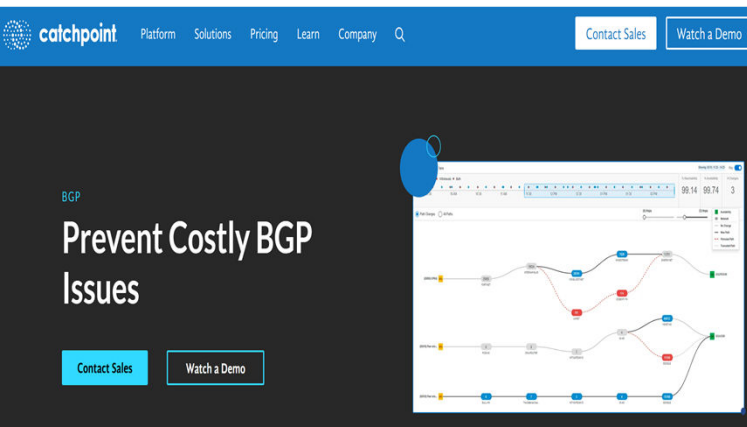
IODA

Outage Severity Overview

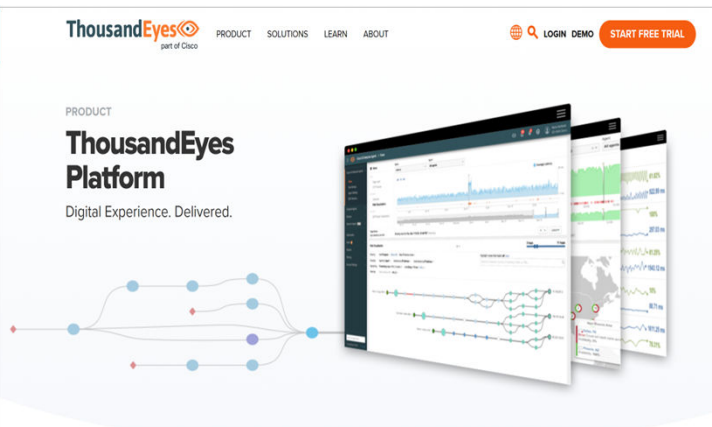
All Events for BGP Stream.

Event type	Country	ASN	Start time (UTC)	End time (UTC)	More info
Outage	HT	N/A	2023-08-21 11:24:00		More detail
Outage	HT	N/A	2023-08-21 11:03:00	2023-08-21 11:15:00	More detail
Outage	HT	N/A	2023-08-21 10:47:00	2023-08-21 10:52:00	More detail
Outage	HT	N/A	2023-08-21 10:31:00	2023-08-21 10:35:00	More detail
Outage	HT	N/A	2023-08-21 10:04:00	2023-08-21 10:20:00	More detail
Outage	HT	N/A	2023-08-21 09:37:00		More detail
Possible Hijack		Expected Origin AS: KISTNET-AS:KR Korea Institute of Science and Technology, KR (AS 17866) Detected Origin AS: CMNET-GUANGDONG-AP China Mobile communications corporation, CN (AS 56040)	2023-08-21 05:53:11		More detail
Outage		IPXO, US (AS 834)	2023-08-21 05:22:00	2023-08-21 05:37:00	More detail
Outage	SY	N/A	2023-08-21 02:00:00		More detail
Outage	SY	N/A	2023-08-21 01:59:00		More detail

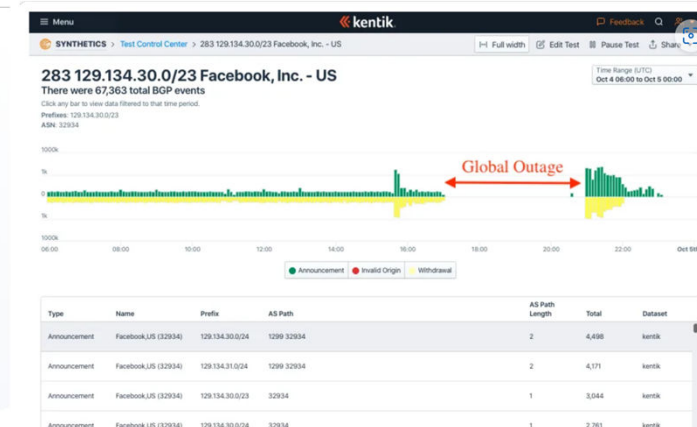
CISCO BGPSTREAM



CATCHPOINT



ThousandEyes

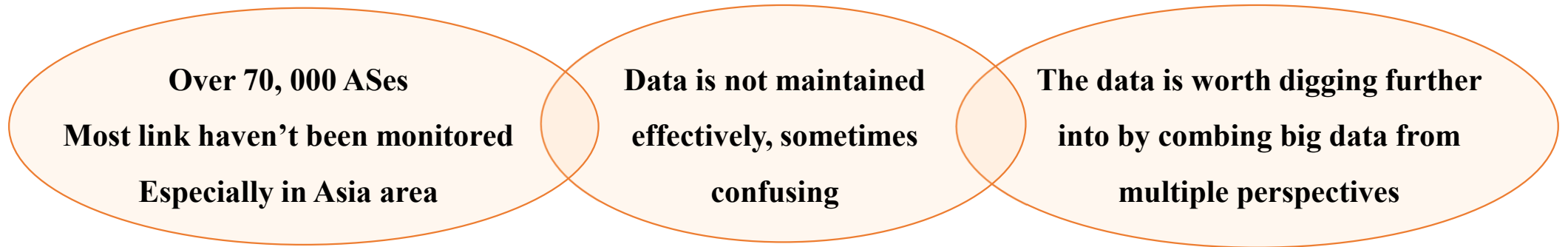


KENTIK



Is it enough?

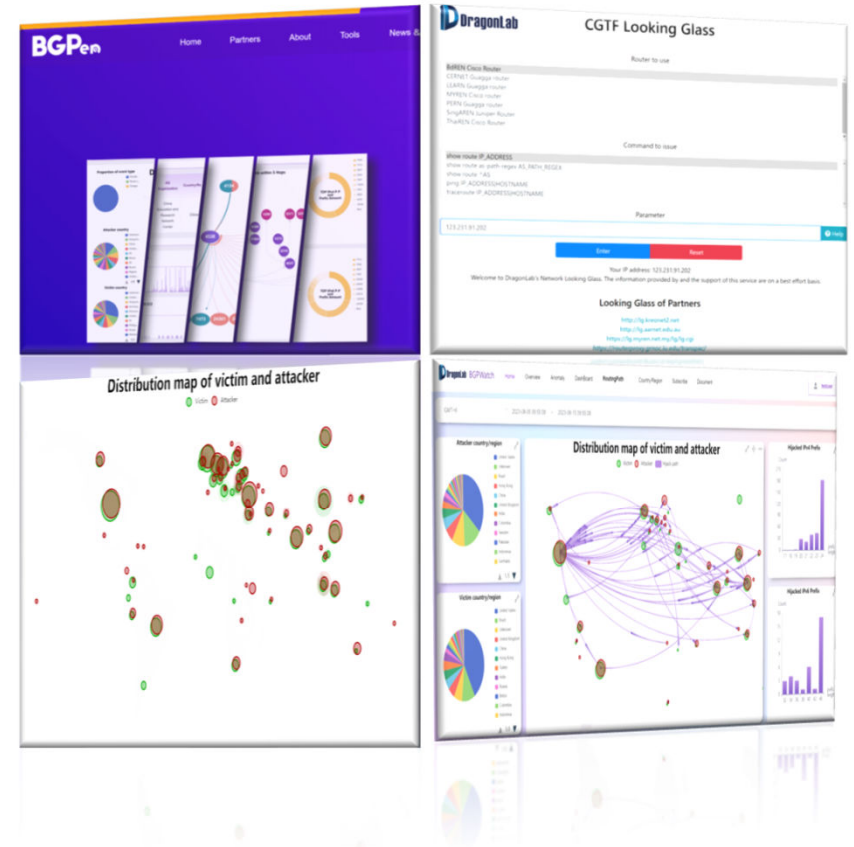
What's the meaning of the project



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

Objectives

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



Activities

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

Project Web Site

<https://bgper.net>

BGPWatch

BGPWatch is a global BGP monitor system that provides free service monitoring BGP hijacking events, conducting AS-specific route statistics and analysis, and helping operators effectively monitor their ASes.

Documents

- Meeting Materials
- Other Presentations
- Technical Documents

Meeting Materials	Date
[APNIC Project] 5th Technical Committee Report	2023-01-19
[APNIC Project] Third Coordination Committee Report	2023-01-19
[APNIC Project] Second Coordination Committee Report	2022-09-29
[APNIC Project] Fourth Technical Committee Report	2022-09-29
[APNIC Project] Third Technical Committee Report	2022-08-03
[APNIC Project] Second Technical Committee Report	2022-06-20
[APNIC Project] First Coordination Committee Report	2022-05-10
[APNIC Project] First Technical Committee Report	2022-05-10

Other Presentations	Date
APNIC ISIF Presentation at APAN53	2022-03-08

Partners

Organization: AARNET

Since 1989, AARNET, Australia's Academic and Research Network has provided high-performing telecommunications and an expanding range of cyber security, data and collaboration services for Australia's research and education sector, including universities, research organisations, schools, vocational training providers and cultural institutions. AARNET serves over two million end users who access AARNET's network and services for teaching, learning and research. For more information, visit [AARNET](#)

News & Event

The First Collaborative and Technical Meeting of "Collaborative BGP Routing Analyzing and Diagnosing Platform" Project

News On May 10, 2022, the First Collaborative and Technical Meeting of the "Collaborative BGP Routing Analyzing and Diagnosing Platform"...

[Read More →](#)

"Collaborative BGP Routing Analyzing and Diagnosing Platform" Project Kick-off Meeting



CGTF RIS

<https://bgp.cgtf.net>

We have established BGP session with **15 partners**.

Configuration manual can be accessed at

<https://www.bgper.net/index.php/document/>

Index of /ribs/2022/07

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		

[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 our collector:
- Our Collector ASN: 65534
- Our Collector1 IPv4 address: 47.241.43.108
- Our Collector1 IPv6 address: 240b:4000:b:db00:8106:7413:738f:e9ed
- Our Collector2 IPv4 address: 203.91.121.227
- Our Collector2 IPv6 address: 2001:da8:217:1213::227

CGTF Looking Glass

<https://lg.cgtf.net>

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

DragonLab CGTF Looking Glass

Router to use

- BdREN Cisco Router
- CERNET Guagga router
- LEARN Guagga router
- MYREN Cisco router
- PERN Guagga router
- SingAREN Juniper Router
- ThaiREN Cisco Router

Command to issue

```
show route IP_ADDRESS
show route as-path-regex AS_PATH_REGEX
show route ^AS
ping IP_ADDRESS|HOSTNAME
traceroute IP_ADDRESS|HOSTNAME
```

Parameter

123.231.91.202

Enter Reset

Your IP address: 123.231.91.202

Welcome to DragonLab's Network Looking Glass. The information provided by and the support of

Looking Glass of Partners

- <http://lg.kreonet2.net>
- <http://lg.aarnet.edu.au>
- <https://lg.myren.net.my/lg/lg.cgi>
- <https://routerproxy.grnoc.iu.edu/transpac/>

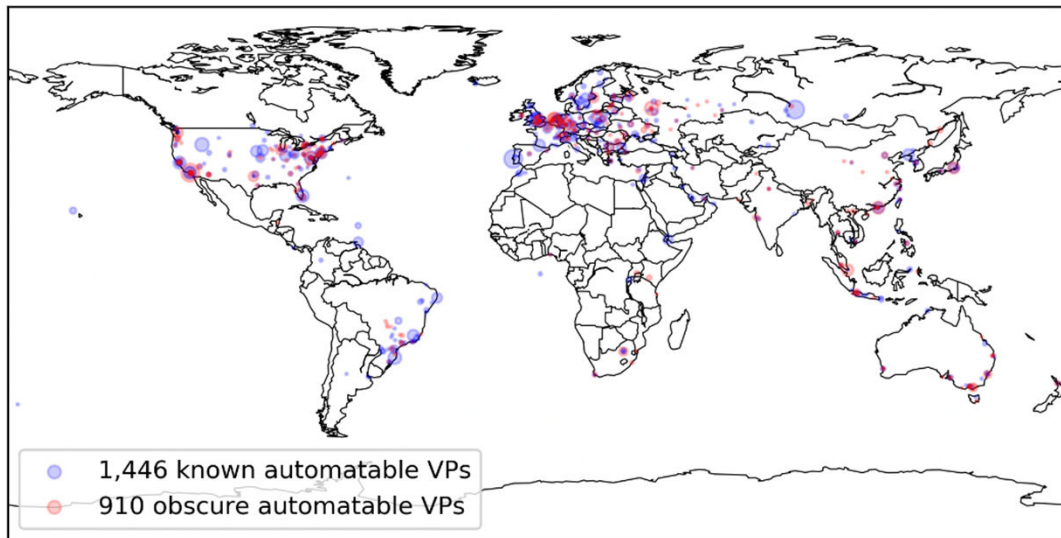
Link to partners' looking glass

7 Education & Research network joined
Add links to 4 partners' looking glass



Open Looking Glass Vantage Point

- Paper: “Discovering obscure looking glass sites on the web to facilitate internet measurement research”——CoNEXT’21



1,446 known LG VPs in 386 cities of 75 countries
910 obscure LG VPs in 282 cities in 55 countries

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



https://github.com/zhuangshuying18/discover_obscure_LG

Periscope has found several hundred VPs (364)

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

Collect AS paths from LG VPs

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

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

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

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

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

Improve AS-level topology completeness

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

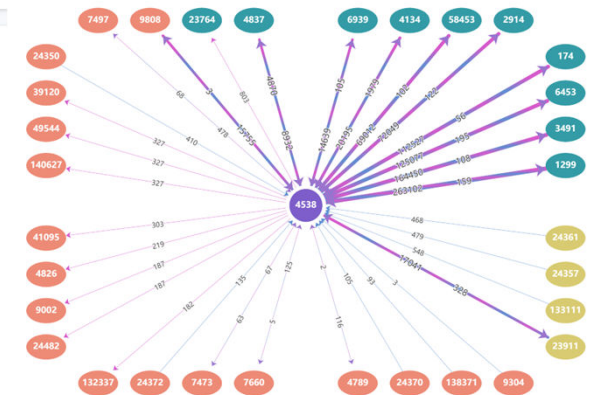
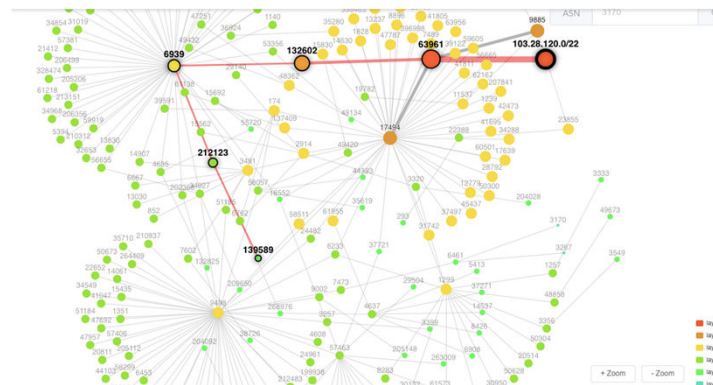
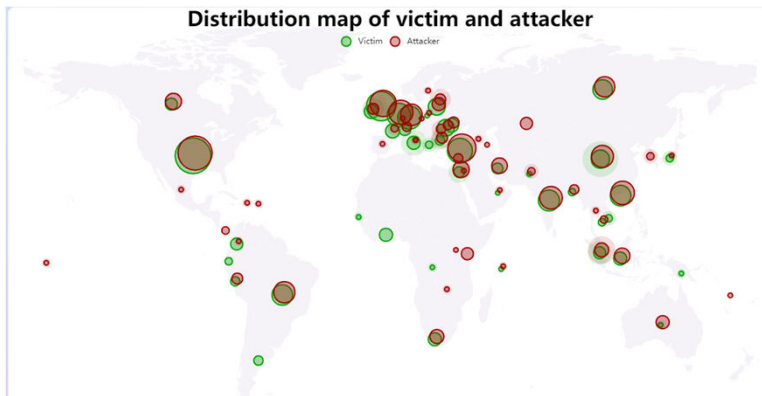
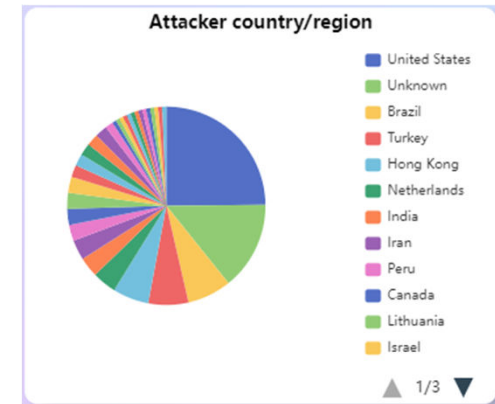
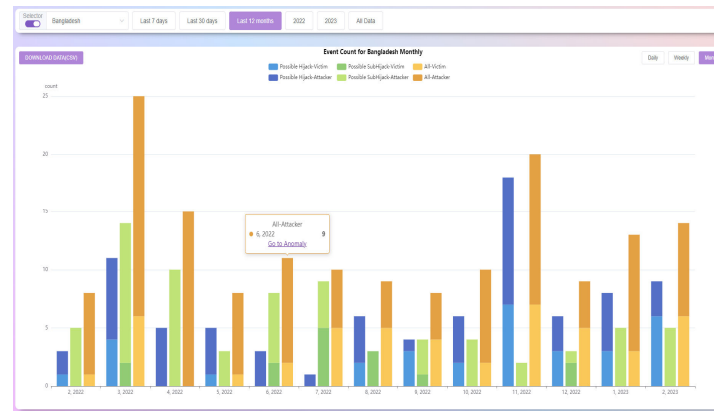
Table 6: The number of observed and exclusive ASes, AS links extracted from each dataset.

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

10 new ASes, and 1428 new links

BGP Routing Monitoring and Analysis: BGPWatch

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



Hijacking Detection

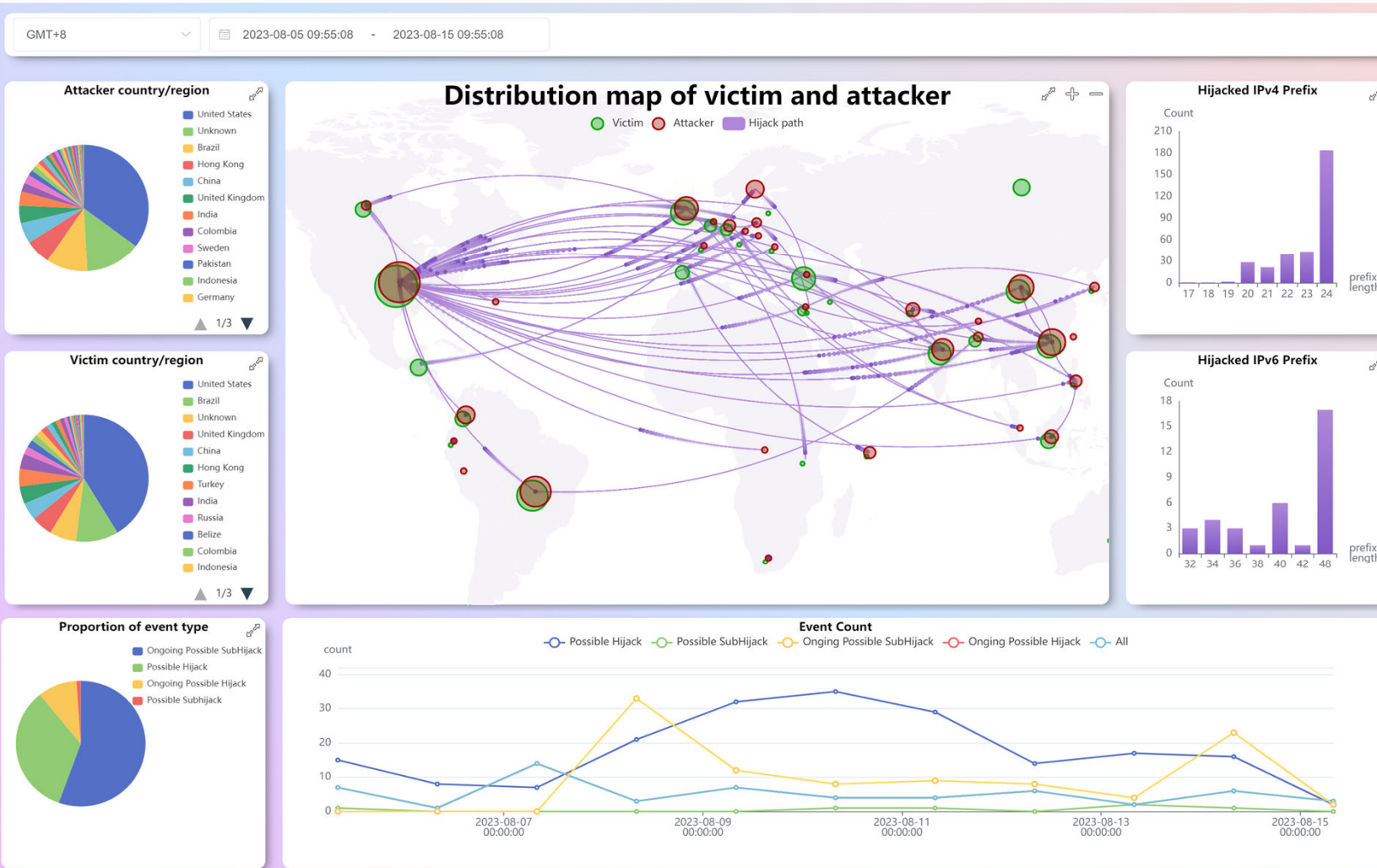
- Knowledge-based real-time BGP hijacking Detection System
- Public BGP event reporting service

- Based on MOAS(subMOAS)
- Rely on Domain Knowledge (ROA, IRR, AS relationship etc)



Event ID	Event Type	Level	Event Info	Prefix Num	Prefix	Start Time	End Time	Duration	Detail
1	Ongoing Possible Hijack	low	Victim:TR/AS204843 (TR-STERLY) Attacker:US/AS397373(H4Y-TECHNOLOGIES)	1	206.206.119.0/24	2023-03-11 11:28:28	-	-	detail
2	Possible SubHijack	low	Victim:VN/AS45903 (CMCTELECOM-AS-VN) Attacker:HK/AS45474(NEXUSGUARD-AS-AP)	1	prefix: 144.48.27.0/24 subprefix: 144.48.27.132/32	2023-03-11 10:34:50	2023-03-11 11:34:55	1:0:5	detail
3	Possible Hijack	low	Victim:AS209260 () Attacker:IN/AS135752(EVOKEDS-AS)	3	84.32.26.0/24	2023-03-11 08:48:40	2023-03-11 08:48:41	0:0:1	detail
4	Ongoing Possible Hijack	low	Victim:PK/AS38616 (WORLDALL-AS-KHI) Attacker:PK/AS141432(Tzees-AS-AP)	1	203.81.219.0/24	2023-03-11 07:53:48	-	-	detail
5	Possible Hijack	low	Victim:US/AS834 (IPXO) Attacker:AS200010()	3	206.206.109.0/24	2023-03-11 07:27:33	2023-03-11 07:50:05	0:22:32	detail
6	Ongoing Possible Hijack	low	Victim:HK/AS38136 (AKARI-NETWORKS-AS-AP) Attacker:AS393427()	1	46.3.243.0/24	2023-03-11 06:38:15	-	-	detail
7	Ongoing Possible Hijack	low	Victim:US/AS22773 (ASN-CXA-ALL-CCI-22773-RDC) Attacker:AS393427()	1	46.3.202.0/24	2023-03-11 06:38:13	-	-	detail

BGP Routing Monitoring and Analysis: BGPWatch



Home Page
Statistic Info



Hijacking Detection

Select event type: **Download** | Select harm level: All | Time zone: GMT+8 | Select time period (by Start Time): 2023-04-13 10:24:41 - 2023-04-23 10:24:41 | Duration: All | Select for event by keywords:

Event ID	Event Type	Level	Event Info	Prefix Num	Prefix Example	Start Time	End Time	Duration	Detail
221	Possible Hijack	low	Victim:IS/AS12969 (Vodafone_Iceland) Attacker:KR/AS9860(NHIS-AS-KR)	Multi Prefix 193.4.4.0/24 193.4.5.0/24	193.4.4.0/24	2023-04-13 13:56:24	2023-04-13 13:58:24	0:2:0	detail
222	Possible Hijack	low	Victim:IS/AS12969 (Vodafone_Iceland) Attacker:KR/AS9860(NHIS-AS-KR)	2	193.4.4.0/24	2023-04-13 13:43:36	2023-04-13 13:49:53	0:6:17	detail
223	Possible Hijack	high	Victim:US/AS398823 (PEGTECHINC-AP-02) Attacker:ZA/AS328608(Africa-on-Cloud-AS)	1	154.93.32.0/19	2023-04-13 11:47:11	2023-04-14 06:47:14	19:0:3	detail
224	Possible SubHijack	low	Victim:US/AS6253 (PRUASN) Attacker:US/AS8030(WORLDDNET5-10)	2	prefix: 161.151.112.0/22 subprefix: 161.151.114.0/24	2023-04-13 10:52:15	2023-04-13 13:58:59	3:6:44	detail

Total 224 | < 1 ... 18 19 20 21 22 23 >

- Support download and show multi prefix
- Sync ROA & RIR data daily

Features --- Event Level Evaluation

- Evaluate event impact based on importance of AS and prefix.

45.58.36.0/23-hijack1692553572 Ongoing Possible Hijack Events

high level

Ongoing Possible Hijack Events

Victim AS: 13768

Victim Country: CA (Canada)

Victim Description: COGECO-PEER1

Normal Prefix: 45.58.36.0/23

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

During Time: no data

Hijacker AS: 6364

Hijacker Country: US (United States)

Hijacker Description: ATLANTIC-NET-1

End Time: -

Time Zone: UTC

Website:

easteuropeanbrides.com

theloop21.com

dnscalifornia.net

bigonsports.com

riversideclinictrail.ca

trackword.net

mqjsolutions.net

swarovski-crystal.co

royaltytheme.com

thetreethockeyshop.com

renewablelogic.com.au

gamefocus.ca

essay-writer.ca

jimcrownhistory.org

formalium.com

sstenligne.com

tobyspeople.com

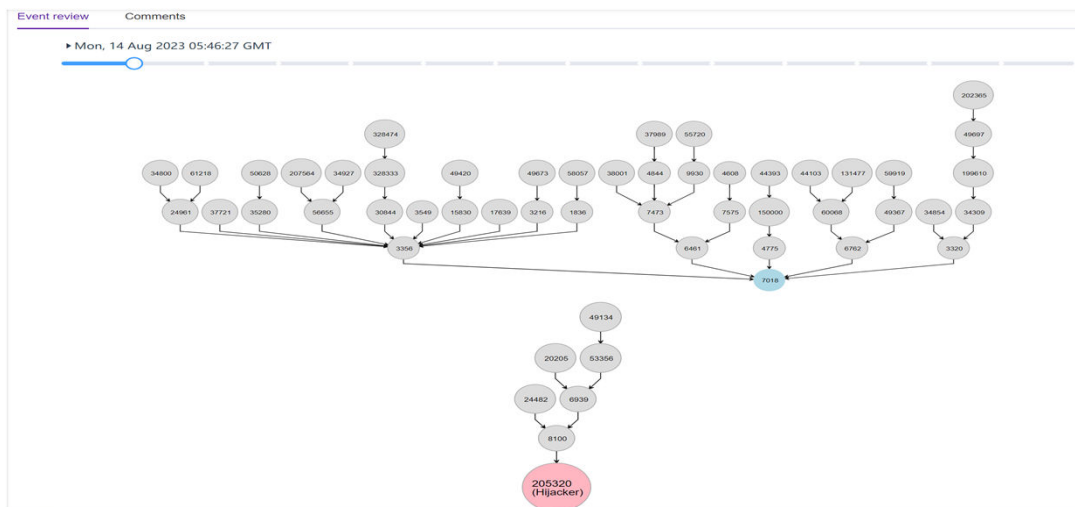
the-northface.com.co

benitezmodernconstruction.com

triofertility.com

Features --- Quick Response, Event replay, Comments

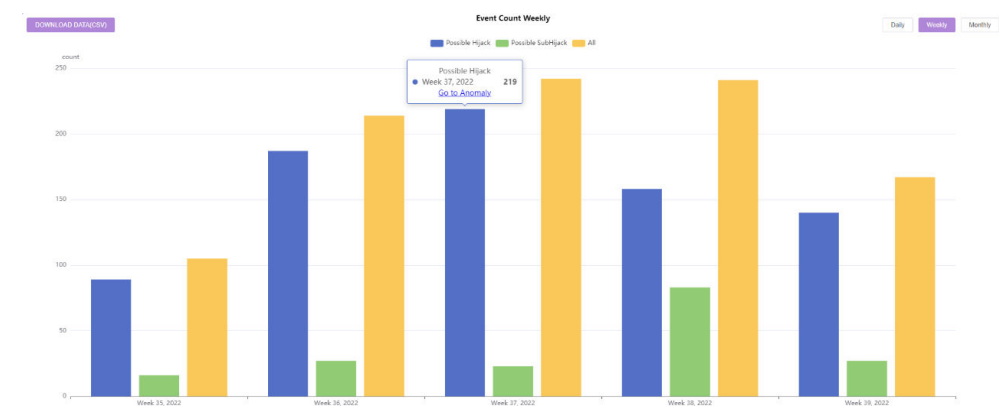
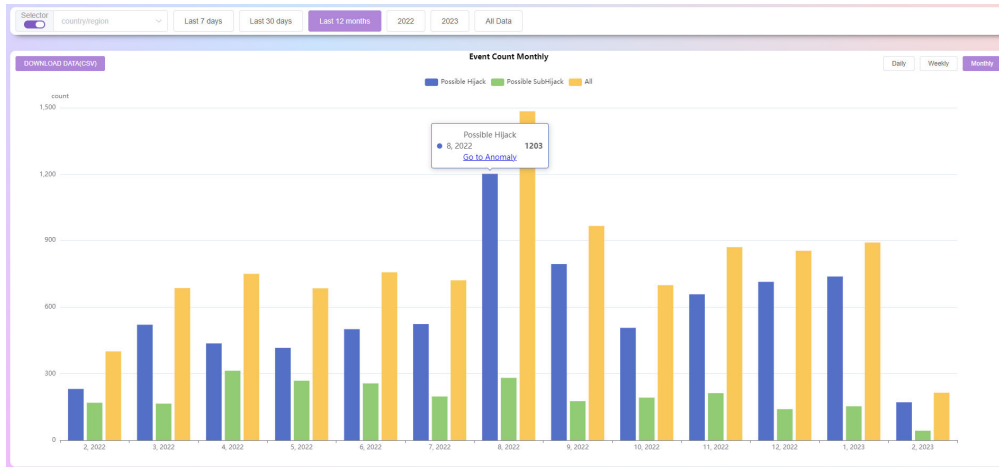
- About 5 mins delay, much better than most systems
- Notify immediately when an event is detected, minimizing damage from hijackings
- Understanding how the BGP routing changes
- Analyze the extent of the impact of the event



The dialog box is titled "Add Comment" and has a close button (X) in the top right corner. It contains the following elements:

- Accept/Reject: Accept Reject
- Description: A text input field containing the text "I'm owner of this AS, I confirm that"
- Buttons: "Cancel" and "OK" buttons at the bottom right.

Overview--Statistics for Anomaly Events



DashBoard

DragonLab BGPWatch Home Overview Anomaly Dashboard RoutingPath Country/Region Document Login Register

4538 Q Last Update: 2023-04-24

Basic IPv4 Peers IPv6 Peers

4538 **China** **ERX-CERNET-BKB** **China Education and Research Network Center**

AS NUM Country/Region AS Name AS Organization

Search by AS number

4538 Q

AS Name 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

asn	Organization	Cone
132551	China Innovate Network Environment (CINE)	1
132552	CERNET-TERNET-AS (CN)	1
132886	CERNET-LCU-AS (CN)	1
135570	CERNET2-SGECN-AS-AP (CN)	1
136446	CERNET2-BUPT-CINE-BGP-AS (CN)	1
138000	CERNET2-BUPT-CINE-INS-AS (CN)	1
138011	CERNET2-BUPT-CINE-SDN-AS (CN)	1
139205	CERNET2-BUPT-CINE-AS (CN)	1
139738	CERNET-GDHED-AS (CN)	1
139774	CERNET-IVION-AS (CN)	1

Search by organization name

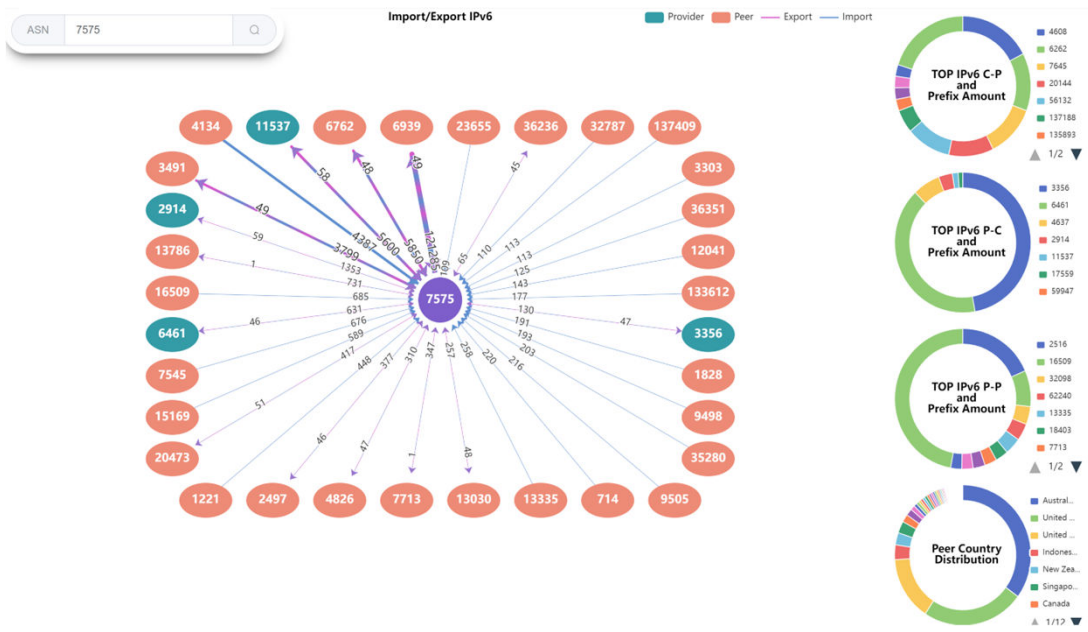
Selected Search for Prefix Q

Prefix	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

All prefixes of the AS



Dashboard: IPv4/IPv6 Key Peers and All neighbors Information



Key Peers

Provider Peer Customer Unknown

Search for ASN, Organization name or country

All IPv6 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

Total 458 < 1 2 3 4 5 6 ... 48 >

All neighbors

Routing Path Search

APAN-JP AARNET BDREN CERNET HARNET ITB KREONET LEARN MYREN NREN PERN REANNZ SINGAREN ThaiREN TransPAC

IP 2001:200::/32

You can input an IP address or prefix address. For example: 1.0.0.0/16, 2001:200::/32. The system will return all the subset and superset network of it.

2001:200:900::/40
2001:200:e000::/35
2001:200::/32
2001:200:c000::/35
2001:200:e00::/40

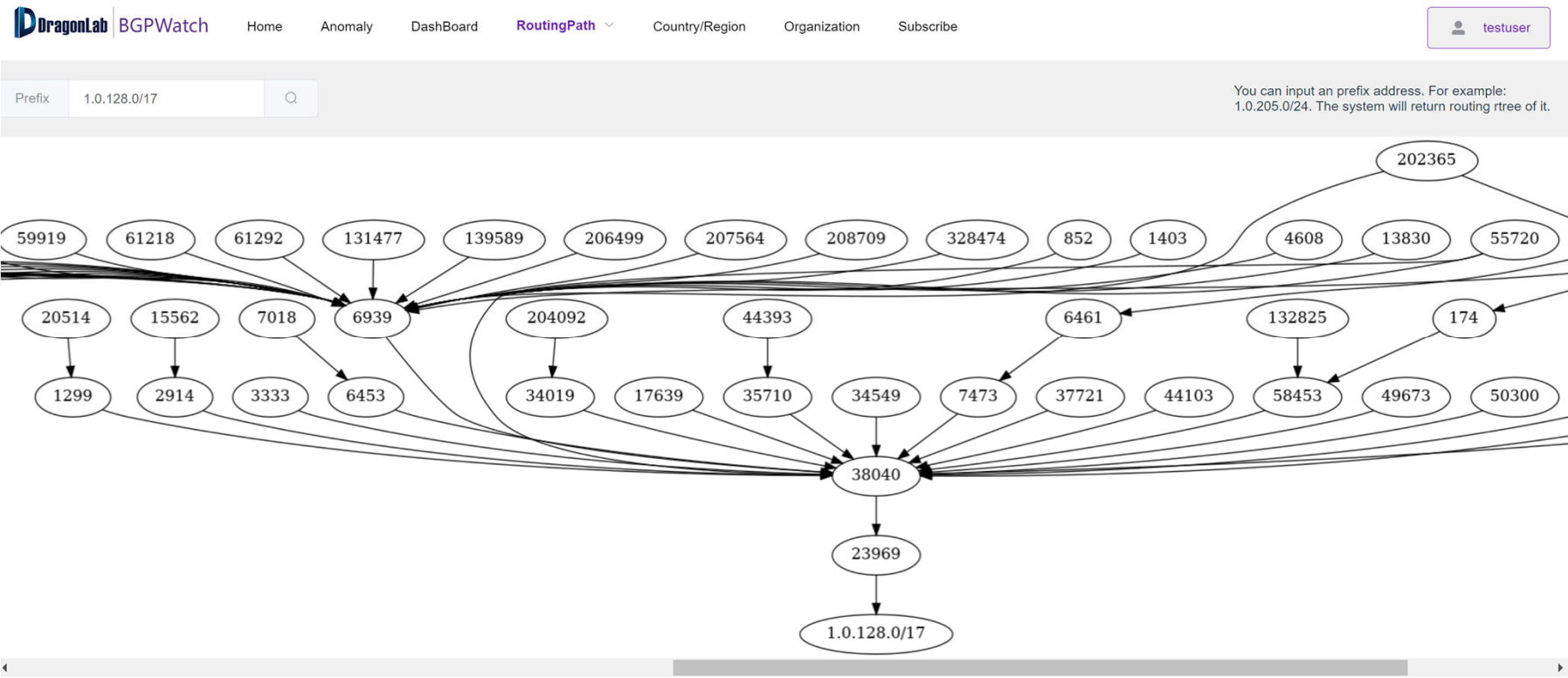
2001:200:e00::/40 AS PATH 1090415 Prefix Total

```
graph LR; 38022 --> 9607; 38022 --> 3356; 38022 --> 6939; 38022 --> 2907; 38022 --> 2914; 3356 --> 9607; 3356 --> 7500; 3356 --> 7660; 3356 --> 2914; 6939 --> 7500; 6939 --> 7660; 6939 --> 7530; 2907 --> 7660; 2907 --> 7530; 9607 --> 23634; 9607 --> 2500; 9607 --> 7530; 7500 --> 23634; 7500 --> 2500; 7500 --> 7530; 7660 --> 2500; 7660 --> 7530; 23634 --> 4690; 2500 --> 4690; 7530 --> 4690;
```

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.



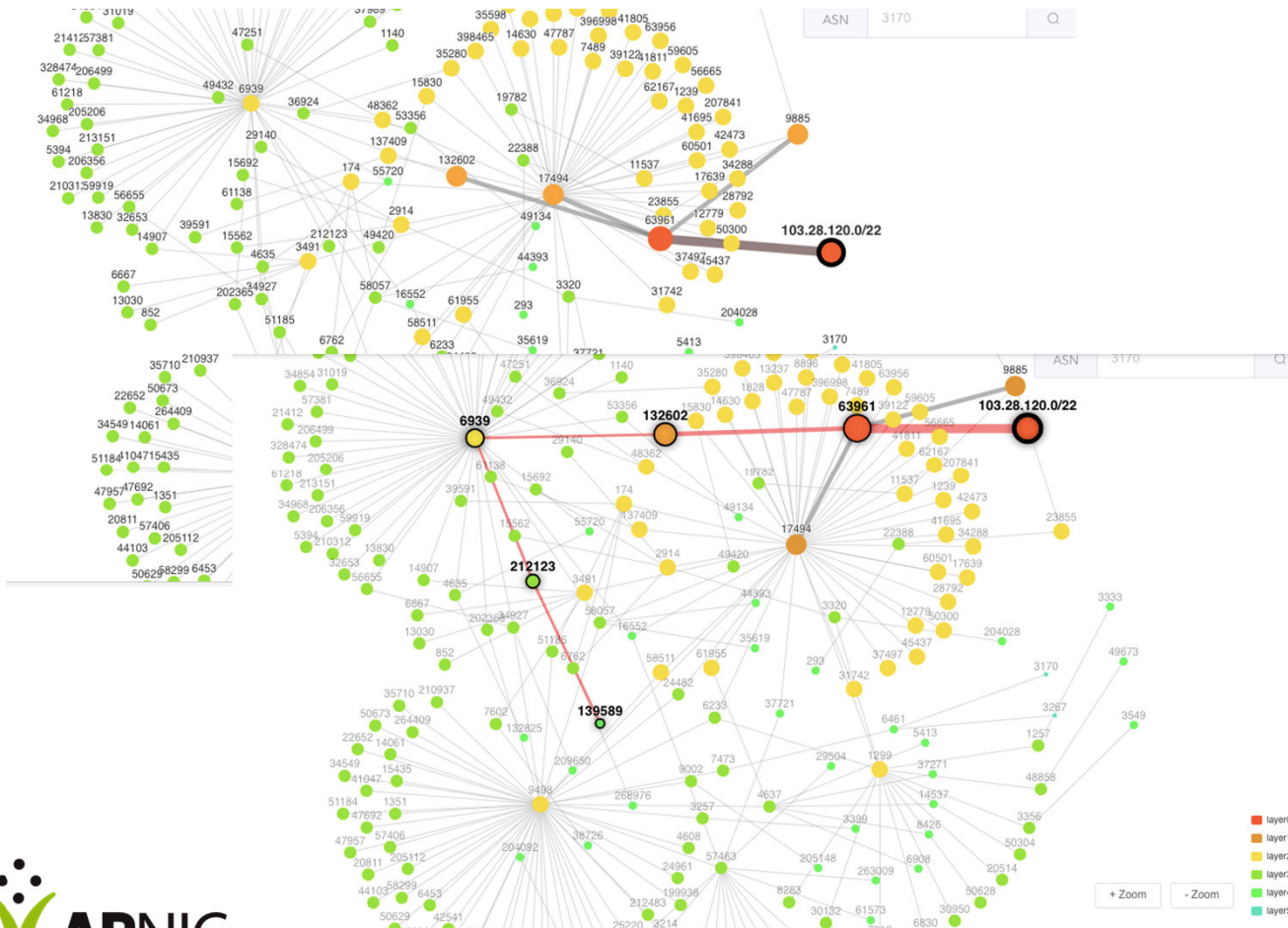
Reverse Routing Path



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

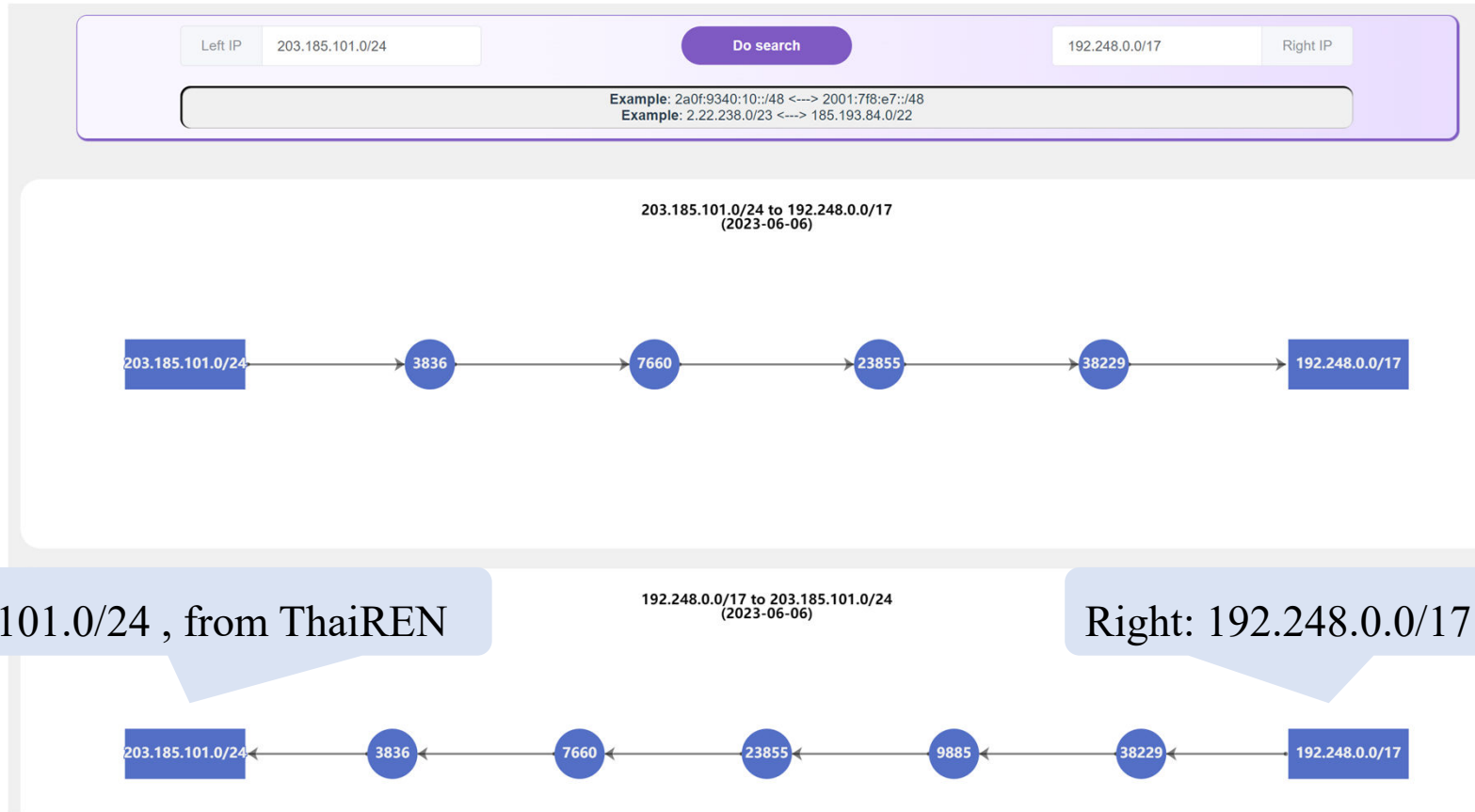


Reverse Routing Path (TOPO)



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

Bi-Routing Path



Support Prefix /IP, IPv4 / IPv6.
The system will search the best matched prefix.

Subscribe and Send Alarm Email when Prefix Change

ASN
4538

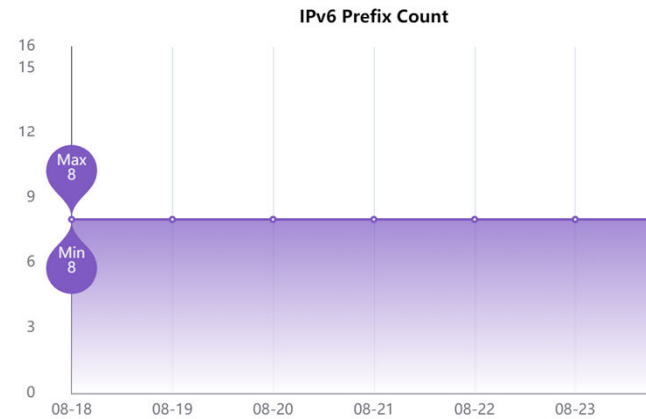
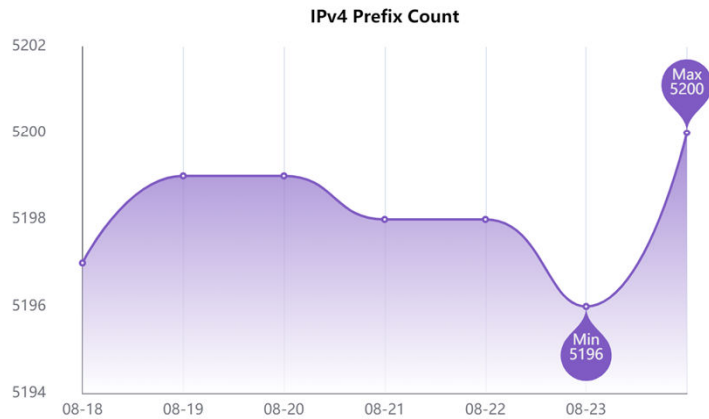
Country/Region
CN

Name
ERX-CERNET-BKB

Organization
China Education and Research Network Center

Prefixes Changed
+ 4 - 0

Prefix Change



+59.64.64.0/20
+121.194.32.0/20
+211.68.32.0/20
+211.82.96.0/20

Announced prefixes changes between 2022-08-24 00:00:00 (GMT) and 2022-08-23 00:00:00 (GMT)

ASN 7575 #
+ 203.6.255.0/24

ASN 4538 #
+ 59.64.64.0/20
+ 121.194.32.0/20
+ 211.68.32.0/20
+ 211.82.96.0/20

subscribe ASN [4538,4630]

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



Path Change

subscribe prefix 174

Prefix 5.150.158.0/24

Prefix Change Hijack AS Peer Change AS Path Change

174 166.111.0.0/16 166.111.1.1/32

Date:2023-08-15



Date:2023-08-16



Date:2023-08-17



Date:2023-08-18



Subscribe Hijacking Events for AS and Send Alarm

Event Type	Level	Event Info	Prefix Num	Prefix Example	Start Time	End Time	Duration	Detail	Comment	
1	Ongoing Possible Hijack	low	Victim:US/AS174(COGEN-174) Attacker:US/AS6488(DS6488-0)	1	204.62.193.0/24	2023-08-13 23:36:31	-	-	detail	<input checked="" type="checkbox"/> <input type="checkbox"/>
2	Ongoing Possible Hijack	low	Victim:US/AS174(COGEN-174) Attacker:BT/AS141680(SUPERNET1-AS-AP)	1	38.7.145.0/24	2023-08-13 19:44:14	-	-	detail	<input checked="" type="checkbox"/> <input type="checkbox"/>

sec 代表 CGTF SEC

发给 acq

2023-08-09 20:04 [隐藏信息](#)

发件人: sec<sec@cgtf.net> 代表 CGTF SEC<CGTF SEC>

收件人: acq<acq@tsinghua.edu.cn>

时间: 2023年8月9日 (周三) 20:04

大小: 4 KB

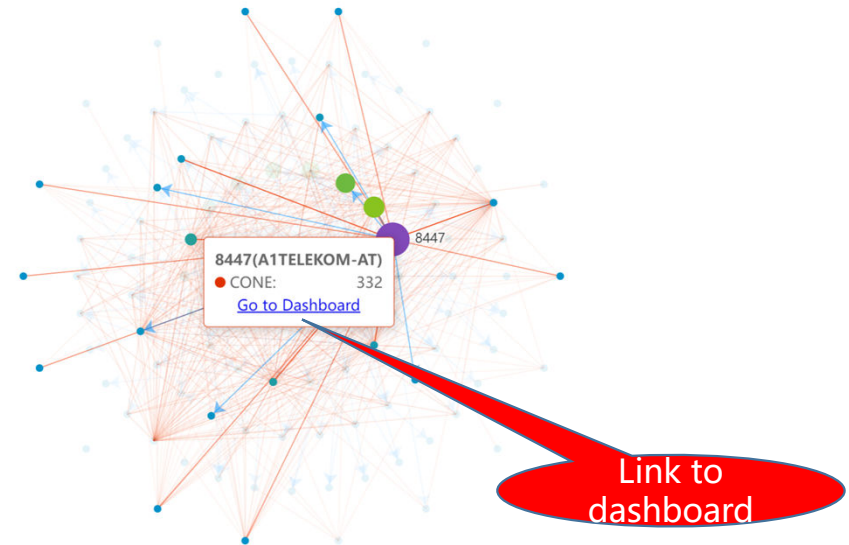
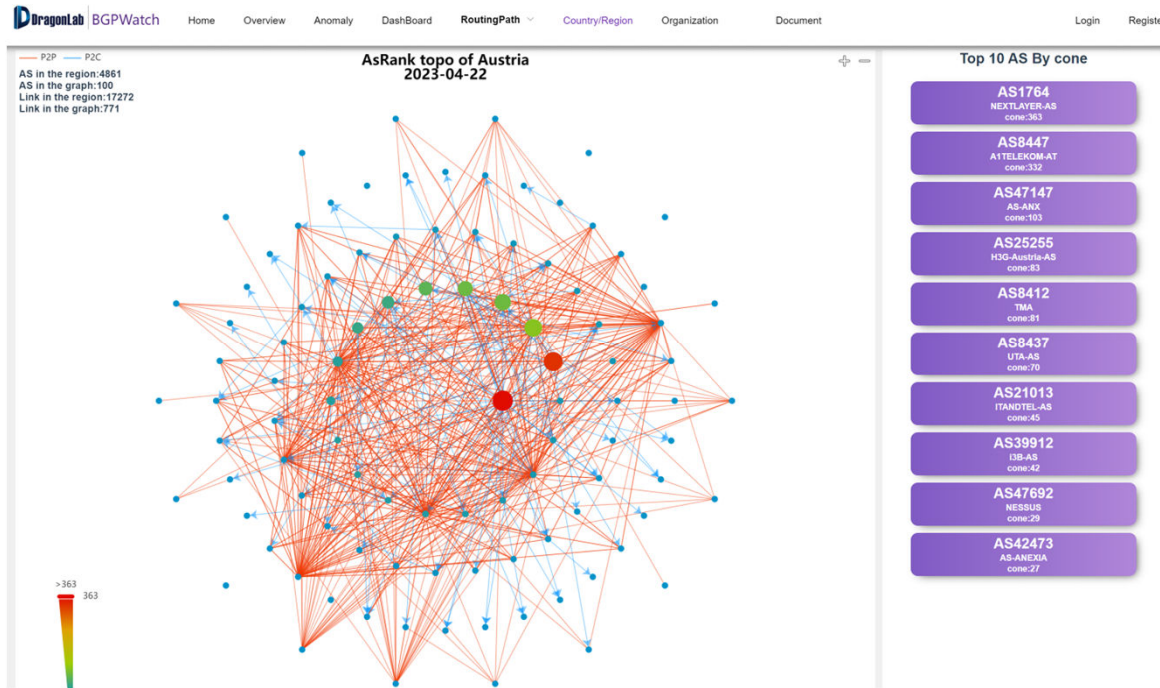
Hi, we are from Institute of Network Sciences and Cyberspace, Tsinghua University and we have developed a BGP hijacking detection system (BGPwatch, <https://bgpwatch.cgtf.net>).

Our system shows that prefix 38.75.36.0/22 is normally announced by your 174, however, at 2023-08-09 11:55:35, prefix 38.75.36.0/22 is also announced by 399527. Detailed information is available [here](#).

We would like to know if this is a hijacking event or a false alarm of the system. Please click [here](#) give us feedback. It would be very helpful for our research! Thanks.



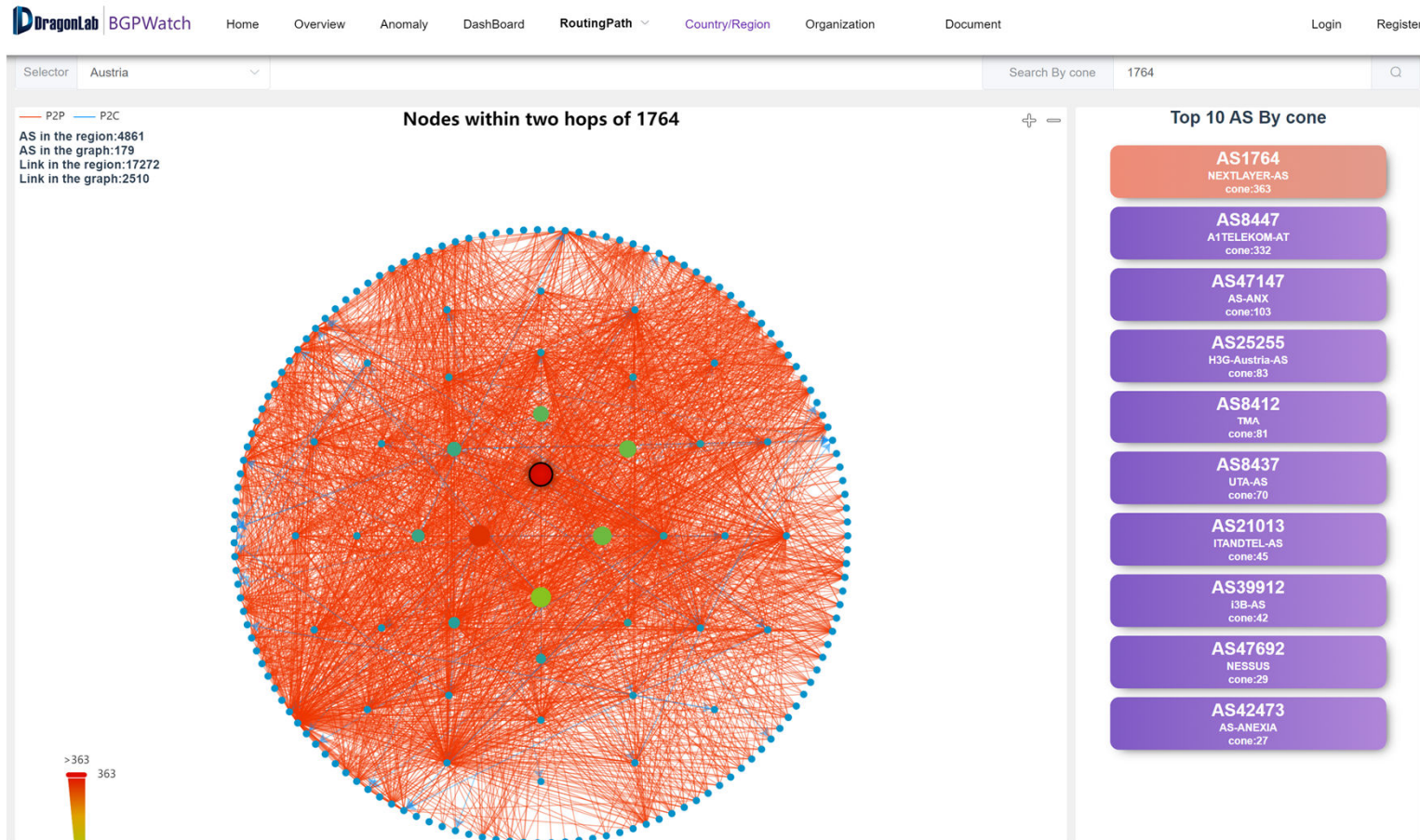
Topo of Country/Region



Show Topology and TOP 10 ASes

Show connection of a node,
and can go to Dashboard

Topo of Country/Region



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

Manual and Video

- [User Manual for BGPWatch](#)
- [User Manual for BGPWatch\(Video\)](#)
 - Joint efforts of BdREN and Tsinghua University
- [CGTF BGP RIS Platform Manual](#)
- [CGTF Looking Glass Platform Manual](#)
- [Analysis of Suspected Hijacking Events in 2022](#)



Feedback from Partners I

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

Feedback from Partners II

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

Feedback from Partners III

- Reporting Anomaly: Incomplete information, Timezone undefined
- Fault alarm (Must sync ROA & RIR data timely)
- Bidirectional Routing Path: some paths are missing
- Can we mention the name of the Top-10 organizations and their cone size next to the diagram? That will give an idea about the top service providers in each country.
- In the “Dashboard”, it searches advertised prefixes but there is no subnet-wise search. Suppose, it will find out 103.28.120.0/22 under BdREN but cannot locate 103.28.121.0/24.
- There is not much usage of “Reverse Route Path”. It generates a file in “image” format which also doesn’t provide a legible view when enlarged. Better if it could be made available in pdf format.

Feedback from Partners IV

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



Open source the project

Been Fixed

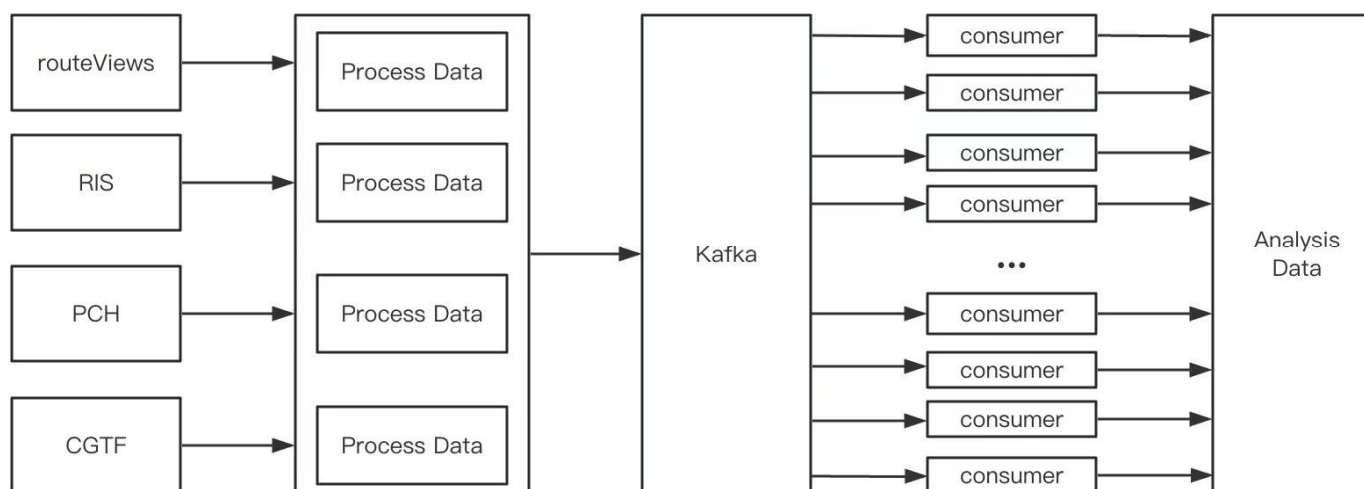
Been Fixed Lately



清华大学
Tsinghua University

Parallel Computing and Clusters to handle big routing data

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



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

- Project name: An Extension of the Ongoing Project ‘Developing a Collaborative BGP Routing Analyzing and Diagnosing Platform’ Project
- Funds: USD85,000
- Duration: 18 months
- Objectives (Draft):
 - Develop an **integrated looking glass** platform and api, which can leverage many looking glasses and return data to users
 - **Use looking glass** to further check routing hijacking at the data plan, and **to improve detection accuracy**
 - Develop **path hijacking** detection and **routing leak** detection
 - Continue to maintain and fix bugs of BGPWatch platform
 - Continue the community development and international collaboration

An Integrated Looking Glass and Open API

DragonLab CGTF Looking Glass

Integrated Looking Glass Platform

routes are matched , route are selected

Operation router

IP Address: 78130.176.4
ASN:AS9070
Country: Bulgaria
City: Sofia

DragonLab
Welcome to DragonLab's Network

Related links:
CGTF CyberBank

Looking Glass of Partners
<http://lg.kreonet2.net>

Contact Us
dev@dragonlab.org



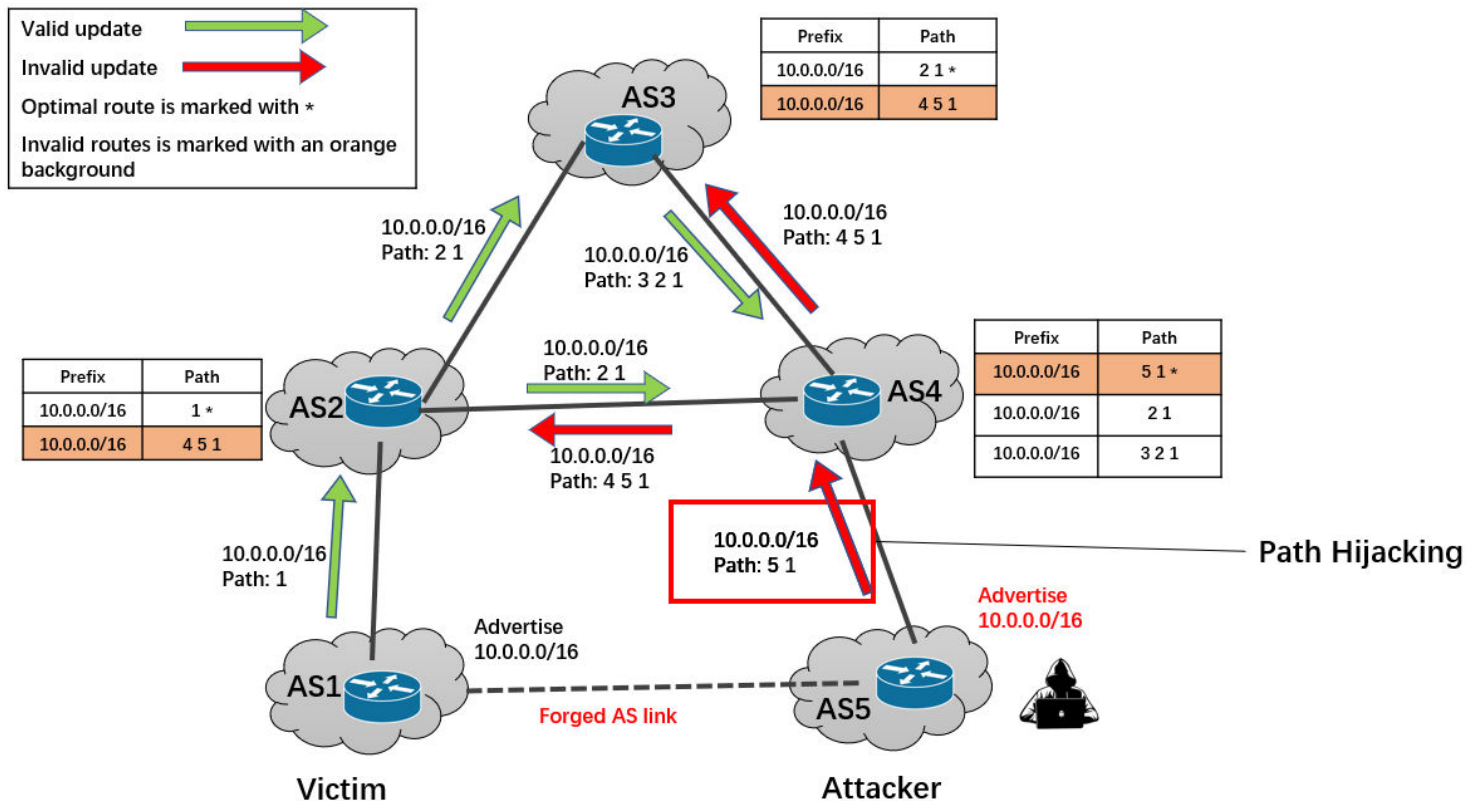
Based on the found VP, providing:
Open API, Open source, Open Platform



Detecting Fake AS-PATHs based on Link Prediction

--Paper published at ISCC2023

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

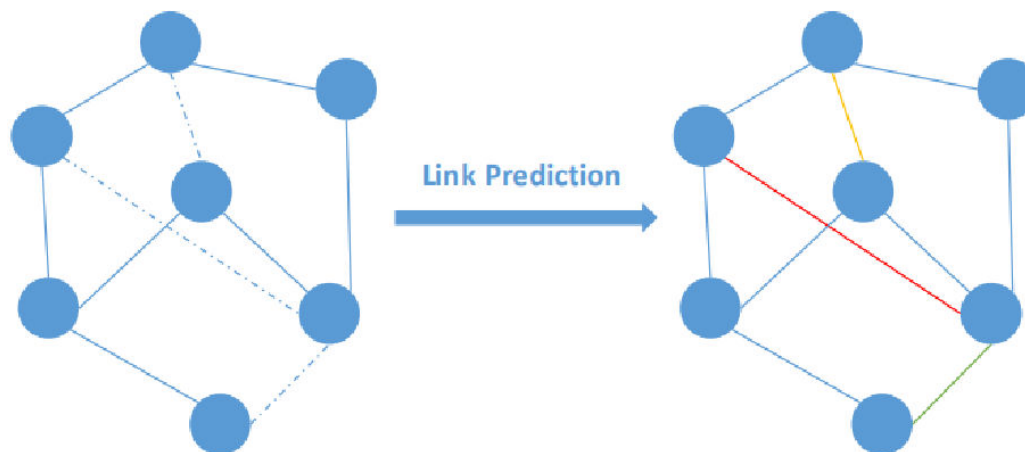


State-of-the-art for path hijacking detection

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

Idea

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

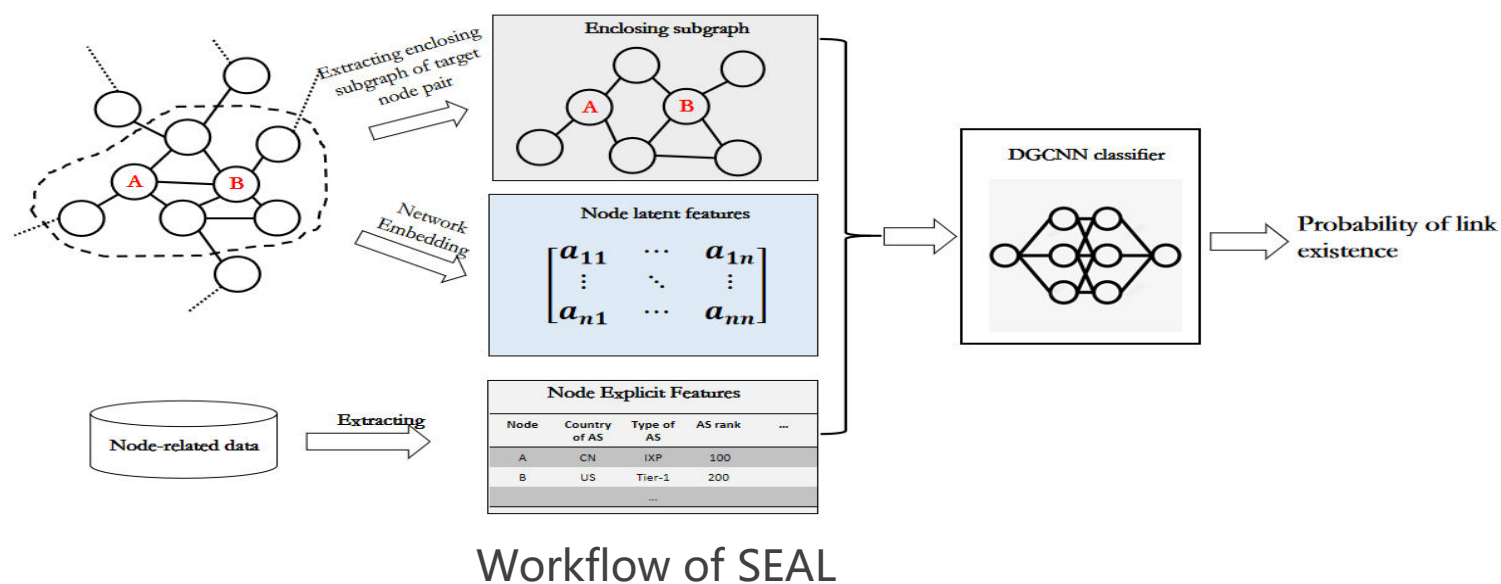


Is AS link predictable?

- Zhuang et al recently formulate the link prediction as a matrix completion task. Their work explain the predictability of AS link.
- Graph characteristics of AS-level topology
 - power-law distribution
 - negative degree-degree correlation
 - Hierarchical
 - AS links usually connect two ASes with the same properties.

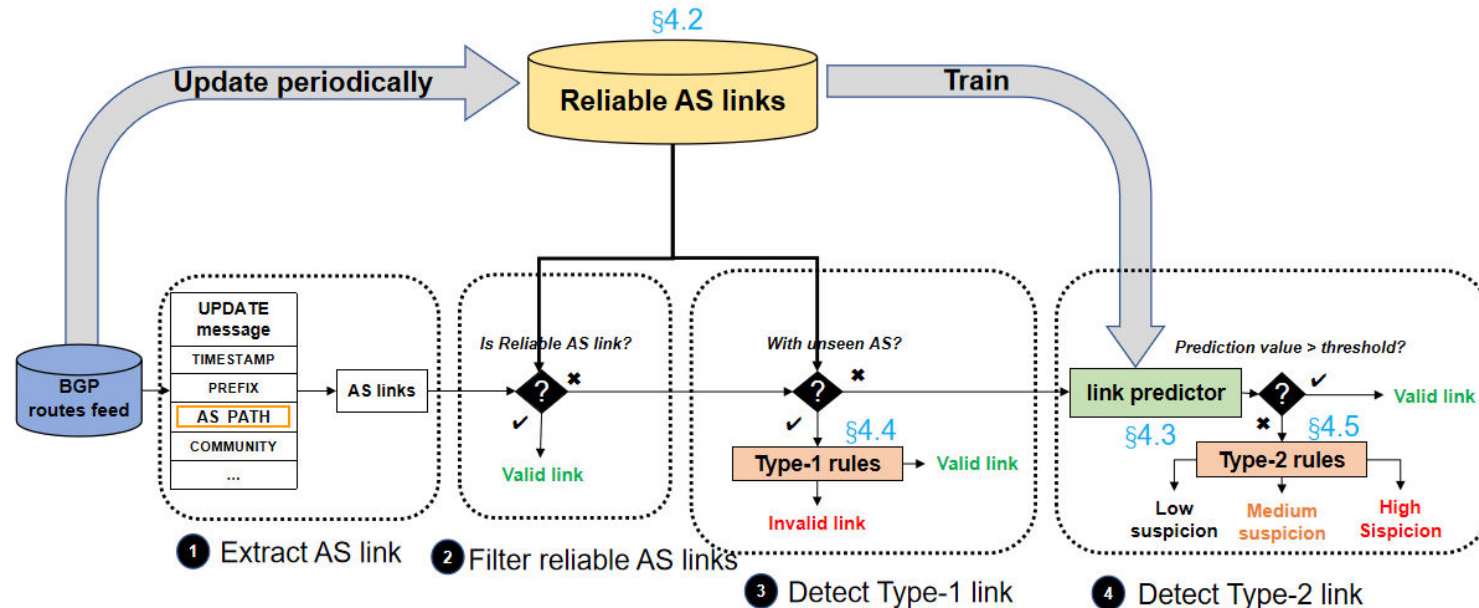
Unseen link classification

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



Metis: a fake AS-PATHs detection framework

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



Reliable links

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

CAIDA'S IPV4 AS CORE GRAPH
JANUARY 2020

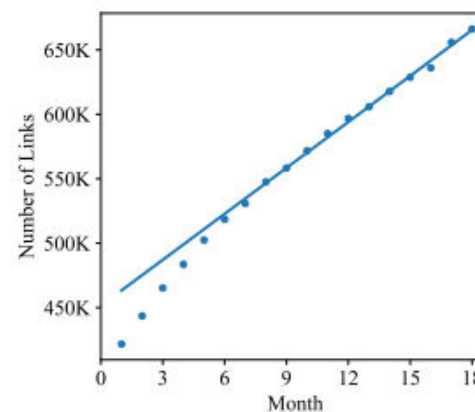
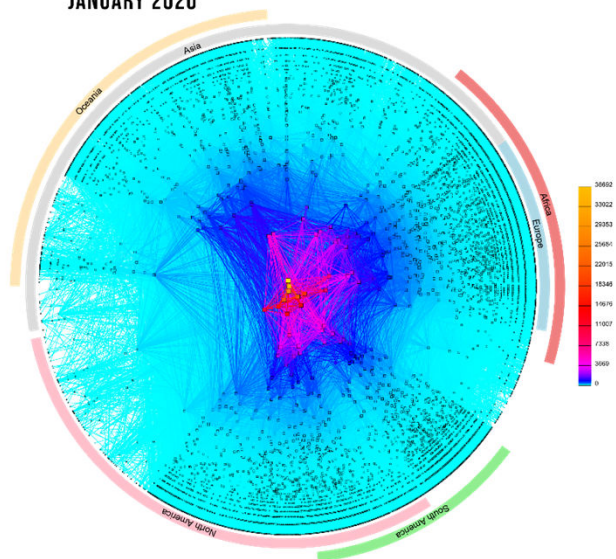
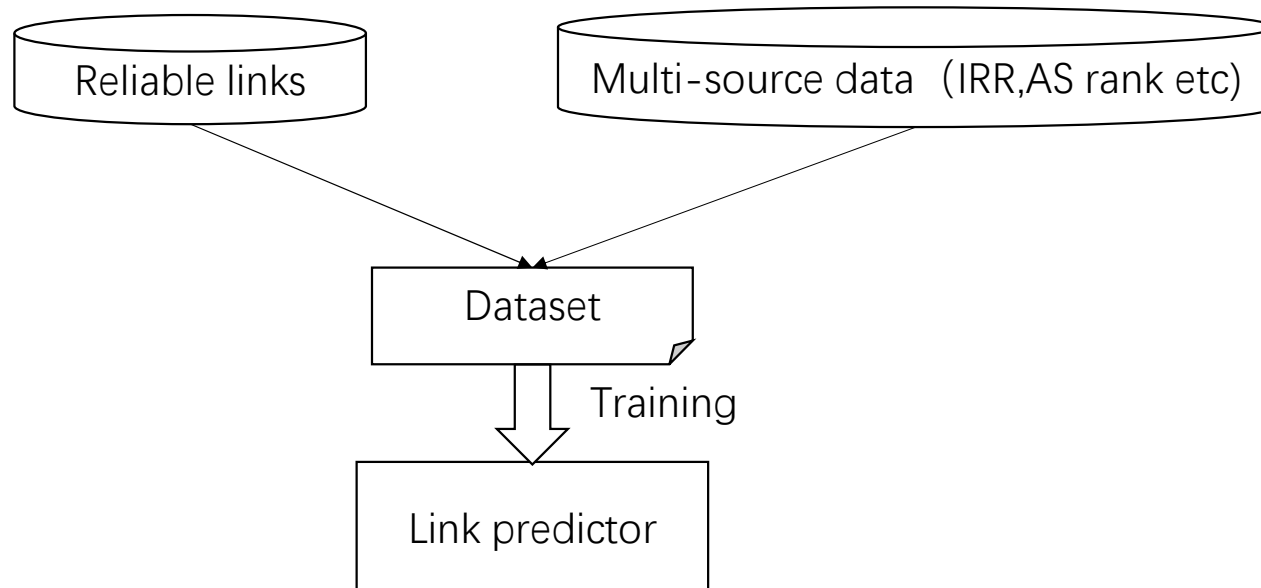


Fig. 7: The number of union AS links in CAIDA AS relationship data of the past N months of November 2021

Link predictor

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

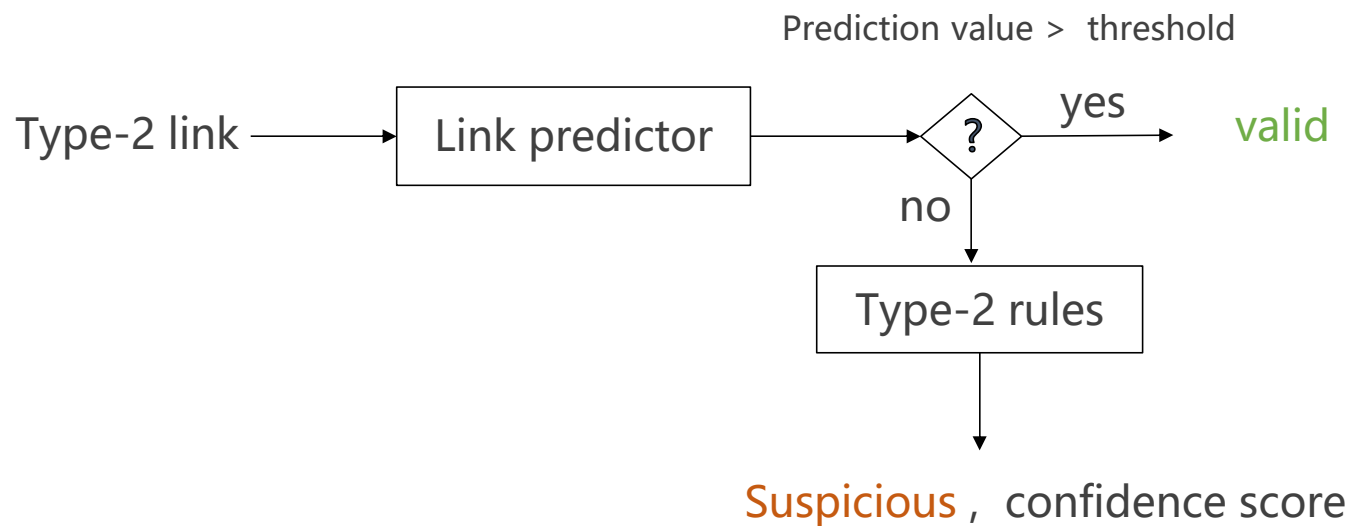


Type-1 unseen link detection

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

Type-2 unseen link detection

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



Type-2 rules

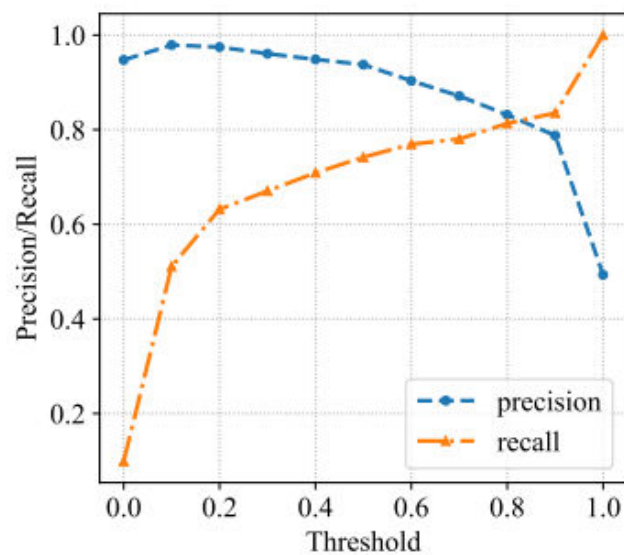
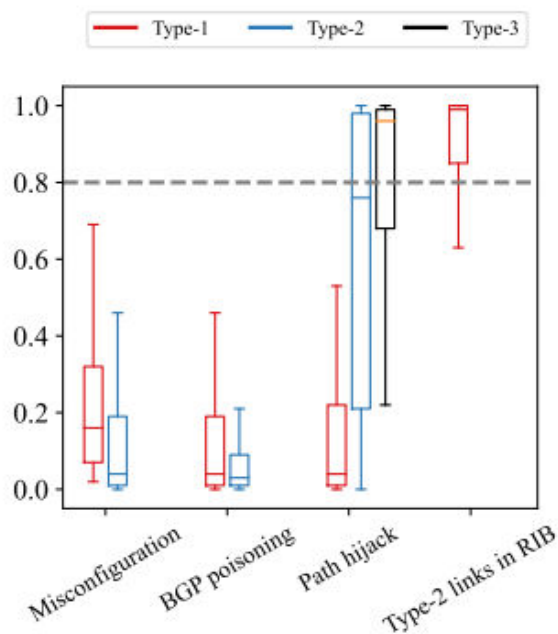
- Initial confidence score is 0
- The score increases 1 when:
 - AS-PATH is longer than the pre-set length threshold
 - The link with single digit ASN in the right side
 - The edit distance of the ASes is 1
 - Loop in AS-PATH, and the link is in the loop
 - AS-PATH violate valley-free rule
 - Traffic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

Evaluation

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

Evaluation

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



Evaluation

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

TABLE III: Result of crafted AS-PATHs

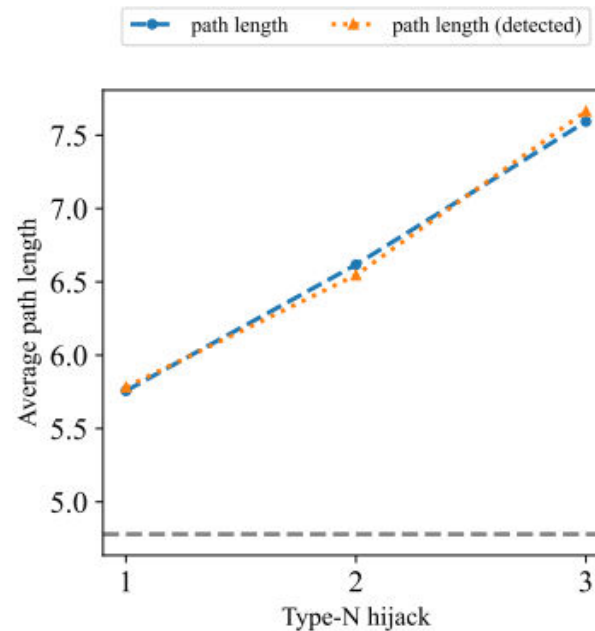
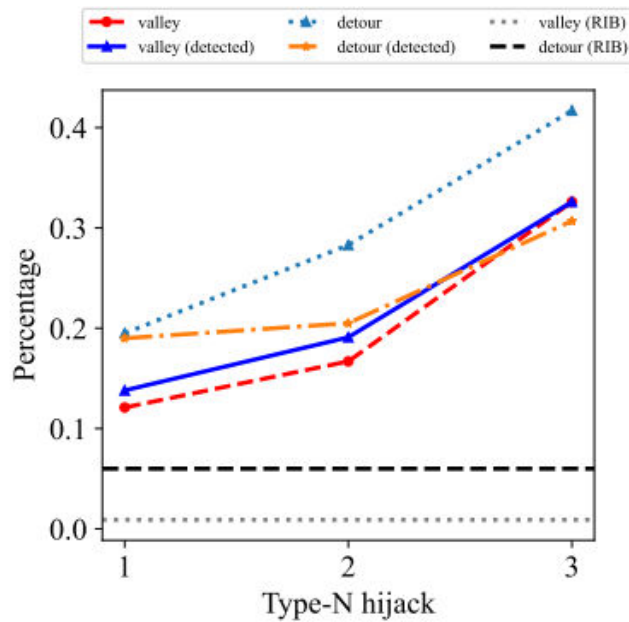
Type of AS-PATH	Number	Reliable link	Type-1 link	Type-2 link	valid AS-PATH	Suspicious AS-PATH				Accuracy
						Type-1	high	medium	low	
GREEN AS-PATHs	7000	11181	358	187	6966	5	3	6	20	99.5%
Type-1 Misconfiguration	1000	2231	108	985	167	0	924	0	0	92.4%
Type-2 Misconfiguration	1000	2174	496	582	256	247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

Evaluation

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

Evaluation

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



Evaluation

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

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

Comments and Suggestions?

Contact us at: sec@cgtf.net