User Experience and Suggestions to Improve - LEARN on BGPWatch Platform

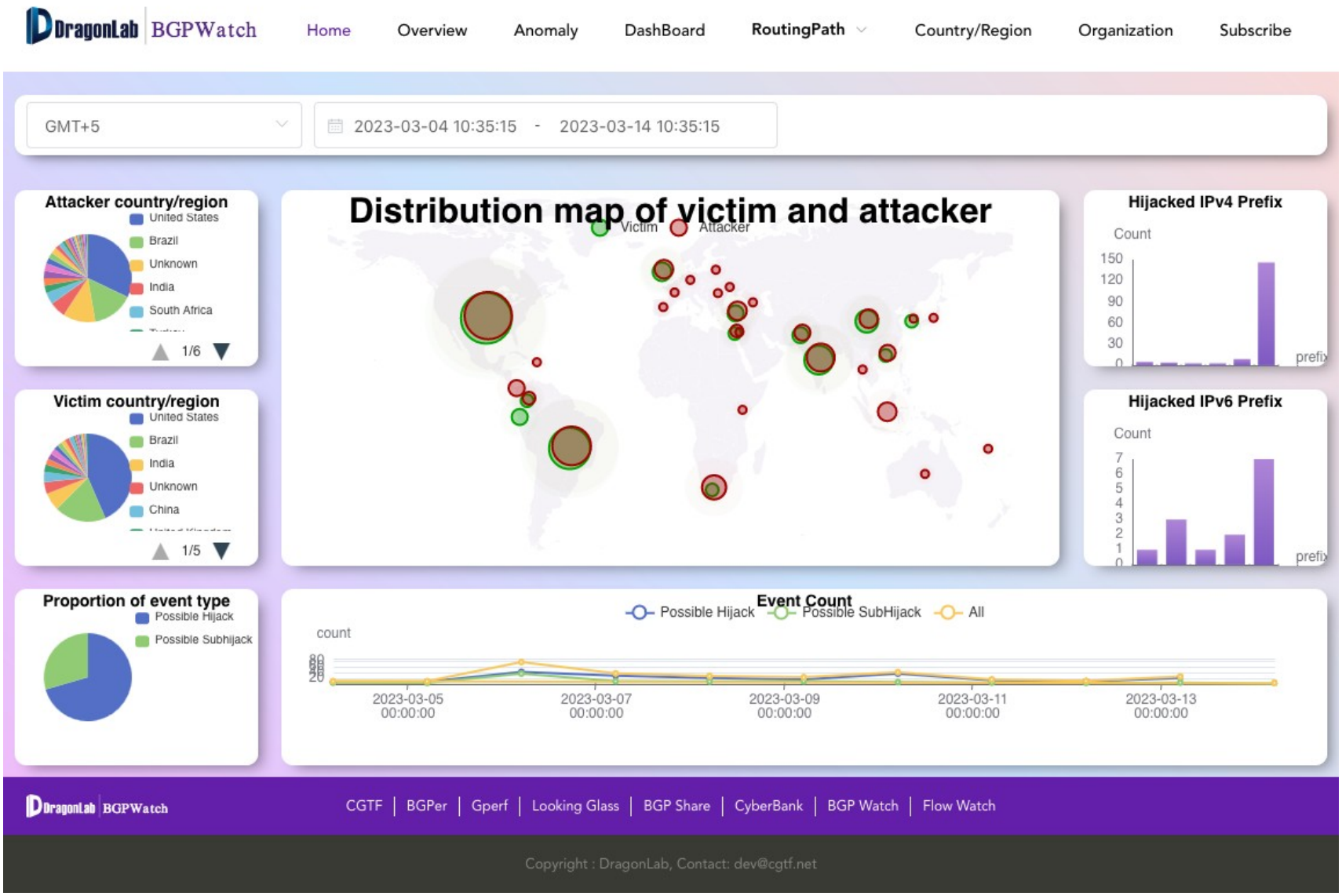
Nepal

14th March 2023

The IPv4/IPv6 Joint Research Project Updates @ APAN 55 - Kathmandu

Dhammika Lalantha / LEARN

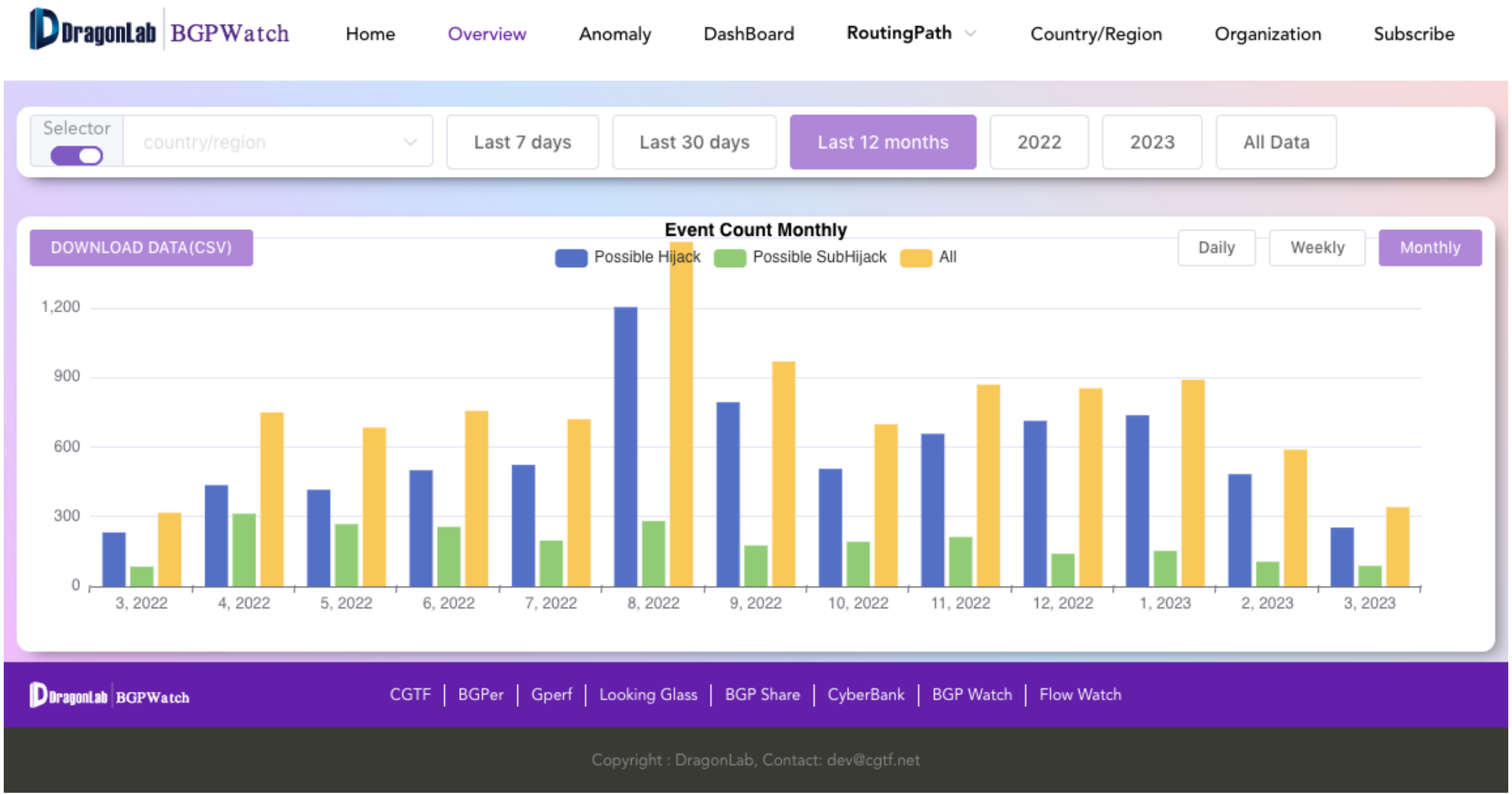
Home Page


DragonLab BGPWatch
Home
Overview
Anomaly
DashBoard
RoutingPath
Country/Region
Organization
Subscribe
GMT+5
2023-03-04 10:35:15 - 2023-03-14 10:35:15
Attacker country/region
United States
Brazil
Unknown
India
South Africa
1/6
Victim country/region
United States
Brazil
India
Unknown
China
1/5
Distribution map of victim and attacker
Victim
Attacker
Hijacked IPv4 Prefix
Count
150
120
90
60
30
0
prefix
Hijacked IPv6 Prefix
Count
7
6
5
4
3
2
1
0
prefix
Proportion of event type
Possible Hijack
Possible Subhijack
Event Count
Possible Hijack
Possible SubHijack
All
count
2023-03-05 00:00:00
2023-03-07 00:00:00
2023-03-09 00:00:00
2023-03-11 00:00:00
2023-03-13 00:00:00
DragonLab BGPWatch
CGTF | BGPer | Gperf | Looking Glass | BGP Share | CyberBank | BGP Watch | Flow Watch
Copyright : DragonLab, Contact: dev@cgtf.net

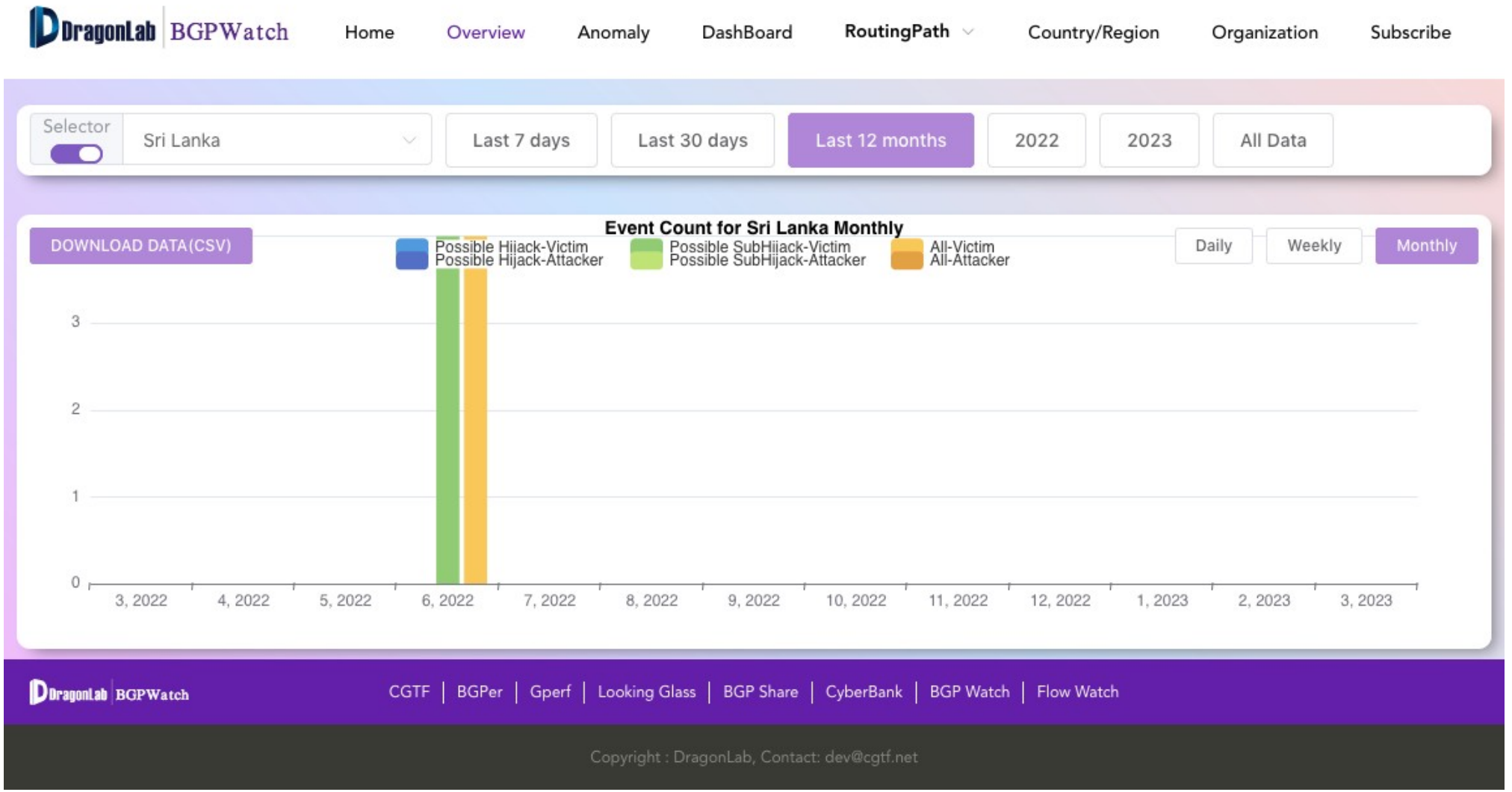
Home Page

- Gives and statistical graphical overview of BGP hijack detection
- Victim & Attacker pie charts and bar charts on count of hijacked Prefix numbers are informational and useful
- Hijack and Sub-Hijack detection
- Suggestion on Visual improvements
  - Visual directional relationship from attacker to victim
  - Zooming of Map
  - Larger view/pop-out view of other surrounding windows

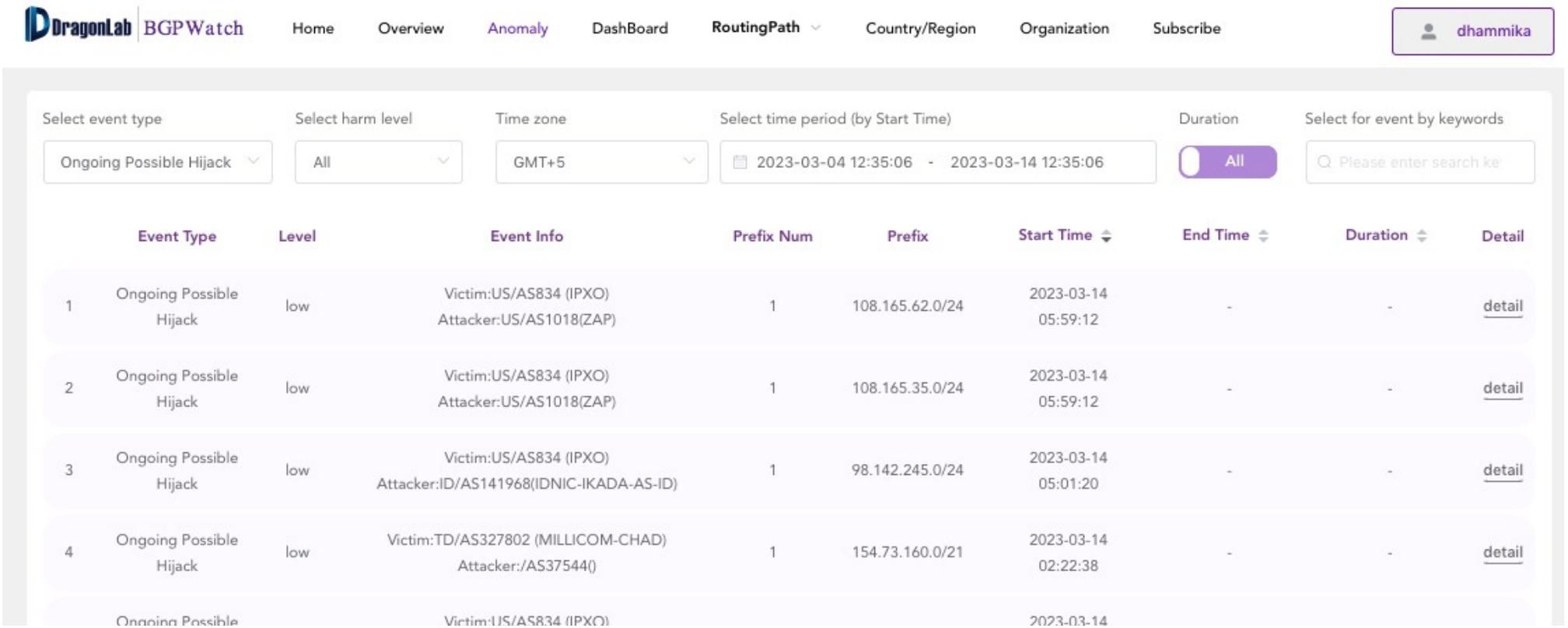
Overview


DragonLab BGPWatch
Home
Overview
Anomaly
DashBoard
RoutingPath
Country/Region
Organization
Subscribe
Selector
country/region
Last 7 days
Last 30 days
Last 12 months
2022
2023
All Data
DOWNLOAD DATA(CSV)
Event Count Monthly
Possible Hijack
Possible SubHijack
All
Daily
Weekly
Monthly
1,200
900
600
300
0
3, 2022
4, 2022
5, 2022
6, 2022
7, 2022
8, 2022
9, 2022
10, 2022
11, 2022
12, 2022
1, 2023
2, 2023
3, 2023
DragonLab BGPWatch
CGTF | BGPer | Gperf | Looking Glass | BGP Share | CyberBank | BGP Watch | Flow Watch
Copyright : DragonLab, Contact: dev@cgtf.net

Overview


DragonLab BGPWatch
Home
Overview
Anomaly
DashBoard
RoutingPath
Country/Region
Organization
Subscribe
Selector
Sri Lanka
Last 7 days
Last 30 days
Last 12 months
2022
2023
All Data
DOWNLOAD DATA(CSV)
Event Count for Sri Lanka Monthly
Possible Hijack-Victim
Possible Hijack-Attacker
Possible SubHijack-Victim
Possible SubHijack-Attacker
All-Victim
All-Attacker
Daily
Weekly
Monthly
3
2
1
0
3, 2022
4, 2022
5, 2022
6, 2022
7, 2022
8, 2022
9, 2022
10, 2022
11, 2022
12, 2022
1, 2023
2, 2023
3, 2023
DragonLab BGPWatch
CGTF | BGPer | Gperf | Looking Glass | BGP Share | CyberBank | BGP Watch | Flow Watch
Copyright : DragonLab, Contact: dev@cgtf.net

Anomaly detection



Anomaly detection

- Gives real time anomaly detection as well historical events
- Can filter the events based on type of attack, level of harm, time happened, duration of attack and keywords (ASN, IP prefix, Country etc.)
- Can find the ongoing hijack detection
- Didn’t find any anomalies related to our ASN AS38229
- Attacker:LK or Victim:LK also didn’t give any result

Anomaly detection – Detailed view part 1

high level

Ongoing Possible Hijack Events

43.229.152.0/24-hijack1678635084 Ongoing Possible Hijack Events

Victim AS: 21859

Victim Country: US (United States)

Victim Description: ZEN-ECN

Start Time: 2023-03-12 15:31:24

During Time: no data

Hijacker AS: 64021

Hijacker Country: HK (Hong Kong)

Hijacker Description: Network-Transit

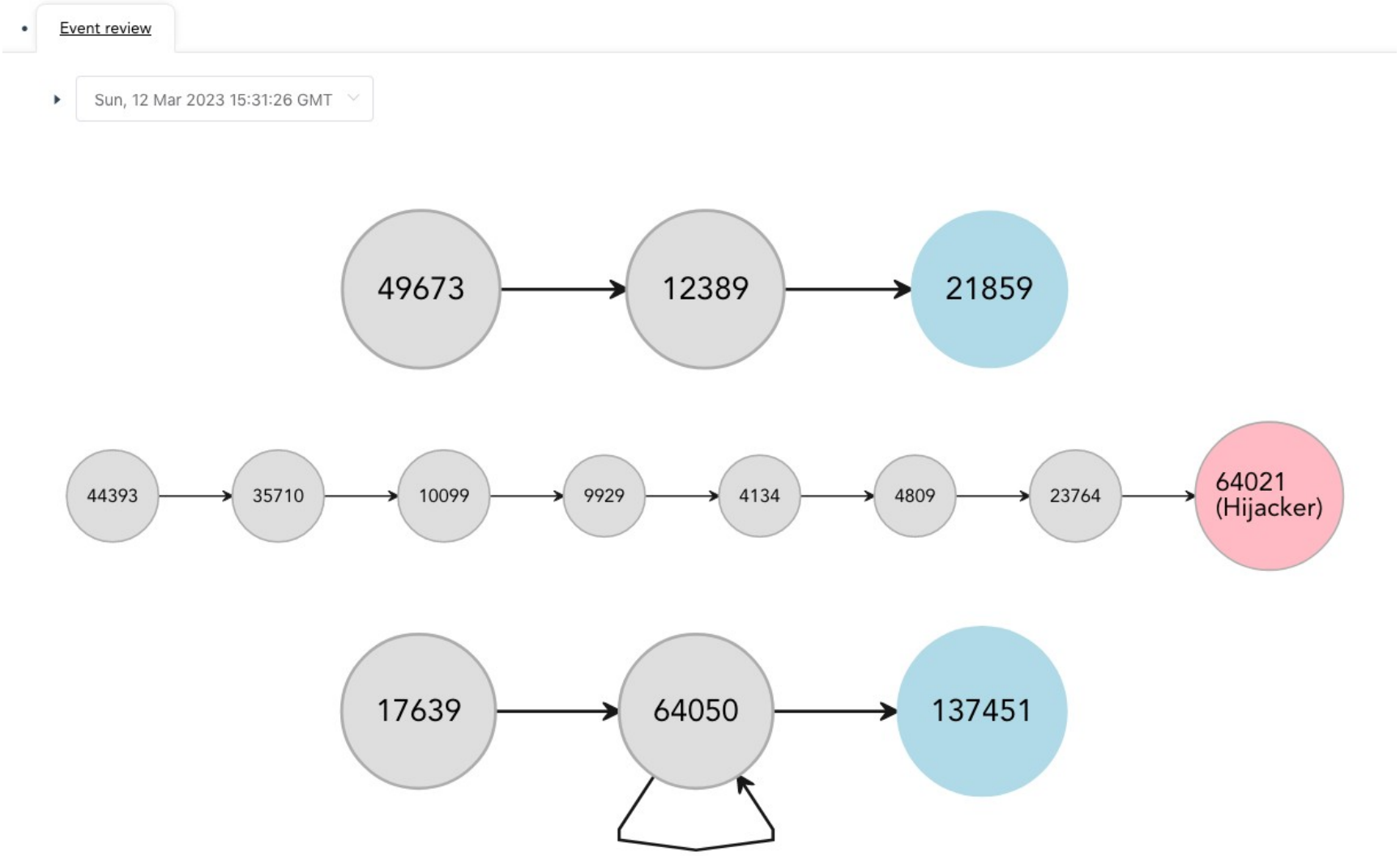
End Time: -

Anomaly detection – Detailed view part 2

Website :

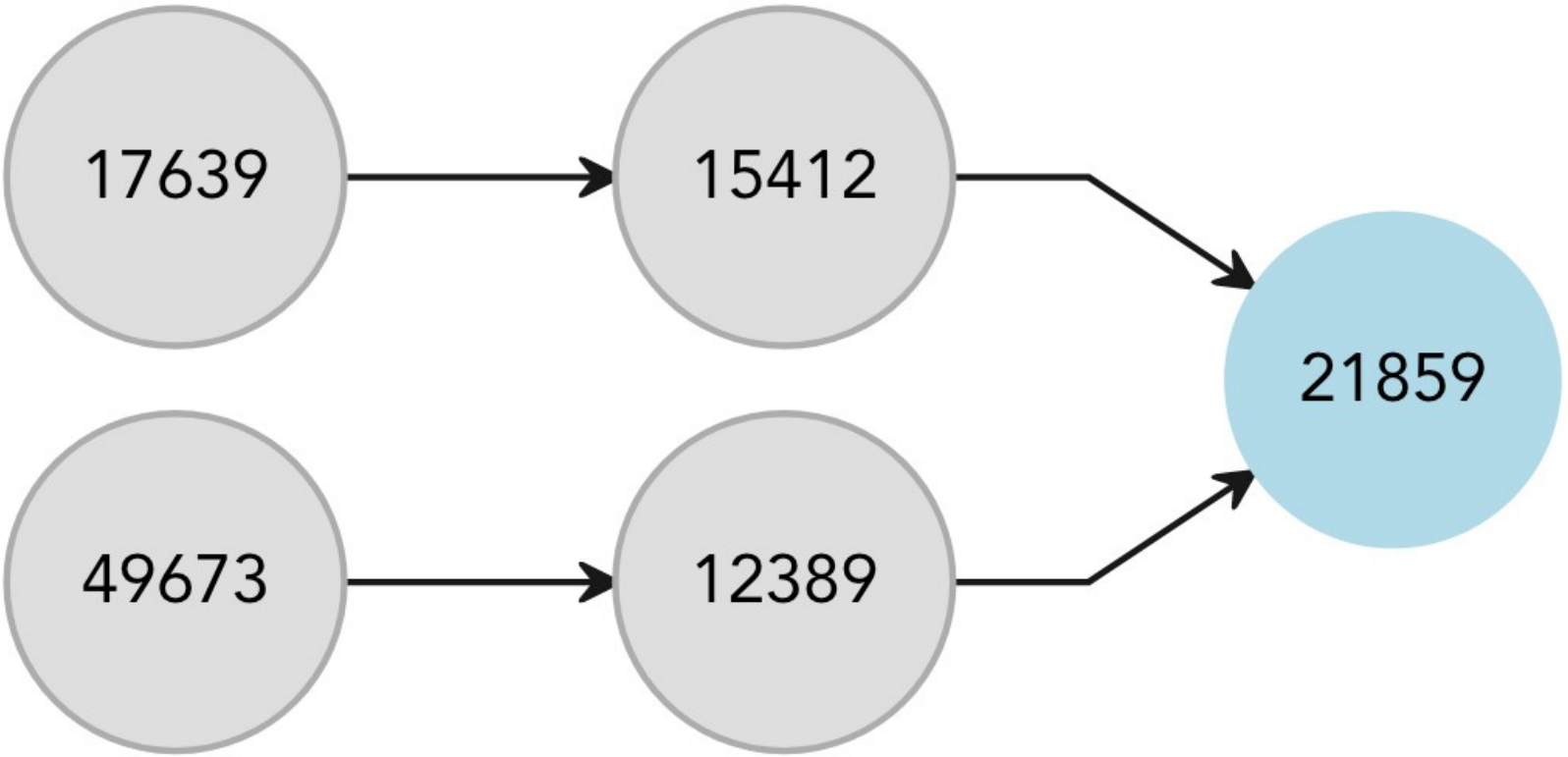
www.zzpengyuan.com	www.clxkjx.com	www.ahvi.com.cn	www.cheyinz.cn	www.yongchangcizhuang.com	www.sansi.cn	www.musooguitars.com
www.zzygzy.cn	www.chinabw.net	www.yzsda.com.cn	www.eastensound.com	www.zzwx100.com	www.zddown.com.cn	www.xmklj.cn
www.barula.cn	www.rouzila.cn	www.dyexpo.cn	www.91al.com	www.hxjrsy.com	www.wxfhm1688.com	www.gcyiyao.com
www.crmkj.com	www.newhonest.com	www.cinm.hk	www.jbshj.cn	www.houshimy.com	www.chaoshenghic.com.cn	www.hnssj.com
www.zzpsjx.cn	www.5xxx.cc	www.sqxnmj.com	www.yugongzengyang.com	www.sy165.com.cn	www.hnkxkj.cn	www.zjlvsen.cn
www.hntlkjssws.com	www.chinaflanges.cn	www.zgsdaw.com	www.dayig.cn	www.ypkj.com	www.676767.com	www.dasxiong.cn
www.hongsys.com	www.shlinzhi.cn	www.jlydja.com	www.tshskj.cn	www.yxyz6974.com	www.cfzyjz.com	www.sysmfl.com
www.yalijixie.com	www.cwjkw.cn	www.1580371.com	www.zggys.com	www.kmklhs.cn	www.yytianbao.com	www.0432cx.com
www.chongdiandian.com.cn	www.yangjuwu.cn	www.hzshunfa.cn	www.jianghaihuanbao.com.cn	www.13663818739.com	www.seanpharma.com	
www.xmbygg.com	www.mianshaozhuanjiqi.com	www.hbshutong.cn	www.lisozipper.com	www.ruyifood.cn	www.hongruijixie.com	www.kejte.cn
www.心静科技.com	www.hyjn.com.cn	www.diawan.club	www.clhongganji.com	www.firstpacifics.com	www.chinapcb.hk	www.3e-sky.cn
www.sxxdtjd.com	www.szdyhy.cn	www.bj-xbl.com	www.syztyb.com	www.玉逢惠德.com	www.alicungu.com	www.62444311.com

Anomaly detection – Detailed view part 3

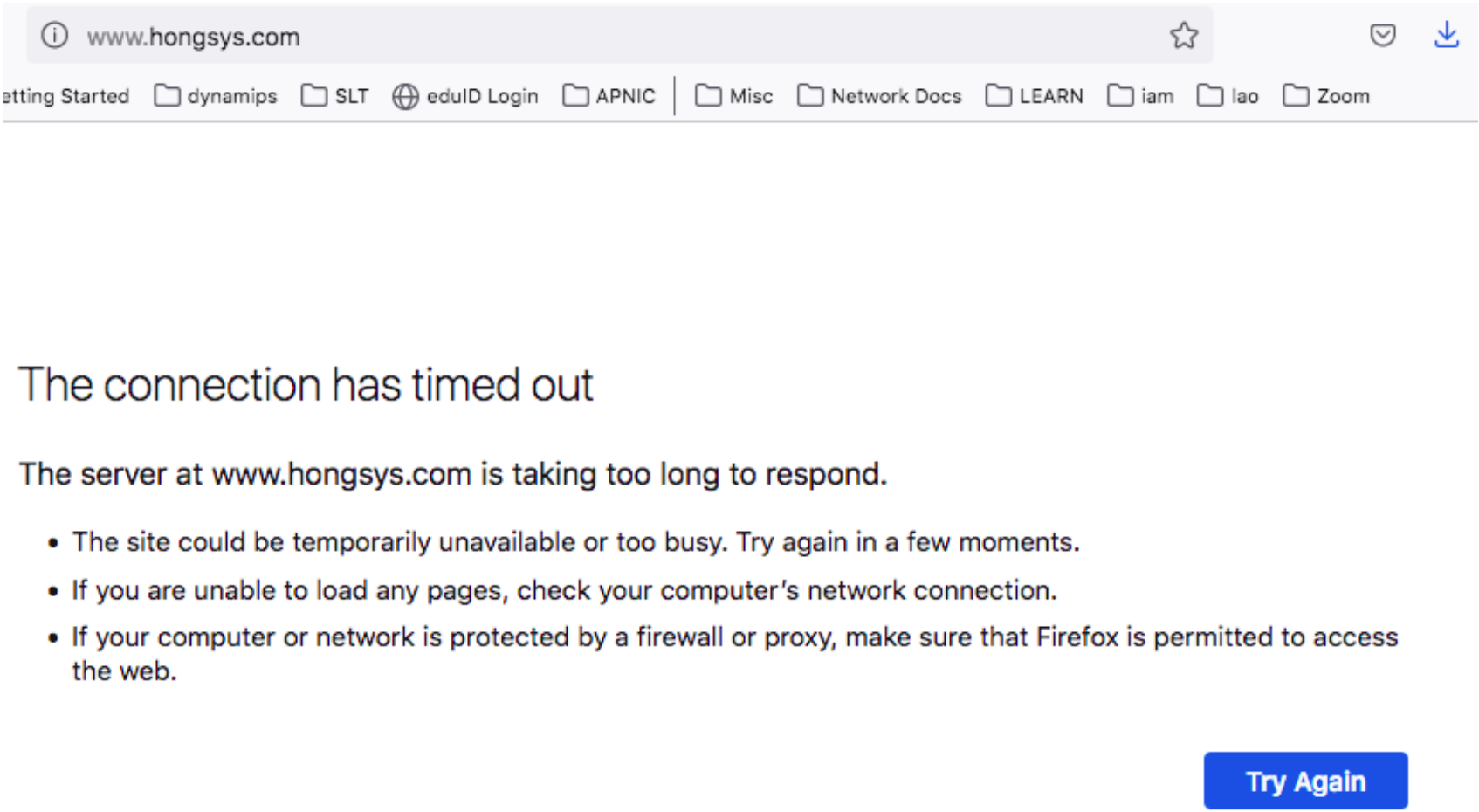


Anomaly detection – Detailed view part 4

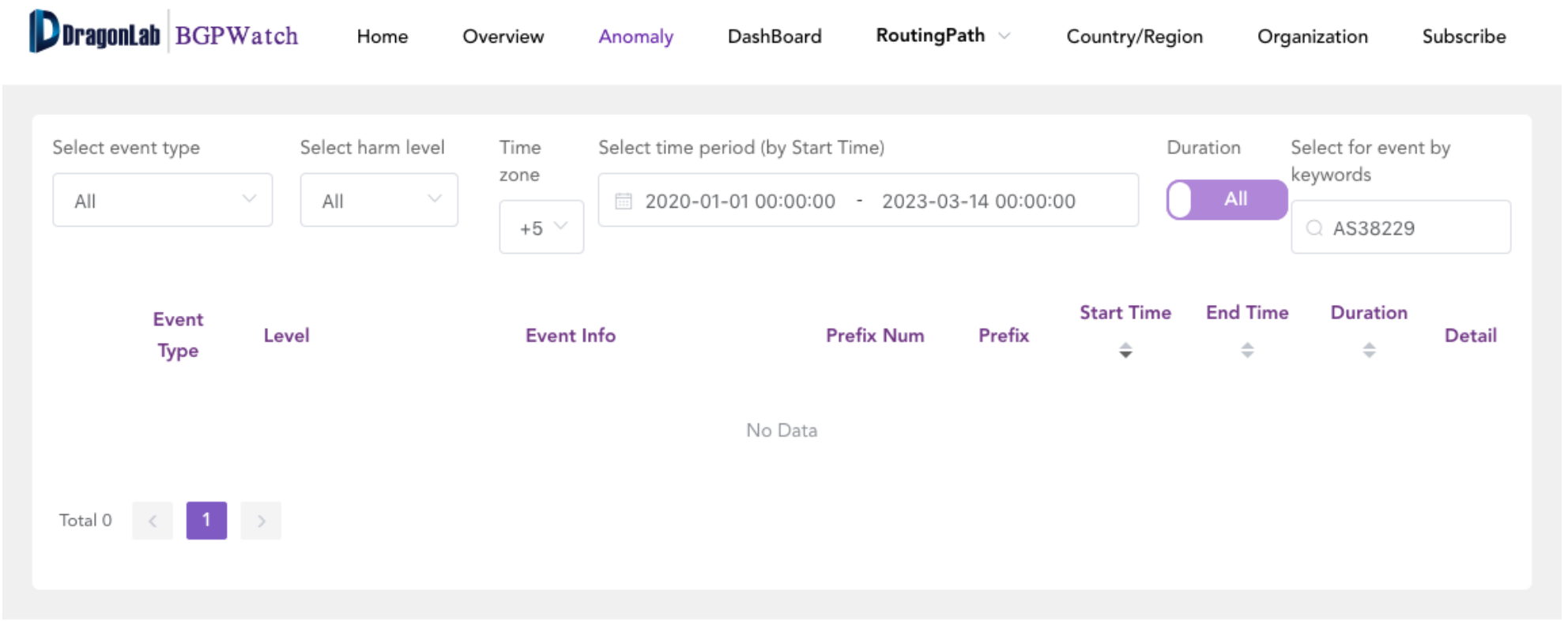
- Before event:



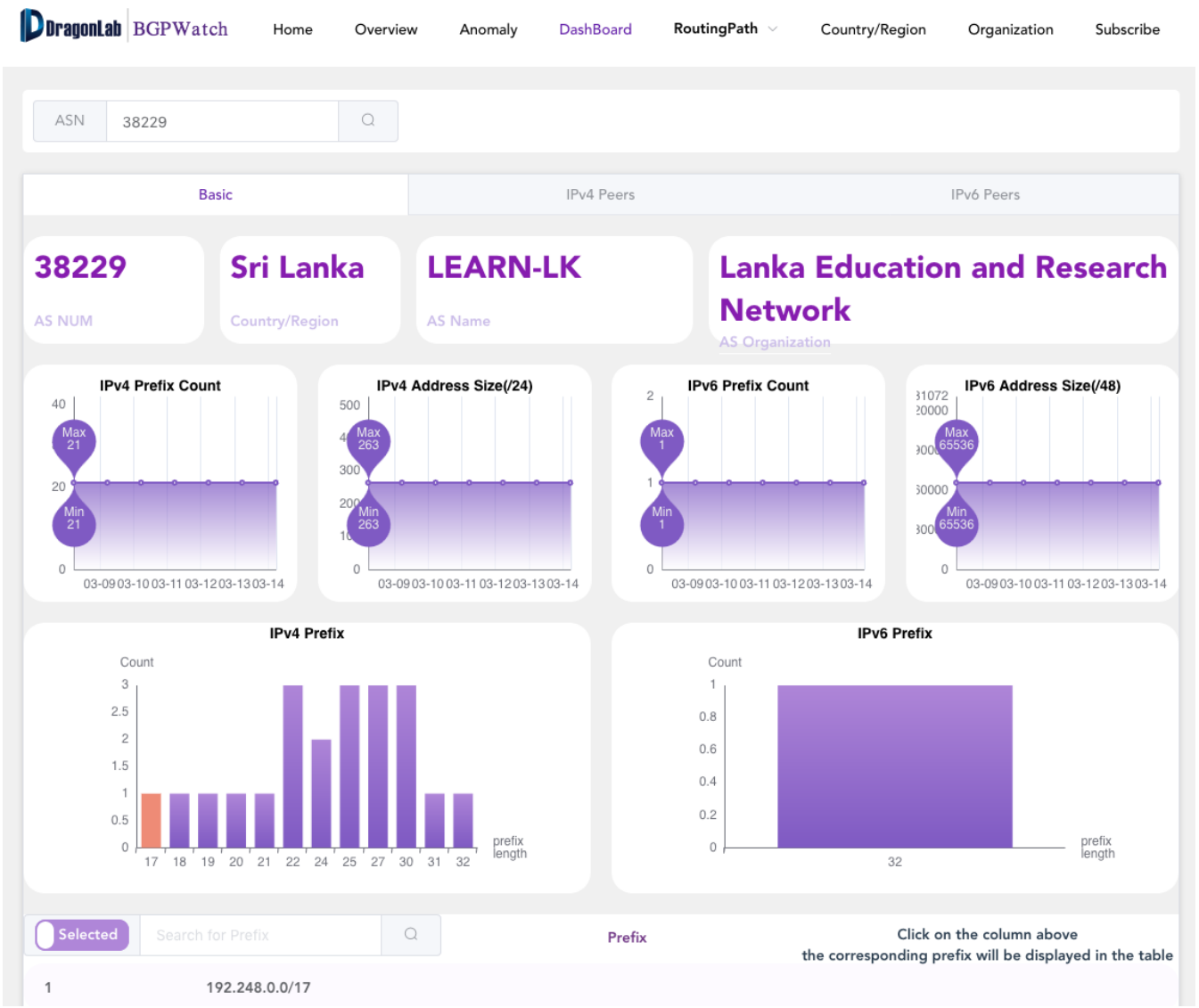
Anomaly detection – Verification



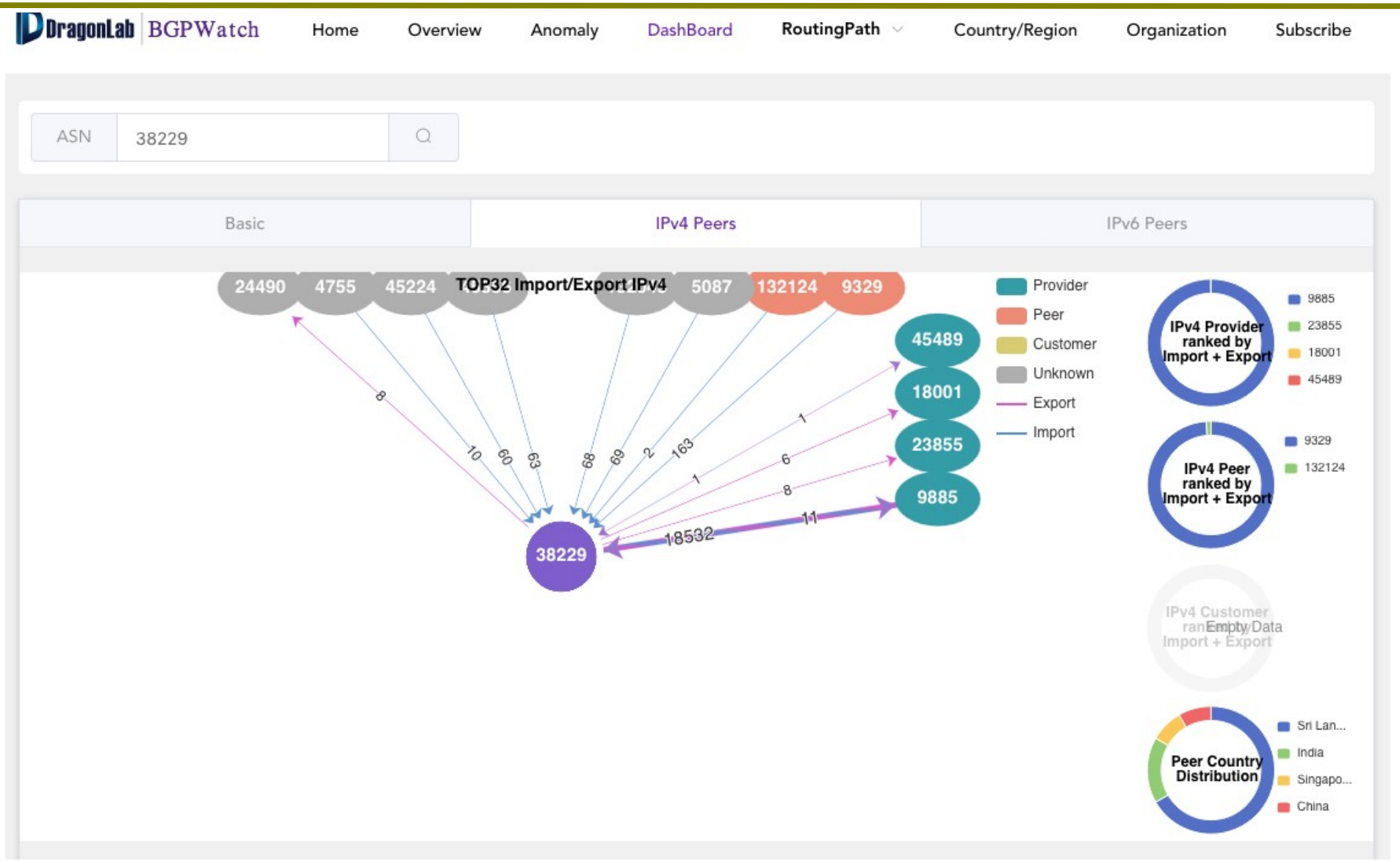
Anomaly detection – LEARN ASN



Dashboard


DragonLab BGPWatch
Home
Overview
Anomaly
DashBoard
RoutingPath
Country/Region
Organization
Subscribe
ASN
38229
Basic
IPv4 Peers
IPv6 Peers
38229
AS NUM
Sri Lanka
Country/Region
LEARN-LK
AS Name
Lanka Education and Research Network
AS Organization
IPv4 Prefix Count
IPv4 Address Size(/24)
IPv6 Prefix Count
IPv6 Address Size(/48)
IPv4 Prefix
Count
prefix length
IPv6 Prefix
Count
prefix length
Selected
Search for Prefix
Prefix
Click on the column above
the corresponding prefix will be displayed in the table
1
192.248.0.0/17

Dashboard – IPv4 Peers

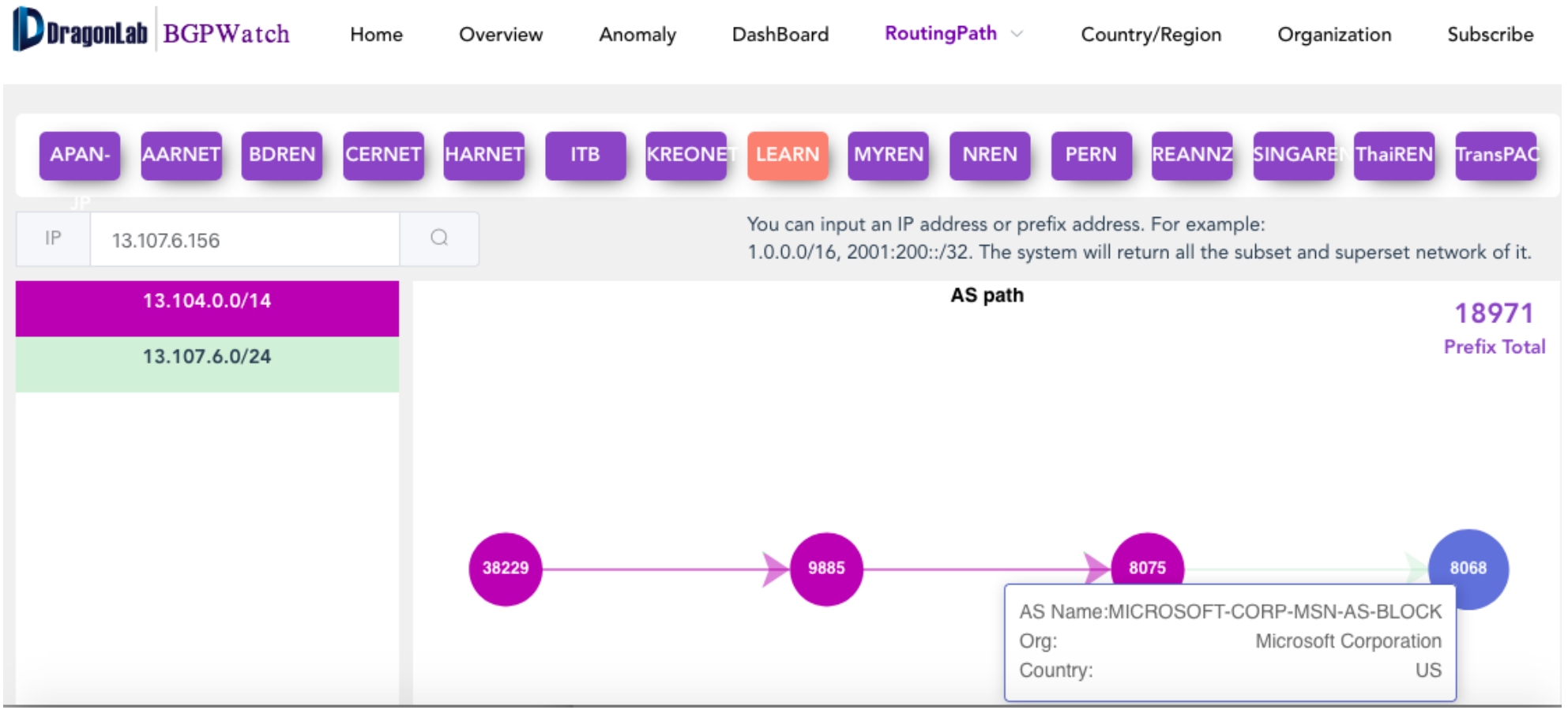


Dashboard – IPv4 Peers

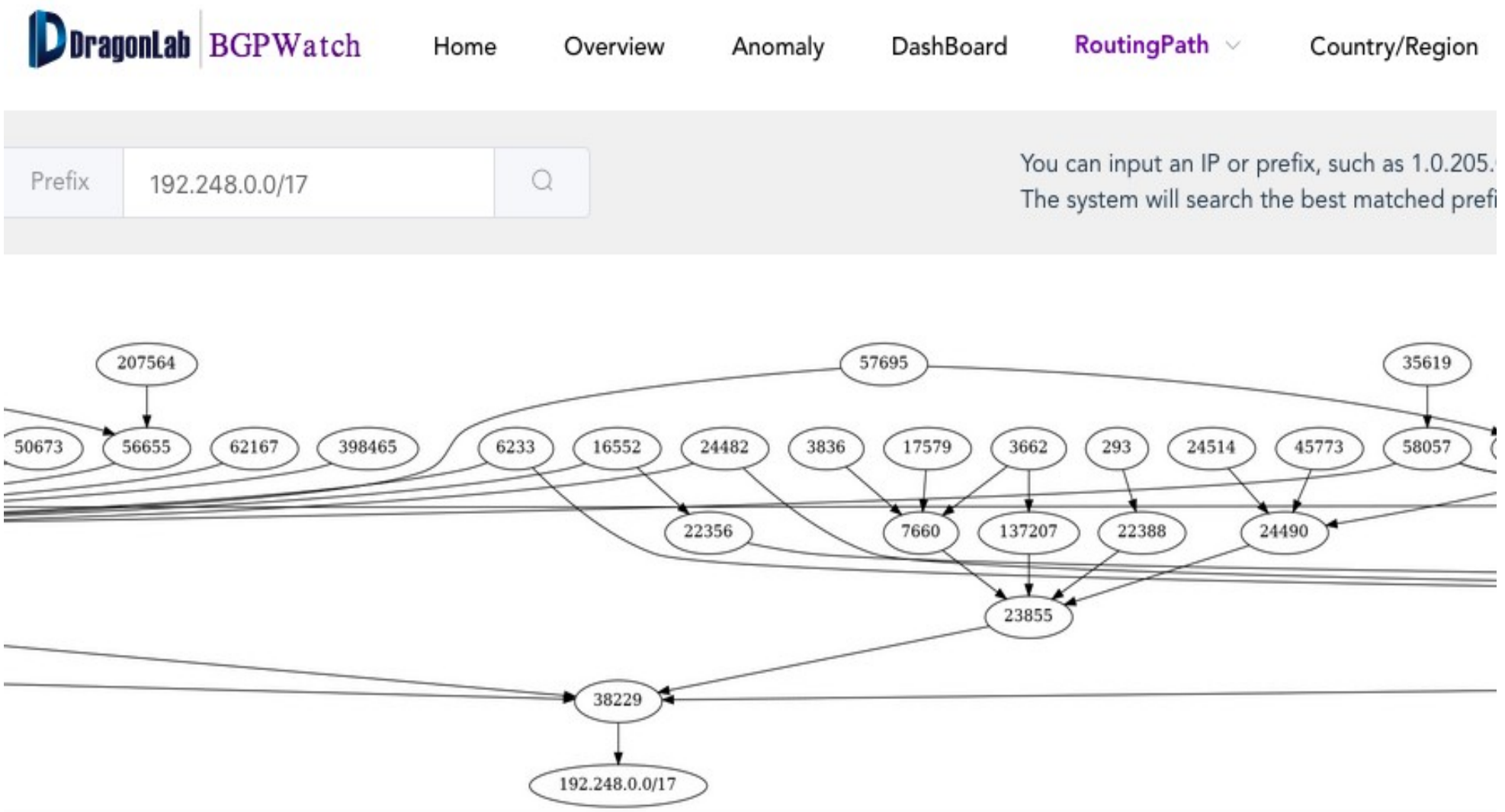
All IPv4 Neighbors

	AS neighbors	Organization	Country/Region	AS customer cone	Relationship	Export	Import
1	9329	Sri Lanka Telecom Ltd	Sri Lanka	9	peer	0	163
2	9885	National Knowledge Network	India	83	provider	11	18532
3	18001	Dialog Axiata Plc	Sri Lanka	11	provider	6	0
4	23855	SingAREN	Singapore	105	provider	8	0
5	45489	Sri Lanka Telecom Ltd	Sri Lanka	56	provider	1	1
6	132124	Information and Communication Technology Agency of Sri Lanka	Sri Lanka	1	peer	0	2

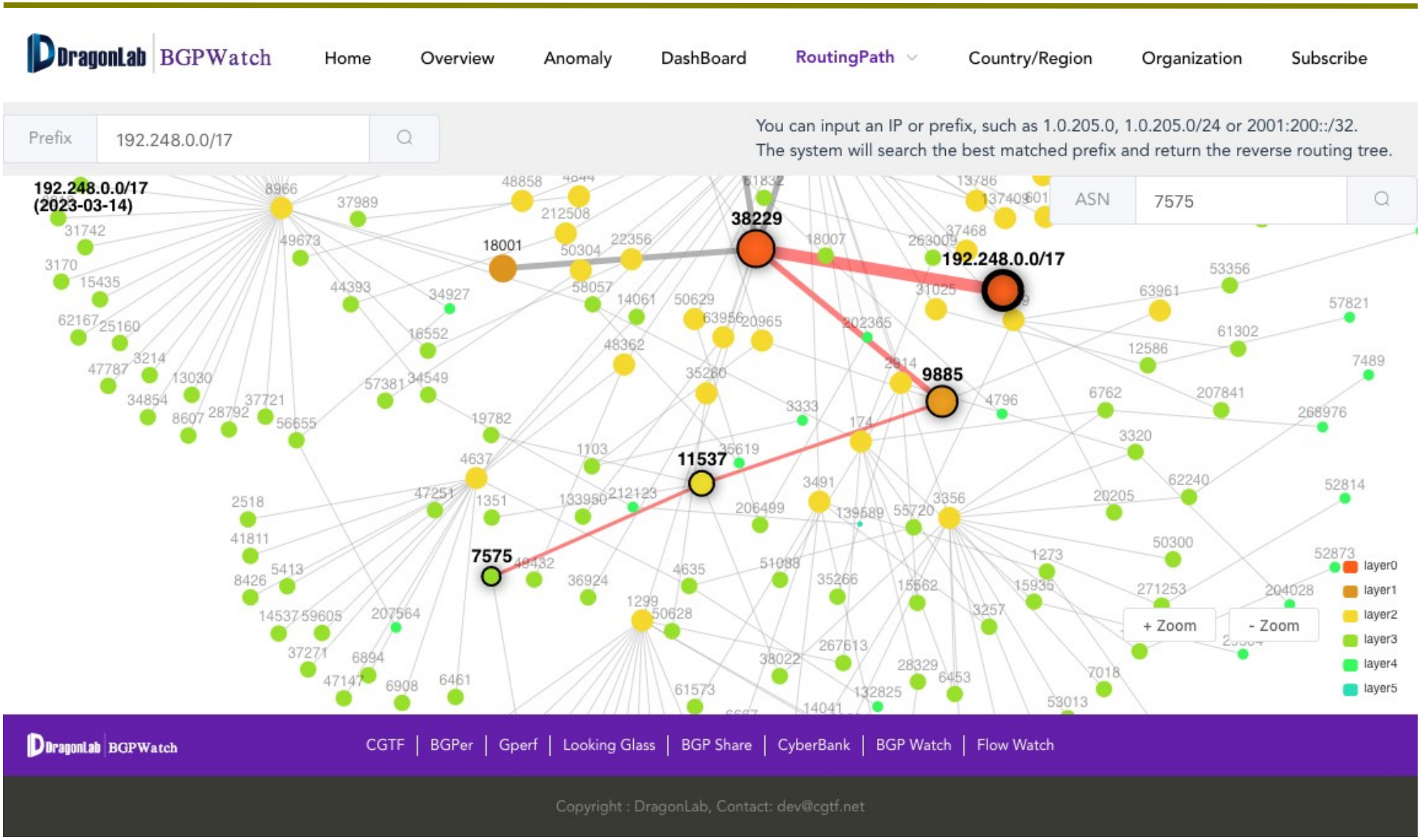
Routing Path (Forward)



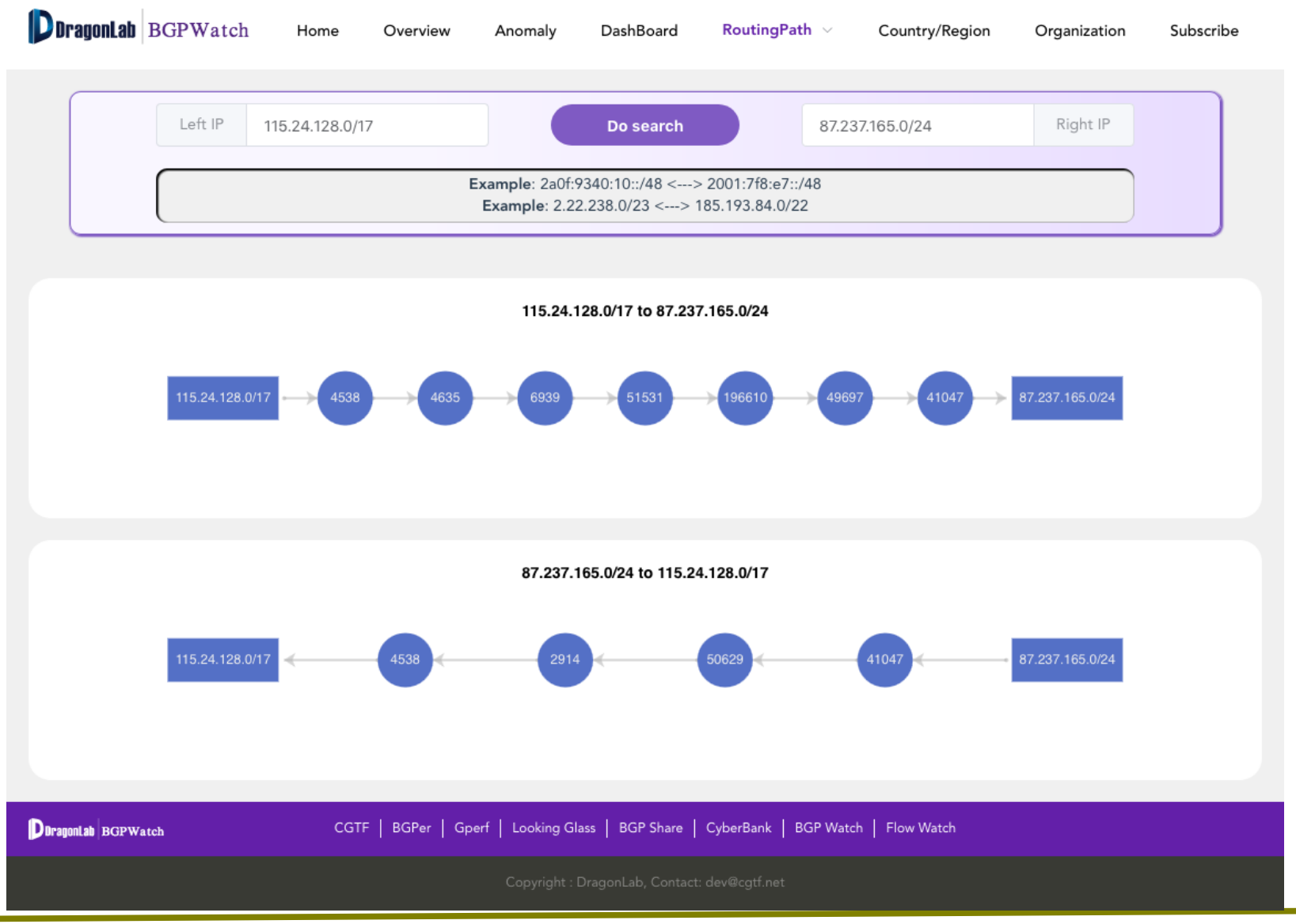
Reverse Routing Path



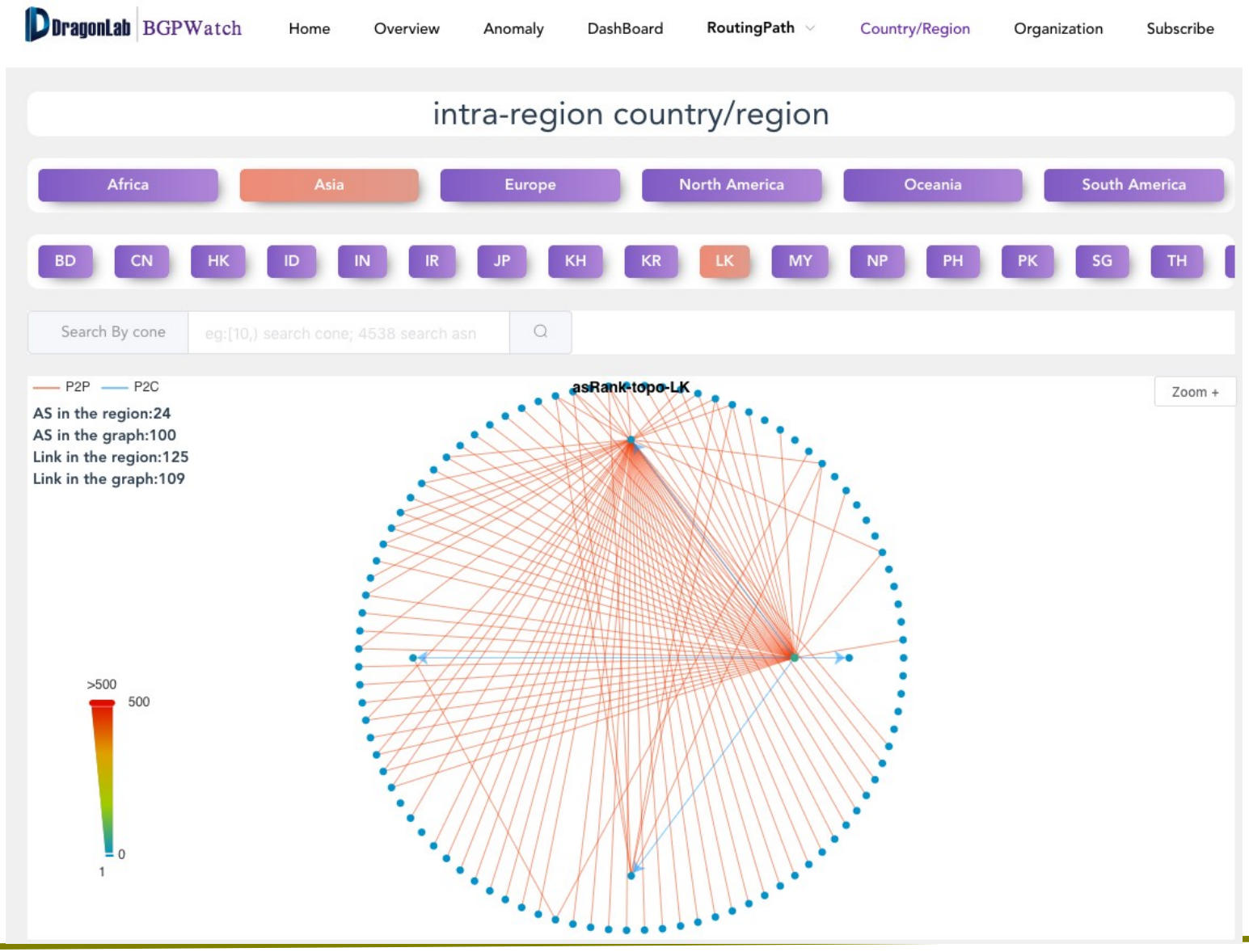
Reverse Routing Topology



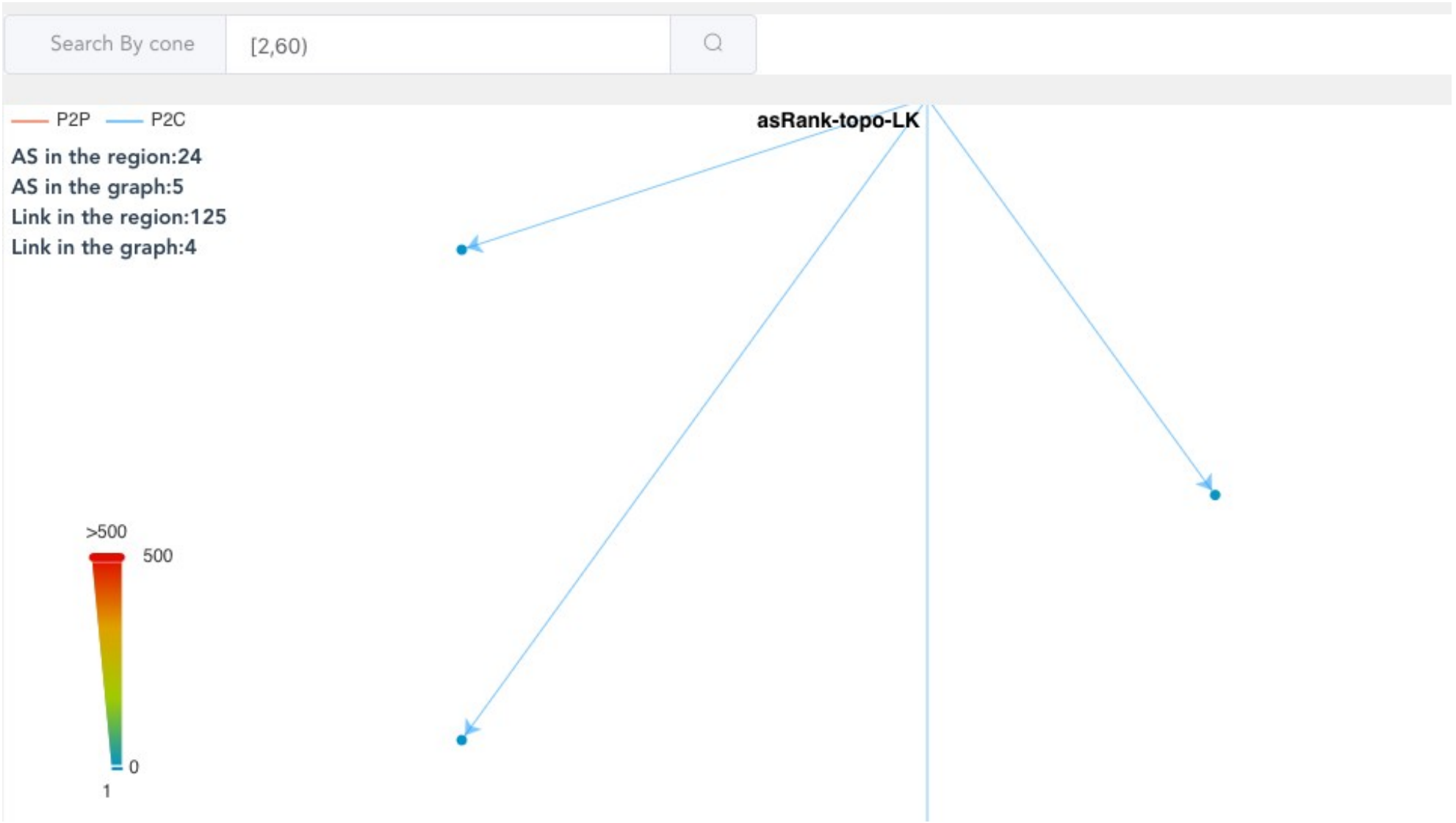
Bi-Routing Path



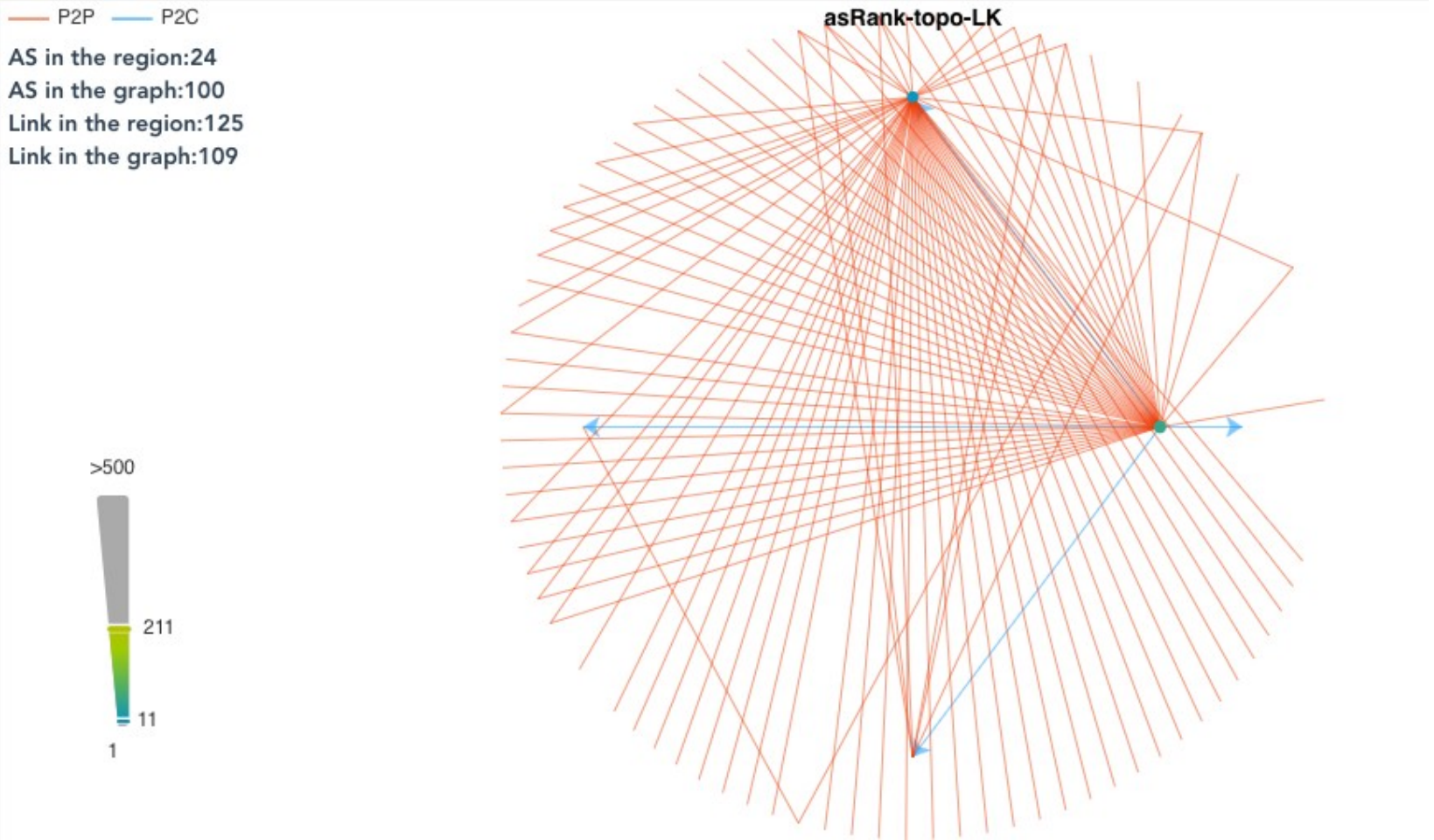
AS Rank Topology



AS Rank Topology - Filtering



AS Rank Topology - Filtering



Some more suggestions

- 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

Thank You

Dhammika Lalantha/LEARN

Email: lalantha@learn.ac.lk