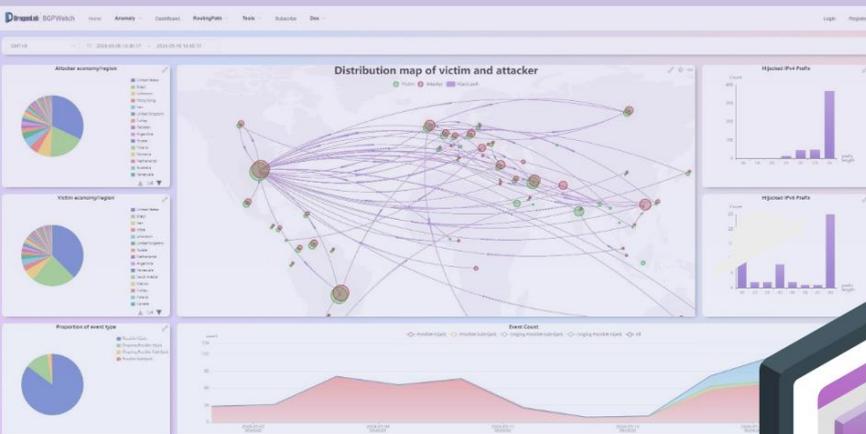


BGPWatch

User Manual





清華大學
Tsinghua University



APNIC
FOUNDATION



清華大學
Tsinghua University

User Manual on BGPWatch

Section 1. Registration and Logging in	3
Section 2. Homepage.....	6
Introduction	6
Navigating the Page.....	6
Section 3. Anomaly.....	10
Introduction	10
Navigating the Page	10
Overview.....	10
Anomaly.....	12
Anomaly Event Detail.....	14
Section 4. Dashboard.....	21
Introduction	21
Navigating the Page	21
Basic	21
IPv4 Peers	23
IPv6 Peers	25
WHOIS.....	26
Section 5. Routing Path	28
Introduction	28
Navigating the Page.....	28
Routing path.....	28
Reverse Routing Path (TOPO)	29
Bi-directional Routing Path	30
Jitter Route	31
Daily Bogan.....	32
Section 6. Tools	35
Introduction	35
Navigating the Page.....	35
Economy/Region	35
MOAS	36
Section 7. Subscription.....	39
Introduction	39
Navigating the Page.....	39
Section 8. Documentation.....	44
Introduction	44
Navigating the Page.....	44
User Manual PDF.....	44
User Manual Video.....	44
API Document.....	44

Background

Researchers and Engineers of Tsinghua University, under its initiated “Joint IPv4/IPv6 project” supported by Chinese Government, have developed a platform – called BGPWatch - which gives a full landscape of BGP routing and analyzing view by displaying the bi-directional routing path between Autonomous Systems, the incidents about route hijacking, the identity of the victims and the attackers, the hijacking statistics, the routing topology and many other features.

With the support from Tsinghua University and two phases of APNIC Foundation ISIF projects called “Developing a Collaborative BGP Routing Analyzing and Diagnosing Platform” and “An Extension of the Ongoing Project ‘Developing a Collaborative BGP Routing Analyzing and Diagnosing Platform’ Project”, this platform has been further developed by Tsinghua team based on the technical advice and experiences provided by the 19 NREN and 2 universities partners, including AARNET, APAN-JP, BdREN, CERNET, DOST-ASTI, ERNET, Göttingen University, HARNET, ITB, KREONET, LEARN, MYREN, NREN, PERN, REANNZ, RedCLARA, RNP, SingAREN, University of Surrey, ThaiREN, and TransPAC.

Website

The URL to this platform is: <https://bgpwatch.cgtf.net/>

Contact

The platform is in continual improvement. We welcome and greatly value every feedback and suggestions. The contact email is sec@cgtf.net.

BGPWatch

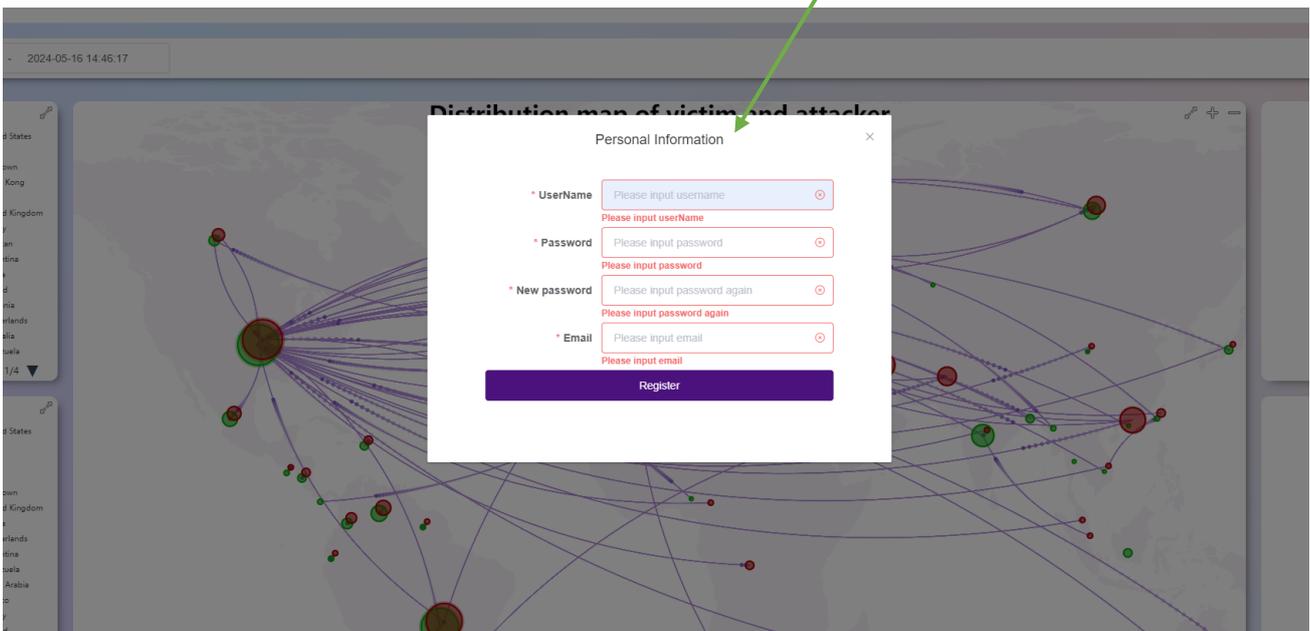
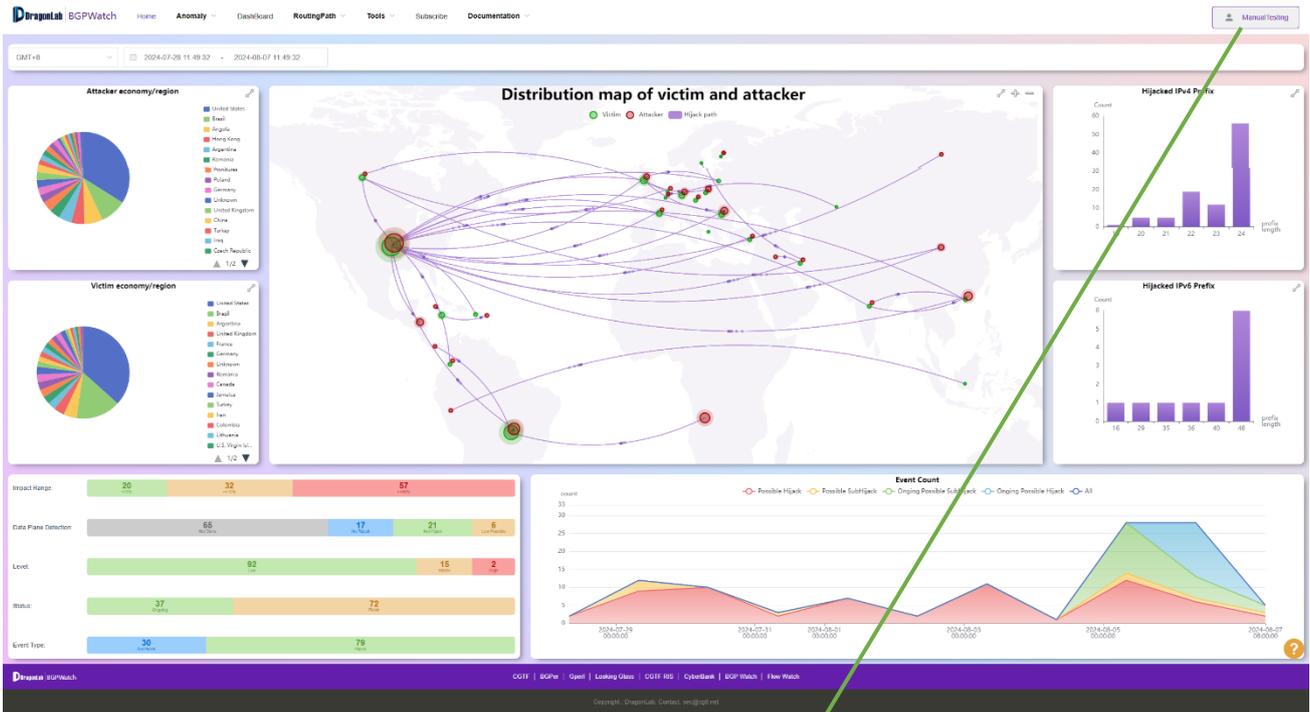
User Manual

Section 1 Registration and Logging in

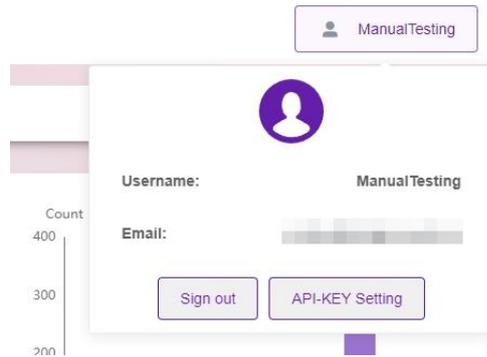


Section 1. Registration and Logging in

First, you can register in the BGPWatch by clicking on the “Register” Button located at the top-right corner of the homepage. In the pop-up window, you need to put your username, password [twice for confirmation], and email address in the text boxes and then click on “Register” button to request for your registration. You are going to receive an email from sec@cgf.net. If you put a username which is already in the system, it will give an error message “Duplicate Username”.

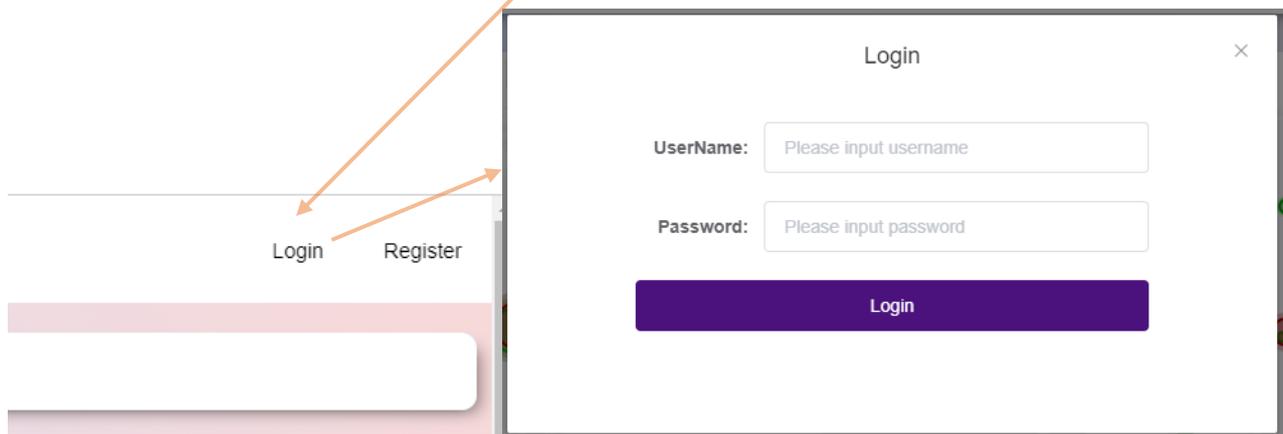


When you confirm your registration by clicking in the link received at your given email address, you will be automatically “logged in” to your account.



You can signout from the site by clicking the “**Sign out**” button.

Next time you log in, you simply click on the this **login** Button and login with your registered username and password. Logged-in users will get additional options like Subscription and Email Notifications which is described at the Subscribe Section.



DragonLab | BGPWatch

BGPWatch

User Manual

Section 2 Homepage



www.bgpwatch.net

Section 2. Homepage



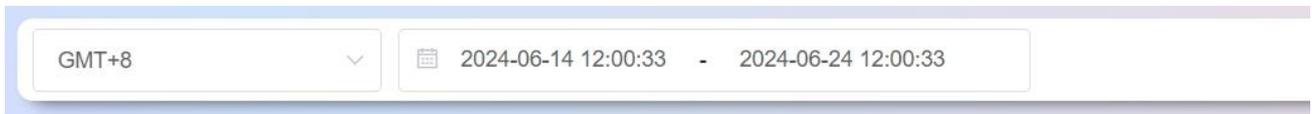
Introduction

Home page shows summary hijacking information.

Navigating the Page

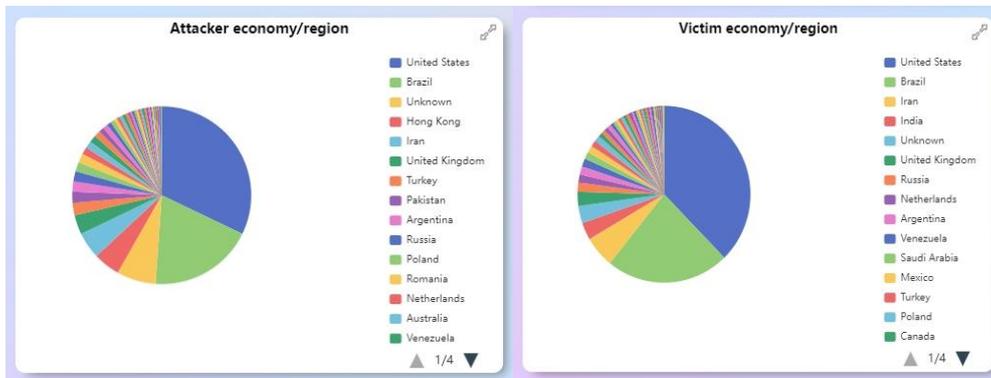
On top of the homepage, there is a menu and a calendar where you can select:

- Time zone
- Date range
 - Start Date
 - End Date

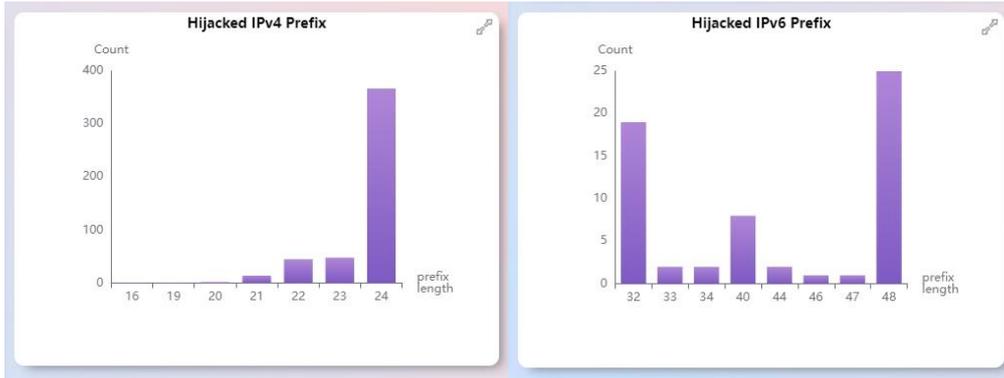


Following the time selections, there are four (4) zones:

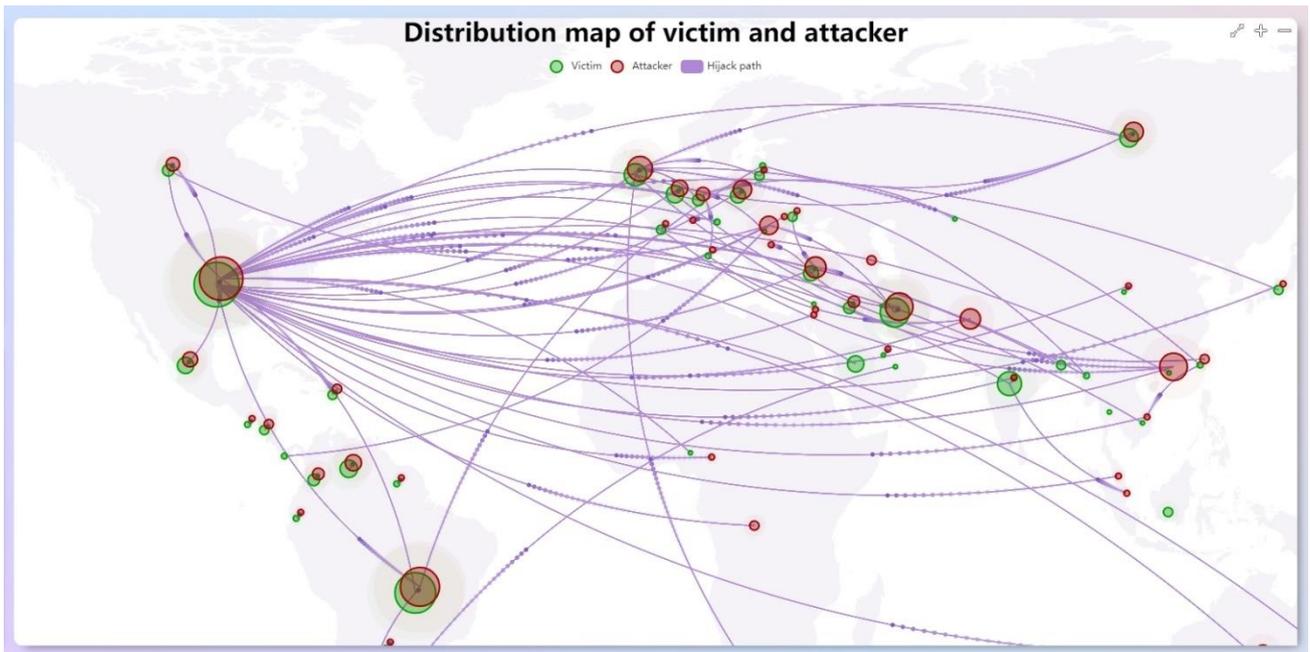
1. As shown below, the top-left zone contains two pie-charts portray economy/region wise distribution of “attackers” and “victims”. Depending on your time filter, you will be able to see: attackers’ and victims’ economy/regions. This is an “interactive chart” and you can click on the legends to show or hide statistics of any of these economies. You can click on the expand button to enlarge the section for a better view.



2. As shown below, the top-right zone contains two bar charts on Hijacked IPv4 and IPv6 Prefix based on prefix length for your selected date range. The “Y-axis” defines the hijack count whereas the “X-axis” defines the prefix-length. Hover your mouse to show the exact count of each bar. You can click on the expand button to enlarge the sections for a better view in here as well.



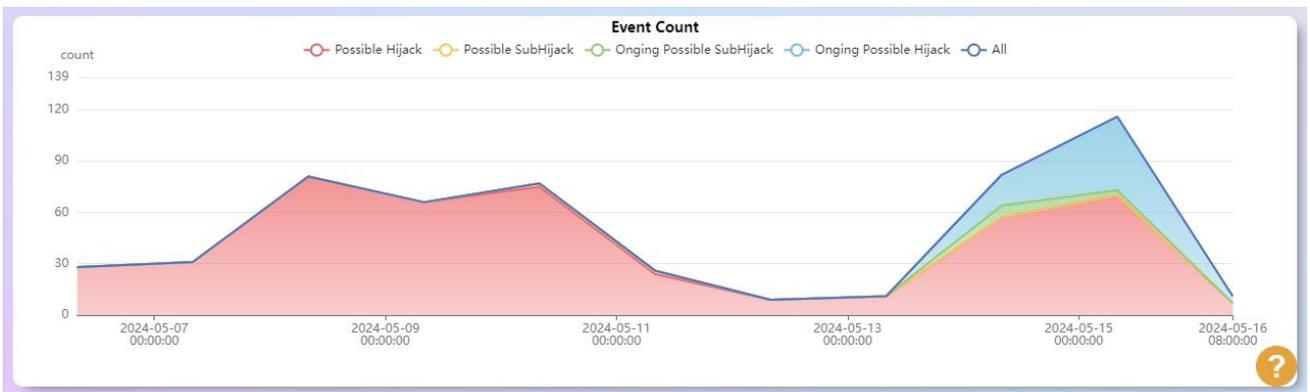
3. As shown below, the top-middle zone portrays a worldwide distribution map in the form of a “Bubble Chart” displaying the volume of economy-wise Victims and Attackers. Hover your mouse to show the “Economy” of the “Attacker” and the “Victim” as well as the “counts” of the event on the selected date range. As it is a bubble chart, “the bigger the bubble, the higher the number of attackers/victims”. The red bubbles denote the attacker and the green bubbles denote victim. The animated purple line shows the hijacker to victim direction. Clicking on the bubble, the page will be directed to the corresponding information of the hijacking event in the Anomaly section.



4. The bottom zone contains two charts:
 - a. As shown below, a segmented bar chart displays an overview of detecting information including “Impact Range”, “Data Plane Detection”, “Level”, “Status” and “Event Type”.



b. As shown below, a line graph to show the day-wise count of “Possible Hijack”, “Possible SubHijack”, “Ongoing Possible Hijack”, “Ongoing Possible SubHijack” and the “Total Hijack” events. Along the X-axis the graph shows the "Date" and Along the Y-axis it shows the “Count of the events”.



These are interactive graphs, if you hover your mouse on any of the bars or lines, the detailed information will show on the mouse. You can also click on the Legends to see the detailed information for the bar chart, and show/hide any of the hidden/displayed line-graph, for the Event Count graph.

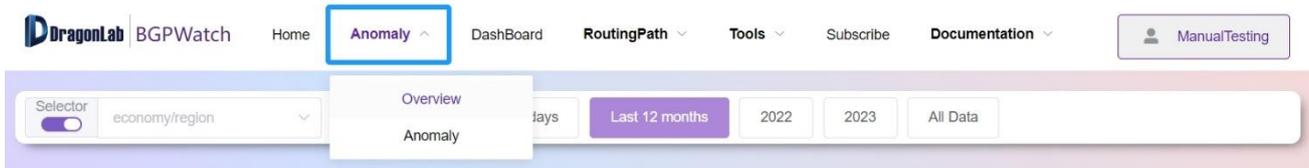
BGPWatch

User Manual

Section 3 Anomaly



Section 3. Anomaly



Introduction

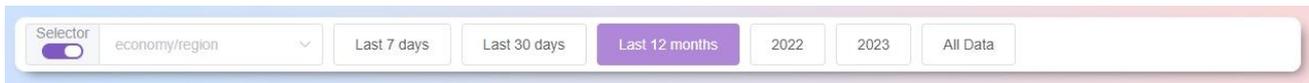
The Anomaly section contains two sub-sections:

1. Overview
2. Anomaly

Navigating the Page

1. Overview

On the top of the Overview sub-section, there lies the “filter-bar” [as displayed below] using which you can tailor the graph.



You can filter it on two (2) criteria:

- Based on economy
- Based on ASN

By default, it is based on economy. But, if you click on the “Selector” button at the beginning of the “filter-bar”, the filter will automatically switch to “ASN”. Each of the categories [Economy or ASN] can be displayed filtering them over time as follows:

1. Last 7 Days [can be displayed only on Daily basis]
2. Last 30 Days [can be displayed either on Daily or Weekly basis]
3. Last 12 Months [can be displayed on Daily, Weekly or Monthly basis]
4. Years (2022, 2023, years to come) [can be displayed on Daily, Weekly, Monthly or Yearly basis]

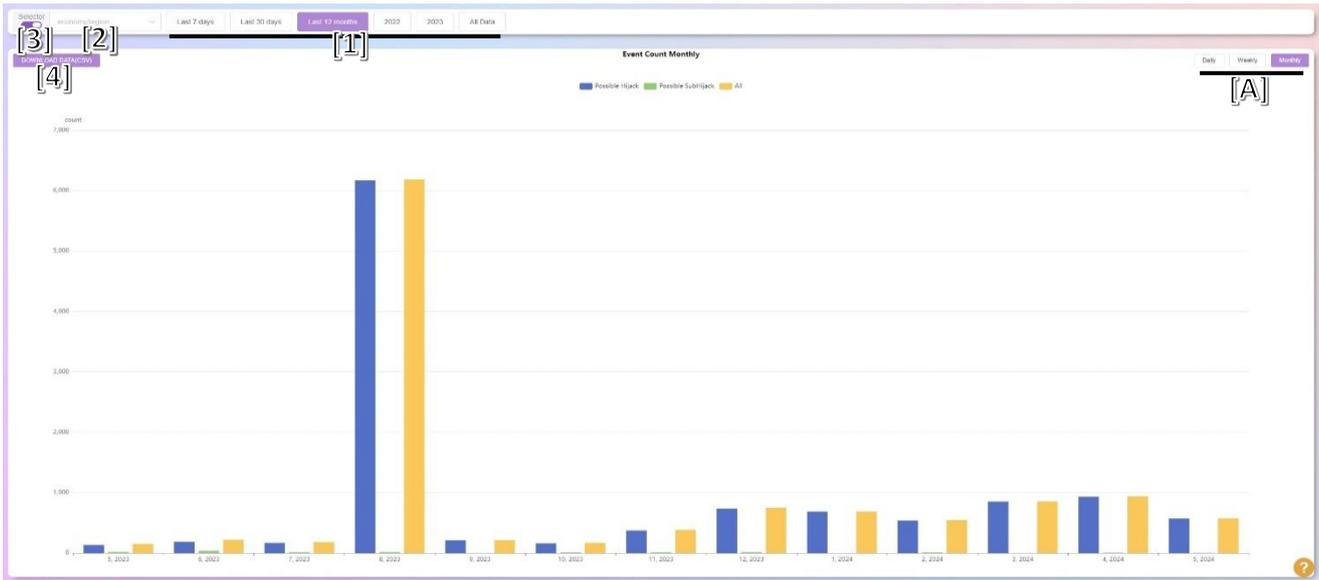
If you leave on no specific economy or AS, the global hijacking event statistics will be displayed.

The bar chart shows three events:

- Possible Hijack
- Possible SubHijack
- Total Hijack – All

Each of the above events has two players “Victims” and “Attackers” which are displayed only in the displayed chart for a specific economy.

Along the “Y-axis” the number of hijack-counts are displayed whereas along the “X-axis” the time-period is displayed.



You can swift [A] the graph displayed on Daily, Weekly, Monthly or Yearly basis.

You can click on the graph legends in order to toggle the display of the graph. You can download and save the displayed graph-statistics by clicking the “Download Data (CSV)” button [4].

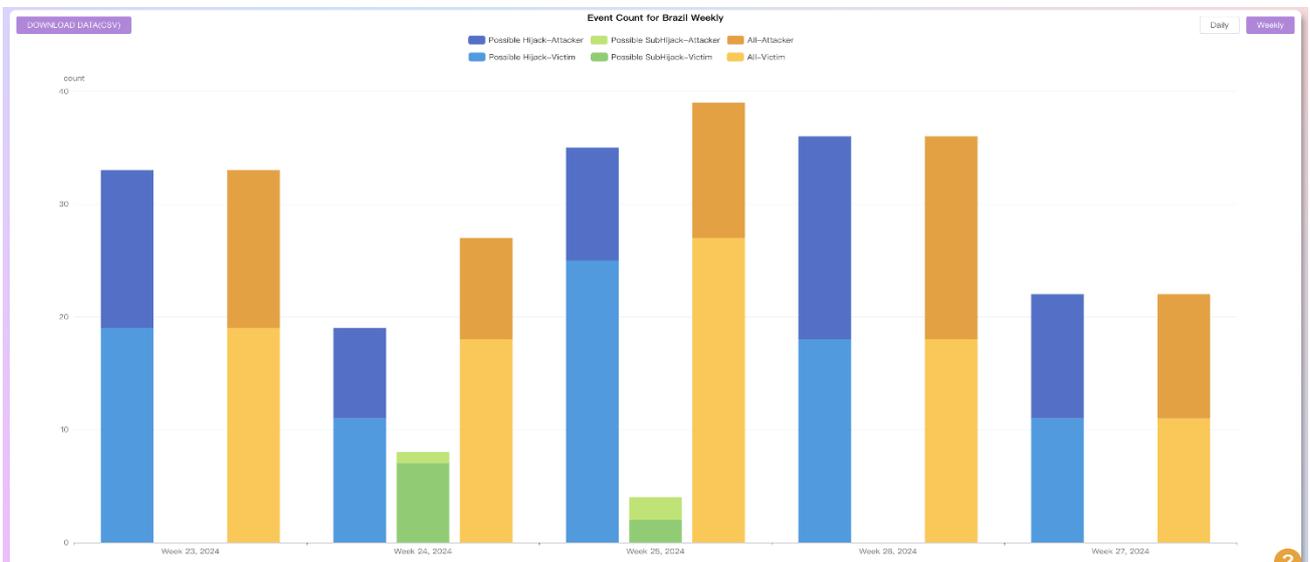
Displaying statistics for a specific economy/AS

If you select the economy or AS, you are going to get the statistics for the hijacking with it as “Victims” or “Attackers” in a “Stacked-Bar” graph.

The bar chart will show you the hijack-count of six (6) events:

- Possible Hijack-Victim
- Possible Hijack-Attacker
- Possible SubHijack-Victim
- Possible SubHijack-Attacker
- All-Victim
- All-Attacker

Hover your mouse on top of each bar if you want to know the value of a particular bar. As displayed below, clicking a bar displaying “Monthly” statistics [Left-side graph] switched it to “Weekly” statistics for that particular month [Right-side graph].



If you want to go to the Details of events for a desired time period of a bar, hover your mouse to the bar defining the statistics of the desired time period and click on “Go to Anomaly”. You will be redirected to “Anomaly” section.

2. Anomaly

In the “Anomaly” section all of BGP hijacking is reported in different categories. There are two major categories of hijacking:

- **Possible Hijack:** A “Possible Hijack” refers to a BGP hijacking attack that targets the entire block that has been allocated. By advertising the entire prefix, an attacker can redirect traffic intended for a full network within the legitimate network to a malicious destination. For example, if the legitimate network is assigned the IP address block 191.168.0.0/16, an attacker can hijack the full prefix such as 191.168.0.0/16, which represents full-network containing multiple hosts or services. By advertising a route for this prefix, the attacker can redirect traffic intended for the full network to their own network, where it can be monitored or manipulated.
- **Possible SubHijack:** A “Possible SubHijack” refers to a BGP hijacking attack that targets a more specific sub-prefix of an IP address block rather than the entire block. By advertising a more specific route announcement for a sub-prefix, an attacker can redirect traffic intended for a specific host or service within the legitimate network to a malicious destination. For example, if the legitimate network is assigned the IP address block 191.168.0.0/16, an attacker can subhijack a more specific prefix such as 191.168.1.0/24, which represents a sub-network containing a particular host or service. By advertising a route for this sub-prefix, the attacker can redirect traffic intended for the specific host or service to their own network, where it can be monitored or manipulated.

For each of the above categories there can be two events. “Ongoing” if the event is still continuing and “Terminated” if the event has already ceased. For the “Terminated” one the event will be branded either as Possible Hijack or Possible SubHijack depending on the type of Hijack. For “Ongoing” one, the event will be termed as “Ongoing Possible Hijack” or “Ongoing Possible SubHijack”.

Each event is tagged with the “level of damage” with “High”, “Middle” and “Low” level. When the number of websites contained in the hijacked prefix is greater than 5, the event is “High” level; when the number of websites contained in the hijacked prefix is greater than 1 but less than 5 or the victim AS is an IDC/CDN or a top ICP, the event is “Middle” level, otherwise the event is “Low” level.

An event is checked from data plan by submitting probing from multiple ASes if some active IP addresses exist in the specified prefix. By computing correlation coefficient of the hijacking event and the ping results, the data plane detection result can be classified into 5 types:

1. Not Done: There doesn’t exist an active IP address in the specified prefix.
2. No Result: The system try to ping some active IP addresses by get no result.
3. High Possible: The correlation coefficient ≥ 0.7 .
4. Low Possible: The correlation coefficient < 0.7 and > 0 .
5. Not Hijack: The correlation coefficient = 0.



By calculating the amount of ASes in the hijacking path compared with all amount of ASes in the replay tree, the Impact Range of each event is classified into three ranges: $\geq 50\%$, $\geq 10\%$, and $<10\%$

Each event is also tagged with “Event Info” which further describes the event, number of prefixes and the particular prefix, start time, end time and duration of the event. As mentioned, if the event is “Ongoing”, there will be no associated “End Time” and also the “Duration” field will remain blank.

Click on “Anomaly” on the main menu. The following information will come up:

[9]	[10]	[11]	[12]	[13]	[14]	[15]	[16]	[17]	[18]	[19]	[20]
#	Event Type	Level	Data Plane	Impact Range	Event Info	Prefix Num	Prefix Example	Start Time	End Time	Duration	Detail
1	Possible Hijack	Low	Not Done	9.53%	Victim: GB/AS193990(PNEHOST NET) Attacker: P/AS194036(FHEAMLINK-AS)	1	89.25.237.0/24	2024-09-07 11:03:03	2024-09-07 11:16:40	0:13:37	Detail
2	Possible Hijack	Low	Not Hijack	98%	Victim: BR/AS226120 Attacker: AD/AS37468(ANGOLA-CABLES)	1	179.124.130.0/24	2024-09-07 11:00:27	2024-09-07 11:06:40	0:6:13	Detail
3	Ongoing Possible Subhijack	Middle	No Result	20%	Victim: US/AS16509(AMAZON-02) Attacker: US/AS400366(HM-NET)	1	prefix: 185.149.88.0/23 subprefix: 185.149.88.0/24	2024-09-07 11:00:19	-	-	Detail
4	Possible Subhijack	Low	Not Hijack	86.38%	Victim: BR/AS226530 Attacker: AD/AS37468(ANGOLA-CABLES)	1	prefix: 177.105.208.0/23 subprefix: 177.105.208.0/24	2024-09-07 19:31:46	2024-09-07 11:05:18	0:33:32	Detail
5	Ongoing Possible Subhijack	Low	Not Done	86.19%	Victim: US/AS37630(CALIXTO-NET) Attacker: US/AS6451(ZAYO-6451)	1	prefix: 2620.13c.0/24 subprefix: 2620.13c.0/24	2024-09-07 08:10:15	-	-	Detail
6	Ongoing Possible Hijack	Middle	Not Hijack	6.88%	Victim: US/AS37630(CALIXTO-NET) Attacker: US/AS37630(CALIXTO-NET)	1	154.16.94.0/24	2024-09-07 03:26:23	-	-	Detail
7	Ongoing Possible Hijack	Low	Not Done	6.19%	Victim: BR/AS226438 Attacker: BR/AS226120	1	177.91.38.0/24	2024-09-07 02:52:46	-	-	Detail
8	Ongoing Possible Hijack	Low	Not Done	86.67%	Victim: SE/AS20685(MANIRAME-NET) Attacker: IR/AS115212824-AS)	1	2001.676.0/24	2024-09-06 23:25:33	-	-	Detail
9	Possible Hijack	Low	Not Done	86.67%	Victim: BR/AS226120 Attacker: AD/AS37468(ANGOLA-CABLES)	1	179.124.130.0/24	2024-09-06 21:32:01	2024-09-06 21:41:40	0:9:39	Detail
10	Ongoing Possible Hijack	Low	Not Done	10%	Victim: BR/AS193170 Attacker: AD/AS37468(ANGOLA-CABLES)	1	186.157.64.0/22	2024-09-06 20:45:00	-	-	Detail

On this page, you will see a table that organizes information about various BGP hijacking events in a structured format.

Filtering Options:

[1] Status:

- Allows users to filter events by the following status: “All”, “Ongoing”, and “Finish”.

[2] Event Type:

- Allows users to filter events by the following types: “All”, “Hijack” and “SubHijack”.

[3] Harm Level:

- Allows users to view events based on their severity level, which can be “Low”, “Middle”, or “High”.

[4] Data Plane:

- Allows users to filter the data plane results from the following results: “All”, “Not Done”, “No Result”, “Not Hijack”, “High Possible” and “Low Possible”.

[5] Impact Range:

- Allows users to filter the impact range from the following ranges: “All”, “<10%”, “>= 10%”, and “>= 50%”.

[6] Time Zone:

- Users can select the time zone for the timestamps displayed on the page, such as “GMT+8”.

[7] Time Period (By Start Time):

- Users can specify a time period to search events with the start time between the time period.

[8] Search Event:

- An advanced search feature that enables users to enter specific keywords related to hijacking events. This can include terms such as AS numbers, IP prefixes, event types, or geographical locations.

[9]



- Clicking this button, users can download the complete statistics displayed in the table as a .csv file for offline analysis or further processing.

[10] Event Type:

- The type of hijacking event, such as “Ongoing Possible Hijack”.

[11] Level:

- The severity level of the event.

[12] Data Plane:

- The data plane detecting result.

[13] Impact Range:

- The percentage of the impact range.

[14] Event Info:

- The victim and attack ‘s AS numbers and details of the event.

[15] Prefix Num:

- The number of prefixes involved in the hijack.

[16] Prefix Example:

- An example of the prefix affected, such as “204.19.32.0/24”.

[17] Start Time:

- The timestamp when the hijacking event began.

[18] End Time:

- The timestamp when the hijacking event ended (not applicable for ongoing events).

[19] Duration:

- The length of time the hijacking event lasted (displayed only for events that have ended).

[20] Detail:

- An option to view more detailed information about the event.

Anomaly Event Detail

If you want to see the hijacking event details, click on the detail button which is placed at the end of each record.

Harm Level

Middle Level

Range of Impact

88.42%

Data Plane Detection

Low Possible

168.194.252.0/24-HIJACK1722397752 Possible Hijack Events

Victim AS: 265415	Hijacker AS: 267593	Start Time (UTC): 2024-07-31 03:49:12
Victim Economy: BR (Brazil)	Hijacker Economy: BR (Brazil)	End Time (UTC): 2024-07-31 03:59:06
Victim AS Name: UNSPECIFIED	Hijacker AS Name: no data	During Time: 0:9:54

Reason:

(267593, 168.194.252.0/24) doesn't align in ROA

(265415, 168.194.252.0/24) doesn't align in ROA

(267593, 168.194.252.0/24) doesn't align in WHOIS

(265415, 168.194.252.0/24) aligns in WHOIS

Prefix Info: [168.194.252.0/24](#)

Website: [168.194.252.0/24](#)

qweb.com.br

wave.net.br

waveplus.com.br

This page provides detailed information about a specific hijacking event detected within the BGP routing system, which are:

1. Event Overview:

- **Harm Level:** Indicates the severity of the hijack.
- **Range of Impact:** Indicates the percentage of the impact range.
- **Data Plane Detection:** Indicates the result of data plane detection.

2. Involved Autonomous Systems (AS) Information:

- **Victim AS Number:** The AS number that is being affected by the hijack.
- **Victim Economy:** The economy code for the victim AS.
- **Victim AS Name:** The name of the victim AS number.
- **Hijacker AS Number:** The AS number suspected of performing the hijack.
- **Hijacker Economy:** The economy code for the hijacker AS.
- **Hijacker AS Name:** The name of the hijacker AS number.

3. Duration of the Hijack:

- **Start Time (UTC):** The date and time when the hijack event began.
- **End Time (UTC):** The date and time when the hijack event ended.
- **During Time:** The total duration of the hijack event.

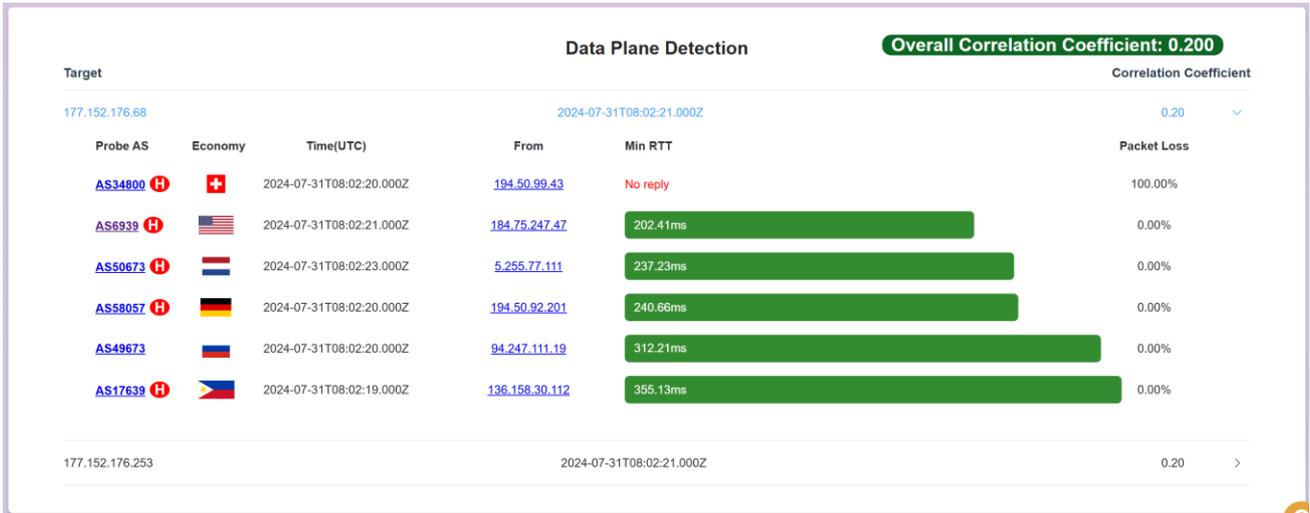
4. Additional Information

- **Reason:** Here lists reasons why the event is classified as a possible hijack. Typically, it will show the reasons regarding Route Origin Authorizations (ROA) and WHOIS information.
- **Prefix Info:** The IP address range involved in the hijack.

- **Website:** A link to the website associated with the hijacked prefix is provided for further investigation.

5. Data Plane Detection

This section is designed to display the outcomes of data plane detections of the hijacking events. This information is vital for understanding the actual reachability and response times of specific IP addresses.

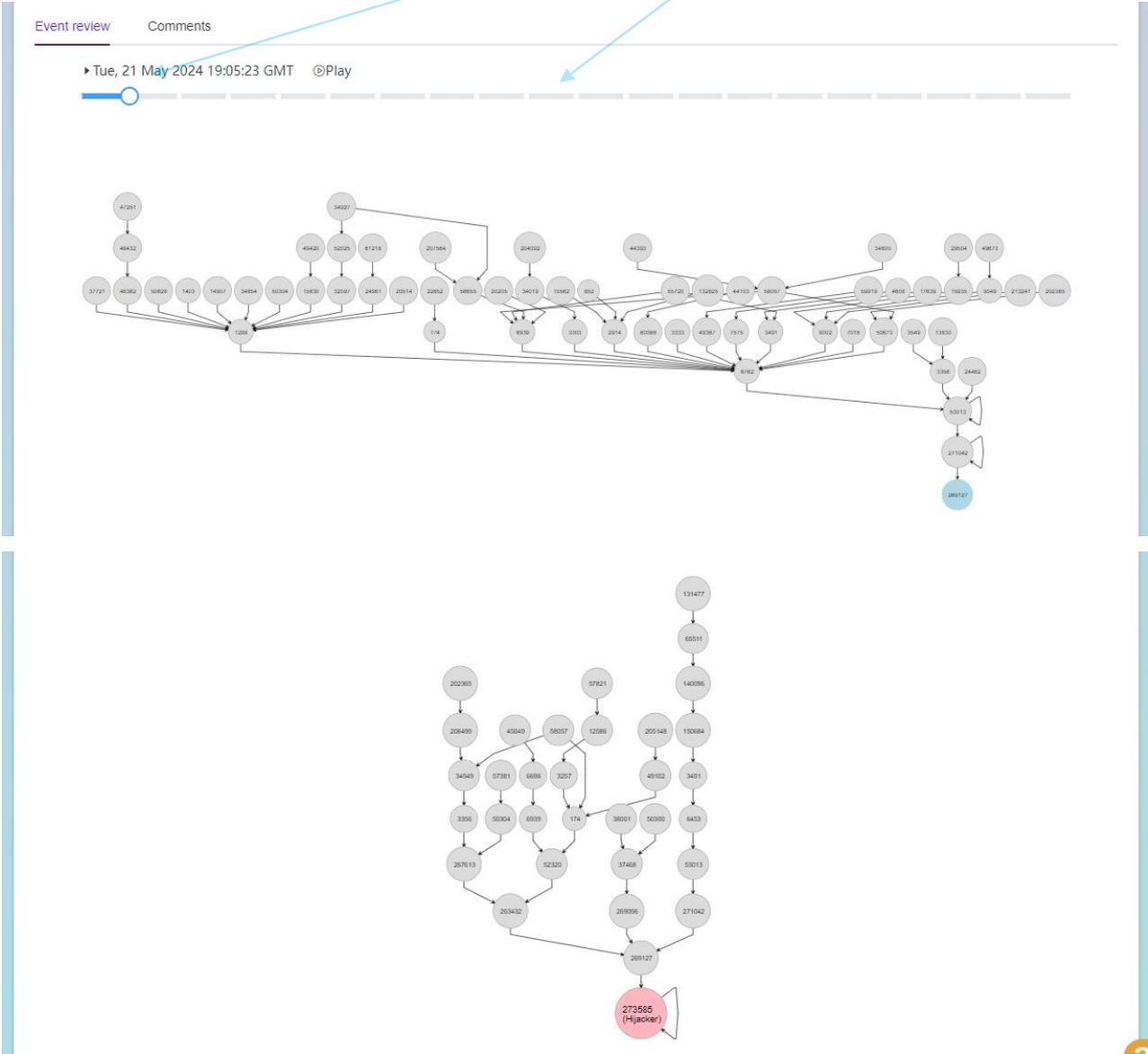


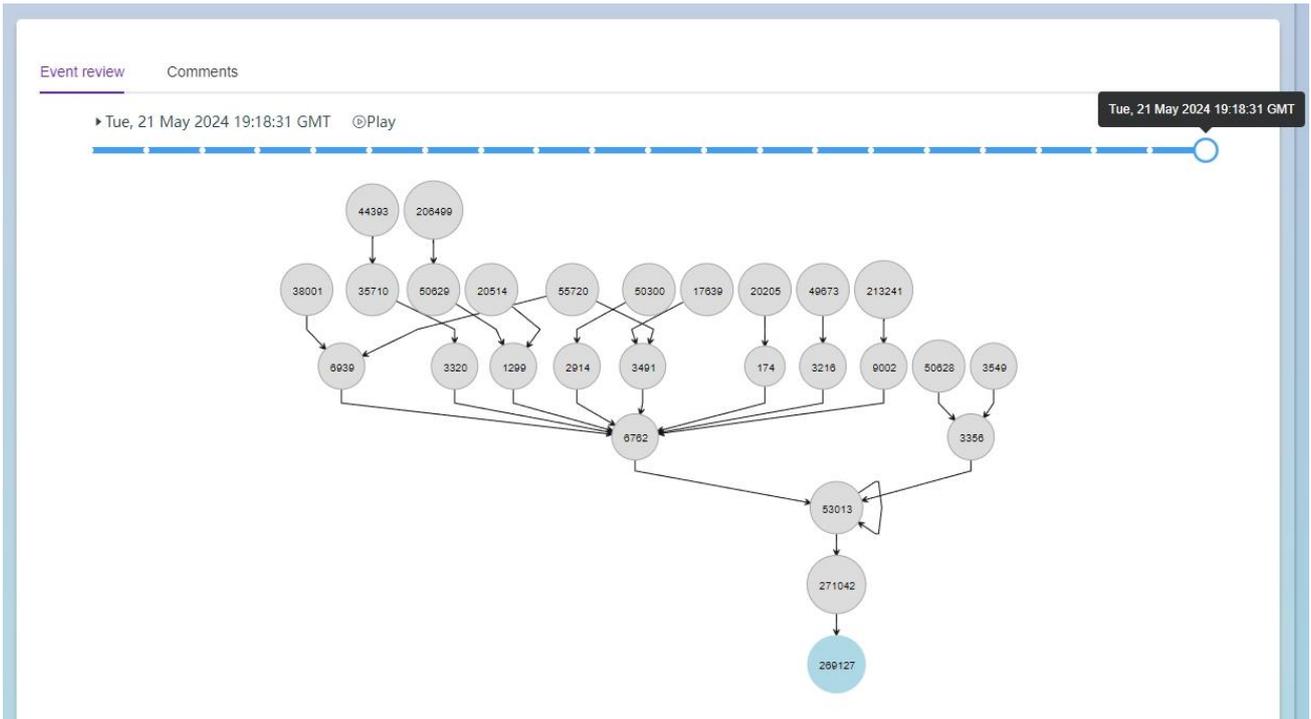
Key Information Displayed on the Page:

- 1) Target IP Address and Detected Date and Time:**
 - Lists the IP addresses that were probed along with any associated domain names for reference, and the date and time when the detections were conducted.
- 2) Probe AS, Possible Hijacking Associated Economies, Date and Time, and IP:**
 - Identifies the Autonomous System number and IP address of the probe that conducted the ping test.
- 3) Min RTT:**
 - Provides the results of Min RTT when the command was replied, otherwise it presents “No reply”.
- 4) Packet Loss:**
 - Shows the percentage of packet loss.
- 5) Overall Correlation Coefficient:**
 - Displays correlation coefficient of the hijacking event and the ping results.

6. Event Review

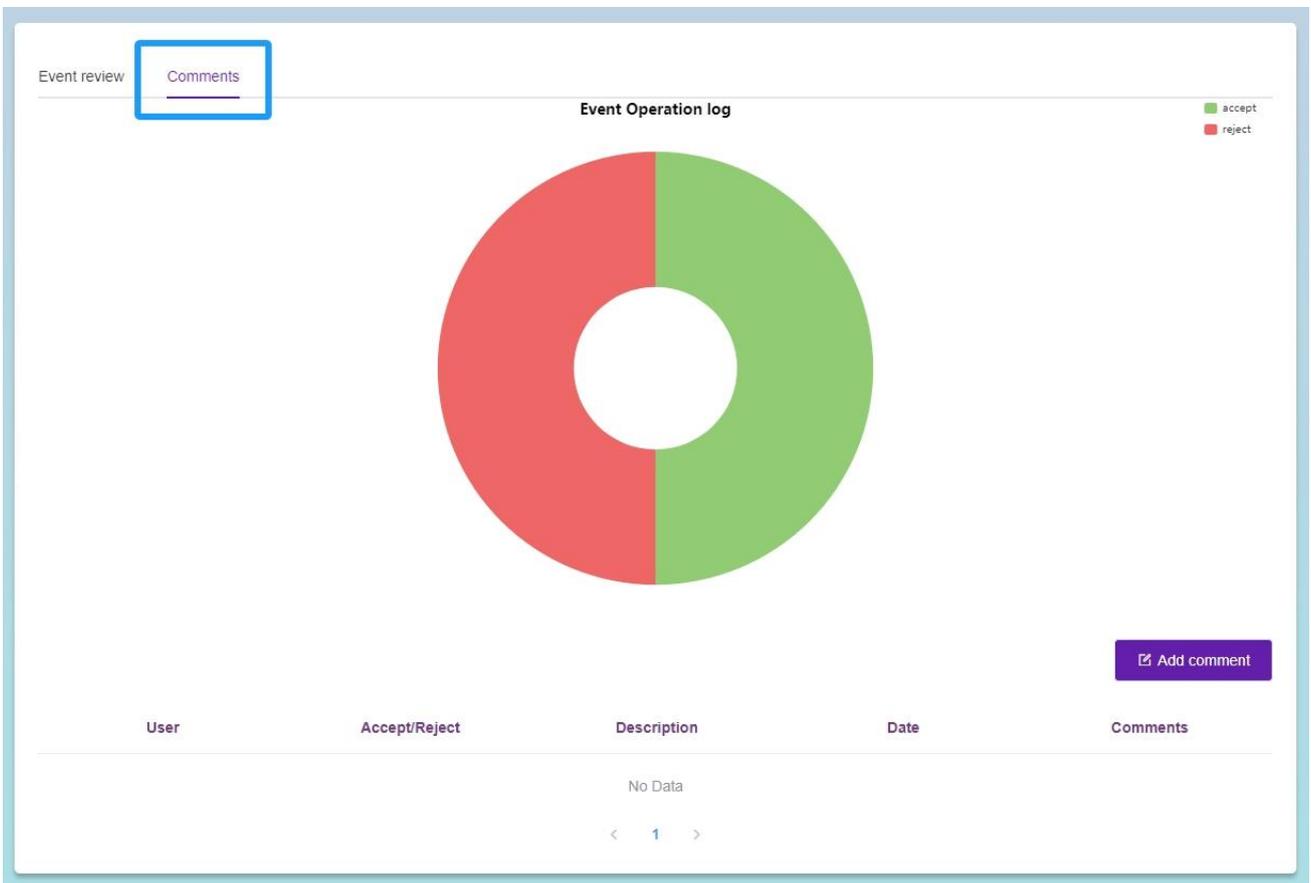
In this section, you will find information about the reverse routing path of the victim and hijacker of the hijacking event in a time stamped manner. You can use the **[Slider]** to move into different timestamps to get this information. You can also click on the **Play** button to automatically slide from one time to another for the full event. The following series of screenshots illustrate the progression and resolution of a BGP hijacking event involving a victim AS:



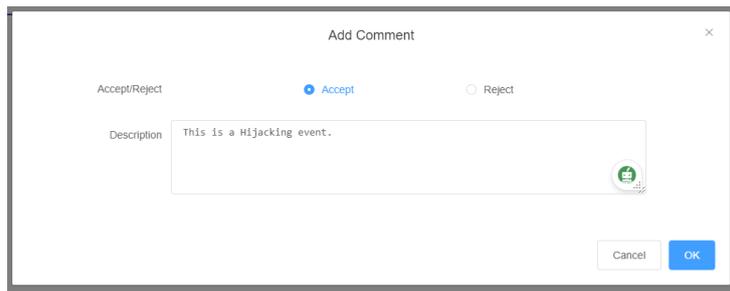


Comments:

At the right side of the Event review section, you will find the Comments section. You can check whether the hijacking event is intentional or by mistake from the site users comments and voting. Here, users can see the event acceptance and reject ratio in a pie chart.



The users can add comments and place accept/reject votes by clicking on the “Add comment” button.



The screenshot shows a modal dialog box titled "Add Comment". At the top, there are two radio buttons for voting: "Accept" (which is selected) and "Reject". Below the radio buttons is a text input field labeled "Description" containing the text "This is a Hijacking event.". At the bottom right of the dialog, there are two buttons: "Cancel" and "OK".

After voting the section will show the information placed by the user.

BGPWatch

User Manual

Section 4 Dashboard



Section 4. Dashboard



Introduction

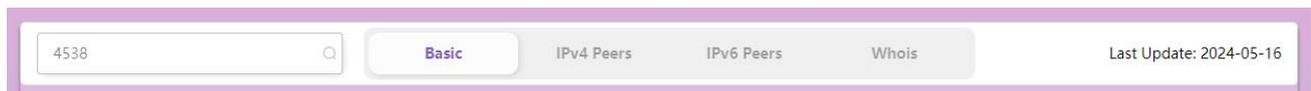
The “Dashboard” is a comprehensive tool that provides detailed information on an Autonomous System Number (ASN). It includes:

- Basic information of the ASN.
- Details of IPv4 and IPv6 prefixes originating from the ASN.
- Information about other Autonomous Systems the particular AS is peering with.

The dashboard also displays the number of prefixes being exchanged in these peering relationships.

Navigating the Page

If you click on the “Dashboard” button you will come up with a page having the following “Filter-bar” at the top:



You can key-in whatever ASN or AS Name or Organization name you want the information about.

For an ASN, the result contains four tabs.

1. Basic
2. IPv4 Peers
3. IPv6 Peers
4. WHOIS

1. Basic

The basic information is displayed under the following sections/fields:

1. **AS Number**
2. **AS Name**
3. **Economy/Region**
4. **AS Organization**
5. **IPv4 Prefix:**
 - Length distribution of IPv4 prefixes originating from the ASN is shown in a histogram, with the three max prefix length number listed.
6. **IPv6 Prefix:**
 - Length distribution of IPv6 prefixes originating from the ASN is shown in a histogram, with the three max prefix length number listed.
7. **IPv4 Prefix Count:**

- Numbers of IPv4 prefixes originating from the ASN over the past seven days shown in a line graph, along with the differences between the last day and the day before it.

8. IPv6 Prefix Count:

- Numbers of IPv6 prefixes originating from the ASN over the past seven days shown in a line graph, along with the differences between the last day and the day before it.

9. IPv4 Address Size (/24):

- Numbers of IPv4 addresses originating from the ASN (measured in units of /24) over the past seven days shown in a line graph, along with the differences between the last day and the day before it.

10. IPv6 Address Size (/48):

- Numbers of IPv6 addresses originating from the ASN (measured in units of /48) over the past seven days shown in a line graph, along with the differences between the last day and the day before it.

11. IPv4 Bogon:

- Count of IPv4 bogon routes.

12. IPv6 Bogon:

- Count of IPv6 bogon routes.

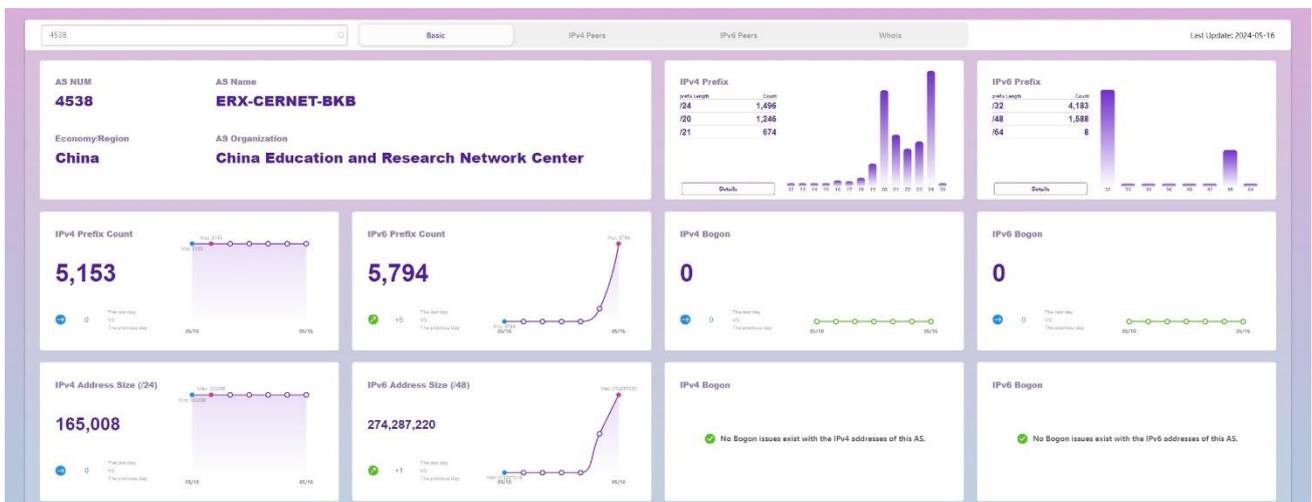
13. IPv4 Bogon Statement:

- Indicating if there are bogon issues with IPv4 addresses.

14. IPv6 Bogon Statement:

- Indicating if there are bogon issues with IPv6 addresses.

All the graphs here are interactive. As you hover through the bars on the graphs, the actual count will be displayed.

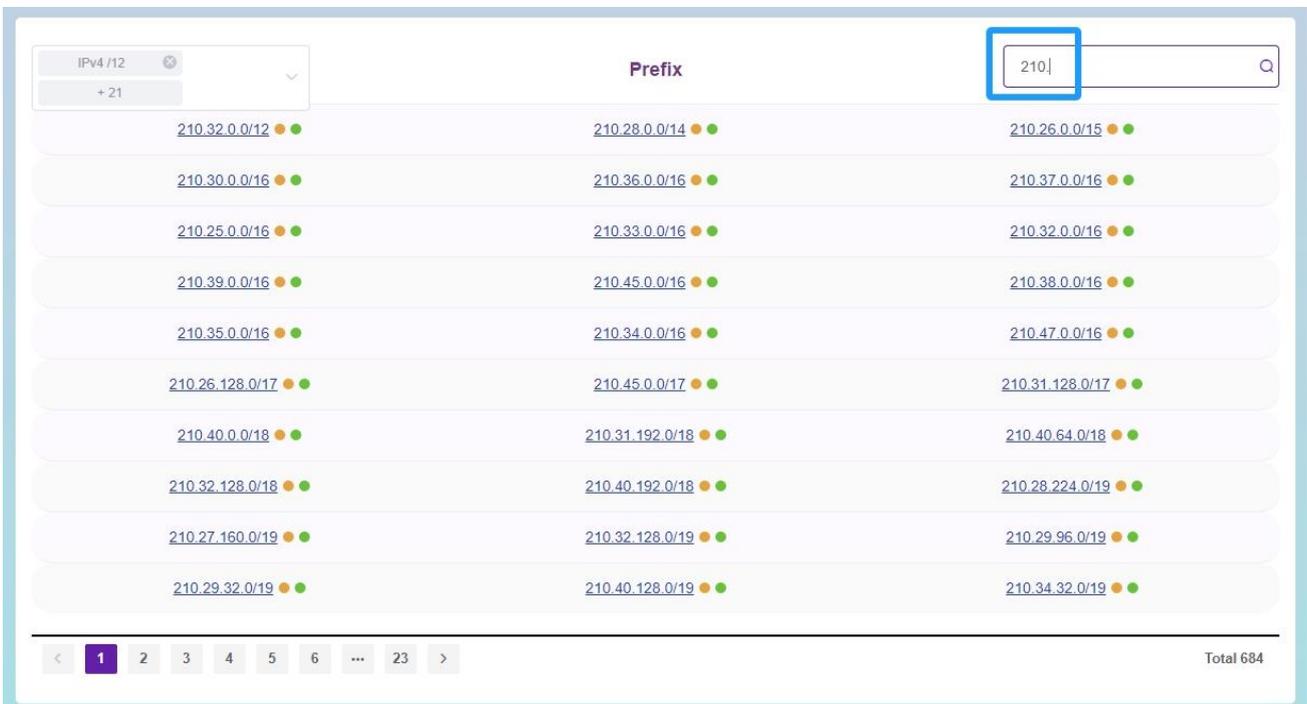


At the bottom of the page, you will find a table displaying IP prefix lists that have originated from the selected AS.

The toggle button on the top-left corner can be used to select “IPv4”, “IPv6”, or certain length prefixes.



As shown below, the search box on the top-right corner allows users to look up specific super prefixes, sub prefixes, or prefixes within the table.



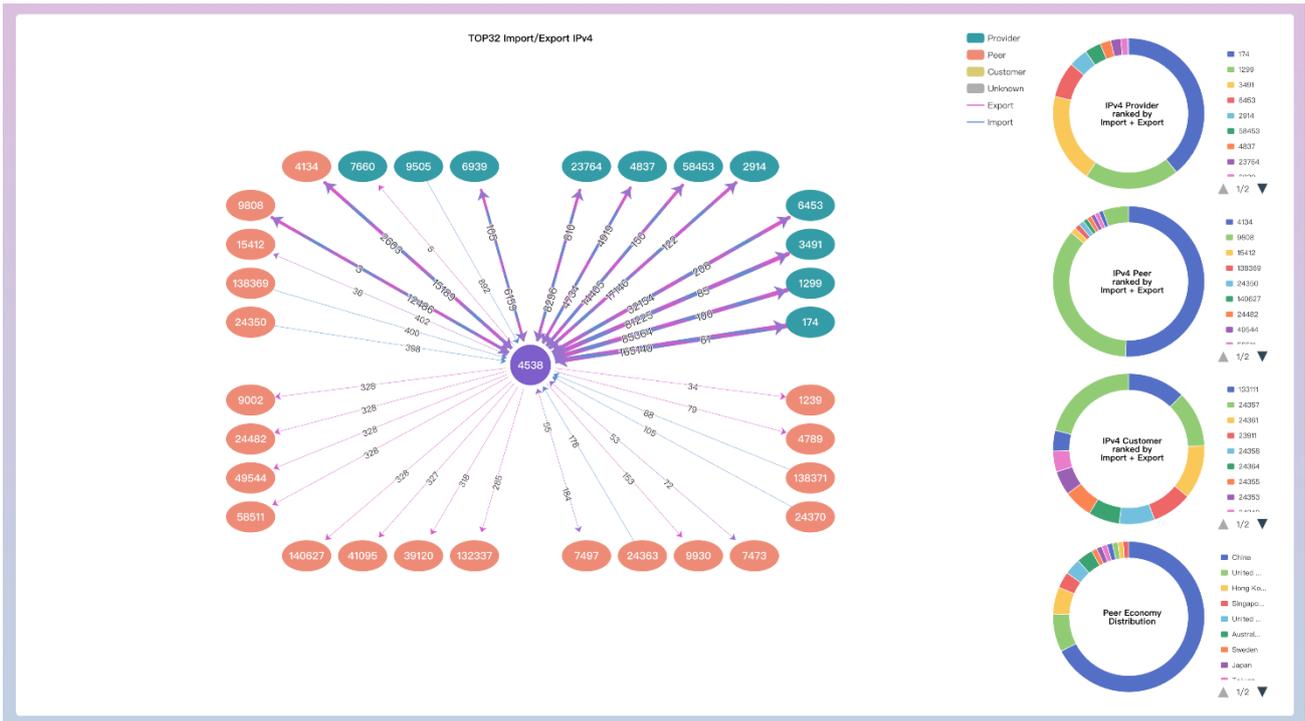
The orange and green dots next to the prefixes indicate the ROA and WHOIS information found and match or not.

The prefixes are hyperlinked. If you click on them, you will be redirected to the reverse routing path topology page of that prefix.

The total number on the bottom-right corner indicates the total number of the prefixes.

2. IPv4 Peers

If you select the “IPv4 Peers” tab, you will find a connectivity diagram of IPv4 BGP neighbors of selected AS (shown as below).



On the right side of this diagram, you will find four pie charts of the top ten peers ranked by sum of advertised and received prefixes [import plus export].

1. **Based on IPv4 Providers**
2. **Based on IPv4 Peers**
3. **Based on IPv4 Customers**
4. **Based on Peer Economy**

Along the line connecting the peers, the number of prefixes that are being received and advertised respectively from and to the providers, peers, and customers are displayed. The thicker the lines, the more the numbers of prefixes that are being received and advertised. If the user hovers the mouse on a specific line in the graph, the details of numbers of prefixes that are being received and advertised will show.

In this picture, you can see that AS4538 has many neighbors including peers and providers. If you hover your mouse on top of any link, you will be able to find the number of prefixes that the AS4538 is importing from or exporting to.

Below that, you will find a table showing all of its IPv4 neighbors.

The key features can be filtered from the four neighbor types on the top-left corner:

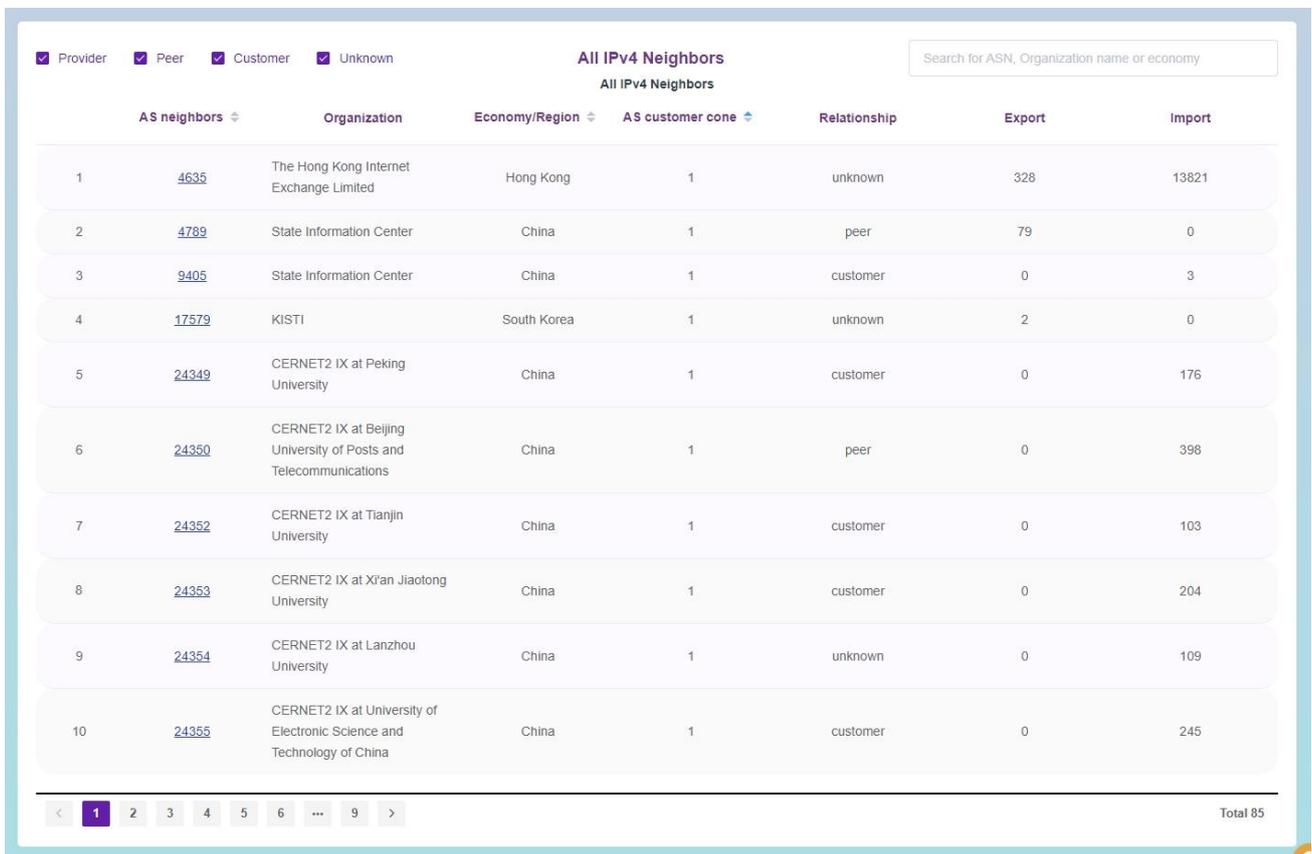
1. **Provider**
2. **Peer**
3. **Customer**
4. **Unkown**

The table shows detailed information including:

1. **ASN**

2. **Organization**
3. **Economy/Region**
4. **AS Customer Cone:**
 - A metric indicating the customer cone of an AS, which can be useful for understanding the downstream networks connected to a particular AS.
5. **Relationship:**
 - The neighbors' types.
6. **Export:**
 - The number of IPv4 prefixes announced by an AS to its neighbors.
7. **Import:**
 - The number of IPv4 prefixes received from its neighbors.

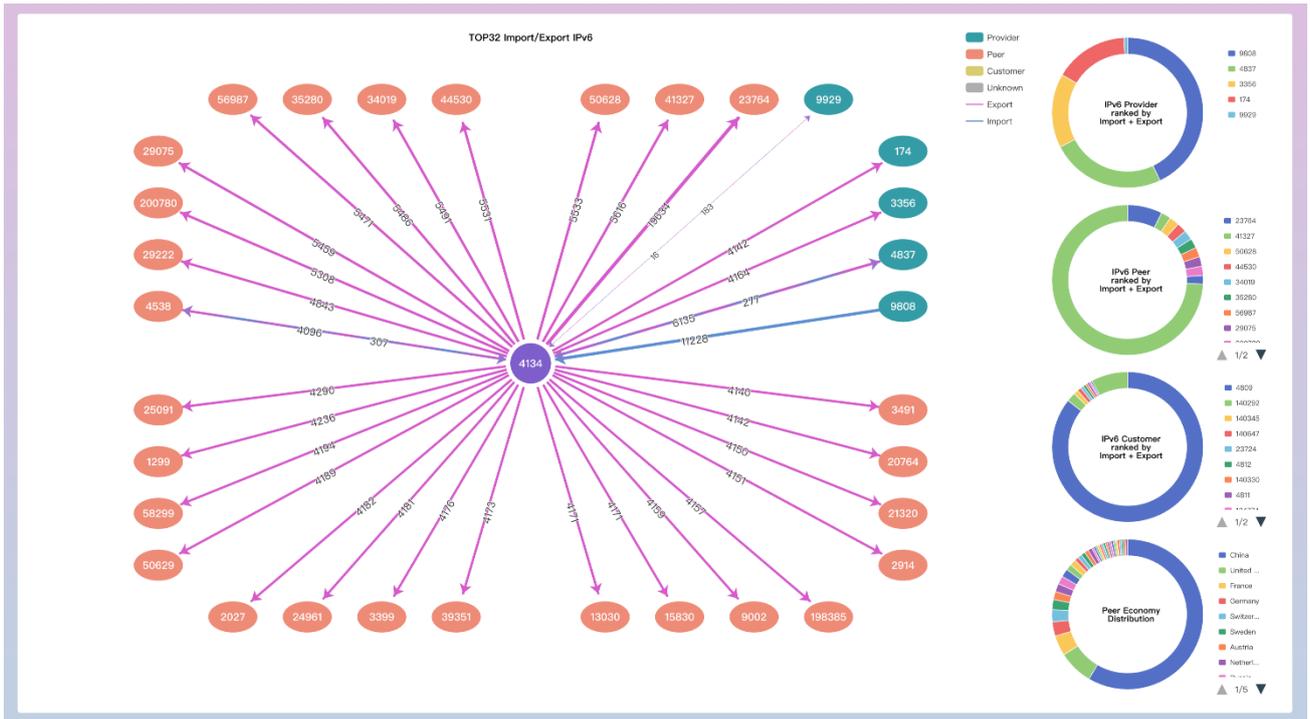
These are hyperlinked and if you click on any of the ASNs, you will be redirected to the dashboard section of that ASN.



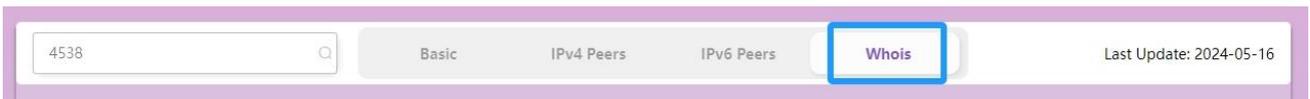
	AS neighbors	Organization	Economy/Region	AS customer cone	Relationship	Export	Import
1	4635	The Hong Kong Internet Exchange Limited	Hong Kong	1	unknown	328	13821
2	4789	State Information Center	China	1	peer	79	0
3	9405	State Information Center	China	1	customer	0	3
4	17579	KISTI	South Korea	1	unknown	2	0
5	24349	CERNET2 IX at Peking University	China	1	customer	0	176
6	24350	CERNET2 IX at Beijing University of Posts and Telecommunications	China	1	peer	0	398
7	24352	CERNET2 IX at Tianjin University	China	1	customer	0	103
8	24353	CERNET2 IX at Xi'an Jiaotong University	China	1	customer	0	204
9	24354	CERNET2 IX at Lanzhou University	China	1	unknown	0	109
10	24355	CERNET2 IX at University of Electronic Science and Technology of China	China	1	customer	0	245

3. IPv6 Peers

In the IPv6 Peers tab, you will find the same information as you are getting from the IPv4 tab, except that the information is based on IPv6 BGP neighbors.



4. WHOIS



In the WHOIS tab, the user can check the registration information of AS numbers. Those information are collected from Regional Internet Registry (RIR). Depending on the registries that AS registered with, here is showing the corresponding information.

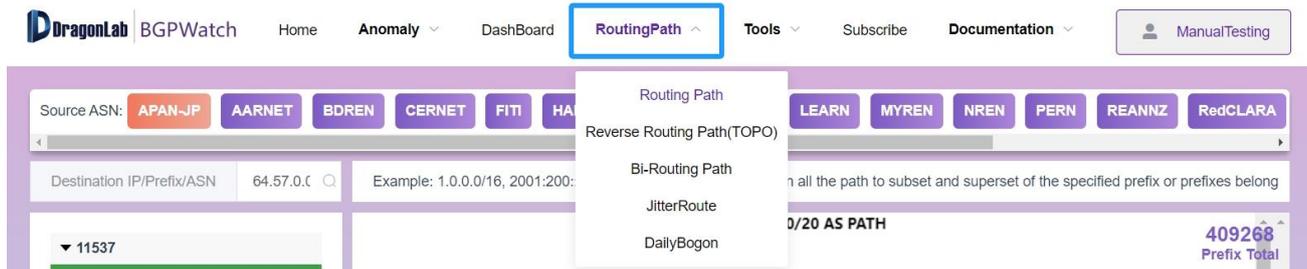
BGPWatch

User Manual

Section 5 Routing Path



Section 5. Routing Path



Introduction

In BGP, the forward routing path is used to determine the best route for a data packet to take from its source to its destination. The router evaluates various attributes of the different paths, such as the length of the path and the origin of the prefix, to determine the best route. The best route is then added to the BGP routing table and used to forward data packets.

The reverse path shows how a data packet is routed from an AS to a prefix of your AS.

It includes the following 5 options:

1. **Routing Path:** provides you the forward routing path to a given prefix from the selected NREN.
2. **Reverse Routing Path (TOPO):** provides you the routing path from other ASes to a particular prefix in topology. Usually operators are interested how traffic is routed to their network.
3. **Bi-Routing Path:** provides you both the forward path and the reverse path between two selected prefixes.
4. **Jitter Route:** identifies the top prefixes and peers that exhibit the most jitters in the network
5. **Daily Bogon:** shows the overview of bogon routes.

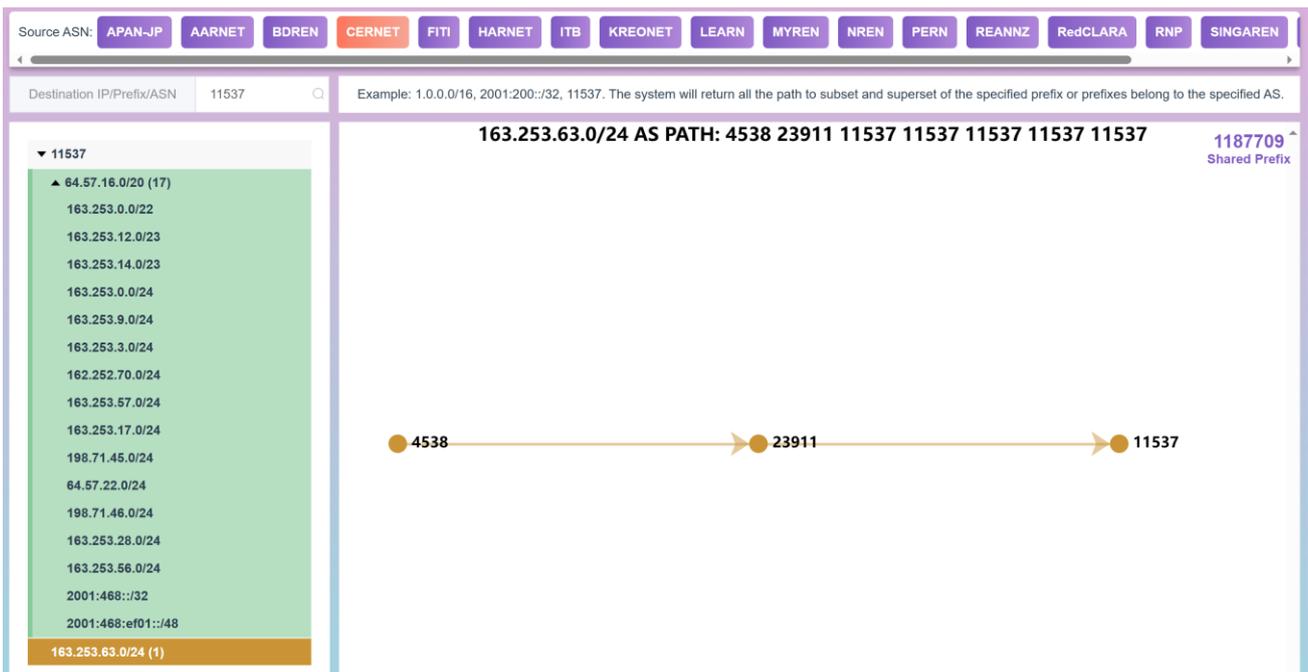
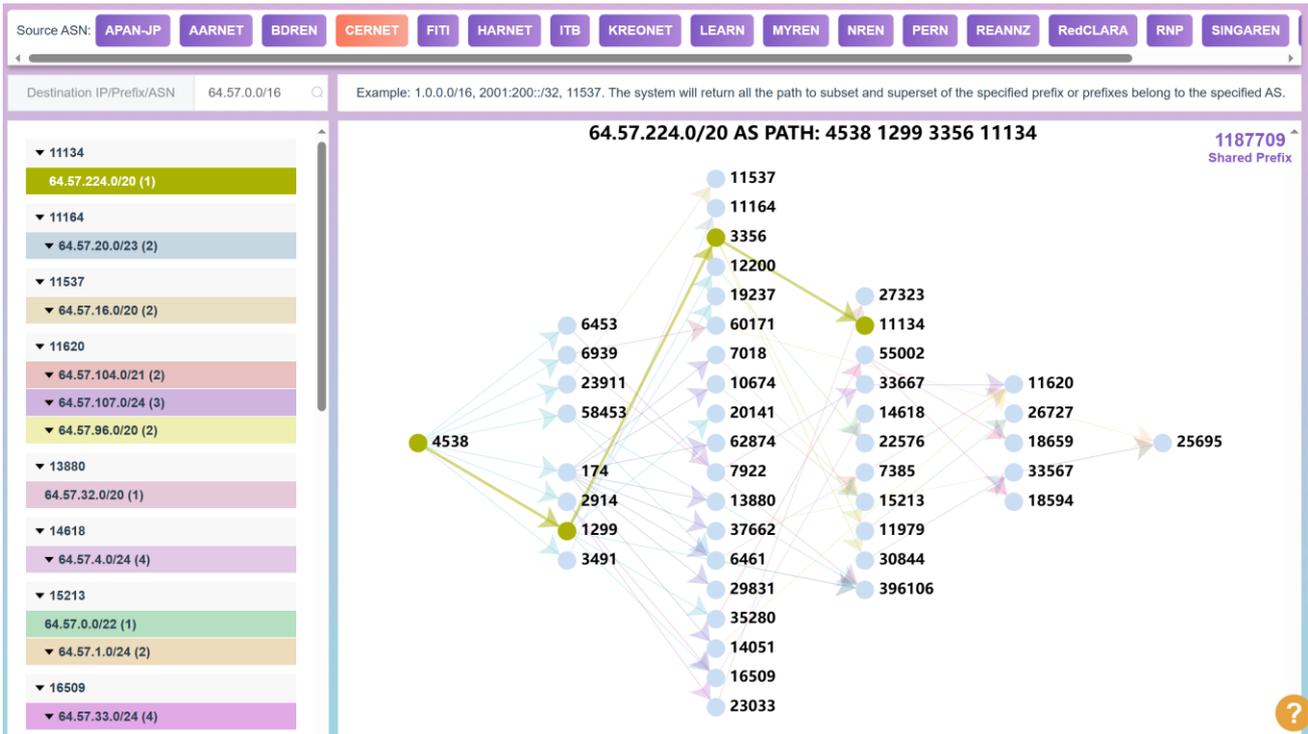
Navigating the page

1. Routing Path

First you can select one of NRENs from the top as the source. Then input an IP prefix or ASN as the destination. The system will return paths from the specified NREN to the destination. If the destination is a prefix, the platform will return all the path to subset and superset of the destination prefix from the specified NREN. If the destination is an ASN, the platform will return all the path to all the prefixes belong to the destination AS from the specified NREN.

As shown in the below screenshot, on the list of prefixes in the left, some networks sharing the same path are grouped together having the same color. If you click on any of the same-colored block of prefixes, the forward path for that group will be highlighted.

The “Shared Prefix” at the top-right corner shows the total number of prefixes the source ASN shares with the platform.



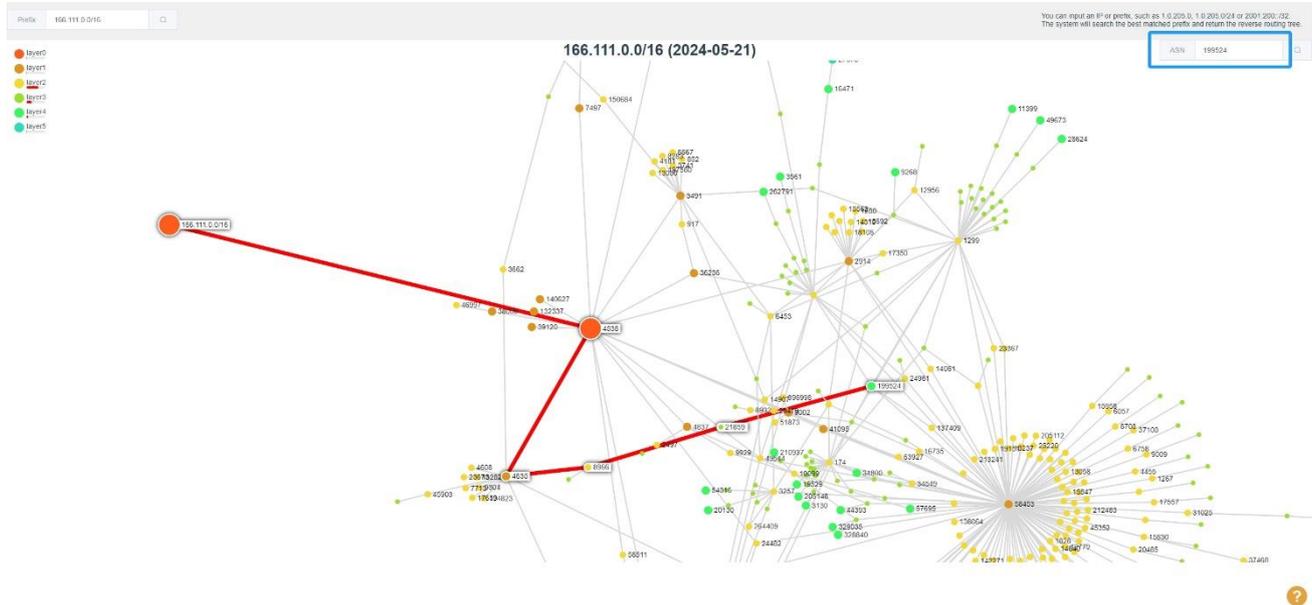
2. Reverse Routing Path (TOPO)

“Reverse Routing Path (TOPO)” provides the user with the routing path from other ASes to a particular prefix in topology. It takes an “IP prefix” as an input and the system will search the best matched prefix and return the reverse routing topology.

The legends on the top-left corner shows the layer of the reverse path with a color code. For example, the red color nodes are layer 0, which is your searched prefix or IP. You can click on the legends to remove or add the layers to your routing tree.

Moreover, if you want to see the routing path of the prefix from a specific AS, you can simply click on that AS. The corresponding path will be highlighted.

The same can be obtained by putting an ASN in the “Search box” at the top-right corner.



3. Bi-directional Routing Path

In the “Bi-Routing Path” submenu, you can find forward and reverse routing path between a source and destination IP address or prefix.

This is very much similar to the ‘Routing Path’ except that the routing path is bi-directional here.

There is a search-box at the top where you can put under “Left IP” the source prefix and under the “Right IP” the destination prefix. It will give you both the forwarding and the reverse path as displayed below.

Due to the huge amount of data, now the system only selects a portion of the full data from all the routing information sharing platform. If the system return “no data found”, it doesn’t mean there isn’t a routing path, it maybe just because the system hasn’t processed the corresponding data.

Left IP
203.185.101.0/24

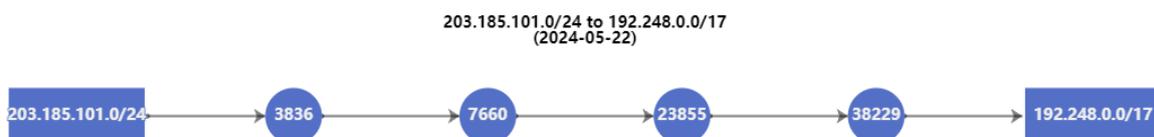
Do search

Right IP
192.248.0.0/17

Example: 2a0f:9340:10::/48 <----> 2001:7f8:e7::/48

Example: 2.22.238.0/23 <----> 185.193.84.0/22

You may find that the forward and reverse routing paths are actually different.



192.248.0.0/17 to 203.185.101.0/24
(2024-05-22)



4. Jitter Route

The Jitter Route section is designed to monitor the routing table change of a specific ASN and identify the prefixes and peers that exhibit the most update. This function can help network operators monitor their AS and find peers and prefixes with frequent updates and find potential problem. Jitter, in this context, refers to announcement and withdraw updates in routing paths.

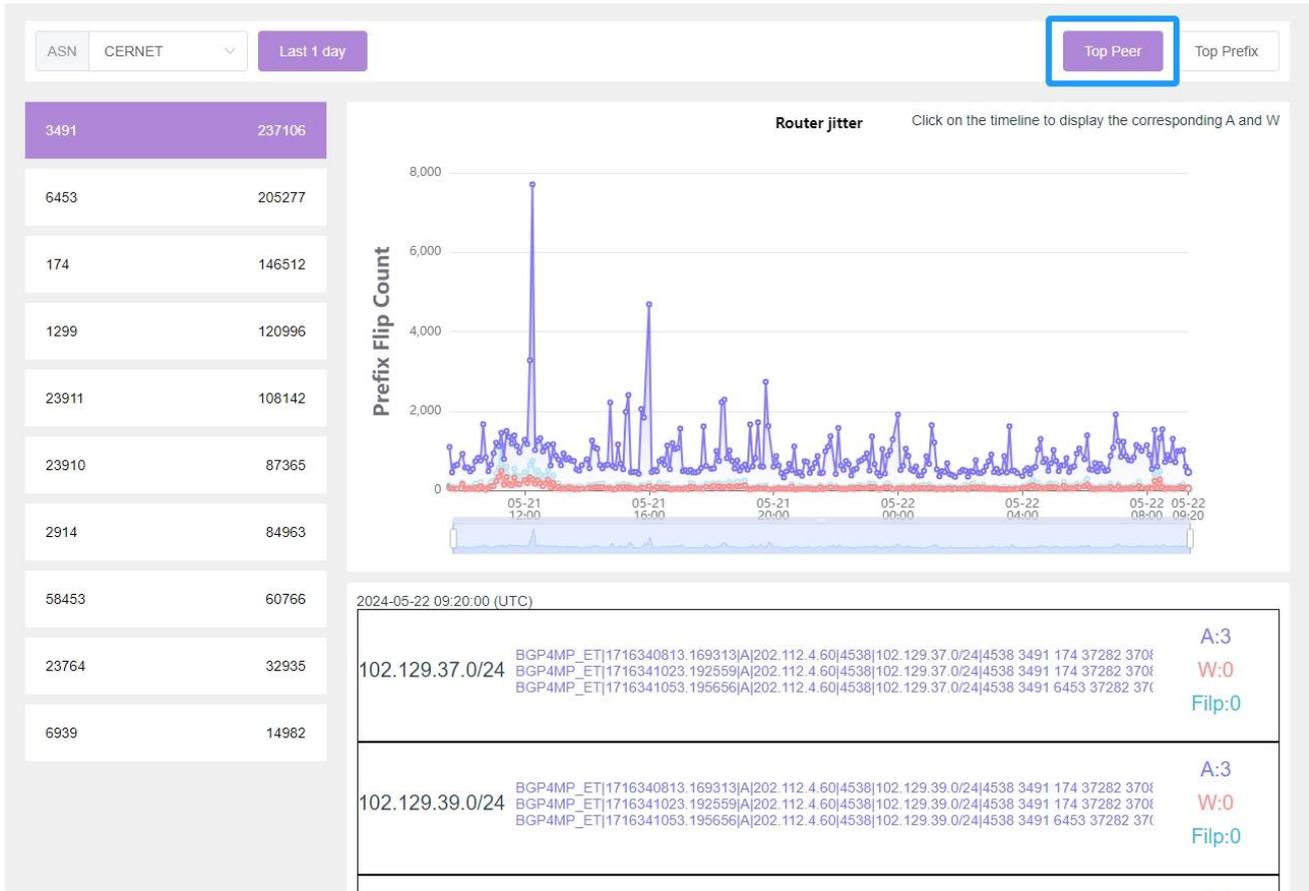
First select ASN from the left top corner, then select to show TOP peers or Top Prefix with frequent updates by clicking one button from top-right corner.

For Top Prefix, the topN prefixes will be listed on the left.

On the right, A graph of prefix flip count on the Y-axis and timeline on the X-axis is shown to help users correlate BGP updates with changes in routing paths over time. Each BGP update is detailed, showing the type of update (A for Announcement, W for Withdrawal), the prefix involved, and the ASN path.



For Top Peers, the topN peers will be listed on the left. Also, a graph of prefix flip count associated with the AS on the Y-axis and timeline on the X-axis is shown on the right.



5. Daily Bogon

Bogons are IP addresses that should not be present in the global routing table due to being reserved, private, or unused. Monitoring these routes is essential for maintaining network security and ensuring proper routing policy adherence. This section provides an overview of bogon routes, including:

- **IPv4 and IPv6 Bogon Counts:**
 - Displays the total count of IPv4 and IPv6 bogon routes, providing a quick overview of the number of non-routable addresses being tracked.
- **AS Number, Economy, Organization:**
 - Shows the relevant information and ranked by its count.
- **Prefix Length:**
 - Offers a breakdown of bogon counts based on prefix length, allowing users to understand the distribution of bogon routes across different address blocks.



Users can search for specific prefix, ASN, ASN name, organization name, economy, or continent to filter the desired information. IPv4 or IPv6 ranges also can be filtered.

Prefix / ASN / ASN Name / Org Name Economy / Continent IPv4 IPv6

Users can click the TopN bar to see the detailed information listed in the table, as shown below.

AS TopN

1 3786 1286

2 13536

3 3269

4 5713

5 56655

AS 3786 1,286

2024-06-05

Economy TopN

1 1286

2 816

3 131

4 66

5 50

South Ko...
United St...
Italy
South Afr...
Norway

2024-06-05

Org TopN

1 1286

2 769

3 129

4 64

5 50

LG DACO...
First Lig...
Telecom I...
Telkom S...
TerraHos...

2024-06-05

15.8

7/128: 7

Economy / Continent IPv4 IPv6

	Prefix	ASN	ASN Name	Org Name	Economy	Continent
1	172.30.108.111/32	3786	LGDACOM	LG DACOM Corporation	South Korea(KR)	Asia
2	172.21.42.43/32	3786	LGDACOM	LG DACOM Corporation	South Korea(KR)	Asia
3	172.30.12.114/32	3786	LGDACOM	LG DACOM Corporation	South Korea(KR)	Asia
4	172.30.42.143/32	3786	LGDACOM	LG DACOM Corporation	South Korea(KR)	Asia
5	172.30.108.234/32	3786	LGDACOM	LG DACOM Corporation	South Korea(KR)	Asia
6	172.30.65.93/32	3786	LGDACOM	LG DACOM Corporation	South Korea(KR)	Asia
7	172.30.38.103/32	3786	LGDACOM	LG DACOM Corporation	South Korea(KR)	Asia
8	172.30.33.161/32	3786	LGDACOM	LG DACOM Corporation	South Korea(KR)	Asia
9	172.20.42.84/32	3786	LGDACOM	LG DACOM Corporation	South Korea(KR)	Asia
10	172.20.62.113/32	3786	LGDACOM	LG DACOM Corporation	South Korea(KR)	Asia

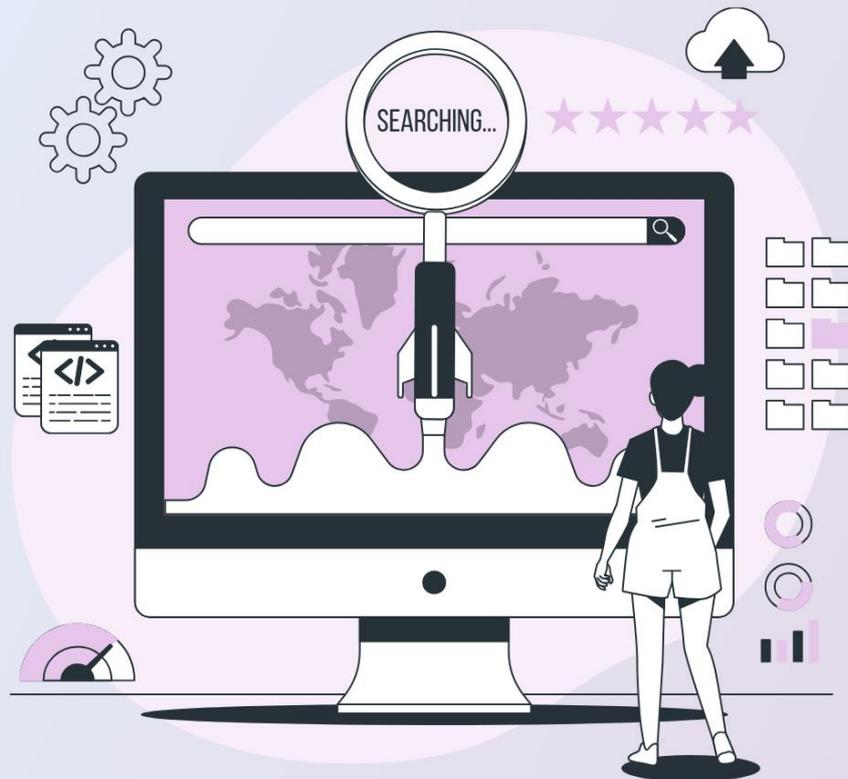
Total 1286 < 1 2 3 4 5 6 ... 129 >

D DragonLab | BGPWatch

BGPWatch

User Manual

Section 6 Tools



www.bgpwatch.net

Section 6. Tools



Introduction

This section aims to provide two features.

1. Economy/Region
2. MOAS

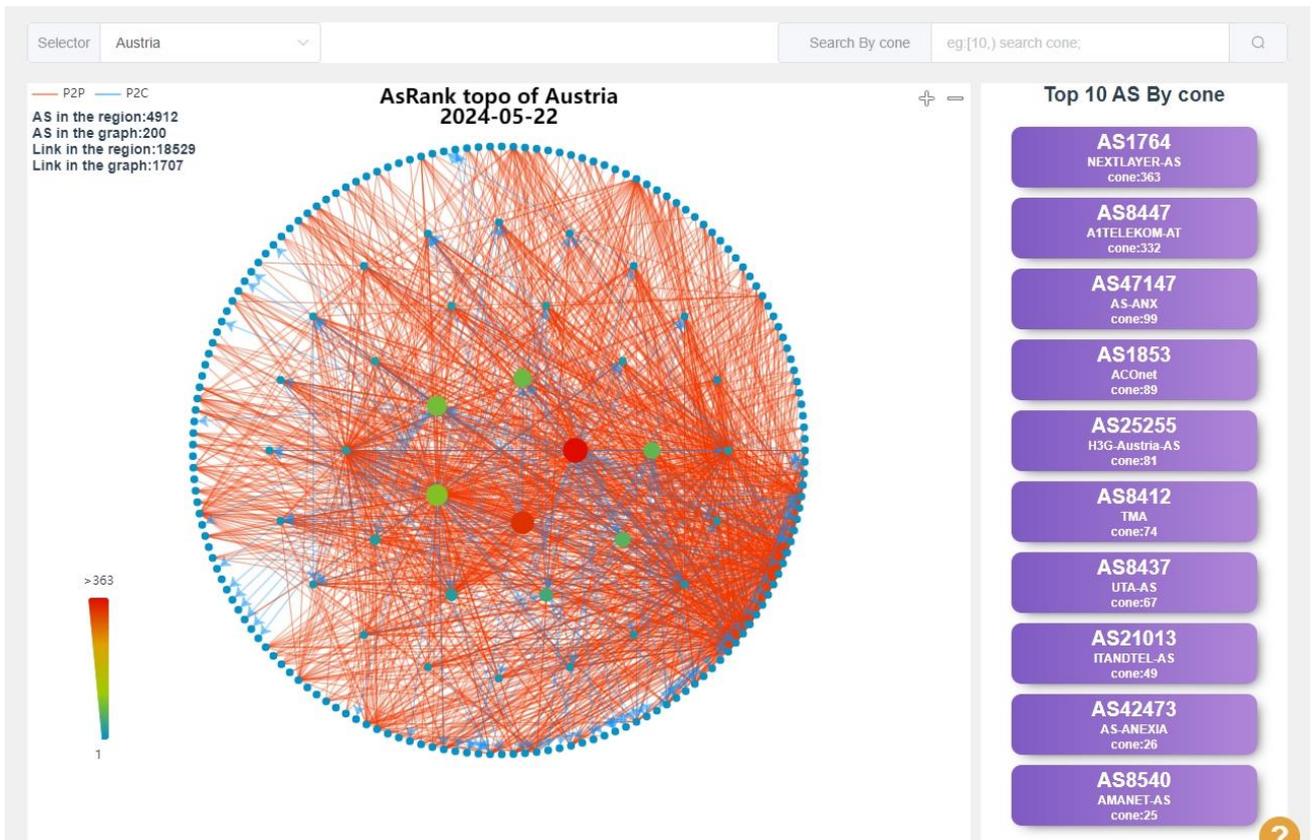
Navigating the Page

1. Economy/Region

The Economy/Region section tries to give a global picture of AS topology of the specified economy based on the “Cone” size of each AS.

Users can filter AS by the cone, which represents the customer cone of an AS.

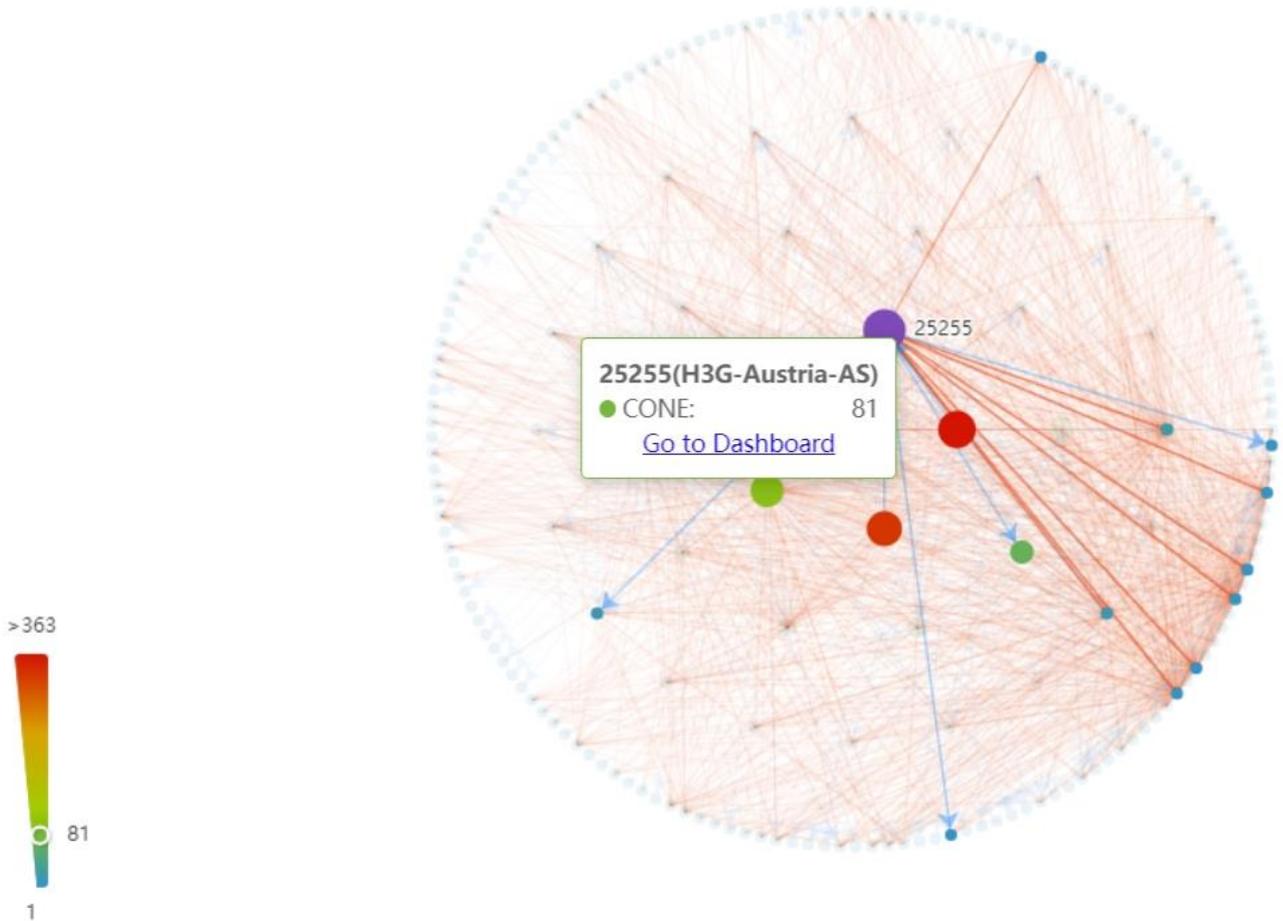
After user select an economy or region and the cone range, a topology graph of the economy or region will be shown.



In this figure, the selected economy was Austria which has the 4912 number of ASes and 18529 links.

The graph can be zoomed in and zoomed out by clicking on the +/- sign at the top-right side of the graph.

The Top-10 AS with their AS number, AS Name and cone size is shown at the right side of the graph.



If hovering the mouse over any node, it will show the AS number and cone size of that node as follows. User can click on “Go to Dashboard” and check detailed information.

The size of the nodes depends on the cone size and color of the nodes depends on the color scale located at the bottom left of the page.

2. MOAS

MOAS events typically indicate scenarios where a prefix is announced from multiple ASes, which may suggest routing anomalies or policy violations.

The information here is quite similar with the Anomaly page. User can filter by event type, harm level, time zone, start time period, duration, or simple search a specific event. There is a download button to download the statistics in CSV format.

The table displays the event type, event information, prefix number, prefix example, start time, end time, duration, and a link to details.

Select event type		Time zone	Select time period (by Start Time)		Duration	Select for event by keywords		
All		GMT+8	2024-05-21 17:38:26 - 2024-05-22 17:38:26		All	Please enter search key		
Event Type	Event Info	Prefix Num	Prefix Example	Start Time	End Time	Duration	Detail	
1 Ongoing SubMoas	Before: CA/AS13768(COGECO-PEER1) After: US/AS6640(CENTURYLINK-TIER3-CLOUD)	1	prefix: 66.155.28.0/22 subprefix: 66.155.28.0/24	2024-05-22 17:37:10	-	-	detail	
2 Ongoing SubMoas	Before: CA/AS13768(COGECO-PEER1) After: US/AS6640(CENTURYLINK-TIER3-CLOUD)	1	prefix: 66.155.16.0/20 subprefix: 66.155.18.0/24	2024-05-22 17:37:10	-	-	detail	



BGPWatch

User Manual

Section 7 Subscription



Section 7. Subscription

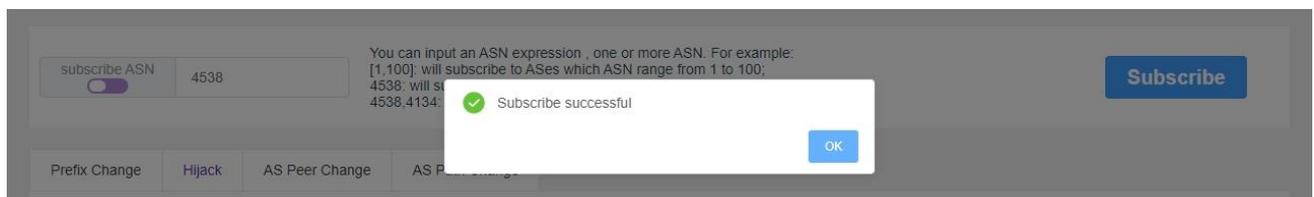
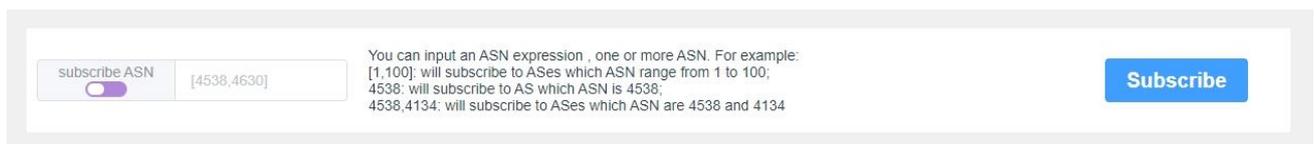
Introduction

User can subscribe ASNs and prefixes they are interested in. Then BGPWatch system will monitor the subscribed ASes and Prefixes, and send alert message via email to the user in case of any prefix change, Hijack, AS Peer Change and AS Path Change. For subscription, user have to login with an account.

Navigating the Page

In the subscribe section, user can find the AS details based on the subscription that have added. On the input box, user can put an ASN expression to add one or more ASNs. For example:

1. [1,100]: will subscribe all ASes ranging from AS1 to AS100;
2. 4538: will subscribe only AS4538;
3. 4538,4134: will subscribe both AS4538 and AS4134.



If clicking on this Toggle Button, it will be changed from “subscribe ASN” to “subscribe prefix” and a new input field for prefix subscription will appear at the right.



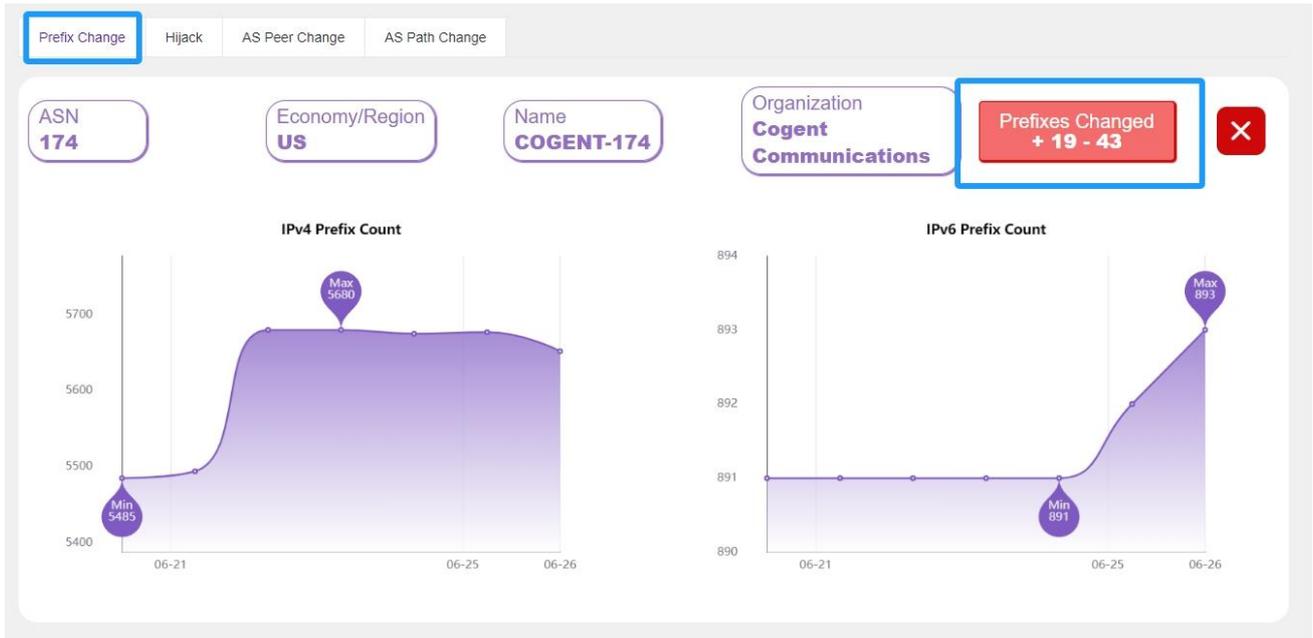
In this mode, user can key in ASN and a prefix to subscribe.

After subscription, you will see four types of information in four tabs.

1. **Prefix Change**
2. **Hijack**
3. **AS Peer Change**
4. **AS Path Change**

The first three tabs work for “Subscribe ASN” mode and the last one, means the “AS path Change” only works for “Subscribe Prefix” mode subscription.

1. **Prefix Change**

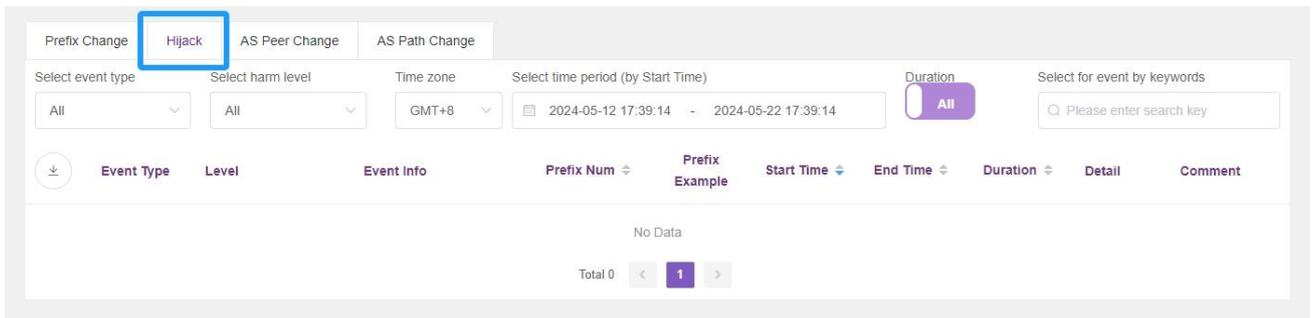


Prefix Change tab shows similar information with the dashboard. It shows basic information, then IPv4 prefix count and an IPv6 prefix count in a line graph for the last seven days for the subscribed ASes. If there is any change in the prefix for any particular ASN on the last two days, it will show an alarm button about the change. In the above example, in the last 2 days, ASN 174's prefixes have changed. There were 19 prefixes added and 43 prefixes removed. User will also be notified through email in case of any prefix change for the subscribed ASes.

Clicking the alarm button, user can see the related prefixes added and removed.

2. Hijack

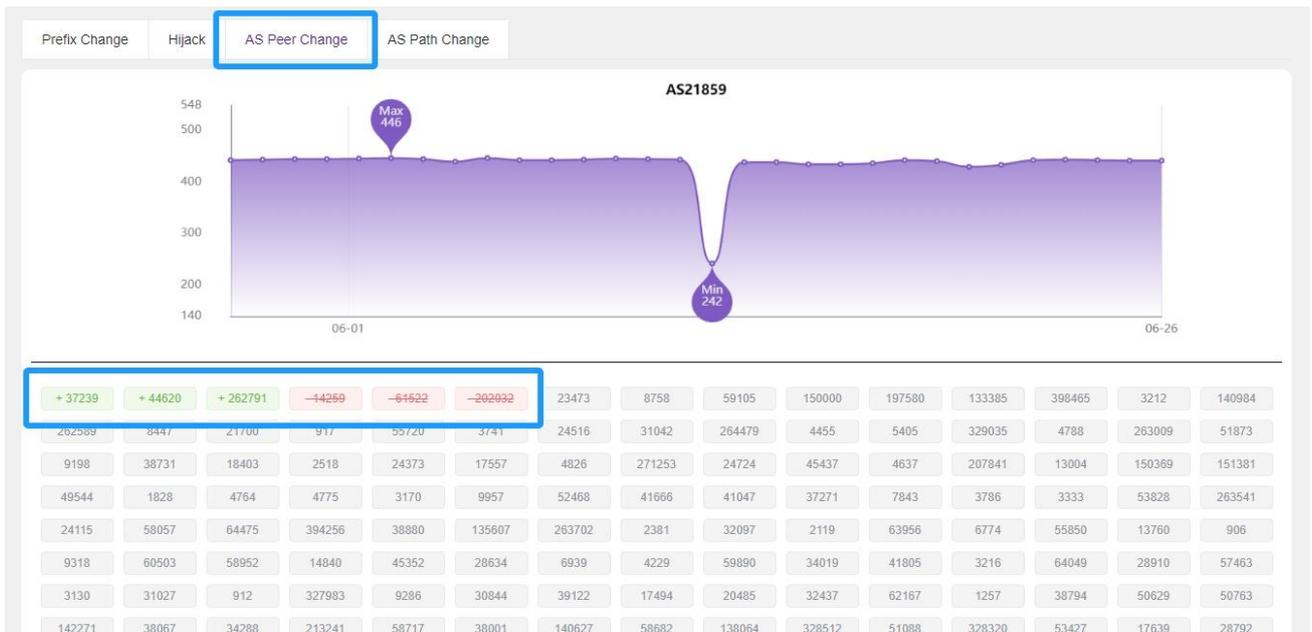
In this tab, user will find if there is any hijacking event in the subscribed ASes which is the similar information as shown in "anomaly menu". User will also be notified through email when there is a hijacking event occurring.



In the above case, it is showing "No Data", which means there's no hijacking event for the subscribed prefix in selected time period.

3. AS Peer Change

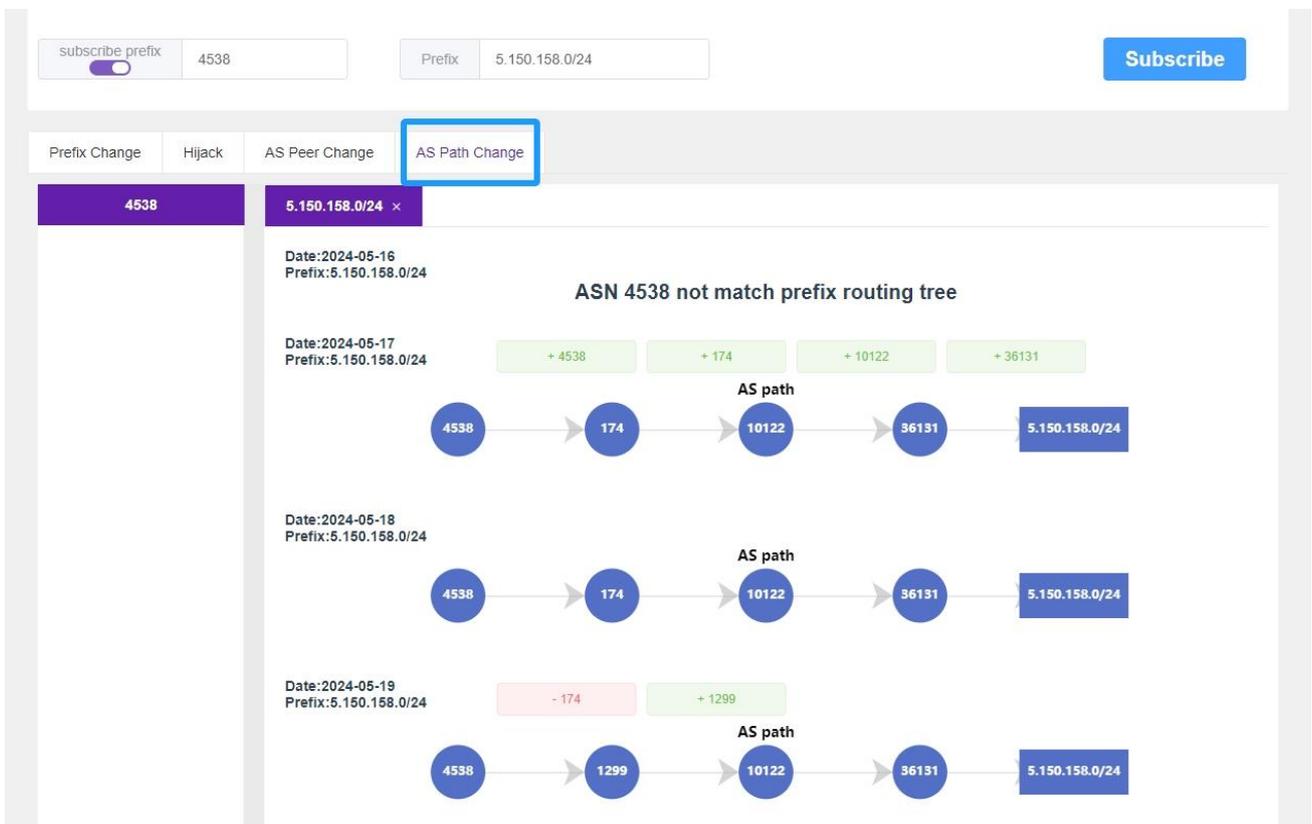
This tab shows the information about any change of Peers for the AS that user have subscribed.



This shows the information about the daily AS peer count in a line graph for the last thirty days. It also shows the peer ASN of the recent day and the changes comparing to the previous day below the graph. "+" represents an increase and "-" represents a decrease. In the above example, AS21859 has added 3 peers and removed 3 peers.

4. AS Path Change

AS path change tab shows the information on any change in the AS path for the subscribed ASN and subscribed prefix.



This tab only works for the “Subscribe Prefix” mode on the toggle button. User can key in ASN and a prefix in pair to subscribe and view the AS path change. The subscribed ASNs are listed on the left side and the subscribed prefixes are tabbed on the right. The system shows the AS Path information for the last seven days.

D DragonLab | BGPWatch

BGPWatch

User Manual

Section 8 Documentation



www.bgpwatch.net

Section 8. Documentation



Introduction

This page stores useful documentations for this BGPWatch platform.

Navigating the Page

Three parts are included in this part.

1. User Manual PDF

The user manual PDF provides a comprehensive overview of the BGPWatch platform, detailing each section with thorough explanations, words, and screenshots. It serves as an essential resource for users, offering step-by-step instructions on how to navigate and utilize the platform's features.

2. User Manual Video

The user manual video offers a comprehensive visual guide to the BGPWatch platform. It includes detailed explanations of each section's features and functionalities, illustrated with real-time demonstrations and step-by-step instructions. This video serves as an interactive companion to the PDF manual, making it easier for users to understand and navigate the platform effectively.

3. API Document

The API document offers detailed information and guidelines for utilizing the BGPWatch API. It provides step-by-step instruction on acquiring API.