

BGPWatch

User Manual



User Manual of BGPWatch

Section 1.	Registration and Logging in	4
Section 2.	Homepage.....	7
Section 3.	Anomaly.....	10
1.	Prefix Hijack/Subprefix Hijack anomaly.....	10
2.	Path Anomaly	15
3.	RouteLeak Anomaly.....	17
4.	Overview	17
Section 4.	Dashboard.....	20
1.	Basic	20
2.	IPv4 Peers.....	25
3.	IPv6 Peers.....	26
4.	WHOIS.....	27
5.	PeeringDB	27
Section 5.	Routing Path	29
1.	Forward Routing Path.....	29
2.	Reverse Routing Path	31
3.	Bi-directional Routing Path	31
4.	Jitter Route	32
5.	Daily Bogan	33
Section 6.	Tools	36
1.	Economy/Region	36
Section 7.	Subscription.....	39
1.	Anomaly	40
2.	AS Info	40
3.	Path Change	41
Section 8.	About	43
Section 9.	Documentation.....	45
1.	User Manual PDF	45
2.	User Manual Video	45
3.	API Document	45
Section 10.	Appendix.....	47
1.	Data Sources and Retrieval Periods	47
2.	Data Processing Frequencies	47
3.	CGTF RIS	48



Background

BGPWatch is an international initiative led by the CERNET/Tsinghua University team. The platform is now live at <https://bgpwatch.cgtf.net/> and provides functions in four aspects: Anomaly Detection (including prefix hijacking, path hijacking, route leaking detection, source IP address spoofing detection, and bogon IP announcement detection), AS Dashboard (summary information for AS, RIR, and ROA registrations), Routing (forward routing, reverse routing, bidirectional routing paths, and jitter monitoring), and Subscription (alerts for prefix changes, peer changes, routing path changes, and anomaly events, as well as weekly reports).

It is funded by the National Key Research and Development Program of China and the APNIC Foundation, along with 22 NRENs and 2 university partners, including AARNET, APAN-JP, BdREN, CERNET, DOST-ASTI, ErdemNET, ERNET, Göttingen University, HARNET, ITB, KAUST, KREONET, LEARN, MYREN, NREN, PERN, REANNZ, RedCLARA, RNP, SANReN, SingAREN, ThaiREN, TransPAC, and the University of Surrey.

In particular, BdREN and ThaiREN have provided extensive training support, while HARNET has offered VMs to host the platform.

Website

<https://bgpwatch.cgtf.net/>

Contact

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

BGPWatch

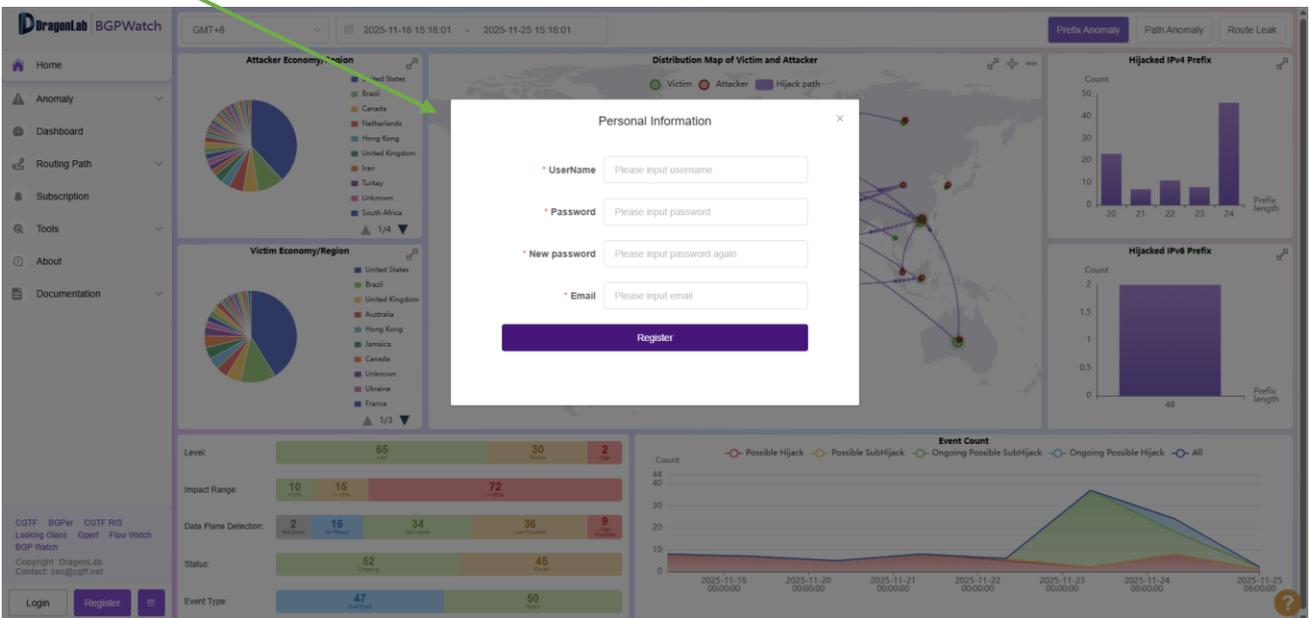
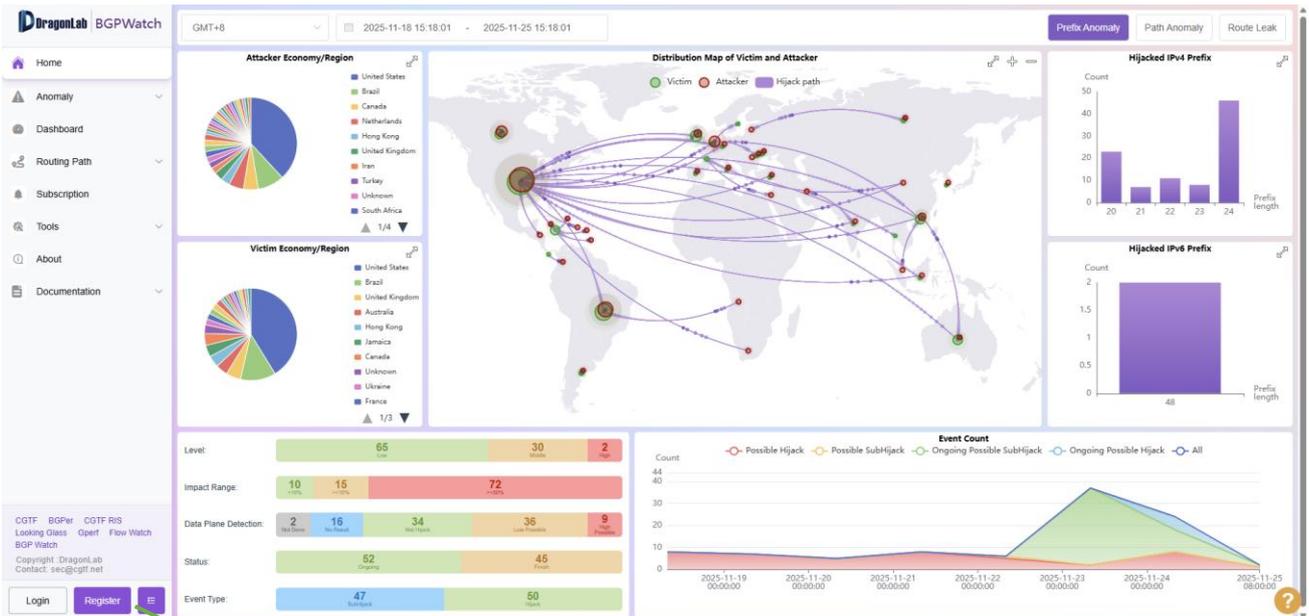
User Manual

Section 1 Registration and Logging in

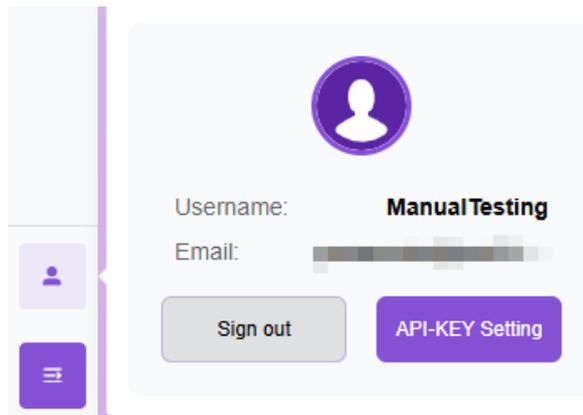


Section 1. Registration and Logging in

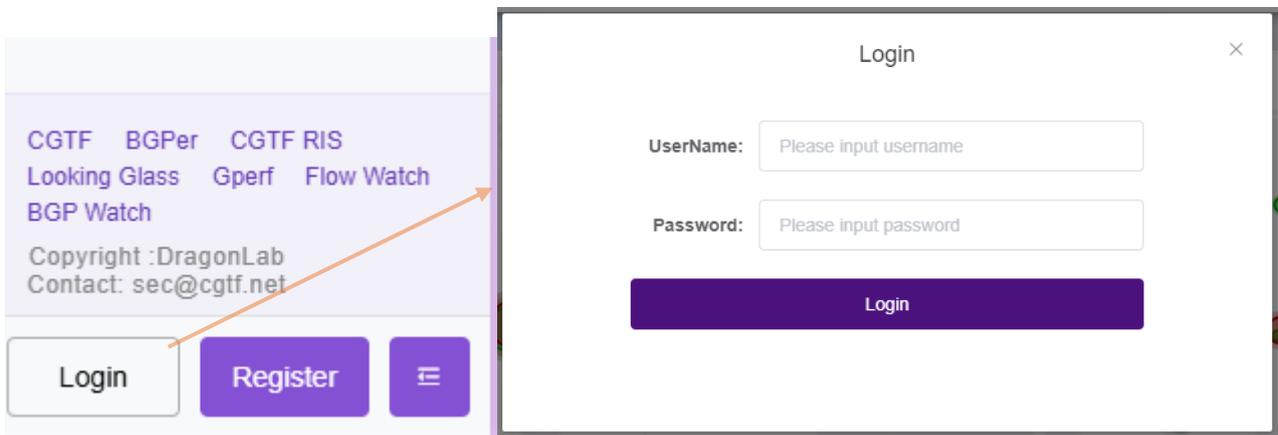
First, you can register on BGPWatch by clicking the “Register” button. In the pop-up window, you need to enter your username, password, and email address in the text boxes, then click the “Register” button to submit your registration request. You will receive an email from sec@cgtf.net. If you enter a username that is already in the system, the system will display an error message: “Duplicate Username”.



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



Logged-in users will get additional options like Subscription and Email Notifications, which are described in the **Subscription** Section.



BGPWatch

User Manual

Section 2 Homepage

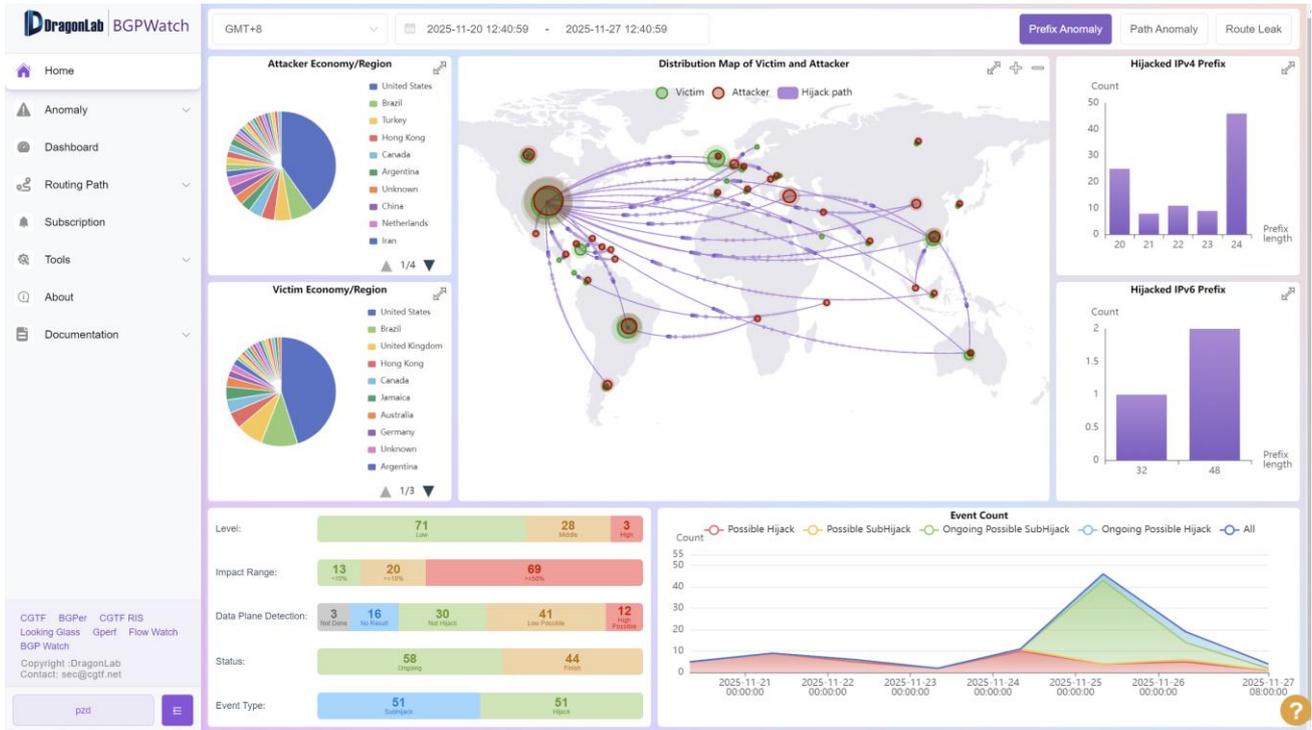


Section 2. Homepage

Introduction

The home page displays a summary of anomaly information.

Navigating the Page



On top of the homepage, there is a **time zone dropdown list** and a **calendar** where you can select the time zone and date range.

In the top right corner of the page, there are 3 buttons:

- Prefix Anomaly
- Path Anomaly
- Route Leak

Click each button to view the corresponding information. The layout of all pages is the same. Here we only take Prefix Anomaly as an example for introduction.

Top Left

The top-left area contains two pie charts illustrating the economy/region-wise distribution of “attackers” and “victims”. Based on your time filter, you will be able to view the economies/regions of attackers and victims. These are interactive charts—you can click on the legends to show or hide

statistics for any of these economies. You can also click the expand button to enlarge the section for a better view.

Top Right

The top-right area contains two bar charts displaying hijacked IPv4 and IPv6 prefixes by prefix length for your selected date range. The Y-axis represents the hijack count, while the X-axis represents the prefix length. Hover your mouse over the bars to display the exact count for each one. You can also click the expand button here to enlarge the section for a better view.

Top Middle

The top-middle area features a worldwide distribution map in the form of a “Bubble Chart”, showing the volume of economy-wise victims and attackers. Hover your mouse over the bubbles to view the economy of the attacker and victim, as well as the event counts for the selected date range. As this is a bubble chart, the bigger the bubble, the higher the number of attackers/victims. Red bubbles represent attackers, green bubbles represent victims, and animated purple lines indicate the direction from hijacker to victim.

Clicking on a bubble will direct the page to the corresponding anomaly event information in the Anomaly section. This page also distinguishes between prefix and path anomalies.

Bottom Left

On the bottom left, a segmented bar chart provides an overview of detection information, including “Impact Range”, “Data Plane Detection”, “Level”, “Status”, and “Event Type”. The colored segments indicate different types and levels within the corresponding categories, and the numbers represent the total number of anomaly events. Clicking on the segments allows you to view more information about the events.

Bottom Right

On the bottom right, a line graph shows the daily count of hijack events.

All these graphs are interactive

Hovering your mouse over any bars or lines will display detailed information. For the bar chart, you can also click on the legends to view detailed information. For the Event Count line graph, you can click on the legends to show or hide any lines.

BGPWatch

User Manual

Section 3 Anomaly



Section 3. Anomaly

Introduction

In this section, all BGP hijacking events are reported and statistically analyzed.

There are 3 major categories of anomalies: Prefix Hijack / Subprefix Hijack anomaly, Path Hijack anomaly, Route Leak anomaly

- **Prefix Hijack/Subprefix Hijack anomaly**

Prefix Hijack refers to a BGP hijacking attack that targets the entire allocated IP block. By advertising the entire prefix, an attacker can redirect traffic intended for the entire network within the legitimate network to a malicious destination.

Subprefix Hijack 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 the sub-prefix, an attacker can redirect traffic intended for a specific host or service within the legitimate network to a malicious destination.

- **Path Hijack anomaly**

Path Hijack refers to malicious behavior where attackers induce traffic to pass through unexpected paths by forging or tampering with AS numbers (ASNs) in the path, rather than directly forging IP prefixes.

- **Route Leak anomaly**

Route Leak refers to a situation where an AS broadcasts BGP route information that should not be propagated to other ASs due to incorrect configuration or malicious operations, thereby disrupting normal routing policies and traffic flow.

For each of the above categories, there are two event statuses: "**Ongoing**" if the event is still continuing, and "**Finished**" if the event has already ceased.

Navigating the Page

1. Prefix Hijack/Subprefix Hijack anomaly

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

Event Type	Level	Data Plane	Impact Range	Event Info	Prefix Num	Prefix Example	Start Time	End Time	Duration	Detail
1 Ongoing Possible SubHijack	Low	Not Hijack	96.1%	Victim:BR/AS 268905 () Attacker:/AS 274553 ()	1	prefix: 45.175.84.0/22 subprefix: 45.175.86.0/23	2025-11-26 08:58:34	-	-	detail
2 Possible Hijack	Low	Low Possible	37.93%	Victim:US/AS 13958 (AUTOPHONE-OF-LAREDO) Attacker:MX/AS 265534 ()	22	216.150.40.0/24	2025-11-26 07:24:30	2025-11-26 08:40:27	1:15:57	detail
3 Ongoing Possible SubHijack	Low	Not Hijack	90.91%	Victim:US/AS 3581 (CENTURYLINK-LEGACY-SAVVIS) Attacker:US/AS 54040 (NBCUNI)	1	prefix: 216.39.32.0/20 subprefix: 216.39.34.0/23	2025-11-26 07:21:47	-	-	detail
4 Ongoing Possible Hijack	Low	Low Possible	29.73%	Victim:BR/AS 272739 () Attacker:/AS 274226 ()	1	38.156.70.0/24	2025-11-26 03:48:12	-	-	detail
5 Possible Hijack	Middle	Low Possible	84.71%	Victim:US/AS 203 (CENTURYLINK-LEGACY-LVLT-203) Attacker:US/AS 32988 (MAXIM)	1	205.153.101.0/24	2025-11-26 01:02:17	2025-11-26 01:18:25	0:16:7	detail
6 Ongoing Possible Hijack	Low	Not Done	84.13%	Victim:GB/AS 47272 (HYEHOST) Attacker:/AS 215265 ()	1	2a09:54c5::/32	2025-11-25 23:01:16	-	-	detail
7 Ongoing Possible Hijack	Low	No Result	68.42%	Victim:GB/AS 202525 (CHUNMING-AS) Attacker:US/AS 16509 (AMAZON-02)	1	46.29.36.0/24	2025-11-25 21:40:02	-	-	detail

Options include:

[1] Time Zone:

- Users can select the time zone from the dropdown list.

[2] Time Period (By Start Time):

- Users can specify a time period to search for events where the start time falls within this period.

[3] Search Event

- There is an advanced search feature that enables users to enter specific keywords related to hijacking events. These can include terms such as AS numbers, IP prefixes, event types, or strings in the Event Info.

[4] Download Button:

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

[5] Event Type:

- The events will be categorized as either Possible Hijack or Possible SubHijack depending on the type of hijack. For ongoing ones, the events will be prefixed with "Ongoing" (i.e., termed as "Ongoing Possible Hijack" or "Ongoing Possible SubHijack").

[6] Severity Levels:

- When the number of TOP 1M websites contained in the hijacked prefix is greater than 5, the event is classified as "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 classified as "Middle" level.
- Otherwise, the event is classified as "Low" level.

[7] Data Plane:

If the hijacked prefix includes reachable TOP 1M websites or active IPs from unaffected ASes, the event is verified at the data plane by deploying probes from probe nodes (Probers) in two groups: "Affected ASes" (those potentially impacted by the hijacking) and "Unaffected ASes" (those with normal routing).

Since ASes affected by hijackers cannot access the victim's services, there should be a high correlation coefficient between this inaccessibility and the hijacking event. By calculating the correlation coefficient between the hijacking event and the ping results, the data plane detection results can be classified into 5 types:

- Not Done: There are no active IP addresses in the specified prefix.
- No Result: The system attempts to ping some active IP addresses but obtains no results.
- High Possible: The correlation coefficient ≥ 0.7 .
- Low Possible: The correlation coefficient is between 0 and 0.7 ($0 < \text{correlation coefficient} < 0.7$).
- Not Hijack: The correlation coefficient = 0.
-

[8] Impact Range:

- By calculating the proportion of ASes in the hijacking path relative to the total number of ASes in the replay tree, the Impact Range of each event is classified into three categories: $\geq 50\%$, $\geq 10\%$, and $< 10\%$.

[9] Event Info:

- The AS numbers, names, and affiliated economies of the victim and the attacker.

[10] Prefix Num:

- The number of prefixes involved in the event.

[11] Prefix Example:

- A sample of the affected prefix.

[12] Start Time:

- The timestamp when the hijacking event began.

[13] End Time:

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

[14] Duration:

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

[15] Detail:

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

Prefix Anomaly Event Detail

Harm Level

High Level

89.33.12.0/24-HIJACK1763974849 Possible Hijack Events

Range of Impact

80%

Victim AS: [199414](#)

Victim Economy: DE (Germany)

Victim AS Name: NEOPROTECT-NET

Hijacker AS: [834](#)

Hijacker Economy: US (United States)

Hijacker AS Name: IPXO

Start Time (UTC): 2025-11-24 09:00:49

End Time (UTC): 2025-11-24 11:15:38

During Time: 2:14:48

Reason:

(834, 89.33.12.0/24) doesn't align in ROA

(199414, 89.33.12.0/24) doesn't align in ROA

(834, 89.33.12.0/24) doesn't align in WHOIS

(199414, 89.33.12.0/24) aligns in WHOIS

Prefix

89.33.12.0/24

Info:

Website: 89.33.12.0/24

toffl.top

ultimis.net

bartolamp.com

elementality.fun

opmine.ru

citrine.pro

twerion.net

chillzone.space

etty.su

astral-mc.space

minwix.net

gzmclol

mineheart.net

blocktopia.ru

dottoa.com

twc.su

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

1. Basic Information:

- This part provides basic information about the event, which has already appeared in the previous table.

2. Additional Information

- Reason: Some information about why the event is classified as a possible hijack. Typically, it will display details regarding Route Origin Authorizations (ROA) and WHOIS information.
- Prefix Info: The prefix involved in the event.
- Website: A list of links to the TOP 1M websites associated with the hijacked prefix.

3. Data Plane Detection

- This section is designed to display the outcomes of data plane detection for hijacking events. This information is vital for understanding how the probes are conducted, all the reachable detection results, and the results of correlation coefficient calculation.

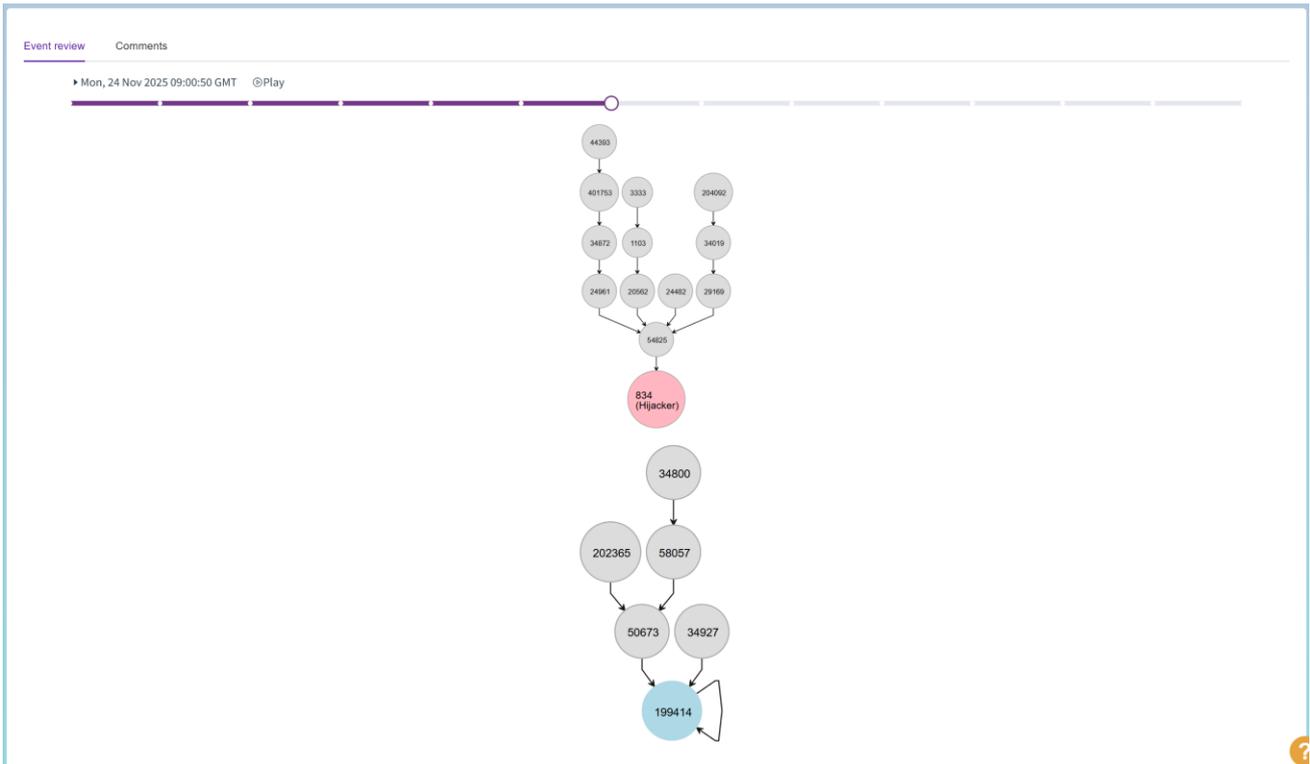
Target		Data Plane Detection			Overall Correlation Coefficient: 0.293
89.33.12.7		2025-11-24T09:02:12.000Z			Correlation Coefficient: 0.29
Probe AS	Economy	Time(UTC)	From	Min RTT	Packet Loss
AS34927		2025-11-24T09:02:12.000Z	193.148.249.35	No reply	100.00%
AS24961		2025-11-24T09:02:11.000Z	89.163.130.251	No reply	100.00%
AS34872		2025-11-24T09:02:12.000Z	194.28.98.93	No reply	100.00%
AS3303		2025-11-24T09:02:12.000Z	217.193.139.97	No reply	100.00%
AS17639		2025-11-24T09:02:12.000Z	161.49.13.250	No reply	100.00%
AS3333		2025-11-24T09:02:12.000Z	193.0.0.164	No reply	100.00%
AS29169		2025-11-24T09:02:11.000Z	217.70.178.109	No reply	100.00%
AS204092		2025-11-24T09:02:12.000Z	80.67.190.218	No reply	100.00%
AS62000		2025-11-24T09:02:11.000Z	89.234.181.105	No reply	100.00%
AS58057		2025-11-24T09:02:12.000Z	193.33.94.201	No reply	100.00%
AS34800		2025-11-24T09:02:12.000Z	194.50.99.201	No reply	100.00%
AS24482		2025-11-24T09:02:12.000Z	203.175.175.206	No reply	100.00%
AS34019		2025-11-24T09:02:12.000Z	193.17.192.184	No reply	100.00%
AS41327		2025-11-24T09:02:11.000Z	185.157.231.49	No reply	100.00%
AS47160		2025-11-24T09:03:26.000Z	31.14.69.87	No reply	100.00%
AS50673		2025-11-24T09:02:12.000Z	5.255.77.111	4.09ms	0.00%

Key information displayed in this part:

- 1) **Target IP Address and Detected Date and Time:**
 - If the hijacked prefix includes reachable TOP 1M websites or active IPs from unaffected ASes, their IP addresses are selected. The probed IP addresses and the date and time of detection are listed here..
- 2) **Probe AS, Possible Hijacking Associated Economies, Date and Time, and IP:**
 - Shows the Autonomous System (AS) number and IP address of the probe that conducted the ping test.
- 3) **Min RTT:**
 - Provides the minimum RTT (Min RTT) results when the command was executed; otherwise, it displays "No reply".
- 4) **Packet Loss:**
 - Shows the percentage of packet loss.
- 5) **Overall Correlation Coefficient:**
 - Displays the correlation coefficient of the hijacking event and the ping results. Since the ASes affected by hijackers cannot access the victim's services, a higher correlation coefficient value indicates a higher likelihood of a hijacking event.

4. Event Review

- In this section, you will find information about the reverse routing paths of the victim and the hijacker of the hijacking event in a time-stamped manner. You can use the [Slider] to navigate to different timestamps to obtain this information. You can also click the Play button to automatically slide from one timestamp to another to view the entire event.



5. Comments:

This part provides an interface for users to give feedback on the event.

2. Path Anomaly

This interface is similar to the Prefix Anomaly page; you will see a table that organizes information about various anomaly events in a structured format. Only its unique options and information are listed below.

Event Type	Level	Possible	Impact Range	Affected ASN	Affected Prefix	Suspicious Links	Start Time	End Time	Duration	Detail
1 Finish Path Hijack	Low	High Possible	<10 View Point	273103	38.191.197.0/24	["267823", "27951"]	2025-11-22 05:30:50	2025-11-22 07:54:20	2:23:30	Detail
2 Ongoing Path Hijack	Low	High Possible	<10 View Point	327885	196.249.70.0/24	["37349", "37035"]	2025-11-21 15:36:51	2025-11-21 15:56:54	0:20:3	Detail
3 Finish Path Hijack	Low	High Possible	>10 View Point	131310	143.192.102.0/24	["140866", "136978"]	2025-11-20 18:46:38	2025-11-21 12:22:54	17:36:16	Detail
4 Finish Path Hijack	Low	High Possible	>10 View Point	49367	188.215.94.0/24	["49367", "12874"]	2025-11-19 17:50:02	2025-11-20 21:07:42	27:17:40	Detail
5 Finish Path Hijack	Low	High Possible	<10 View Point	54994	138.113.116.0/24	["54994", "131219"]	2025-11-20 07:02:47	2025-11-20 07:50:29	0:47:42	Detail
6 Finish Path Hijack	Low	High Possible	<10 View Point	43256	197.215.222.0/24	["33763", "37020"]	2025-11-19 17:15:53	2025-11-19 18:12:29	0:56:36	Detail
7 Finish Path Hijack	Low	High Possible	>10 View Point	131310	143.192.102.0/24	["140866", "136978"]	2025-11-19 00:57:42	2025-11-19 13:27:31	12:29:49	Detail
8 Finish Path Hijack	Low	High Possible	<10 View Point	132203	211.152.128.0/23	["21859", "4800"]	2025-11-18 00:10:55	2025-11-18 22:30:46	22:19:51	Detail
9 Finish Path Hijack	Low	High Possible	<10 View Point	262612	177.85.192.0/24	["262612", "3549"]	2025-11-16 09:13:06	2025-11-16 23:02:39	13:49:33	Detail

- [1] Possible: The "Possible" value is based on the differences between the routing tree of an event and the normal routing tree; the greater the difference, the higher this value.
- [2] Impact Range: Indicates the number of routing observation points that can observe this anomaly.
- [3] Suspicious Link: Indicates the fake link(s) involved in the event.

Path Anomaly Event Detail

This page provides detailed information about a specific event.

The first part is the basic information. The second part list reasons and prefix info.

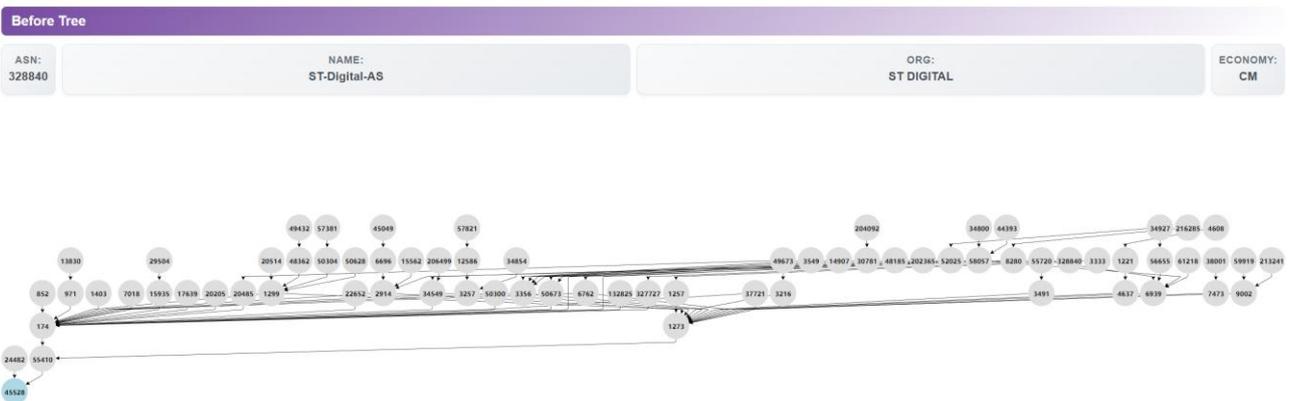
<p>Harm Level Low Level</p> <p>Range of Impact <10 View Point</p> <p>Possible High Possible</p>	<p>ARES-HIJACK-1763896300-45528-1.22.129.0/24-Hijack-AGGREGATED Ongoing Path Hijack Events</p> <table border="0" style="width: 100%; font-size: small;"> <tr> <td>Victim AS: 45528</td> <td>Suspicious AS: 45528 137491</td> <td>Start Time (UTC): 2025-11-23 11:11:40</td> </tr> <tr> <td>Victim Economy: IN</td> <td>Suspicious Economy: IN BD</td> <td>End Time (UTC): no data</td> </tr> <tr> <td>Victim AS Name: TIKONAIN-AS</td> <td>Suspicious AS Name: TIKONAI... PEEREX-...</td> <td>During Time: no data</td> </tr> </table>	Victim AS: 45528	Suspicious AS: 45528 137491	Start Time (UTC): 2025-11-23 11:11:40	Victim Economy: IN	Suspicious Economy: IN BD	End Time (UTC): no data	Victim AS Name: TIKONAIN-AS	Suspicious AS Name: TIKONAI... PEEREX-...	During Time: no data
Victim AS: 45528	Suspicious AS: 45528 137491	Start Time (UTC): 2025-11-23 11:11:40								
Victim Economy: IN	Suspicious Economy: IN BD	End Time (UTC): no data								
Victim AS Name: TIKONAIN-AS	Suspicious AS Name: TIKONAI... PEEREX-...	During Time: no data								

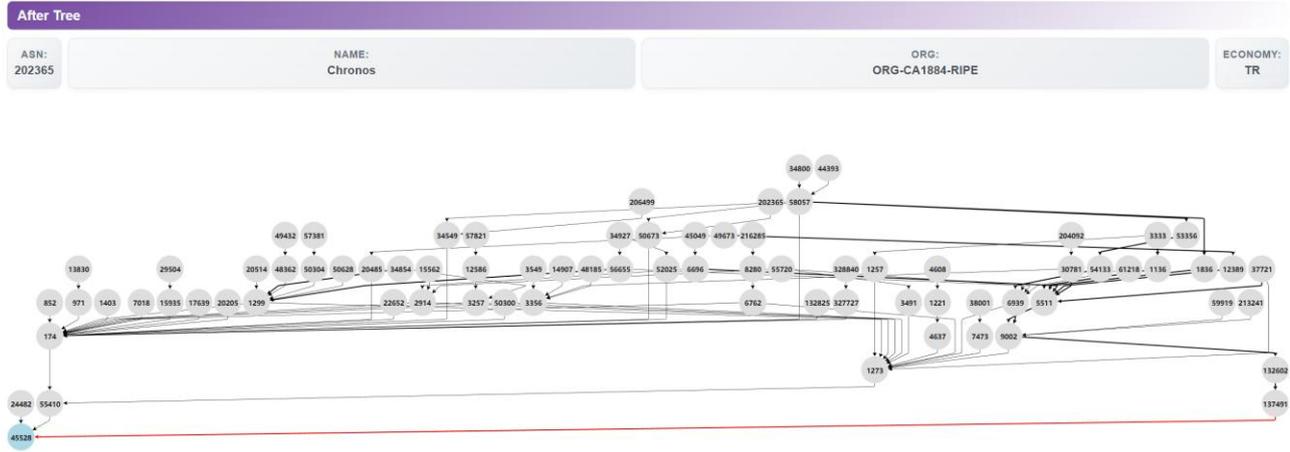
Reason: Link(45528, 137491) have no relationship in dataset but have certain impact in the new routing tree

Prefix Info: 1.22.129.0/24 1.23.112.0/24

The Replay part (third part) displays the routing tree both before the event and at the time of the event. For newly announced prefixes, there may be no pre-event routing tree. Suspicious hijacking links are indicated by red links.

Replay



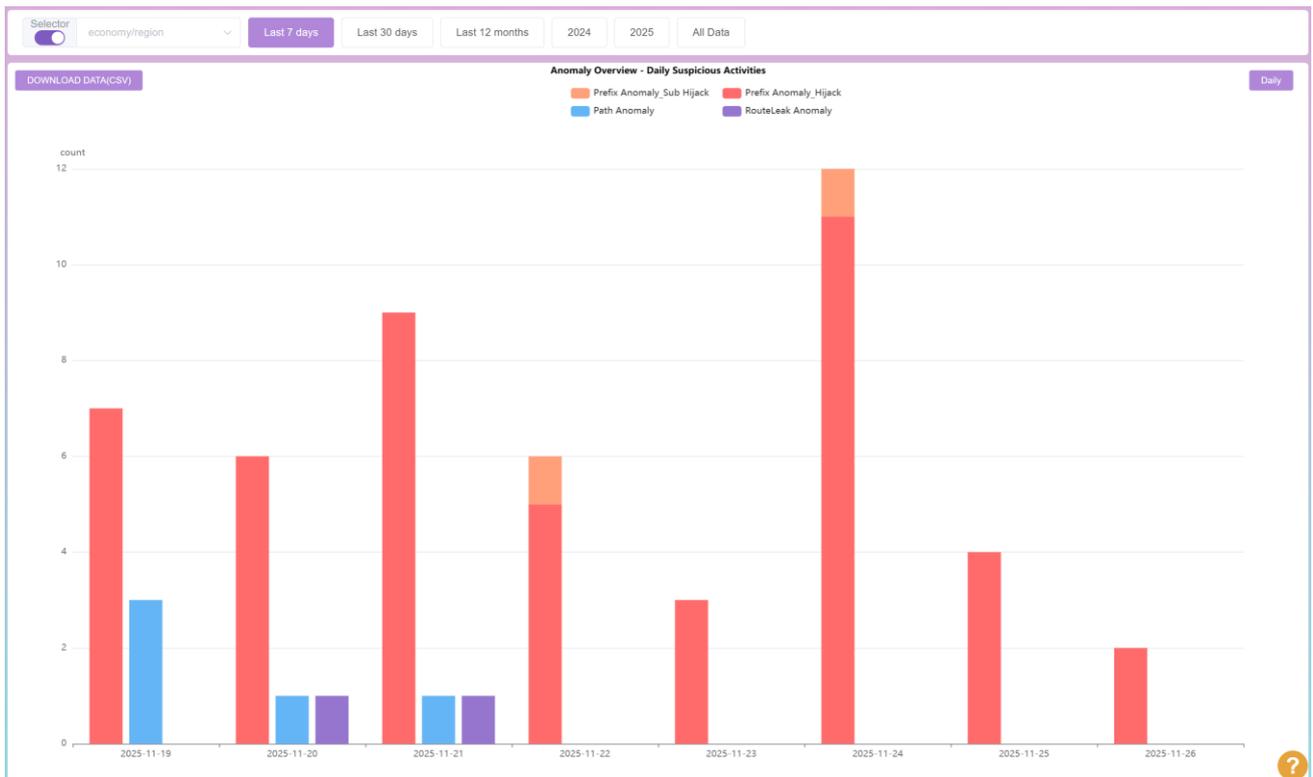


3. RouteLeak Anomaly

The structure and options of the Route Leak Anomaly page are the same as those of the Path Anomaly page.

4. Overview

Summary anomaly information is displayed on this page.



Selector (Top Left)

Users can input an ASN, select an economy, or leave it blank (blank indicates "All").

Time Period (Top Middle)

Users can select one option from the following: Last 7 days, Last 30 days, Last 12 months, 2024, 2025, All Data.

Download Data (CSV) Button

Located just below the Selector. Users can download the statistical data displayed in the graph by clicking the "Download Data (CSV)" button.

Group Data By (Top Right)

Based on the selected time period, this section displays data grouping options: Daily, Weekly, Monthly, or Yearly.

Anomaly Type (Bar Chart)

The bar chart shows the anomaly count of 4 events: Prefix Anomaly Sub Hijack, Path Anomaly, Prefix Anomaly Hijack, RouteLeak Anomaly.

Hover your mouse over any bar to view its specific value. Click a bar to access the next level of detail (e.g., from yearly to monthly). To view the anomaly events corresponding to a bar, hover over the bar and click "Go to Anomaly"—you will be redirected to the "Anomaly" section.



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.

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.

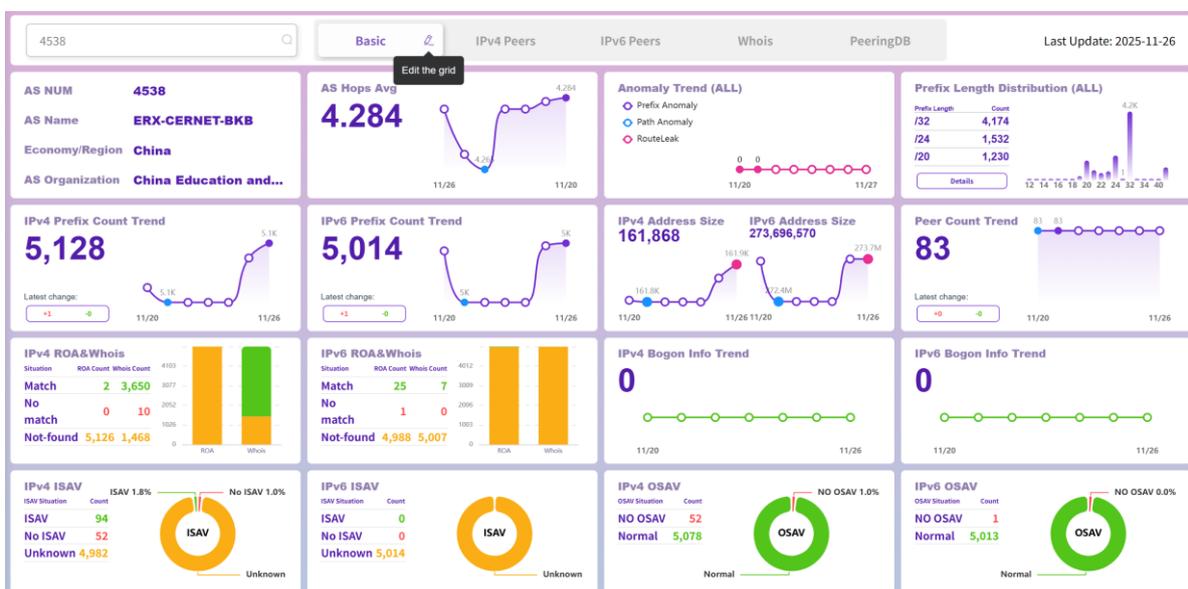
For an ASN, the result contains following tabs.

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

Navigating the Page

1. Basic

The basic information is customizable. Simply click the pen icon next to "Basic" to access the edit interface.

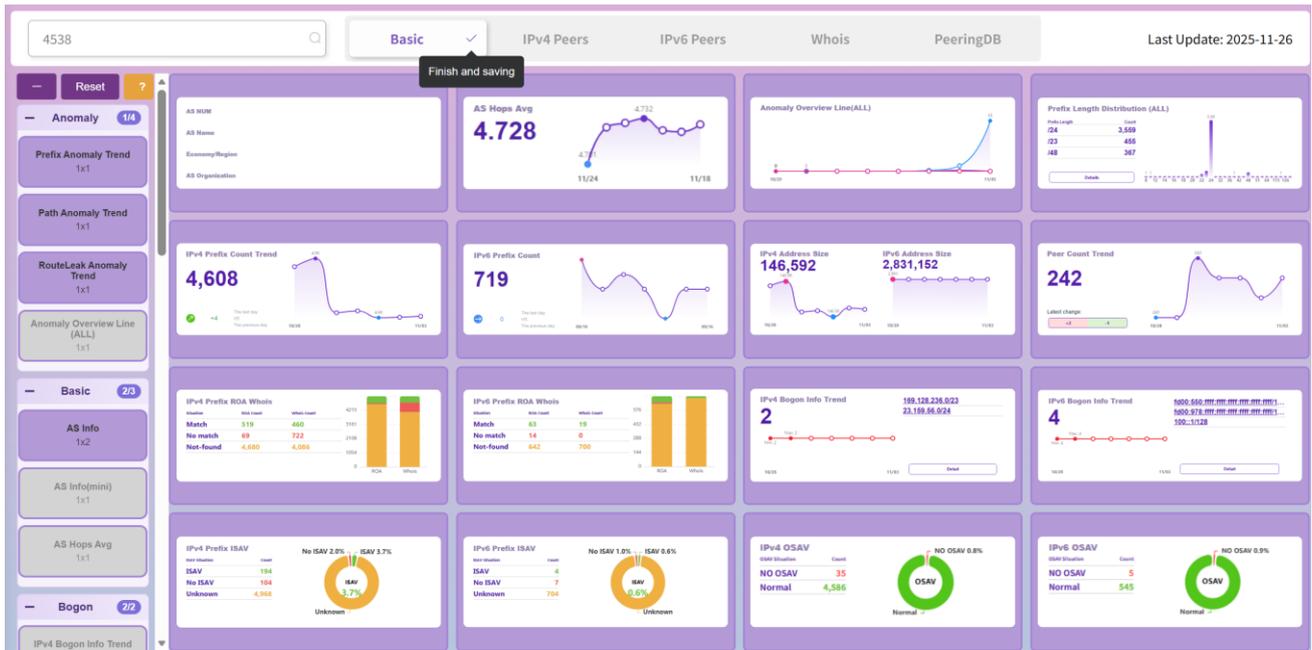


Edit Basic Grid

In the Edit Interface, follow these steps:

1. Delete some components to free up spare space.
2. Drag the left components to the available space.
3. Drag to adjust the position of the right components.

Once finished, click the checkmark next to "Basic" to exit the Edit Interface.



Anomaly Trend

Displays the trend of Anomaly event counts (Prefix Anomaly, Path Anomaly, RouteLeak Anomaly) related to the ASN over the past seven days in a line graph. If events exist, click "Detail" to view the corresponding information in a table at the bottom of the interface.



Event Type	Level	Data Plane	Impact Range	Event Info	Prefix Num	Prefix Example	Start Time
Ongoing Possible Hijack	Low	Low Possible	40.96%	Victim:HK/AS 4637 (ASN-TELSTRA-GLOBAL) Attacker:TR/AS 197450 (SUNUCUN)	2	173.239.233.0/24	2025-11-26 21:43:27
Ongoing Possible Hijack	Middle	High Possible	16.67%	Victim:US/AS 64286 (LOGICWEB) Attacker:TR/AS 197450 (SUNUCUN)	1	173.244.60.0/24	2025-11-26 21:43:27
Ongoing Possible Hijack	Low	No Result	8.2%	Victim:US/AS 6939 (HURRICANE) Attacker:TR/AS 197450 (SUNUCUN)	1	64.64.103.0/24	2025-11-26 21:43:24
Ongoing Possible Hijack	Low	No Result	17.39%	Victim:US/AS 11426 (TWC-11426-CAROLINAS) Attacker:TR/AS 197450 (SUNUCUN)	1	98.159.236.0/23	2025-11-26 21:43:23

Prefix Length Distribution (IPv4/IPv6/All) and Detail Prefix Information

Displays the distribution of IP address counts across different prefix lengths, and lists the top 3 prefixes by count along with their respective quantities. Click "Detail" to view the prefix information corresponding to the AS in a table at the bottom of the interface.

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

The screenshot shows a table of IP prefixes. At the top left is a 'Select prefix' dropdown. At the top right is a search box labeled 'Search prefix'. The table contains three columns of prefixes, each with a small colored dot indicator. At the bottom, there is a pagination bar with page numbers 1 through 338, and a 'Total 10137' label on the right.

You can click on any prefix to be directed to the reverse routing tree page.

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

The screenshot shows a dropdown menu for 'IPv4 /12' with '+ 19' items. The menu lists various prefix lengths: /32, /33, /34, /36, /40, and /48, each with a checked checkbox. The background shows a list of IP prefixes with their respective counts and status indicators.

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

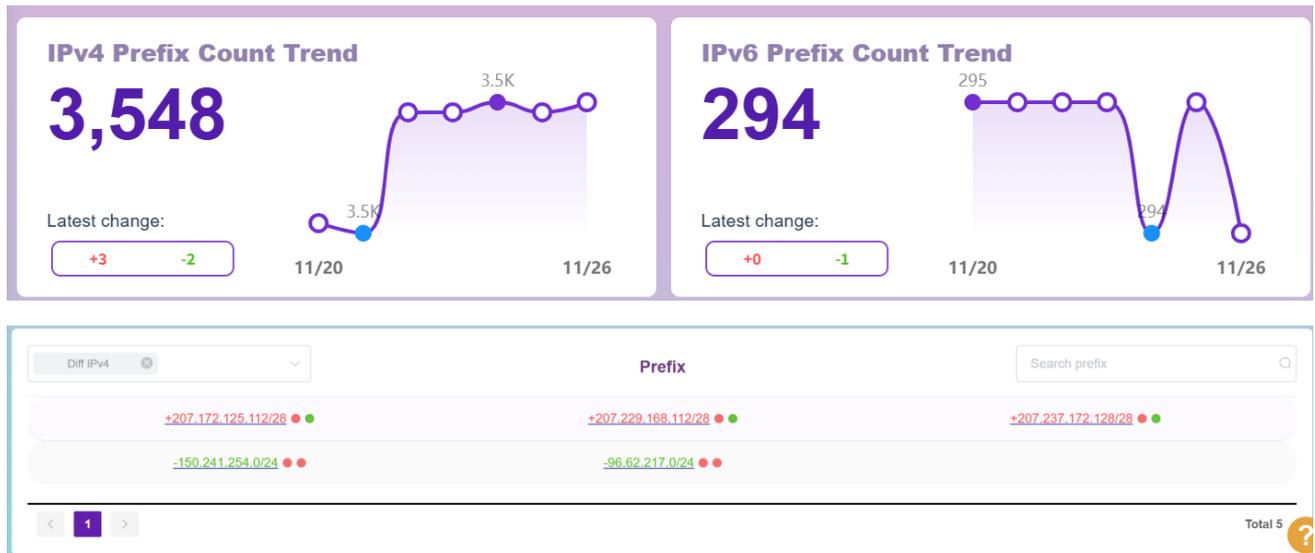
The screenshot shows the same table of IP prefixes as before, but with a search box at the top right containing the text '210'. The table is filtered to show only prefixes that contain '210'. The pagination bar at the bottom shows page 1 of 23, with a 'Total 678' label on the right.

Address Size (IPv4/IPv6/All)

Displays the IPv4 Address Size (/24) and IPv6 Address Size (/48) originating from the ASN over the past seven days in a line graph (measured in /24 units).

Prefix Count Trend (IPv4/IPv6/All)

Displays the number of IPv4/IPv6/All prefixes originating from the ASN over the past seven days in a line graph, along with the difference between the last day and the previous day. It includes a button that shows the increased and decreased prefixes as well as the daily difference result. Click the button to view the corresponding information in a table at the bottom of the interface.



Peer Count Trend

Displays the trend of the number of ASNs establishing peer relationships with the target ASN over the past seven days in a line graph, along with the difference between the last day and the previous day. It includes a button that shows the increased and decreased peers as well as the daily difference result. Click the button to view the corresponding information in a table at the bottom of the interface.

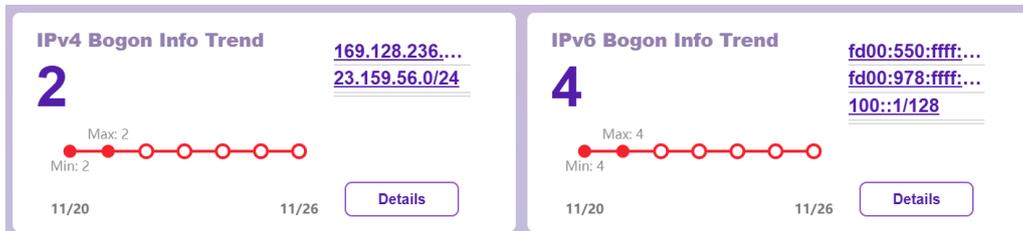


Provider
 Peer
 Customer
 Unknown

	AS neighbors	Organization	Economy/Region	AS customer cone	Relationship	Export	Import
1	-11430	Austin Bestline	United States	1	Unknown		
2	-268308	VIVA CONNECTION TELECOMUNICAÇÕES LTDA ME	Brazil	1	Unknown		
3	-32863	Trinsic Technologies, Inc.	United States	1	Unknown		
4	-395607	Casey's Retail Company	United States	1	Unknown		
5	-396122	BEC Fiber	United States	1	Unknown		
6	-53533	Entravision Communications Corporation	United States	1	Unknown		
7	+18516	Molalla Communications Systems Inc.	United States	1	customer	0	3
8	+32446	Harbor Capital Advisors, Inc.	United States	1	customer	0	2
9	+40764	Digital Network Access Communications, INC	United States	1	customer	0	1
10	+46195	ACTIVO INC	Canada	1	customer	0	1

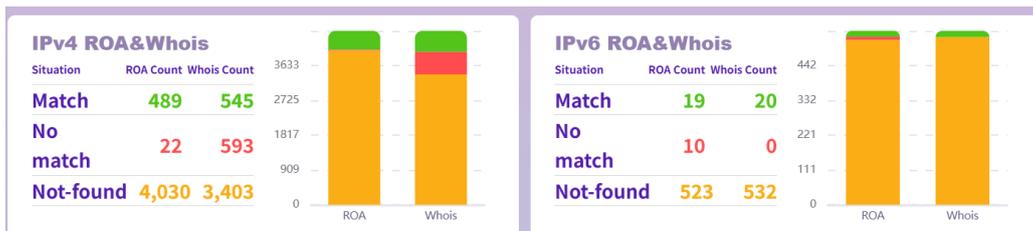
Bogon Info Trend (IPv4/IPv6)

Displays the trend of the number of bogon routes for the ASN over the past seven days in a line graph. If bogon routes exist, a "Detail" button is available—click it to view the corresponding prefixes in a table.



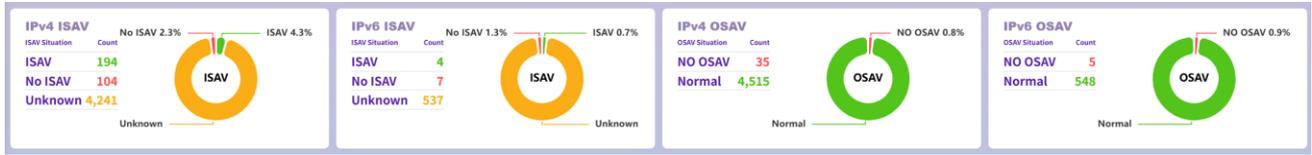
ROA/Whois (IPv4/IPv6)

Displays the registration status of the ASN's prefixes in ROA (Route Origin Authorization) and Whois.



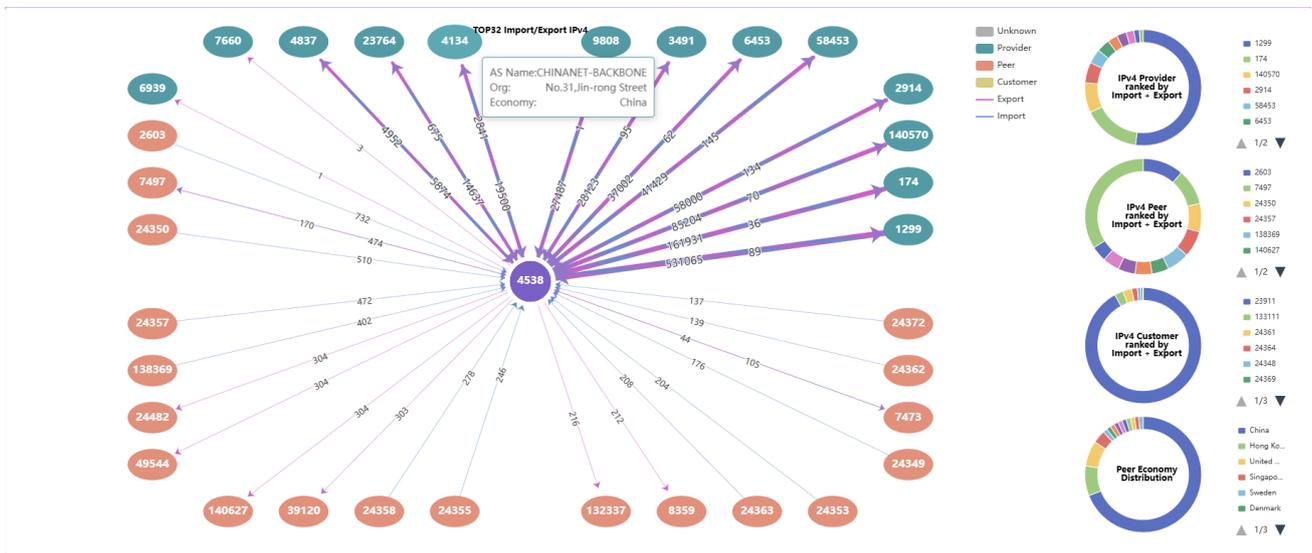
ISAV/OSAV Deployment Status (IPv4/IPv6)

Displays the deployment information of ISAV/OSAV for this AS in both IPv4 and IPv6 environments. Green indicates detected deployment, red indicates no deployment, and yellow indicates unknown status.



2. IPv4 Peers

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



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.

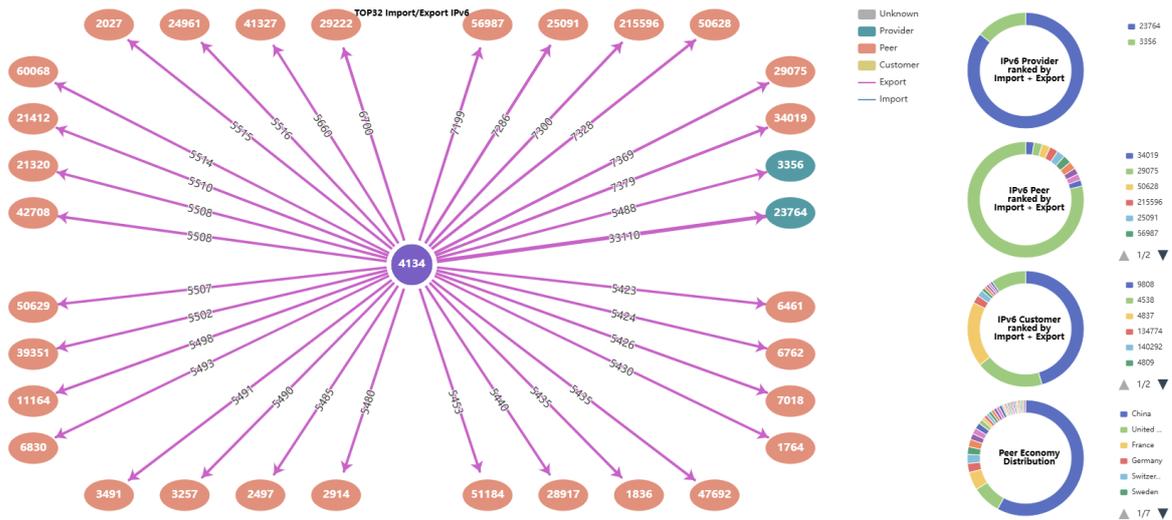
These are hyperlinked and if you click on any of the ASNs, you will be redirected to the dashboard section of that ASN.



	AS neighbors	Organization	Economy/Region	AS customer cone	Relationship	Export	Import
1	174	Cogent Communications	United States	40495	provider	47	105550
2	1292	Arelion Sweden AB	Sweden	41343	provider	95	433678
3	2914	NTT America, Inc.	United States	26526	provider	103	34376
4	3491	PCCW Global, Inc.	United States	11685	provider	93	15564
5	4134	No.31,Jin-rong Street	China	436	provider	2598	14163
6	4635	The Hong Kong Internet Exchange Limited	Hong Kong	1	peer	305	14200
7	4789	Test platform Service Center	China	1	peer	0	1
8	4837	CHINA UNICOM Industrial Internet Backbone	China	262	provider	4899	5151
9	6453	TATA COMMUNICATIONS (AMERICA) INC	United States	20624	provider	64	63388
10	6929	Hurricane Electric LLC	United States	21309	provider	1	0

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.

5. PeeringDB

Ex	ASN	IPv4	IPv6	Speed	Port Location	RS Peer	BF
Equinix Miami	4134	198.32.242.217	2001:504:0:6::4134:1	10G			
LINX LONT: Main	4134	195.66.225.54	2001:718:4::1026:1	100G			
Amy2West	4134	206.72.210.117		10G			
DE-CIX New York: DE-CIX New York	4134	206.82.104.247	2001:504:36::1026:0:1	10G			
AMS-IX	4134	80.249.212.76	2001:718:1::a500:4134:1	20G			
DE-CIX Frankfurt: DE-CIX Frankfurt	4134	80.81.195.33	2001:718::1026:0:2	100G			
AMS-IX	4134	80.249.214.131	2001:718:1::a500:4134:2	100G			
Asteroid Mombasa: Main	4134	195.60.66.29	2001:718:b6:2::1026:1	10G			

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

In the PeeringDB tab, users can check the PeeringDB registration information for AS numbers.

DragonLab | BGPWatch

BGPWatch

User Manual

Section 5 Routing Path



www.bgpwatch.net

Section 5. Routing Path

Introduction

We obtain data from public routing sharing organizations, including Routeviews, RIPE RIS, and CGTF RIS. In the current internet, approximately 1,600 Autonomous Systems (ASes) are willing to act as Vantage Points (VPs) to report their routing information to public platforms. However, this number accounts for only a tiny fraction of the total number of active routing ASes in the internet (about 80,000). Globally, only over 300 VPs share full routing information. Therefore, compared to around 80,000 ASes worldwide, the routing paths visible to over 1,000 VPs in the internet are limited.

If no routing paths are returned for your search, do not panic—this only means the routing paths have not been observed by routing VPs in the internet, not that the routes do not exist.

It includes the following options:

1. Forward Routing Path: Provides the forward routing path to a specified prefix from the selected NREN.
2. Reverse Routing Path: Provides routing paths from other ASes to specific prefixes in the topology and maps them on a geographic map. Operators are typically interested in how traffic is routed to their networks.
3. Bi-Routing Path: Provides both the forward and reverse routing paths between two selected prefixes and displays them on the geographic map.
4. Jitter Route: Identifies the top prefixes and peers with the highest jitter in the network.
5. Daily Bogon: Shows an overview of bogon routes.

Navigating the page

1. Forward Routing Path

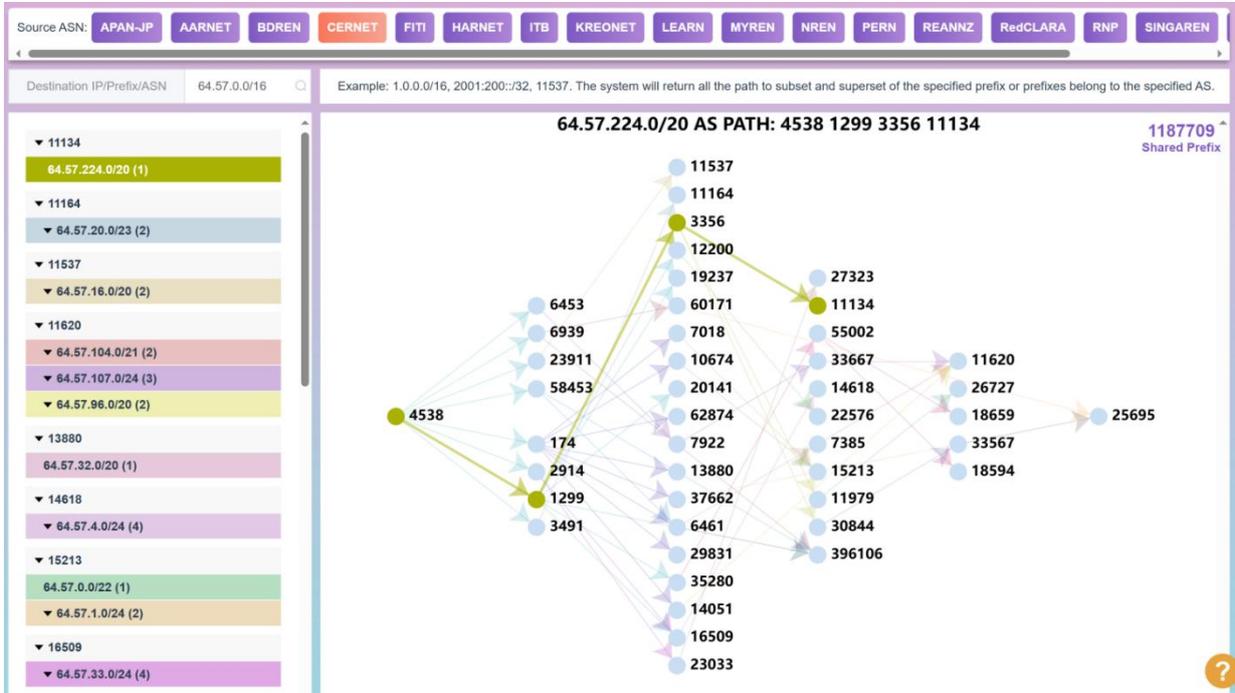
This page displays the forward routes of the source AS that has established a BGP connection with CGTF RIS.

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

Users can first select a source AS. Then input an IP prefix or ASN as the destination. The system will return paths from the specified AS 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 source AS. If the destination is an ASN, the platform will return all the path to all the prefixes belong to the destination AS from the source AS.

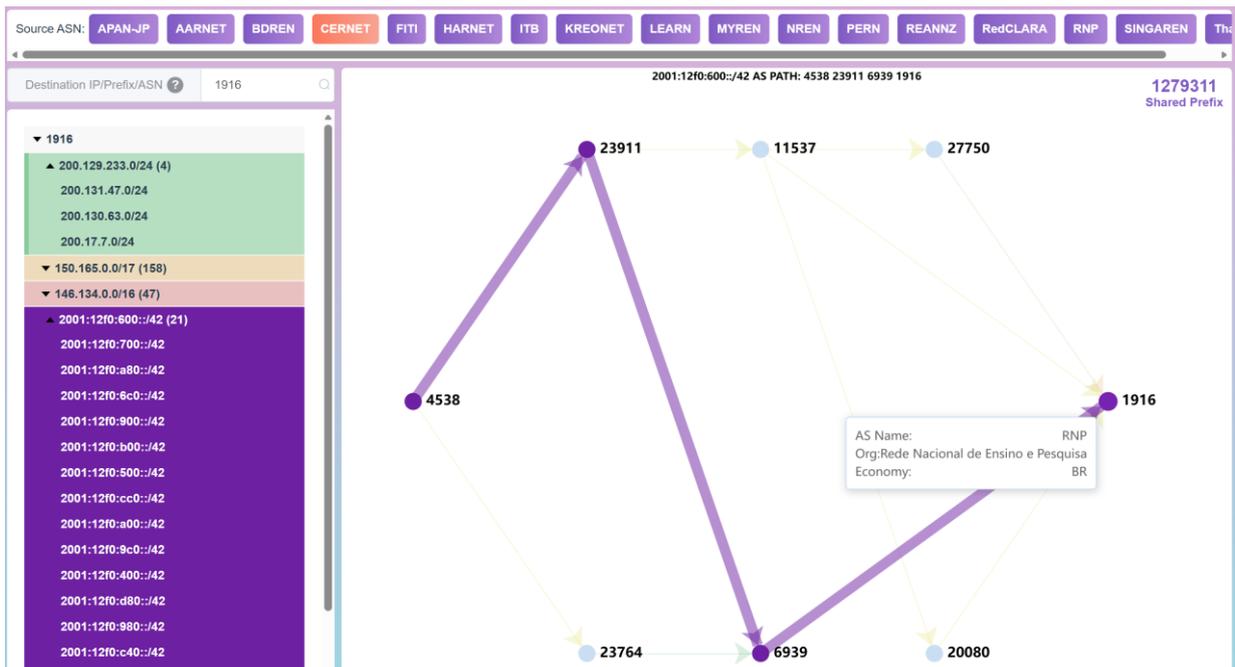
Input an IP prefix as the destination

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.



Input an ASN as the destination

If an ASN is entered as the destination, the left panel still displays all prefixes of that ASN and clusters prefixes with the same path. As shown in the figure, although CERNET and RNP are both R&E (Research and Education) institutions, some prefixes from CERNET to RNP still pass through commercial ISPs.



2. Reverse Routing Path

“Reverse routing path” provides users with routing paths to specific prefixes.



Input Prefix

Takes an "IP prefix" as input. The system searches for the most matching prefix and returns the reverse routing topology mapping on geographic coordinates, with the corresponding topology structure displayed in the top right corner.

View the Prefix Routing Path from a Specific ASN

After entering the prefix, the "From ASN" section will list all ASNs on the routing paths from all vantage points. Additionally, if you want to view the prefix's routing path from a specific AS, you can select one or more ASNs, or click a node on the map or the topology diagram in the top right corner. The corresponding routing path will be highlighted, with detailed information displayed in the bottom right corner.

Click the right arrow or down arrow, and the economic and organizational information of the relevant ASNs will be displayed.

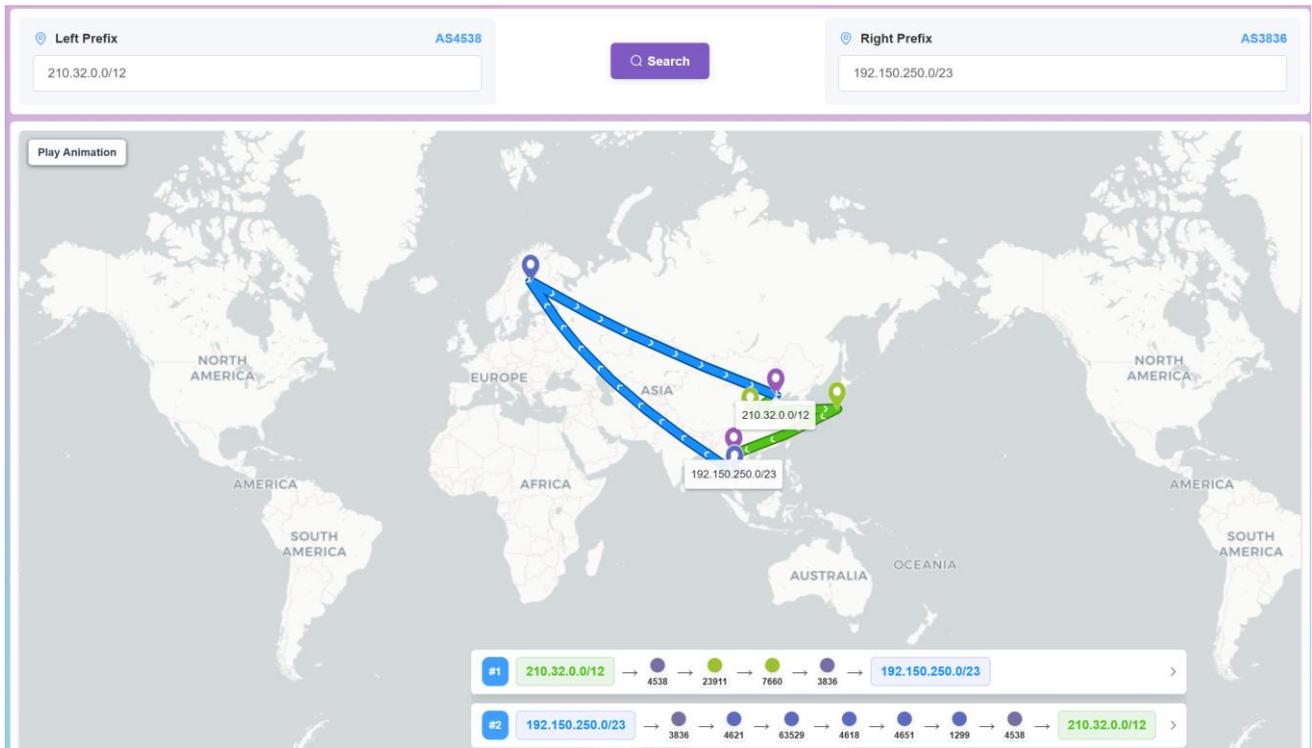
Legend

The legend in the upper left corner indicates the reverse path layers with different colors. You can click on the legend items to increase or decrease the number of layers you want to view.

3. Bi-directional Routing Path

In the search box, you can enter the source prefix in "Left prefix" and the target prefix in "Right prefix". The system will list the corresponding two paths, which may be completely asymmetric. Click the right arrow or down arrow to expand or collapse the corresponding detailed information.

This function is mainly used to help identify potential routing asymmetry or optimize network connections. By visualizing bidirectional paths, users can more intuitively compare the differences between forward and reverse routes and detect issues such as asymmetric routing.



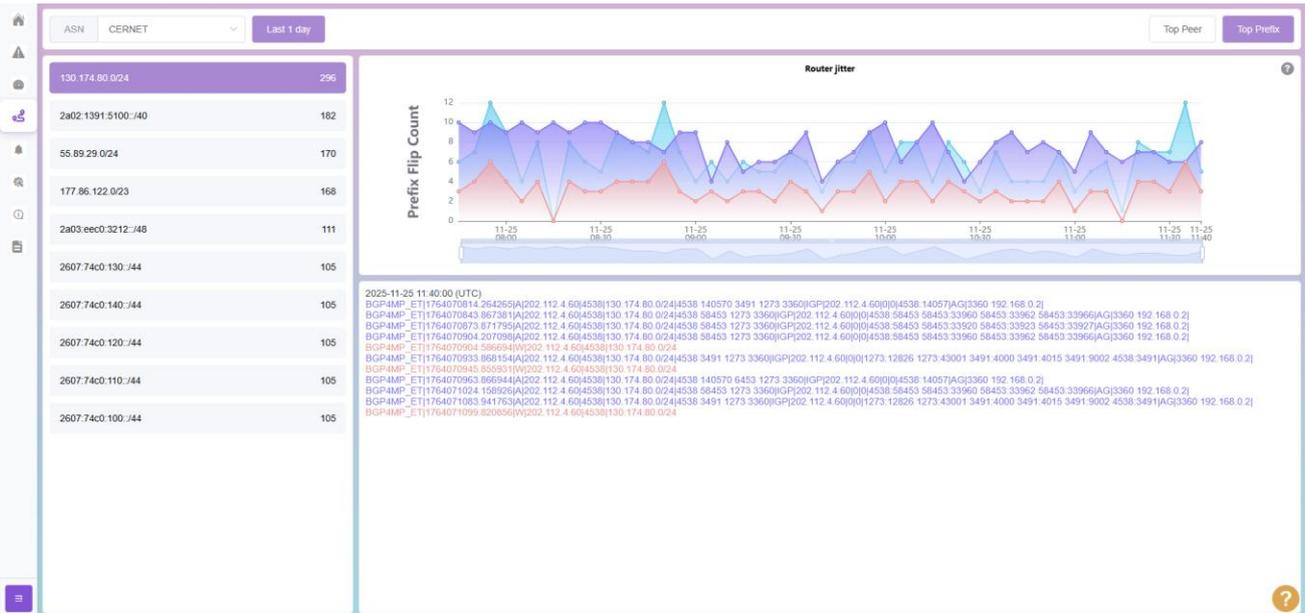
4. Jitter Route

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.



5. Daily Bogan

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.

Search filters: Prefix / ASN / ASN Name / Org Name | Economy / Continent | IPv4 IPv6 | 2025-07-25

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

AS

375

2025/07/25

TopN

1	20
2	30
3	31
4	32
5	34

214174
36911
19462
9341
266037

Economy

59

2025/07/25

TopN

1	88
2	85
3	58
4	47
5	49

United St...
Unknown
Brazil
India
Hong Kong

Org

294

2025/07/25

TopN

1	166
2	39
3	13
4	14
5	11

Unknown
HOSTDAT...
PT Indone...
Network L...
Latitude...

max-prefix

214174 Economy / Continent IPv4 IPv6 2025-07-25

	Prefix	ASN	ASN Name	Org Name	Economy	Continent	Detail
1	102.236.15.0/24	214174	HOSTDATOS-BUSINESS-SERVICES-PVT	HOSTDATOS BUSINESS SERVICES PRIVATE LIMITED	India(IN)	Asia	Detail
2	102.236.24.0/24	214174	HOSTDATOS-BUSINESS-SERVICES-PVT	HOSTDATOS BUSINESS SERVICES PRIVATE LIMITED	India(IN)	Asia	Detail
3	102.236.31.0/24	214174	HOSTDATOS-BUSINESS-SERVICES-PVT	HOSTDATOS BUSINESS SERVICES PRIVATE LIMITED	India(IN)	Asia	Detail
4	102.236.30.0/24	214174	HOSTDATOS-BUSINESS-SERVICES-PVT	HOSTDATOS BUSINESS SERVICES PRIVATE LIMITED	India(IN)	Asia	Detail
5	102.236.36.0/24	214174	HOSTDATOS-BUSINESS-SERVICES-PVT	HOSTDATOS BUSINESS SERVICES PRIVATE LIMITED	India(IN)	Asia	Detail
6	102.236.27.0/24	214174	HOSTDATOS-BUSINESS-SERVICES-PVT	HOSTDATOS BUSINESS SERVICES PRIVATE LIMITED	India(IN)	Asia	Detail
7	102.236.57.0/24	214174	HOSTDATOS-BUSINESS-SERVICES-PVT	HOSTDATOS BUSINESS SERVICES PRIVATE LIMITED	India(IN)	Asia	Detail
8	102.236.29.0/24	214174	HOSTDATOS-BUSINESS-SERVICES-PVT	HOSTDATOS BUSINESS SERVICES PRIVATE LIMITED	India(IN)	Asia	Detail

BGPWatch

User Manual

Section 6 Tools



Section 6. Tools

Introduction

This section aims to provide the AS topology for a specific economy or region.

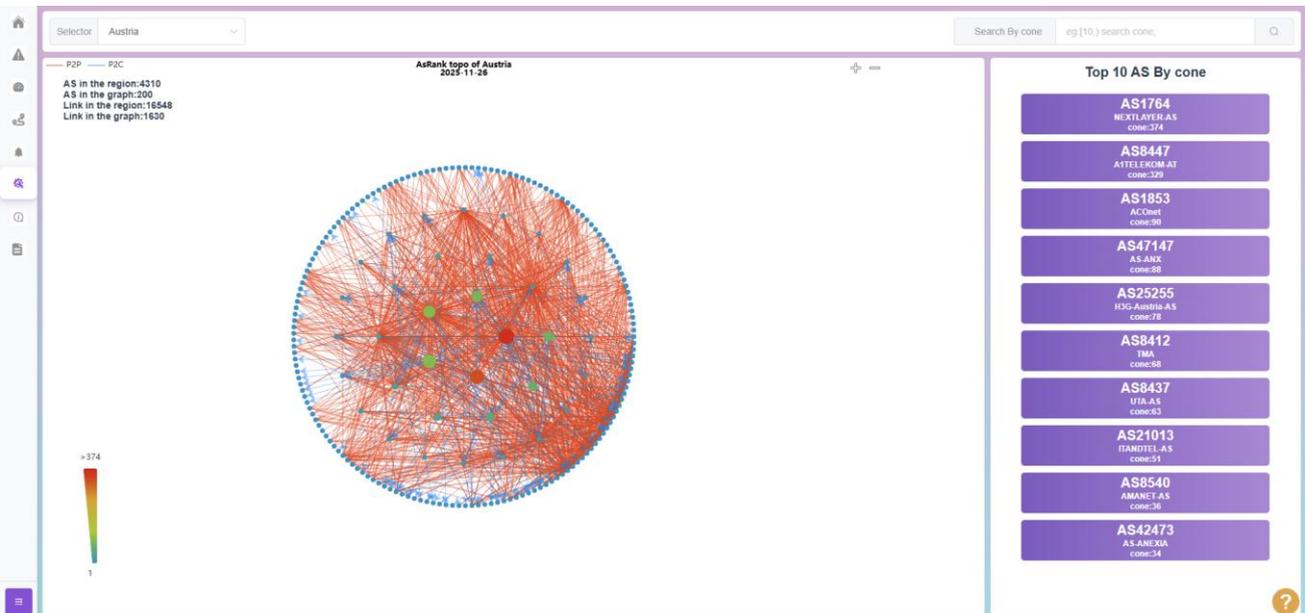
Navigating the Page

1. Economy/Region

The Economy/Region section tries to give a 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.

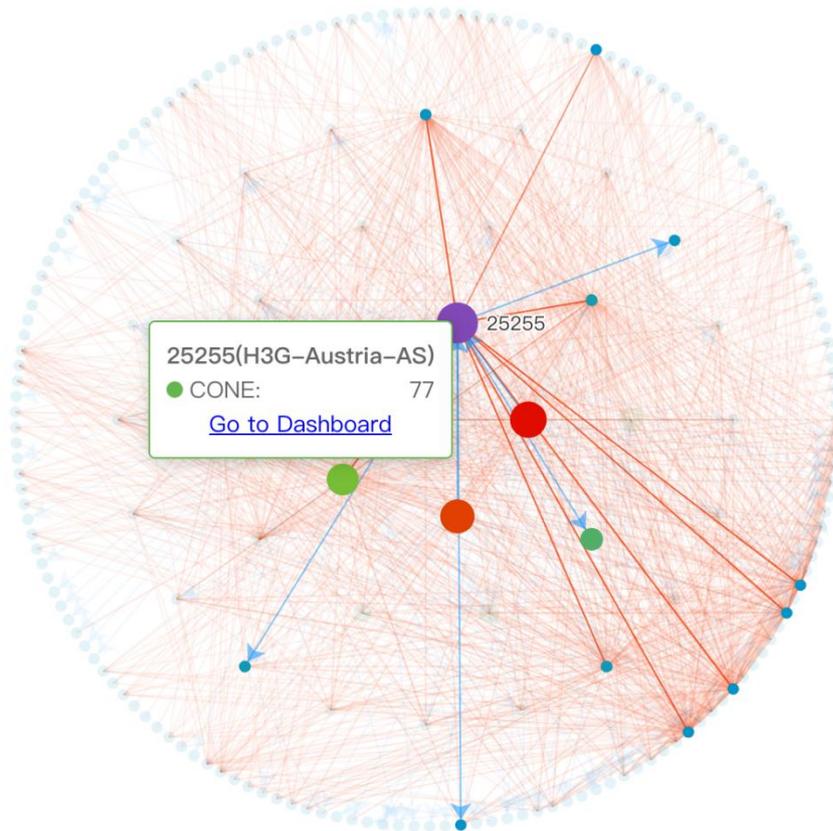
After user select an economy or region and the cone range, a topology graph of the economy or region will be shown.



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.

DragonLab | BGPWatch

BGPWatch

User Manual

Section 7 Subscription



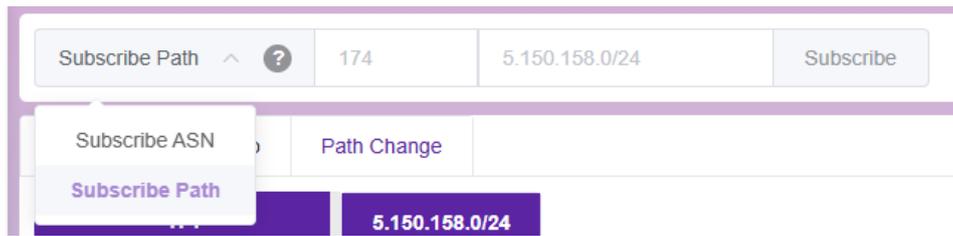
www.bgpwatch.net

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



Toggle Between the Two Modes

Click the dropdown list in the upper left corner to select either mode.

Subscribe AS Mode

In Subscribe AS Mode, users can enter an ASN expression in the input box to add one or more ASNs. Examples include:

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

Subscribe Prefix Mode

In this mode, users can enter an ASN and a prefix to complete the subscription.



After subscribing to an ASN/Prefix, the system will automatically add it to position [A] for display. You can select different ASNs/Prefixes by clicking on them.

Position [B] features a set of buttons, arranged from left to right as follows:

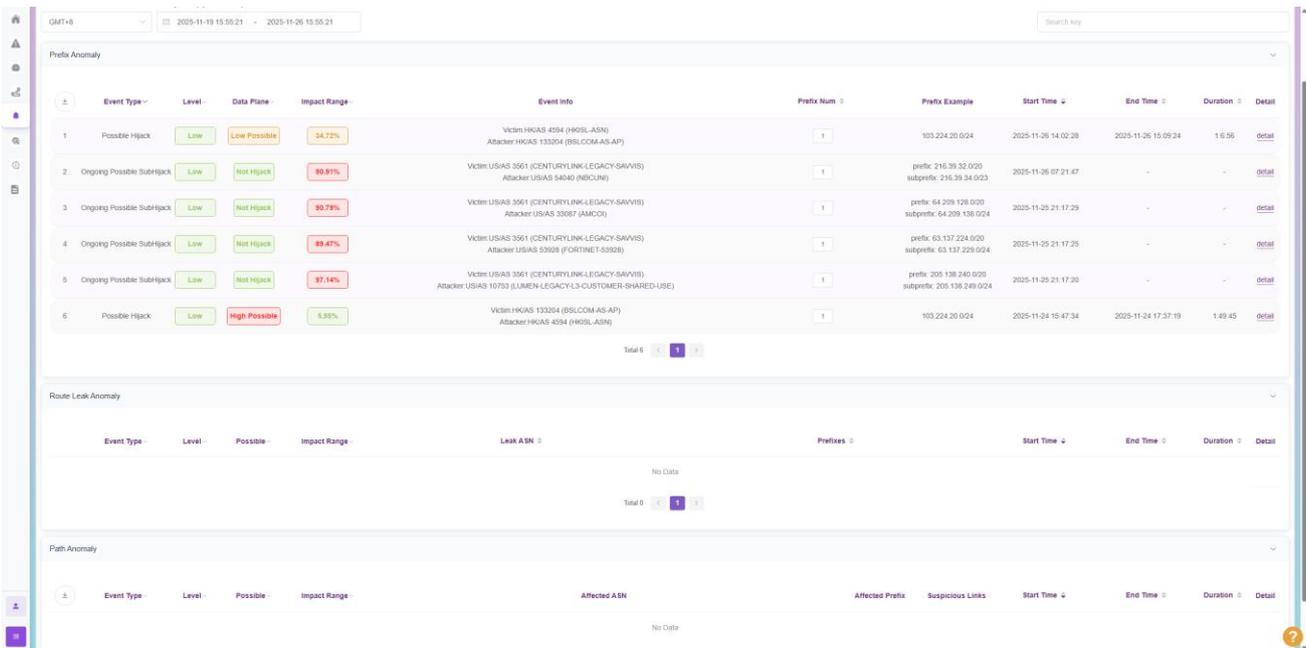
1. Delete: Click this button to select one or more ASNs/Prefixes via the dropdown box and remove them from the subscription list.
2. Export Weekly Report: Click this button to select one or more ASNs via the dropdown box. Relevant content of the selected ASNs will be included in the exported document.
3. Email Settings: Used to configure whether to send email notifications when a specified hijacking occurs and triggers an alert.

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

1. Anomaly
2. AS Info
3. Path Change

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

1. Anomaly



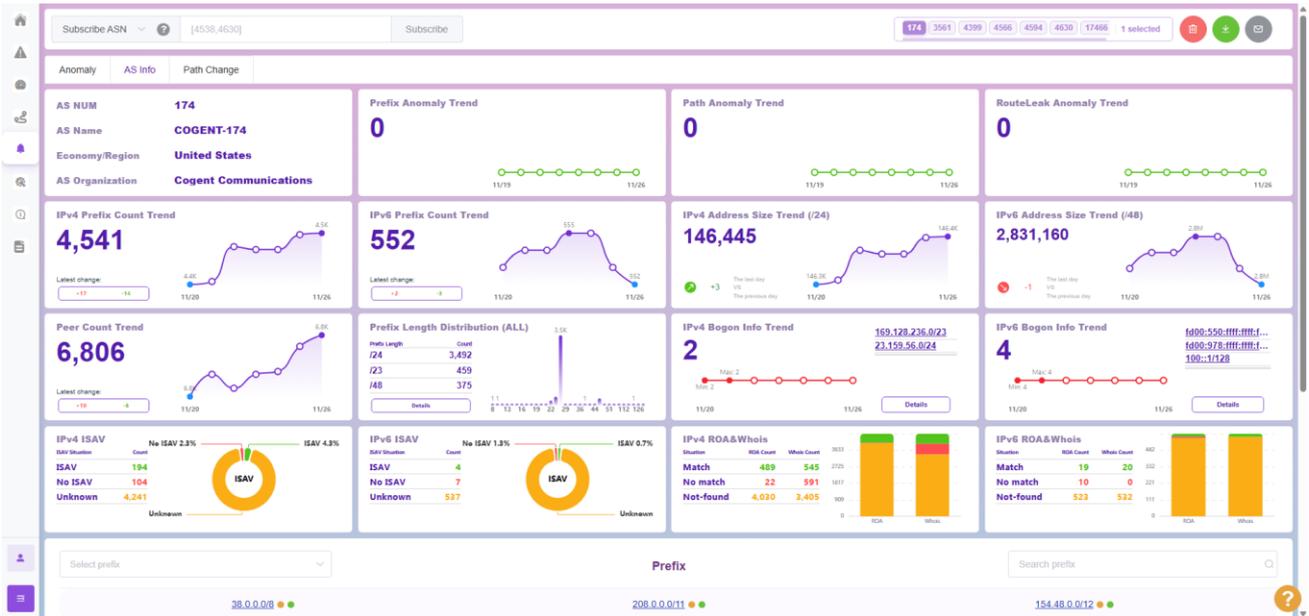
#	Event Type	Level	Data Plane	Impact Range	Event Info	Prefix Num	Prefix Example	Start Time	End Time	Duration	Detail
1	Possible Hijack	Low	Low Possible	34.72%	Victim HKAS 4594 (HQSLS-ASN) Attacker HKAS 133004 (BSL.COM-AS-AP)	1	103.224.20.0/24	2025-11-26 14:02:28	2025-11-26 15:09:24	1:6:56	detail
2	Ongoing Possible Subhijack	Low	Not Hijack	90.91%	Victim USAS 3561 (CENTURYLINK-LEGACY-SAVVIS) Attacker USAS 54040 (NBCUN)	1	prefix: 216.39.32.0/20 subprefix: 216.39.34.0/23	2025-11-26 07:21:47	-	-	detail
3	Ongoing Possible Subhijack	Low	Not Hijack	90.79%	Victim USAS 3561 (CENTURYLINK-LEGACY-SAVVIS) Attacker USAS 33087 (AMCO)	1	prefix: 64.209.128.0/20 subprefix: 64.209.138.0/24	2025-11-25 21:17:29	-	-	detail
4	Ongoing Possible Subhijack	Low	Not Hijack	89.47%	Victim USAS 3561 (CENTURYLINK-LEGACY-SAVVIS) Attacker USAS 53928 (FORTINET-53928)	1	prefix: 63.137.224.0/20 subprefix: 63.137.229.0/24	2025-11-25 21:17:25	-	-	detail
5	Ongoing Possible Subhijack	Low	Not Hijack	97.14%	Victim USAS 3561 (CENTURYLINK-LEGACY-SAVVIS) Attacker USAS 10753 (LUMEN-LEGACY-3-CUSTOMER-SHARED-USE)	1	prefix: 205.138.240.0/20 subprefix: 205.138.249.0/24	2025-11-25 21:17:20	-	-	detail
6	Possible Hijack	Low	High Possible	5.95%	Victim HKAS 133004 (BSL.COM-AS-AP) Attacker HKAS 4594 (HQSLS-ASN)	1	103.224.20.0/24	2025-11-24 15:47:34	2025-11-24 17:37:19	1:49:45	detail

Total 6

In the Anomaly tab, users can check if there are any hijacking incidents and their details among the subscribed and selected ASNs. When an abnormal incident occurs and the user’s configuration allows email notifications, the user will receive an email alert.

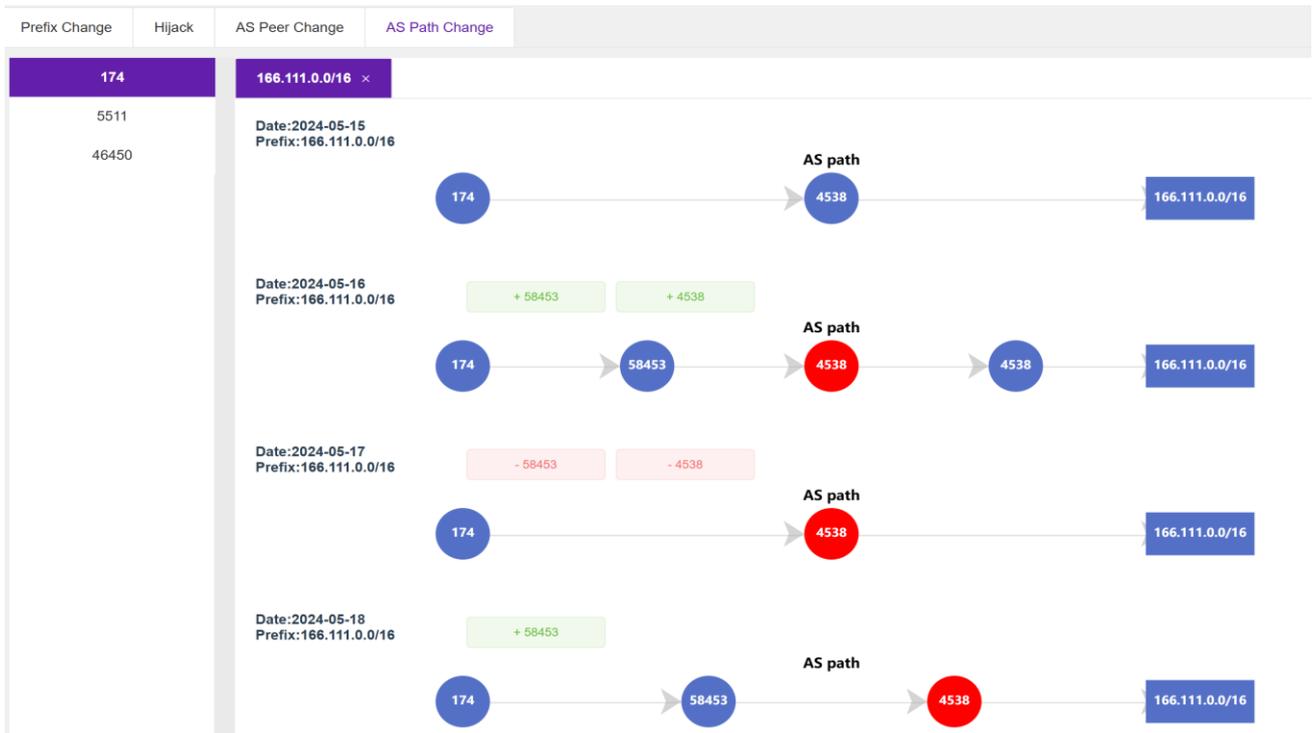
2. AS Info

The AS Info tab displays the custom content configured by users in the Dashboard. The interaction method is consistent with that in the Dashboard menu. Users can click any ASN shown in the top right corner, and the corresponding AS information will be displayed in this tab.



3. Path Change

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



The corresponding ASNs are listed on the left side, and the corresponding prefixes are displayed in tabs on the right. The system shows the AS Path information for the past seven days.

When an administrator pays close attention to changes in a specific routing path, or when their configuration modifications may affect certain routing paths, they can add a subscription for the corresponding paths here.

BGPWatch

User Manual

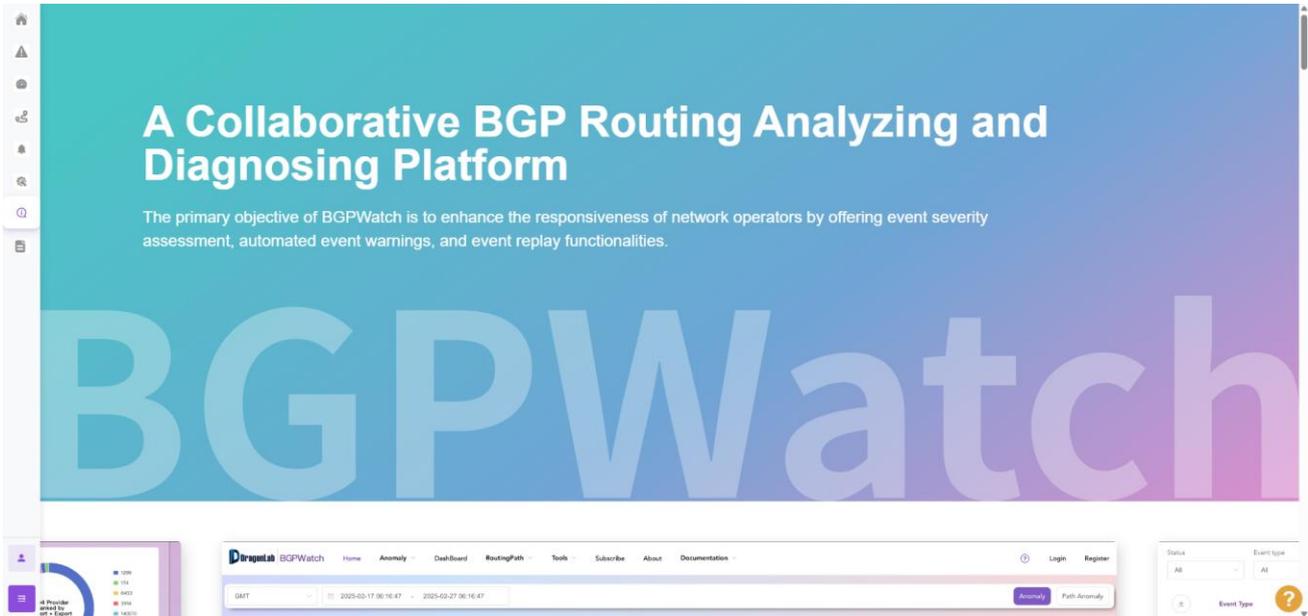
Section 8 About



Section 8. About

Introduction

This page provides an overview of the main functions of the system.



BGPWatch

User Manual

Section 9 Documentation



Section 9. 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.

DragonLab | BGPWatch

BGPWatch

User Manual

Section 10 Appendix



www.bgpwatch.net

Section 10. Appendix

1. Data Sources and Retrieval Periods

The system retrieves data from multiple sources—including routing platforms (Routeviews, RIPE RIS, CGTF RIS), ROA, WHOIS/RIR registries, CAIDA datasets, and PeeringDB—with retrieval methods varying between real-time and periodic, as detailed in Table 1.

Table 1. Data Sources and Retrieval Periods

Data Source	Retrieval Periods
Routing data (Routeviews, RIPE RIS, CGTF RIS)	Real time
ROA (Route Origin Authorization)	Real time
WHOIS, RIR (Regional Internet Registry)	00:30 UTC daily
CAIDA Data (AS Relation, AS Name, Org)	00:30 UTC daily
PeeringDB	00:30 UTC daily

2. Data Processing Frequencies

The system processes data either in real time or periodically: tasks such as anomaly detection are updated in real time, while Routing Path/Prefix/BGP Connection Updates are handled daily, as shown in Table 2.

Table 2. Data Processing Frequencies

Data Processing	Updates Frequencies
Anomaly Updates	Real time
Routing Path Updates / Prefix Updates / Peers Updates/	Retrieves routing data at 00:30 UTC daily and finishes processing by 04:00 UTC

Bogon Routing Updates	Retrieves Bogon Prefixes from bgp.he.net at 00:30 UTC daily and finishes processing by 04:00 UTC
Source Address Spoofing Detection	Not regular; updated every several months

3. CGTF RIS

CGTF RIS is a routing information sharing platform, similar to Routeviews and RIPE RIS, that has established BGP sessions with 17 partners. Data from this platform is accessible via the URL: <https://bgp.cgtf.net>.

Two collectors have been deployed. Establishing peer connectivity with one of the CGTF collectors is sufficient—please feel free to choose and connect to any one.

Below is the collector information:

- **Collector ASN:** 65534
- 1. Collector 1 (Hosted in HARNET)**
 - IPv4 address: 203.188.118.90
 - IPv6 address: 2001:ce0:1:2::3
 - 2. Collector 2 (Hosted in CERNET)**
 - IPv4 address: 203.91.121.227
 - IPv6 address: 2001:da8:217:1213::227