

(APNIC ISIF Project)

**An Extension of the Ongoing Project
“Developing a Collaborative BGP Routing Analyzing
and Diagnosing Platform” Project**

Technical Report

**Tsinghua University
November 19th, 2024**



Contents

◎ Updates

- ◎ Developed data plan detection method
- ◎ Developed path hijacking detection method
- ◎ Finished middle project report

◎ Future Work Plan

- ◎ Continue software development
- ◎ Continue community development
- ◎ Continue to secure new funds

◎ Demo of New Functions

Data Plan Detection

| Probe AS | Economy | Time(UTC) | From | Min RTT | Packet Loss |
|----------|---------|--------------------------|-----------------|----------|-------------|
| AS34549 | | 2024-11-06T03:45:12.000Z | 185.150.98.36 | No reply | 100.00% |
| AS49420 | | 2024-11-06T03:45:12.000Z | 91.212.242.241 | No reply | 100.00% |
| AS17639 | | 2024-11-06T03:45:14.000Z | 161.49.13.234 | No reply | 100.00% |
| AS3333 | | 2024-11-06T03:45:12.000Z | 193.0.0.165 | No reply | 100.00% |
| AS48362 | | 2024-11-06T03:45:12.000Z | 94.199.170.201 | No reply | 100.00% |
| AS204092 | | 2024-11-06T03:45:13.000Z | 80.67.190.218 | No reply | 100.00% |
| AS49673 | | 2024-11-06T03:45:12.000Z | 94.247.111.19 | No reply | 100.00% |
| AS34800 | | 2024-11-06T03:45:12.000Z | 194.50.99.201 | No reply | 100.00% |
| AS1403 | | 2024-11-06T03:45:12.000Z | 198.16.163.75 | 13.81ms | 0.00% |
| AS20205 | | 2024-11-06T03:45:12.000Z | 38.67.212.178 | 16.77ms | 0.00% |
| AS7018 | | 2024-11-06T03:45:14.000Z | 162.225.60.96 | 22.56ms | 0.00% |
| AS3549 | | 2024-11-06T03:45:13.000Z | 66.162.17.4 | 23.65ms | 0.00% |
| AS1299 | | 2024-11-06T03:45:12.000Z | 62.115.192.103 | 27.96ms | 0.00% |
| AS13830 | | 2024-11-06T03:45:12.000Z | 161.129.155.179 | 41.25ms | 0.00% |
| AS3356 | | 2024-11-06T03:45:13.000Z | 4.8.13.234 | 42.41ms | 0.00% |

- Choose probes in certain ASes
- Choose destinations from the hijacked prefixes
- Do Probing
- Calculate Correlation Coefficient

Correlation Coefficient:

$$r(X, Y) = \frac{Cov(X, Y)}{\sqrt{Var[X] Var[Y]}}$$

- Vector X:
For each prober, set to 0 if located in the affected AS; otherwise, set to 1.
- Vector Y:
For probe result from each prober, set to 1 if reachable; otherwise, set to 0.

Anomaly – Detail

DragonLab BGPWatch Home Anomaly DashBoard RoutingPath Tools Subscribe Documentation Login Register

Harm Level: **Middle Level**

108.165.54.0/24-HIJACK1730844054 Possible Hijack Events

Range of Impact: **87.18%**

Data Plane Detection: **High Possible**

Victim AS: [32780](#) Hijacker AS: [834](#) Start Time (UTC): 2024-11-05 22:00:54
Victim Economy: US (United States) Hijacker Economy: US (United States) End Time (UTC): 2024-11-07 14:10:47
Victim AS Name: HOSTINGSERVICES-INC Hijacker AS Name: IPXO During Time: 40:9:53

Reason: ● (834, 108.165.54.0/24) doesn't align in ROA ● (32780, 108.165.54.0/24) doesn't align in ROA ● (834, 108.165.54.0/24) doesn't align in WHOIS ● (32780, 108.165.54.0/24) aligns in WHOIS

Prefix Info: [108.165.54.0/24](#)

| Target | Data Plane Detection | Correlation Coefficient |
|--------------|--------------------------|-------------------------|
| 108.165.54.2 | 2024-11-05T22:02:15.000Z | 1.00 > |
| 108.165.54.3 | 2024-11-05T22:02:16.000Z | 1.00 > |
| 108.165.54.2 | 2024-11-06T03:45:12.000Z | 0.76 > |
| 108.165.54.3 | 2024-11-06T03:45:12.000Z | 0.76 > |
| 108.165.54.3 | 2024-11-06T23:15:11.000Z | 0.17 > |
| 108.165.54.2 | 2024-11-06T23:15:11.000Z | 0.17 > |

Overall Correlation Coefficient: 0.752

• Data Plane Detection

- Not Done:
No measurable target found
- No Result:
Probed, but received no results
- Not Hijack:
Correlation Coefficient = 0
- Low Possible:
Correlation Coefficient < 0.6
- High Possible:
Correlation Coefficient ≥ 0.6

Anomaly

DragonLab | BGPWatch Home Anomaly Dashboard RoutingPath Tools Subscribe Documentation

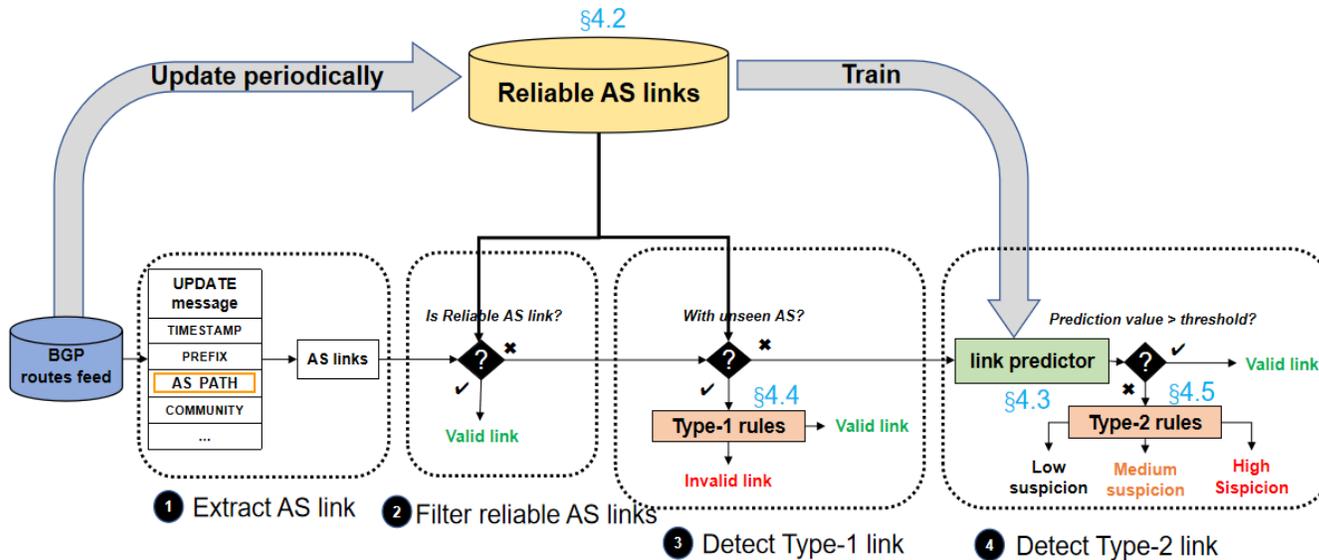
Status: All Event type: All Harm level: All Data plane: All Impact Ra: All

| ↓ | Event Type | Level | Data Plane | Impact Range | Event Info | Detail |
|---|-------------------------|-------|---------------|--------------|--|------------------------|
| 1 | Possible Hijack | Low | Not Done | 10.26% | Victim:CN/AS63673(PINGANC Attacker:UA/AS48031(XServe | detail |
| 2 | Possible Hijack | Low | High Possible | 10.45% | Victim:LT/AS212609(Internet- Attacker:US/AS55081(24SHEL | detail |
| 3 | Ongoing Possible Hijack | Low | High Possible | 16.88% | Victim:LT/AS200017(Ecoland Attacker:US/AS55081(24SHEL | detail |
| 4 | Ongoing Possible Hijack | Low | No Result | 44.26% | Victim:/AS213990() Attacker:US/AS3356(LEVEL: | detail |

- **Impact Range**

- <10%: Fewer than 10% of ASNs in the replay path are affected.
- >=10%: More than 10% of ASNs in the replay path are affected.
- >=50%: More than 10% of ASNs in the replay path are affected.

Path Anomaly Detection: Combining Link Prediction and Rules



- Link prediction is used to find suspicious unseen links, and rules are used to improve the confidence level.
- Two Type Events:
 - New Link: New and Suspicious Link
 - New AS: New and Suspicious AS

- Possible
 - Low Possible: Confidence level < 0
 - Middle Possible: Confidence level = 0
 - High Possible: Confidence level > 0

| Reason | Confidence level |
|--|------------------|
| new link | |
| AS-PATH is too long | +1 |
| The last hop is single-digital ASN | +1 |
| The edit distance of ASNs in the link is 1 | +1 |
| There exists loop in the AS-PATH and the suspicious link is in the loop. | +1 |
| The AS-PATH violates valley-free rule:'({a},{b},{c}). | +1 |
| Domestic traffic ({country},{asn1},{asn2}) detour. | +1 |
| Suspicious links is at the end of the AS-PATH and a domestic link ({irr_dict.get(self._u)}). | -4 |
| Suspicious links is same country ({irr_dict.get(self._u)}). | -2 |
| new as | |
| ASN{asn} is not registered.(new AS) | +1 |
| ASN{asn} is reserved ASN.(new AS) | +1 |
| ASN{asn} is not the last hop.(new AS) | +1 |

Path Anomaly

| | Event Type | Level | Possible | Impact Range | Event Info | Prefix Num | Example Prefix | Start Time |
|----|---------------------|-------|---------------|--------------|--|------------|-----------------|------------------------|
| 61 | Ongoing New Link | Low | Low Possible | <=1 path | New Link: 11014(AR) -> 269818(AR) Reason:The suspicious link is at the end of the AS-PATH and is a domestic link (AR) | 1 | 45.184.152.0/24 | 2024-11-13 15:05:30 |
| 62 | Ongoing New AS | Low | High Possible | >5 path | New AS: 31196 Reason:ASN31196 is not the last hop | 1 | 202.36.221.0/24 | 2024-11-13 14:40:48 |
| 63 | Ongoing New Link | Low | Low Possible | <=1 path | New Link: 32307(US) -> 400707(US) Reason:The suspicious link is at the end of the AS-PATH and is a domestic link (US) | 1 | 38.109.250.0/24 | 2024-11-13 14:29:20 |
| 64 | Ongoing New Link | Low | High Possible | <=1 path | New Link: 58212(DE) -> 214309(GB) Reason:Detour of domestic traffic (34854,GB) (1299,SE) (199524,LU) (58212,DE) (214309,GB) | 1 | 45.151.91.0/24 | 2024-11-13 14:14:44 |
| 65 | Finish New Link | Low | Low Possible | <=1 path | New Link: 52863(BR) -> 264485(BR) Reason:The suspicious link is at the end of the AS-PATH and is a domestic link (BR) | 1 | 189.91.147.0/24 | 2024-11-13 14:10:47 |

Path Anomaly Detail – Suspicious New Link

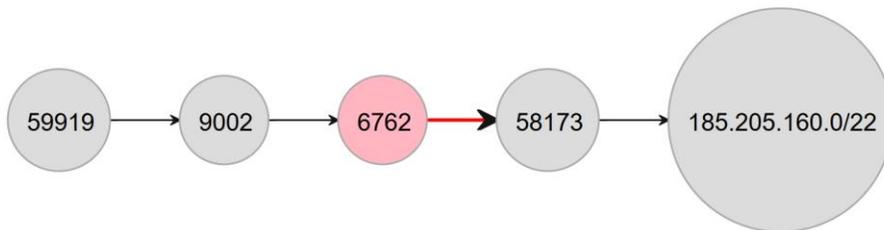
| | | | |
|-----------------|--|----------------------------------|---------------------------------------|
| Harm Level | AS6762-AS58173-TYPE2-1731344495 New Link Events | | |
| Low | Suspicious AS: 6762 | Victim AS: 58173 | Start Time (UTC): 2024-11-12 01:01:35 |
| Range of Impact | Suspicious Economy: IT | Victim Economy: GB | End Time (UTC): 2024-11-12 01:26:35 |
| <=1 path | Suspicious AS Name: SEABONE-NET | Victim AS Name: ONWAVE | Duration: 0:25:0 |
| Possible | | | |
| High Possible | | | |

Time Lines:

Reason: Detour of domestic traffic (58173,GB) (6762,IT) (9002,GB)

Prefix Info: 185.205.160.0/22

Reason:
Detour of domestic traffic
(58173,GB) (6762,IT) (9002,GB)



The suspicious AS and link are marked red.

Path Anomaly Detail – Suspicious New AS

Harm Level: **High**

Range of Impact: **>5 path**

Possible: **High Possible**

AS61974-TYPE1-1731583577 New AS Events

| | | |
|--------------------------------------|-------------------------|---------------------------------------|
| Suspicious AS: 61974 | Prefix Count: 1 | Start Time (UTC): 2024-11-14 19:26:16 |
| Suspicious Economy: IR | Path Count: 13 | End Time (UTC): - |
| Suspicious AS Name: LOTUSNET | Possible: High Possible | Duration: - |

Reason: **ASN61974 is not the last hop**

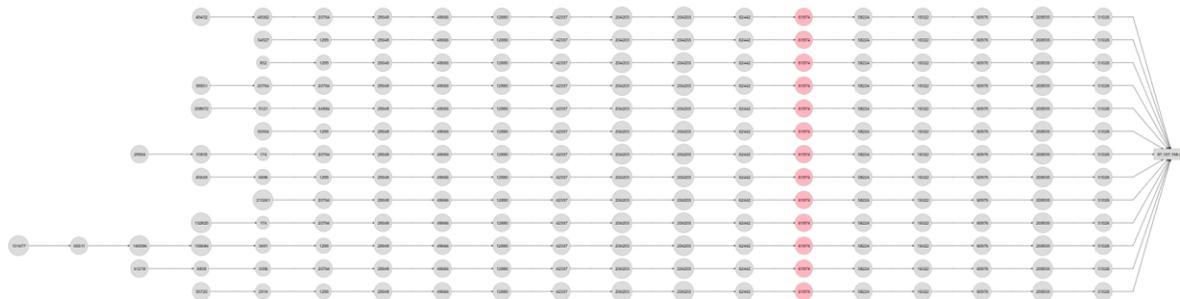
Prefix Info: [87.107.166.0/24](#)

Website: [looksfle.com](#) [optimist.style](#) [mimt.gov.ir](#) [seanalisa.shop](#) [m0nalisa.ir](#) [karafariniomid.ir](#)

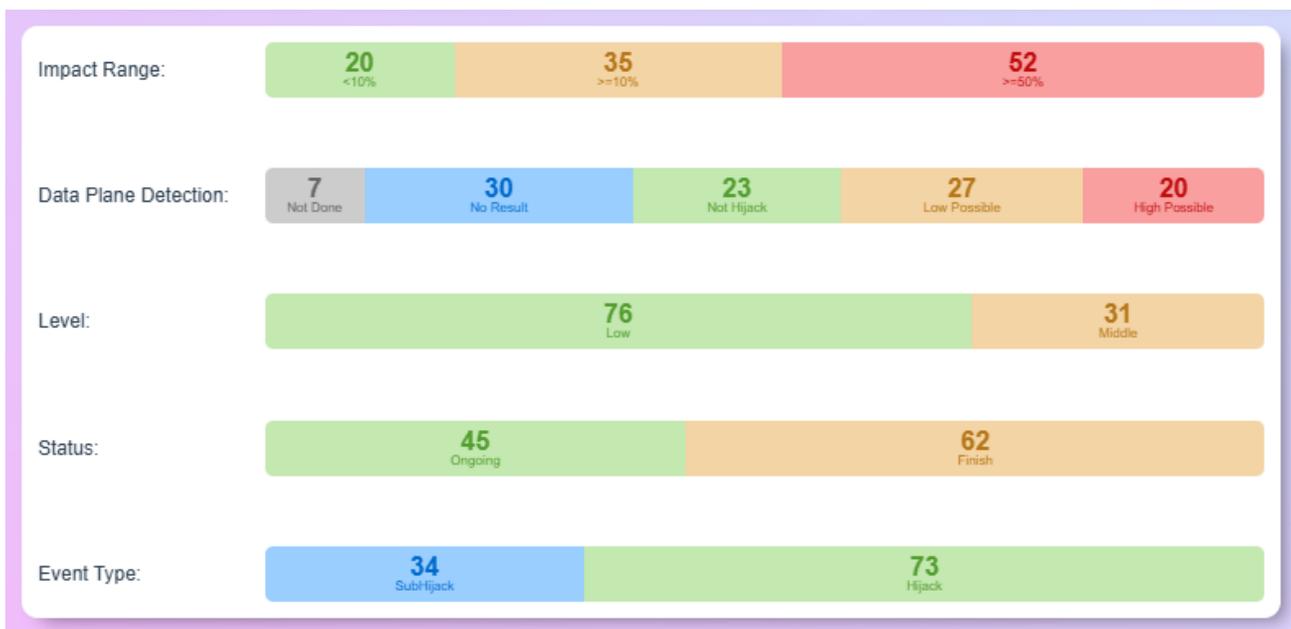
Reason:
ASN61974 is not the last hop.

87.107.166.0/24

All the paths affected.



Homepage



- Impact Range
 - <10%, >=10%, >=50%
- Data Plane Detection
 - Not Done, No Result, Not Hijack, Low Possible, High Possible
- Level
 - Low, Middle, High
- Status
 - Ongoing, Finish
- Event Type
 - Subhijack, Hijack

Dashboard

Basic IPv4 Peers IPv6 Peers Whois Last Update: 2024-10-31

AS NUM
4538

AS Name
ERX-CERNET-BKB

Economy/Region
China

AS Organization
China Education and Research Network Center

| prefix Length | Count |
|---------------|-------|
| /24 | 1,499 |
| /20 | 1,245 |
| /21 | 675 |

IPv4 Prefix

| prefix Length | Count |
|---------------|-------|
| /32 | 4,184 |
| /48 | 1,600 |
| /64 | 8 |

IPv6 Prefix

IPv4 Prefix Count
5,160

+1 The last day VS The previous day

IPv6 Prefix Count
5,807

0 The last day VS The previous day

IPv4 Bogon
0

0 The last day VS The previous day

IPv6 Bogon
0

0 The last day VS The previous day

IPv4 Address Size (/24)
165,193

+1 The last day VS The previous day

IPv6 Address Size (/48)
274,352,768

0 The last day VS The previous day

IPv4 Bogon

✔ No Bogon issues exist with the IPv4 addresses of this AS.

IPv6 Bogon

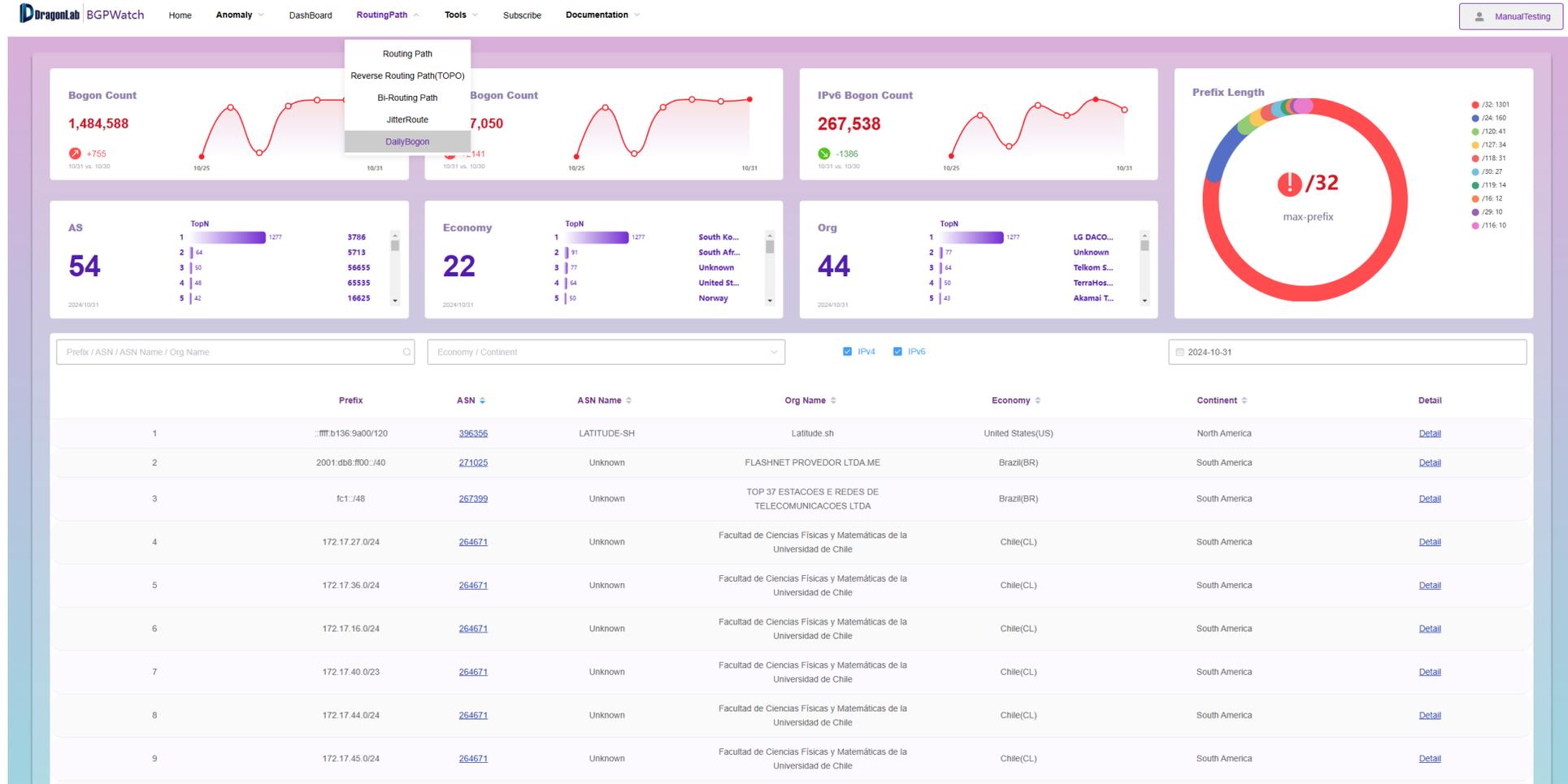
✔ No Bogon issues exist with the IPv6 addresses of this AS.

Select prefix

| Prefix | Status |
|----------------|--------|
| 202.192.0.0/12 | ●● |
| 222.192.0.0/12 | ●● |
| 202.112.0.0/13 | ●● |
| 211.80.0.0/13 | ●● |
| 58.200.0.0/13 | ●● |
| 210.32.0.0/12 | ●● |
| 222.16.0.0/12 | ●● |
| 202.200.0.0/13 | ●● |
| 219.216.0.0/13 | ●● |
| 218.192.0.0/13 | ●● |
| 58.192.0.0/12 | ●● |
| 59.64.0.0/12 | ●● |
| 202.192.0.0/13 | ●● |
| 125.216.0.0/13 | ●● |
| 222.24.0.0/13 | ●● |

Search prefix

Routing Path – Daily Bogon



Support searching by continent, economy, and ASN

Future Work Plan

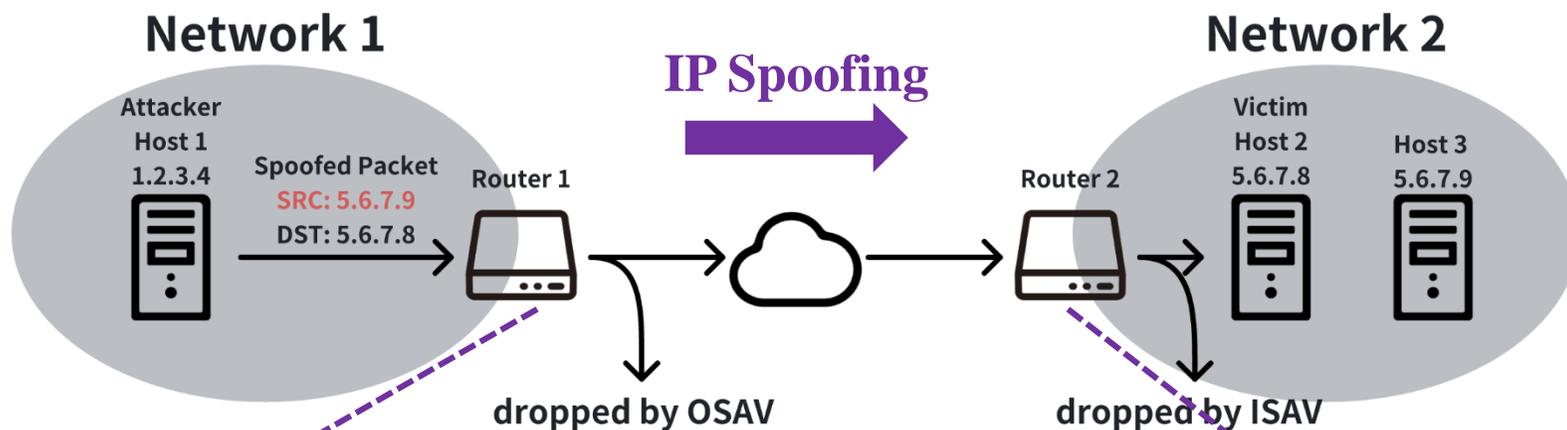
| Objectives | Work Plan | Tentative Timeline |
|---|---|--|
| Develop an integrated Looking Glass platform | Find obscure Looking Glass VP regularly | Dec. 2023 Done |
| | Develop integrated Looking Glass platform | Feb. 2024 Done |
| | Develop Looking Glass API | Mar. 2024 Done |
| Use Looking Glass to further check routing hijacking at the data plan | Develop data plan detection method and decision algorithm | June 2024 Done |
| | Integrate the algorithm to the system | Aug. 2024 Done |
| Implement path hijacking detection and routing leak detection methods | Develop path hijacking detection method | Nov. 2024 Done |
| | Develop routing leak detection method | Jan. 2025 |
| Continue to maintain and fix bugs in the BGPWatch platform | Continually test and get suggestions from user | Throughout the entire project duration |
| Continue community development and engagement, and international collaboration | The second phase of the project (Dec.06, 2023 – June 06, 2025 (18 months)) Welcome new partners to join! | Throughout the entire project duration |

Continue to Secure New Funds

- ◎ Two topics are considered:
 - ◎ Source Address Validation deployment measurement
 - ◎ Achieving realistic routing policy through multiple resources

Source Address Validation (SAV)

- **IP spoofing:** Use fake source address for attack
- **SAV:**
 - Filter spoofed packets
 - Defined in RFC 2827 (BCP 38) and RFC 3704 (BCP 84)



- **OSAV:**

- Filter outbound packets
- Block the source of an attack

- **ISAV:**

- Filter inbound packets
- Protect victims

ISAV Deployment Measurement

- Two novel methods
 - **ICMP unreachable method**
 - **ICMP fragmentation method**
- **Goal:** Send “**Rumors**” to find the “**Wise**”

↓
Spoofed ICMP Messages

↓
Networks with ISAV

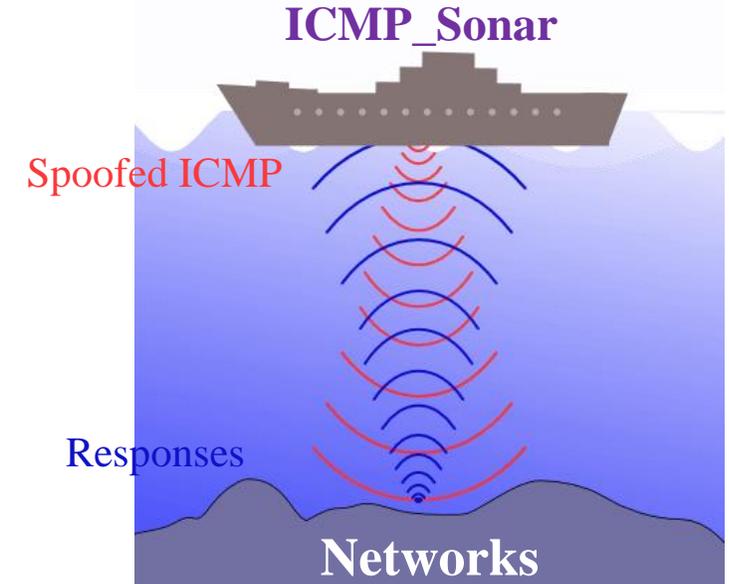
ICMP unreachable method

- Supported by a wider range of target operating systems

ICMP fragmentation method

- Does not require an open TCP port of the target

↘
Complementary

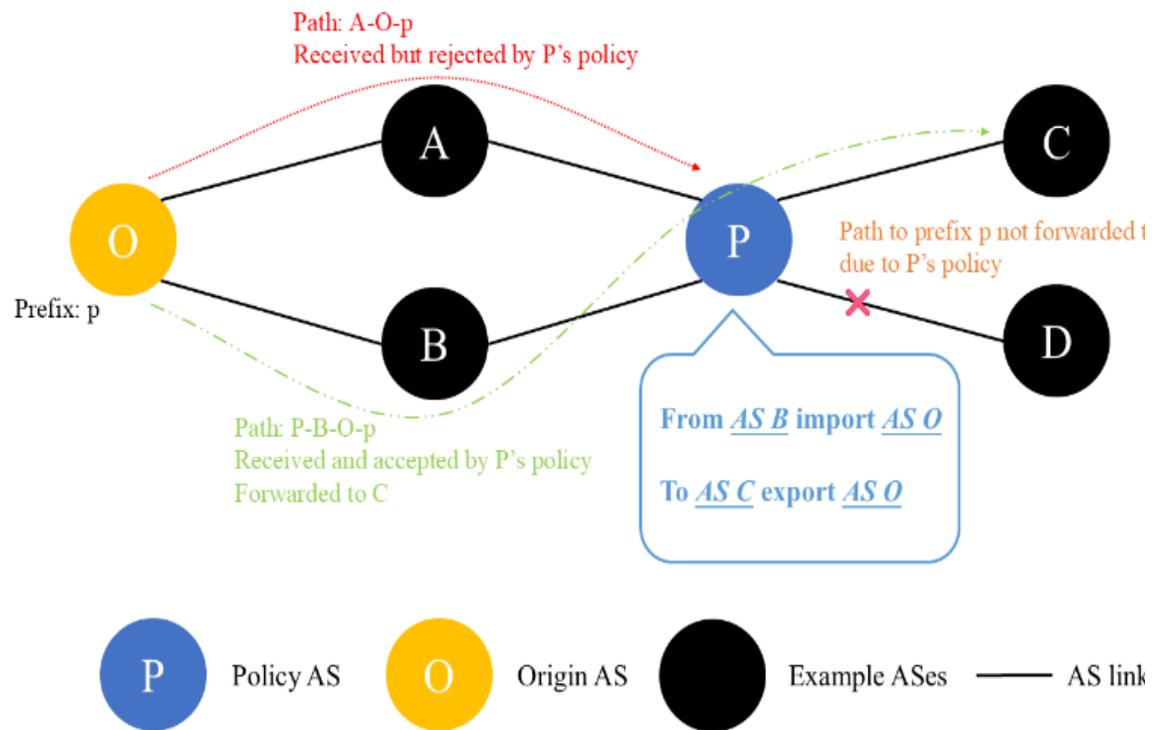


ISAV Detection Results

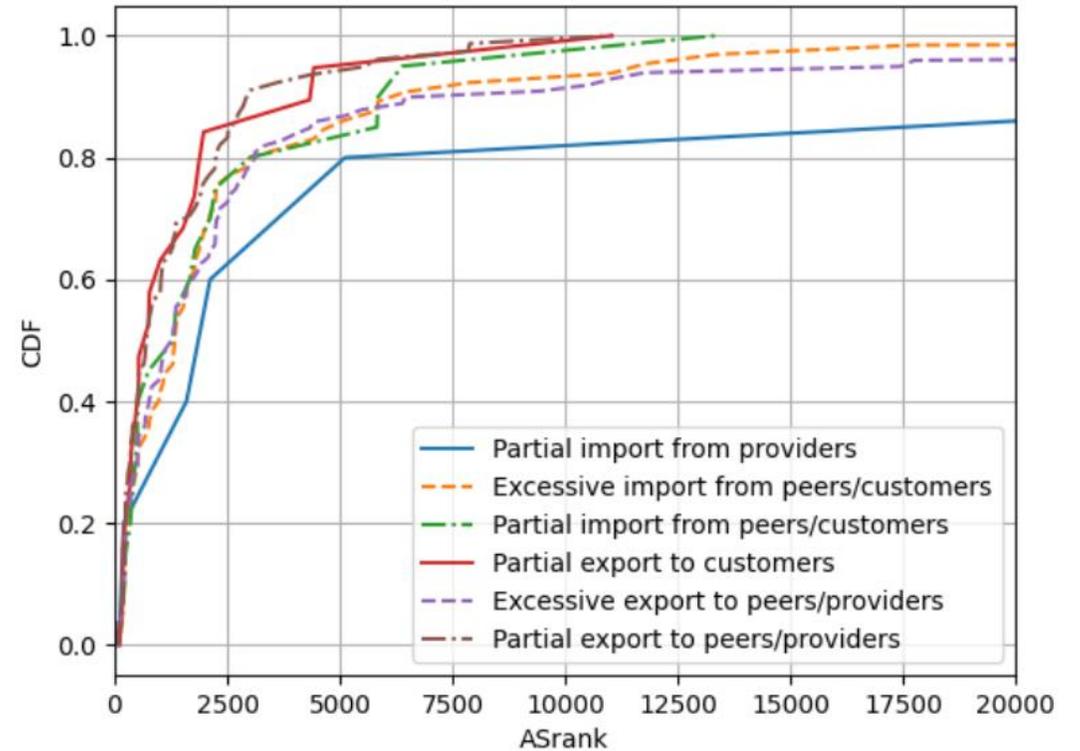
| IP Version | Level | No ISAV | ISAV | Partial ISAV | Sum |
|------------|------------|-----------|-----------|--------------|-----------|
| IPv4 | AS | 23,700 | 6,509 | 28,682 | 58,891 |
| | Subnet /24 | 1,406,663 | 1,161,444 | 959,344 | 3,527,451 |
| IPv6 | AS | 4,518 | 1,115 | 2,731 | 8,364 |
| | Subnet /40 | 12,775 | 6,062 | 5,886 | 24,723 |

- About **60% IPv4 ASes** and **46% IPv6 ASes** have deployed (or partially deployed) ISAV, much higher than previously reported.
- Widely distributed targets help capture deployment status more accurately.

Achieving Realistic Routing Policy through Multiple Resources



Example of routing policy



CDF of ASes with different routing policy

Comments / Suggestions?

Contact us at:

sec@cgf.net