Analysis of Suspected Hijacking Events of Internet Routing Prefixes in 2022

1 OVERVIEW

The Internet is a distributed autonomous network, which is currently composed of nearly 80,000 **Autonomous Systems** (AS). The BGP protocol is used to exchange routing information between domains to ensure the connectivity between ASes. BGP protocol is an ancient protocol that has been used for more than 25 years, but there is a security defect that has not been resolved, that is, the BGP protocol lacks a route authenticity verification mechanism. Any false routing information forged by an AS will be unconditionally accepted by other ASes. Therefore, the current BGP routing system is a trust-based system, and its normal and stable operation depends on the authenticity and reliability of the routing information exchanged between each AS.

BGP hijacking is a traffic hijacking attack that takes advantage of the security flaw of BGP. BGP hijacking attackers can hijack traffic by announcing false routes to the routing system. The occurrence of BGP hijacking can be divided into two situations: misconfiguration and malicious attack.

The Pakistan Telecom hijacking of YouTube in 2008 is a well-known prefix hijacking incident caused by administrator misconfiguration. In this incident, Pakistan Telecom only wrongly announced a prefix of YouTube to the world, which caused the traffic in most parts of the world to not reach YouTube correctly.

In 2018, a small ISP in Colombia used BGP hijacking to successfully hijack the IP address of Amazon's authoritative DNS server, and then used the IP address to build a fake DNS server, thereby achieving DNS hijacking. Then the attacker redirected the domain name of a cryptocurrency wallet to a phishing server set up by the attacker, and finally successfully stole the user's login information.

At present, the research on resisting BGP hijacking is mainly divided into two categories: hijacking prevention technology and hijacking detection technology.

Hijacking prevention technologies include RPKI[1], BGPSEC[2], and ASPA[3]. To date, the deployment of RPKI in the world has reached about 30%; hijacking detection technology is an after-event remedy, using detection technology to detect hijacking, and then respond in time to reduce losses.

A typical feature of BGP routing address prefix hijacking is that two ASes announce a certain IP address prefix at the same time. However, this phenomenon is not a sufficient condition for judging BGP routing prefix hijacking. Due to various situations such as multi-homed routing and DDOS hijacking protecting in the Internet, it may be a normal behavior for an IP address prefix to be announced by multiple ASes. Therefore, the detection system needs to use rich domain knowledge and rules to filter legitimate MOAS (Multiple Origin AS, MOAS) events. Due to the characteristics of Internet distributed autonomy, it is therefore impossible to accurately filter all legal MOAS events. As the purpose of the detection system is to discover suspicious phenomena and give early warning to operators, these detected events are therefore called "suspected hijacking events".

This report analyzes the suspected BGP routing prefix hijacking incidents from January 2022 to December 2022 and reveals the general characteristics of the suspected BGP hijacking incidents in the last year.

2 MEASUREMENT METHOD

The source of the analysis event is from the routing hijacking monitoring platform BGPWatch[4]. BGPWatch is a prefix hijacking event detection system based on Multiple Origin AS (MOAS) events developed by the Dragonlab Laboratory of the Network Research Institute of Tsinghua University. Launched in October 2021, the system uses rich domain knowledge and rules to filter legitimate MOAS events, thereby filtering out false prefix hijacking events. The system then grades the events according to the importance of the hijacked prefix and the victim AS. In addition, the system provides event analysis and playback functions.

---

[1] https://rpki-monitor.antd.nist.gov/

[2] https://en.wikipedia.org/wiki/BGPsec

[3] https://datatracker.ietf.org/meeting/102/materials/slides-102-sidrops-as-path-verifcation-using-aspa-00

[4] https://bgpwatch.cgtf.net/#/

The suspected hijacking events reported by BGPWatch consist of fields such as hijacker AS information, victim AS information, hijacked prefix information, hijacking time, hijacking level, and hijacking playback. Figure 1 shows a hijacking event. The level rules of the event are as follows: when the number of websites contained in the hijacked prefix is greater than 5, the event level 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 level is middle level, otherwise the event level is low level.

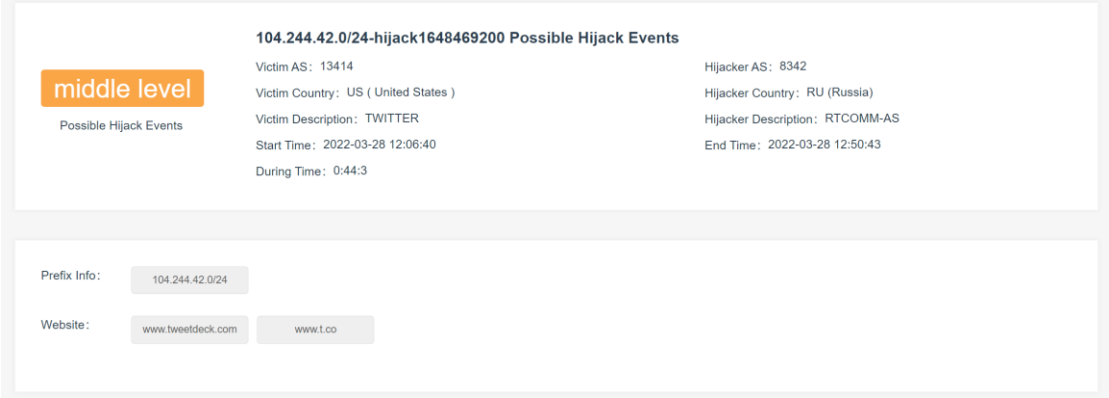


Figure 1 A route hijacking event

3 Analysis of Suspected Hijacking Events

3.1 Distribution of the number of daily events

The historical curve of suspected hijacking events from January 1, 2022, to December 31, 2022, as reported by the BGPWatch system, is shown in Figure 2. The blue line shows the number of daily suspected hijacking events, and the orange line shows suspected hijacking events with a duration of less than 3 minutes filtered (considering that the BGP convergence time is about 3 minutes).

As shown in the blue curve in the figure, the system reported a total of 2599 suspected hijacking events, of which there were no suspected hijacking events for 19 days. There are 7 reports per day on average, the median is 5.0, the maximum is 560, and the variance is 923.79. figure 2.

As shown in the orange curve in the figure, for suspected hijacking events longer than or equal to 3 minutes, BGPWatch system reported 1346 suspected hijacking events.

There are 4.15 reports per day on average, the median is 4.0, the maximum is 28, and the variance is 9.66.

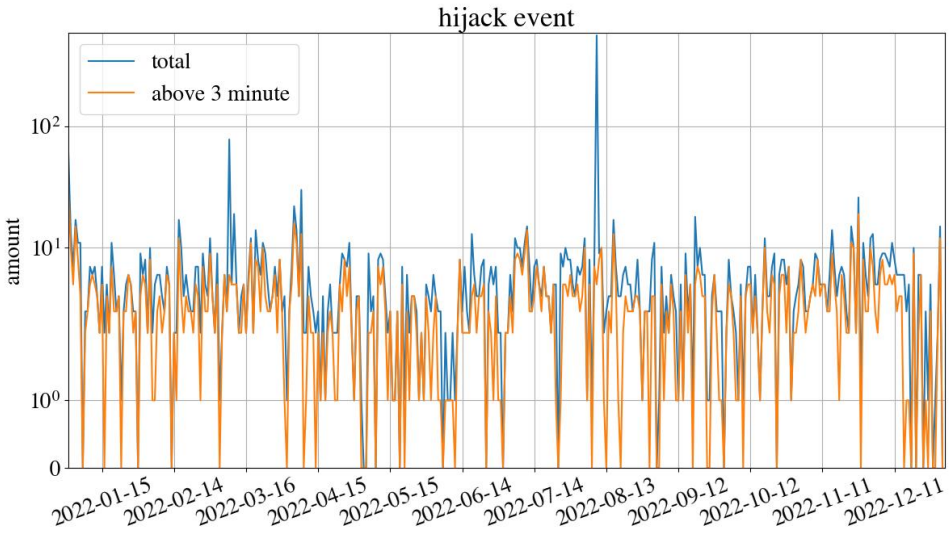
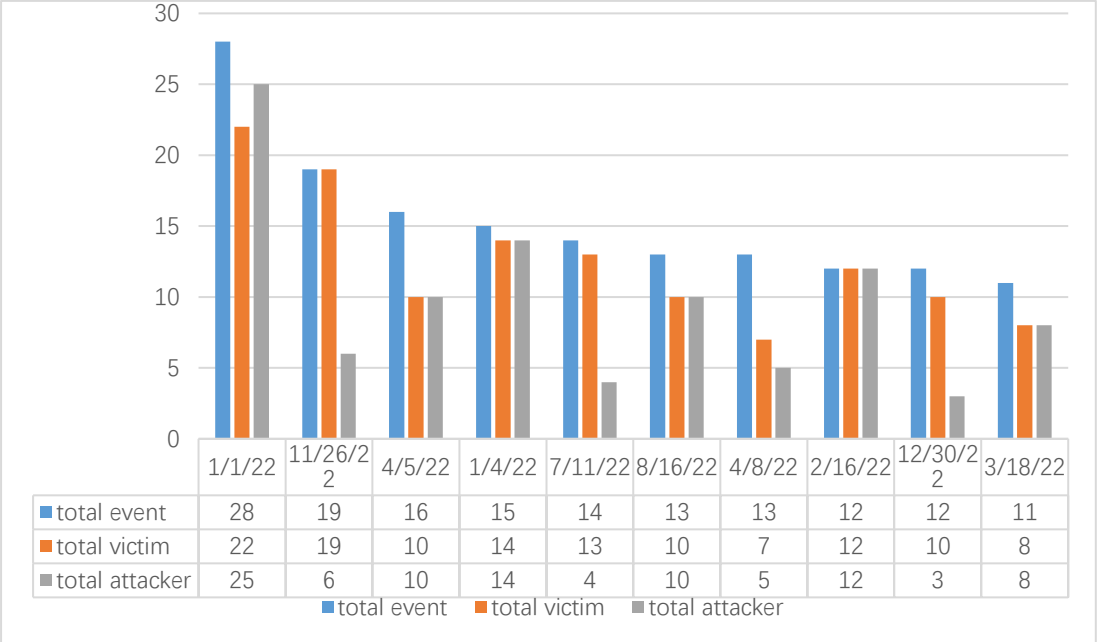


Figure 2. Historical curve of daily suspected hijacking events

It can be seen from Figure 2 that the number of suspected hijacking incidents notified on more than 99% of the days is less than 100. After filtering out the incidents of less than 3 minutes, the overall distribution basically does not change, but the number decreases.

Considering that the BGP convergence time is about 3 minutes, the follow-up statistics in this analysis report only focus on suspected hijacking events longer than or equal to 3 minutes.

Figure 3 shows the relevant information of the 10 days with the largest number of notified events.



	1/1/22	11/26/22	4/5/22	1/4/22	7/11/22	8/16/22	4/8/22	2/16/22	12/30/22	3/18/22
total event	28	19	16	15	14	13	13	12	12	11
total victim	22	19	10	14	13	10	7	12	10	8
total attacker	25	6	10	14	4	10	5	12	3	8

Figure 3 TOP 10 daily attack events

The CDF distribution of the number of daily attack events is shown in Figure 4, and the distribution of the number of daily hijacking event reports basically satisfies the power law distribution[5].

[5] https://en.wikipedia.org/wiki/Power_law#Power-law_probability_distributions

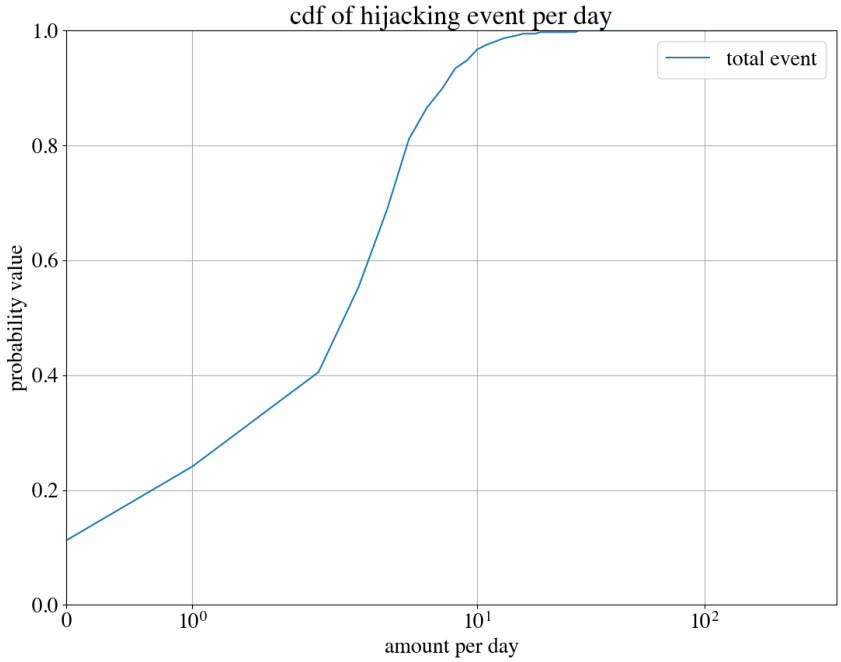


Figure 4 CDF chart of the number of daily attack events

3.2 DURATION DISTRIBUTION

The mean of the duration is 0 days, 6 hours and 15 minutes, the median is 44.0 minutes, the variance is 421884.69, the minimum is 3 minutes, and the maximum is 2856 minutes (note that this system regards MOAS events that last longer than 48 hours as normal events, because the administrator will respond quickly after the hijacking event occurs, so the hijacking time will generally not exceed 48 hours). The CDF diagram of the distribution of duration is shown in Figure 5. It can be seen that 80% of the hijacking events lasted less than 500 minutes (8.33h), and 60% of the hijacking events lasted less than 100 minutes.

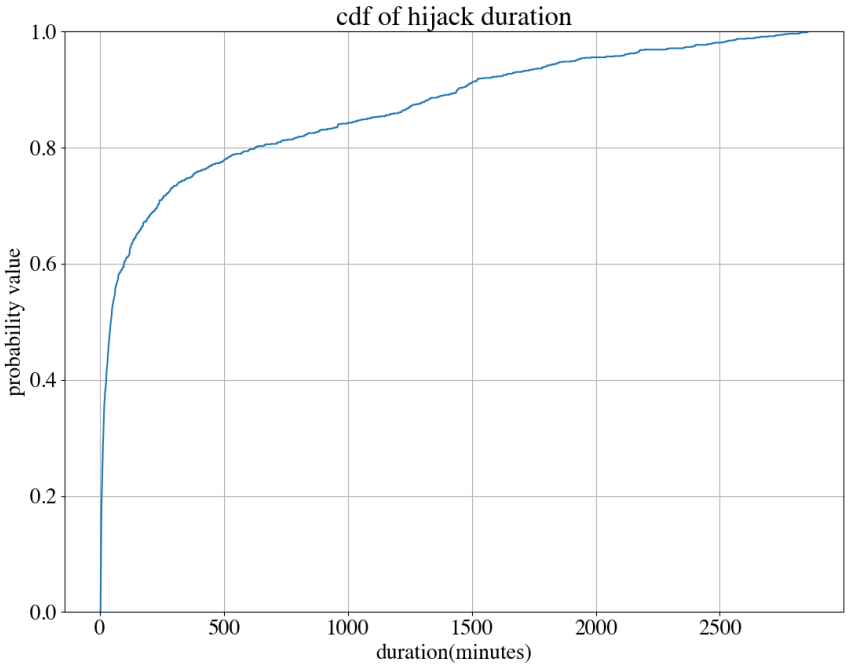


Figure 5. Distribution of duration of hijacking events

3.3 DISTRIBUTION OF HIJACKED PREFIXES

There are 1,352 hijacked prefixes (after deduplication), among which there are 59 victim prefixes in high-harm events, and 173 victim prefixes in medium-hazard events.

The prefix length distribution of IPv4 hijacked prefixes is shown in Figure 6. More than 80% of the hijacked prefix lengths are 24, and the remaining prefix lengths are mostly 23 and 22.

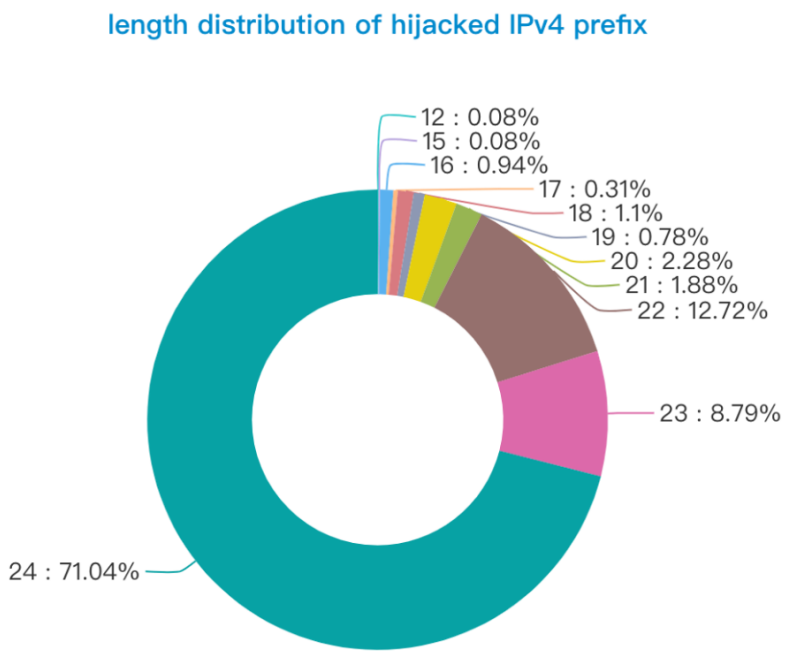


Figure 6 The prefix length distribution of hijacked IPv4 prefixes

The prefix length distribution of IPv6 hijacked prefixes is shown in Figure 7. Prefixes with a length of 48 accounted for one-third, and the remaining prefix lengths are mostly 44 and 32.

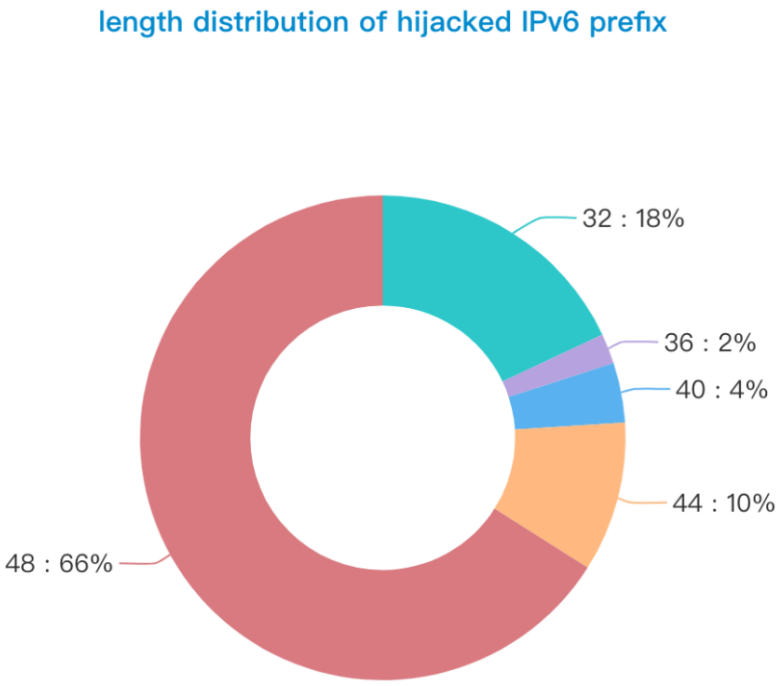


Figure 7 The prefix length distribution of IPv6 hijacked prefixes

3.4 HAZARD LEVEL DISTRIBUTION OF HIJACKING EVENTS

The system divides hijacking events into 3 levels, high, medium, and low, according to the harm caused by the hijacking event. Among all 1348 incidents, there were 94 high-hazard incidents, 177 medium-hazard incidents and 1077 low-hazard incidents. The hijacking event level statistics are shown in Figure 8.

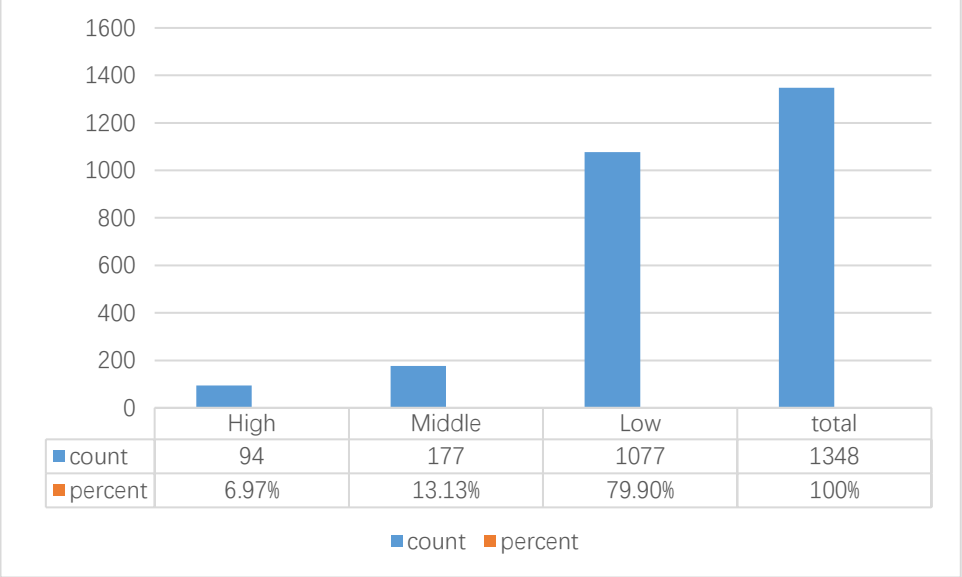


Figure 8 The proportion of hijacking event levels

An average of 0.29 high-hazard events occurred every day, with a median of 0 and a variance of 0.48. After removing all days reported as 0, the average number of high-hazard events per day was 1.34, with a median of 1.0 and a variance of 0.83. The average number of websites owned by the victim prefixes of all high-harm events is 322.89, and the median is 61.0.

The historical curves of high-risk, medium-risk, and all events are shown in Figure 9.

Among the 365 days, 70 days had high-risk events, accounting for 19.72% of the total days. And the number of high-risk events is positively correlated with the total number of events on the day.

The CDF distribution of daily high, medium and all events is shown in Figure 10.

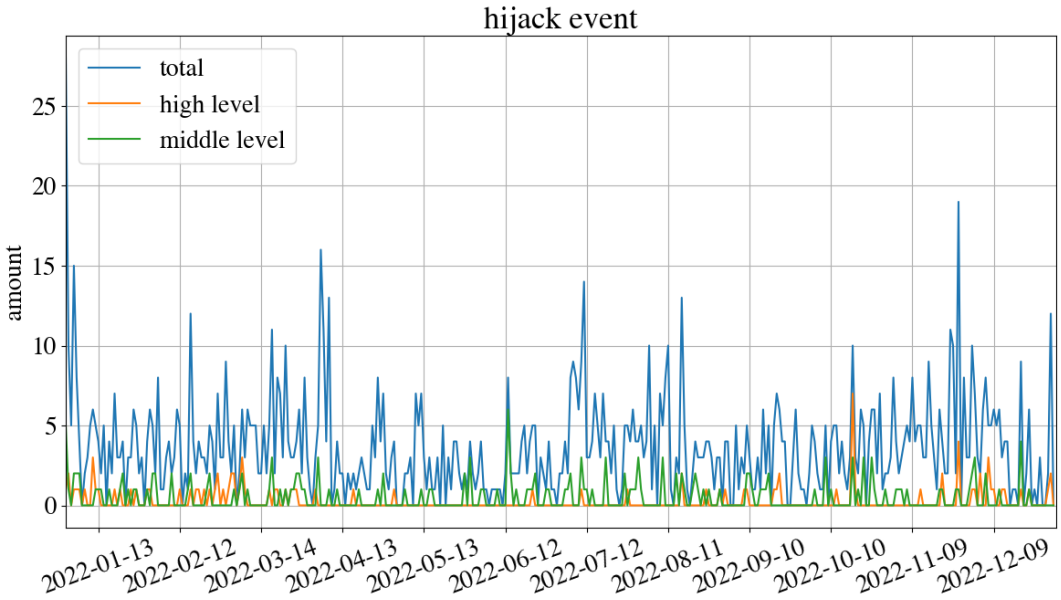


Figure 9 High, medium and all event history curves

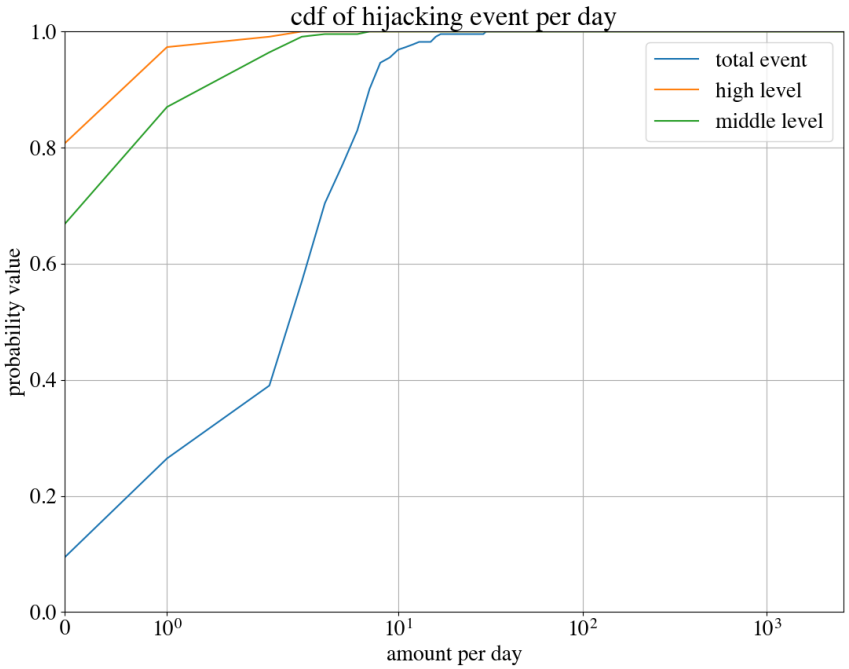


Figure 10 CDF distribution chart of daily high, medium and total event numbers

The TOP 10-day data of daily high-risk events are shown in Figure 11, and the data of the TOP 10 events with a high degree of harm (sorted according to the number of websites included in the victim prefix) are shown in Table 1.

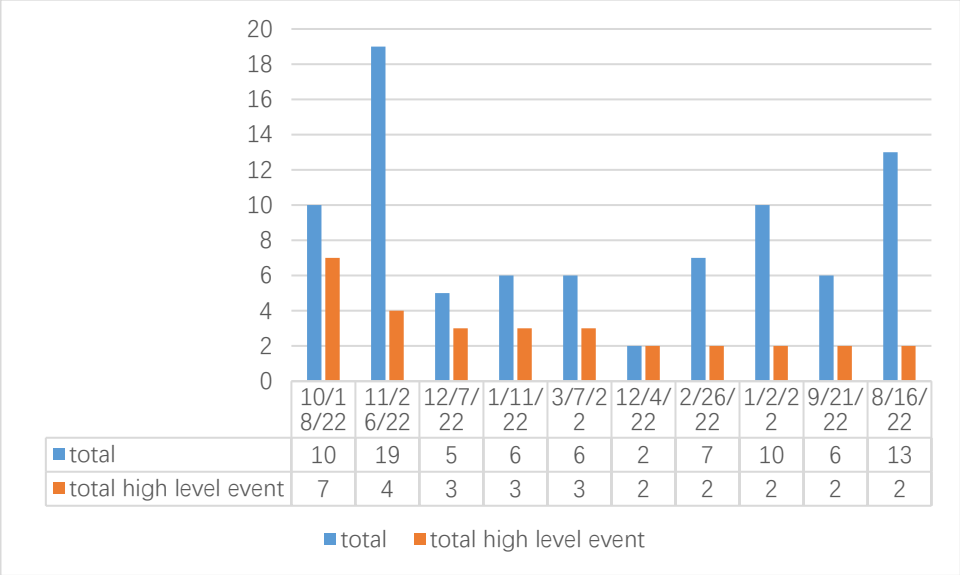


Figure 11 TOP 10-day data of daily high-hazard events

Table 1 TOP 10 incidents with the degree of harm (sorted according to the number of websites contained in the victim prefix)

Date	Prefix	Attacker	Country/Region of Attacker	Victim	Country/Region of Victim	Website number in prefix
2022-03-07	156.231.128.0/17	328608	South Africa	139879	Pakistan	1688
2022-06-22	163.197.128.0/18	400506	America	140107	China	1681
2022-09-01	198.185.159.0/24	263047	Brazil	53831	America	1301
2022-12-09	154.195.64.0/18	398993	America	328608	South Africa	1128
2022-10-18	45.142.96.0/22	138968	Japan	203020	India	1079
2022-10-18	85.239.40.0/23	138968	Japan	197648	Cyprus	399
2022-12-07	103.99.40.0/23	137443	Hong Kong	138538	China	367
2022-10-18	45.80.204.0/22	138968	Japan	50340	Russia	364
2022-01-11	62.60.200.0/21	15611	Iran	1239	America	337
2022-04-17	157.245.128.0/20	147176	Thailand	14061	America	155

3.5 ATTACKER AND VICTIM AS ANALYSIS

Figure 12 shows the historical curves of the number of attackers and victims AS on a daily basis.

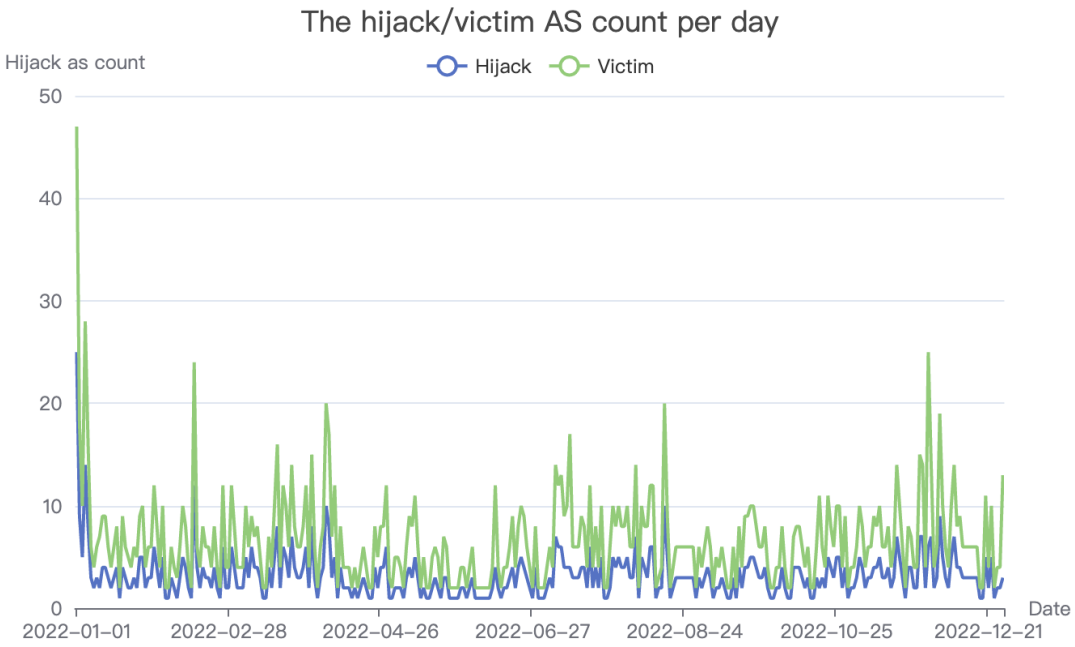


Figure 12 Historical curves of daily attacker and victim AS numbers

Figure 13 shows the distribution of the AS rankings (after deduplication) of the attacker and the victim AS on CAIDA[6]. It can be seen from Figure 13 that the ranking of the victim AS is obviously higher than that of the attacker AS.

[6] AS Rank: A ranking of the largest Autonomous Systems (AS) on the Internet. (caida.org), https://asrank.caida.org/

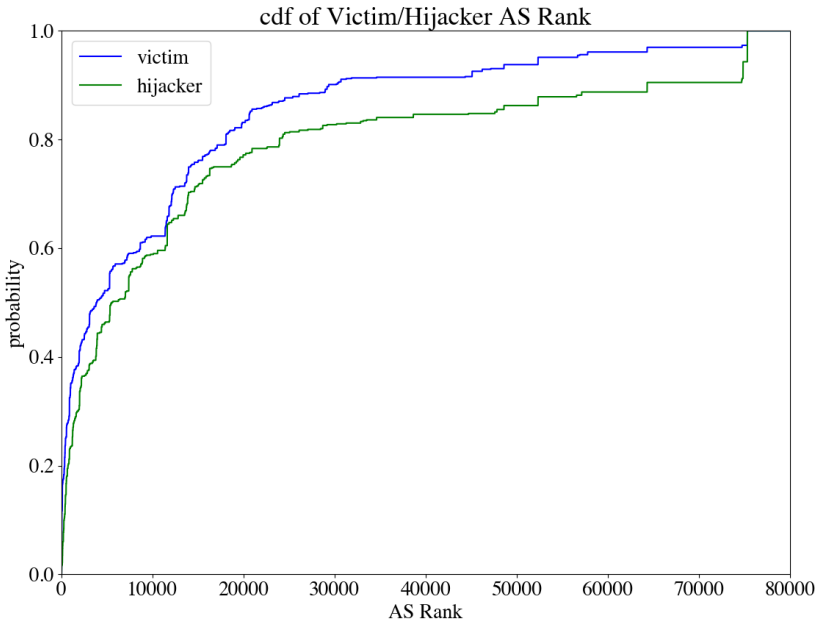


Figure 13 AS ranking distribution of attacker and victim AS on CAIDA

3.6 COUNTRY/REGION DISTRIBUTION OF HIJACKING INCIDENTS

Among all suspected hijacking incidents, the map of the event amount with country/region as victim is shown in Figure 14, and the specific number distribution is shown in Figure 15.

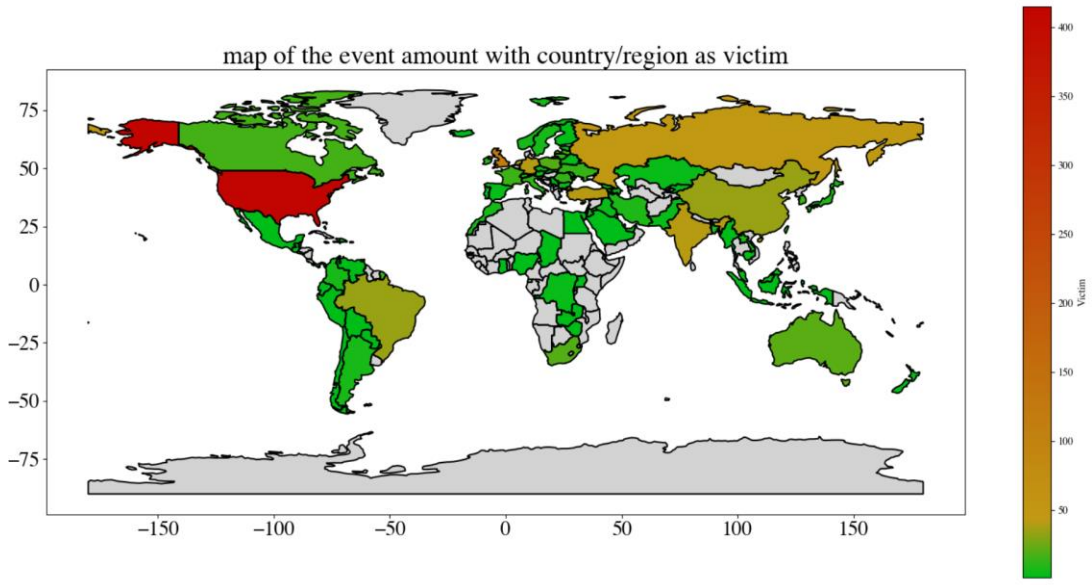


Figure 14 Map of the event amount with country/region as victim

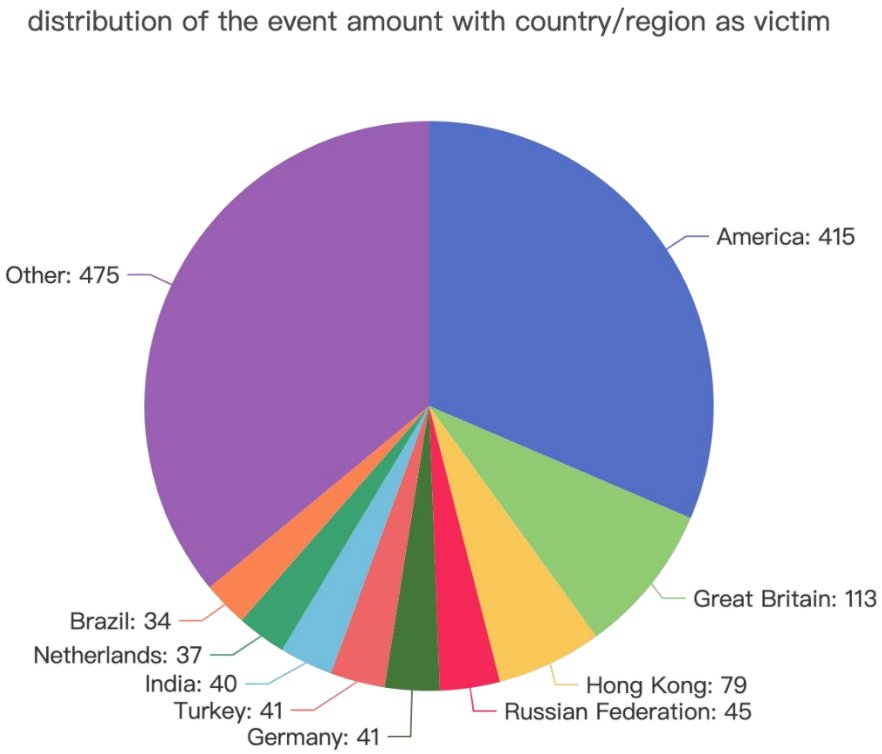


Figure 15 Distribution of the event amount with country/region as victim

Among all suspected hijacking incidents, the map of the event amount with country/region as hijacker is shown in Figure 16, and the specific number distribution is shown in Figure 17.

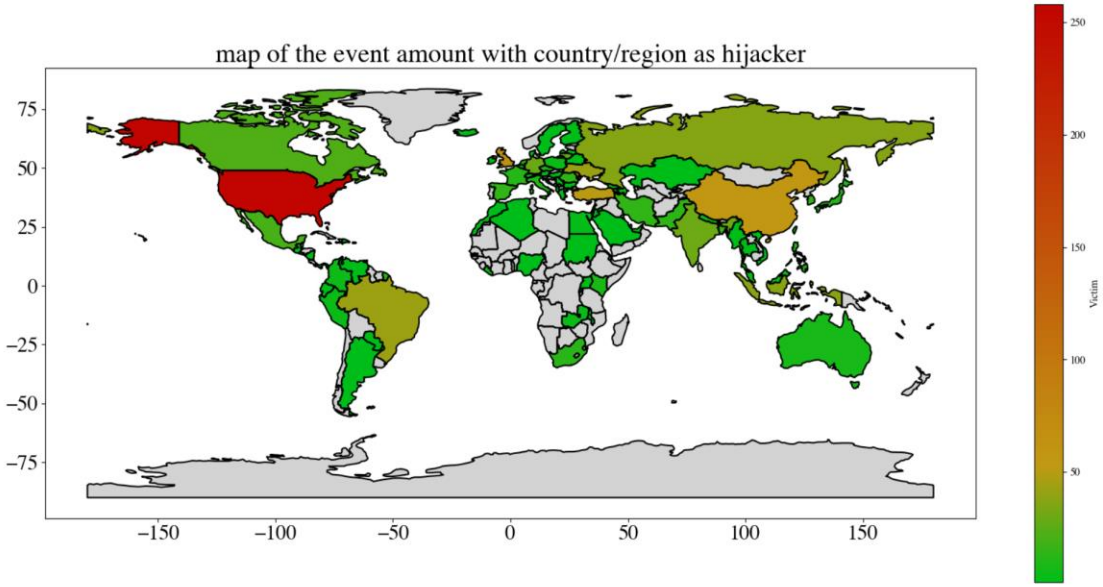


Figure 16 Map of the event amount with country/region as hijacker

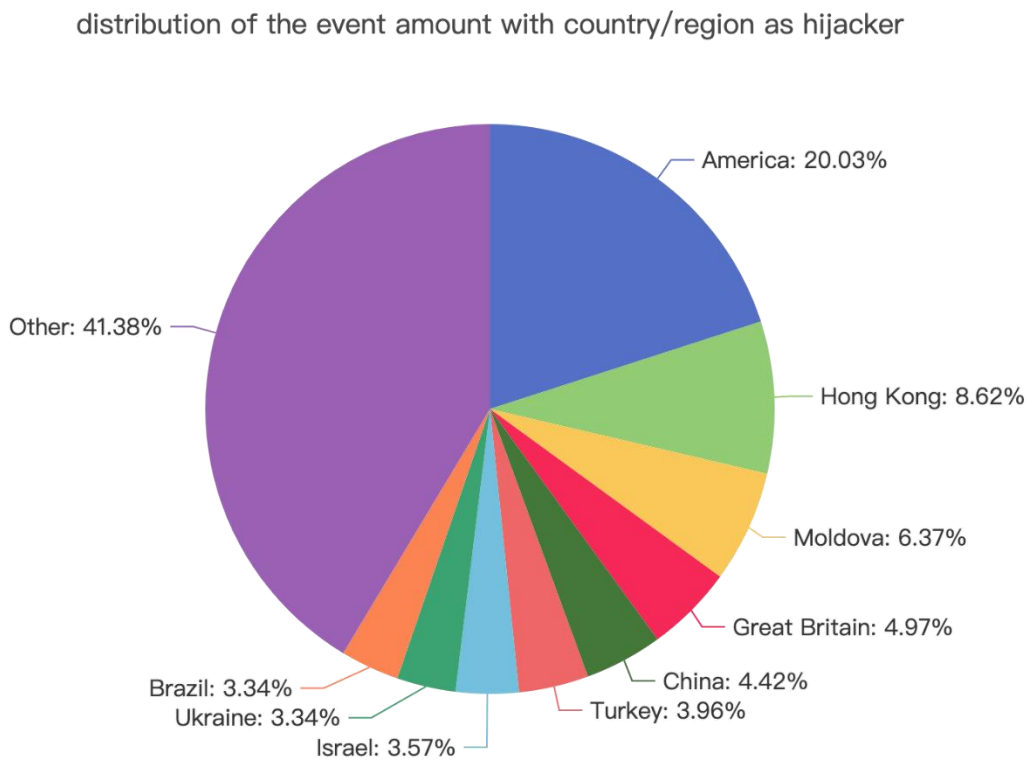


Figure 17 Distribution of the event amount with country/region as hijacker

As can be seen above, the United States has the largest number of attacker ASes and the largest number of victim ASes. In addition, Hong Kong, the United Kingdom, China, Turkey, and Brazil also rank in the TOP 10 in terms of the number of ASes in both attacker and victim countries/regions.

3.7 SCOPE OF INFLUENCE OF HIJACKING EVENT

The system collects data through multiple observation points. After the attacker announces the hijacked prefix, the announcement spreads across the Internet. However, due to the influence of factors such as the current deployment of ROA and the selection of the shortest path, the hijacking announcement cannot spread to all observation points.

Most of the hijacking events are captured by multiple observation points, as shown in Figure 18, about 60% of the events will be observed by 1%-20% of the observation points.

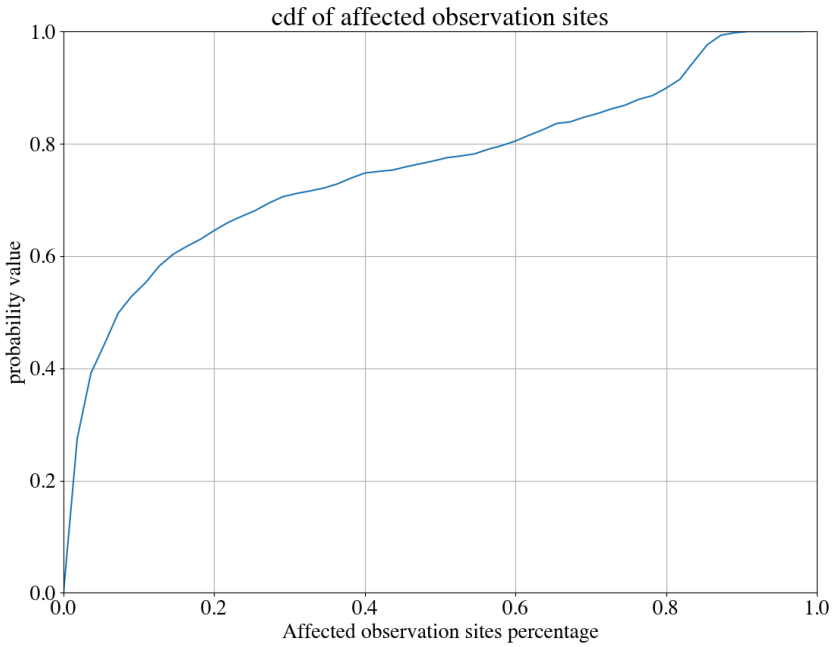


Figure 18 CDF diagram of the proportional distribution of observation points affected by suspected hijacking events

Using (attacker AS, date) as a fingerprint, merging and counting the data can get 1142 attack events. Among them, there were 332 (29.07%) incidents, and more than half of the observation points observed suspected hijacking. In 1 (0.09%) of the incidents, hijackings were observed at all observation points. Figure 19 shows the hijacking events counted by (attacker AS, date), and Figure 20 shows the proportion distribution of observation points affected by hijacking events as fingerprints (attacker AS, date).

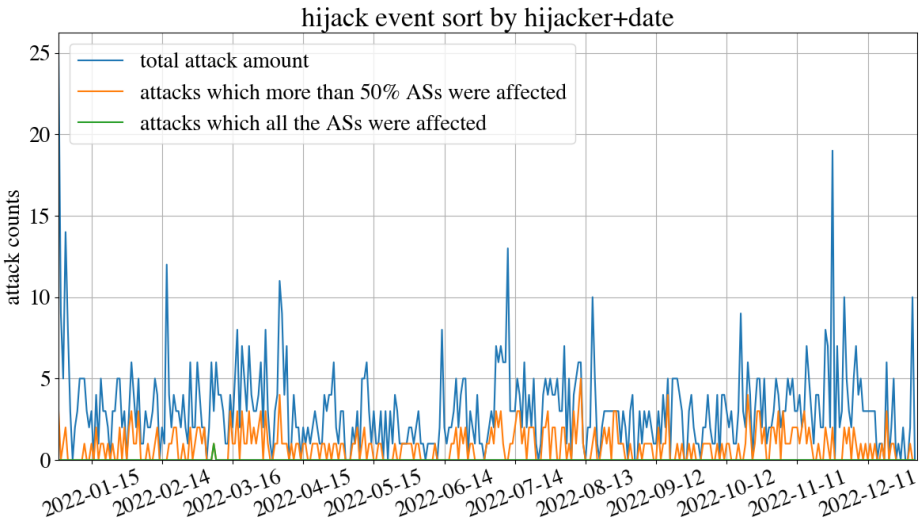


Figure 19 The historical curve of the number of suspected hijacking events using (attacker AS, date) as a fingerprint

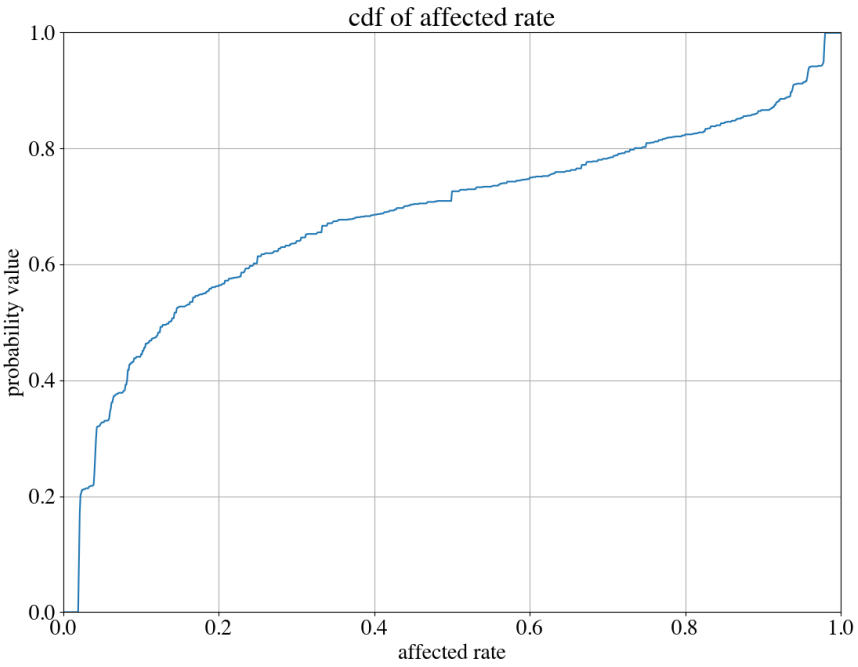


Figure 20 Proportional distribution of observation points affected by suspected hijacking events using (attacker AS, date) as a fingerprint

4 SUMMARY

This paper analyzes the suspected hijacking events of BGP routing prefixes in 2022, using a range of BGPWatch-generated metrics. Based on the data, we can conclude that;

(1) The broadcast of prefix hijacking is restricted to a limited area

This can be seen from the observation points of each event. About 60% of the events were observed by only 1%-20% of the observation points. This is because that the current deployment of RPKI is increasing and so prevents the hijacking announcement from spreading to all observation points.

(2) Most prefix hijackings do not have much impact

Among all the incidents, there were 6.97% high-hazard incidents, 13.13% medium-hazard incidents and 79.90% low-hazard incidents.

(3) Prefix hijacking is still a big threat to the internet

For example, AS13414 (TWITTER) was hijacked by AS8342 (RTCOMM-AS, RU), and Crypto Exchange KLAYswap lost USD $1.9M after a BGP hijack.

(4) Some events still require more research

Due to the existence of multi-homed routing, DDOS hijacking protection, and IP address selling and leasing on the Internet, it is very difficult to accurately filter all legal MOAS events, and some events still require more ongoing investigation.

Finally, we would suggest that network operators and administrators:

(1) Monitor their networks and get timely alarms

Network operators can subscribe to our platform for their prefix hijacking events and get timely alerts.

(2) Deploy hijacking prevention technology

RPKI is very useful for protecting your own network from hijacking. Other routing path hijacking prevention and inspection technologies are currently under development, and operators should track the progress and deploy them in a timely manner.