THREAT HUNTER RESEARCH

H1 2026 Cybercrime Ecosystem Research Report

A half-year assessment of changing cybercrime infrastructure, malicious mobile-number resources, attack tools, and increasingly specialized fraud operations.

Original publication: 2026-07-27
Research team: Threat Hunter Research Team
Source report: 56 pages

Read instructions

> This text version is reconstructed based on the 56-page original PDF and the full text of the published web page, retaining the report narrative, chapters, tables, and original charts; the cover, repeated table of contents, and purely decorative pages are not repeated.

In the first half of 2026, against the background of continued strengthening of regulatory crackdowns, platform governance, and corporate fraud controls, traditional cybercrime operations resources have shrunk, but the risks have not subsided. Instead, they have accelerated their migration to resources outside mainland China, more covert infrastructure, and more complex malicious links.

Based on the continuous monitoring of the cybercrime ecosystem, the Threat Hunter Anti-Fraud Intelligence Research Team released the "Internet Dark and Ash Industry Research Report for the First Half of 2026", which systematically presents the changes in cybercrime operations resources, the evolution of the industry chain, and typical malicious scenarios. In addition to this report, Threat Hunter will also successively release the "Credit Risk Research Report for the First Half of 2026" and the "Brand Protection Risk Research Report for the First Half of 2026", respectively focusing on key risk scenarios such as credit fraud, data leakage, phishing and counterfeiting, and brand infringement.

This is the Internet cybercrime ecosystem research report that Threat Hunter has released for many consecutive years. It is also the annual trend observation result that Threat Hunter regularly launch for the industry. As a security vendor focusing on cybercrime ecosystem intelligence and business anti-fraud, Threat Hunter has been deeply involved in the field of cybercrime ecosystem intelligence for 10 years. Relying on long-term accumulation of risk data, real attack samples and corporate governance practices, it continues to track cybercrime operations resources, attack methods and changes in the industry chain, and continues to provide reference for enterprises to judge risk trends and formulate governance strategies.

"Outline of Research Report on Internet cybercrime ecosystem in the First Half of 2026"

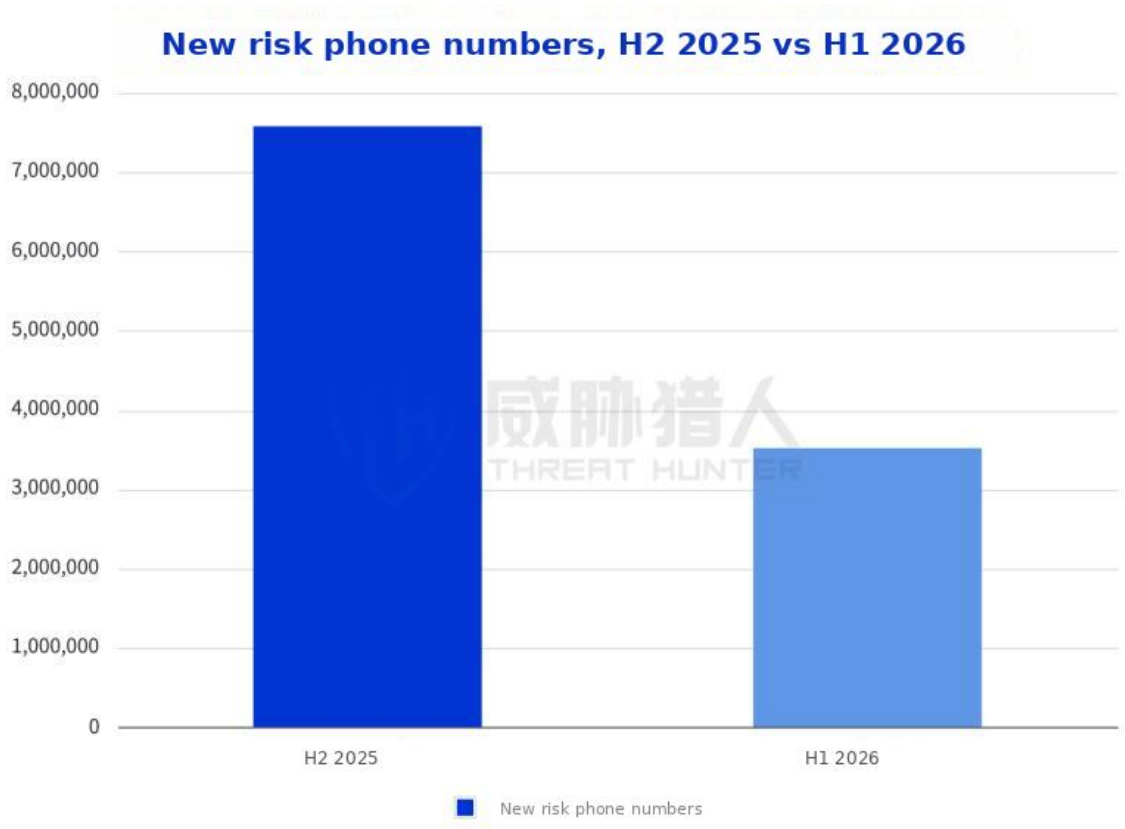
The core findings of this report are as follows:

1. Analysis of cybercrime operations attack resources in the first half of 2026

1.1 Analysis of risky mobile phone card resources in the first half of 2026

1.1.1 The total number of new domestic risk phone numbers in the first half of 2026 fell by 53.6% compared with the second half of 2025.

In the first half of 2026, Threat Hunter monitoring found that the total number of new domestic risky phone numbers showed a downward trend, with the number of new ones reaching 3.516 million, a 53.6% decrease from the second half of 2025. From the perspective of risk type structure, this round of total decline is highly related to the simultaneous shrinkage of the two core illicit SIM-card resources, domestic SIM-pool cards and interception cards: in the first half of 2026, domestic SIM-pool cards decreased by 26.7% compared with the second half of 2025, and domestic interception cards decreased by 68.35% compared with the second half of 2025. Among them, the decline in interception cards was more significant, which was a major driver of the overall decline in the number of new risky phone numbers.



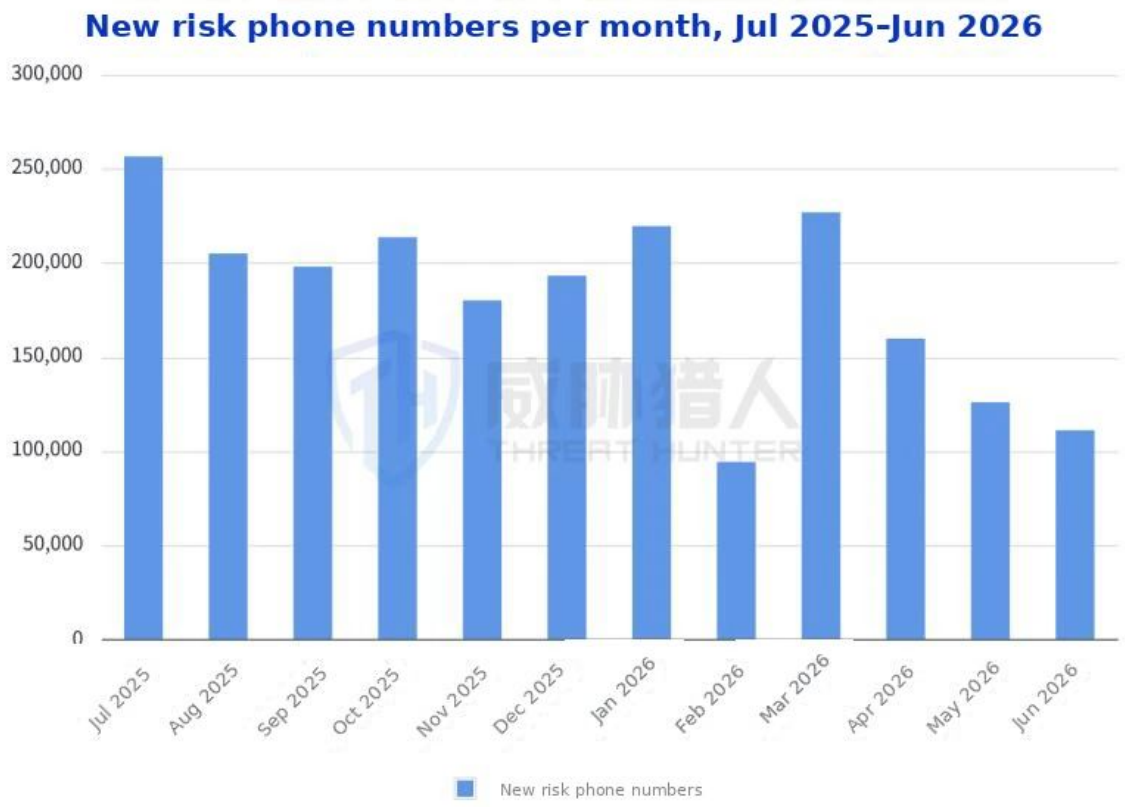
New risk phone numbers, H2 2025 vs H1 2026

Source: Threat Hunter original report, page 6. Original figure with Chinese text replaced by English.

1.1.2 Change trend of SIM-pool card resources in the first half of 2026

(1) The number of domestic SIM-pool cards in the first half of 2026 fell by 26.7% compared with the second half of 2025.

According to data from the Threat Hunter Intelligence Platform, 911,900 new SIM-pool cards were captured in the first half of 2026, a 26.7% decrease from the second half of 2025.



New risk phone numbers per month, Jul 2025–Jun 2026

Source: Threat Hunter original report, page 7. Original figure with Chinese text replaced by English.

According to analysis by Threat Hunter intelligence experts, the main reasons for this trend are:

- The supply side of cybercriminal operations has been attacked, resulting in a decline in service stability. In the first half of 2026, card issuance platforms experienced attacks, site abnormalities, and service switching. Such incidents will cause the card issuing platform to temporarily suspend sales or move sites, which will lead to a phased decline in the number of SIM-pool cards that can be purchased and placed on the cybercrime ecosystem side.
- Some code receiving platforms have suspended services, affecting the procurement links of downstream agents and buyers. In addition to attacks on card-issuing platforms, some mainstream code-receiving platforms also experienced server anomalies and other problems in the first half of the year, causing downstream agents and buyers to be unable to obtain number resources stably.

Taken together, the attack on the card issuance platform and the phased outage of the mainstream code receiving platform have jointly weakened the supply capacity of domestic SIM-pool cards, which is an important reason for the decline in the scale of new SIM-pool cards in the first half of 2026.



Screenshots of SIM-pool card offers

Source: Threat Hunter original report, page 7. Original image retained.

(2) The three provinces with the largest number of new SIM-pool cards in the first half of 2026 are: Chongqing, Guangdong, and Zhejiang

Threat Hunter conducted a statistical analysis of new domestic SIM-pool cards in the first half of 2026 and found that Chongqing, Guangdong, and Zhejiang (including municipalities) are the three provinces with the largest number of SIM-pool cards.



Top 10 provinces for SIM-pool cards, H1 2026

Source: Threat Hunter original report, page 8. Original figure with Chinese text replaced by English.

Province	Rank by new SIM-pool cards, H1 2026	Trend
Chongqing	1st	No change
Guangdong	2nd	No change
Zhejiang	3rd	Up 2
Hunan	4th	No change
Sichuan	5th	Up 7
Henan	6th	Up 1
Heilongjiang	7th	Up 6
Hubei	8th	Down 5
Xinjiang	9th	Up 2
Anhui	10th	Down 2

Province ranking for new SIM-pool cards, H1 2026

Source: Threat Hunter original report, page 8. Table re-typeset in English from the original.

(3) The three cities with the largest number of new SIM-pool cards in the first half of 2026 are: Chongqing, Changsha, and Chengdu

Threat Hunter conducted a statistical analysis of new domestic SIM-pool cards in the first half of 2026 and found that Chongqing, Changsha, and Chengdu were the three cities with the largest number of SIM-pool cards.



Top 10 cities for SIM-pool cards, H1 2026

Source: Threat Hunter original report, page 8. Original figure with Chinese text replaced by English.

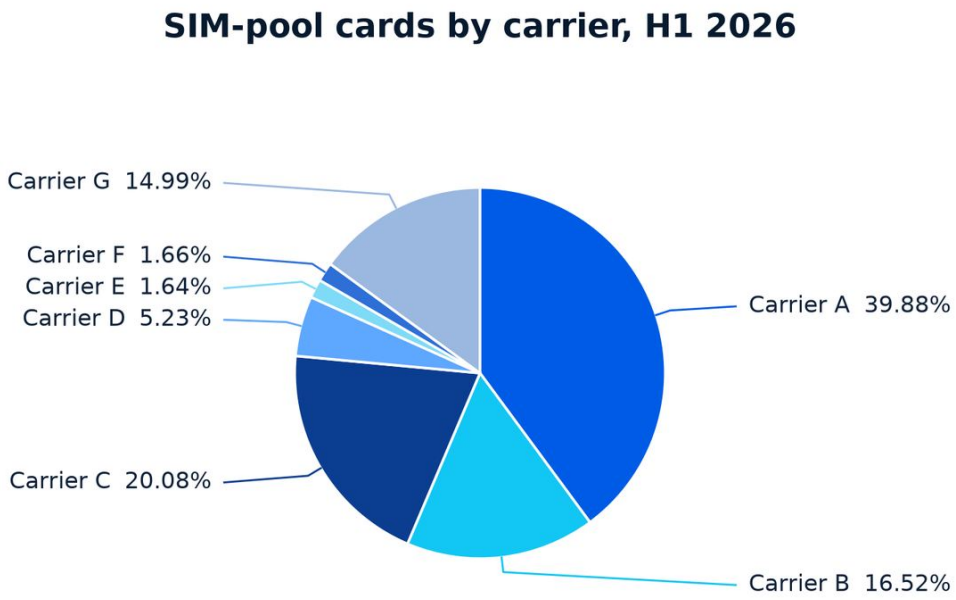
City	Rank by new SIM-pool cards, H1 2026	Trend
Chongqing	1st	No change
Changsha	2nd	Up 1
Chengdu	3rd	Up 7
Urumqi	4th	Up 3
Hangzhou	5th	No change
Beijing	6th	Up 15
Hefei	7th	Up 2
Zhengzhou	8th	Up 4
Guangzhou	9th	Down 3
Shanghai	10th	Down 6

City ranking for new SIM-pool cards, H1 2026

Source: Threat Hunter original report, page 8. Table re-typeset in English from the original.

(4) Among the new SIM-pool cards captured in the first half of 2026, 81.71% belong to the four major domestic operators

Threat Hunter intelligence data shows that in the first half of 2026, 911,900 new SIM-pool cards were detected, of which 81.71% were SIM-pool cards belonging to the four major domestic operators, and 18.29% were SIM-pool cards belonging to virtual operators.



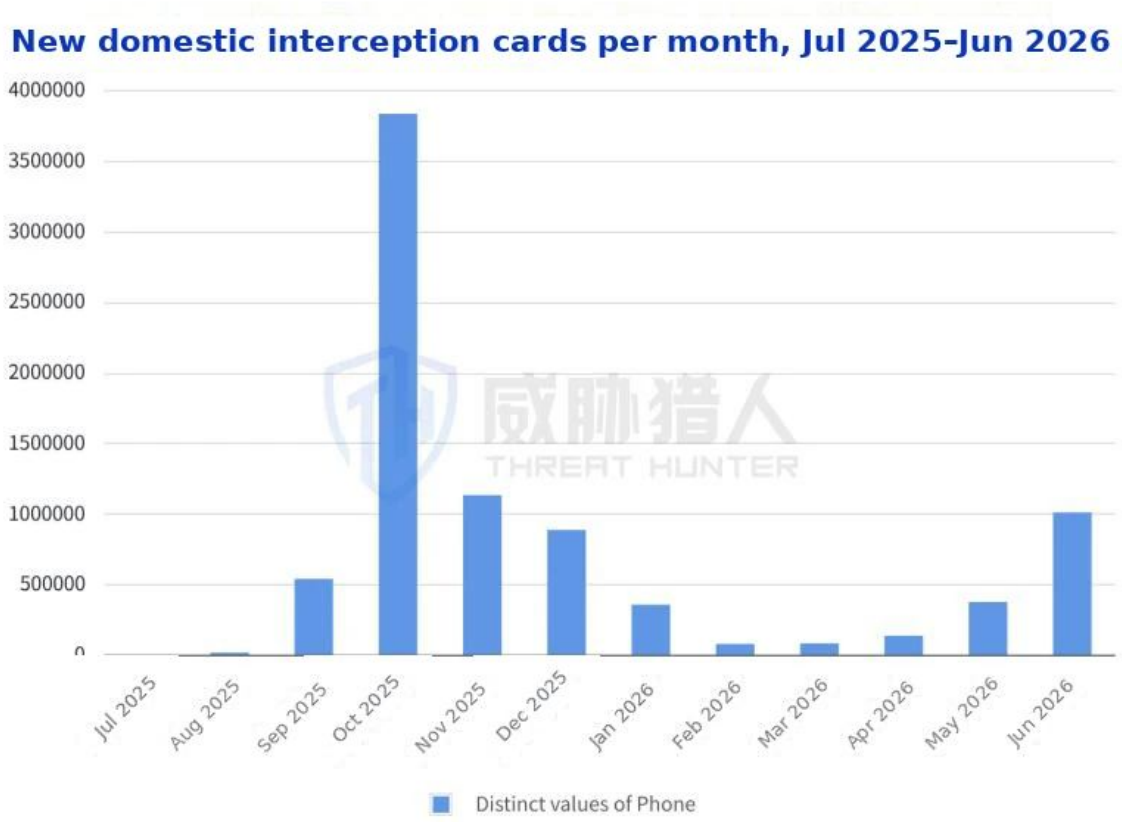
SIM-pool cards by carrier, H1 2026

Source: Threat Hunter original report, page 8. Redrawn in English from the original figure.

1.1.3 Change trends in domestic mobile phone card interception resources in 2026

(1) Domestic interception cards in the first half of 2026 fell by 68.35% compared with the second half of 2025

According to data from the Threat Hunter Intelligence Platform, in the first half of 2026, Threat Hunter captured 2.023 million new interception cards, a 68.35% decrease from the second half of 2025.



New domestic interception cards per month, Jul 2025–Jun 2026

Source: Threat Hunter original report, page 9. Original figure with Chinese text replaced by English.

Further analysis of the cybercrime ecosystem interceptor card supply situation shows:

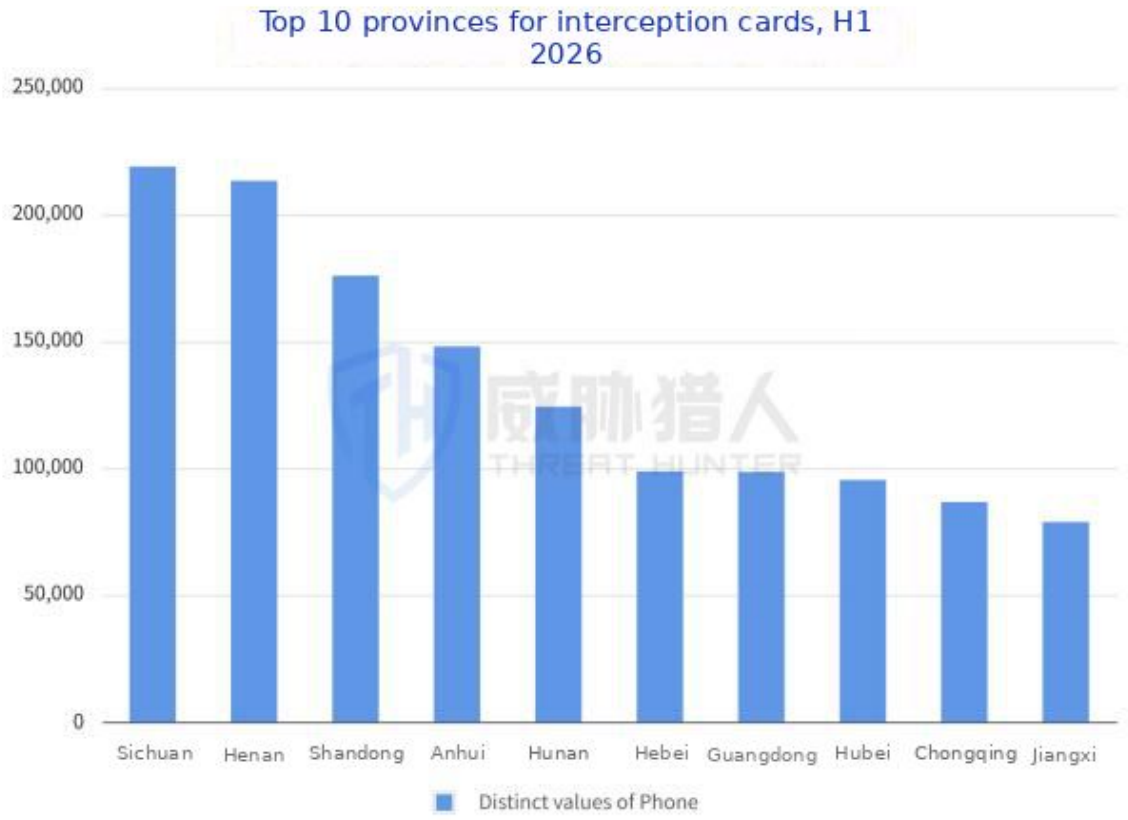


Screenshots of interception-card offers

Source: Threat Hunter original report, page 9. Original image retained.

(2) The three provinces with the most interception cards in the first half of 2026 are: Sichuan, Henan, and Shandong

A statistical analysis of domestic interception cards captured in the first half of 2026 found that Sichuan, Henan, and Shandong are the three provinces with the largest number of interception cards.



Top 10 provinces for interception cards, H1 2026

Source: Threat Hunter original report, page 10. Original figure with Chinese text replaced by English.

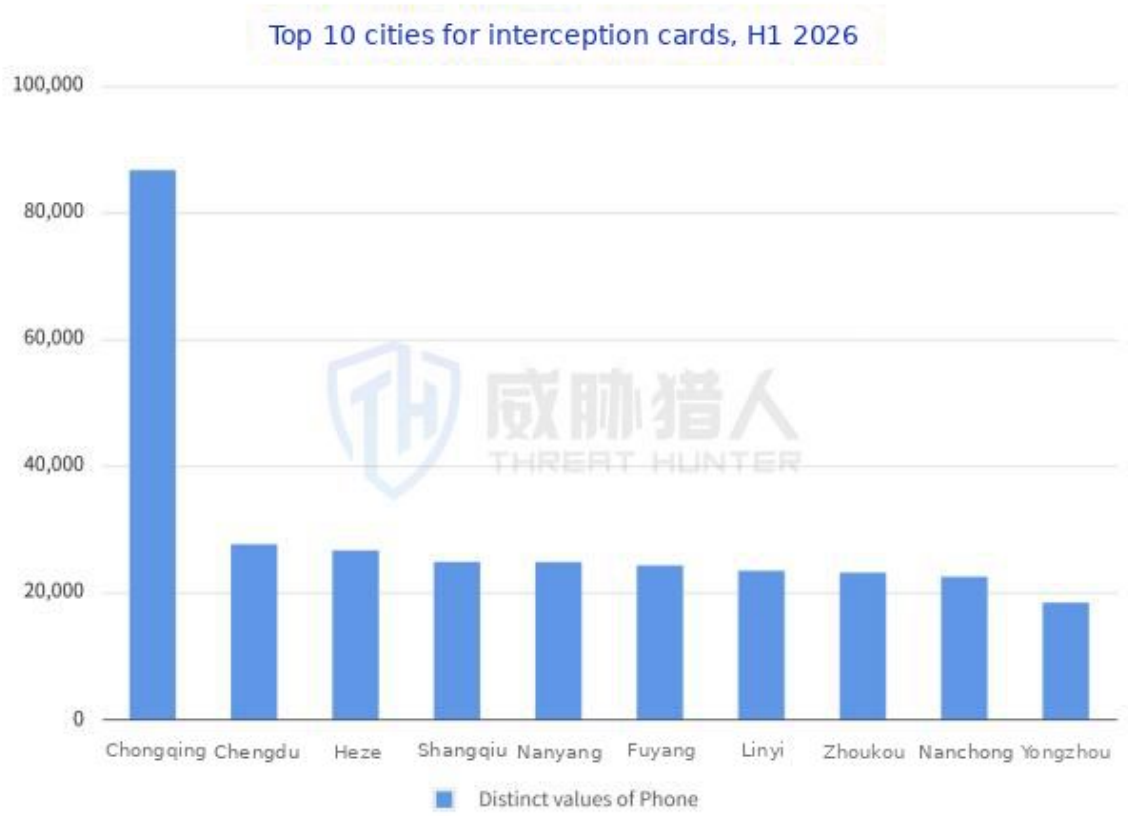
Province	Rank by new interception cards, H1 2026	Trend
Sichuan	1st	Up 2
Henan	2nd	No change
Shandong	3rd	Up 1
Anhui	4th	Up 1
Hunan	5th	Up 1
Hebei	6th	Up 1
Guangdong	7th	Down 6
Hubei	8th	No change
Chongqing	9th	No change
Jiangxi	10th	Up 1

Province ranking for new interception cards, H1 2026

Source: Threat Hunter original report, page 10. Table re-typeset in English from the original.

(3) The three cities with the largest number of new interception cards in the first half of 2026 are: Chongqing, Chengdu, and Heze

Threat Hunter conducted a statistical analysis of new domestic interception cards in the first half of 2026 and found that Chongqing, Chengdu, and Heze were the three cities with the most interception cards.



Top 10 cities for interception cards, H1 2026

Source: Threat Hunter original report, page 10. Original figure with Chinese text replaced by English.

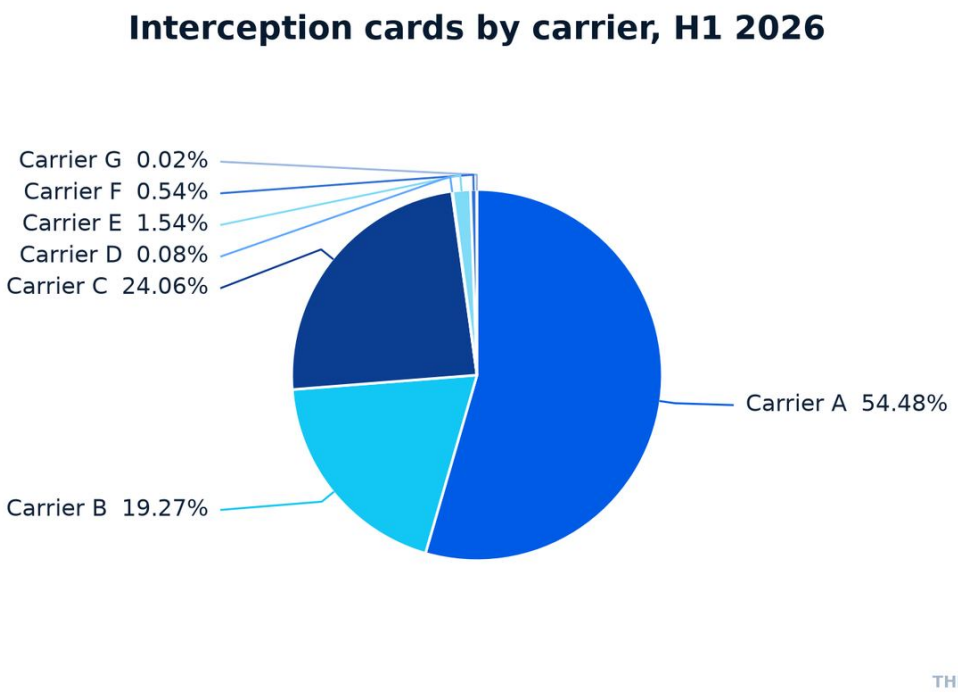
City	Rank by new interception cards, H1 2026	Trend
Chongqing	1st	No change
Chengdu	2nd	Up 4
Heze	3rd	Up 1
Shangqiu	4th	Up 1
Nanyang	5th	Up 3
Fuyang	6th	Up 1
Linyi	7th	Up 2
Zhoukou	8th	Up 2
Nanchong	9th	Up 6
Yongzhou	10th	Up 9

City ranking for new interception cards, H1 2026

Source: Threat Hunter original report, page 10. Table re-typeset in English from the original.

(4) Among the new interception cards captured in the first half of 2026, 97.89% belong to the four major domestic operators.

In the first half of 2026, the Threat Hunter intelligence operation platform captured 2.023 million new interception cards, of which 97.89% were interception cards belonging to the four major domestic operators, and 2.11% were interception cards belonging to virtual operators.



Interception cards by carrier, H1 2026

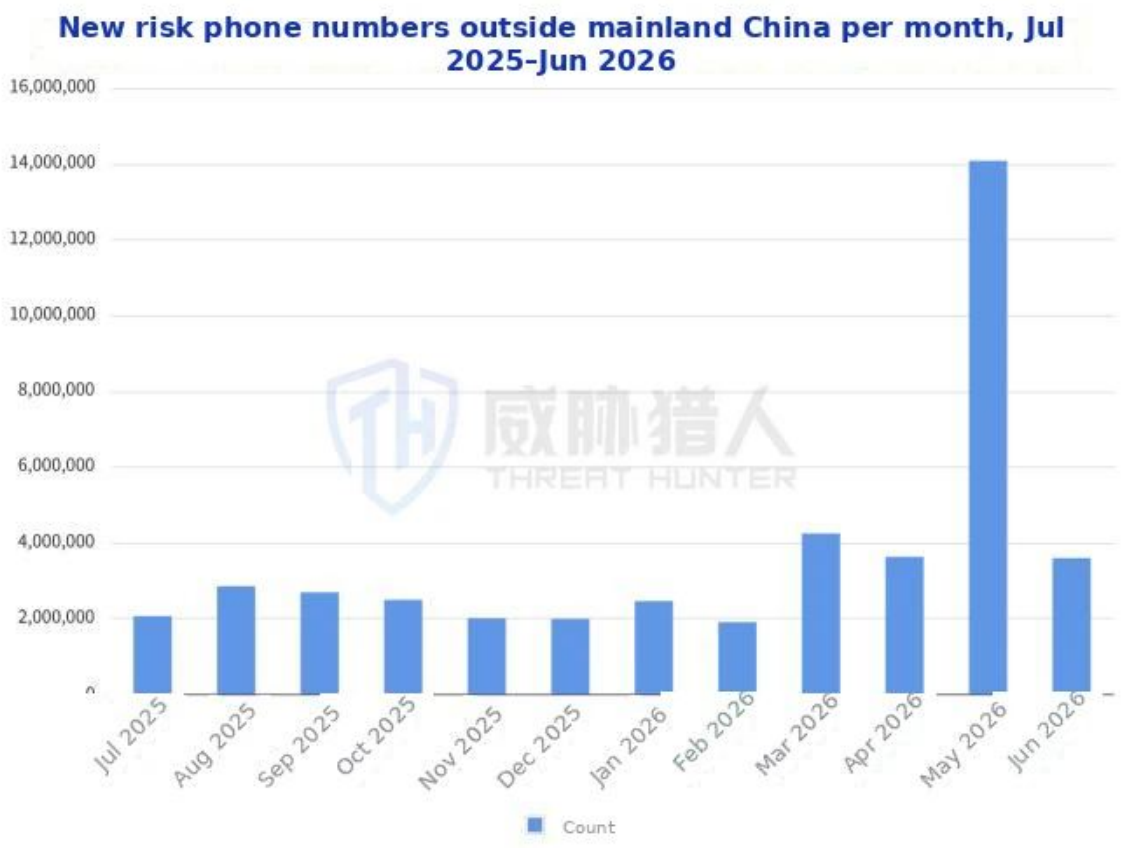
Source: Threat Hunter original report, page 10. Redrawn in English from the original figure.

1.1.4 Resource Change Trends of [Malicious Mobile Phone Cards in Non-Mainland China] in 2026

Non-Mainland China: including Hong Kong, Macau, Taiwan, and all other regions outside mainland China.

(1) In the first half of 2026, SIM-pool cards in non-mainland China areas rose by 110.55% compared with the second half of 2025.

According to data from the Threat Hunter Intelligence Platform, 2.94 million new cases of SIM-pool cards were captured in the first half of 2026, an increase of 110.55% compared with the second half of 2025.



New risk phone numbers outside mainland China per month, Jul 2025–Jun 2026

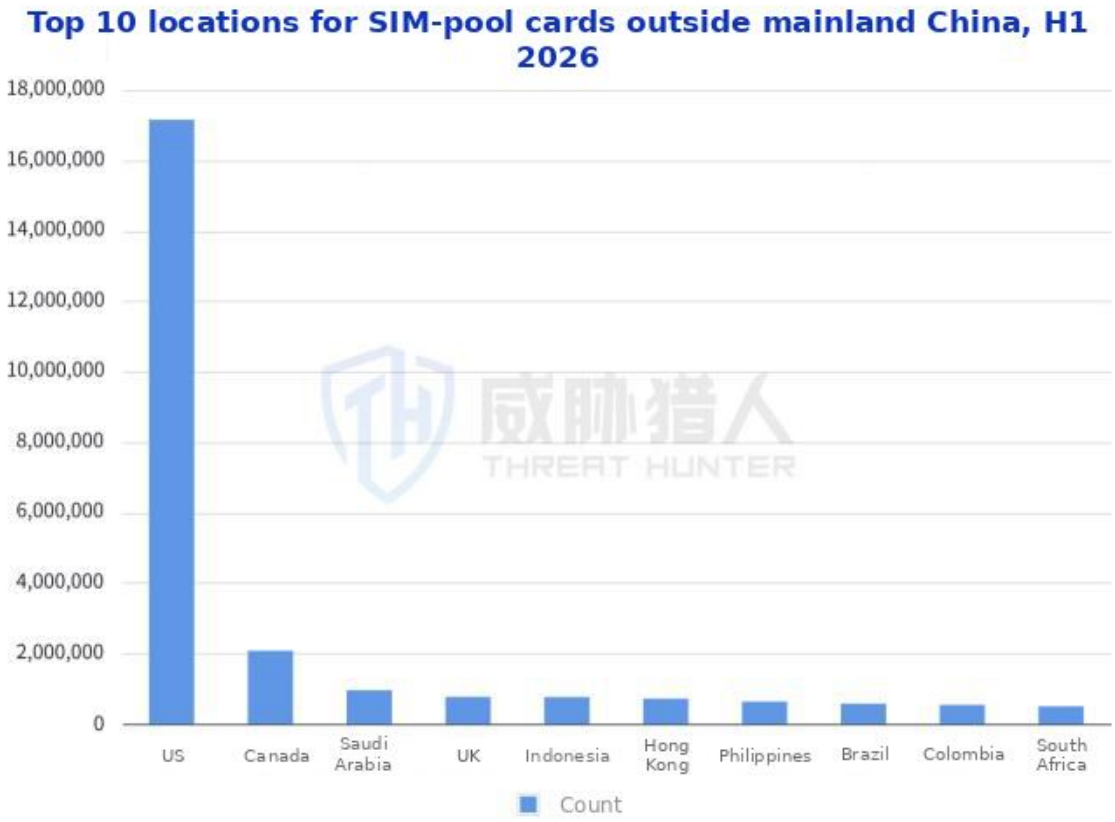
Source: Threat Hunter original report, page 11. Original figure with Chinese text replaced by English.

According to analysis by Threat Hunter intelligence experts, the main reasons for this trend are:

Based on the situation on the cybercrime ecosystem side, in May 2026, a leading code-receiving platform based outside China launched a batch of SIM-pool cards, which significantly expanded the supply of available card sources in the short term, allowing a large number of new numbers to enter the code receiving circulation link and be captured on the platform. Observing the platform, it shows the characteristics of regular batch release of cards every year, rather than sporadic abnormal batch release of cards, reflecting that the supply side of cybercriminal operations in non-mainland China is relatively stable.

(2) Top 3 destinations for new SIM-pool cards in non-mainland China in the first half of 2026: the United States, Canada, and Saudi Arabia

Threat Hunter Intelligence data statistics show that in the first half of 2026, the new SIM-pool cards in non-mainland China are mainly located in the United States, Canada, and Saudi Arabia.



Top 10 locations for SIM-pool cards outside mainland China, H1 2026

Source: Threat Hunter original report, page 11. Original figure with Chinese text replaced by English.

1.2 Analysis of risk IP resources in the first half of 2026

1.2.1 The total daily average active risk IP in the first half of 2026 fell by 16.31% compared with the second half of 2025.

In the first half of 2026, Threat Hunter monitoring found that the average daily number of active risk IPs continued to decline, with the number of risk IPs reaching 11.65 million, a 16.31% decrease from the second half of 2025.



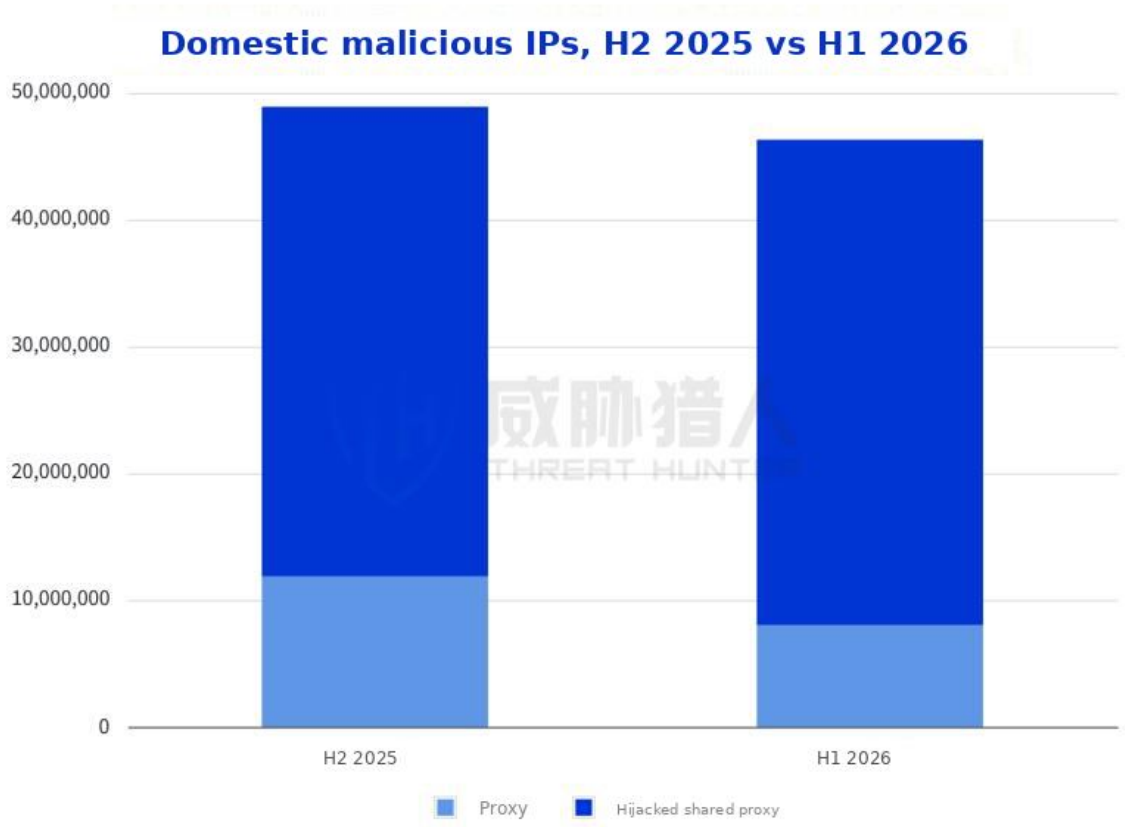
Daily active risk IPs, H2 2025 vs H1 2026

Source: Threat Hunter original report, page 12. Original figure with Chinese text replaced by English.

According to the analysis of Threat Hunter intelligence experts, the main reason for this trend is: the decline in the number of malicious IPs outside China in the first half of 2026 is related to the concentrated attacks on global residential proxy networks and the infrastructure of proxy platforms outside China. In January 2026, a leading global large-scale residential proxy network platform shut down dozens of domain names used to control equipment and proxy traffic. Some proxy nodes failed, the availability of proxy services decreased, and the proxy resources that could be called by cybercriminal operations were compressed.

1.2.2 Analysis of domestic malicious IP resources in the first half of 2026

(1) In the first half of 2026, there were 46.31 million domestic malicious IPs, a decrease of 5.3% from the second half of 2025.

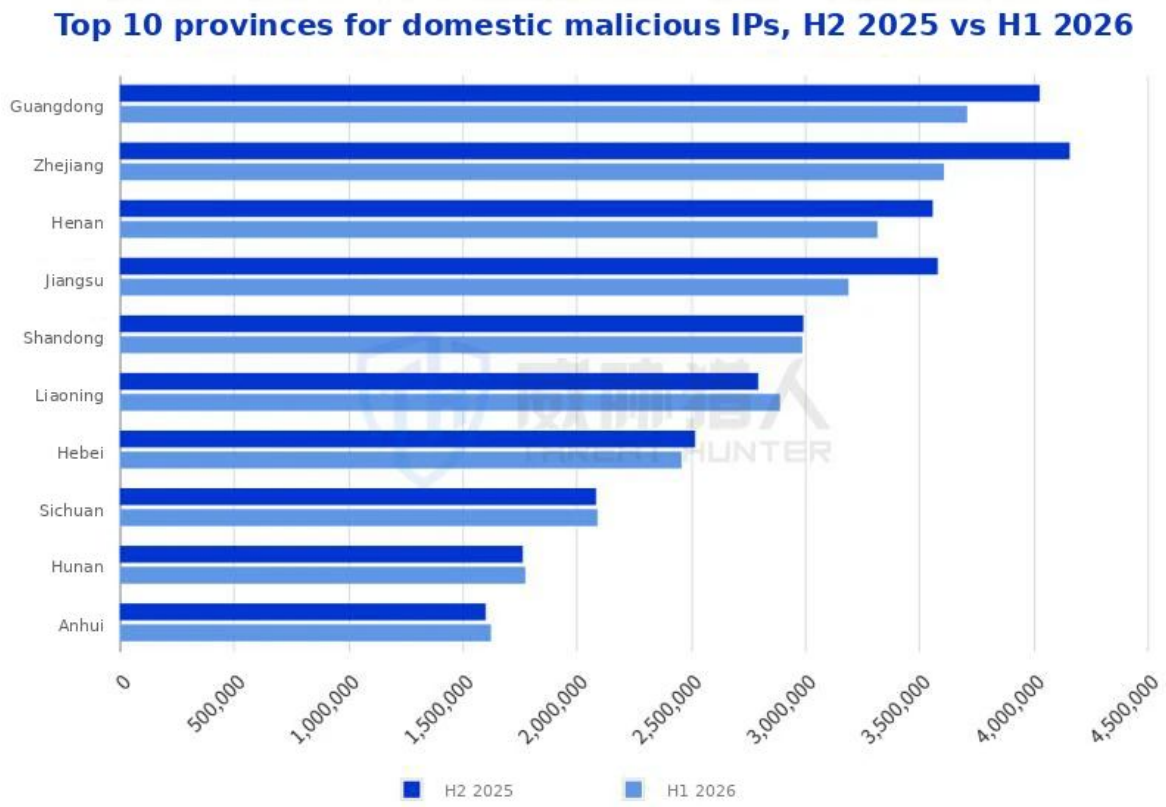


Domestic malicious IPs, H2 2025 vs H1 2026

Source: Threat Hunter original report, page 13. Original figure with Chinese text replaced by English.

(2) Top 3 provinces where domestic malicious IP belongs in the first half of 2026: Guangdong, Zhejiang, and Henan

Threat Hunter Intelligence data statistics show that in the first half of 2026, the provinces (including municipalities) active in domestic malicious IPs are mainly concentrated in Guangdong Province, Zhejiang Province and Henan Province.



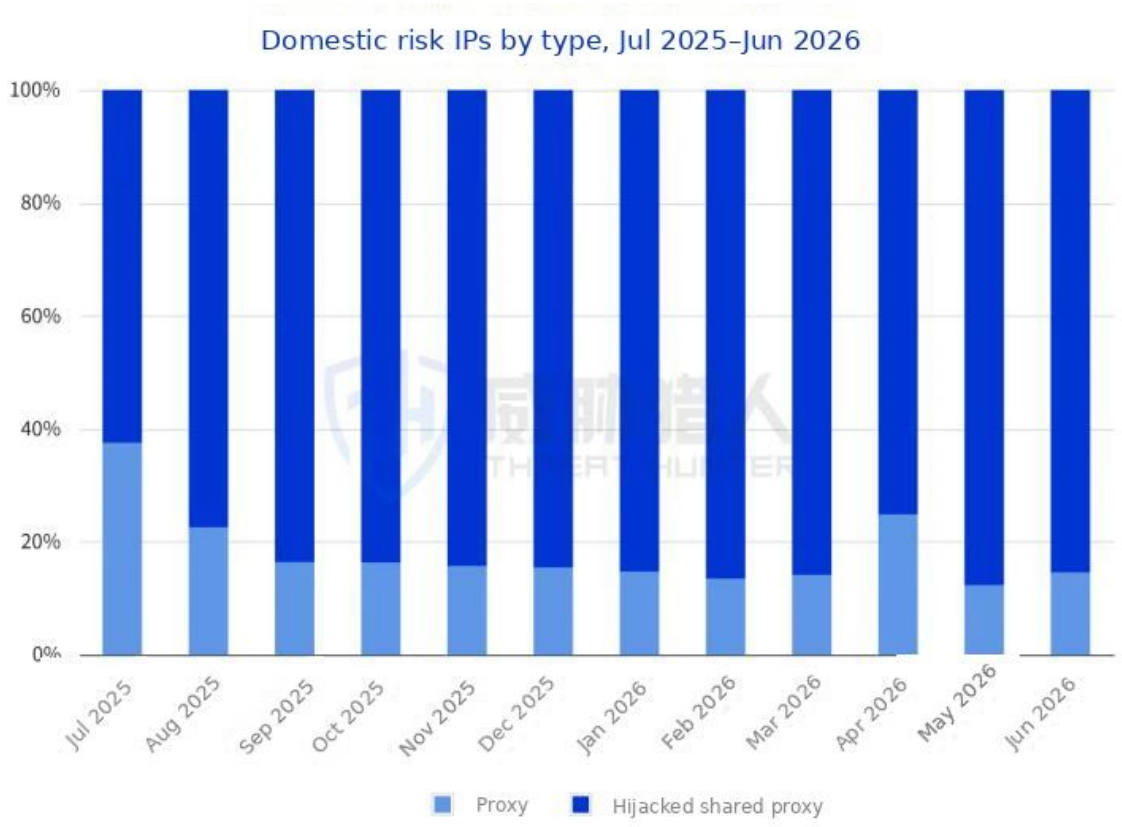
Top 10 provinces for domestic malicious IPs, H2 2025 vs H1 2026

Source: Threat Hunter original report, page 13. Original figure with Chinese text replaced by English.

(3) In the first half of 2026, "hijacking shared proxy" IP attacks accounted for 83.91% of the total, and the supply of IP resources is more stable and the billing model is more diverse.

Threat Hunter continue to monitor the proxy IP platform. Judging from the capture data in the first half of 2026, the average monthly capture number of "hijacked shared proxy" IPs reached 16.3 million.

Since this type of IP is used by normal users most of the time, such as clicking, recharging, browsing, etc., a small amount of time will be hijacked and shared by threat actors, and short-term malicious behaviors will occur. Therefore, the platform may identify the user as a normal user, and then ignore his short-term malicious behaviors, giving threat actors an opportunity to take advantage of.

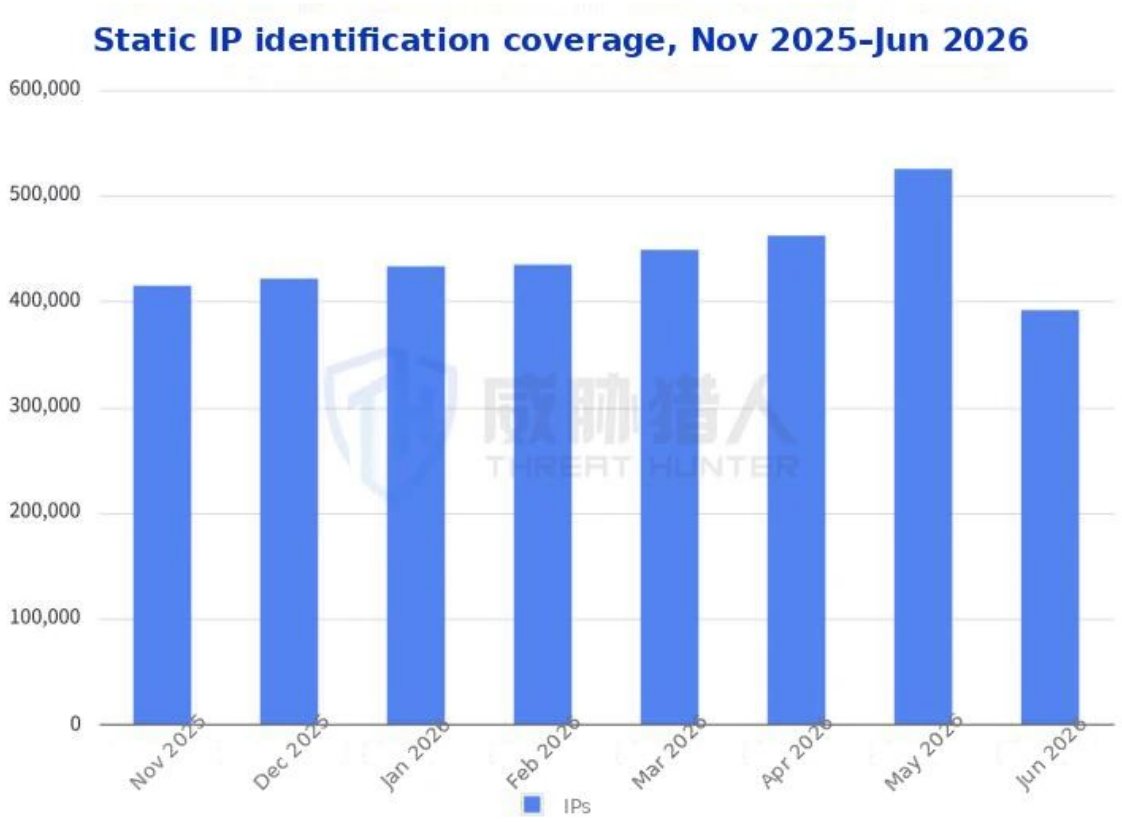


Domestic risk IPs by type per month, Jul 2025–Jun 2026

Source: Threat Hunter original report, page 14. Original figure with Chinese text replaced by English.

(4) IP profiling upgrade: static proxy IP coverage added

In view of the risk scenario where threat actors use static proxy IPs to forge user locations, circumvent fraud controls strategies, and launch batch attacks, the Threat Hunter IP profiling capability has added static proxy IP identification coverage. This capability enables accurate identification and coverage of abnormal proxy networks by continuously precipitating static proxy IP resource characteristics and behavior patterns. Data shows that the overall monthly static proxy IP deduplication coverage remains above 400,000, and will increase to 525,000 in May 2026, an increase of approximately 26.6% from November 2025, and coverage capabilities continue to increase. This capability can help customers identify risky behaviors such as false registration, fraudulent orders, profiteering, and batch login, and improve the accuracy and pre-identification capabilities of business fraud controls and interception.

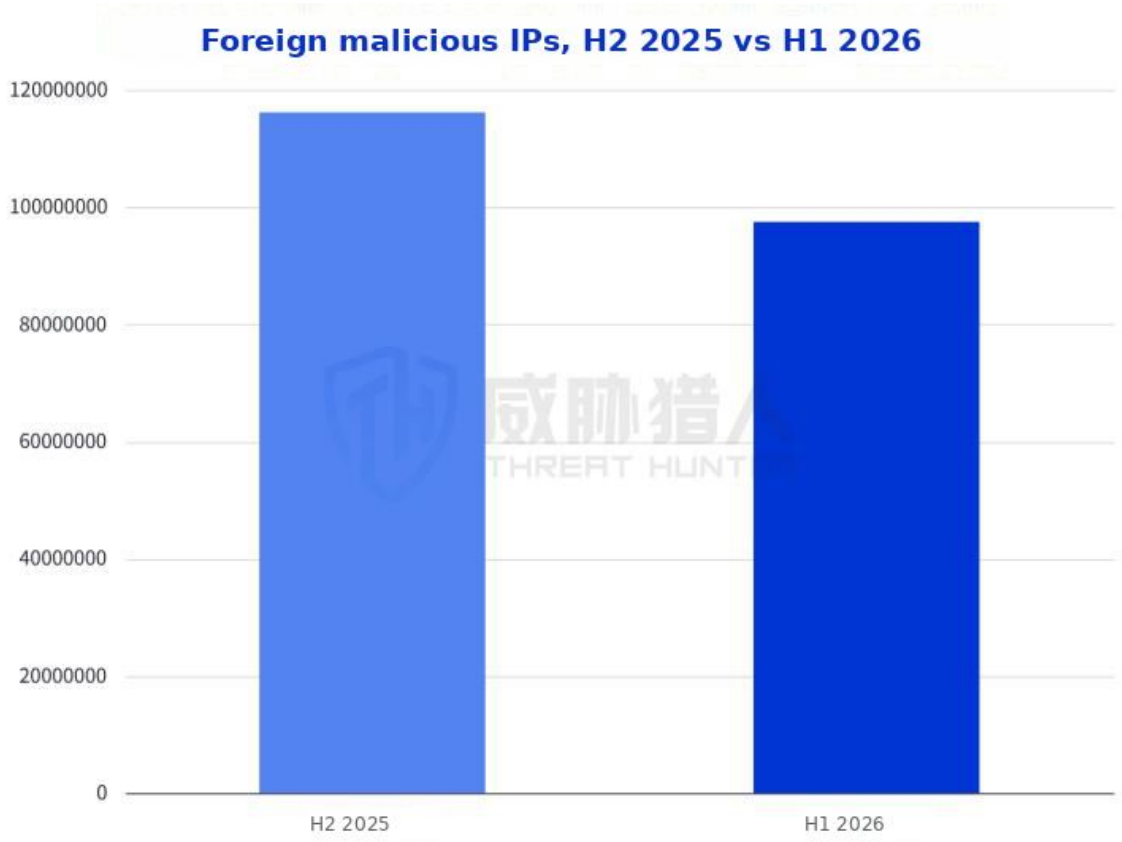


Static IP identification coverage, Nov 2025–Jun 2026

Source: Threat Hunter original report, page 14. Original figure with Chinese text replaced by English.

1.2.3 Analysis of foreign malicious IP resources in the first half of 2026

(1) In the first half of 2026, 9.74 million foreign malicious IPs were captured, a decrease of 16.1% from the second half of 2025.

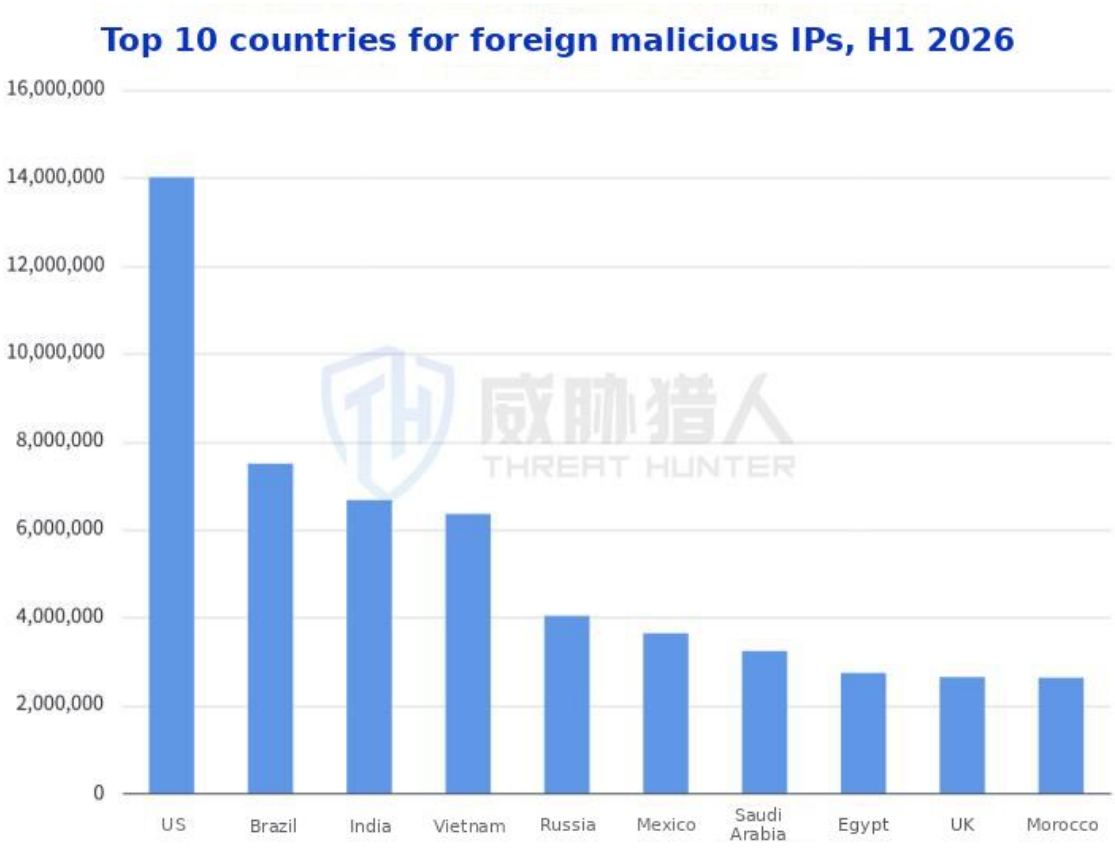


Foreign malicious IPs, H2 2025 vs H1 2026

Source: Threat Hunter original report, page 15. Original figure with Chinese text replaced by English.

(2) Top 3 countries belonging to foreign malicious IPs in the first half of 2026: the United States, Brazil, and India

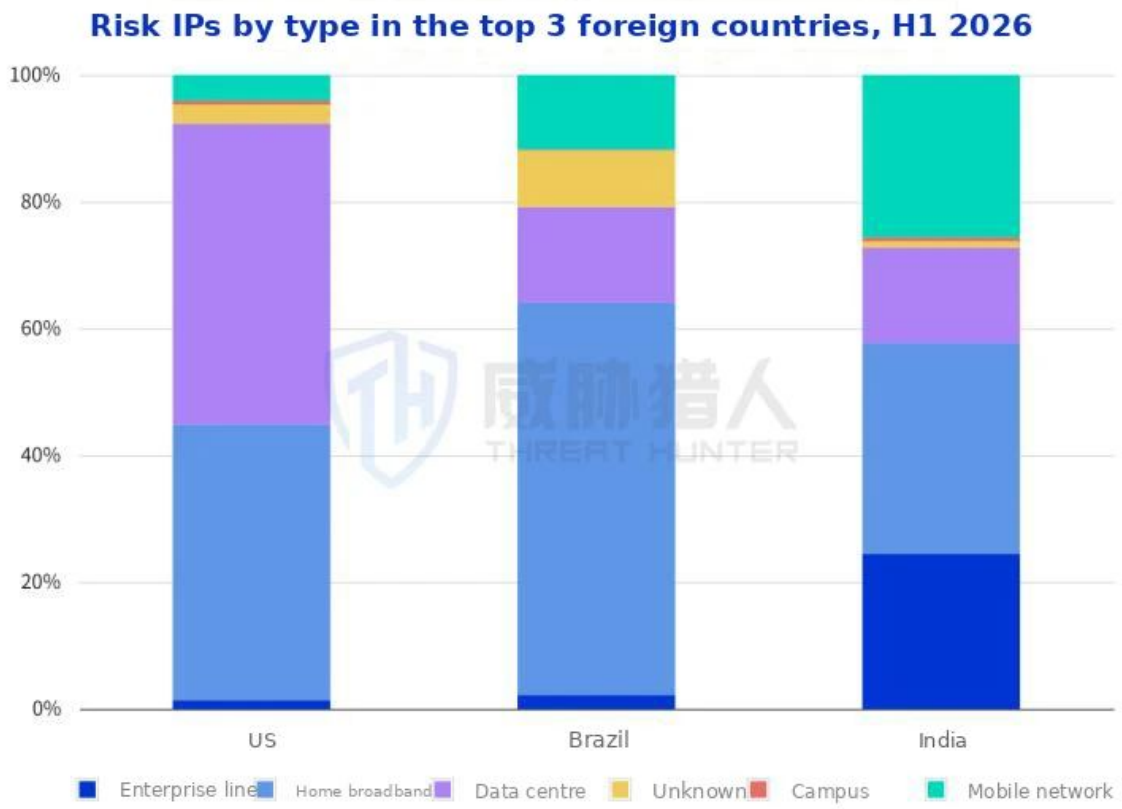
Threat Hunter Intelligence data statistics show that in the first half of 2026, malicious IP countries active abroad are mainly concentrated in the United States, Brazil and India.



Top 10 countries for foreign malicious IPs, H1 2026

Source: Threat Hunter original report, page 15. Original figure with Chinese text replaced by English.

Threat Hunter has discovered that there are differences in the distribution of malicious IP types in different countries. The following is the distribution of malicious IP types in the top 3 foreign countries.



Risk IPs by type in the top 3 foreign countries, H1 2026

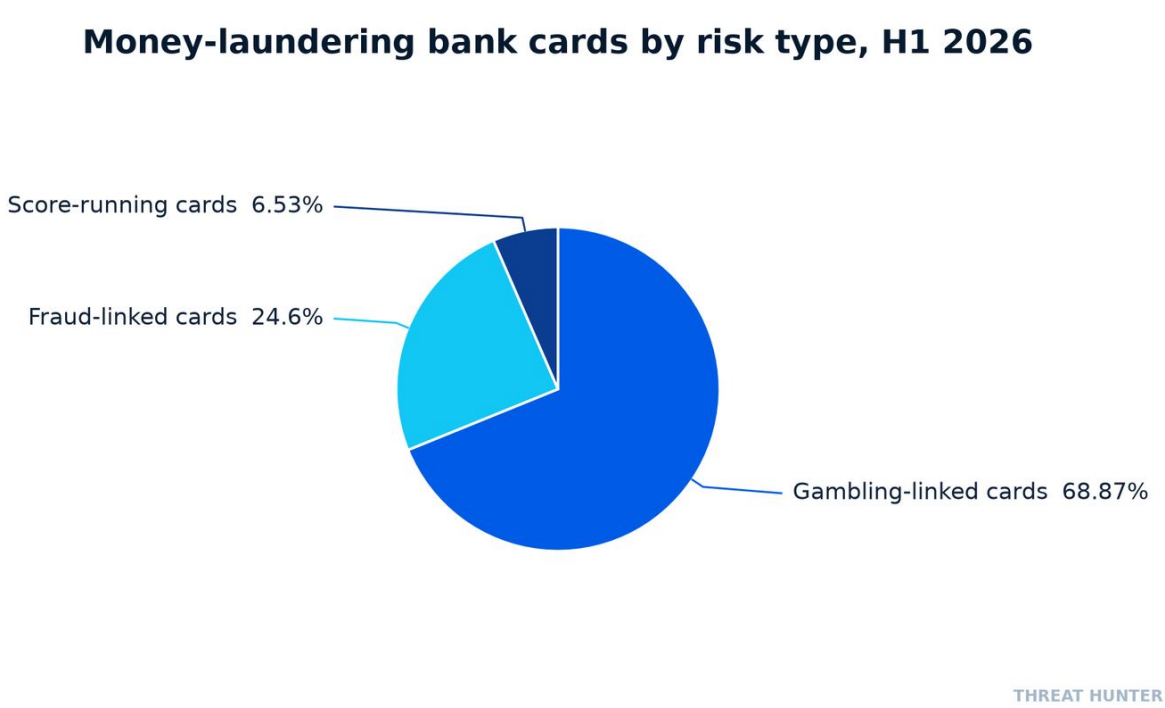
Source: Threat Hunter original report, page 15. Original figure with Chinese text replaced by English.

1.3 Analysis of online money laundering resources in the first half of 2026

1.3.1 Analysis of money laundering bank card resources in the first half of 2026

(1) Among bank cards involved in money laundering in the first half of 2026, gambling-related cards account for the largest proportion, accounting for 68.87%

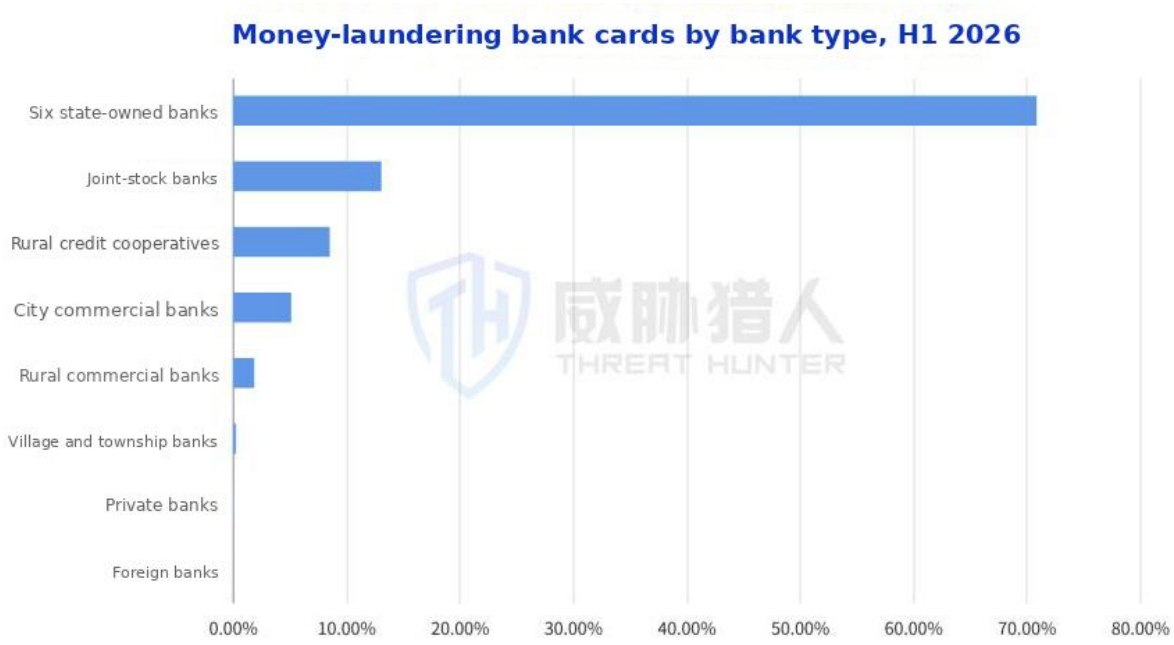
Threat Hunter analyzed 80,000 money laundering bank cards monitored in the first half of 2026 and found that the risk types were mainly concentrated in two categories: gambling-related cards and fraud-related cards. Among them, gambling-related cards accounted for the highest proportion, accounting for 68.87%.



Money-laundering bank cards by risk type, H1 2026

Source: Threat Hunter original report, page 16. Redrawn in English from the original figure.

(2) The proportion of the six major state-owned banks in money laundering bank cards remained stable in the first half of 2026, with little change from the second half of 2025.



Money-laundering bank cards by bank type, H1 2026

Source: Threat Hunter original report, page 16. Original figure with Chinese text replaced by English.

(3) Among the cities where bank cards involved in money laundering belong to in the first half of 2026, the top three cities are: Shenzhen, Chongqing, and Guangzhou



Top 10 cities for money-laundering bank cards, H1 2026

Source: Threat Hunter original report, page 17. Original figure with Chinese text replaced by English.

1.3.2 Analysis of money laundering corporate account resources in the first half of 2026

(1) In the first half of 2026, the number of new public accounts for money laundering decreased by 70.81% month-on-month, and related money laundering groups decreased by 21.29%

Threat Hunter monitoring data in the first half of 2026 shows that the number of new public accounts used for money laundering dropped by 70.81% compared with the second half of 2025, and the number of related money laundering groups simultaneously decreased by 21.29%. Overall, the scale and degree of organization of corporate money laundering activities have shrunk significantly.

Threat Hunter analysis found that the main reason is that the capital channels of cybercrime operations have been continuously frustrated: "Haowang" in May 2025 and "Potato Guarantee" were successively attacked in January 2026, and the capital circulation channels of cybercrime operations were repeatedly cut off; at the same time, frequent problems occurred in the guarantee system, internal trust of cybercrime operations decreased, and collaboration was blocked, further compressing the space for money laundering activities.

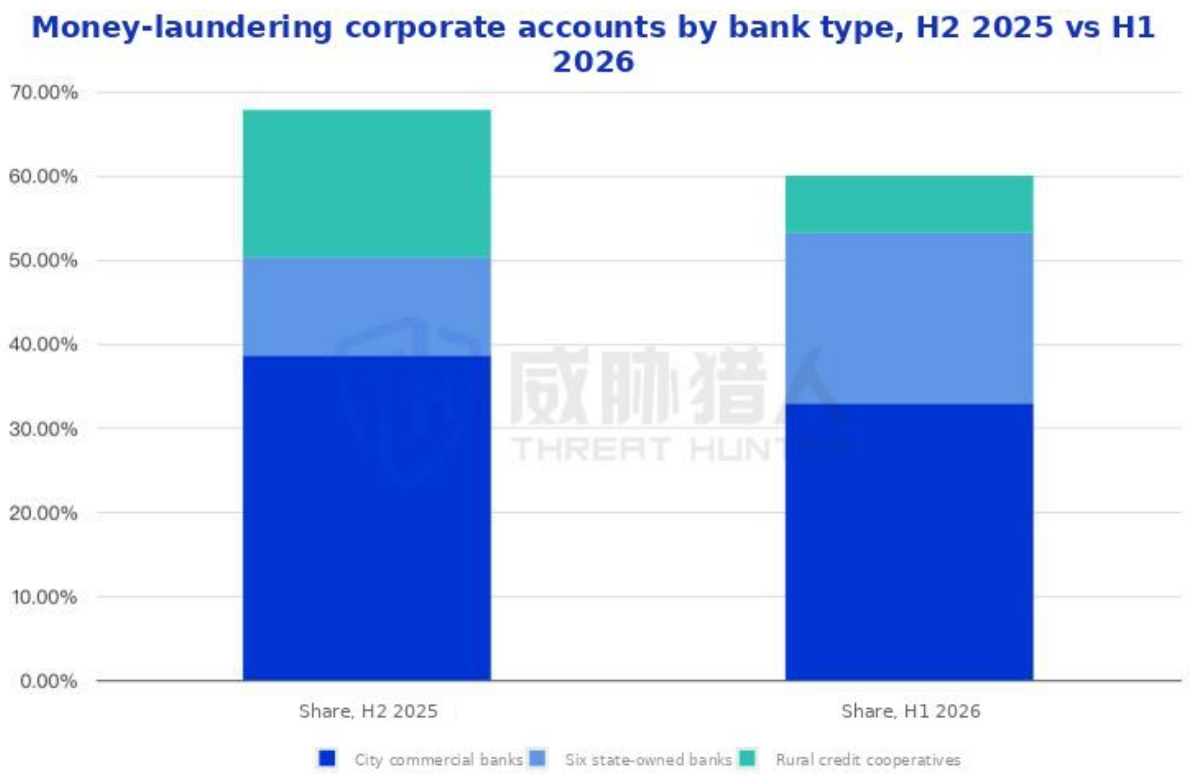


New money-laundering corporate accounts, H2 2025 vs H1 2026

Source: Threat Hunter original report, page 17. Original figure with Chinese text replaced by English.

(2) In the first half of 2026, among the banks with corporate money laundering accounts, there was a shift from rural credit cooperatives to the six major state-owned banks.

Threat Hunter monitoring data in the first half of 2026 shows that the distribution of banks with public accounts for money laundering has changed significantly: the proportion of rural credit cooperatives dropped from 17.55% in the second half of 2025 to 6.78%; the proportion of the six major state-owned banks increased from 11.66% to 20.34%. Overall, there is a trend of money laundering public accounts moving from rural credit cooperatives to the six major state-owned banks.



Money-laundering corporate accounts by bank type, H2 2025 vs H1 2026

Source: Threat Hunter original report, page 18. Original figure with Chinese text replaced by English.

(3) Among the provinces where money laundering public accounts belong in 2026, the top three provinces are Guangdong, Jiangsu, and Zhejiang



Top 10 provinces for money-laundering corporate accounts, H1 2026

Source: Threat Hunter original report, page 18. Original figure with Chinese text replaced by English.

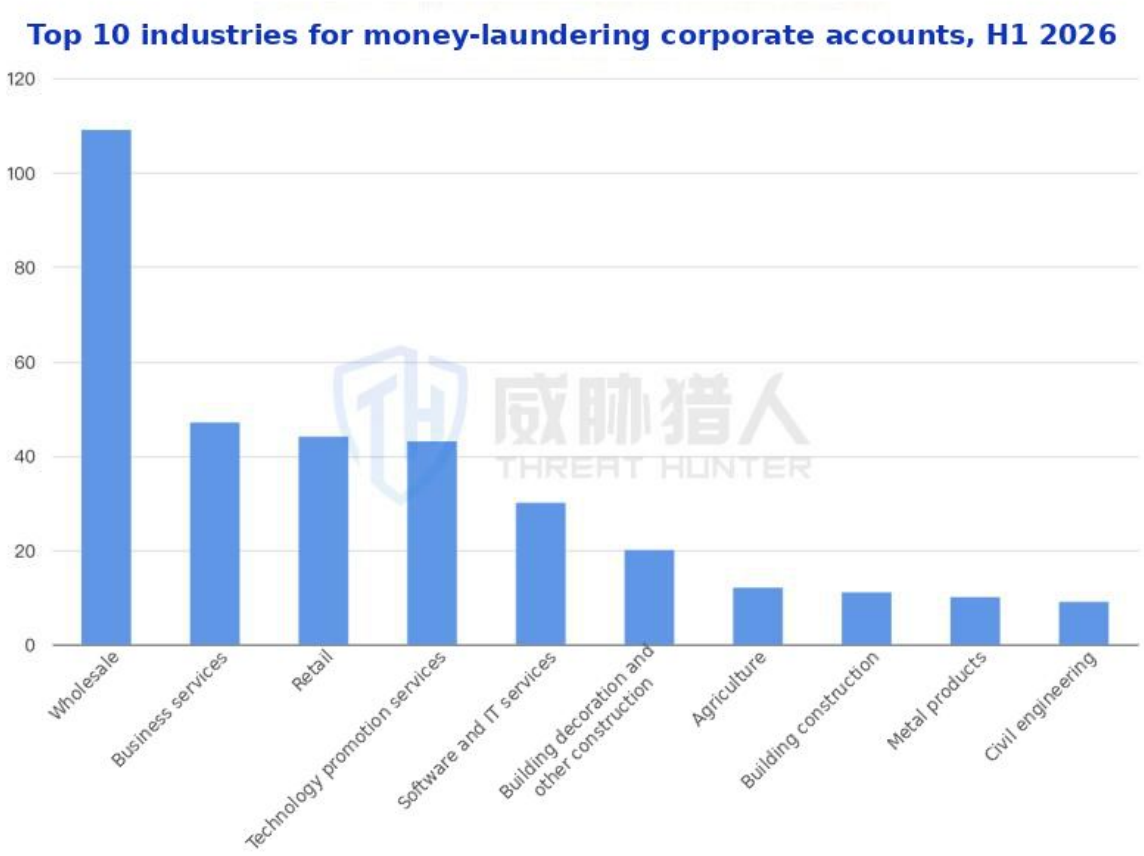
(4) Among the cities with money laundering public accounts in 2026, the top three cities are Shenzhen, Shanghai, and Chengdu



Top 10 cities for money-laundering corporate accounts, H1 2026

Source: Threat Hunter original report, page 18. Original figure with Chinese text replaced by English.

(5) Among the industries to which money laundering public accounts belong in 2026, the top three industries are wholesale industry, business service industry, and retail industry.



Top 10 industries for money-laundering corporate accounts, H1 2026

Source: Threat Hunter original report, page 19. Original figure with Chinese text replaced by English.

1.3.3 Analysis of money laundering merchant resources in the first half of 2026

(1) In the first half of 2026, the number of merchants used by cybercriminal groups to launder money decreased by 48.23% month-on-month.

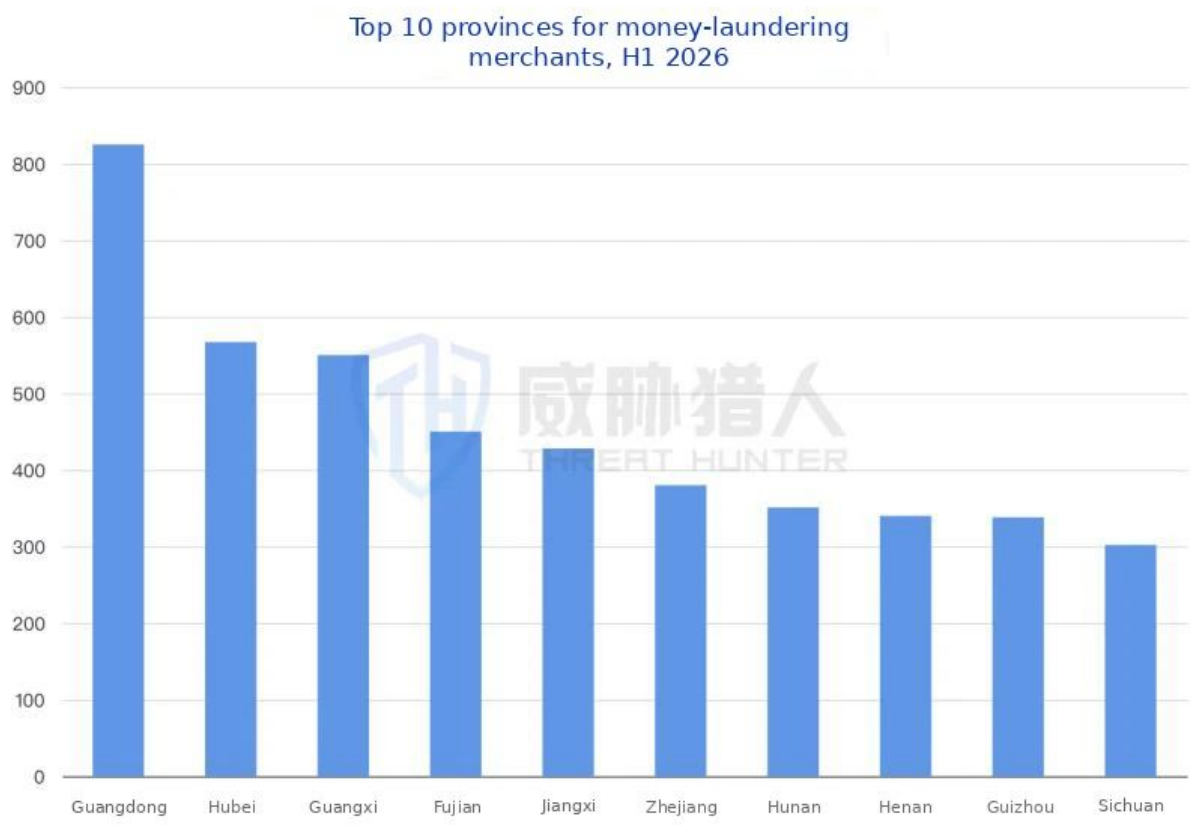
In the first half of 2026, the number of merchants used by cybercriminal groups for money laundering dropped by 48.23% compared with the second half of 2025, showing a clear downward trend. It is mainly related to the crackdown on the above-mentioned guaranteed cybercriminal operation channels.



New money-laundering merchants, H2 2025 vs H1 2026

Source: Threat Hunter original report, page 19. Original figure with Chinese text replaced by English.

(2) Among the provinces where money laundering merchants belong in the first half of 2026, the top three provinces are Guangdong, Guangxi, and Hubei



Top 10 provinces for money-laundering merchants, H1 2026

Source: Threat Hunter original report, page 20. Original figure with Chinese text replaced by English.

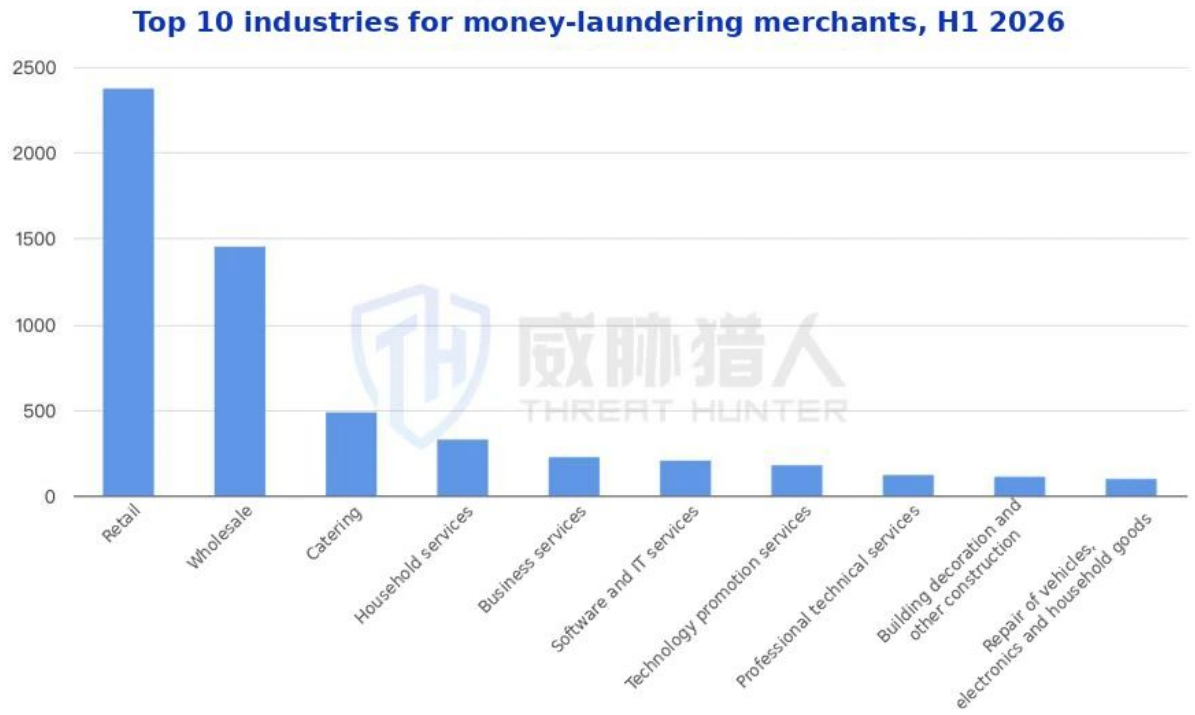
(3) Among the cities where money laundering merchants belong in the first half of 2026, the top three cities are Guangzhou, Wuhan, and Shenzhen



Top 10 cities for money-laundering merchants, H1 2026

Source: Threat Hunter original report, page 20. Original figure with Chinese text replaced by English.

(4) Among the industries to which money laundering merchants belong in the first half of 2026, the top three industries are retail, wholesale, and catering industries



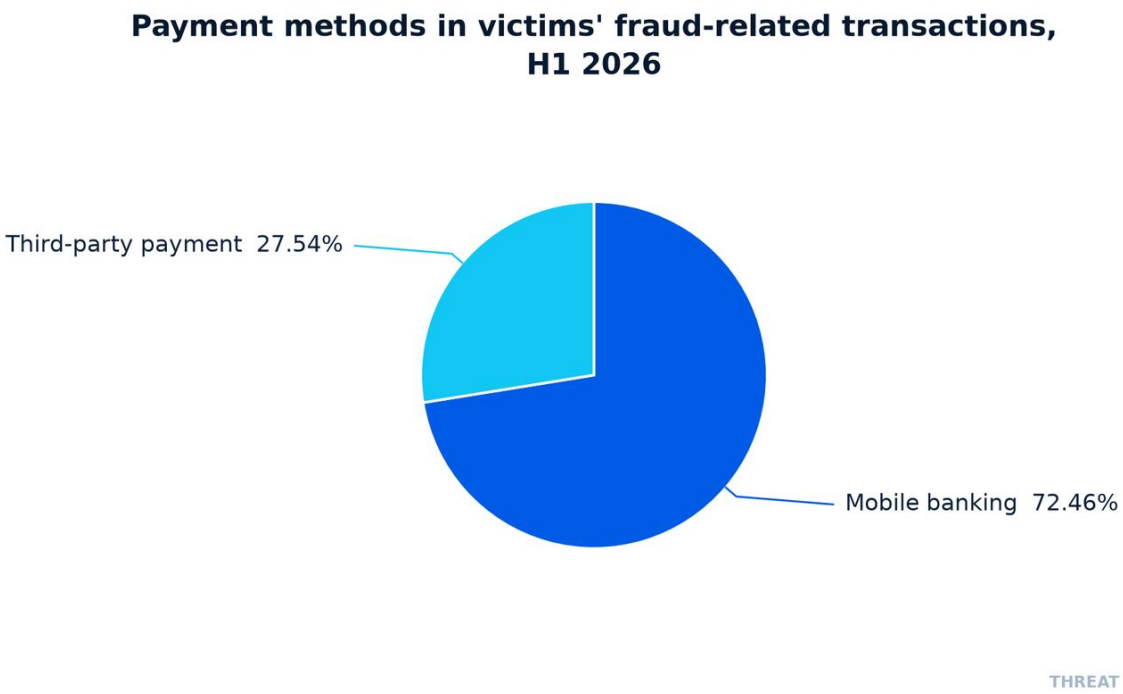
Top 10 industries for money-laundering merchants, H1 2026

Source: Threat Hunter original report, page 20. Original figure with Chinese text replaced by English.

1.3.4 Analysis of money laundering victim resources in the first half of 2026

(1) In the first half of 2026, fraud-related transactions are mainly mobile bank transfers, accounting for 72.46%

Based on the data analysis of 35,000 victim-related fraud transactions newly monitored in the first half of the year, Threat Hunter found that mobile banking transfers dominate the flow of fraudulent funds, accounting for 72.46% of all fraud-related transactions, and are the main channel for cybercrime operations to guide victims to complete fund transfers.

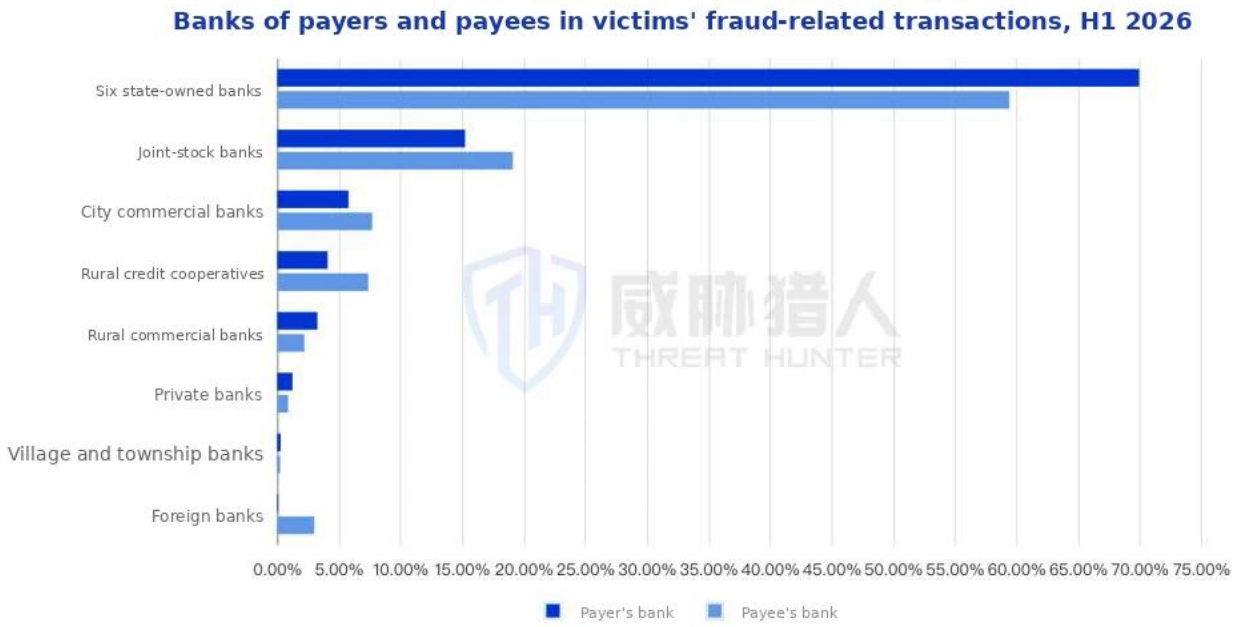


Payment methods in victims' fraud-related transactions, H1 2026

Source: Threat Hunter original report, page 21. Redrawn in English from the original figure.

(2) In fraudulent transactions in the first half of 2026, both the fund transfer parties and the illegal recipient banks are highly concentrated in the six major state-owned banks.

Threat Hunter's monitoring of fraud-related transaction data shows that the six major state-owned banks accounted for 69.97% of the banks where victims' funds were transferred out; and the six major state-owned banks accounted for 59.43% of the banks receiving money laundering funds from illegal assets. The data shows that banks on both sides of the fraud-related capital flow link show a high degree of concentration.



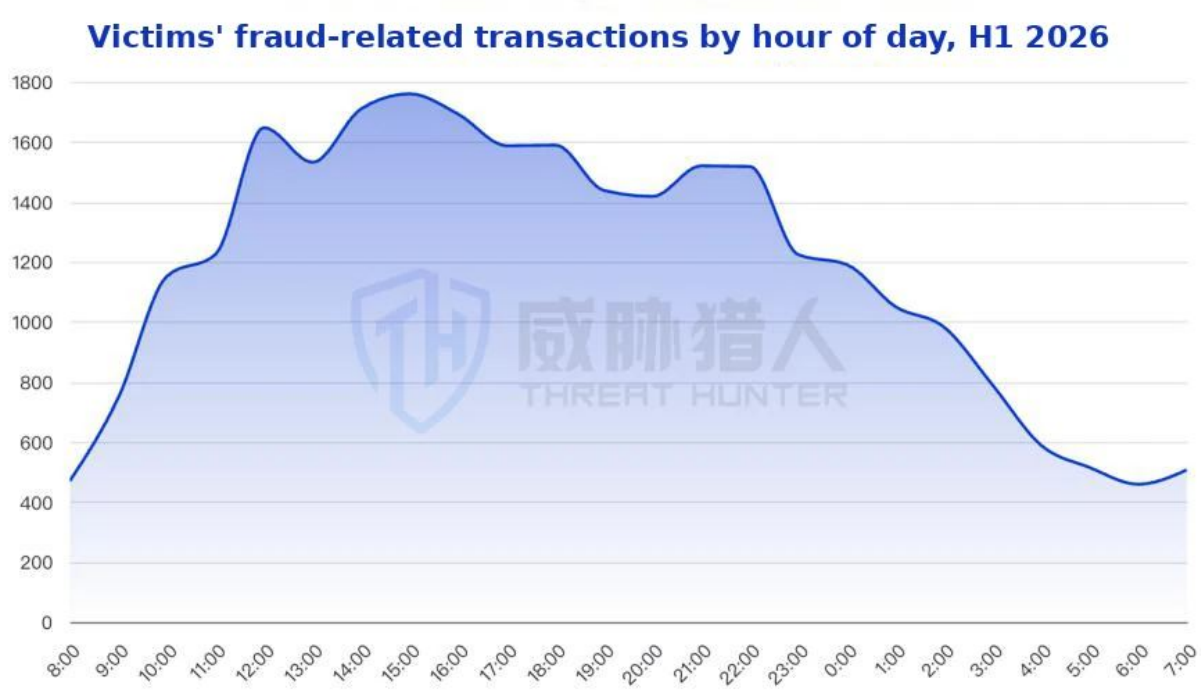
Banks of payers and payees in victims' fraud-related transactions, H1 2026

Source: Threat Hunter original report, page 21. Original figure with Chinese text replaced by English.

(3) The peak value of fraud-related transactions in the first half of 2026 was between 14:00 and 16:00

Threat Hunter analysis found that the time distribution of fraudulent transactions in the first half of 2026 showed two characteristics:

- The trading peak is concentrated between 14:00 and 16:00, with the highest at 15:00 (1488 transactions), followed by 14:00 (1440 transactions) and 16:00 (1446 transactions), forming a continuous high range.
- In terms of overall distribution, fraud-related transactions gradually increased from the morning (the increase was obvious after 10:00), reached a peak in the afternoon and then fell back; it remained at a relatively high level in the evening (19:00–22:00), and reached a low point from early morning to early morning (0:00–7:00). The overall distribution is basically consistent with the schedule of domestic personnel.



Victims' fraud-related transactions by hour of day, H1 2026

Source: Threat Hunter original report, page 22. Original figure with Chinese text replaced by English.

(4) In the first half of 2026, the amount of fraudulent transfers is concentrated in the integer range of 1,000 yuan, with 1,000 yuan and 5,000 yuan being the most obvious.

Threat Hunter analyzed the distribution of fraud transaction amounts and found that the victims' fraud transfer amounts were not randomly distributed, but were significantly clustered in multiple integer ranges, mainly around 1,000 yuan, 2,000 yuan, 3,000 yuan, 4,000 yuan and 5,000 yuan.

Among them, the number of transactions around 1,000 yuan and 5,000 yuan is more prominent, indicating that cybercrime operations tends to operate around a specific amount range when guiding victims to transfer funds. Some amount ranges may have become common amounts in fraudulent fund transfers.



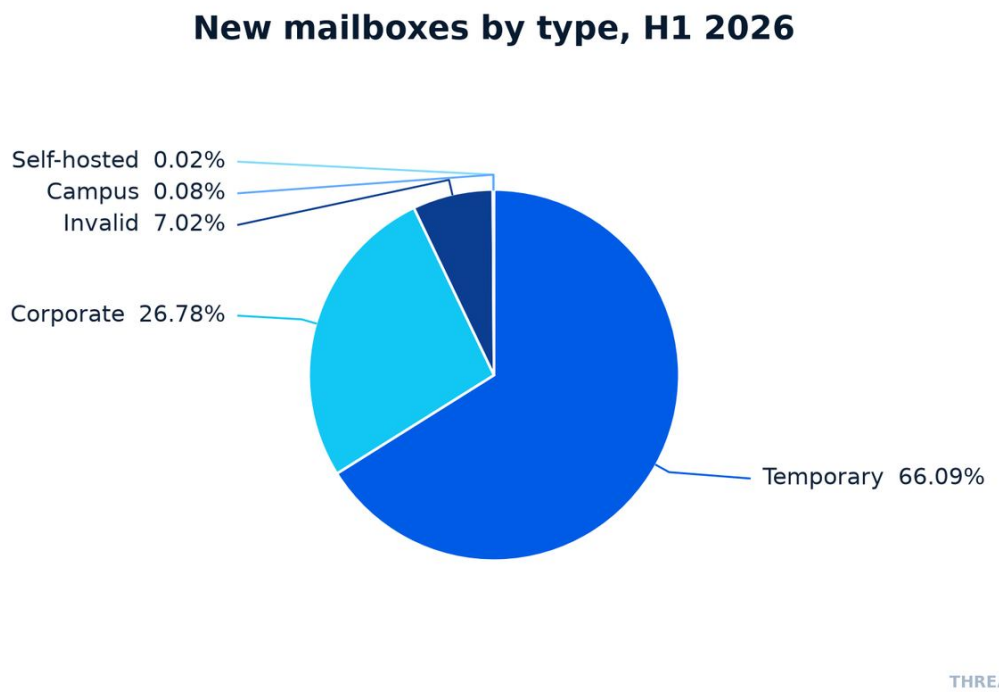
Victims' fraud-related transactions by amount, H1 2026

Source: Threat Hunter original report, page 22. Original figure with Chinese text replaced by English.

1.4 Analysis of risk mailbox resources in the first half of 2026

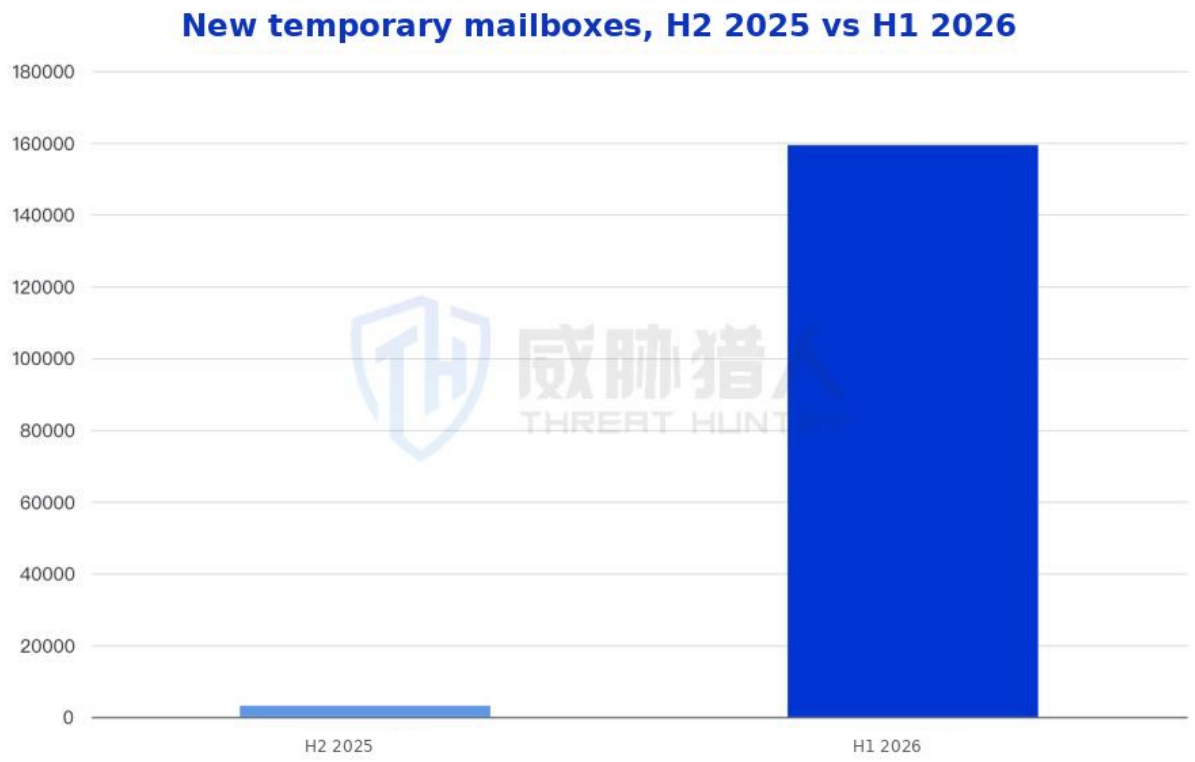
1.4.1 In the first half of 2026, the proportion of temporary email domain names reached 66.09%, and new additions grew about 50-fold compared with the second half of 2025.

Threat Hunter added 159,200 temporary email domain names in the first half of 2026, accounting for 66.09% of the total new email domain names. Compared with the second half of 2025, new additions grew roughly 50-fold. The growth mainly comes from the 400+ mainstream temporary mailbox service sites around the world, which has significantly improved the temporary mailbox identification capabilities.



New mailboxes by type, H1 2026

Source: Threat Hunter original report, page 23. Redrawn in English from the original figure.



New temporary mailboxes, H2 2025 vs H1 2026

Source: Threat Hunter original report, page 23. Original figure with Chinese text replaced by English.

2. Analysis of cybercrime attack scenarios in the first half of 2026

2.1 Business fraud scenario analysis

2.1.1 Business fraud risk landscape in the first half of 2026

2.1.1.1 In the first half of 2026, the risk of online business fraud continues to be hot, with a total of approximately 900 million risk line reports

In the first half of 2026, the Threat Hunter anti-fraud intelligence platform captured approximately 900 million business fraud risk reports. The peak occurred in June, with approximately 243 million items, accounting for more than a quarter of the first half of the year. The volume of cybercrime operations activities essentially follows the rhythm of the platform’s marketing budget: major promotion nodes where subsidies are concentrated are the nodes where cybercriminal operations are harvested intensively.



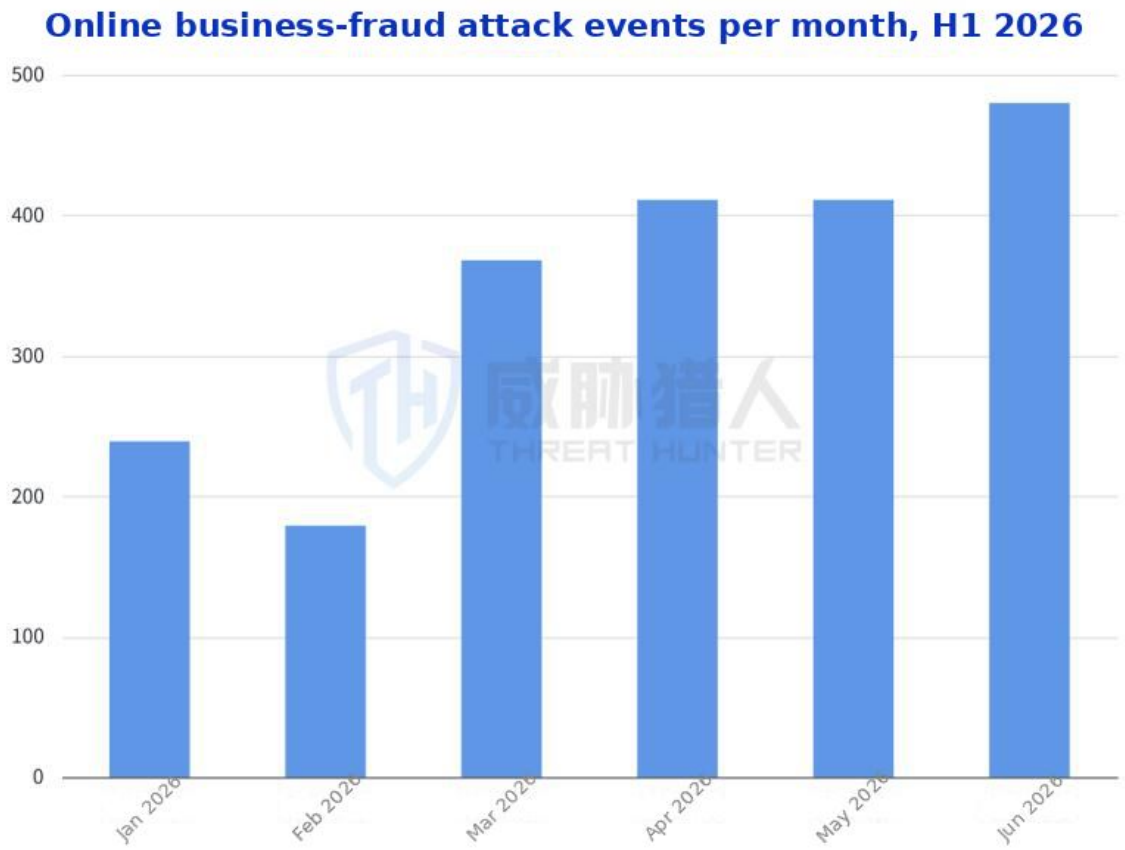
Online business-fraud attack intelligence per month, H1 2026

Source: Threat Hunter original report, page 25. Original figure with Chinese text replaced by English.

2.1.1.2 Early warning business fraud risk events reached 2,088 in the first half of 2026

A total of 2,088 business fraud risk events were warned in the first half of the year, and 1,302 in the second quarter, an increase of approximately 65.54% from the first quarter (786). Different from the single peak of online reporting volume, the number of incidents has remained above 400

for three consecutive months since April; cybercriminal operations did not break out once at the big promotion node, but maintained high-intensity attacks throughout the second quarter.

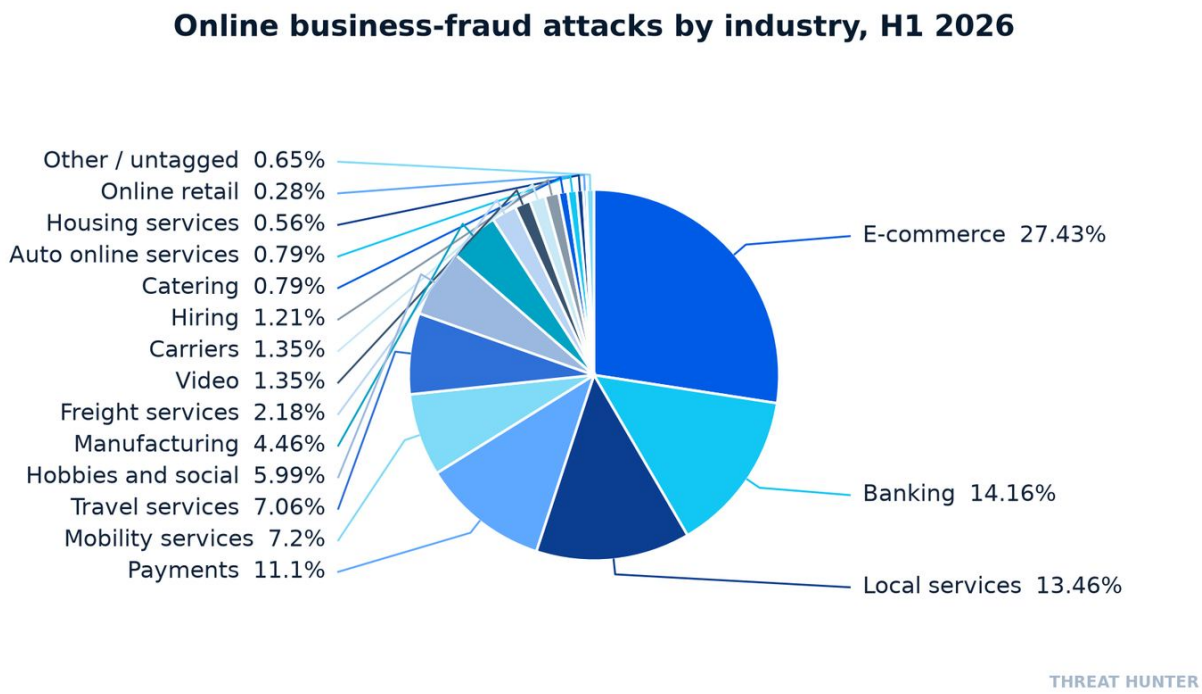


Online business-fraud attack events per month, H1 2026

Source: Threat Hunter original report, page 26. Original figure with Chinese text replaced by English.

2.1.1.3 The industrial distribution of cybercrime operations attacks is concentrated in high-frequency transactions, high subsidies, and high-traffic Internet business scenarios, with e-commerce accounting for 27.44% of the total.

E-commerce topped the list with 27.44%; the financial sector (banking 14.16% + payment 11.10%) followed closely with a total of 25.26%; local life (13.46%) and travel and tourism (14.26%) followed - the four major sectors accounted for 80.24% in total. Wherever the subsidies and traffic are, there are cybercriminal operations: big promotion subsidies, marketing rights, and high-frequency orders constitute the three main cash flow entrances for cybercrime operations arbitrage in the first half of the year.

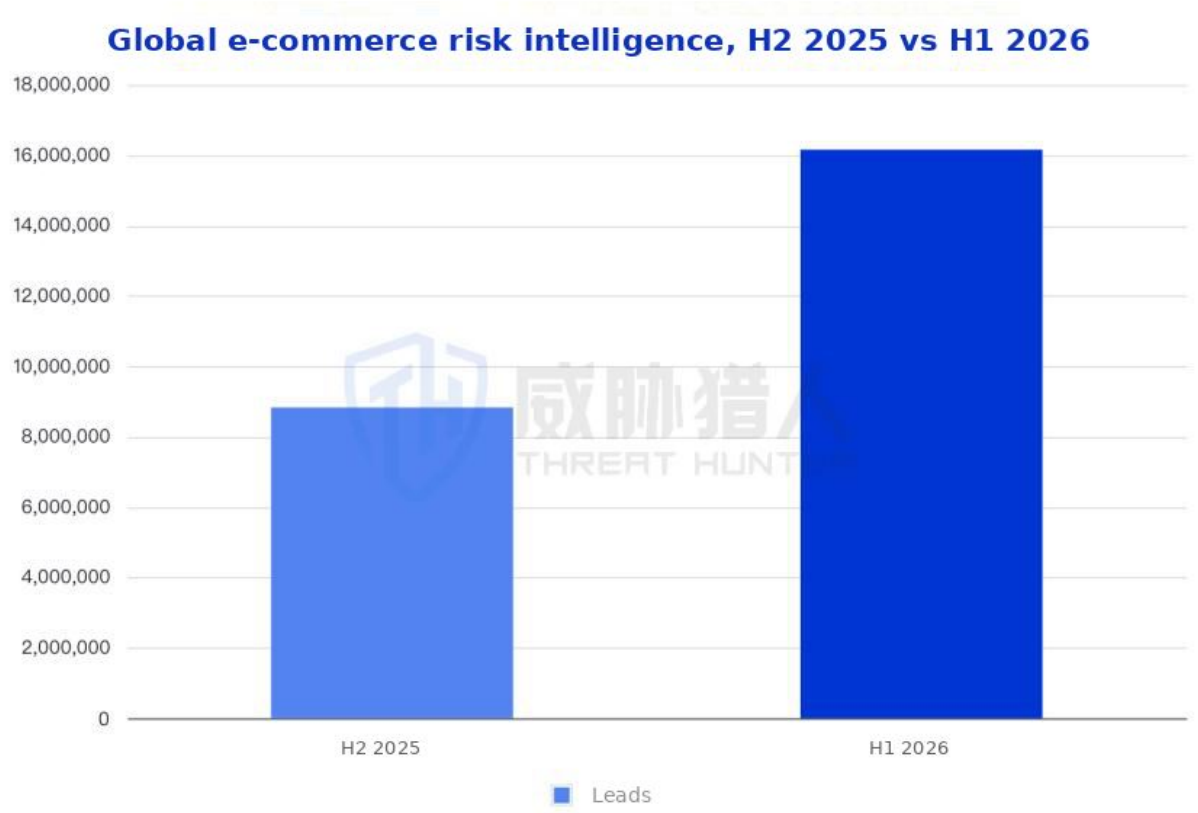


Online business-fraud attacks by industry, H1 2026

Source: Threat Hunter original report, page 26. Redrawn in English from the original figure.

2.1.1.4 The scale of e-commerce cybercrime risk intelligence jumped to 16.15 million, a month-on-month increase of 83%

The amount of e-commerce risk intelligence in the first half of 2026 was 16.15 million, an increase of 7.32 million from 8.83 million in the second half of 2025, a month-on-month increase of 83%.

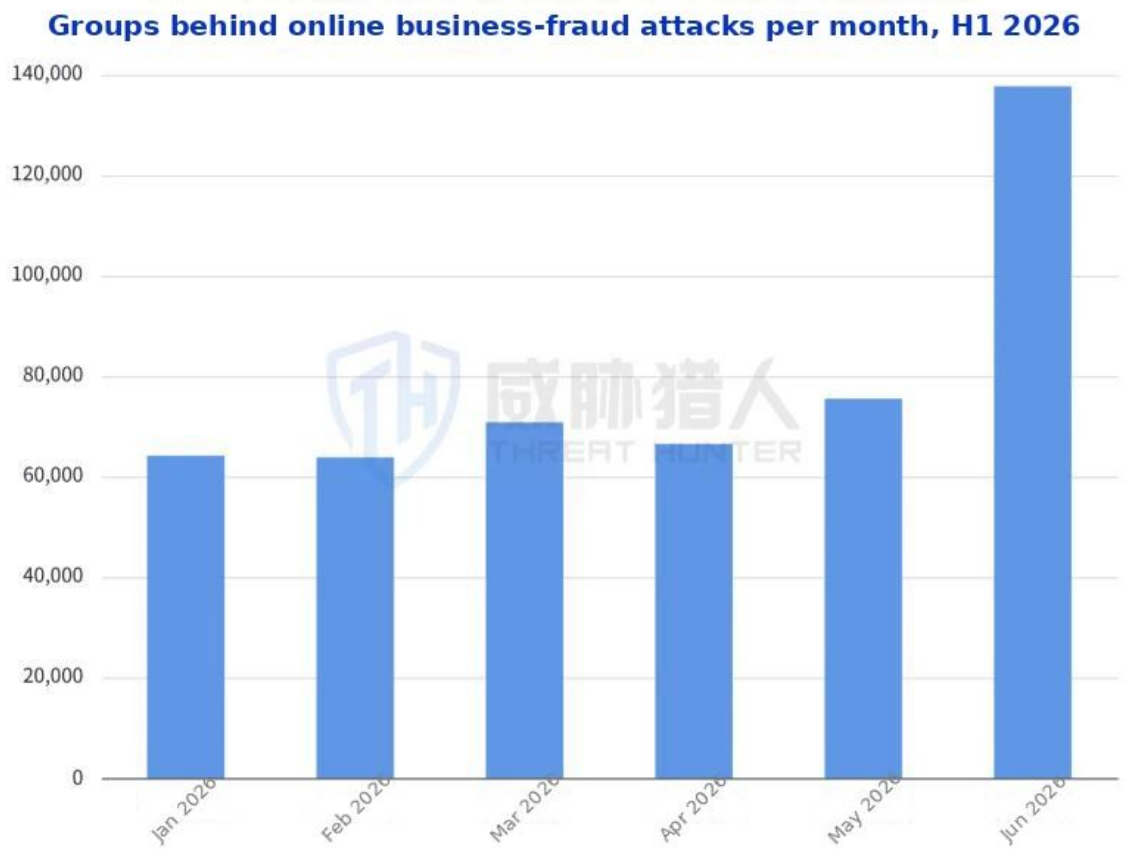


Global e-commerce risk intelligence, H2 2025 vs H1 2026

Source: Threat Hunter original report, page 27. Original figure with Chinese text replaced by English.

2.1.1.5 In the first half of 2026, the monthly average number of captured criminal groups and forums was about 80,000

The Threat Hunter Anti-Fraud Intelligence Platform captured approximately 80,000 criminal groups and forums each month in the first half of the year, which increased sharply to approximately 138,000 in June, nearly double the number in the previous month. Groups are the organization and mobilization unit of cybercriminal operations. This large-scale increase shows that cybercriminal operations have carried out organized temporary expansion before the big promotion - rather than the natural activity of existing groups. Whether it will fall back after the holiday and how much will be retained are signals worth tracking in the second half of the year.



Groups behind online business-fraud attacks per month, H1 2026

Source: Threat Hunter original report, page 27. Original figure with Chinese text replaced by English.

2.1.1.6 In the first half of 2026, the monthly average number of malicious accounts captured was approximately 1.15 million

In the first half of the year, an average of approximately 1.15 million active malicious accounts were captured each month, with a peak number of approximately 1.35 million in June. Accounts are consumables for criminals. Compared with May, the growth rate is much smaller than the expansion rate of cybercriminal groups at the same time. The cybercriminal operators of big promotion nodes mainly rely on new group chats to commit malicious. The account pool itself is a stock asset that has been cultivated for a long time. This is confirmed by the data of normal account maintenance and centralized realization of big sales.



Accounts behind online business-fraud attacks per month, H1 2026

Source: Threat Hunter original report, page 28. Original figure with Chinese text replaced by English.

2.1.2 Key trends and typical cases of cybercrime operations attacks in the first half of 2026

In the first half of 2026, business fraud and cybercriminal operations showed stronger "industrialization, organization, and confrontation" characteristics. This chapter selects several of the most representative industry trends that have rarely been systematically disclosed in previous reports: the integrated infringement chain of brand "recycling-channelling-counterfeiting-trampling", the "industrialization of agency distribution" that leads to gambling on World Cup events, and the industry chain of FMCG brands placing orders on behalf of others, and dismantles their industrial structure, scale evolution and crime links one by one, and attaches actual arrest cases.

2.1.2.1 The brand’s integrated cybercrime operations chain of “recycling – grey-market diversion – counterfeits – smear content”

- Trend judgment

Threat Hunter monitoring found that in the first half of 2026, brand infringement in categories with high customer unit prices and strong channel control, such as maternal and infant health care and clothing, is no longer limited to scattered fakes or channeled goods, but has gradually formed an integrated link of "recycling of genuine products - low-priced channeled goods - mixed sales of fakes - competing products", supplemented by scalpers, preferential arbitrage and other means.

This type of risk also affects the brand's channel price, product reputation and intellectual property rights, and has evolved from a single point of infringement into a systemic brand management risk. Taking a maternal and infant health care brand as an example, we can restore the operation of this link more completely.

- Industrial chain dismantling

The infringement of a certain maternal and infant brand (high customer unit price, strong channel control category) has evolved from scattered fakes and channeled goods to an integrated industry chain with four-stage coordination and long-term stable operation of "recycling-channelled goods-fake goods-trading":

Upstream recycling of genuine products. Cybercriminal operations have been publishing "high-price recycling" information on social platforms and second-hand trading platforms for a long time, clearly marking the recycling price, collection quantity and contact information, and setting up collection points and distribution warehouses in many places. After the recovered genuine products are collected together, they continue to flow into unauthorized sales channels.

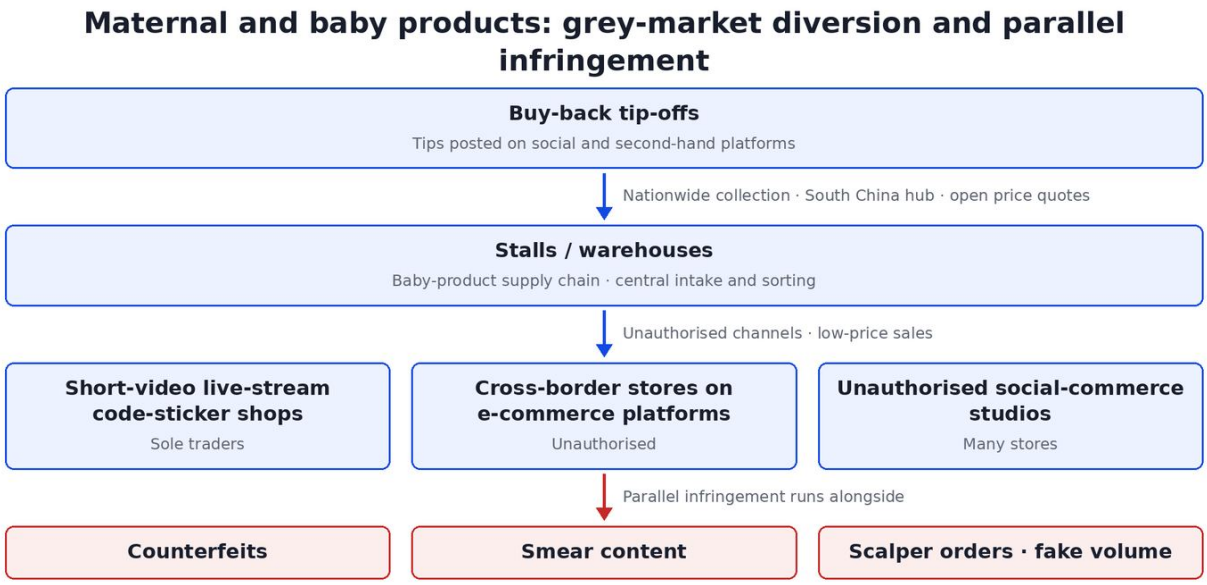
Midstream goods are sold at low prices. Recycled goods are mainly sold through unauthorized channels such as short-video live-streaming rooms, newly opened stores on comprehensive e-commerce platforms, and social e-commerce "studio". Some merchants avoid brand verification by pasting product codes and registering multiple stores with the same entity, and sell at prices significantly lower than official channels, impacting the normal price system of the brand.

Downstream counterfeit goods are mixed-sold and counterfeited. There is a risk of genuine products being mixed with fakes and high-imitation products in some unauthorized channels. In consumer reviews, there are doubts about authenticity such as "product quality is different from official self-operated products" and "discomfort after use". At the same time, some third-party merchants imitate product names, packaging and visual designs to gain brand awareness and traffic.

Content attracts traffic. Some accounts continue to publish content that disparages the brand in the form of product reviews, comparisons of competing products, etc., and direct consumers to other brands or unauthorized products promoted by them, further affecting brand reputation and purchasing decisions.

In addition, cybercriminal operations also conduct arbitrage by receiving red envelopes from live broadcast rooms, superimposing platform coupons and selling scalpers to further expand the circulation scale of low-priced goods.

Overall, there is a strong synergy between the various links: the upstream is responsible for recycling and organizing the supply of goods, the midstream is cashing in at low prices through unauthorized channels, and the downstream adulterates fake goods to expand profit margins. At the same time, content promotion and scalper arbitrage are used to gain traffic and reduce costs, which ultimately causes continuous erosion of the brand price system, consumer trust and intellectual property rights.



Maternal and baby products: grey-market diversion and parallel infringement

Source: Threat Hunter original report, page 29. Redrawn in English from the original figure.

- Malicious link analysis

Take a certain brand monitored by Threat Hunter as an example. In the first half of 2026, Threat Hunter continued to find recycling information of this brand on grass planting platforms, second-hand trading platforms and other channels. Relevant information is generally publicly marked with recycling prices, minimum collection quantities and contact information. The delivery addresses are highly concentrated in Buji, Longgang, Shenzhen. Some recyclers claim to have fixed stalls and receive goods for a long time.

Threat Hunter discovered through continuous monitoring and correlation with historical intelligence that the consignee and address of a piece of recycling information captured in June highly overlapped with the cybercrime operations information discovered in March; another consignee that appeared again in July was also consistent with the recycling party that had actually been traded in February. This shows that the relevant gangs are not committing sporadic crimes in the short term, but are continuing to operate a stable recycling network.

The following is relevant to the case:

Unauthorized channels sell goods at low prices. Threat actors have opened a number of "import-only" stores on the leading comprehensive e-commerce platform. The relevant stores were all newly opened from April to May 2026, and none of them were authorized after official verification by the brand. In June, Threat Hunter researchers found in actual measurements that the prices of some products after adding coupons were as low as about 77.66 yuan per can. At the same time, Threat Hunter also discovered in January and May that multiple maternal and baby live-streaming accounts on a short-video platform were selling the brand's products by "sticking codes". Most of the relevant delivery stores were individual industrial and commercial households, and their business licenses and legal person information had been collected.

Malicious counterfeiting. On March 20, Threat Hunter discovered a high-imitation product on a social e-commerce platform. Its product name and packaging design were highly similar to the brand's original product. When consumers asked about the difference between the two, customer

service deliberately avoided relevant questions. At present, the business entity and business license information of the counterfeit store have been collected.

Competing products are rejected. Since January 2025, some accounts have continued to publish comparative content between the brand and two competing products. The relevant rhetoric, content structure and publishing rhythm are highly consistent. It mainly disparages the brand by comparing product ingredient content and other methods, and guides consumers to switch to other brands, which has obvious characteristics of organized marketing.

Scalper discount arbitrage. From February to March 2026, Threat Hunter continuously discovered that some messaging-app groups posted tasks for scalpers who released the brand's products. The purchase cost can be reduced by stacking live broadcast room red envelopes, platform coupons, etc. Some orders can even be purchased for "0 yuan", which may then enter resale or other unauthorized circulation channels.



Screenshot of a cross-border store listing

Source: Threat Hunter original report, page 30. Original image retained.

Risk analysis: This chain affects the brand price system, product reputation and intellectual property rights at the same time. Unauthorized low-price sales disrupt channel prices, mixed sales of fake products damage consumer trust, and counterfeit packaging further amplifies the risk of brand infringement. Since most of the relevant entities are truly operating individual industrial and commercial households and are highly concealed, management should focus on continuous monitoring and joint disposal of recycling distribution centers, unauthorized stores and links to counterfeit goods.

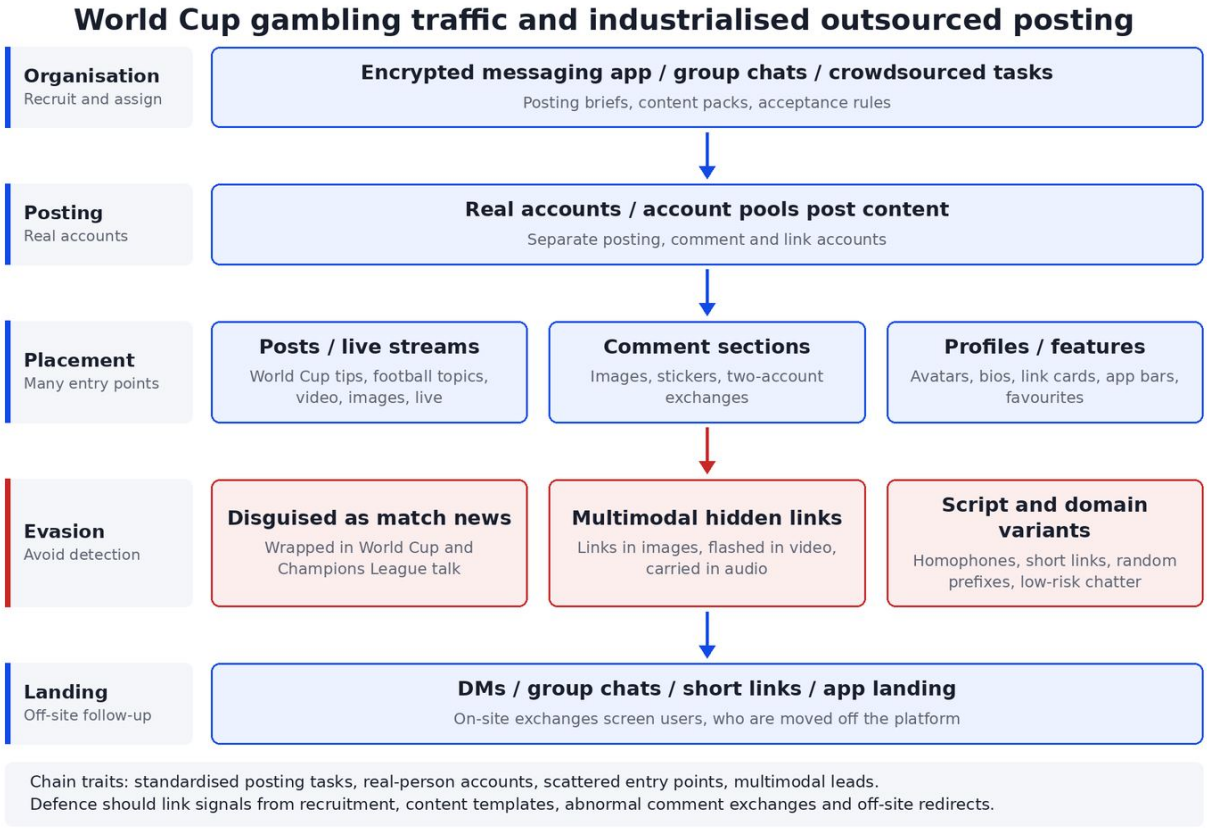
2.1.2.2 World Cup Cybercriminal Operations Special Topic: "The industrialisation of outsourced posting for sports-betting traffic"

- Trend judgment

The 2026 World Cup has spawned an outbreak of cybercriminal operations related to sports events, the core of which is the "industrialization of agency distribution" to attract traffic from gambling (and pornography) - cybercriminal operations no longer create their own accounts to attract traffic, but recruit accounts of real users on a large scale through deposit-based public groups for "agency distribution". They use the activity of accounts operated by real users to avoid platform fraud controls, complete gambling-related traffic under the sports content of various short video social platforms, and form "organized recruitment-human-operated agency-confrontation fraud controls" — Landed gambling — a complete chain of money laundering by running points. Scale and evolution: The number of related events reached 130+ in the first half of the year, showing strong event timeliness - with a sharp monthly increase as the World Cup approaches

- Industrial chain dismantling
- Organizational level: The cybercrime operations releases distribution tasks through encrypted messaging app, group chat and crowdsourcing channels, and disassembles gambling diversion requirements into standardized task packages. The task packages usually include distribution materials, entrance requirements, account requirements, release location, screenshot return and acceptance rules.
- Agency layer: Undertake agency tasks through real accounts, alt accounts, other people's accounts or account pools, forming a division of roles such as publishing accounts, comment accounts, and link accounts. Compared with illegal self-operated accounts, accounts operated by real users have stronger natural active characteristics, which can reduce the risk of single-point accounts being identified and banned.
- Delivery layer: The distributed content is no longer concentrated in a single entrance, but is distributed in scenarios such as works/live broadcasts, comment areas, homepage information, and platform function entrances. For example, use World Cup predictions, football topics, videos/graphics/live broadcasts as content shells, post pictures or emoticons in the comment area, or carry traffic leads through avatar profiles, link cards, application bars, favorites and other entrances.
- Countermeasures layer: Cybercriminal operations avoid identification through "camouflage of event hot spots + multi-modal hidden links + rhetoric/domain name variations". On the one hand, the jump clues are hidden in pictures, video flashes, audio or homepage information, and the keywords and regular hits are reduced by using homophones, short links, random prefixes, low-risk interactive techniques, etc. (domain names such as sm84.my, sw33.me, 7sx.my, 22xx.me, etc.). On the other hand, the comment area adopts "double act + domain name splitting" - number A posts profits, number B asks questions, and number A splits the domain name into two paragraphs and replies separately to avoid regular detection.
- Implementation layer: The content on the site is mainly responsible for screening and reaching. Subsequently, through comment interaction, private messages, group chats, short links or app/website, off-site acceptance is completed, forming a gambling drainage link of "on-site grass planting/interactive screening - off-site conversion and acceptance".

Crime link:



World Cup gambling traffic and industrialised outsourced posting

Source: Threat Hunter original report, page 32. Redrawn in English from the original figure.

- Malicious link analysis
- Outsourced comments + split domain names + a two-account double act:

On June 9, Threat Hunter found comments posting recruitment information in a chat group hosted outside China. The account operated by a real user of the cybercrime operations organization "cooperated with double accounts" in the comment area of □□World Cup-related videos: Account A first posted comments with betting implications such as "I bought it first, Spanish champion 3k", Account B then asked "Where did I buy it?", Account A then split the domain name "2 7.tw" into two replies of "2 7." and "tw" to avoid the platform's detection of complete domain names and sensitive content. The recruitment information is also accompanied by multiple designated short-video links, indicating that this type of traffic has clear task distribution and targeted execution characteristics.

The next day, Threat Hunter once again captured a case using the same technique. The relevant personnel split the domain name "4**.vin" and published it, and completed the actual placement in the comment section of a short-video platform. As a whole, an malicious link of "group recruitment-task distribution-human-operated comments-dual account interaction-domain name split-off-site gambling diversion" was formed.



Screenshots of outsourced posting for gambling traffic

Source: Threat Hunter original report, page 33. Original image retained.

Risk research and judgment: This method combines human-operated posting, dual-account interaction and domain name splitting to make malicious comments closer to normal user communication. Traditional keywords and regular detection are prone to missed judgments. Platforms should focus on identifying abnormal comment interactions, domain name fragments in continuous replies, repeated words and account coordination behaviors, and plan risk strategies in advance based on major events such as the World Cup.

2.1.2.3 Analysis of the industrial chain behind proxy ordering for consumer food and drink brands

- Industrial Chain Overview: From a single point of promotion abuse to a factory-based "ordering on behalf of" platform

The digital growth of brands such as fast food, coffee, and new tea drinks generally relies on marketing activities such as gifts for newcomers, stored value rebates, member discounts, subscription cards, and social coupons. Since these rights and interests are mainly bound to member accounts, and the threshold for account registration is low, a factory-like cybercrime operations chain of "ordering on behalf of others" has gradually emerged.

Its core model is: Cybercriminal operations acquire and operate accounts with stored value balances, coupons and membership rights in batches, and then sell packages to consumers at a price lower than the official original price but higher than the actual cost, converting the marketing subsidies invested by the brand into their own income. Consumers have received low-priced goods, and the brand's backend shows an increase in new members, stored value, and orders, but actual profits and operating data are continuing to be eroded.

In the first half of 2026, Threat Hunter monitored and obtained a sample of an operating multi-brand ordering platform, which more completely restored its technical links, distribution model and upstream and downstream ecology.

- Four-layer ecology: upstream suppliers core platform agent distribution end consumers

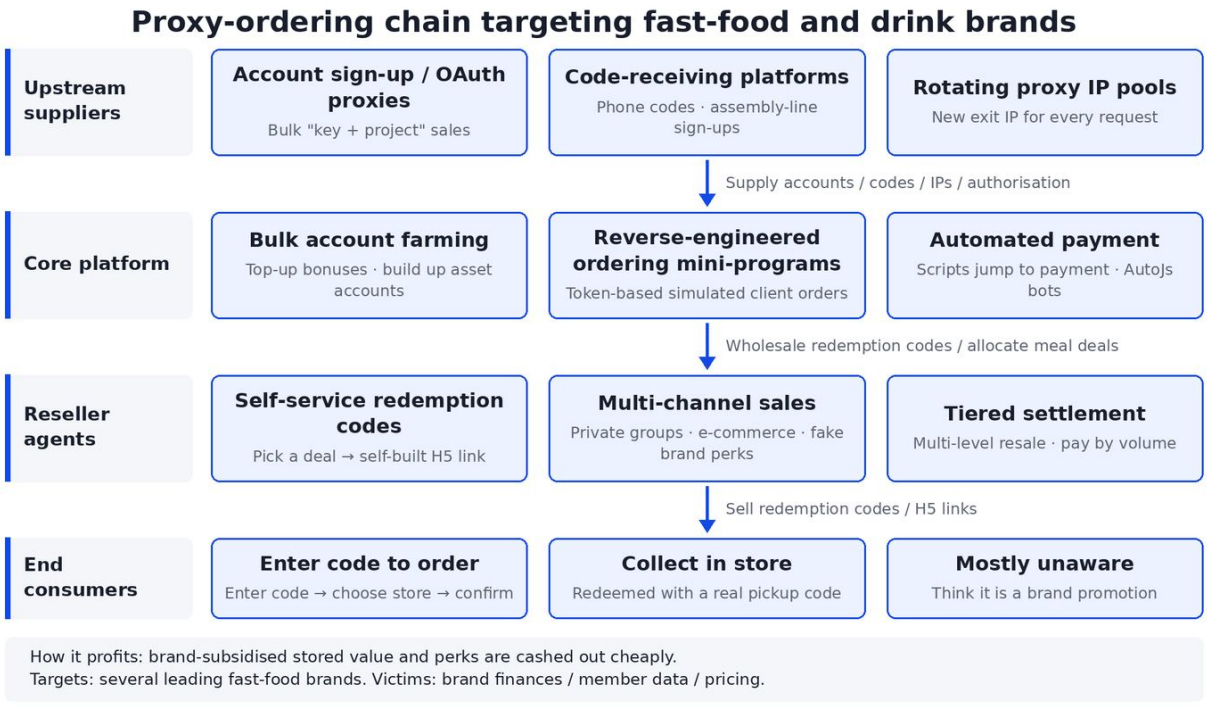
In today's proxy-ordering trade, placing orders is no longer a scattered operation by individuals, but has formed an industrial chain with a clear division of labor.

Upstream suppliers mainly provide basic resources such as account registration, code retrieval, OAuth authorization proxy and dynamic proxy IP. Some suppliers are based on normally registered technology companies and sell account authorization and interface capabilities through the "Card Code + Project" method to provide continuous supply for downstream platforms.

The core platform is responsible for managing member accounts in batches, synchronizing account balances and rights, simulating brand ordering systems to place orders, generating redemption codes, and completing agency management and order settlement. It has formed a relatively mature cybercrime operations system.

Agent distributors generate package redemption codes through the platform's backend, and then sell to consumers through messaging-app groups, e-commerce stores and other channels. Consumers open the self-built H5 page of the platform, enter the redemption code, select a store and complete the order. Most consumers do not know that the order is actually submitted by a cybercrime operations account.

Overall, the core platform is only an intermediate link in the industry chain. Its account number, access code, IP and authorization capabilities are all provided by professional suppliers. The maturity of the industry chain has obviously surpassed the traditional personal discount model.



Proxy-ordering chain targeting fast-food and drink brands

Source: Threat Hunter original report, page 34. Redrawn in English from the original figure.

- Attack link: reverse applet + order with account + automated payment

The technical link of the agent ordering platform mainly includes four links.

First, cybercriminal operations register brand member accounts in batches through the code receiving platform and account authorization services, and use recharge rebates, new member activities and subscription cards to cultivate the accounts into "asset accounts" that hold balances and preferential rights, and then manage them according to brand, rights and usage scenarios.

Secondly, since brands usually do not disclose ordering interfaces, cybercriminal operators will reverse-engineer ordering mini-programs on messaging and payment apps to obtain their interface addresses, request parameters and business processes.

Subsequently, the platform uses the account login credentials and user identity information it holds to simulate the mini program client to initiate an order request to the brand's backend. Since the request uses a real member account and valid rights and interests, it is difficult for the brand backend to determine that it is a machine placed based on a single order.

Finally, the platform polls pending payment orders through an automated script running on a real mobile phone, automatically evokes the payment software to complete the payment, and cooperates with the dynamic proxy IP to switch network exits to reduce the risk of identification of high-frequency orders placed by the same IP.

- Business model: self-built H5 + redemption code distribution

This type of platform does not rely on the brand's official sales channels, but builds its own complete transaction and write-off process.

- The agent generates a redemption code: The agent selects a package in the background, clicks Generate, and the system outputs a redemption code link pointing to the self-built H5 site. This "redemption code" is an electronic delivery voucher created by the platform. It has nothing to do with the brand's official coupon code and can only be verified on the platform's own site.
- External distribution and shipment: Agents sell redemption codes to consumers through social groups and e-commerce stores. Package names are often embedded with marketing channel marks, disguised as "brand activity benefits."
- Consumer verification: Open the H5 link □ Enter the redemption code □ Select a city/store □ Confirm the order □ Obtain the real meal pickup code □ Pick up the meal at the store.
- The essence of profit: It is not to earn the price difference of the order, but to realize the stored value and equity assets of the brand discount into cash by placing orders on behalf of the customer at a low price; the core "property" of the platform is the scale of assets accumulated by maintaining the account.
- Multi-brand horizontal replication: One middle platform can be replicated to multiple leading fast food brand scenarios

Threat Hunter discovered that the platform does not only target a single brand, but has formed a multi-brand order matrix that can be replicated horizontally. The relevant systems are deployed in multiple servers and different cloud service provider environments. The same set of technology and distribution system can quickly access the ordering scenarios of different brands, and has obvious large-scale expansion capabilities.

The ability of some brands to place orders is no longer limited to in-store pickup, but can also support takeout delivery, which means that their attack scope is further expanding from store pickup to online delivery scenarios.

- Triple Hazard: Far more than just "getting a little discount"

Direct financial loss: The brand’s marketing budget used to attract new customers, store value, and increase repurchase is systematically cashed out, and ultimately needs to be paid out with real goods, store labor, and fulfillment costs, resulting in direct financial losses.

Ghost members contaminate data assets: A large number of accounts registered and operated in batches through the code-receiving platform enter the membership system, which will pollute key operating indicators such as the number of new customers, active users, repurchase rate and stored value growth, making it difficult for brands to accurately judge real user growth and marketing activity effects.

Impact on the price system and brand reputation: Products sold through unofficial channels for a long time at prices significantly lower than the original price will also impact the brand price system and the interests of franchisees. Once consumers discover that low-price orders come from illegal channels, it may further raise questions about brand management capabilities and member security.

- Why is traditional fraud controls so difficult to intercept?
- Single transaction compliance: Every order placed on the brand's backend is viewed as "a valid member purchased an order with his own balance". There is no flaw when viewed in isolation. The problem only exists in the correlation analysis of cross-accounts and cross-orders;
- Internal game between fraud controls and marketing: The discounts that were collected were deducted from the marketing budget, and the marketing side saw growth and lacked motivation for rectification;
- Anti-reconnaissance investment for cybercriminal operations: dynamic proxy + equipment dispersion + balance payment (without triggering abnormal payment fraud controls), systematically circumventing existing rules;
- Cybercriminal operations have emergency response capabilities: During monitoring, it was found that the platform will quickly go offline, migrate, and rebuild assets after sensing abnormalities; one-time security assessments are difficult to capture, and continuous threat intelligence monitoring must be relied on to form a closed loop of discovery-tracing-disposal.

2.1.2.4 Evolution of e-commerce business risk scenarios

In the first half of 2026, e-commerce cybercriminal operations showed an obvious trend of linking and service-oriented. Marketing rights, store accounts, corporate entities, collection accounts, equipment environments and after-sales vouchers are no longer used individually, but are split, combined and traded as standardized services.

Among them, marketing fraud is evolving towards "equity account-based", store transactions are evolving towards "integration of business qualifications", and malicious refunds are beginning to evolve into "generative AI-assisted evidence forgery".

- E-commerce platform marketing fraud and sales risks: preferential rights and interests are packaged and sold as tradable and replicable platform accounts.

Threat Hunter monitoring found that e-commerce marketing fraud is evolving from sporadic coupon abuse to a supply chain centered around the production, account maintenance and transactions of "accounts with benefits".

Threat actors use email, code receiving and automated tools to register accounts in batches, and simulates normal behaviors such as browsing, searching, collecting, purchasing and event interaction through manual operations or scripts to complete marketing tasks. After the account

obtains coupons, points or free shipping rights, it will be sold through the "account-wide delivery" method.

Compared with the direct sale of preferential information, this model can transfer the account number, marketing rights and some behavior records together, separating the preferential rights and interests from the original acquirer, making it more difficult for the platform to identify abnormal transfers.

(1) “Coupon account” has become the main carrier for marketing equity transactions

Related accounts are usually priced differently based on discounts, points balance, task completion status and validity period. After the transaction is completed, the seller delivers the account and related login information to the buyer, and the buyer binds the payment method and completes the order.

The transaction object of marketing fraud is therefore no longer a single coupon, but a combined asset including account number, marketing rights and behavior records.

This model may circumvent some platforms’ restrictions on coupon transfers and abnormal circulation, allowing marketing rights to enter an external market that can be priced and traded in batches.



Screenshots of a proxy-ordering back end

Source: Threat Hunter original report, page 37. Original image retained.

(2) Simulate real behaviors to improve marketing task pass rate

In order to reduce the probability of batch registered accounts being identified by the fraud controls system, Cybercriminal Operations will proactively supplement the accounts with normal user behavior tracks. Common behaviors include:

- Complete new user guidance and activity page browsing;
- Simulate product search, browsing, collection and purchase;

- Complete check-in, answer questions or interact according to task requirements.

Some gangs call this process "making papers" or "earning points." Its core purpose is to improve the behavioral similarity between batch accounts and normal consumers, making it easier for the accounts to obtain marketing rights.

For platforms, it is usually difficult to identify such risks based only on a certain browsing, check-in or coupon collection behavior. The focus of governance needs to shift to a comprehensive analysis of registration resources, device reuse, behavior rhythm, account relationships, and rights usage paths.



Screenshots of chats about proxy ordering

Source: Threat Hunter original report, page 38. Original image retained.

- E-commerce platform store account sales risks: Evolution from single account transactions to integrated services of "enterprise entity-store-collection-after-sales"

E-commerce store transactions are no longer limited to account numbers and passwords, but have gradually formed an integrated service chain covering identity collaboration, enterprise registration, store opening, payment configuration, environment migration and continuous identity verification.

The object of the cybercrime transaction is no longer just login permission, but a "business qualification package" that can pass the review, receive payment and continue to operate. Its main feature is that the nominal registration entity, actual controller and actual operator may be separated from each other.

(1) Separation of nominal subject and actual controller

Some service providers recruit natural persons for a fee to provide identity and tax information, and cooperate with business registration, bank account opening and subsequent identity verification. After the store is registered, the actual operating rights and control rights may be transferred to other entities.

Subsequently, the intermediary or service provider is responsible for completing business registration, tax registration, bank account configuration and e-commerce platform settlement, and combining relevant information into store assets with a local operating appearance.

Store transactions may usually include:

- Store account and login permissions;
- Business and tax registration information;
- Business collection account;
- Browser session and related environmental information;
- Follow-up identity verification and information supplement services.



Screenshot of a debt-assumption recruitment post

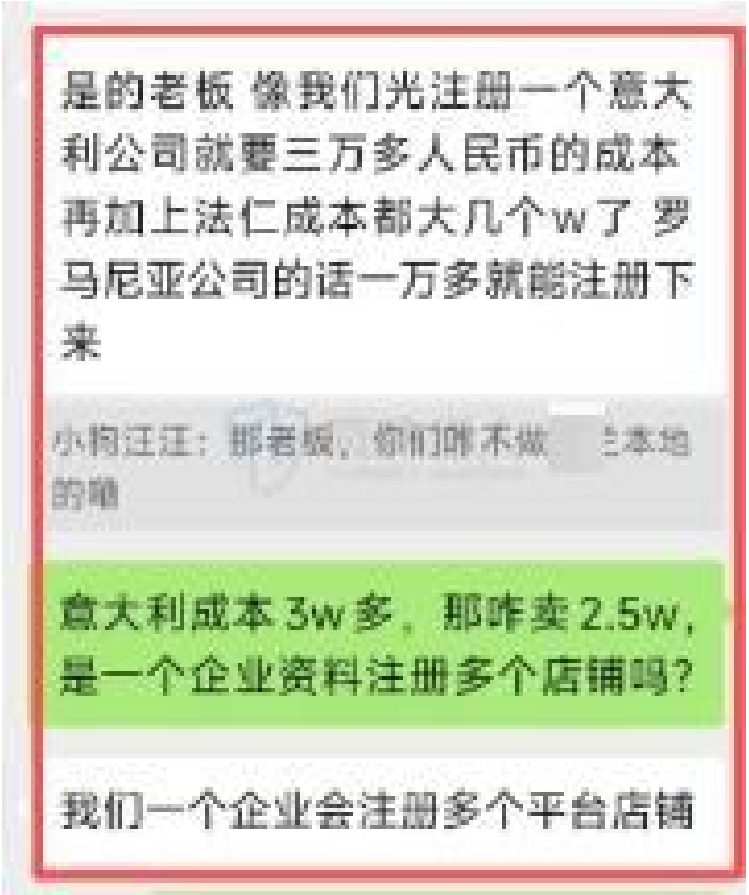
Source: Threat Hunter original report, page 39. Original image retained.

(2) “One enterprise with multiple stores” improves the monetization efficiency of the same set of qualifications

Service providers may use the same business entity, registered personnel, and tax information to apply for stores in multiple e-commerce scenarios, and sell or put different stores into operation separately.

This model of "reuse of enterprise entities, split sales in stores, and monetization in multiple scenarios" can spread the cost of enterprise registration and maintenance, allowing the same set of entity qualifications to be reused.

Even if the transaction price of a single store cannot cover the entire registration cost, the service provider may still achieve cost recovery and profit amplification by selling multiple stores.



Screenshot of a chat about company-registration costs

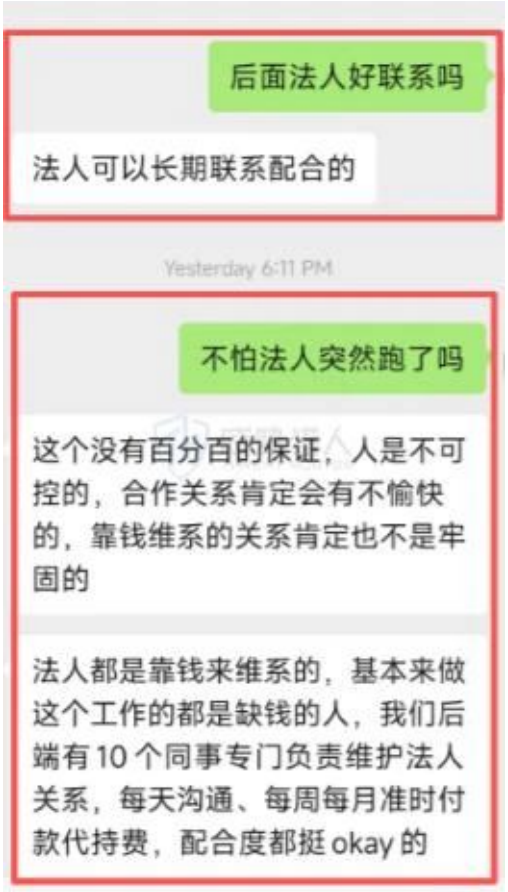
Source: Threat Hunter original report, page 40. Original image retained.

(3) Continuous identity verification is packaged as after-sales service to ensure account survival

After the store is sold, the original registration personnel may not exit completely, but continue to serve as account maintenance resources, cooperating with video authentication, identity review, information supplement and account appeal.

Relevant services may be charged on a one-time, weekly or monthly basis, making the natural person's identity cooperation ability a resource that can be purchased continuously.

This means that if the platform initiates human-operated verification again during the operation process, it may not be able to identify that store control has been transferred. Identity verification is being transformed from a one-time access mechanism into an after-sales service that can be called on demand.



Screenshot of a chat about nominee legal representatives

Source: Threat Hunter original report, page 40. Original image retained.

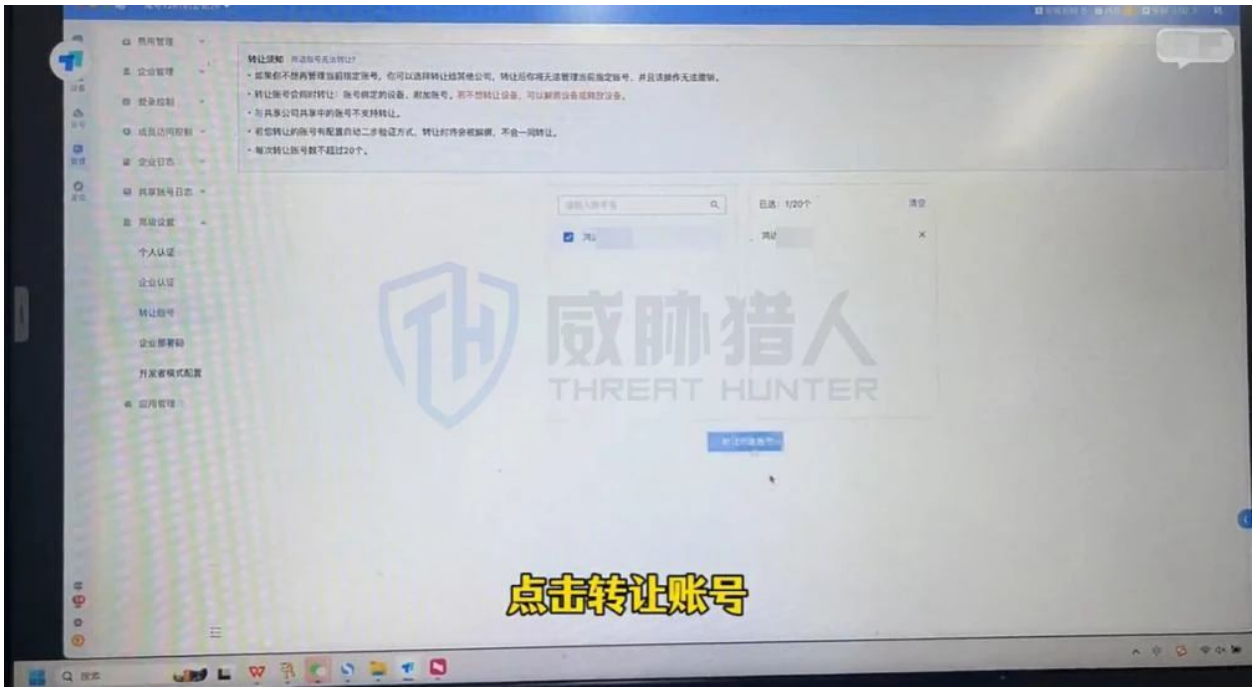
(4) Fingerprint browser migration reduces abnormal exposure during account delivery

Some account service providers will simultaneously transfer browser sessions, device fingerprints, cookies and network environments, allowing buyers to take over the store in a state close to the original operating environment.

After the buyer completes the purchase, the service provider synchronizes the store session, browser fingerprint and IP environment to the buyer through the browser's built-in account migration function. The buyer can directly take over the store without re-entering the account and password in the new environment.

This delivery method can reduce abnormal features such as remote login, device mutation, cookie invalidation, and IP changes that are common in traditional account transactions, making the transfer of account control appear as a continuation of the original operating environment on the platform side.

The platform needs to focus on identifying subtle changes after the environment is migrated, including operating time zones, input habits, access rhythm, receiving relationships, product changes, and capital flows, and cannot rely solely on whether IP or equipment has mutated.



Screenshot from a video about the scheme

Source: Threat Hunter original report, page 41. Original image retained.

- Generative AI drives post-sales fraud to evolve into evidence forgery

Threat Hunter monitoring found that current malicious refund fraud on e-commerce platforms no longer relies solely on customer service tactics, logistics loopholes, and rule pressure. Instead, it introduces capabilities such as AI-generated pictures to package fake product damage, equipment failures, and abnormal conditions into "evidence materials" that can be submitted, verified, and can promote the after-sales process.

Cybercriminal operations use AI to generate damage and fault pictures and customer complaint vouchers, and cooperate with traditional malicious return techniques such as return label inducement, delay in investigation cycle, and pressure from regulatory complaints to form a fraud chain of "false evidence generation, after-sales process triggering, customer service rule gaming, and refund result fulfillment."

This model reduces the reliance of malicious refunds on real product status, real shooting environment and real logistics anomalies, and further evolves after-sales risks from single rule abuse to AI-assisted evidence-based fraud.

(1) AI-generated pictures become key credentials for malicious refunds

During the monitoring of communications related to cybercriminal operations on an e-commerce platform, it was found that cybercriminal operations may generate pictures with characteristics of damage, deformation, leakage or contamination based on product categories, reasons for refunds, and after-sales review requirements to enhance the surface credibility of customer complaint materials. For example: Some cybercriminal operations use AI to generate abnormal product pictures such as "smartphone lithium battery leakage", submit after-sales applications to the platform, and ultimately achieve refund results without the need for returns.



AI-generated image of a leaking phone battery

Source: Threat Hunter original report, page 42. Original figure with Chinese text replaced by English.

(2) AI fraud is combined with traditional bad withdrawal links to amplify after-sales fraud controls pressure

Suspected AI-generated content usually does not work alone, but is used in combination with false customer complaint grounds, logistics label avoidance, investigation cycle delays, repeated complaints and complaint pressure.

In this link, the generated content is mainly used to supplement "evidence materials", while traditional words and process operations are used to promote after-sales processing. Relevant personnel may extend the processing cycle through repeated communication and appeals, increasing the verification costs of the platform's customer service and fraud controls teams.

2.2 Analysis of brand external risk scenarios

2.2.1 Panorama of brand external risks

Risks external to the enterprise are not concentrated on a single phishing page or a single data breach. Data and identities may continue to flow beyond corporate control, and user touchpoints may be dispersed across search, content, social, download and private channels. The core issue facing brand protection is expanding from "whether there are counterfeit assets" to "whether the trusted connection between the enterprise and the user is still identifiable and controllable."

2.2.1.1 Brand protection revolves around four types of objects

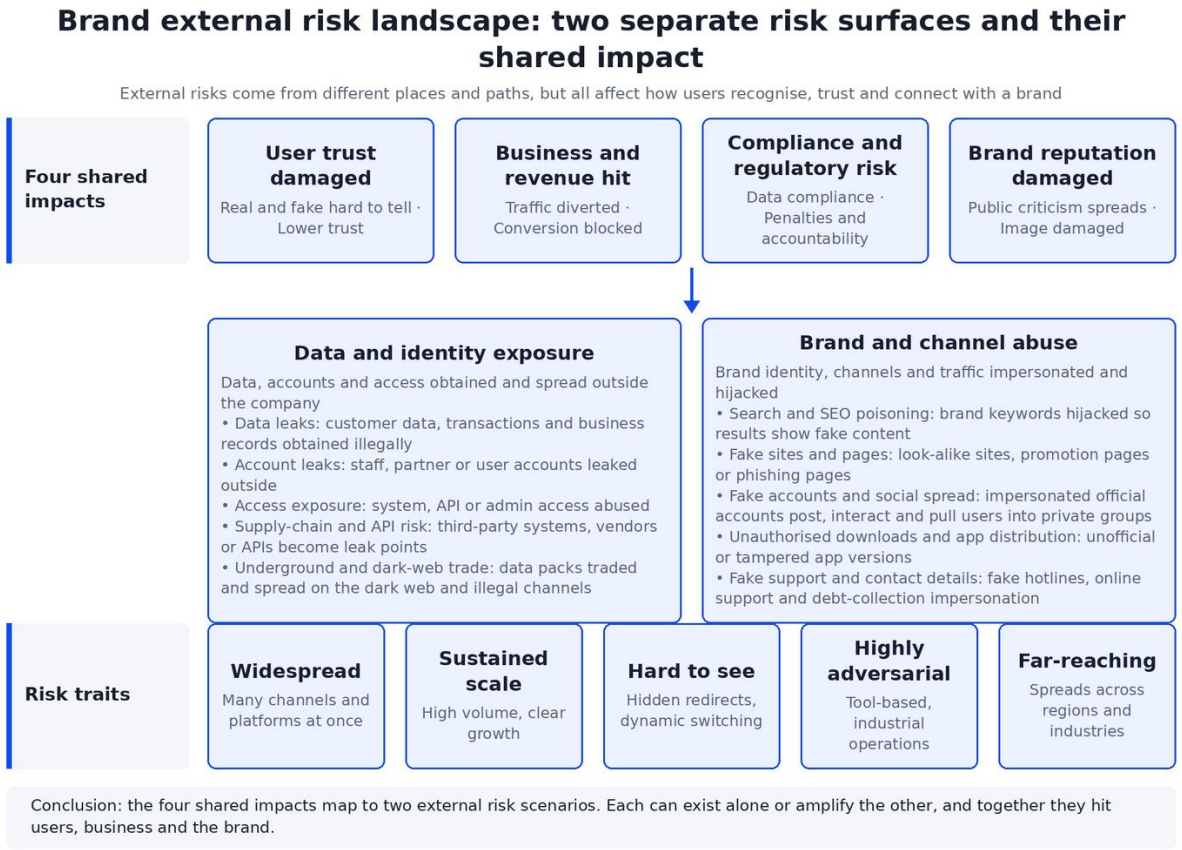
Focusing on the above four types of protection objects, the external risks faced by enterprises can be summarized into two relatively independent risk areas: exposure of data, identity and permissions, and abuse of brand, channel and traffic. The two can occur independently or overlap each other, jointly affecting customer relationships, user trust and brand reputation.

Protected object	Main external risks	Typical impact
Brand identity	Company names, product names, logos, domains, apps and official accounts are impersonated	Users struggle to tell who provides the service; authorisation relationships and brand recognition suffer
Official channels	Search results, websites, customer-service numbers, download pages, content accounts, campaign pages and QR codes are intercepted	Before reaching the official service, users land on fake contacts, unauthorised downloads or fraud pages
Customer relationships	Real business records such as loans, payments, orders, memberships, refunds and collections reach outside channels	Business context is rebuilt and targets are screened, so fake support or collection scripts become more targeted
Public reputation	Dark-web disclosures, attack claims, data samples and infringing content spread publicly	Customer doubts, partner reviews, reputational pressure and higher business-continuity risk

Brand protection covers four kinds of target

Source: Threat Hunter original report, page 43. Table re-typeset in English from the original.

Figure - Two types of independent risk surfaces and joint impacts of brand external risks



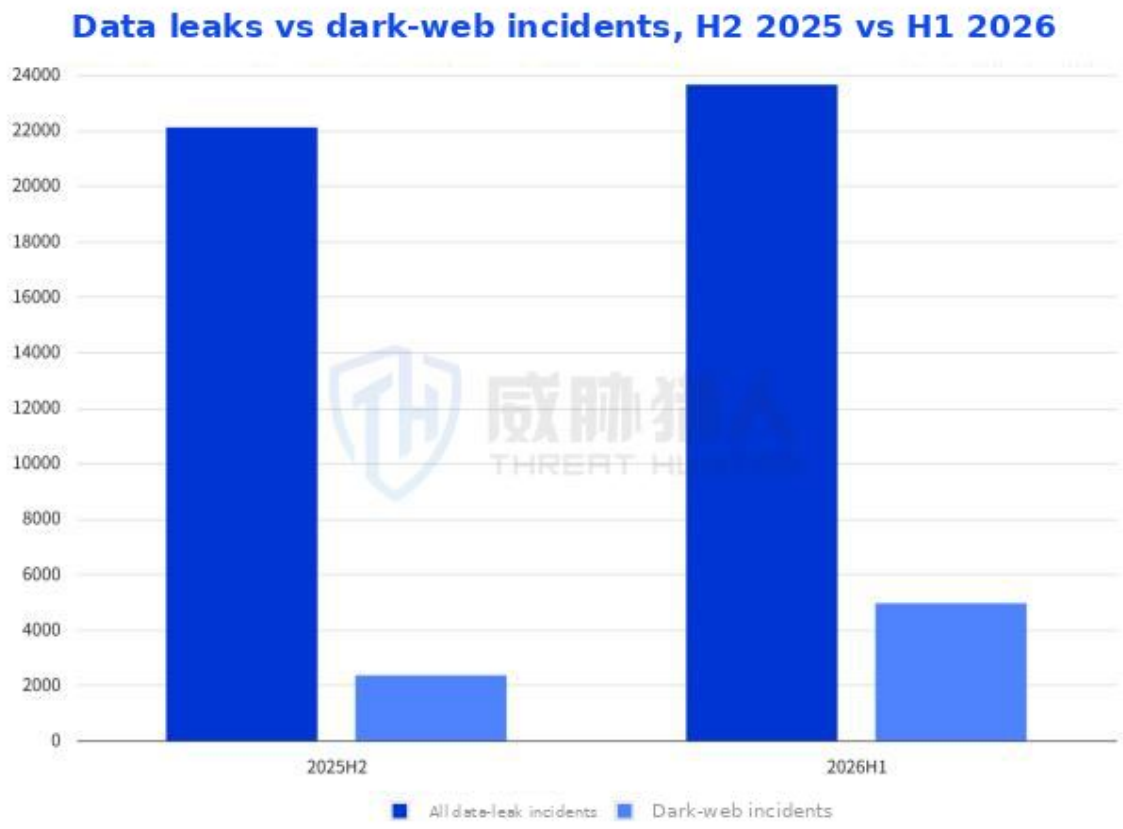
Brand external risk landscape

Source: Threat Hunter original report, page 43. Redrawn in English from the original figure.

2.2.1.2 Data and identity exposure: The total number of incidents increased slightly, and major risks were concentrated on the dark web

From January to June 2026, there were a total of 23,645 verified and confirmed valid data leakage incidents, an increase of 6.98% from 22,102 incidents in the second half of 2025. Among them, darknet channel records increased from 2,353 to 4,952, an increase that was significantly higher than the increase in overall incidents. The dark web has become the main external channel for the public disclosure and dissemination of major data breach risks.

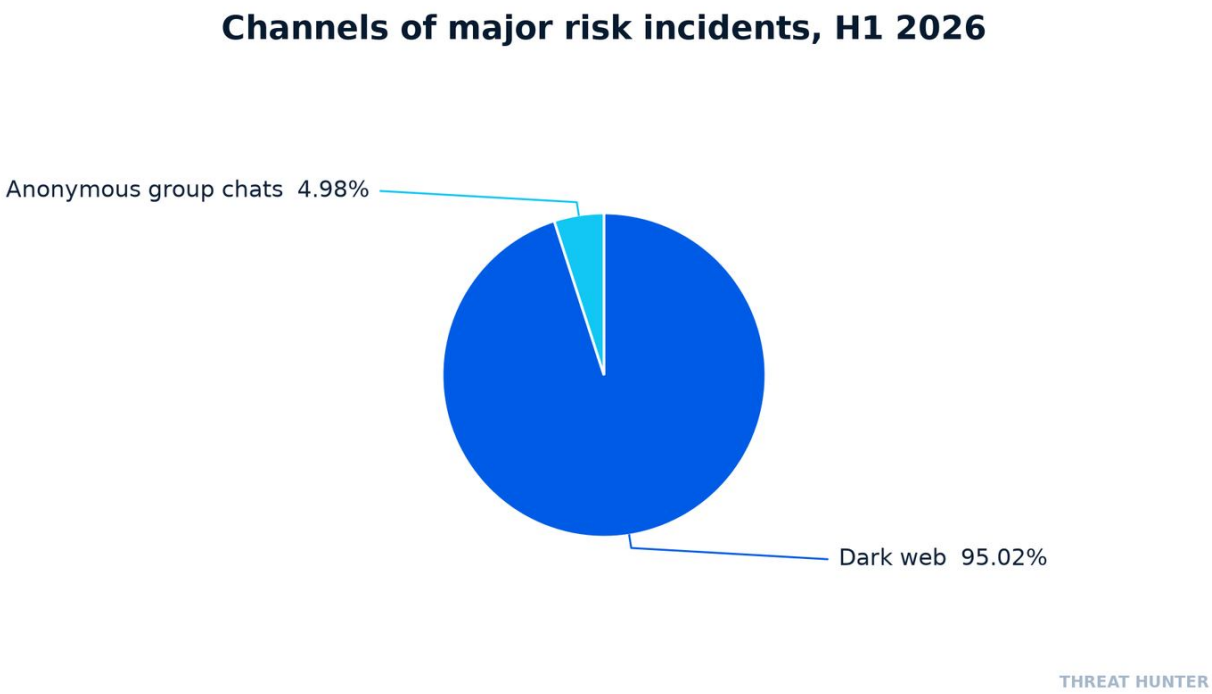
Figure - Comparison of the total amount of data leakage and the amount recorded in darknet channels



All data-leak incidents and dark-web incidents, H2 2025 vs H1 2026

Source: Threat Hunter original report, page 44. Original figure with Chinese text replaced by English.

Figure - Major data leakage risk event channel composition and inter-temporal changes

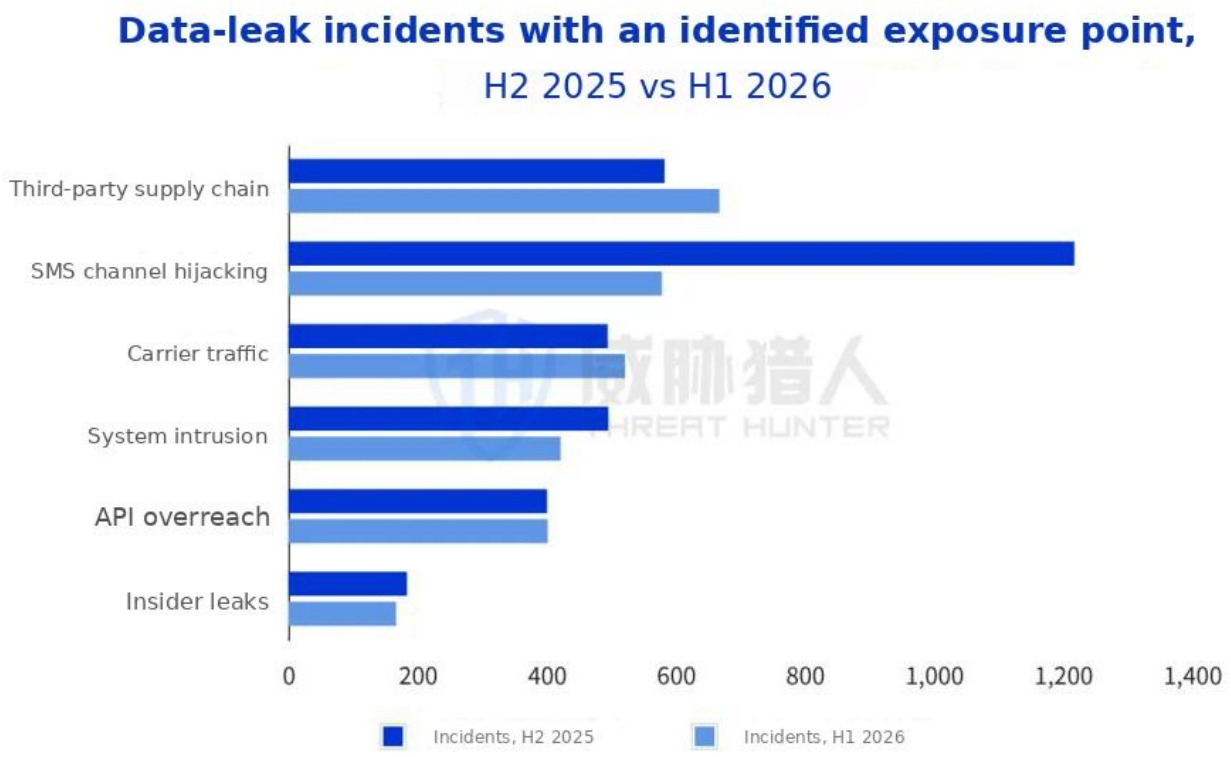


Channels of major risk incidents, H1 2026

Source: Threat Hunter original report, page 44. Redrawn in English from the original figure.

Judging from the identified risk sources, data leakage records involve third-party services, SMS channels, operator traffic, system penetration, API override and internal permissions, etc., reflecting that enterprise data exposure has extended from single system security issues to multiple types of external and internal nodes such as supply chains, communication links and permission management.

Figure - Full data leakage event source record volume changes



Data-leak incidents with an identified exposure point, H2 2025 vs H1 2026

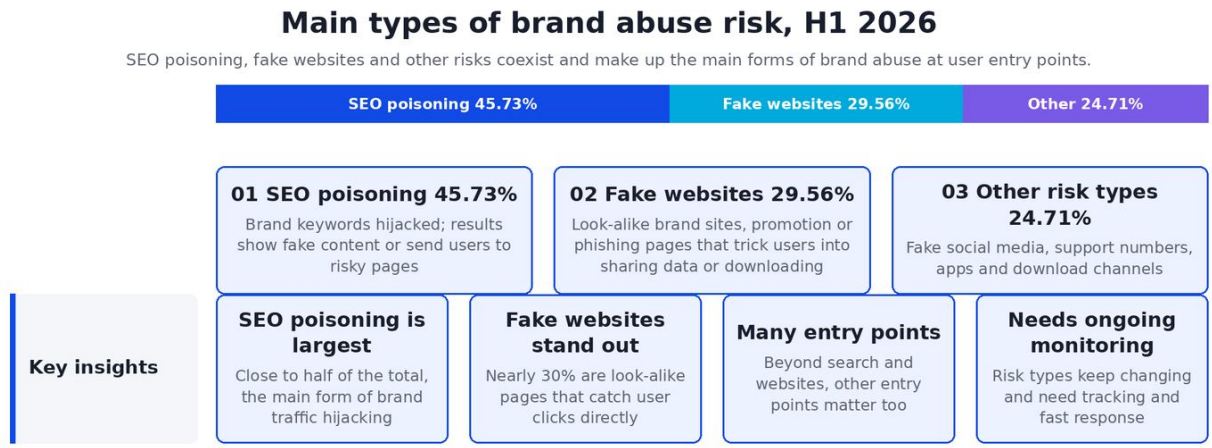
Source: Threat Hunter original report, page 44. Original figure with Chinese text replaced by English.

2.2.1.3 Brand and channel abuse: User contact risks are distributed across multiple entrances

In the first half of 2026, a total of 45,321 phishing, counterfeiting and brand abuse risk incidents were recorded. Related risks appear in multiple user portals such as search results, fake websites, social media, customer service hotlines, applications, and download channels.

Judging from the risk distribution in this period, there were 20,726 SEO pollution records, accounting for 45.73% of the 45,321 main samples; counterfeit websites accounted for 29.56%. Search results and counterfeit pages are still important places for brand abuse: the former may intercept users' needs when they are looking for customer service hotlines, account exception handling, refund claims, loan processing, or application downloads, while the latter may be responsible for information collection, malicious downloads, fake customer service contacts, or fund fraud.

Figure - Major brand abuse risk types in the first half of 2026

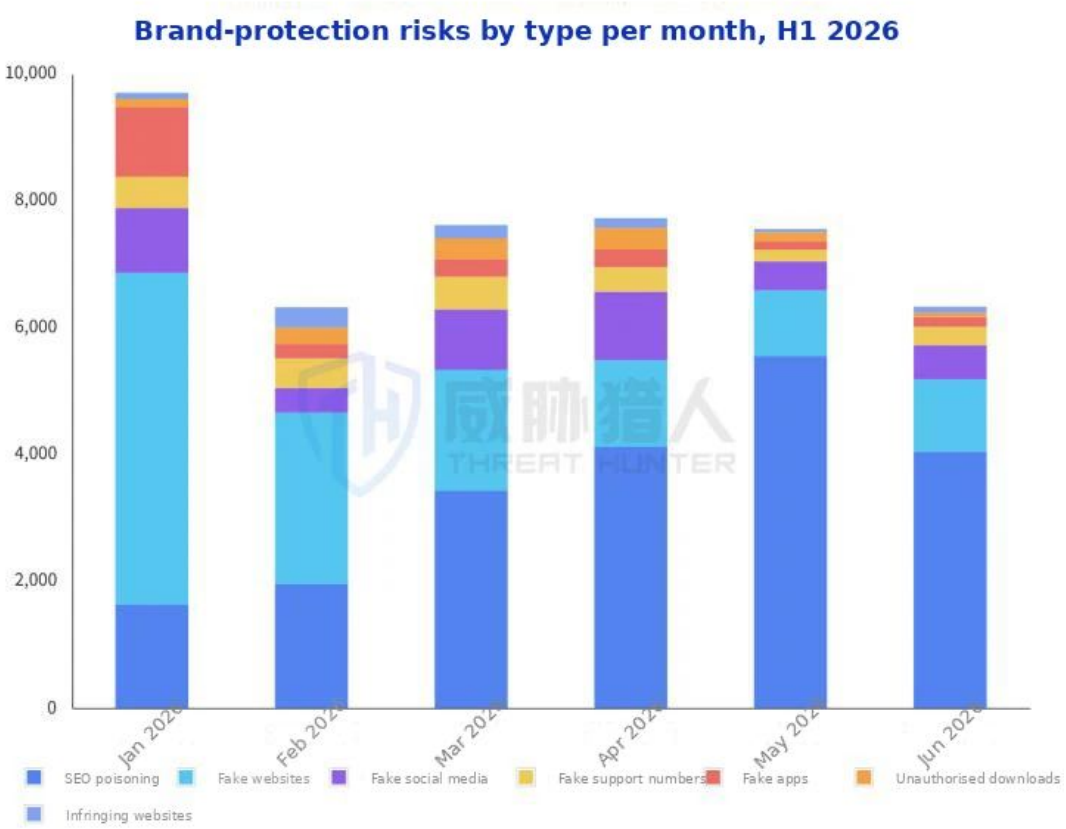


Main types of brand abuse risk, H1 2026

Source: Threat Hunter original report, page 45. Redrawn in English from the original figure.

In the first half of 2026, multiple types of entrances such as SEO pollution, counterfeit websites, counterfeit social media, counterfeit customer service hotlines, counterfeit applications, unauthorized download channels and infringing websites existed in parallel within half a year. The monthly distribution shows that multiple types of risk entrances continued in parallel within half a year, and brand abuse was not concentrated in a single channel.

Figure - Monthly distribution of phishing counterfeiting and brand abuse risk types in the first half of 2026



Brand-protection risks by type per month, H1 2026

Source: Threat Hunter original report, page 45. Original figure with Chinese text replaced by English.

2.2.2 Differences in brand risk in key industries

2.2.2.1 Industry distribution: The same industry may be exposed to risks from different external locations

In the first half of 2026, financial-related industries ranked high for data leakage risks and brand abuse risks. Among the 23,645 data breaches, banks recorded 5,251, accounting for 22.2%; consumer finance recorded 3,359, accounting for 14.2%. Among the 45,321 phishing, counterfeiting and brand abuse incidents, banks and consumer finance accounted for 44.74% and 16.33% respectively, and the payment industry accounted for 5.74%.

This distribution reflects that the financial industry not only faces the risk of customer and business information entering external channels, but also has long been affected by identity fraud problems such as counterfeit websites, fake customer service, search traffic, and unofficial applications. In addition to the financial industry, industries such as e-commerce, social tools, software applications, securities, express delivery, short videos, and insurance also present external exposures of varying scales.

Figure - Industry composition of external risks for two types of brands in the first half of 2026

Data-leak risk: industry	Share	Phishing, impersonation and brand abuse: industry	Share
Banking	22.20%	Banking	44.74%
Consumer finance	14.20%	Consumer finance	16.33%
E-commerce	9.20%	E-commerce	14.86%
Social apps	7.80%	Payments	5.74%
Software apps	5.50%	Other	18.33%
Securities	4.70%		
Express logistics	3.60%		
Short video	3.00%		
Insurance	2.50%		
Other	27.30%		
Total: 23,645 records	100%	Total: 45,321 records	100%

Note: the two risk types differ in monitoring scope, data volume and classification. The table shows each one's internal mix, i.e. how concentrated each industry is within that risk type.

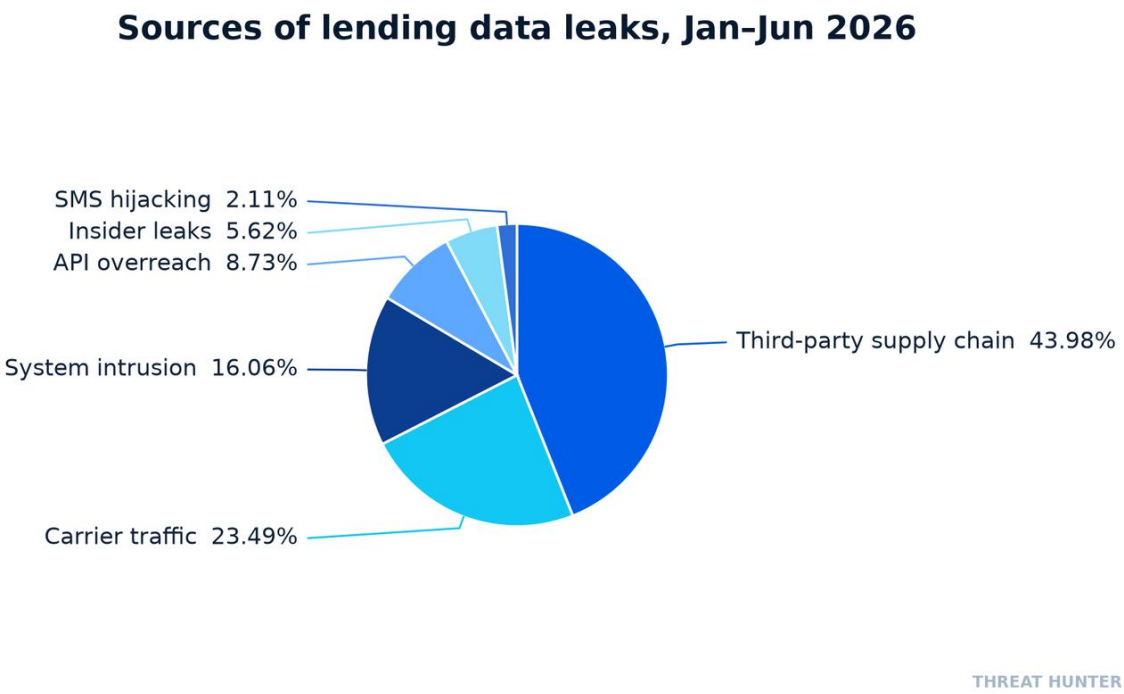
Data-leak and brand-abuse risk by industry

Source: Threat Hunter original report, page 46. Table re-typeset in English from the original.

2.2.2.2 Finance and Lending: Exposure of business data increases the risk of identity fraud

The financial and lending business covers multiple aspects such as application, lending, payment, repayment and collection. Once the relevant data enters external channels, it may be used to restore the true business relationship with customers and enhance the credibility of false customer service, fake collection and counterfeit channels.

Among the loan data samples leaked in the first half of 2026, loan materials accounted for about 64.6%, and application materials accounted for about 28.6%. The risks involve banks, consumer finance, online small loans, loan assistance platforms and other types of institutions, and may originate from third-party services, interface permissions, communication links and internal personnel. The brand risk faced by financial institutions is therefore not only reflected in the fraudulent use of websites, customer service numbers and corporate identities, but is also closely related to whether customer business information is out of control.



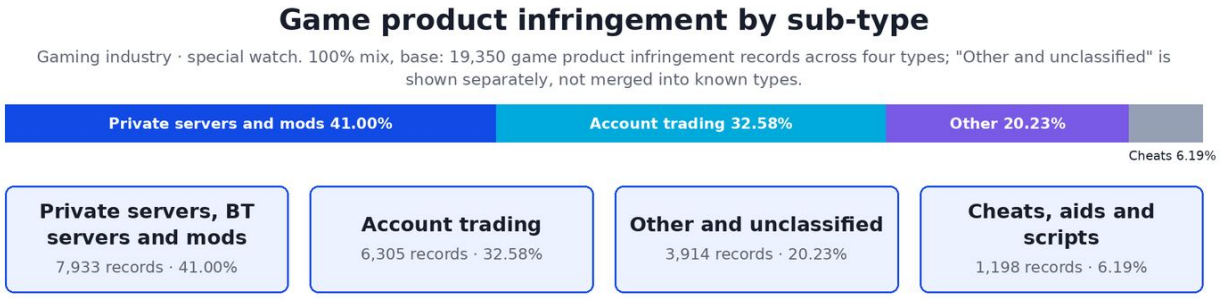
Sources of lending data leaks, Jan–Jun 2026

Source: Threat Hunter original report, page 46. Redrawn in English from the original figure.

2.2.2.3 Game industry: social communication and product infringement form an independent ecosystem

In the first half of 2026, Threat Hunter specifically monitored 77,816 risks related to the gaming industry, including 56,071 cases of social media counterfeiting and 19,350 cases of product infringement. Since the game industry adopts independent monitoring objects and statistical calibers, the relevant data are not directly aggregated or compared horizontally with the total risk amount mentioned above.

Risks in the game industry are mainly concentrated in two types of scenarios: one is to attract players into private channels through content such as benefits, redemption codes, and scarce resources; the other is the product infringement ecosystem formed around private servers, account transactions, plug-ins, auxiliaries, and scripts. Relevant risks are characterized by fragmented platforms, multiple content variations, rapid account reconstruction, and repeated listing of products.



Game product infringement by sub-type

Source: Threat Hunter original report, page 47. Redrawn in English from the original figure.

Regarding the brand protection risks faced by different industries, Threat Hunter will subsequently release the "Report on External Risk Trends of Chinese Enterprise Brands in the First Half of 2026". The report will focus on the analysis of external risks such as data leakage, identity fraud, channel interception and public disclosure, and systematically present how brand protection extends from the disposal of single counterfeit assets to key objects such as brand identity, official channels, customer relations and public reputation.

The report will also further dissect the risk differences in key industries such as finance and lending, e-commerce, manufacturing and retail, and games. It will also combine typical cases to restore real business information and counterfeit identities, and how to enhance the credibility of fraud by combining unofficial channels, and how cybercriminal operations use search, content platforms, social media, customer service portals, and dynamic QR codes to implement traffic diversion and identity fraud.



Contents of the H1 2026 Brand External Risk Trends Report

Source: Threat Hunter original report, page 48. Redrawn in English from the original figure.

2.3 Credit fraud scenario analysis

2.3.1 In the first half of 2026, the development of risk signal on malicious financial loan fraud has remained stable, but the scale has shrunk.

2.3.1.1 Risk signal on the risk of malicious loan fraud in the first half of 2026 rose by 2% compared with the second half of 2025

In the first half of 2026, Threat Hunter captured a total of 1.12 million malicious loan fraud risk signals, and monthly risk signals continued to grow, increasing by 2% compared with the second half of 2025.

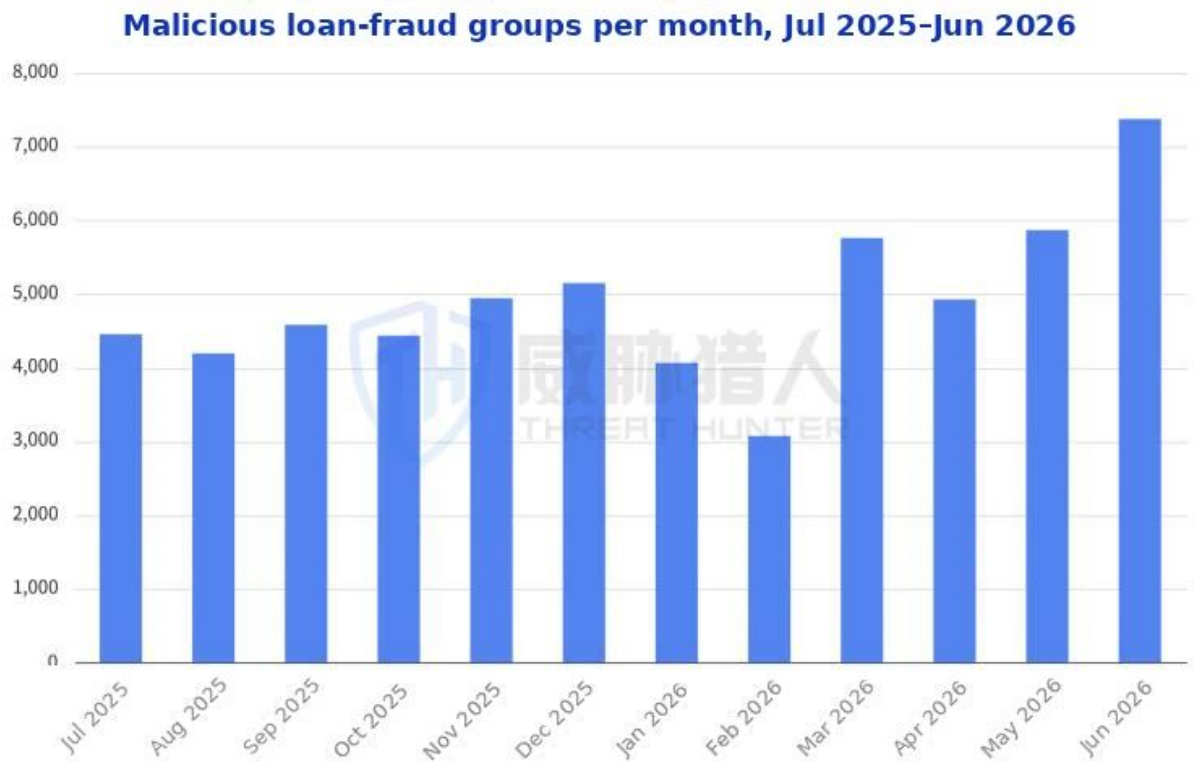


Malicious loan-fraud risk signals per month, Jul 2025–Jun 2026

Source: Threat Hunter original report, page 49. Original figure with Chinese text replaced by English.

2.3.1.2 The number of malicious fraud groups in the first half of 2026 rose by 17% compared with the second half of 2025

In the first half of 2026, Threat Hunter monitored a total of 14,000 active malicious fraud groups, an increase of 17% from the second half of 2025.



Malicious loan-fraud groups per month, Jul 2025–Jun 2026

Source: Threat Hunter original report, page 49. Original figure with Chinese text replaced by English.

2.3.1.3 In the first half of 2026, the number of malicious loan fraud accounts decreased by 3% month-on-month

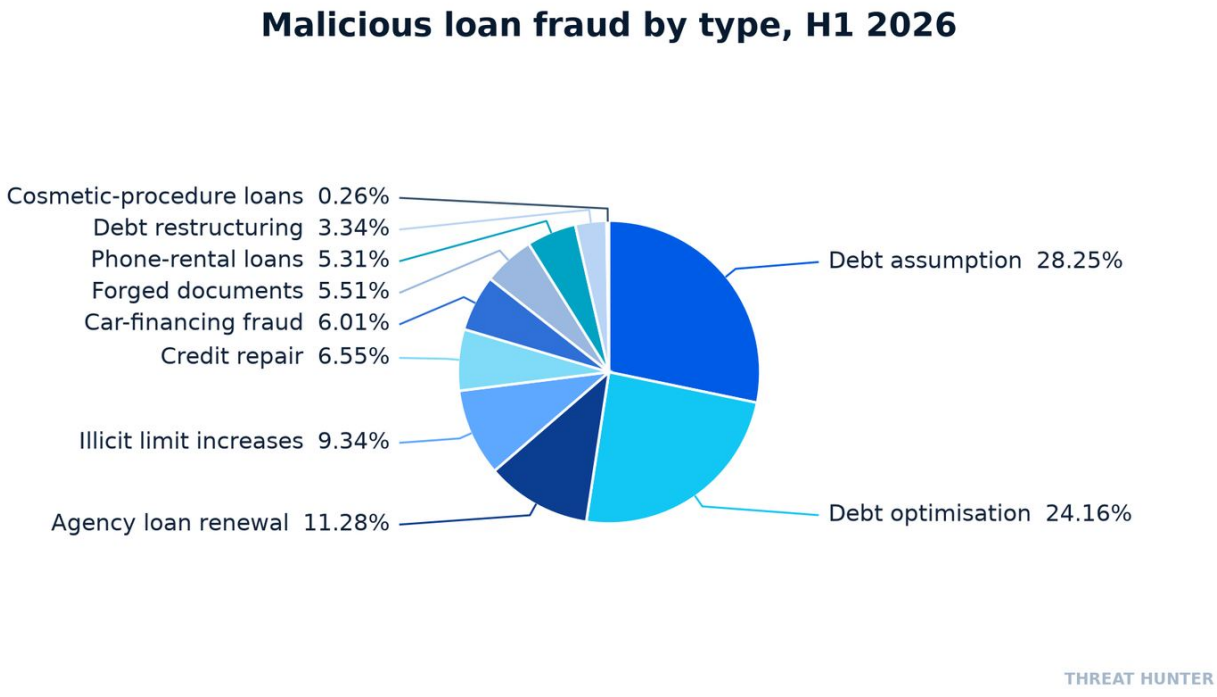
In the first half of 2026, Threat Hunter monitored a total of 56,000 fraudulent accounts (fraudulent credit intermediaries and cybercriminal groups) providing malicious loan services, a decrease of 3% from the second half of 2025.



Malicious loan-fraud accounts per month, Jul 2025–Jun 2026

Source: Threat Hunter original report, page 49. Original figure with Chinese text replaced by English.

2.3.1.4 Top 5 major types of malicious loan fraud in the first half of 2026: professional debt assumption, debt optimization, agency loan renewal, illegal limit increase, and credit report repair

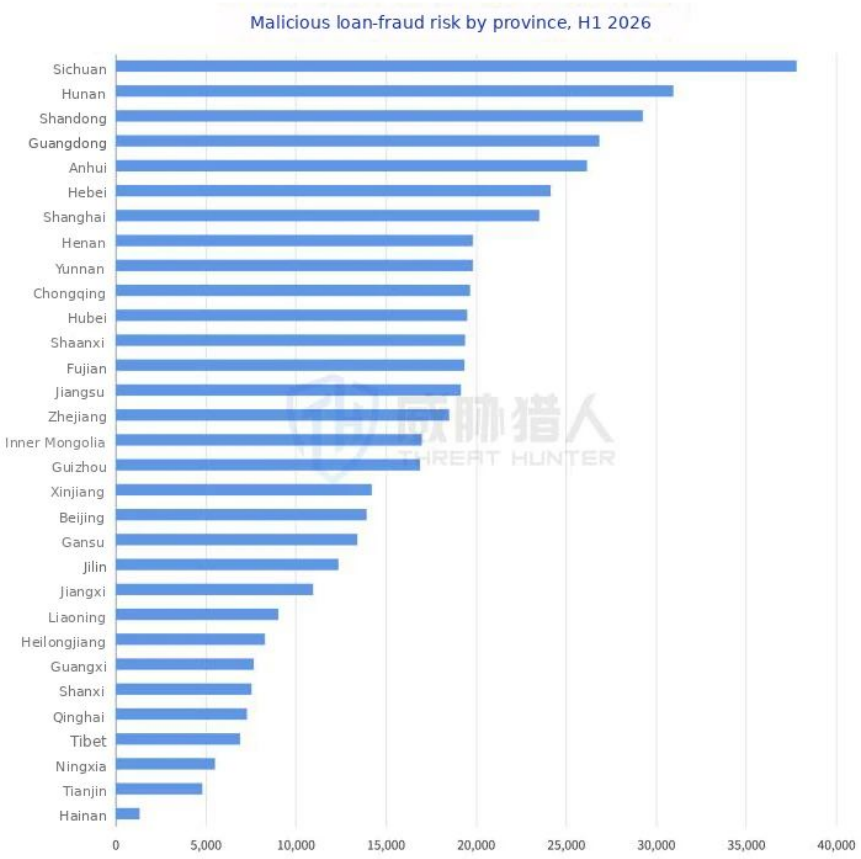


Malicious loan fraud by type, H1 2026

Source: Threat Hunter original report, page 50. Redrawn in English from the original figure.

2.3.1.5 Top 5 malicious loan fraud risk areas in the first half of 2026: Sichuan, Hunan, Shandong, Guangdong, Anhui

Threat Hunter intelligence data shows that the top five provinces (including municipalities) with the most active malicious loan fraud in the first half of 2026 are Sichuan, Hunan, Shandong, Guangdong, and Anhui.



Malicious loan-fraud risk by province, H1 2026

Source: Threat Hunter original report, page 50. Original figure with Chinese text replaced by English.

2.3.2 Professional debt-assumption risks were contained in the first half of 2026

2.3.2.1 Risk signal on professional debt assumption risks in the first half of 2026 fell by 31% compared with the second half of 2025

In the first half of 2026, Threat Hunter captured a total of 220,000 risk signals on professional debt risks. Overall, under the continued tightening of supervision, professional debt risks have been contained to a certain extent, and the amount of risk signal in the first half of the year dropped by 31% compared with the second half of 2025.

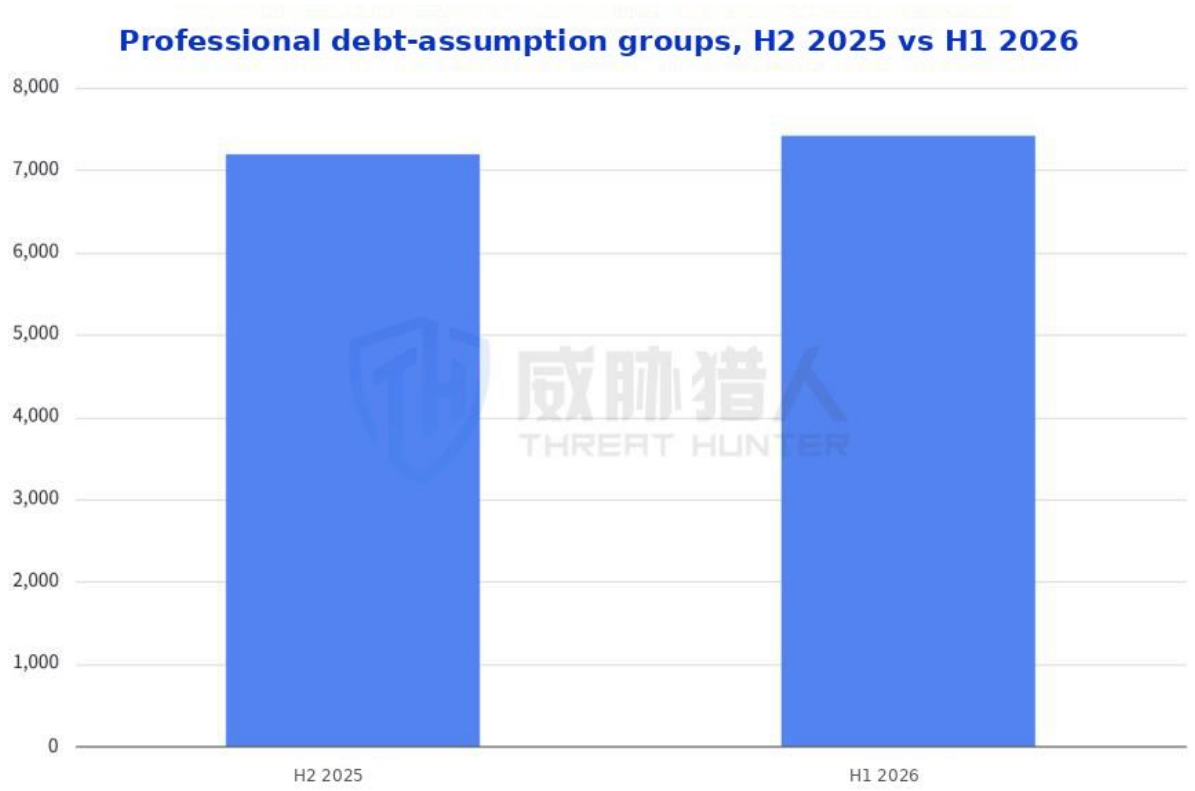


Debt-assumption fraud risk intelligence, H2 2025 vs H1 2026

Source: Threat Hunter original report, page 51. Original figure with Chinese text replaced by English.

2.3.2.2 The number of active debt-bearing groups in the first half of 2026 rose by 3% compared with the second half of 2025

Monitoring data in the first half of 2026 shows that the number of active debt-bearing groups exceeds 7,400, a slight increase of 3% from the second half of 2025, and the gathering trend of cybercrime operations lines is still active.

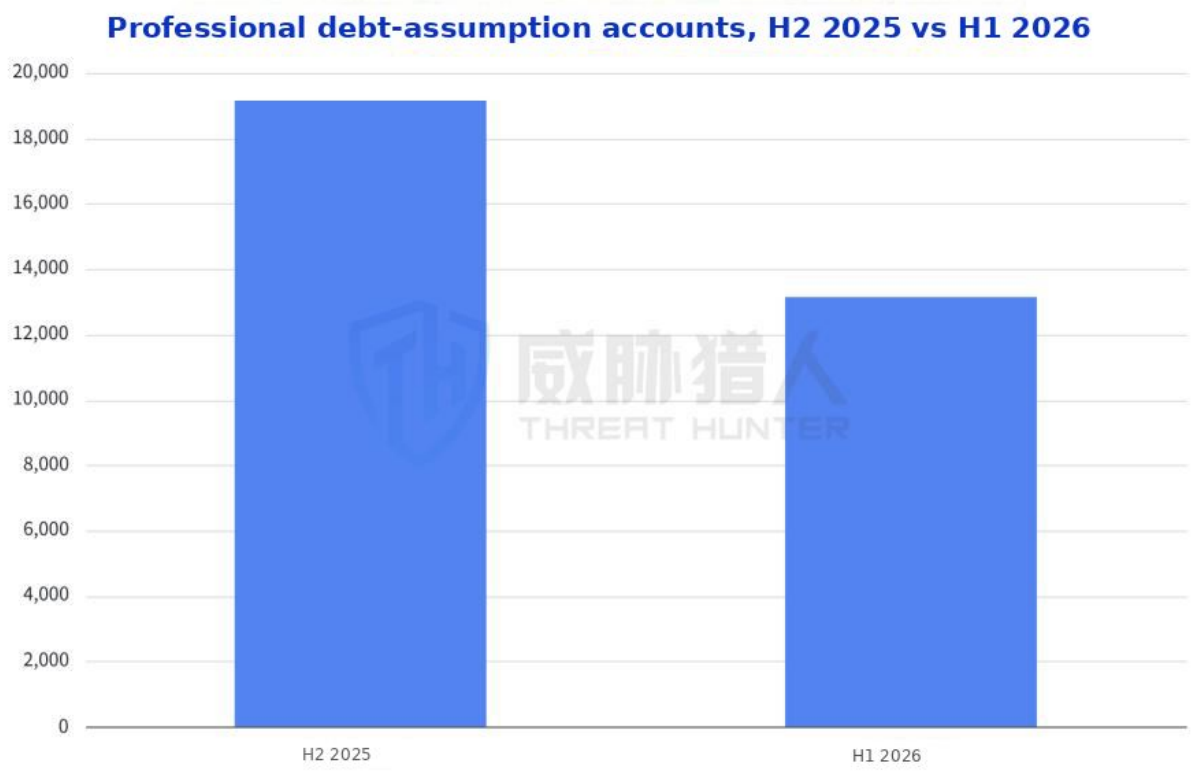


Professional debt-assumption groups, H2 2025 vs H1 2026

Source: Threat Hunter original report, page 51. Original figure with Chinese text replaced by English.

2.3.2.3 The number of debt service accounts in the first half of 2026 fell by 31% compared with the second half of 2025

In the first half of 2026, the number of active debt service accounts exceeded 13,000, a decrease of 31% from the second half of 2025, indicating that the activity of cybercrime operations servers has shrunk.

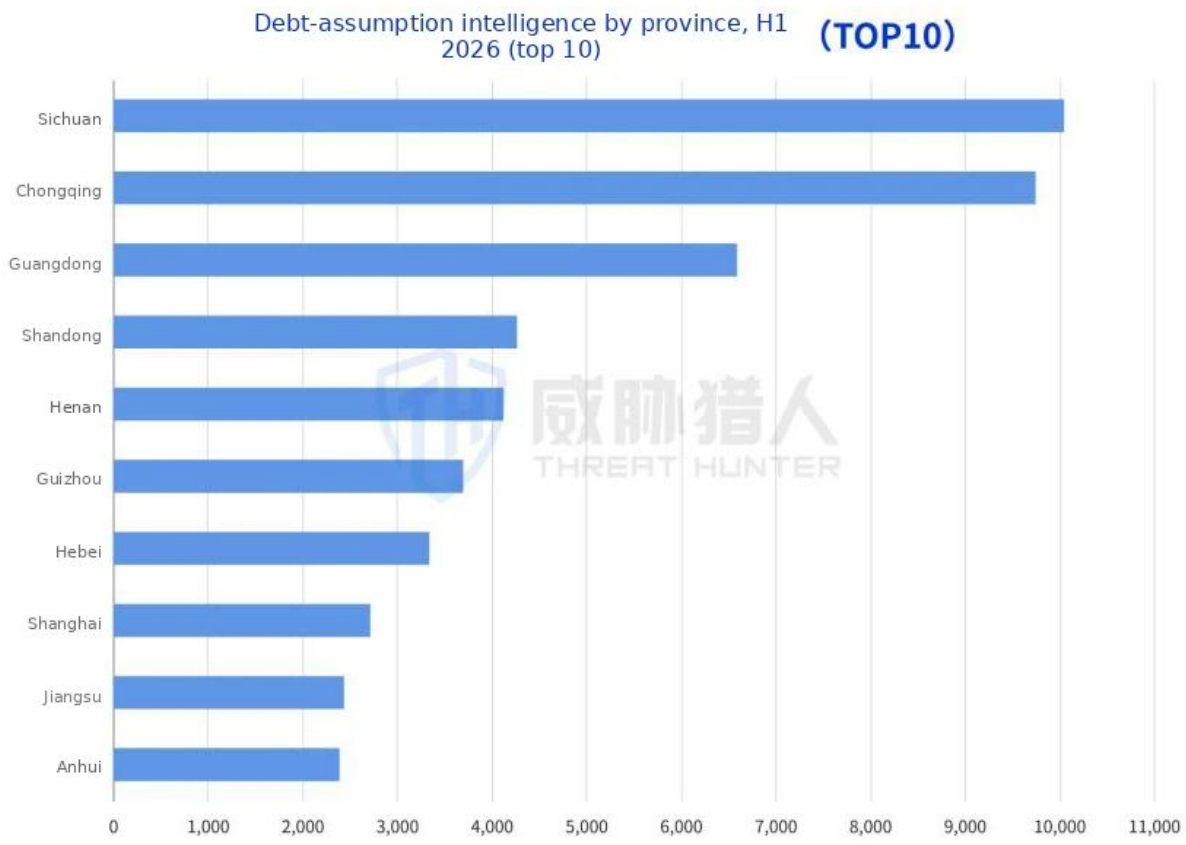


Professional debt-assumption accounts, H2 2025 vs H1 2026

Source: Threat Hunter original report, page 52. Original figure with Chinese text replaced by English.

2.3.2.4 Top 5 most popular provinces with debt in the first half of 2026: Sichuan, Chongqing, Guangdong, Shandong, Henan

Threat Hunter intelligence data shows that the top five most active provinces (including municipalities) for debt-related loan fraud in the first half of 2026 are Sichuan, Chongqing, Guangdong, Shandong, and Henan.



Debt-assumption intelligence by province, H1 2026 (top 10)

Source: Threat Hunter original report, page 52. Original figure with Chinese text replaced by English.

2.3.2.5 The survival status of debt-assumption groups under high pressure

The professional debt industry chain is highly organized and large-scale, and exhibits the characteristics of cross-regionalization, technology and industrialization. In recent years, the financial non-performing assets caused by this industrial chain have continued to rise and have become an important source of risks that threaten financial stability.

In the first half of 2026, supervision continued to intensify and criminal deterrence continued to increase. Under the dual pressure of tightening supervision and fraud controls policies, the pass rate of illegal crimes was significantly limited, the overall profits fell sharply, and the living space was significantly narrowed. A large number of cybercriminal group gangs were destroyed in accordance with the law, and there was a saying in the industry that "economic investigation detention facilities in various places are crowded with financial practitioners."

Overall, under high pressure, debt-assumption operations are undergoing a round of deep reshuffle and reshaping. The low-end players are being eliminated at an accelerated pace, but the remaining cybercrime operations gangs have more sophisticated and covert methods, and will continue to develop new fraud methods, and the offensive and defensive game continues to escalate.

2.3.3 Risks and changes in each loan scenario

Under the current strict rectification environment, risk signal on risks in major loan scenarios such as housing loans, consumer loans, corporate loans, and car loans will overall decline in the first half of 2026 compared with the second half of 2025, and illegal activities will face certain resistance. However, in the face of multiple pressures, the fraudulent methods and performance of cybercrime operations in various scenarios have also evolved differently, as follows:

Loan scenario	Fraud types	Key trends and changes
Mortgages	Property cash-out Combined property, credit, business and car debt assumption Fake mortgages by developers	High valuations and high loan amounts were restricted and margins narrowed, so threat actors turned to "distressed" properties with bigger price gaps. Client qualification thresholds rose and usable resources kept shrinking.
Consumer loans	Packaged loan fraud (debt assumption) Debt restructuring A/B loans	In packaged loan fraud, genuinely back-paid contributions became the norm. As debt-restructuring risks were exposed, threat actors split roles to evade liability. With client quality falling overall, A/B loans were rampant and many regions launched special crackdowns.
Business loans	Professional debt assumption Tech-assisted limit increases QR-code turnover inflation Business-loan fraud Document packaging	In the current economic environment threat actors actively avoided risk and moved to QR-code turnover inflation on the merchant side. They exploited regional policy differences and inconsistent criteria between banks for targeted attacks. Fraud mainly combined real operations with "real data" or supporting packaging.
Car loans	Car-financing cash-out Nominee car purchases Pyramid-scheme car purchases Trap schemes	Targets were popular models with high resale value, to protect cash-out margins and resale speed. High liquidation losses and fast risk exposure forced some threat actors to change course.

Credit fraud by loan scenario: types and trends

Source: Threat Hunter original report, page 54. Table re-typeset in English from the original.

This report is compiled by the anti-fraud intelligence research team based on long-term monitoring data, real risk samples and industry governance practices. There is no end to the confrontation between cybercriminal operations. The attack methods of cybercriminal operations will continue to evolve, and the attack technology of cybercriminal operations will continue to be iterated. In the face of the ever-changing cybercrime ecosystem, Threat Hunter will continue to work closely with enterprises in various industries to jointly protect enterprise business security and user rights.

It is hoped that this report can help anti-fraud, security, fraud controls and business practitioners more accurately understand the changes in the cybercrime ecosystem, identify risk migration and method upgrades, and provide a reference for enterprises to formulate more forward-looking and targeted governance strategies.



Contents of the H1 2026 Credit Fraud Risk Research Report

Source: Threat Hunter original report, page 54. Redrawn in English from the original figure.