THREAT HUNTER RESEARCH

H1 2025 Data Breach Risk Report

A half-year review of data exposure, underground channel migration and the growing circulation of credit-related information.

Original publication: 2025-07-10
Research team: Threat Hunter Research Team
Source report: 40 pages

Original report text

This web edition is reconstructed from the 40-page original PDF. It keeps the report's narrative, chapters and research scope, but leaves out the cover, the duplicate table of contents and purely decorative pages. Figures have been localized and placed in context, and the original PDF remains available for reference.

About Threat Hunter

Threat Hunter was founded in 2017 and helps organizations identify and respond to business fraud, external digital risk, and API security threats. Its work combines cybercrime intelligence, risk data, product platforms, and specialist services.

The company offers a broad, mature portfolio of products and services for the risks that organizations in many industries face as they digitize, including business fraud, data leakage, phishing and impersonation, and API attacks. Leading industry analysts have repeatedly named it a representative vendor in technology maturity and threat intelligence research.

Headquartered in Shenzhen, Threat Hunter also operates offices in Beijing, Shanghai, and Chongqing, with Digital Risk Response Centers in Shenzhen and Chongqing. The company supports customers in China, Europe, the United States, South America, and Southeast Asia.

Preface

As digitalization continued to advance in the first half of 2025, data remained a core business asset, and its security drew growing attention. Data breaches stayed at a high level, while attack methods and trading chains became more complex and harder to see. Together they now pose a major risk to compliant operations and business growth.

Threat Hunter's "H1 2025 Data Breach Risk Report" tracks how data-leak risk is changing. It covers incident volume, industry distribution, trading channels and typical cases, analyzes the latest moves in the criminal data-trading chain, and gives a full picture of data-leak risk in China in the first half of 2025.

Key findings:

1. Data breaches stayed high and recovered quickly after a short dip.

Threat Hunter confirmed 57,092 valid data breaches in the first half of 2025, up 1.54% from the second half of 2024. In April, a group-closure campaign on a major encrypted messaging app cut incidents by almost 30% for a short time. In June, as criminal groups regrouped, the number rebounded quickly.

2. High-value industries were the main targets, and cross-border e-commerce leaks rose sharply.

E-commerce, consumer finance and banking remained the hardest-hit industries. Together, these top 3 accounted for 1.32 times as many incidents as the other seven industries in the top 10.

Within e-commerce, cross-border e-commerce incidents grew more than tenfold from the previous half-year, a clear sign that the trade is going international.

3. Dark-web leaks rose 35.2%, and activity on Chinese-language forums grew sharply.

Dark-web channels accounted for 18,106 leak incidents, up 35.2% from the previous half-year. Users of Chinese-language dark-web forums such as "Chang'an City" and "D*Chinese" grew quickly. Newly registered users posted more than half of these incidents, and most of the leaked data came from platforms outside China.

4. "Haowang Guarantee" collapsed, "Tudou Guarantee" quickly took its place, and guarantee platforms proved easy to replace.

"Haowang Guarantee", the leading guarantee platform on encrypted messaging apps, was hit hard in May and its business stopped. By June, newer platforms such as "Tudou Guarantee" had filled the gap. Both supply and demand in the underground market remain very active, and the trading chain has a strong ability to heal itself.

5. After BF shut down, several platforms took over, and threat-actor trading moved with them.

Before it went offline, BF accounted for 14.5% of dark-web leak incidents. After the shutdown, its core users moved quickly to alternatives such as X*S and D**s and kept trading data, which shows how readily threat actors adapt and migrate.

6. Leaks of "multi-lending" credit data surged and now support a complete criminal supply chain.

Leaks of credit risk data, led by "multi-lending" records, rose sixfold in six months. A full criminal ecosystem has formed around them, from data theft and platform building to targeted fraud. Threat actors have used several risk-check query platforms, such as "Fuyao" and "Xinchen", as relay points for the data.

7. Leaks of bank "scan-code application" data rose more than fourfold and are linked to a third-party marketing tool.

Threat Hunter found 111 leaks of "scan-code application" loan data in the first half of the year, involving more than 80 banks. The core risk lies in a fintech marketing platform used in banks' account-manager systems. An insider or a system flaw is suspected of sending data on high-intent customers to the black market.

Disclaimer: The data in this report is estimated and analyzed using large-sample collection, small-sample surveys, data-model forecasts and other research methods. Every data source and technique in statistical analysis has limits, and Threat Hunter's are no exception. The data is provided for reference only. Threat Hunter gives no warranty as to its accuracy, completeness, fitness for purpose or non-infringement, and accepts no liability for legal consequences of any action that an organization or individual takes based on it. Any resulting disputes or legal liability rest with the party that took the action.

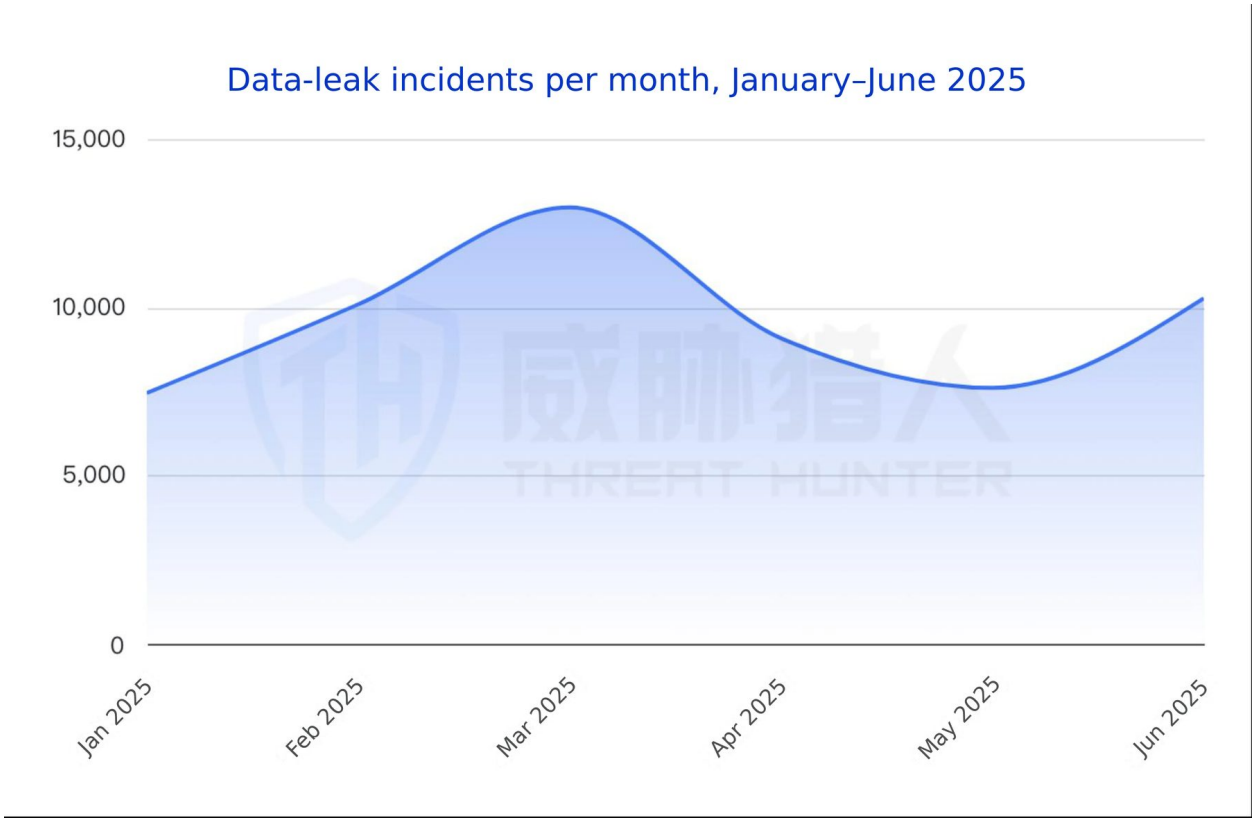
Part 1 reviews the volume, industry spread and channels of data breaches in the first half of 2025.

1. Overview of data breach risks in the first half of 2025

1.1 Data breaches in the first half of 2025 totaled 57,092, up 1.54% from the second half of 2024

Between January and June 2025, Threat Hunter's data-leak risk monitoring platform collected 180 million intelligence leads across the internet. After checks by the authenticity verification engine and manual analysis by the Digital Risk Response Center (DRRC), 57,092 of them were confirmed as valid data breaches.

From January to March 2025, the number of breaches rose steadily. In April, however, it fell 29.93% from March, a drop of 3,882 incidents. It hit its low point in May at 7,609 and began to recover in June.



Data-leak incidents per month, January–June 2025: a rise to March, a fall to a low in May, and a rebound in June

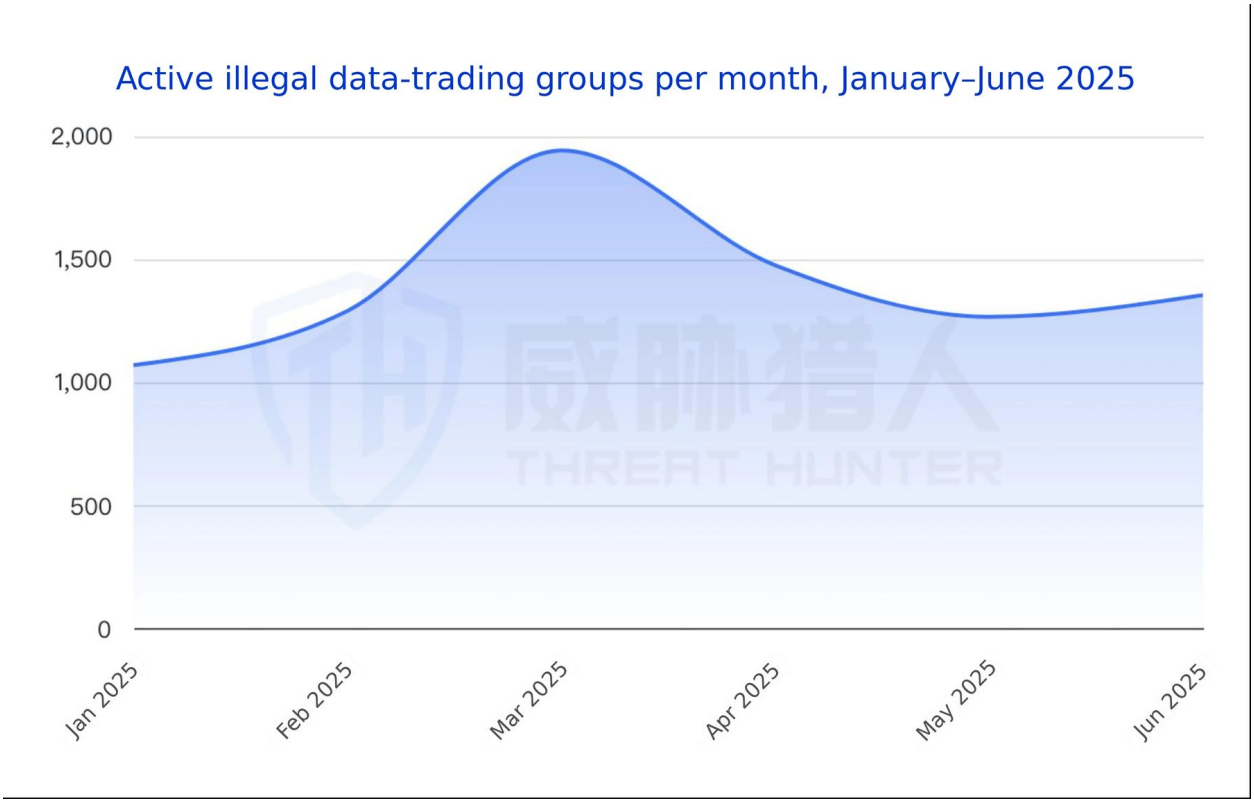
Source: Threat Hunter original report, page 7. Original figure with Chinese text replaced by English.

Threat Hunter traced this swing mainly to a group-closure campaign that a major encrypted messaging app launched against illegal groups in April 2025. The campaign banned a large number of group chats used for illegal data trading (see section 2.1). A closer look at the sources of the leaks showed the following.

In April 2025, Threat Hunter recorded 9,085 data breaches, 29.93% fewer than in March (12,967). Over the same period, the number of active illegal data-trading groups fell from 1,943 to 1,477, a drop of 23.98%.

Of the illegal data-trading groups that were active in March, 33.71% were banned in April.

As a result, the number of data breaches fell sharply.



Active illegal data-trading groups per month, January–June 2025

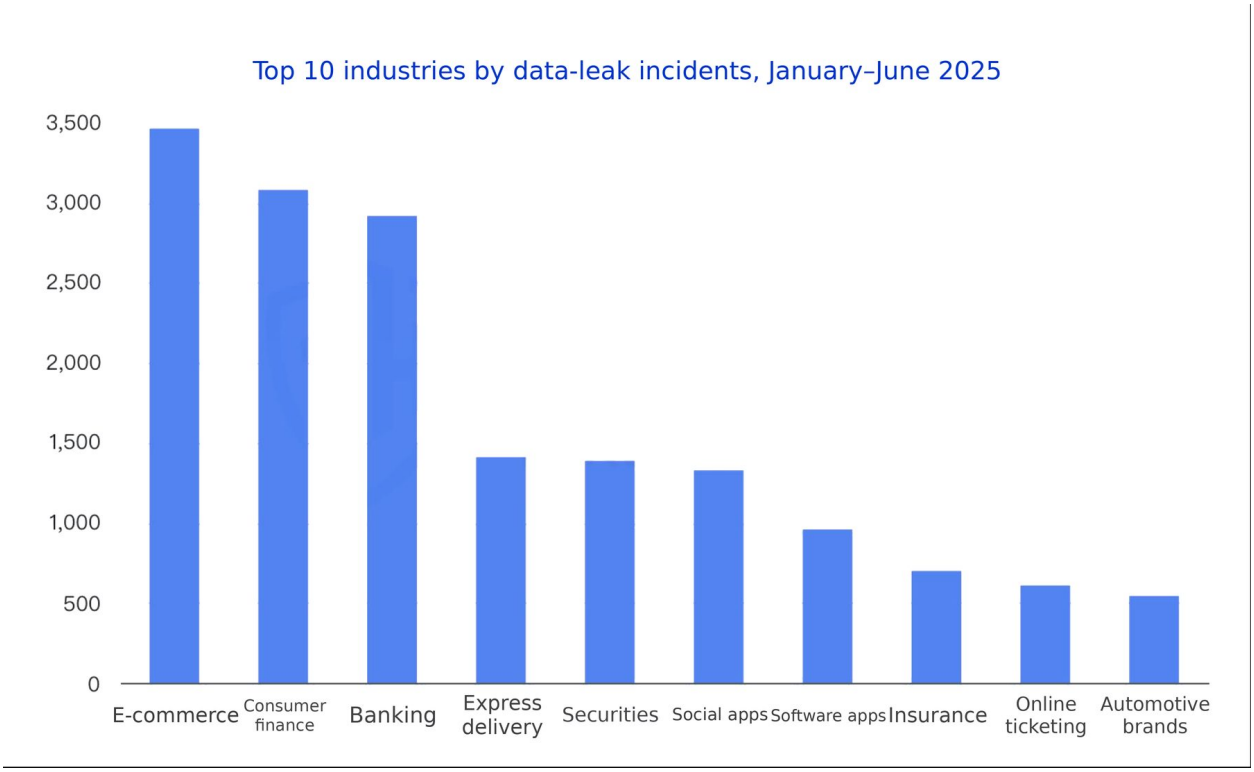
Source: Threat Hunter original report, page 8. Original figure with Chinese text replaced by English.

However, the app could not ban these groups completely, and the gangs proved very good at regenerating. Many new or replacement groups became active again within a short time, and the number of data breaches rose again in June 2025.

1.2 In the first half of 2025, the top 3 industries saw 1.32 times as many data breaches as the rest of the top 10

Attack groups prefer data targets with high value and high activity. Data breaches across the internet in the first half of 2025 involved 76 industries in total, and the top 3 were e-commerce, consumer finance and banking.

E-commerce and finance, where data is highly sensitive and easy to turn into money, remain the hardest-hit sectors.



Top 10 industries by data-leak incidents, January–June 2025

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

The chart below shows how the top 10 industries moved in the rankings in the first half of 2025.

Industry	Rank, H2 2024	Rank, H1 2025	Change
E-commerce	3	1	Up 2
Consumer finance	1	2	Down 1
Banking	2	3	Down 1
Express delivery	4	4	No change
Securities	5	5	No change
Social apps	11	6	Up 5
Software apps	10	7	Up 3
Insurance	8	8	No change
Online ticketing	6	9	Down 3*
Automotive brands	7	10	Down 3

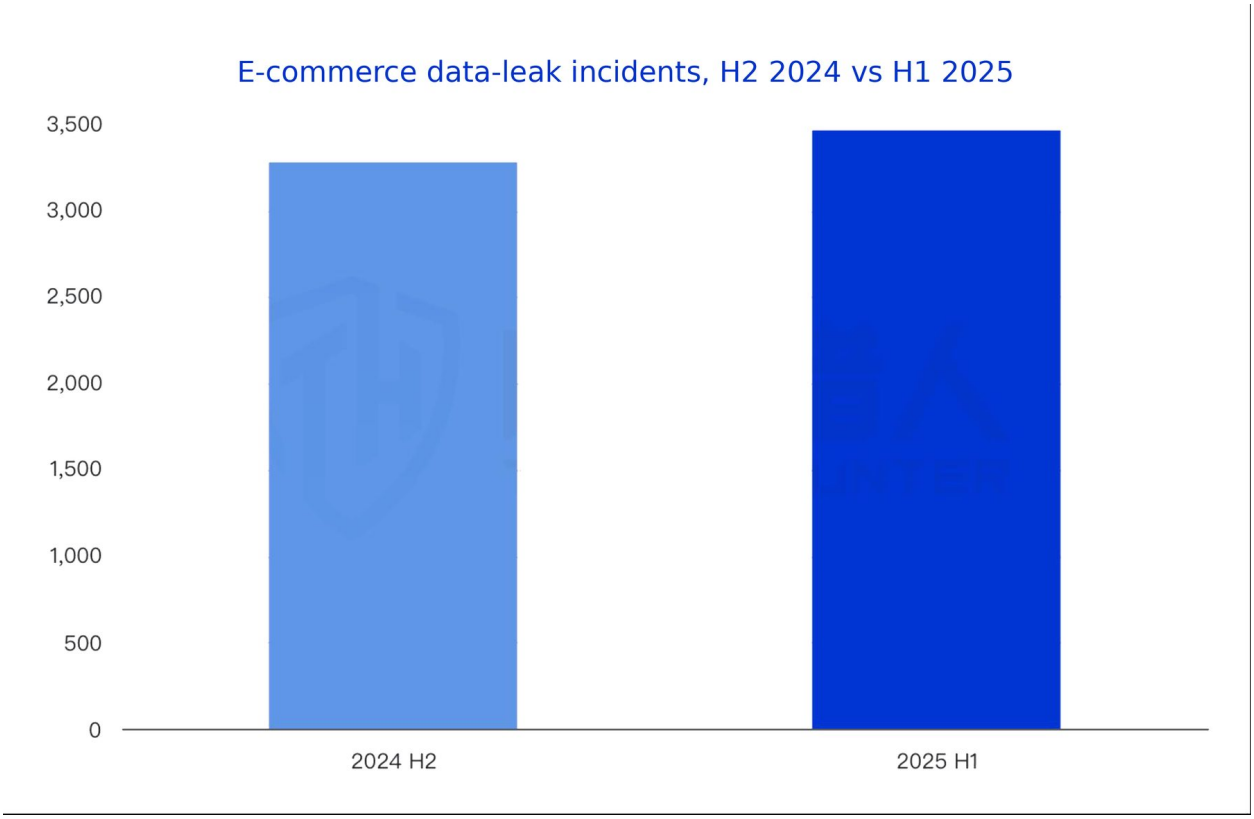
* The original marks this change as a rise; its ranks (6 to 9) show a fall of three places.

Top 10 industries by data-leak incidents: rank in H2 2024, rank in H1 2025 and change

Source: Threat Hunter original report, page 9. Table re-typeset in English from the original.

1.3 E-commerce became the industry with the most data breaches, at 3,465 incidents, and cross-border e-commerce leaks grew more than tenfold

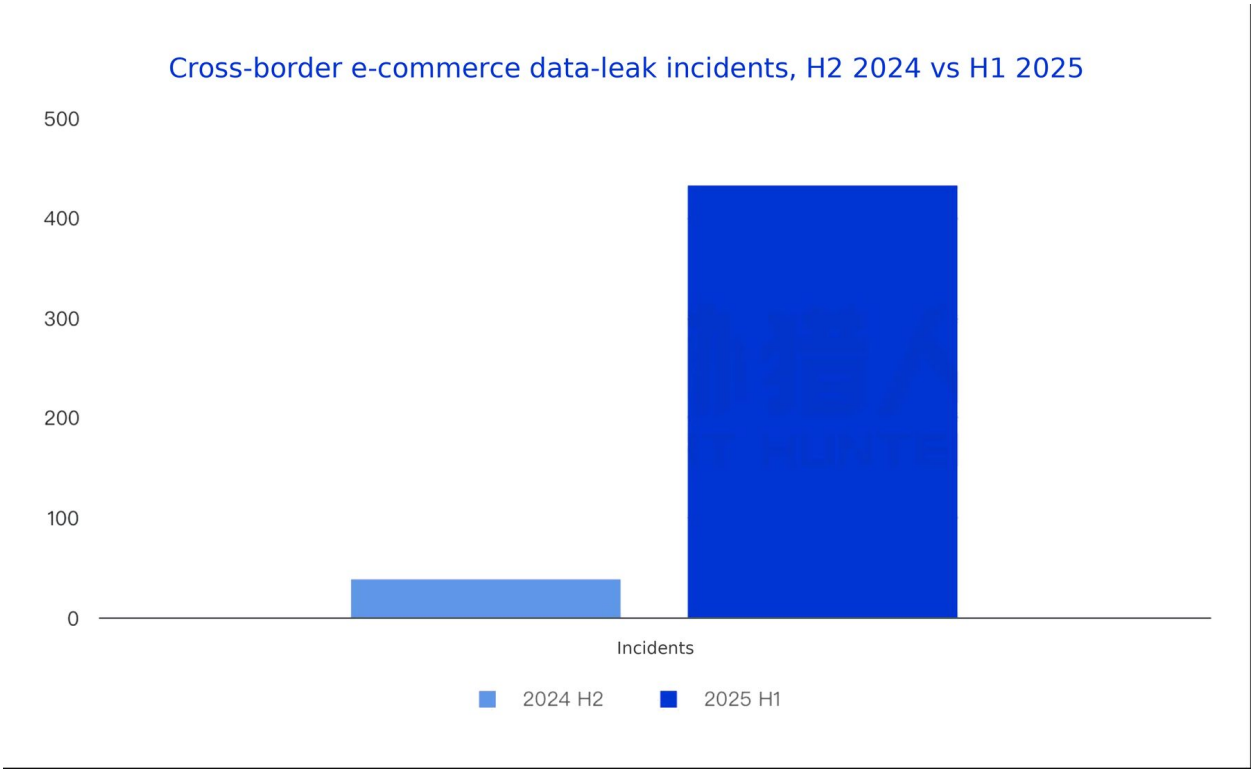
Threat Hunter's data-leak risk monitoring platform recorded 3,465 data breaches in e-commerce in the first half of 2025. That is 184 more than in the second half of 2024, an increase of 5.60%.



E-commerce data-leak incidents, H2 2024 vs H1 2025

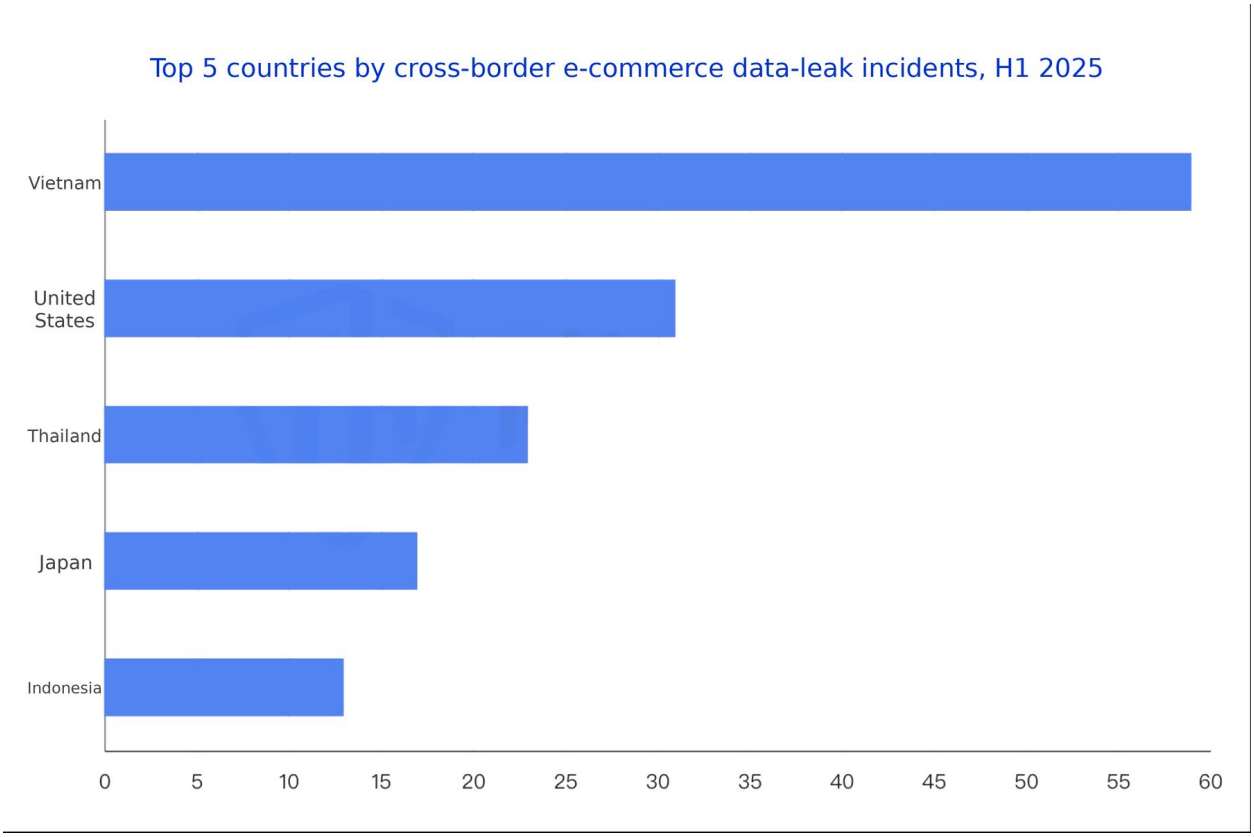
Source: Threat Hunter original report, page 10. Original figure with Chinese text replaced by English.

Cross-border e-commerce stood out. Its incidents rose by 394 compared with the second half of 2024, an increase of more than tenfold. The leaks involved many countries and regions, mostly in Southeast Asia. The top three countries were Vietnam, the United States and Thailand.



Cross-border e-commerce data-leak incidents, H2 2024 vs H1 2025

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



Top 5 countries by cross-border e-commerce data-leak incidents, H1 2025

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

1.3.1 Case study: a security weakness at a third-party logistics company exposed shopper data from several cross-border e-commerce platforms

Threat Hunter recently found a threat-actor group on the dark web selling online shopping data from users of a cross-border e-commerce platform. The seller posted data samples and claimed the data covered Southeast Asia, North America and other countries and regions.

Threat Hunter researchers studied fields such as the shipping label and the product label in the leaked data and concluded that the data probably came from a single international express logistics company. Earlier leaks linked to the same company on Chinese-language dark-web forums confirmed that its systems had a security weakness, which an outside threat-actor group exploited to steal user information.



	订单号	交易号	订单状态	客户	ID	发货时间	仓库	创建时间	物流	快递号	商品名称	图片路径	价格	同步ERP	同步时间	快递标签	电话
新加坡	JOAS29	QW347	发货成功	香港xxx	Alexand	2025/4/18	印度尼西	2025/4/18	虚拟物流	5.84E+09	JIOA30	https://c	237.24	同步成功	#######	https://t	237482
新加坡	JOAS29	QW347	发货成功	香港xxx	Oscar	2025/4/18	印度尼西	2025/4/18	虚拟物流	5.84E+09	DAJOD3	https://c	382.4	同步成功	#######	https://t	237482
新加坡	JOAS29	QW347	发货成功	香港xxx	Elijah	2025/4/18	印度尼西	2025/4/18	虚拟物流	5.84E+09	QOU1J3	https://c	382.4	同步成功	#######	https://t	237482
新加坡	JOAS29	QW347	发货成功	香港xxx	Cedric	2025/4/18	印度尼西	2025/4/18	虚拟物流	5.84E+09	AU249	https://c	382.4	同步成功	#######	https://t	237482
新加坡	JOAS29	QW347	发货成功	香港xxx	Emma	2025/4/18	印度尼西	2025/4/18	虚拟物流	5.84E+09	HDAOO	https://c	237.24	同步成功	#######	https://t	237482
新加坡	JOAS29	QW347	发货成功	香港xxx	Charlott	2025/4/18	印度尼西	2025/4/18	虚拟物流	5.84E+09	QOU1J3	https://c	237.24	同步成功	#######	https://t	237482
新加坡	JOAS74	QW347	发货成功	香港xxx	Sophia	2025/4/18	印度尼西	2025/4/18	虚拟物流	5.84E+09	QOU1J3	https://c	237.24	同步成功	#######	https://t	237482
新加坡	JOAS74	QW347	发货成功	香港xxx	Eleanor	2025/4/18	印度尼西	2025/4/18	虚拟物流	5.84E+09	QOU1J3	https://c	237.24	同步成功	#######	https://t	237482
新加坡	JOAS74	QW347	发货成功	香港xxx	Taylor	2025/4/18	印度尼西	2025/4/18	虚拟物流	5.84E+09	HDAOO	https://c	237.24	同步成功	#######	https://t	237482
新加坡	JOAS74	QW347	发货成功	香港xxx	Quinn	2025/4/18	印度尼西	2025/4/18	虚拟物流	5.84E+09	HDAOO	https://c	382.4	同步成功	#######	https://t	237482
新加坡	JOAS74	QW347	发货成功	香港xxx	Alex	2025/4/18	印度尼西	2025/4/18	虚拟物流	5.84E+09	HDAOO	https://c	382.4	同步成功	#######	https://t	34720
新加坡	JOAS74	QW347	发货成功	香港xxx	Morgan	2025/4/18	印度尼西	2025/4/18	虚拟物流	5.84E+09	DAJOD3	https://c	382.4	同步成功	#######	https://t	34720
新加坡	JOAS74	QW347	发货成功	香港xxx	Casey	2025/4/18	印度尼西	2025/4/18	虚拟物流	5.84E+09	DAJOD3	https://c	39	同步成功	#######	https://t	34720
新加坡	JOAS74	QW347	发货成功	香港xxx	Camero	2025/4/18	印度尼西	2025/4/18	虚拟物流	5.84E+09	DAJOD3	https://c	39	同步成功	#######	https://t	34720

Sample of leaked cross-border e-commerce orders offered on the dark web, with shipping and tracking fields

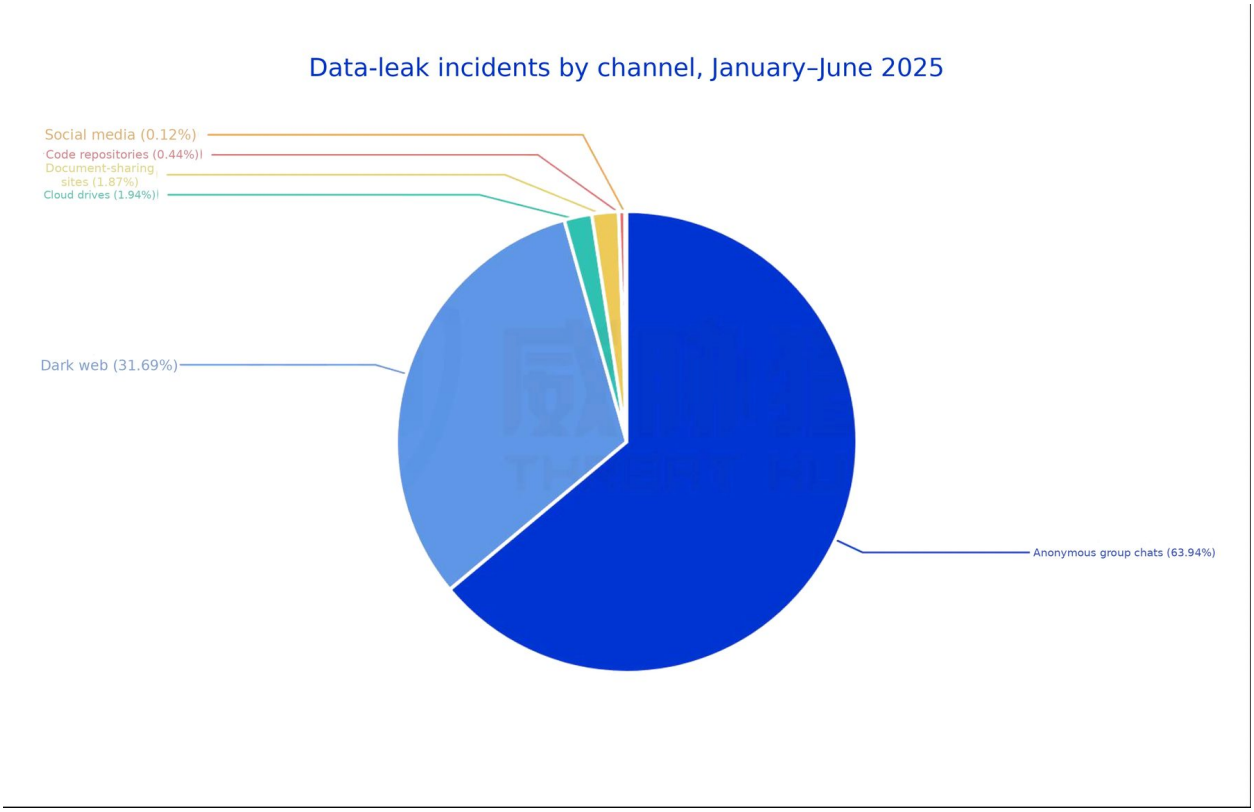
Source: Threat Hunter original report, page 11. Original image retained; numbered translations added by Threat Hunter.

Figure guide

1	Column headers, left to right: country, order number, transaction number, order status, customer, ID, shipping time, warehouse, creation time, logistics, tracking number, product name, image path, price, ERP sync, sync time, shipping label, phone
2	Rows: country "Singapore"; order status "Shipped"; customer "Hong Kong xxx"; warehouse "Indonesia"; logistics "Virtual logistics"; ERP sync "Synced"

1.4 Dark-web data-leak activity kept rising in the first half of 2025, with incidents up 35.2% from the previous half-year

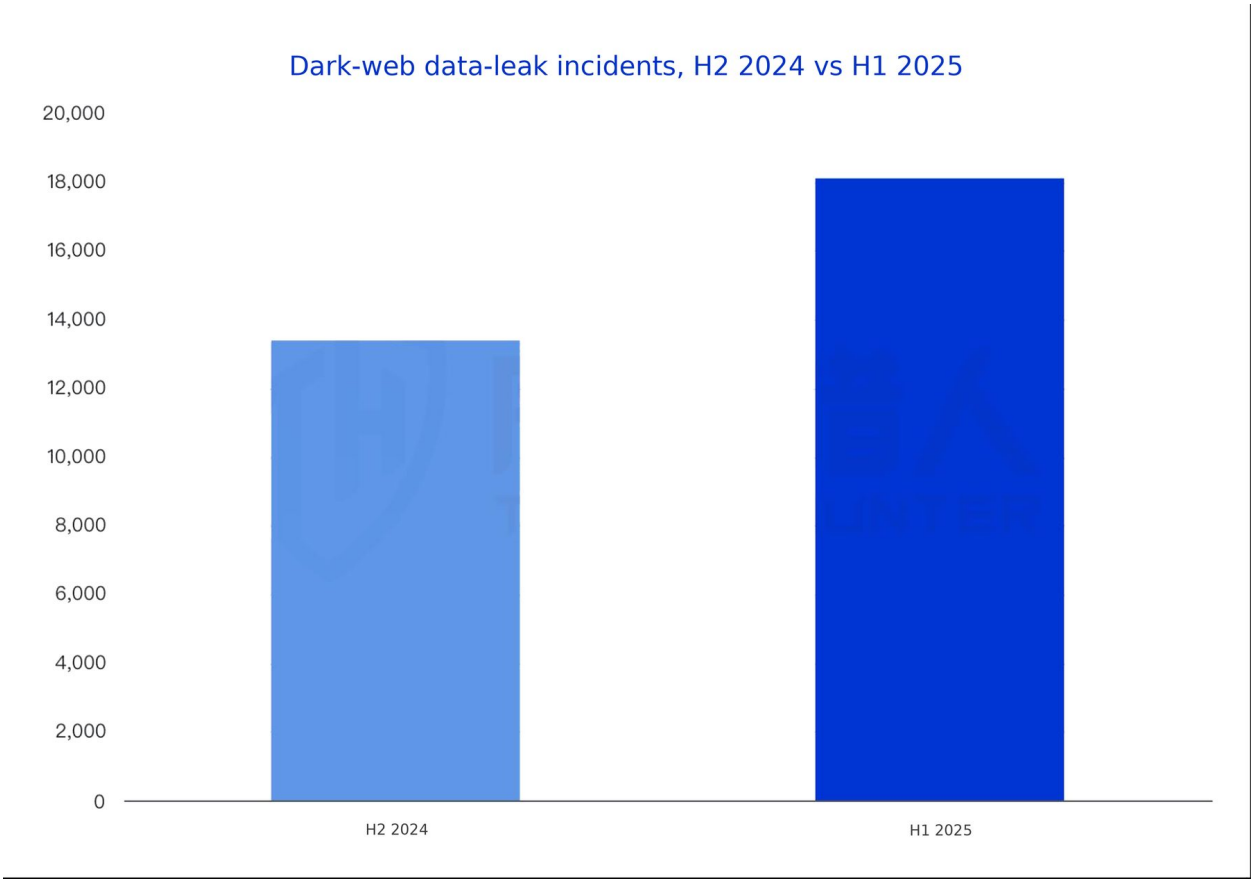
Threat Hunter's statistics show that anonymous group chats and the dark web remained the main channels for data leaks in the first half of 2025.



Data-leak incidents by channel, January–June 2025

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

Dark-web channels accounted for 18,106 data breaches, an increase of 35.2% over the 13,389 incidents recorded in the second half of 2024.



Dark-web data-leak incidents, H2 2024 vs H1 2025

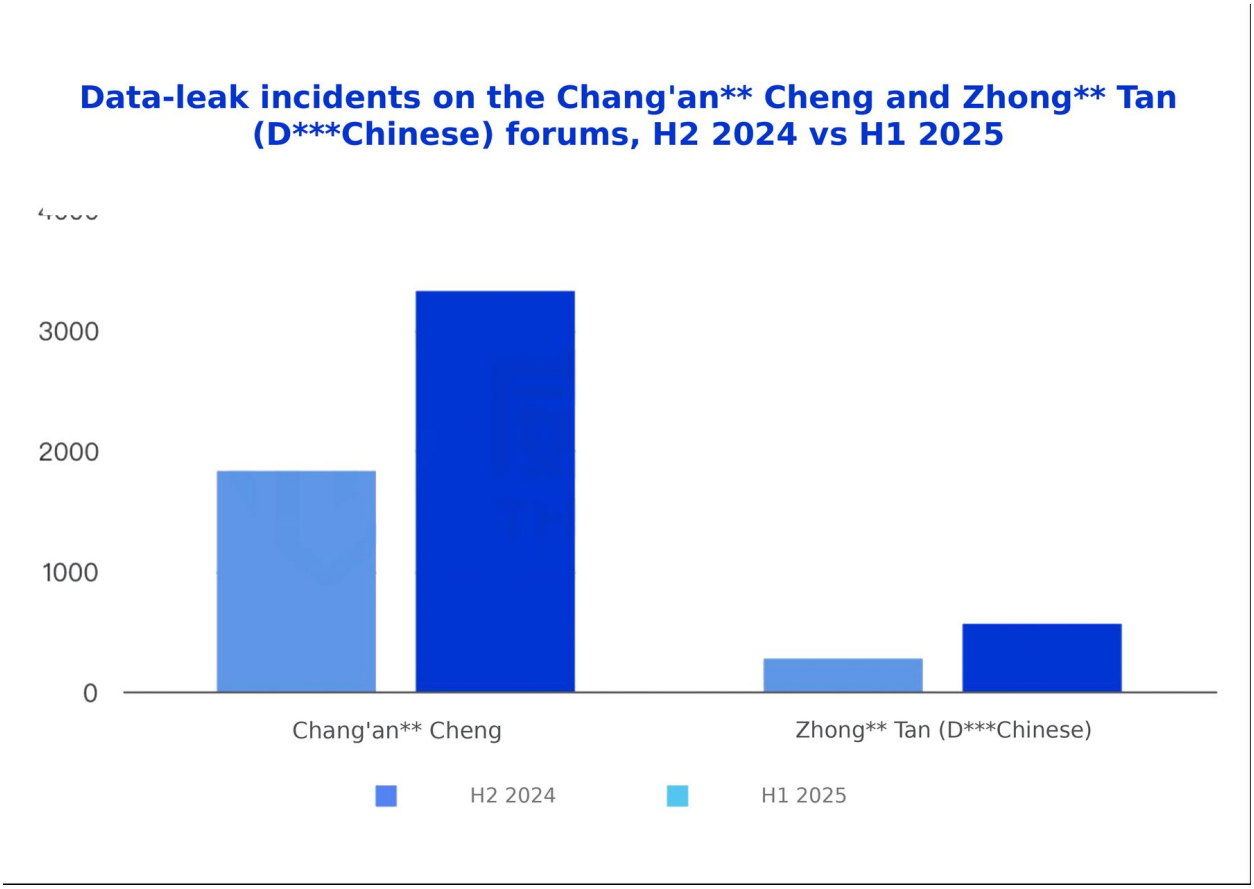
Source: Threat Hunter original report, page 12. Original figure with Chinese text replaced by English.

1.4.1 Activity on Chinese-language dark-web forums surged, and most leaks involved user data from outside China

Further analysis showed that the "Chang'an City" forum had the largest rise in data-leak incidents of any dark-web channel. Its incidents in the first half of 2025 rose 81.7% from the second half of 2024, to 1,493. Another Chinese-language forum, "D*Chinese", went from 272 incidents in 2024 to 560, an increase of 105.9%.

In 2025, 271 users posted data-trading threads on these two forums. Of these, 166 (61.3%) were newly registered users, and their posts covered 1,961 data-leak incidents, more than half of all incidents on the two forums.

Most of these new incidents involved data from platforms or users outside China. "Chang'an** City" alone carried user data from more than 20 countries and regions.



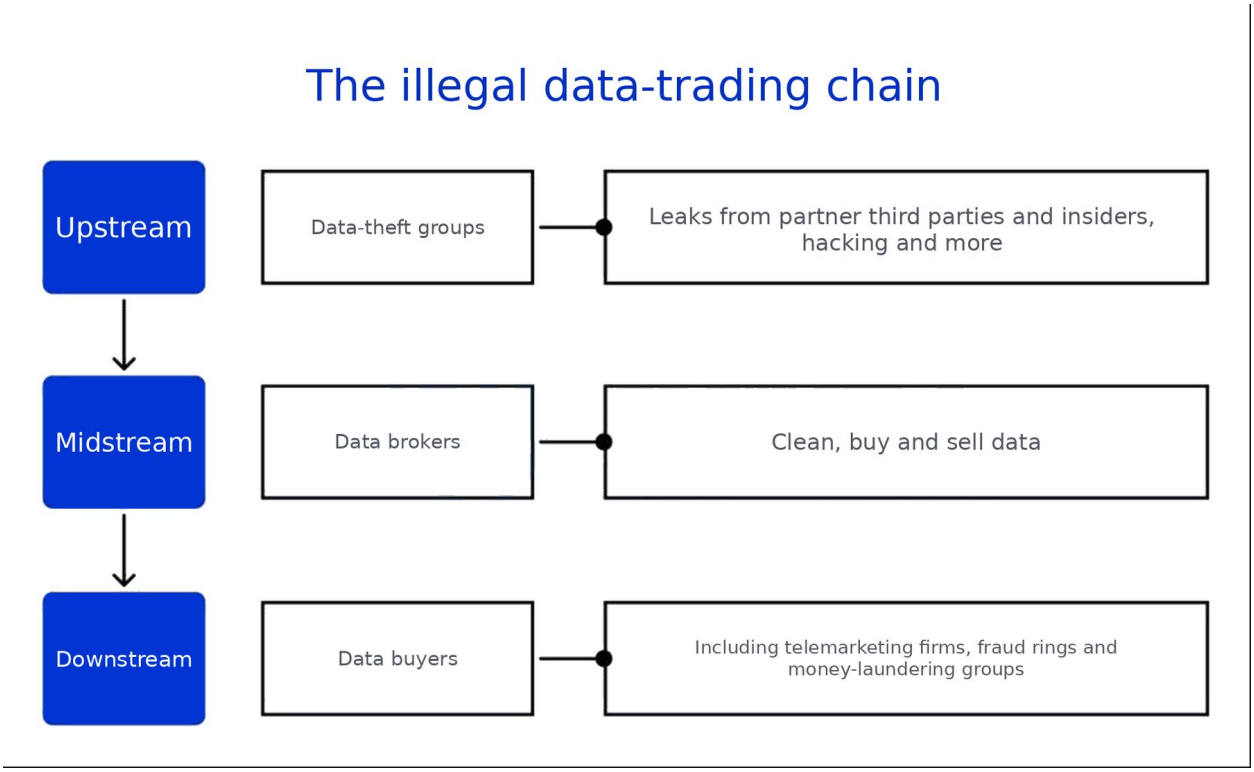
Data-leak incidents on two Chinese-language dark-web forums, H2 2024 vs H1 2025

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

Part 2 looks at how the data-trading market changed in the first half of 2025.

2. Analysis of data trading market trends in the first half of 2025

The illegal data-trading chain is shown below.



The illegal data-trading chain: data-theft groups upstream, data brokers in the middle, data buyers downstream

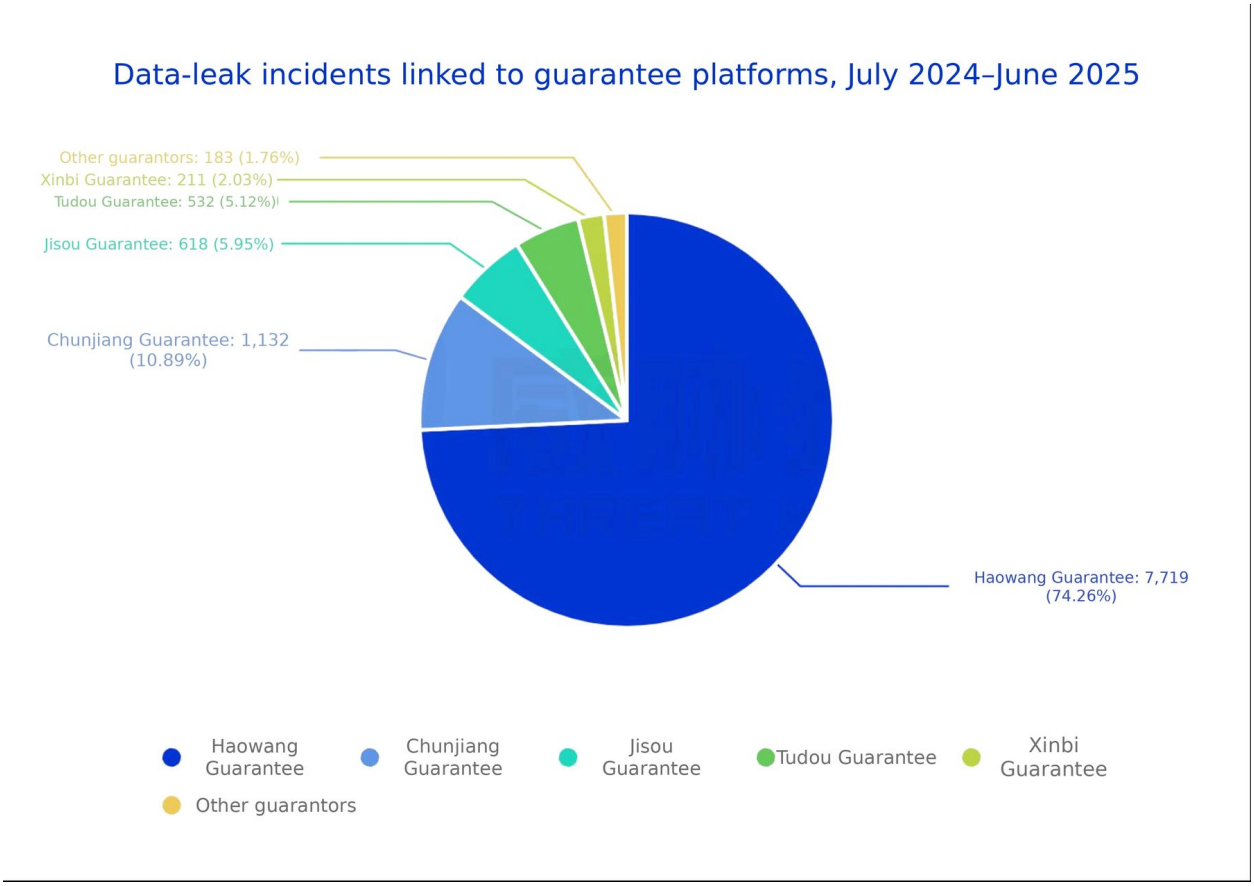
Source: Threat Hunter original report, page 15. Original figure with Chinese text replaced by English.

Data brokers in the middle of the chain operate on the dark web, threat-actor forums and encrypted messaging apps. They clean, sort and package leaked data and match buyers with sellers, which makes them the key hub of the whole trading chain.

Regulatory pressure keeps rising, but fraud gangs, gray-market e-commerce sellers and other buyers downstream still want high-quality data, and this demand keeps the market active.

2.1 The leading guarantee platform was hit hard, and new guarantee services quickly took its place

"Haowang Guarantee" (formerly "Huiwang Guarantee") operated for a long time on anonymous social platforms, mainly a major encrypted messaging app. By acting as a third-party trust intermediary, it became the main guarantee platform for criminal activity such as data trading, fraud and money laundering, and it dominated the market until the first half of 2025, as the chart below shows.

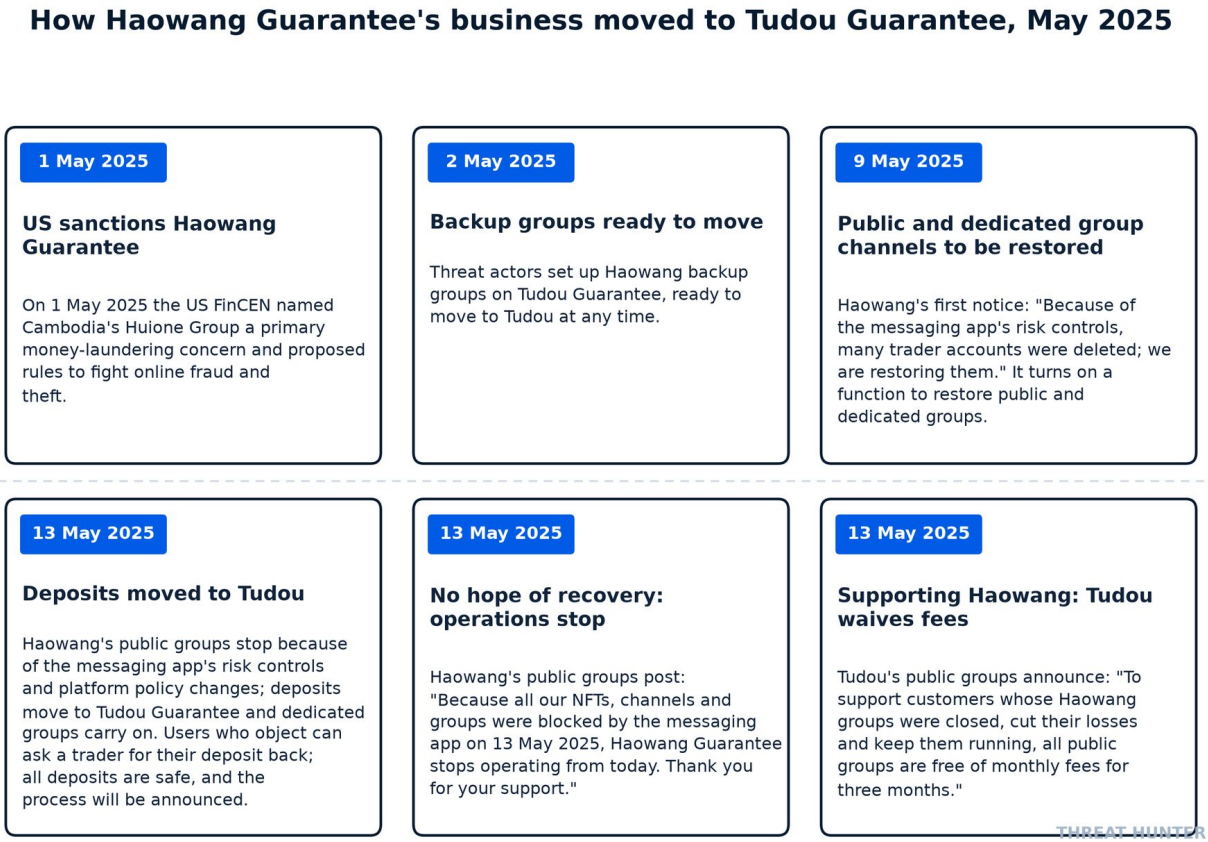


Data-leak incidents linked to guarantee platforms, July 2024–June 2025: Haowang Guarantee accounts for 74.26%

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

In May 2025, however, Haowang Guarantee suffered a major blow:

- On May 1, the US Financial Crimes Enforcement Network (FinCEN) named its parent group a "primary money laundering concern" and cut off its access to the international financial system. In early May, the messaging app then banned its trading groups and accounts.
- On May 9, Haowang announced that "a large number of trader accounts have been closed." Its operations collapsed, and its public trading groups stopped working entirely.

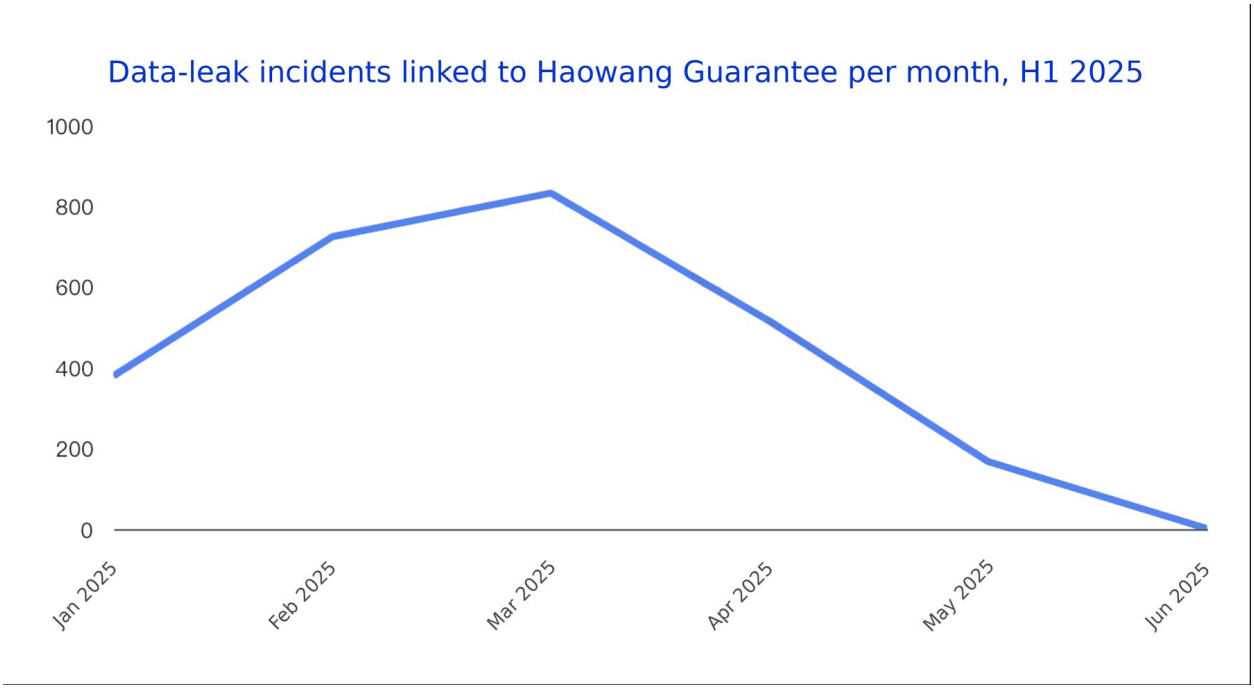


Timeline of Haowang Guarantee's collapse and the move of its business to Tudou Guarantee, May 2025

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

The timeline above shows how Haowang Guarantee collapsed and where its business went.

Threat Hunter's monitoring shows that after Haowang Guarantee went offline, the number of data-leak incidents linked to it fell from 832 in March to almost zero in June.

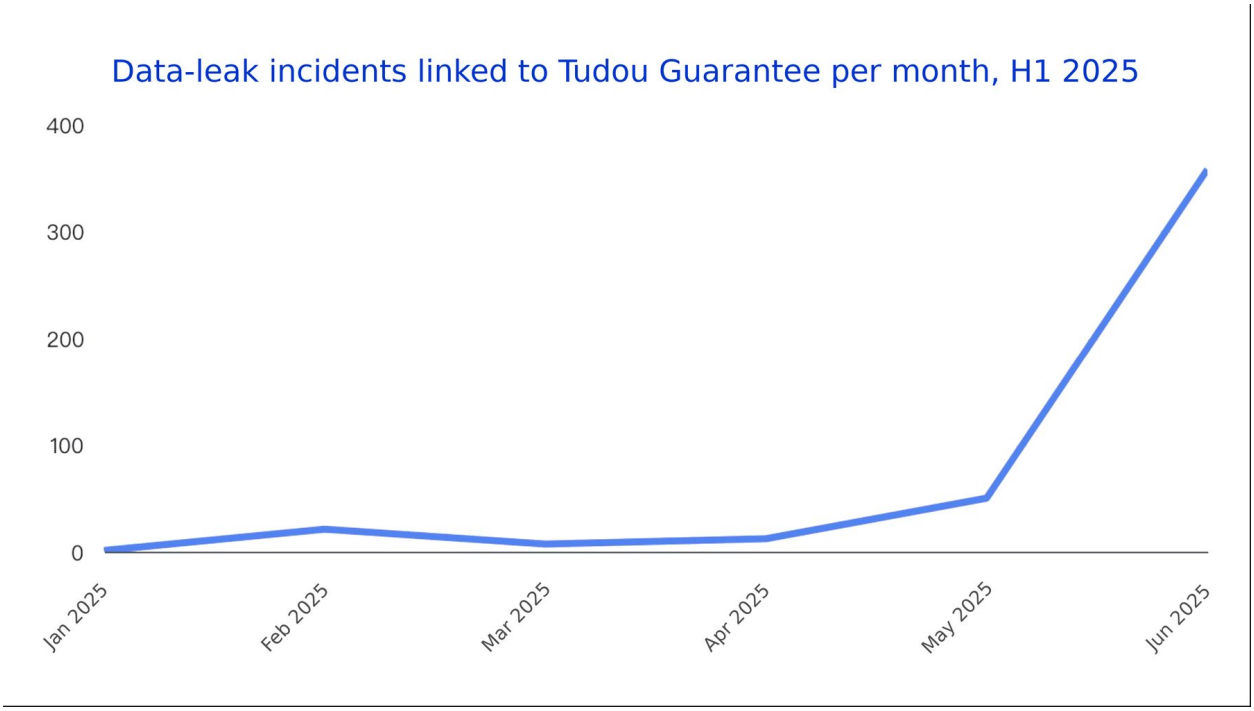


Data-leak incidents linked to Haowang Guarantee per month, H1 2025

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

Demand from threat actors did not go away. After Haowang Guarantee collapsed, new platforms such as "Tudou Guarantee" quickly emerged.

Data-leak incidents linked to Tudou Guarantee jumped from 12 in April to 358 in June, an increase of almost 30 times.



Data-leak incidents linked to Tudou Guarantee per month, H1 2025

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

In the illegal data-trading market, both supply and demand are very active. This strong demand has created a complete criminal trading chain. But the deals themselves carry high risk and uncertainty, so buyers and sellers find it hard to trust each other directly.

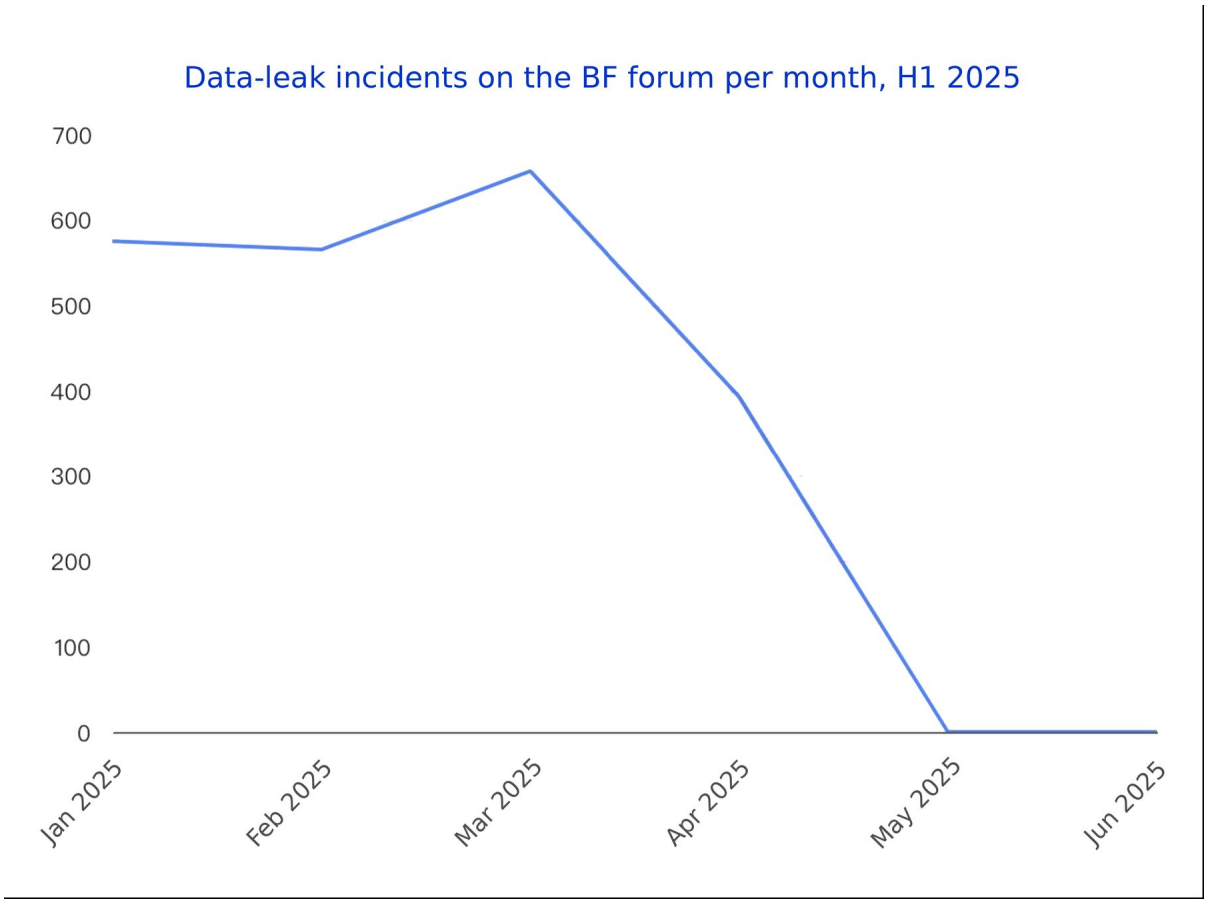
This is why "guarantee platforms" emerged as intermediaries in the criminal ecosystem. They do more than match buyers and sellers: they hold funds in escrow and settle disputes, which makes them a key support for the whole trade. Even when one platform is taken down, new intermediaries soon fill the gap under a different name. As long as the trade exists, there will be demand for these criminal service providers, and that makes them very hard to wipe out.

2.2 Criminal platforms can be shut down, but demand for data trading is hard to eliminate

2.2.1 A crackdown on the leading forum cut supply sharply; before the shutdown it supplied almost 15% of dark-web incidents

Criminal platforms face constant enforcement pressure, yet demand for data trading has not weakened. Take BF, a leading dark-web forum. In the first half of 2025 it was still one of the most important sources of leaked data in the world.

Threat Hunter's monitoring shows that dark-web channels accounted for 15,096 data-leak incidents from January to June 2025. BF contributed 2,190 of them, or 14.5% of all dark-web incidents. Its activity kept rising in the three months before the shutdown and peaked at 657 incidents in March 2025.



Data-leak incidents on the BF forum per month, H1 2025

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

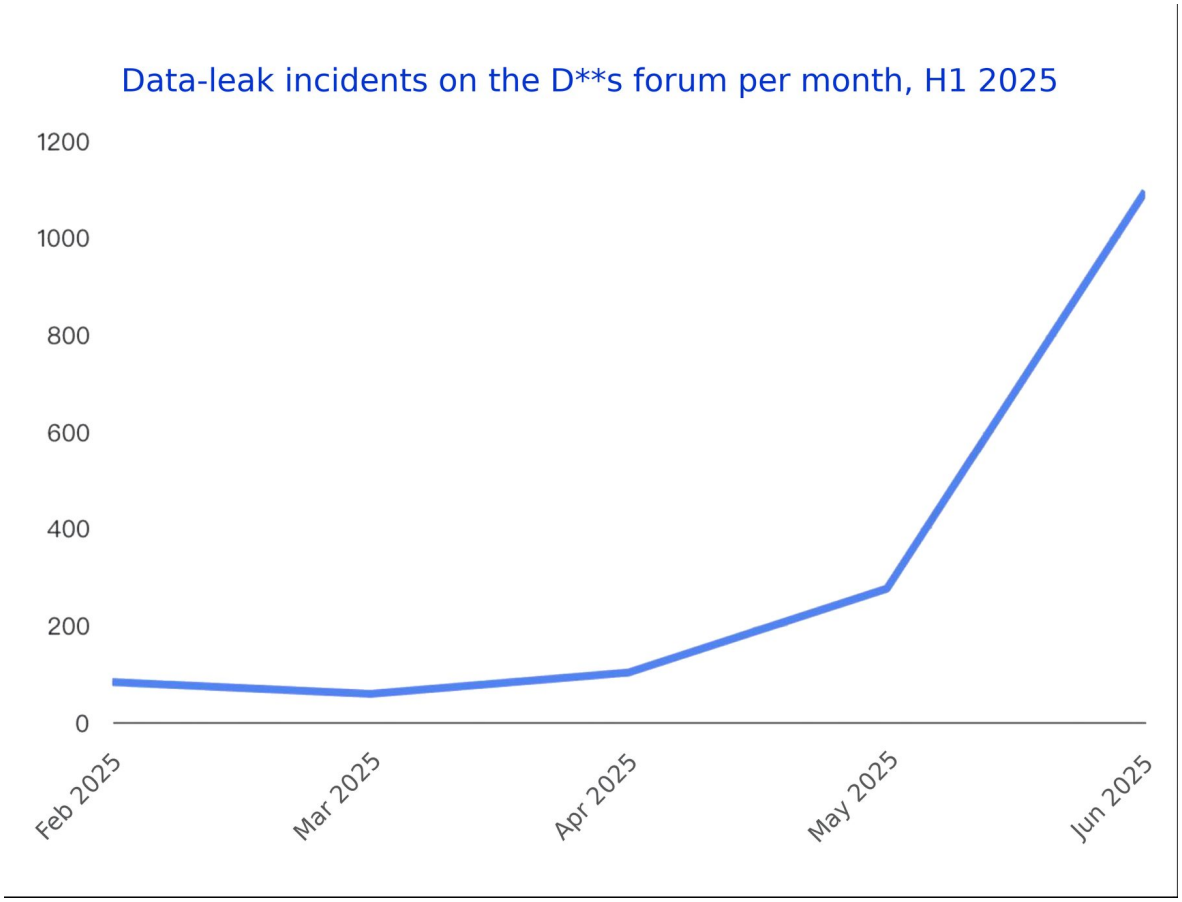
When BF was suddenly shut down on April 15, the number of related incidents fell quickly. Only 393 were recorded in April, a drop of 43.2% from March, and the number fell to zero in May. The platform's supply fell off a cliff.

2.2.2 After BF shut down, several other forums quickly took over

Even so, the shutdown did not reduce overall threat-actor activity. Users simply moved to other dark-web platforms and private messaging tools.

The platforms below, tracked by Threat Hunter, show this shift:

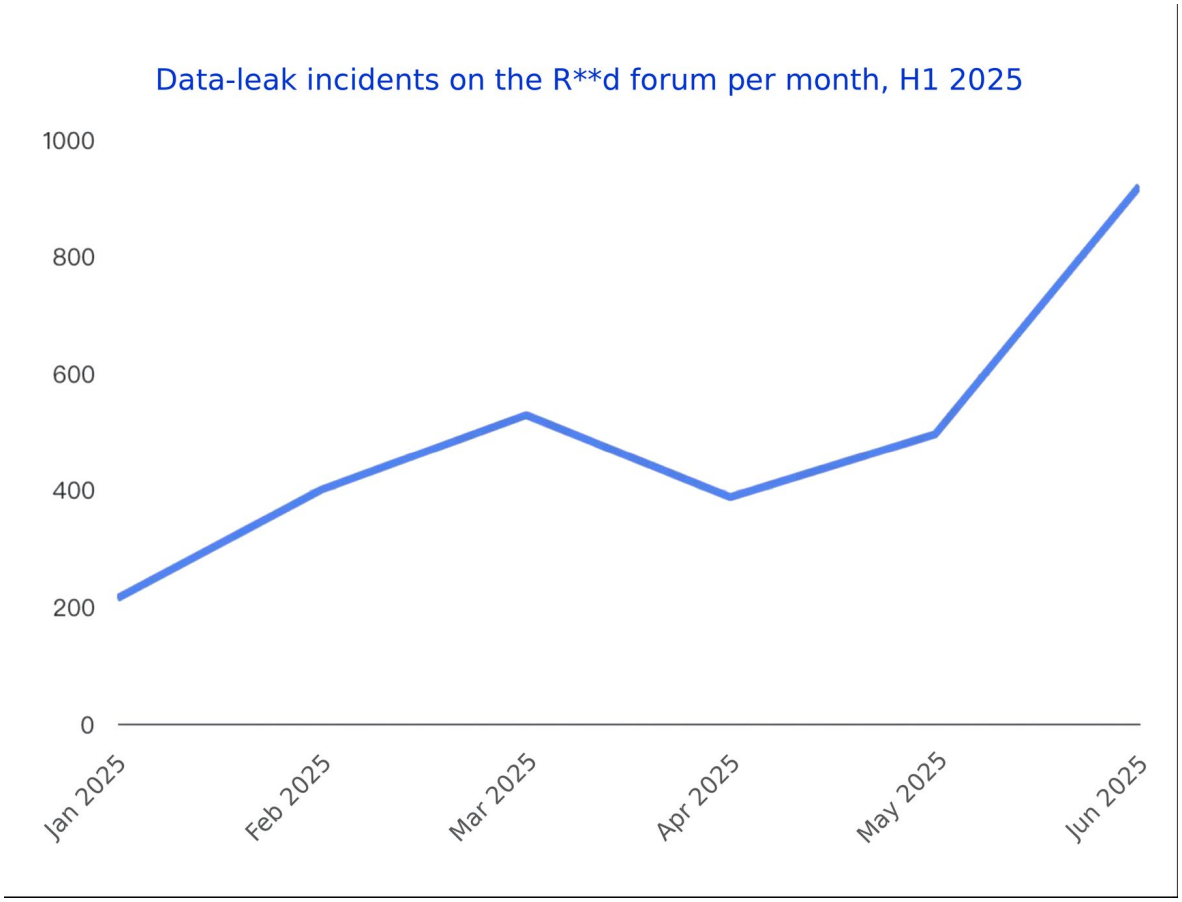
- D**s forum: incidents passed 100 in April, rose to 275 in May (up 374% from March) and jumped to 1,095 in June, almost 20 times the level before the shutdown.



Data-leak incidents on the Ds forum per month, H1 2025**

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

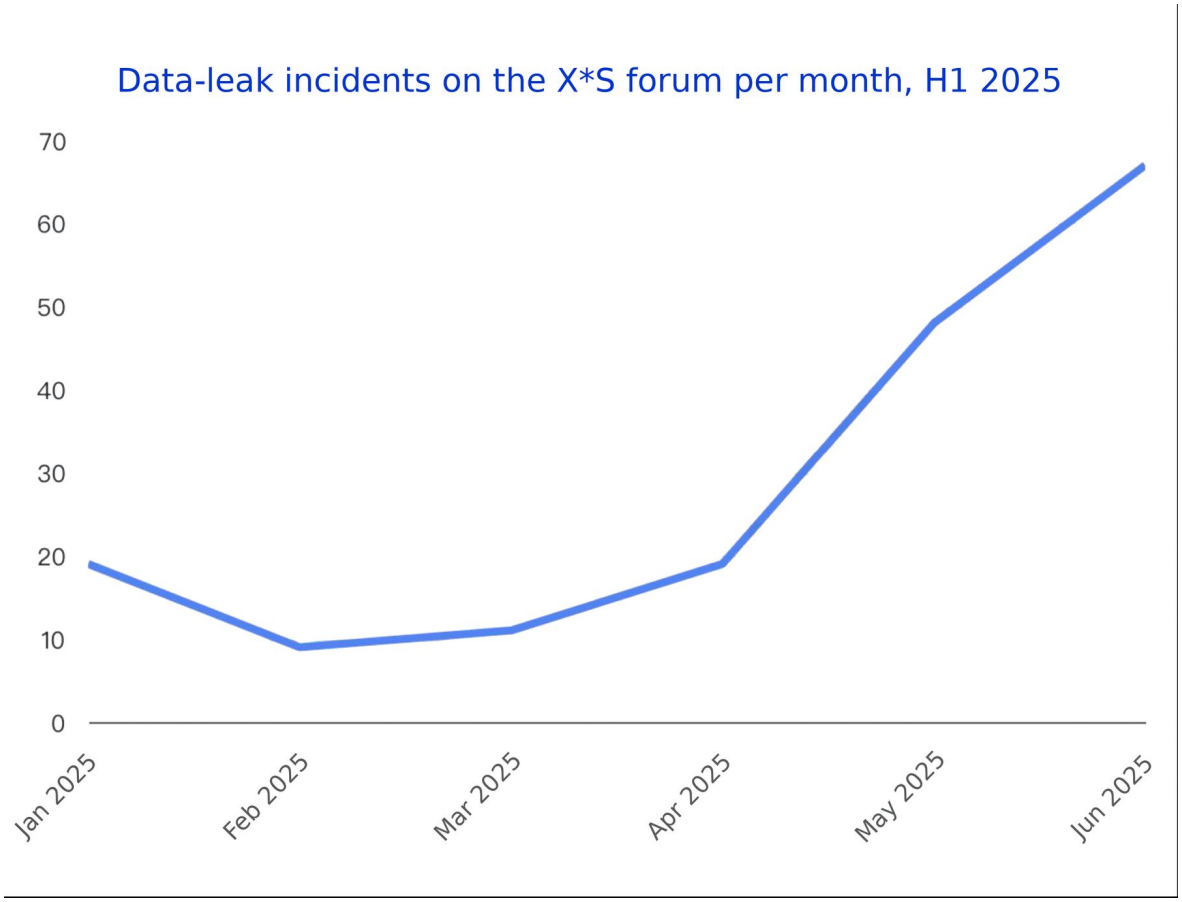
- R**d forum: after a short dip in April linked to the BF shutdown, activity rebounded strongly in May and June. June incidents were 138% higher than in April.



Data-leak incidents on the Rd forum per month, H1 2025**

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

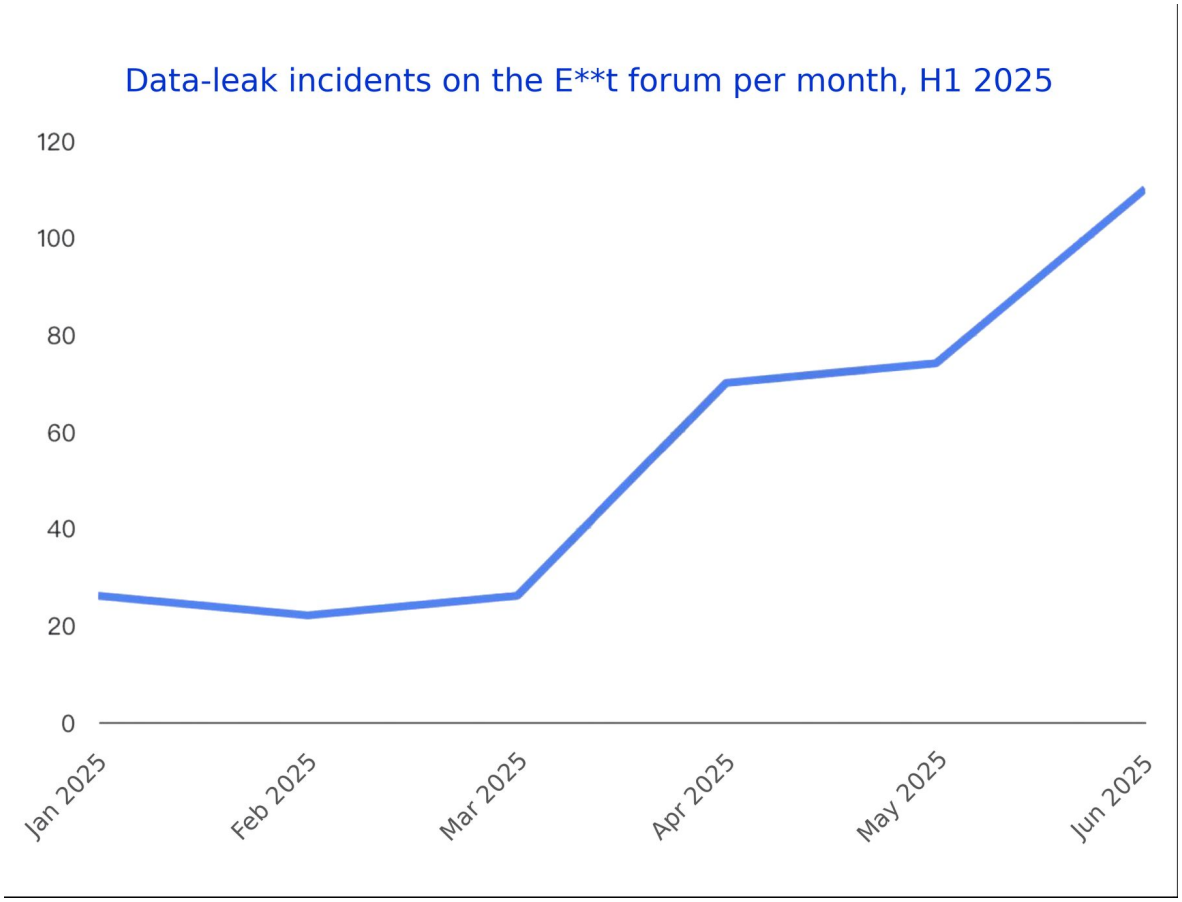
- X*S forum: activity had been very low, averaging only 13 data breaches a month from January to March. It rose to 48 in May and 67 in June, an increase of more than 400%.



Data-leak incidents on the X*S forum per month, H1 2025

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

- E**t forum: incidents rose to 70 in April (up 169% from March) and reached 110 in June, a steady upward trend.



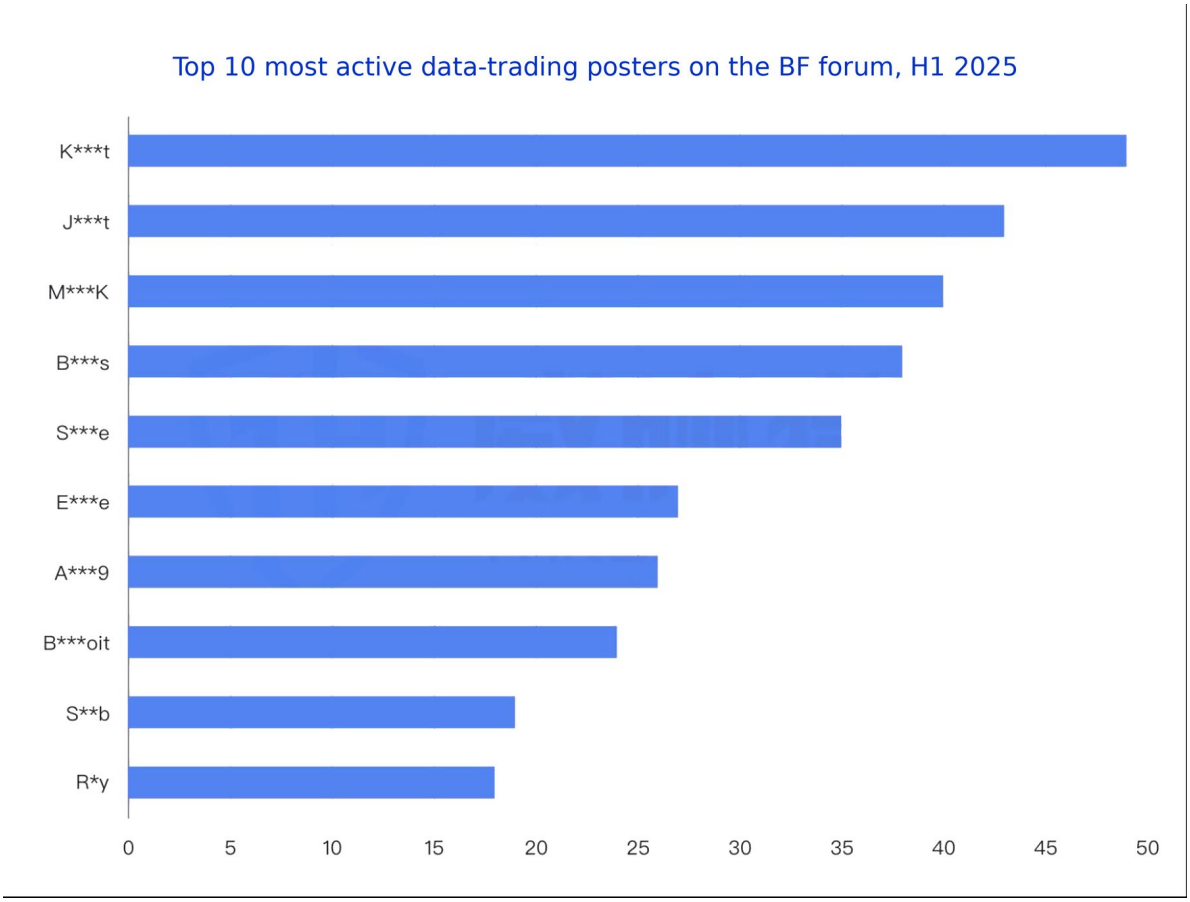
Data-leak incidents on the Et forum per month, H1 2025**

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

These figures show that the criminal ecosystem can repair itself quickly. When a platform is hit, its traffic, resources and participants soon regroup on new platforms, and market activity recovers fast.

2.2.3 BF's core users moved quickly, and threat-actor activity continued without a break

Threat Hunter found that BF's top ten posters, who accounted for 14.6% of the platform's incidents, moved to other platforms right after the shutdown and stayed active.



Top 10 most active data-trading posters on the BF forum, H1 2025 (names masked as in the original)

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

BF's most active user in the first half of the year, K***t, is a good example.

Since BF went offline, "K***t" has moved without interruption to the X*S forum and keeps posting user data from outside China, shopping orders, CRM system records and other data. The data covers many types, countries and industries.

The user posts often and in a consistent data format, which suggests strong data-cleaning and distribution skills. This is a typical professional data reseller who adapts easily to new black-market platforms and moves between them efficiently.

The trend shows that core threat actors are highly mobile and resilient. As long as there is demand for data, they can rebuild trading channels quickly and keep the underground market active.

The BF case confirms a basic rule of the cybercrime market: when a main trading platform is taken down, users and demand move quickly to existing or new alternatives. The data-trading market adapts well. Even if the leading platform is destroyed, threat actors can keep their business running through other channels.

Part 3 looks at new trends in the data-breach trading market in the first half of 2025.

3. New Trends in Data Breach Trading Market Research in the First Half of 2025

3.1 Data-leak risk and the criminal ecosystem around credit approval and risk checks

3.1.1 Leaks of "multi-lending" data on individuals grew more than sixfold from the second half of 2024

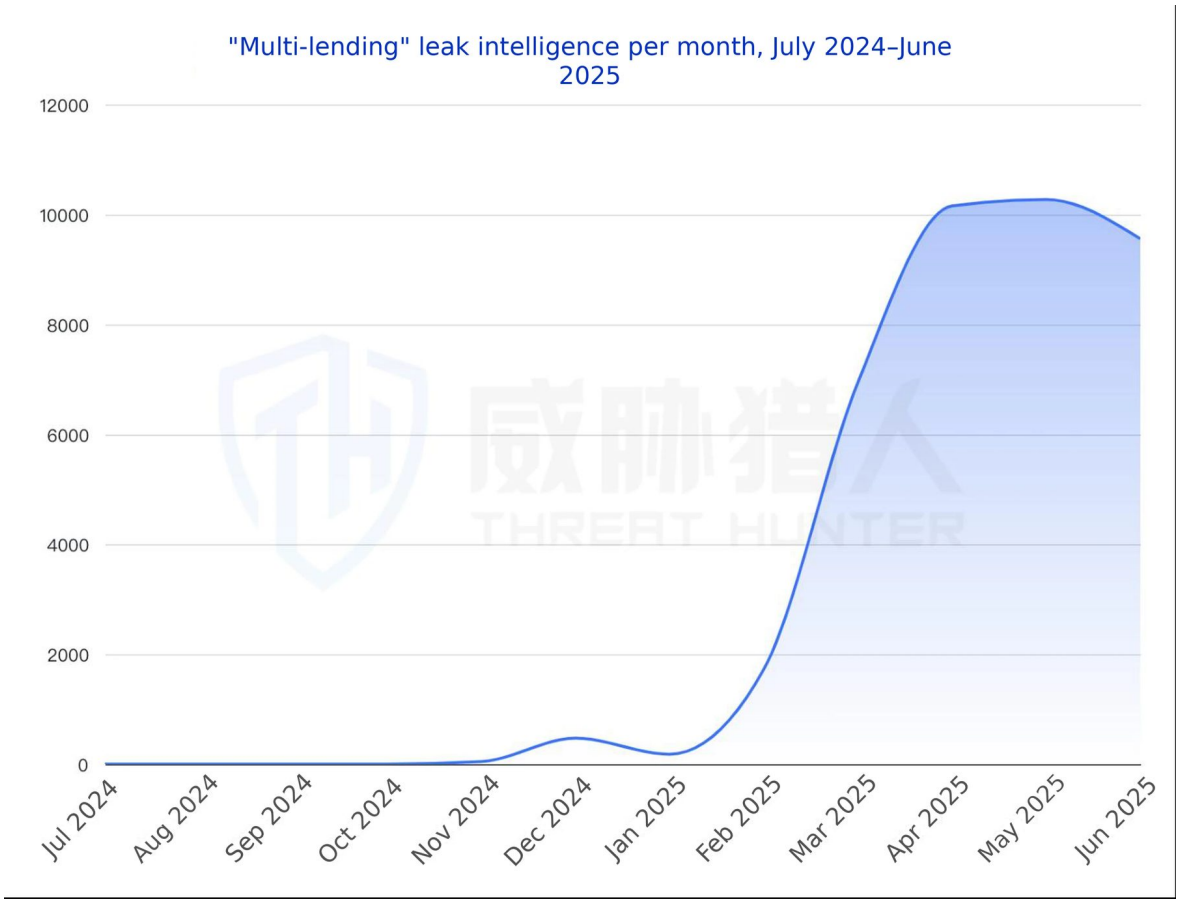
Threat Hunter recorded 117 leaks of a type of loan data known as "multi-lending" data, 101 more than in the second half of 2024, an increase of 631.25%.

Threat Hunter's intelligence on "multi-lending" credit risk shows that these leaks have been rising more or less steadily since November 2024.

Multi-lending: a risk-check mechanism that detects when a borrower borrows from several lenders at once. It is a data-sharing system set up by a third-party data provider and a group of online lenders. When a borrower applies for a loan at any of these lenders, the application itself is captured and recorded like a signal. In practice, "multi-lending data" means the records of a borrower's loans across several lenders.

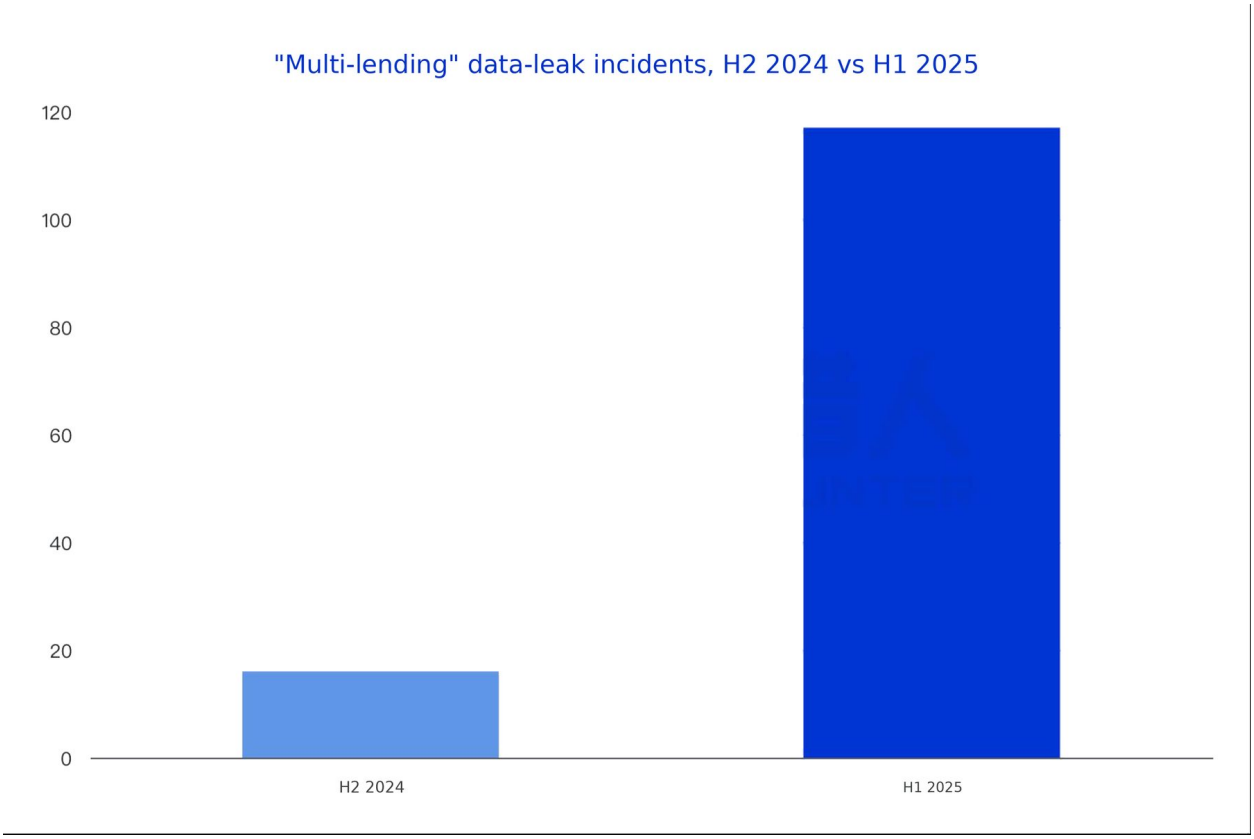
Data-leak intelligence: information that Threat Hunter collects from messaging-app groups, the dark web and other channels showing that sensitive personal or organizational information is being traded or used without authorization. It can include old or duplicate data and is often very large in volume.

Data-leak incidents: cases that Threat Hunter's security researchers confirm as valid after analyzing and checking samples of data-leak intelligence and removing old or fake data.



"Multi-lending" leak intelligence per month, July 2024–June 2025

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



"Multi-lending" data-leak incidents, H2 2024 vs H1 2025

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

Threat Hunter's analysis shows that what threat actors call "multi-lending" data mainly covers borrowers' repayment history and overdue records. This data plays a key role in credit risk checks because it shows whether a borrower is applying for or holding loans on several platforms. When it is misused, it can seriously distort lenders' decisions and risk assessments. It also exposes borrowers' private information and makes them targets for targeted marketing or fraud.



Leaked "multi-lending" sample captured by Threat Hunter: each borrower's repayment record

Source: Threat Hunter original report, page 26. Original image retained; numbered translations added by Threat Hunter.

Figure guide

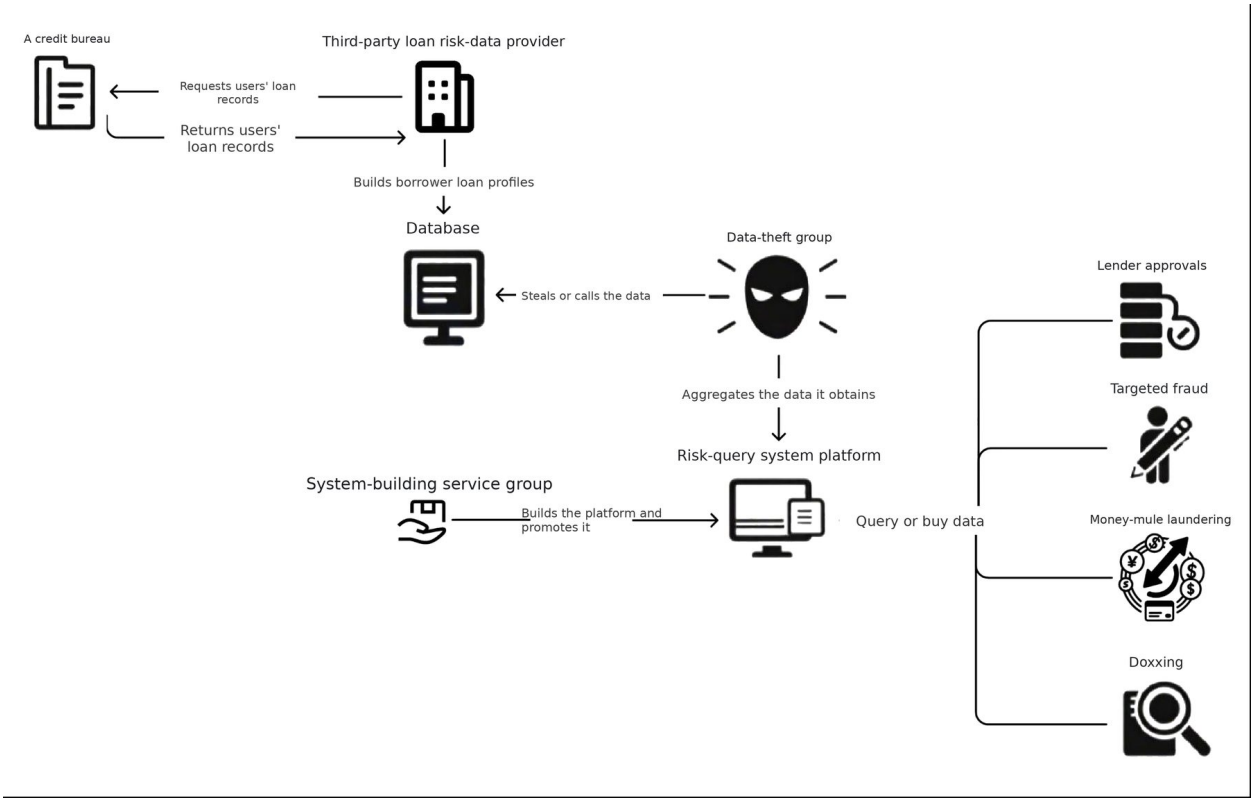
1	Column headers, left to right: name, ID number, phone 1, phone 2, "0: no data found", largest repaid amount, loans repaid, institutions currently overdue, dormant institutions, institutions currently repaying, latest repayment, institutions with abnormal repayment, largest overdue amount, longest overdue days, latest overdue date
2	One borrower per row; names, ID numbers, phone numbers and amounts are partly blurred in the original

The sample above, captured by Threat Hunter, includes borrowers' repayment information.

3.1.2 An underground credit-data supply chain has formed around loan records

Threat Hunter's investigation found that an underground supply chain has formed around loan record data. It covers a range of illegal activity: data theft, platform building, data sales, and targeted marketing and fraud downstream.

The supply chain is shown below.



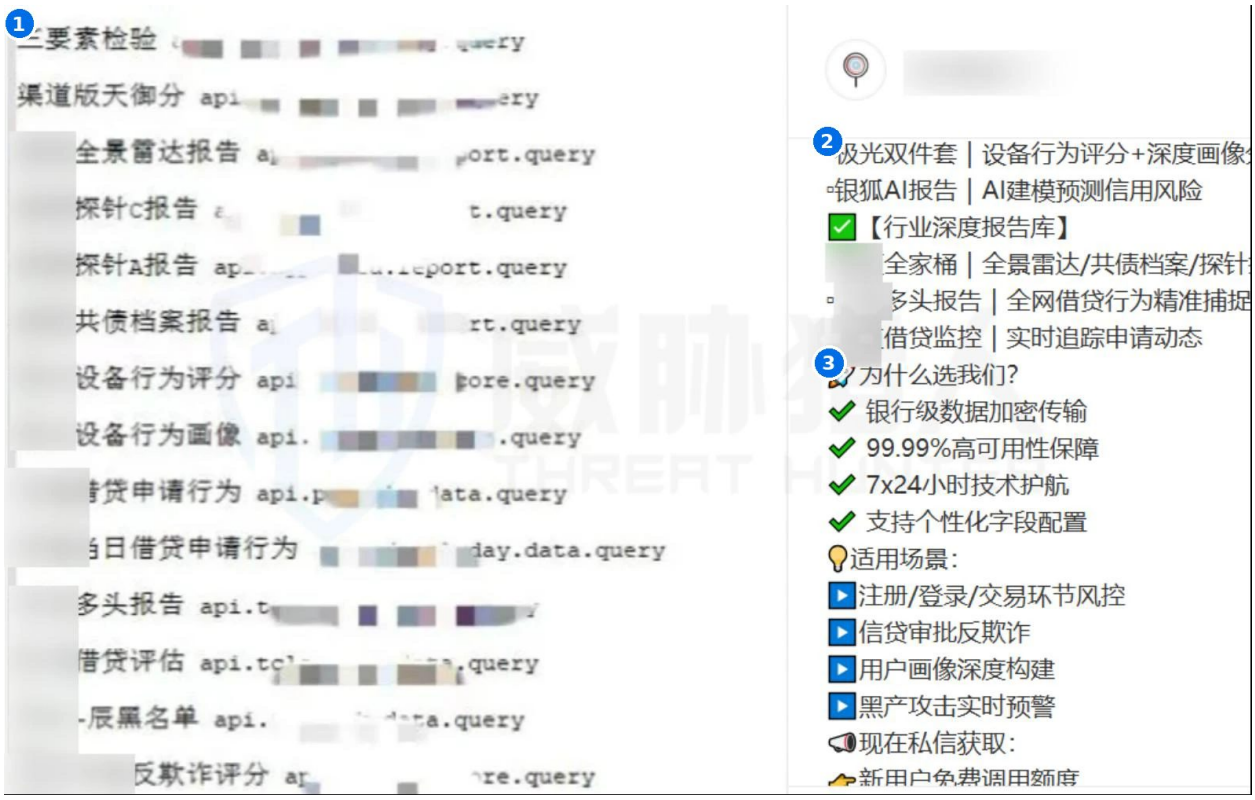
The underground credit risk-data chain: data theft, query platforms and downstream use

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

1. Upstream: the data comes mainly from credit bureaus and licensed third-party risk-data providers.

As noted above, the "multi-lending" data that threat actors trade mainly covers borrowers' repayment history and overdue records, which show whether a borrower is applying for or holding loans on several platforms. Misuse of this data distorts lenders' risk assessments and exposes borrowers to targeted marketing and fraud.

Threat Hunter also examined the risk-data query systems that threat actors offer. In every case, the user authorization letters involved the same domestic credit bureau.



A threat actor's ad for risk-data queries that cites a credit bureau and a third-party risk-data provider

Source: Threat Hunter original report, page 27. Original image retained; numbered translations added by Threat Hunter.

Figure guide

1	List of query APIs on offer (endpoints blurred): three-element check; channel-edition risk score; panoramic radar report; probe C report; probe A report; shared-debt file report; device behaviour score; device behaviour profile; loan-application behaviour; same-day loan-application behaviour; multi-lending report; lending assessment; blacklist; anti-fraud score
2	Ad copy: "Two-pack: device behaviour score plus in-depth profile"; "AI report: AI modelling predicts credit risk"; "Industry in-depth report library": "Full bundle: panoramic radar, shared-debt file, probe"; "Multi-lending report: captures lending behaviour across the whole network"; "Loan monitoring: tracks applications in real time"
3	"Why choose us?" Bank-grade encrypted data transfer; 99.99% availability; 24/7 technical support; customisable fields. "Use cases": risk checks at registration, login and transaction; credit approval and anti-fraud; in-depth user profiling; real-time alerts on threat-actor attacks. "Message us now: free query quota for new users"

The figure above shows a threat actor's ad that cites a credit bureau and a third-party risk-data provider.



A threat actor says the data comes from a licensed third-party data provider

Source: Threat Hunter original report, page 27. Original image retained; numbered translations added by Threat Hunter.

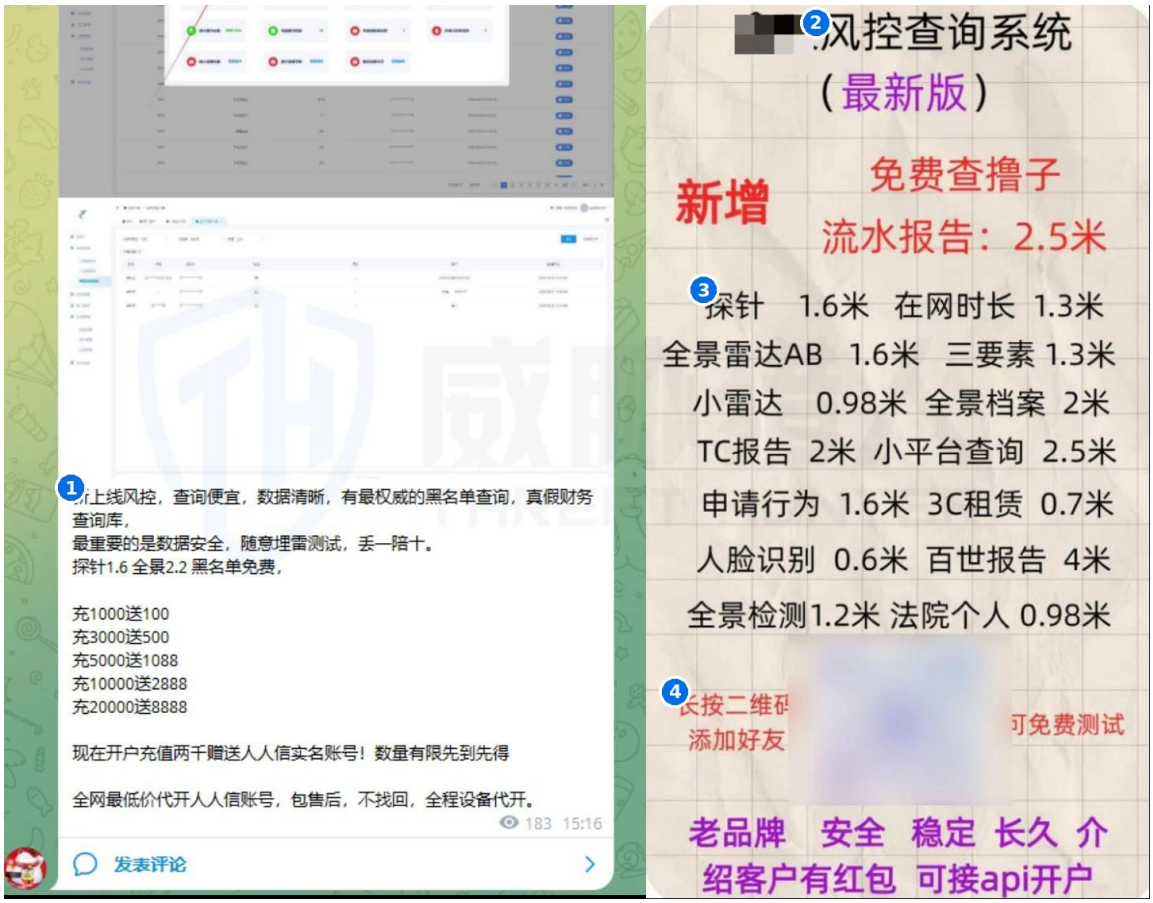
Figure guide

1	Chat message: "The company is the capable one: because they hold a licence, they can get the data volume"

In the figure above, a threat actor says the data comes from a licensed third-party data provider.

2. Midstream: a wave of risk-data query platforms and platform-building services

Threat Hunter found that demand for "multi-lending" data has led many threat actors to advertise risk-data query services or to sell data on borrowers with overdue loans directly. These services usually offer several query and verification functions, such as "multi-lending" checks and "three-factor verification" (name, ID number and phone number). Typical systems Threat Hunter observed include "Fu* risk-check query", "Yi* risk-check system" and "Xin* risk-check query system".



A threat actor's ad for a risk-data query system, with a price list per query

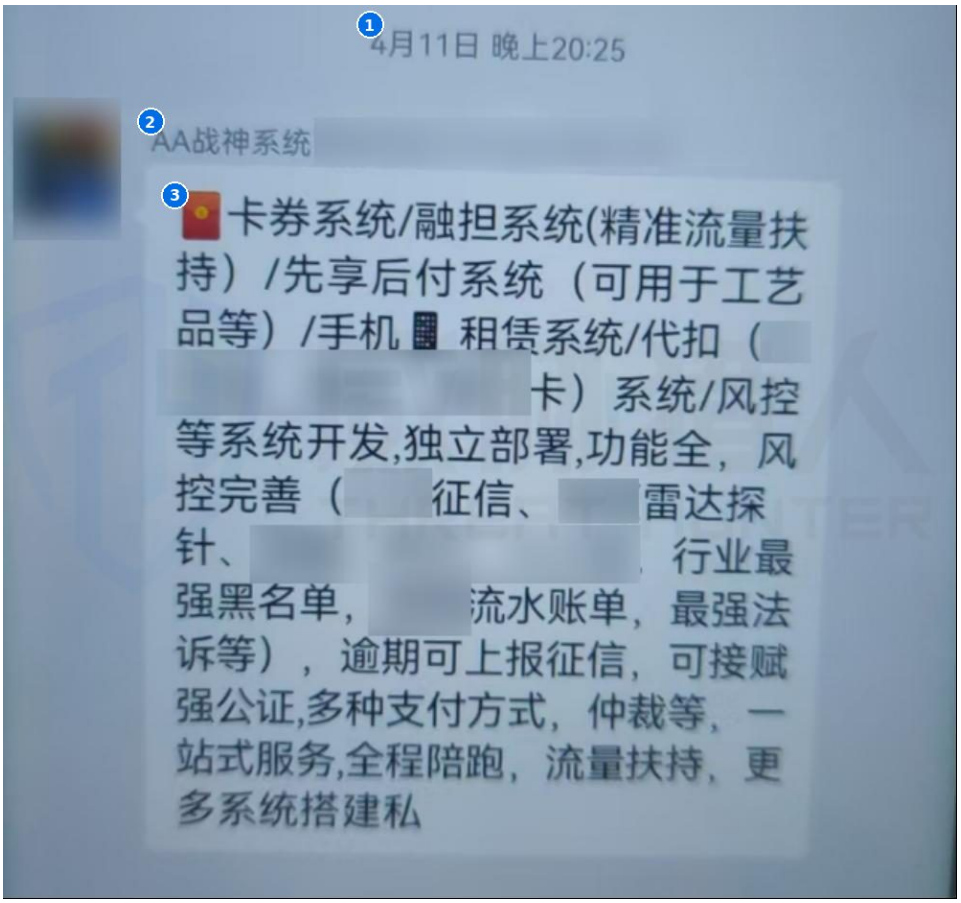
Source: Threat Hunter original report, page 28. Original image retained; numbered translations added by Threat Hunter.

Figure guide

1	Post: "Newly launched risk checks: cheap queries, clear data, the most authoritative blacklist lookup and a database to tell genuine lenders from fake ones. Most important is data security: plant test records at will; lose one, we pay ten. Probe 1.6, panoramic 2.2, blacklist free." Top-up bonuses from "top up 1,000, get 100" to "top up 20,000, get 8,888". Free real-name credit-platform accounts for top-ups of 2,000, and such accounts opened at "the lowest price online"
2	Ad: "[Redacted] risk-control query system (latest version)". "New: free check for borrowers who never repay"; "Bank-statement report: 2.5"
3	Price per query in CNY (written as "mi" in the slang): probe 1.6; time on network 1.3; panoramic radar AB 1.6; three-element check 1.3; mini radar 0.98; panoramic file 2; TC report 2; small-platform query 2.5; application behaviour 1.6; electronics rental 0.7; face recognition 0.6; another vendor's report 4; panoramic check 1.2; court records (individual) 0.98
4	"Long-press the QR code to add us"; "Free trial available"; "Established brand, safe, stable, long-term; referral bonuses; API accounts available"

The figure above shows a threat actor's ad for a risk-data query system.

Threat Hunter also found many threat actors on mainstream social platforms offering to help midstream and downstream groups build the platforms they need, such as "financing guarantee systems", "leasing systems", "risk-check systems", "credit inquiry systems" and "IOU inquiry systems". These offers usually promise full features and complete risk checks, "one-stop services" such as reporting overdue loans to credit bureaus and notarized enforcement of debts, plus "end-to-end support and traffic."



A threat actor's ad for building lending and risk-control platforms

Source: Threat Hunter original report, page 29. Original image retained; numbered translations added by Threat Hunter.

Figure guide

1	Timestamp: 11 April, 8:25 pm
2	Sender: "AA War God System" (rest blurred)
3	Message: "Development of voucher systems, financing-guarantee systems (with targeted traffic support), buy-now-pay-later systems (usable for handicrafts and the like), phone rental systems, direct-debit card systems, risk-control systems and more; deployed independently, full features, complete risk checks (credit reports, radar probe, the industry's strongest blacklist, bank statements, strongest litigation and more; parts blurred). Overdue loans can be reported to the credit bureau; enforceable notarisation, several payment methods, arbitration and more. One-stop service, support from start to finish, traffic support; more systems built privately"

The figure above shows a criminal group's ad for platform-building services.

3. Downstream: fuel for targeted marketing, fraud, money laundering and other crime

Threat Hunter found that the people who buy and use these loan records fall mainly into the following groups:

1. Lending staff: mainly loan approvers at small and mid-sized lending platforms, who use the illegal data to check applicants' credit standing.

They use it to complete approvals or to pick out target customers for targeted marketing.

2. "Score runners": mainly money launderers. After obtaining the data, they win the trust of the people in it and use their bank cards to move illegal funds.

This practice is known as "score running".

3. Fraudsters: they run "fish-killing" (also called "shark") scams, mainly through telecom fraud such as loan scams and impersonation of police, prosecutors and courts.

They use the illegally obtained data to target victims precisely and raise their success rate.

4. File checkers: in the data-trading market, some services look up an individual's credit status on request, a form of doxxing.

The checker submits the person's name, ID number and phone number to an upstream data query and receives the matching credit report.



Left: a threat actor says the data suits money laundering and fraud. Right: a query service that returns personal credit reports

Source: Threat Hunter original report, page 30. Original image retained; numbered translations added by Threat Hunter.

Figure guide

1	Left: post in a "[redacted] guaranteed-trading category group" (channel owner), with a blurred spreadsheet of loan records
2	Post text: "Real-time IOU and probe data"; boxed in red: "Suits lenders, money mules, card fraud and 'shark' scams perfectly"; "Limited quantity; order early"; "Contact the bot". Edited 13:04
3	Right: file "Credit report template.pdf" (360.2 KB); "[Credit report] notice, notice, notice: 45 U" (45 USDT)
4	"Name, ID number and phone must all match to place an order. Checks online-lending big data plus civil judgements; does not show debts, but shows litigation and loan-application records. Stable same-day results; orders taken at the source." 150 views, 20:34

In the figure above, the left image shows a midstream threat actor saying the data suits money laundering and fraud, and the right image shows the output of a personal credit report query.

Appendix: Definitions of related slang words

Threat Hunter has researched and tracked intelligence related to "multi-lending" data in depth. The terms below are common slang among the threat actors involved. Finance (also "cw"): staff of loan-shark or private-lending platforms.

Rongdan (also written "RD"): a family of small online lending platforms, mostly small or micro lending apps with a simple application process and a high approval rate. "Rongdan data" means user data from these small lending platforms.

IOU (also "JT"): loan-shark or private loans for which the borrower signs a paper or electronic IOU. "IOU data" means user data from these signed IOUs.

"Anti-aircraft guns": loan-shark platforms or lenders. "Anti-aircraft gun data" means user data from people who borrowed on these platforms.

Device rental: renting devices in installments on rental platforms, often followed by cashing out. "Rental data" means user data from installment deals on these platforms.

Gold: short for "gold mall", small platforms that let users buy gold and pay in installments, much like device rental cash-outs. "Gold mall data" means user data from cash-outs on these platforms.

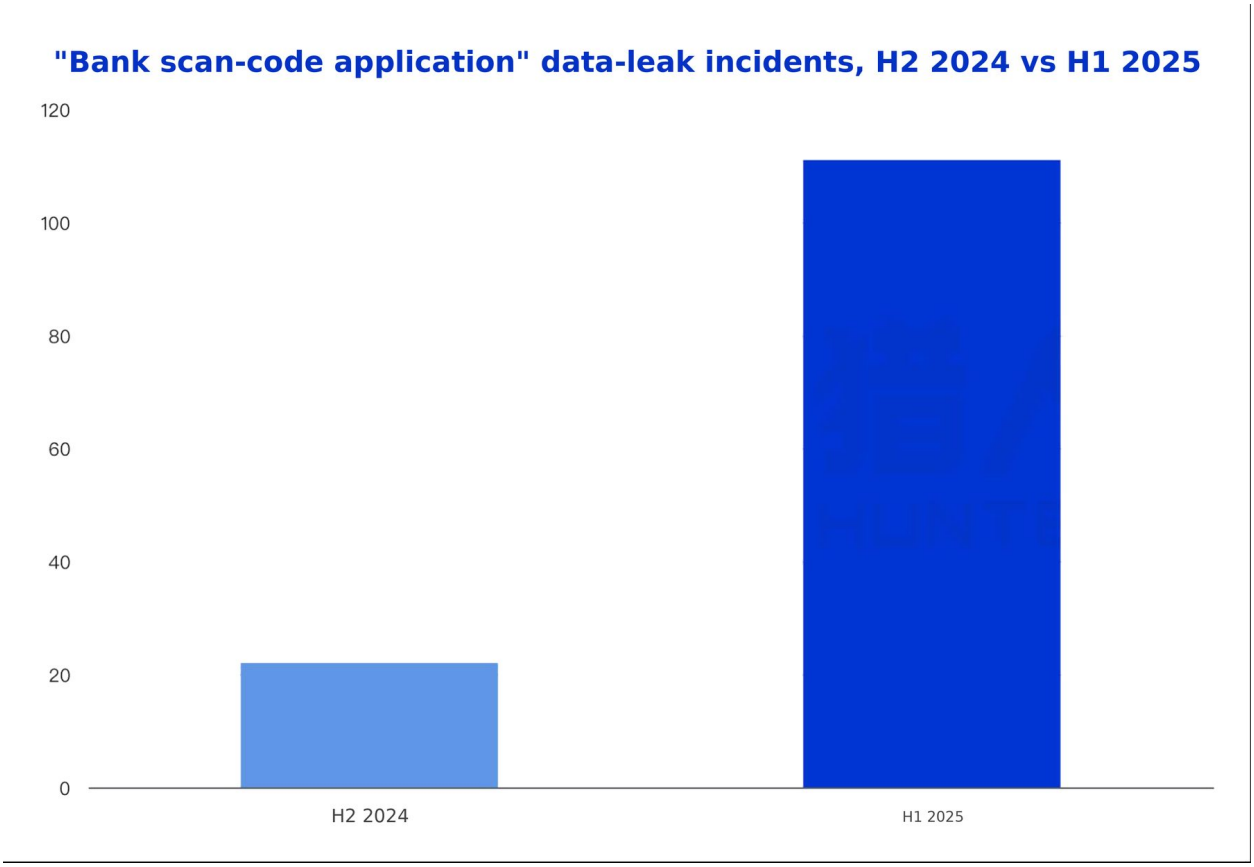
E-cards and vouchers: like device rental and gold malls, small platforms that sell e-cards, vouchers or gift balances on installment. "E-card data" means user data from cash-out purchases on these platforms.

3.2 Leaks of bank "scan-code application" loan data: trends and the ecosystem behind them

3.2.1 Leaks of bank "scan-code application" loan data grew more than fourfold from the second half of 2024

Threat Hunter's ongoing monitoring found another type of loan-data leak in the first half of 2025, known as "bank scan-code application data". There were 111 such incidents, 89 more than in the second half of 2024, an increase of 404.55%.

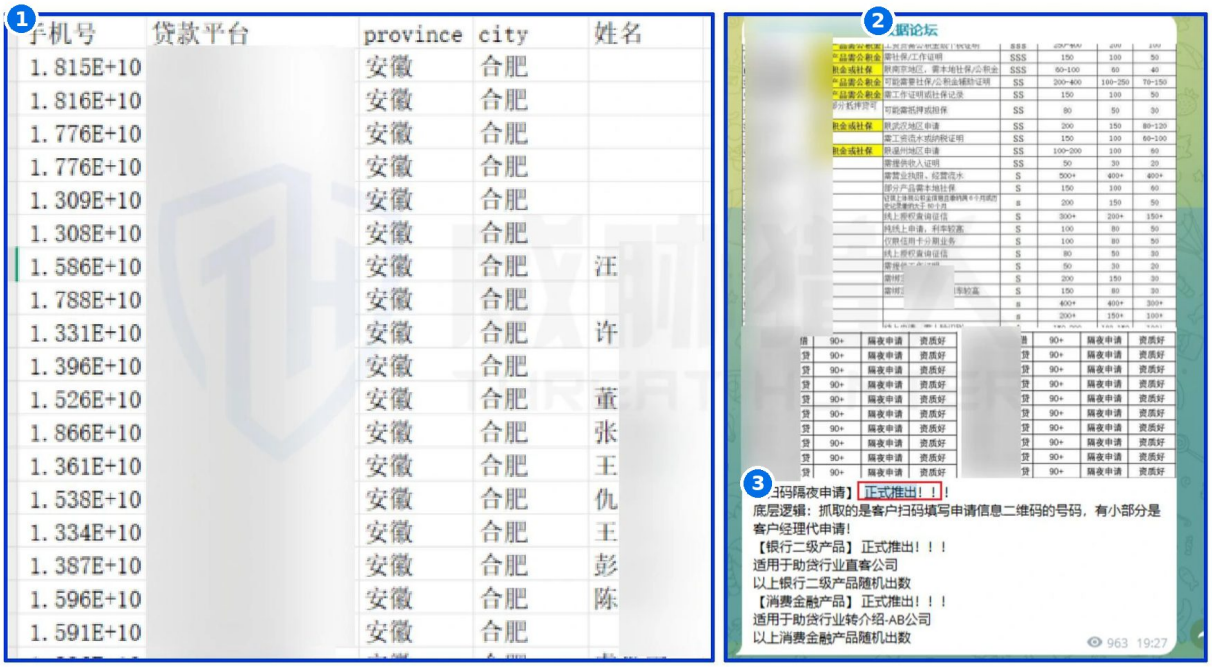
Bank scan-code application: data generated when a customer applies for a loan by scanning a loan-campaign QR code given to them by a bank account manager.



"Bank scan-code application" data-leak incidents, H2 2024 vs H1 2025

Source: Threat Hunter original report, page 32. Original figure with Chinese text replaced by English.

Threat Hunter's analysis shows that what threat actors call "overnight scan-code application" data relates mainly to bank loans. It includes the borrower's phone number, city or region and the result of the loan application. Lists of bank loan platforms provided by threat actors cover more than 80 banks, most of them local or commercial banks.



Left: format of the leaked data. Right: a threat actor launches an "overnight scan-code application" data product

Source: Threat Hunter original report, page 32. Original image retained; numbered translations added by Threat Hunter.

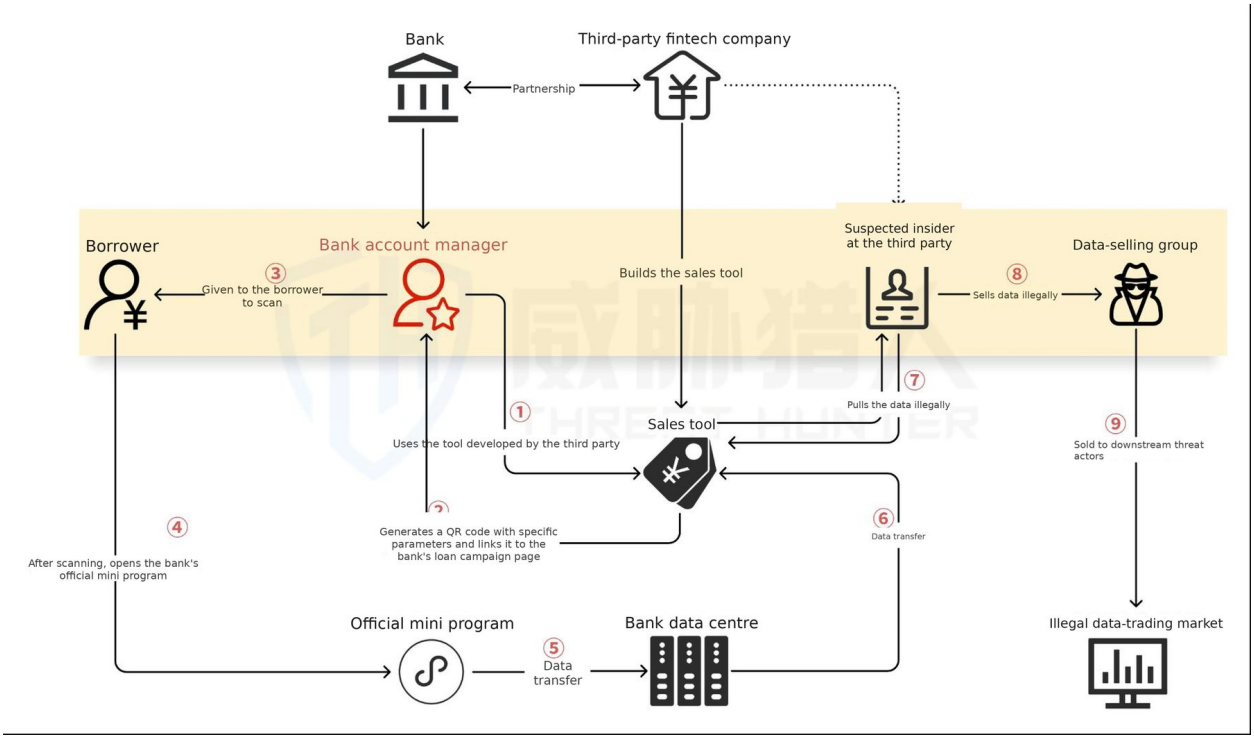
Figure guide

1	Left: format of the leaked data. Columns: phone number, lending platform (blurred), province, city, name. Rows read province "Anhui", city "Hefei"; surnames visible, the rest blurred
2	Right: post in a "[redacted] data forum" channel, listing overnight-application platforms (see the next figure) and rows marked "Overnight application" and "Good credit profile"
3	"[Scan-code overnight applications] officially launched!!! (boxed in red) How it works: we capture the phone numbers of customers who scan the QR code to fill in an application; a small share are filed by account managers on customers' behalf. [Bank second-tier products] officially launched!!! For direct-client loan brokers; numbers from these banks are released at random. [Consumer-finance products] officially launched!! For brokers' referral firms; numbers from these products are released at random." 963 views, 19:27

In the figure above, the left image shows the format of the leaked data, and the right image shows threat actors launching an "overnight scan-code application" data product.

3.2.2 Bank "scan-code application" leaks: a fintech marketing tool is the core risk, affecting more than 80 banks

Threat Hunter traced the bank QR codes in the leaked data and found that all of them pointed to the same "xx Marketing Assistant" platform, built by a well-known fintech service provider. Based on the list of bank loan platforms that threat actors published, more than 80 banks are affected.



How bank loan-application data leaks: from the account manager's QR code to the illegal data-trading market

Source: Threat Hunter original report, page 33. Original figure with Chinese text replaced by English.

The flow chart above shows how bank loan-application data leaks.

Because the incidents involve many banks, Threat Hunter reconstructed the process in detail:

1. To apply for a loan, the customer scans a loan-campaign QR code provided by a bank account manager.

2. The QR code carries the account manager's details and opens the bank's official mini program.

3. The customer then chooses a loan product in the mini program and submits an application.

Threat Hunter learned that the account managers' loan QR codes were in fact generated with a sales tool built by a third-party fintech company. (The tool's pages are sensitive, so they are not shown here.)

Threat Hunter's analysis of this fintech company found that it not only builds application software for banks but also supplies smart risk-check strategies, which set different follow-up approaches for borrowers with different credit profiles to support bank account managers. Its main role is to digitize bank operations and grow their lending business. After a customer applies in the bank's official mini program, the bank syncs the customer's details to the sales tool so that account managers can track performance and follow up. This sync also creates a data-leak risk.



台名称	是否需要公积金	其他材料/备注	推荐级别	每日出量（三网）不固定 预计出量 一线及高配二线	二线	三线及以下
	部分产品需公积金	本地户籍优先	SSS	200左右-300	100-200	40-100
	否	需银行流水或工资证明	SSS	200左右-300	100-200	40-100
	部分产品需公积金	需公积金或个税证明	sss	250-400	200	100
	部分产品需公积金	需社保/工作证明	SSS	150	100	50
	需公积金或社保	限南京地区，需本地社保/公积金	SSS	60-100	60	40
	部分产品需公积金	可能需要社保/公积金辅助证明	SS	200-400	100-250	70-150
	部分产品需公积金	需工作证明或社保记录	SS	150	100	50
	否（部分抵押贷可能需）	可能需抵押或担保	SS	80	50	30
	需公积金或社保	限武汉地区申请	SS	200	150	80-120
	否	需工资流水或纳税证明	SS	150	100	60-100
	需公积金或社保	限温州地区申请	SS	100-200	100	60
	否	需提供收入证明	SS	50	30	20
	否	需营业执照、经营流水	S	500+	400+	400+
	否	部分产品需本地社保	S	150	100	60
	需要	征信上体现公积金信息且缴纳满 6 个月或历史记录缴纳大于 60 个月	s	200	150	50
	否	线上授权查询征信	S	300+	200+	150+
	否	纯线上申请，利率较高	S	100	80	50
	否	仅限信用卡分期业务	S	100	80	50
	否	线上授权查询征信	S	80	50	30
	否	需提供工作证明	S	50	30	20
	否	需绑定 银行卡	S	200	150	30
	否	需绑定 账户，利率较高	S	150	80	30
	否		s	400+	400+	300+
	否		s	200+	150+	100+
	否	线上申请，需人脸识别	A	150-200	100-150	100+
	否	需提供银行流水	A	150-200	100	80
	否	需授权查询征信	A	100	80	30
	否（抵押贷可能需）	可能需房产/车辆抵押	A	80	50	20
	否	线上申请，需人脸识别	A	100	70	30

A threat actor's list of required materials for each bank loan platform, with expected data volumes by city tier

Source: Threat Hunter original report, page 34. Original image retained; numbered translations added by Threat Hunter.

Figure guide

1	Title: "Recommended platforms for overnight applications"; top right: "Daily volume (all three carriers) varies; expected volume"
2	Columns: platform name (blurred); housing provident fund required?; other materials and notes; recommendation grade (SSS, SS, S, A); expected volume in tier-1 and high-end tier-2 cities, in tier-2 cities, and in tier-3 cities and below
3	Fund column: "Some products require the housing provident fund" or "Fund or social insurance required" (highlighted in yellow); otherwise "No", "Yes" or "No (some secured loans may require it)"
4	Notes include: local household registration preferred; bank statements or payslips required; Nanjing, Wuhan or Wenzhou applicants only; proof of income; business licence and business statements; credit report authorised online; fully online application with higher interest; credit-card instalments only; face recognition required; property or vehicle collateral may be required
5	Volumes per platform, for example "about 200–300", "100–200" or "500+"

The figure above shows threat actors listing the materials needed to apply on different bank loan platforms and how data volumes differ by platform, city and region.

In short, every application submitted in a bank's mini program is copied to the third-party sales tool for account managers to track and follow up, and that copy is where the leak risk arises.

When threat actors first advertised this data, they claimed it came from an insider. Because more than 80 banks are involved, a leak by staff at all of these banks is very unlikely. Threat Hunter's initial assessment is that the leak came from staff at the third-party fintech company.



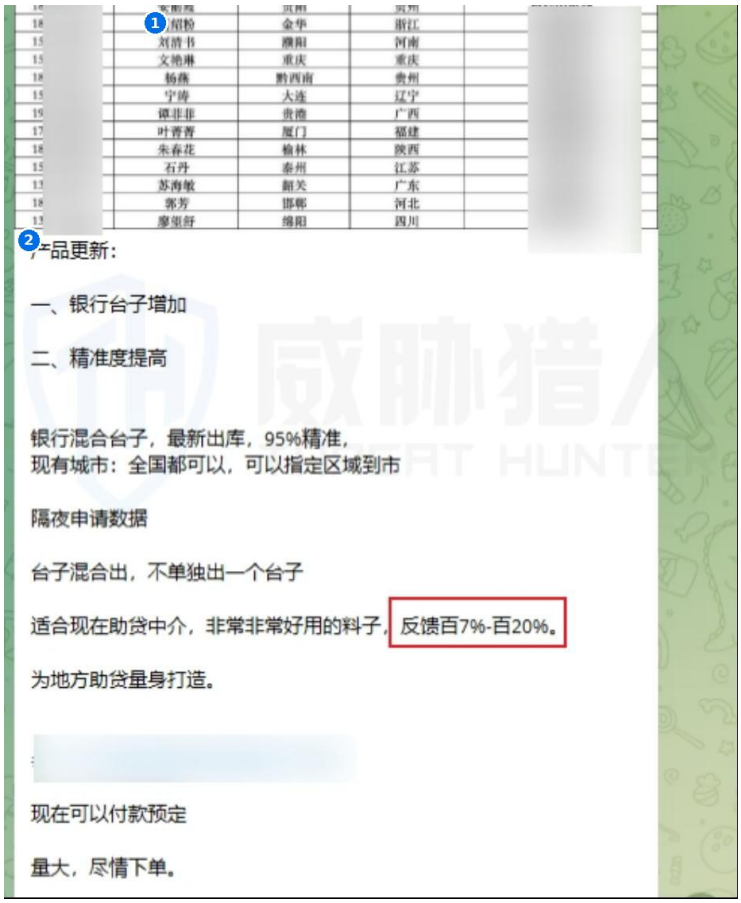
Threat actors trade leaked bank scan-code application data and say it comes from an insider

Source: Threat Hunter original report, page 35. Original image retained; numbered translations added by Threat Hunter.

Figure guide

1	Group header: "[blurred] SDK/DPI/online loans/withdrawal/loans..."; "[Source] customer applications / verified by account managers" (boxed in red)
2	Left chat: "Feedback is great"; "This batch is amazing"; "[blurred] products are always top quality"; "Do not sell these to anyone else for now, dear"; "Shame there is so little volume"; "Tell me when you have more; I will take all of Zhengzhou"
3	Middle chat: a file "12.11 Shanghai within the month 845.xlsx"; "305-800*0.4=-15"; "None left"; "Keep finding them for me"; "When will there be more?"; "Waiting to see whether the insider can still get any out" (boxed); "I love insiders the most; if you get any, tell me any time" (boxed)
4	Caption under the chat: "Feedback on [blurred] applications is good; go for it, but volume is limited"
5	Right: rows of "[bank] scan-code application" records from Suzhou, with phone numbers partly blurred
6	Product post: "[Source] customer applications / verified by account managers. [Threshold] state-owned firms, public institutions, listed companies, civil servants, enterprises. [Format] specified region / name / phone / time. [Region] nationwide. [Delivery] accuracy guaranteed, with after-sales support. Data source: customers scan the code online or offline to apply; account managers visit to verify the customer; application approved or rejected. Delivery time: the insider tabulates by hand, so it is a little slower (boxed); minimum 1,000. Genuine data, good feedback, use with confidence"

Threat Hunter's research shows that once this data reaches the illegal data-trading market, it is used mainly by loan brokers for targeted marketing. Threat actors report that it works very well, with success rates of up to 20%, which also indicates that the data is genuine.



A threat actor's product update: mixed bank data, said to be 95% accurate, with 7%–20% conversion feedback

Source: Threat Hunter original report, page 35. Original image retained; numbered translations added by Threat Hunter.

Figure guide

1	Top: list of names, cities and provinces (for example Jinhua, Zhejiang; Chongqing; Dalian, Liaoning; Mianyang, Sichuan); phone numbers blurred
2	Post: "Product update: 1. More bank sources. 2. Higher accuracy. Mixed bank data, fresh out of stock, 95% accurate. Cities: anywhere in the country, and can be narrowed to a city. Overnight application data. Sources mixed, not one source alone. Ideal for today's loan brokers; very, very useful data; conversion feedback 7%–20% (boxed in red). Tailored for local loan brokering. Payment and pre-orders now open. Large volumes; order as much as you like."

Risks and impact:

Customer loss and lost revenue: high-intent customers are contacted by competitors (loan brokers) the day after they apply and offered cheaper or faster alternatives. The bank loses potential customers along with the interest and fee income it could have expected.

Damage to reputation: the leaks badly undermine customers' trust in the bank's ability to protect data, especially in lending, a core business, and will harm the bank's brand over the long term. Regulatory risk: these incidents amount to serious leaks of personal financial information and violate the Personal Information Protection Law and other regulations. As data handlers, banks face heavy fines and regulatory action.

Part 4 describes Threat Hunter's data-leak risk intelligence service.

4. Threat Hunter data leakage risk intelligence service

In summary, data-leak risk remained severe in the first half of 2025. Incident volume stayed high, the criminal supply chain is mature and can repair itself, and shutting down platforms does little to curb market activity.

To meet this threat, organizations need to strengthen how they identify and respond to risk. That means understanding each incident in detail: verifying whether a risk is real, tracing its source quickly, getting leaked data taken down, following up on related risks, and making data-leak monitoring and early warning more timely.

Threat Hunter offers targeted solutions for these needs.

Threat Hunter's data-leak risk monitoring service monitors and mines intelligence from many channels across the internet in real time. Using its risk authenticity verification engine and manual data checks, it provides 24/7 real-time warnings of data-leak risks and links them to emergency response to keep harm and losses to a minimum.

1. Internet-wide intelligence monitoring and mining: coverage of the dark web, anonymous group chats, file-sharing and document sites, code-hosting platforms and other channels.

Coverage keeps expanding across several dimensions, including continuous discovery of new channels, dedicated mining of deep intelligence sources ("Deep Source"), and multilingual channel coverage.

2. Precise early warning of data-leak risks: for threat-actor trading data that is detected, the risk authenticity verification engine and manual data checks work together.

Together they produce an overall credibility assessment that helps organizations see risks clearly and act on them quickly.

(1) Risk authenticity verification engine: checks whether a risk is real based on three factors: source confidence, three-factor match rate and overlap with historical data.

(2) Manual data verification service: secondary checks, active verification and other methods help organizations judge risks more precisely.

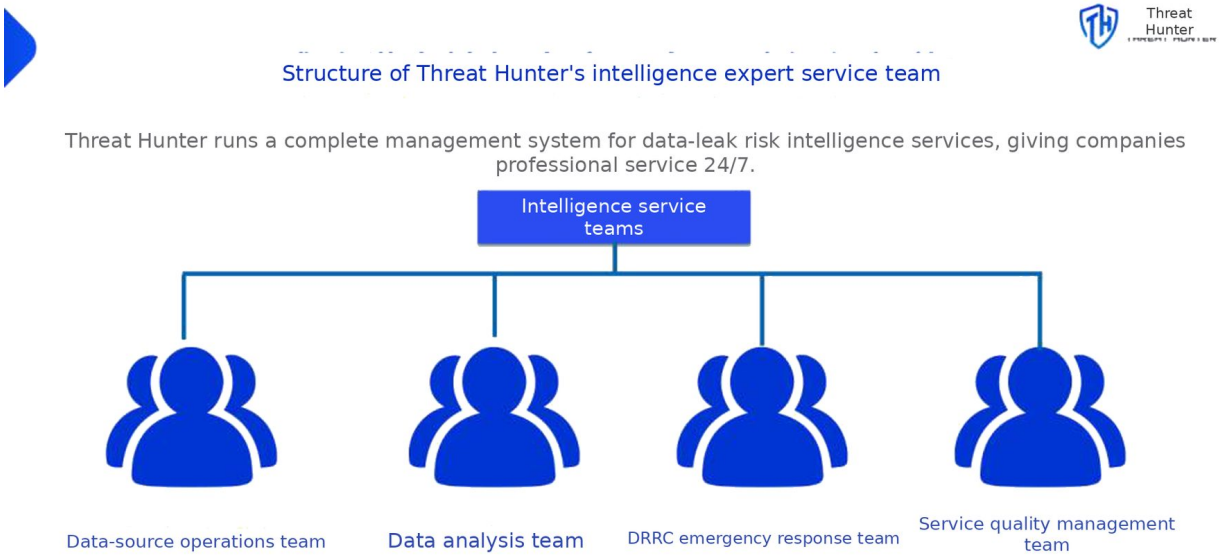
3. 24/7 emergency response: Threat Hunter's Digital Risk Response Center (DRRC) monitors, reviews and warns of risk intelligence related to each customer around the clock.

It provides 24/7 sample collection, intelligence mining, help with tracing sources, and takedown services, along with monthly data-leak risk monitoring reports and analysis of typical risk incidents.



Threat Hunter's DRRC teams provide 24/7 emergency response

Source: Threat Hunter original report, page 39. Original figure with Chinese text replaced by English.



Structure of Threat Hunter's intelligence expert service team

Source: Threat Hunter original report, page 39. Original figure with Chinese text replaced by English.

Company website: www.threathunter.cn Partnership email: Marketing@threathunter.cn