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 text version is reconstructed based on the 40-page original PDF, retaining the report narrative, chapters and research scope; the cover, duplicate table of contents and purely decorative pages are not repeated. Localized figures are placed in context throughout this web edition, with the original PDF retained 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 provides mature and diverse products and services focusing on risk scenarios such as business fraud, data leakage, phishing and counterfeiting, and API attacks that different industries face in the process of digital development. It has been selected as a representative vendor in Gartner's technology maturity curve report and IDC's threat intelligence field for many times.

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

In the first half of 2025, when the wave of digitalization continues to advance, data is the core asset of enterprises, and its security issues have attracted increasing attention from all parties. The number of data breaches continues to rise at a high level, and attack methods and transaction chains have become increasingly complex and hidden, becoming a major risk that threatens corporate compliance operations and business growth.

Threat Hunter's "Data Breach Risk Landscape Report for the First Half of 2025" focuses on the changing trends of current data leakage risks. From incident scale, industry distribution, transaction channels to typical cases, it systematically analyzes the latest trends in the data threat-actor industry chain, and comprehensively displays the overall domestic data leakage risk landscape in the first half of 2025.

Summary of key points in the report:

1. The number of data breach incidents remains high and rebounds rapidly after short-term fluctuations.

A total of 57,092 valid data breaches were detected in the first half of 2025, an increase of 1.54% from the second half of 2024. Among them, in April due to the impact of Telegram’s “group closure operation”, the number of incidents temporarily dropped by nearly 30%. However, in June due to the active reorganization of threat actors’ gangs, the number of incidents rebounded rapidly.

2. High-value industries have become key targets for attacks, and cross-border e-commerce leaks have increased significantly.

The three major industries of e-commerce, consumer finance, and banking are still the hardest-hit areas, and the total number of incidents in the top 3 industries is 1.32 times that of the remaining top 10 industries.

In the e-commerce industry, the volume of cross-border e-commerce events has increased by more than 10 times month-on-month, showing a clear trend of internationalization.

3. Dark web leaks increased by 35.2%, and Chinese forum activity increased significantly

A total of 18,106 leaks were detected through darknet channels, a month-on-month increase of 35.2%. Users of Chinese darknet forums such as "Chang'an City" and "D*Chinese" are growing rapidly. Newly registered users account for more than half of the events. The leaked data is mainly information from overseas platforms.

4. “Haowang Guarantee” collapsed, “Tudou Guarantee” quickly took over, and the guarantee platform is highly substitutable.

Telegram's leading guarantee platform "Haowang Guarantee" was severely hit in May and its business was paralyzed. However, in June new platforms such as "Tudou Guarantee" quickly filled the vacancy, reflecting that the supply and demand sides of the underground market are highly active and the transaction chain has strong "self-healing capabilities."

5. After BF was shut down, multiple platforms took over, and threat actors’ transactions migrated significantly.

BF contributed to 14.5% of the leaks on the dark web before the outage. After the platform was shut down, core users quickly migrated to alternative platforms such as X*S and D**s, and data trading continued, showing the strong adaptability and migration efficiency of threat actors users.

6. Credit risk management data “multiple lending” leaks have surged, building a complete industrial chain

Credit risk management data leakage incidents, represented by "multiple borrowing", have increased six times in half a year, forming a complete ecosystem of threat actors covering data theft, platform construction, and precision fraud. Multiple fraud-control system platforms such as "Fuyao" and "Xinchen" have been used as data transfer stations by threat actors.

7. Bank “scan QR code application” type data leakage increased by more than 4 times, related to third-party marketing tools

There were 111 “scan QR code application” loan information leaks in the first half of the year, involving more than 80 banks. The core risk stems from a certain financial technology marketing platform, involving the bank account manager business system. It is suspected that an insider or system vulnerability caused the data of high-intent customers to flow into the black market.

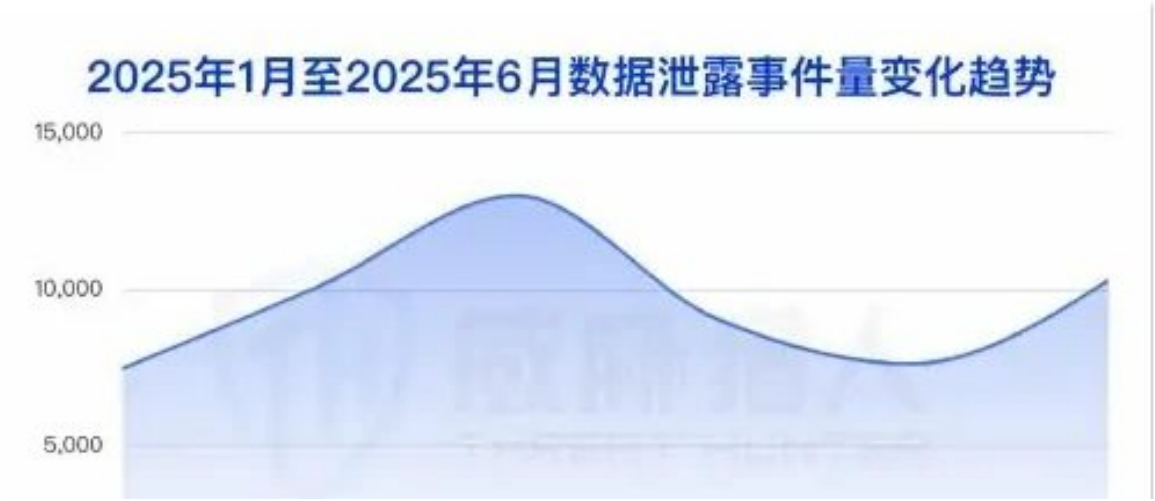
Disclaimer: The data information provided by Threat Hunter is estimated and analyzed based on large sample data sampling collection, small sample survey, data model prediction and other research methods. As any data source and technical method in the field of statistical analysis have limitations, Threat Hunter is no exception. The data information estimated and analyzed by Threat Hunter based on the above methods are for reference only. Threat Hunter does not make any guarantees about the accuracy, completeness, applicability and non-infringement of the above data information. Threat Hunter has nothing to do with any legal consequences caused by any action taken by any organization or individual citing or based on the above data information. Any relevant disputes or legal liabilities arising therefrom shall be borne by the perpetrators.

Data breach risk overview in the first half of 2025

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

1.1 There were 57,092 data breaches in the first half of 2025, which was 57,092 more than in the second half of 2024.

An annual increase of 1.54%. According to data from the Threat Hunter data leakage risk monitoring platform, between January and June 2025, a total of 180 million intelligence clues were monitored across the entire network. After manual analysis by the authenticity verification engine and DRRC, a total of 57,092 data breaches were confirmed to be valid.



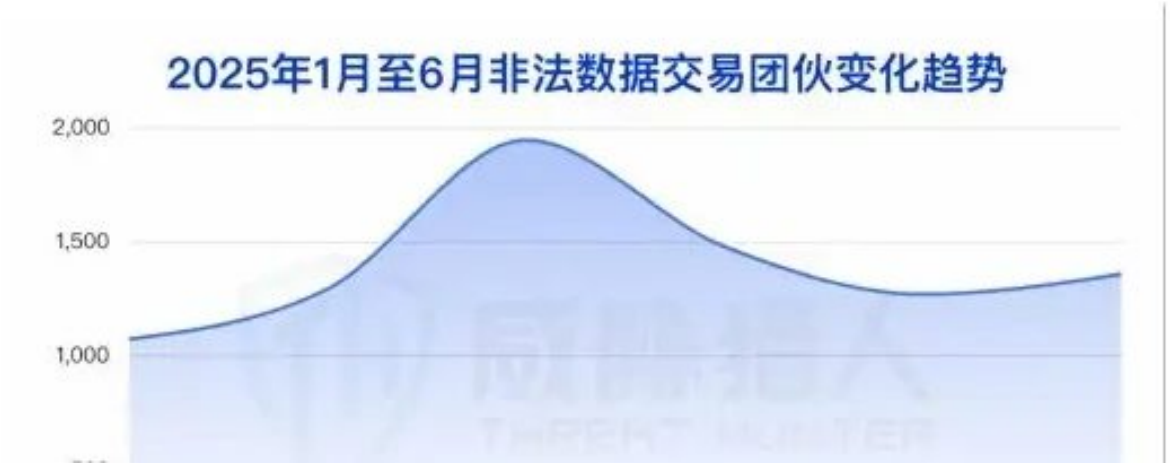
Data leaks in the first half of 2025 totalled 57092, compared to the second half of 2024

Source: Threat Hunter original report, page 7

English figure labels

1	Trends in data leakage incidents from January 2025 to June 2025

Threat Hunter observed that from January to March 2025, the number of data breach incidents showed a gradual increase. However, the number of incidents in April plummeted 29.93% from March, with 3,882 fewer incidents. It reached its lowest point in May with just 7,609 cases, before starting to pick up in June.



Data leaks in the first half of 2025 totalled 57092, compared to the second half of 2024

Source: Threat Hunter original report, page 8

English figure labels

1	Trends in illicit data trading groups, January-June 2025

Threat Hunter found that the main reason for this fluctuation was mainly due to the "group blocking operation" launched by the Telegram platform in April 2025 against illegal gangs, which resulted in the banning of a large number of illegal data trading group chats (see Chapter 2.1 of this report for details). Further analysis from the source of data leakage revealed:

In April 2025, Threat Hunter detected a significant decrease in the number of data breach incidents, with a total of 9,085 incidents, a decrease of 29.93% from March (12,967 incidents). Correspondingly, the number of active illegal data trading gangs also dropped from 1,943 to 1,477, a decrease of 23.98%.

At the same time, 33.71% of the illegal data trading gangs active in March were banned in April.

Affected by this, the number of data breach incidents has dropped significantly.

However, due to the difficulty of completely banning the Telegram platform and the extremely strong "regeneration ability" of illegal gangs, a large number of new or alternative groups became active again in a short period of time, driving the number of data breaches to rebound again in June 2025.

1.2 In the first half of 2025, the number of data breach incidents in the Top 3 industries was greater than that of the remaining Top 10

1.32 times that of the industry. Attack groups prefer data target events with high net worth and high activity. From the perspective of industry distribution, data leakage incidents across the entire network in the first half of 2025 involved a total of 76 industries. The top 3 industries are e-commerce, consumer finance, and banks.

Among them, highly sensitive and high-realizability industries, represented by e-commerce and finance, are still the hardest hit areas for data leakage.

The changes in the rankings of the top 10 industries in the first half of 2025 are as follows:

1.3 The e-commerce industry has become the top industry with the number of data leakage incidents, with the number of incidents reaching

Data disclosure industry ranking and e-commerce risk (Chart 1)

Source: Threat Hunter original report, page 9

English figure labels

1	Top 10 industries affected by data exposure, January–June 2025
2	E-commerce · Consumer finance · Banking
3	Express delivery · Securities · Social media
4	Software apps · Insurance · Online ticketing · Automotive

2025 年上半年 TOP10 行业排名变化情况如下：

行业	2024年下半年排名	2025年上半年排名	排名变化
电商	3	1	↑2
消费金融	1	2	↓1
银行	2	3	↓1
快递	4	4	-

Data leakage industry ranking and e-commerce risk (Chart 2)

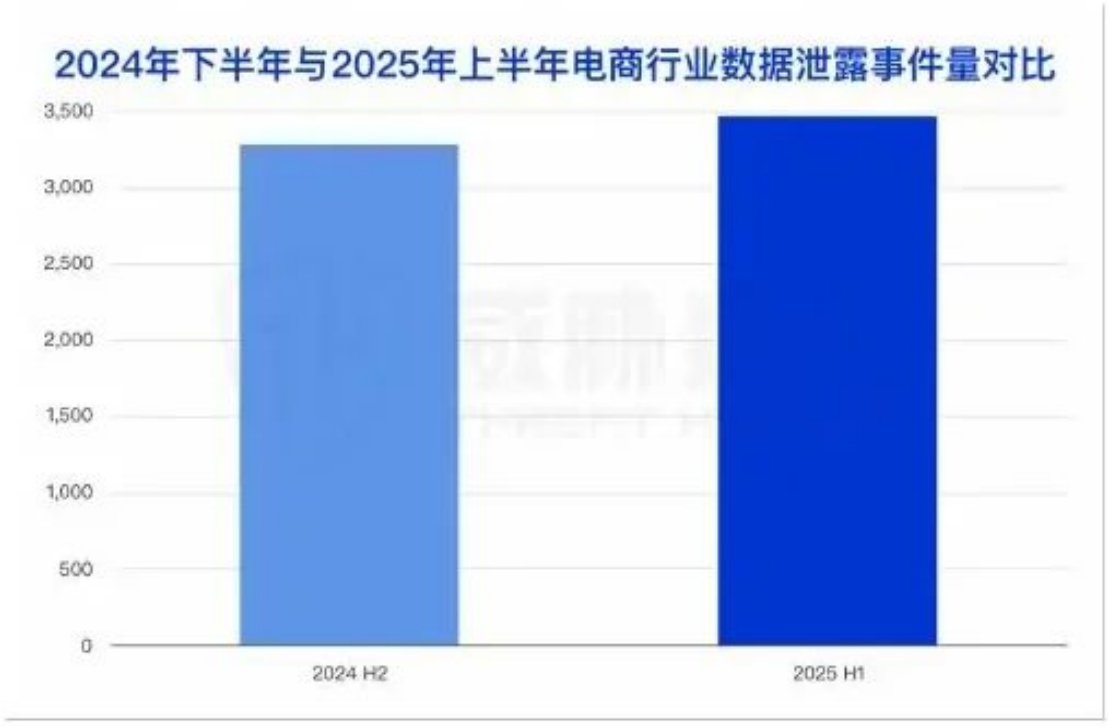
Source: Threat Hunter original report, page 9

English figure labels

1	In the first half of 2025, the ranking of the top 10 sector changed as follows:
2	Industry
3	Second half of 2024.
4	Ranking in the first half of 2025
5	Change in ranking
6	There's a eee on the top.

3,465 cases, cross-border e-commerce leakage incidents increased more than 10 times month-on-month. Threat Hunter data leakage risk monitoring platform data shows that a total of 3,465 data leakage incidents occurred in the e-commerce industry in the first half of 2025, an increase of 184 cases from the second half of 2024, an increase of 5.60%.

Among them, data leakage incidents in the cross-border e-commerce field are particularly prominent. The number of incidents increased by 394 compared with the second half of 2024, an increase of more than 10 times. The leakage incident involves many countries and regions around the world, mainly concentrated in Southeast Asia. The top three countries are Vietnam, the United States and Thailand.

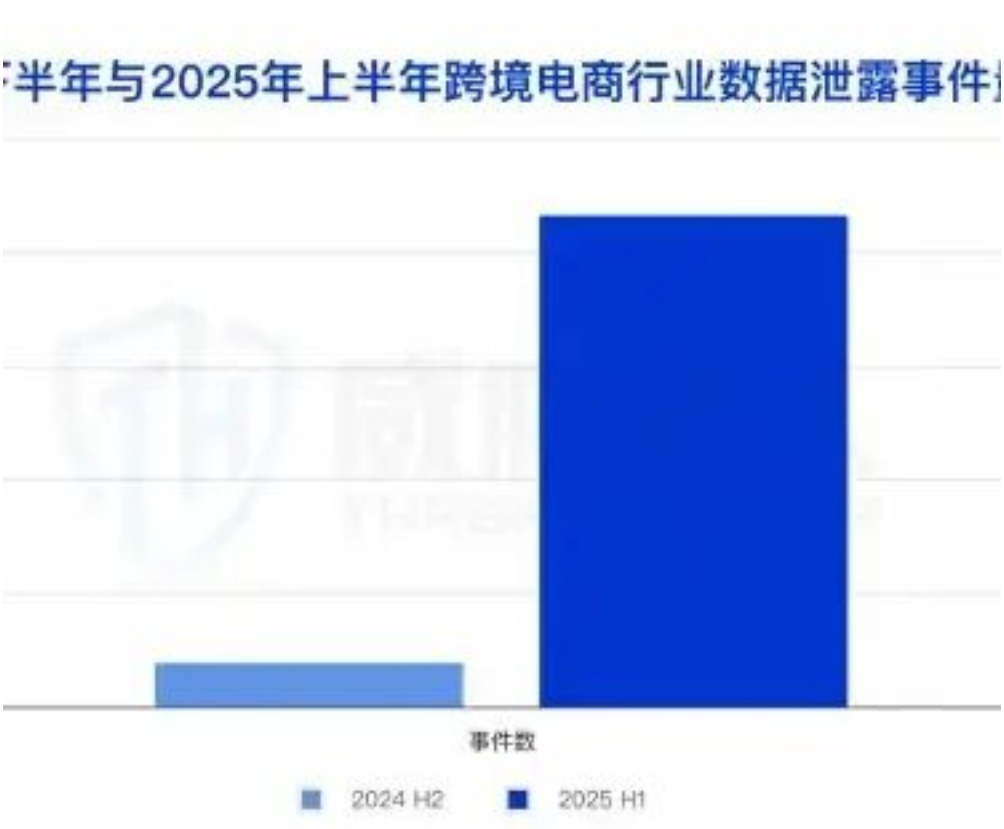


Number of data leaks in the electric power industry Top1 industry, number of incidents (Chart 1)

Source: Threat Hunter original report, page 10

English figure labels

1	E-commerce data-exposure events: 2024 H2 vs 2025 H1



Number of data leaks in the electric power industry, Top1 industry, number of incidents (Chart 2)

Source: Threat Hunter original report, page 10

English figure labels

1	Data leaks from the cross-border e-commerce industry in the six months and the first half of 2025:
2	Events

1.3.1 Typical case analysis: Multiple cross-border e-commerce shopping user information leaked due to security protection deficiencies in third-party logistics

Recent monitoring by Threat Hunter found that there is a group of threat actors on the dark web that is selling user online shopping information data of a cross-border e-commerce platform. The publisher provided some data samples and claimed that the data covers Southeast Asia, North America and other countries and regions.

Threat Hunter researchers analyzed the fields such as "express label" and "commodity label" in the leaked data and inferred that the data was suspected to come from the same international express logistics company. Combined with the company-related leaks previously monitored on dark web Chinese forums, it was further confirmed that the company's system had a security flaw, and was exploited by a group of external threat actors to carry out attacks and obtain relevant user information.

1.4 In the first half of 2025, the activity of darknet data leaks continued to increase, and the number of incidents increased year-on-year.

Increased 35.2% Threat Hunter statistics show that in the first half of 2025, anonymous group chats and the dark web will still be the main channels for data leaks.

It is worth noting that a total of 18,106 data breaches occurred in dark web channels. The total number of incidents increased by 35.2% compared to the 13,389 incidents monitored in the second half of 2024.

In the first half of the year 2025, darknet data leaks continued to increase in activity, events ring. That's right.

Source: Threat Hunter original report, page 12

English figure labels

1	Sources of data leakage from January to June, 025;

1.4.1 The activity of Chinese dark web forums surged, and the leakage incidents mainly pointed to overseas user data

Further analysis by Threat Hunter found that the "Chang'an City" forum was the platform with the largest increase in data leakage incidents among dark web channels. The number of data breaches contributed by it in the first half of 2025 increased by 81.7% compared with the second half of 2024, with 1,493 incidents. At the same time, the number of incidents on another Chinese forum "D*Chinese" also increased from 272 in 2024 to 560, an increase of more than double, reaching 105.9%.

A total of 271 users of these two Chinese dark web forums posted data transaction posts in 2025, of which 166 were new registered users, accounting for 61.3%; the content posted by these new users involved a total of 1,961 data leakage incidents, accounting for more than half of the overall incidents in the two major forums.

Most of these new data leakage incidents involve the leakage of data information from overseas platforms or users. Among them, the "Chang'an** City" single platform involves user data from more than 20 countries and regions around the world.

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

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

The following is the illegal data trading industry chain:

Among them, midstream data middlemen are active on the dark web, threat actors forums, Telegram, Potato and other platforms. They are responsible for cleaning, classifying, packaging and matching transactions of leaked data. They are the key hub of the entire transaction chain.

Although regulatory pressure continues to increase, downstream fraud gangs, gray e-commerce companies, etc. have always had strong demand for high-quality data, which has prompted the data trading market to remain active.

2.1 The top guarantee gang was attacked, and new guarantees quickly filled their positions

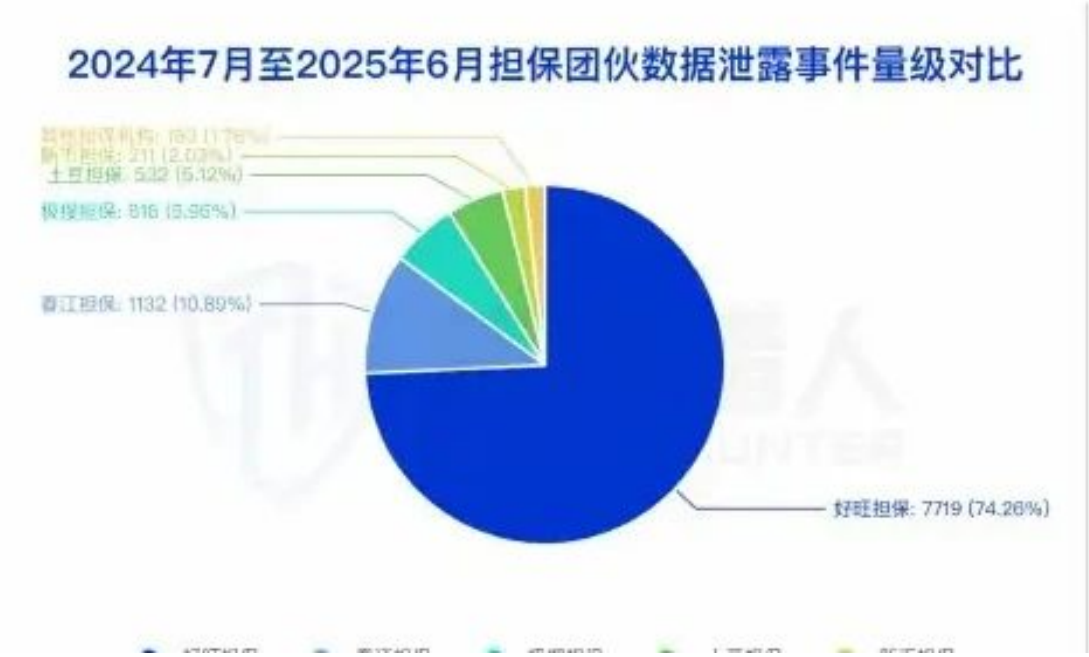
"Haowang Guarantee" (formerly "Huiwang Guarantee") has been active on anonymous social platforms such as Telegram for a long time. With its third-party credit intermediary services, it has become the core guarantee platform for threat actors such as data trading, fraud, and money laundering. It held a dominant position in the market before the first half of 2025. Details can be found at:

However, in May 2025, Haowang Guarantee suffered a heavy blow:

- On May 1, the US Financial Crimes Enforcement Network (FinCEN) listed its parent company Huione Group as an institution of “primary money laundering concern” and cut off its international financial channels. Subsequently, Telegram officials banned its trading groups and accounts in early May.

- On May 9, Haowang officially announced that "a large number of trader accounts have been canceled." At this point, its operating system completely collapsed, and the public group business interruption rate reached 100%.

(Timeline of the whole process of Haowang Guarantee migration)



The head guarantee group is under attack. The new guarantee is being filled quickly.

Source: Threat Hunter original report, page 16

English figure labels

1	Quantitative comparison of incidents of disclosure of data from guarantee groups, July 2024 to June 2025
2	fre.12 for N.
3	AL - Guarantee - 7719 (74.26%)

Threat Hunter monitoring found that since the outage of "Haowang Guarantee", the number of related data leakage incidents plummeted from 832 in March to basically zero in June.

But the demand for threat actors has not disappeared. After the collapse of "Haowang Guarantee", new platforms such as "Tudou Guarantee" quickly emerged.

Data shows that data breaches related to Tudou Guarantee surged from 12 in April to 358 in June, an increase of nearly 30 times.

In the illegal data trading market, both the data supply side and the demand side are highly active, forming a strong supply and demand relationship and giving rise to a complete transaction chain of threat actors. However, due to the high risks and high uncertainties in the transaction itself, it is difficult for buyers and sellers to establish a direct trust relationship.

Therefore, the intermediary role of "guaranteed platform" gradually emerged in the threat actors ecosystem. The existence of intermediaries not only brokers transactions, but also undertakes the functions of hosting funds and arbitrating disputes. It is an important fulcrum for the continuous operation of the entire threat actors transaction. Because of this, even if a certain platform is cracked down, new intermediaries will quickly fill their positions and reappear with different vests.

As long as transactions exist, the market demand for such "threat actors service providers" will not disappear, making it difficult for them to be completely eradicated.

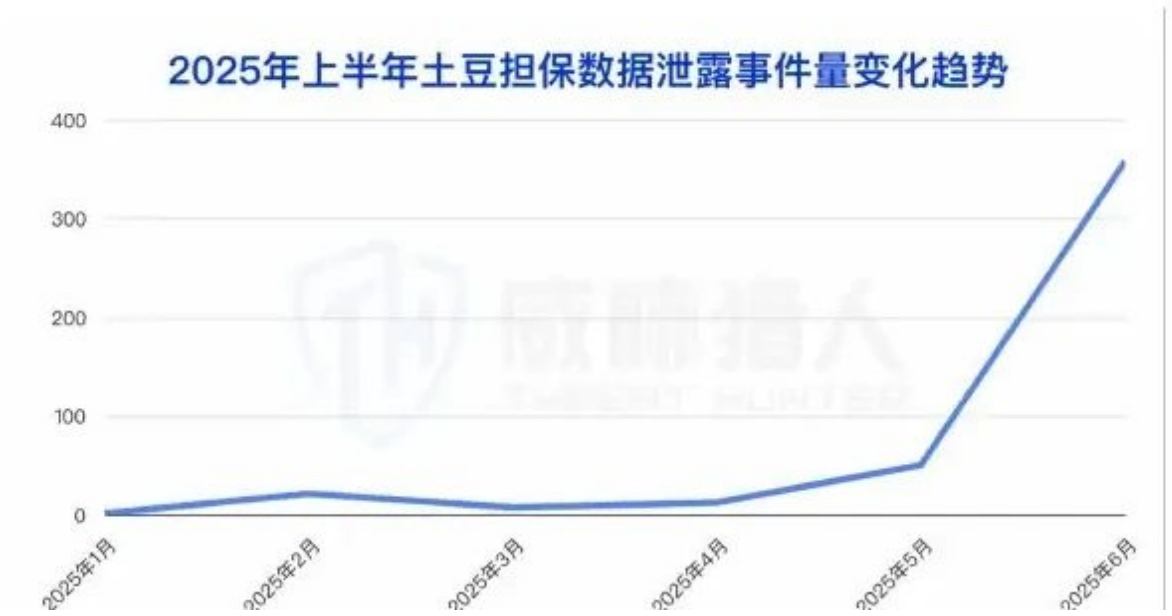
2.2 The threat-actor platform can be attacked, but the transaction demand is difficult to eradicate

Head guarantee groups hit, new guarantees filled quickly (Chart 1)

Source: Threat Hunter original report, page 17

English figure labels

1	Trends in the volume of leaking data during the first half of 2025



The head guarantee group was hit and the new guarantee was quickly filled (figure 2)

Source: Threat Hunter original report, page 17

English figure labels

1	Trends in the number of potato-back data leaks during the first half of 2025

2.2.1 The leading forum was attacked and the supply dropped sharply; before the shutdown, it contributed nearly 15% of the data events to darknet channels

Although the threat-actor platform faces continued high-pressure attacks, the market demand for data transactions has never weakened. Take the leading darknet forum BF as an example. In the first half of 2025, the platform was still one of the most important data leakage supply nodes in the world.

Threat Hunter monitoring data shows that from January to June 2025, darknet channels contributed a total of 15,096 data leakage incidents, of which the BF platform contributed 2,190, accounting for 14.5% of the total number of darknet incidents. Especially in the first three months before the outage, the activity of the BF platform continued to rise, reaching a monthly peak of 657 in March 2025.

However, as BF was suddenly shut down on April 15, the number of related data leakage incidents dropped rapidly. Only 393 cases were detected in April, a month-on-month decrease of 43.2%. The number of incidents returned to zero in May; the platform's supply capacity showed a clear cliff-like decline.

2.2.2 After the BF platform was shut down, multiple alternative forums quickly took over.

Despite this, the shutdown of BF did not dampen the overall activity of threat actors, but they quickly moved to other darknet platforms and private communication tools.

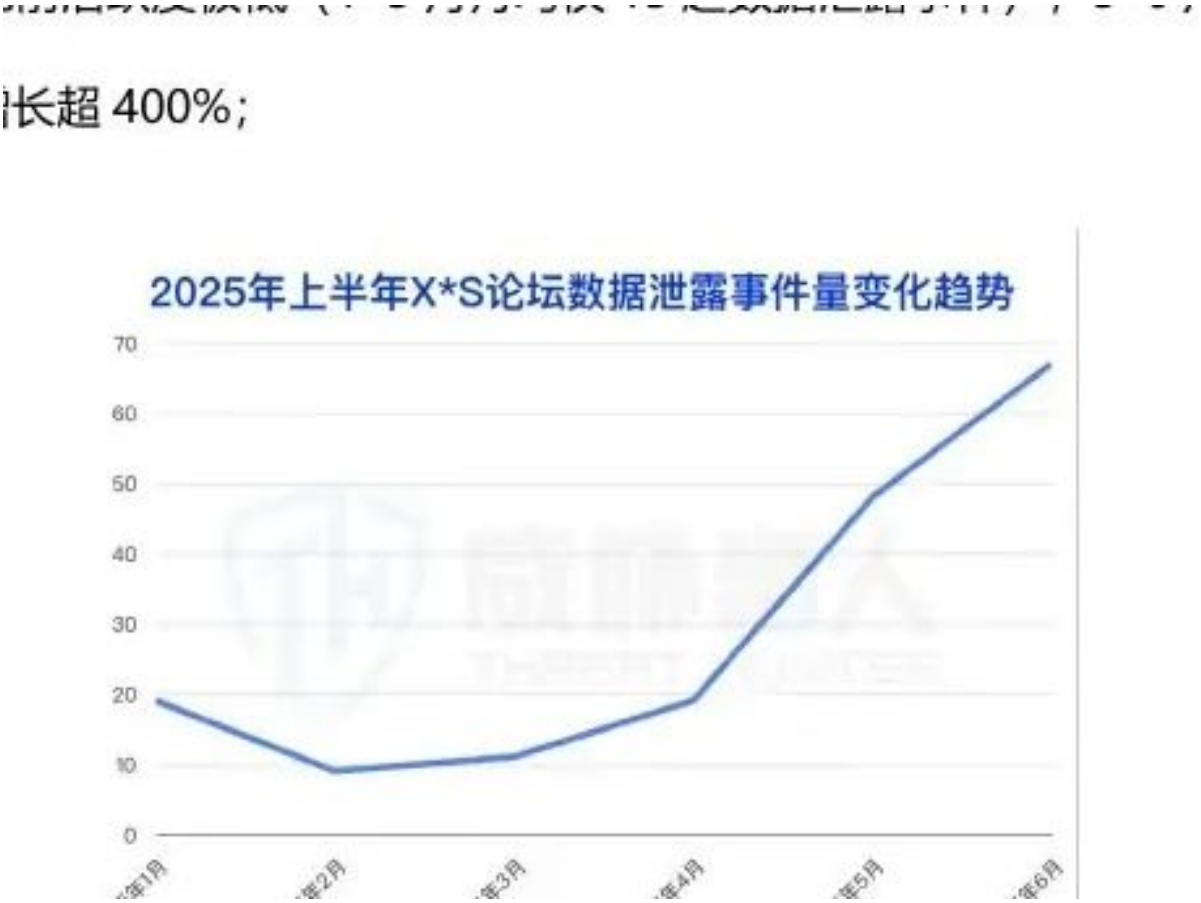
Take the following platform data observed by Threat Hunter as an example:

- D**s Forum: The number of incidents exceeded 100 in April, soared to 275 in May (a 374% increase from March), and skyrocketed to 1,095 in June, an increase of nearly 20 times compared with before the shutdown;
- R**d Forum: Although there was a brief decline in April due to the impact of BF, it rebounded strongly from May to June. The number of leaks in June increased by 138% compared with April;
- X*S Forum: Previously very low in activity (an average of only 13 data breaches per month from January to March), it surged to 48 and 67 from May to June, a month-on-month increase of over 400%;
- E**t Forum: The number of incidents rose to 70 in April (a 169% increase from March) and 110 in June, showing a steady upward trend.

The above data shows that the threat actors ecosystem has a strong "self-healing" ability. Although the platform was hit, traffic, resources and participants were quickly rebuilt on the new platform, and market popularity recovered quickly.

2.2.3 The core users of the BF platform migrate quickly, and the activities of threat actors have strong continuity

Threat Hunter tracking found that BF’s top ten core publishers (contributing 14.6% of the platform’s event volume) quickly moved to other platforms and continued to be active after the platform was shut down.



Several alternative forums fast-tracked after the BF platform was discontinued

Source: Threat Hunter original report, page 20

English figure labels

1	Over 400% long;
2	Trends in the number of leaks of X*S data in the first half of 2025

Take BF’s most active user K***t in the first half of the year as an example:

"K***t" has been seamlessly transferred to the XSS forum since the suspension of BF, and continues to publish overseas user data, shopping orders, CRM system information, etc., with rich data types, covering many countries and industries;

He has a high posting frequency, standardized data structure, and is suspected to have strong data cleaning and distribution capabilities. He is a typical "professional data porter", showing strong adaptability and migration efficiency to black market trading platforms.

This trend shows that the core practitioners of threat actors have extremely strong mobility and resilience. As long as the demand for data transactions exists, they can quickly rebuild trading channels and keep the underground market active.

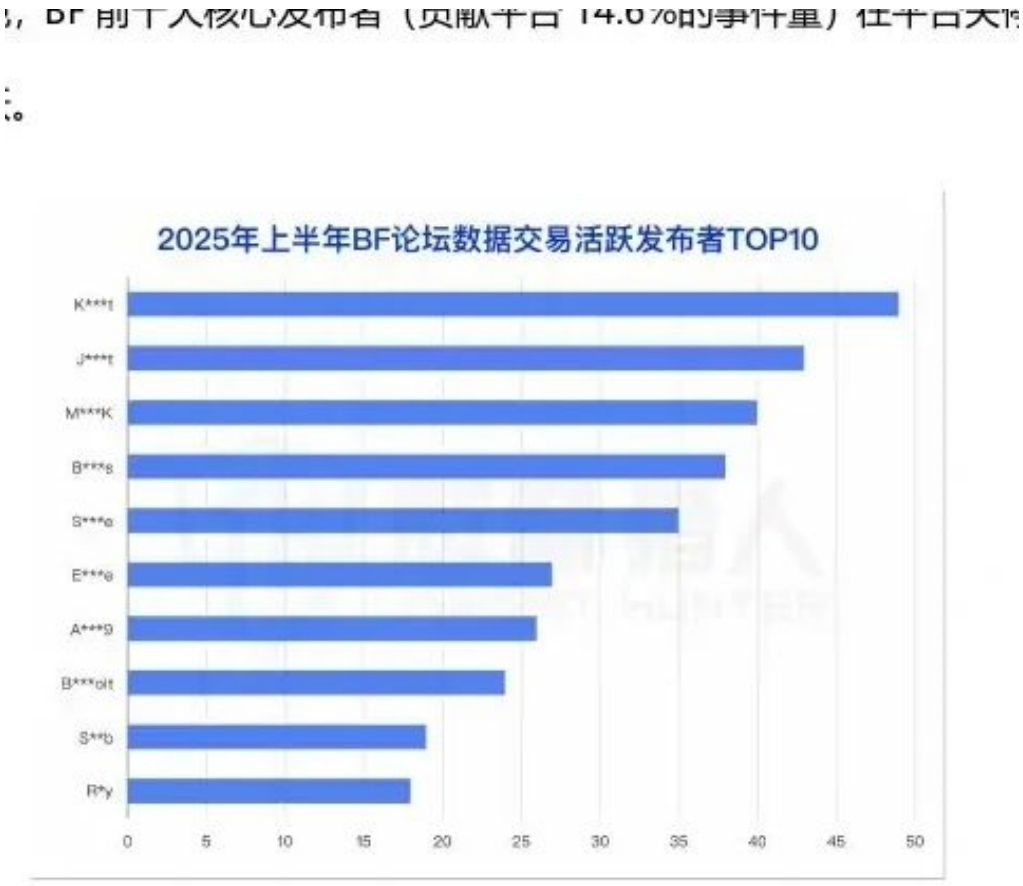
BF’s case confirms the core law of the cybercrime ecosystem market: when the main trading platform is cracked down, users and demand will quickly migrate to existing or emerging alternatives. The data trading market has strong adaptability. Even if the head platform is destroyed, threat actors can still rely on other channels to maintain business operations.

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

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

3.1 Analysis of data leakage risk landscape and industrial ecology in credit risk management approval scenario

3.1.1 Citizen multiple borrowing data leakage incidents have increased significantly compared with the second half of 2024, with an increase of more than 6 times



BF Platform core users rapidly migrated and cybercrime activity was sustained

Source: Threat Hunter original report, page 21

English figure labels

1	BF Forum Data Exchange Active Issuer top 10 in the first half of 2025

There were a total of 117 data leaks of loan information in a category called "multiple borrowing", an increase of 631.25% compared to 101 new cases in the second half of 2024.

Capture data of credit "multiple borrowing" risk intelligence shows that since November 2024, such data breaches have basically shown a continuous upward trend.

multiple borrowing: refers to a fraud-control mechanism that specifically detects borrowers' "multiple borrowing" behavior. It is actually a data sharing system established by a third-party data

service provider and a number of online lending companies. When a borrower initiates a loan application to one of these institutions, the "application behavior" itself will be captured and recorded by the system like a signal. In fact, it refers to the record information data of the borrower's long loan.

Data leakage intelligence: Threat Hunter captures "unauthorized personal/organizational sensitive information being publicly traded or used" intelligence information captured through TG groups, dark web and other channels, which may include historical data, duplicate data, etc., and is often of huge magnitude;

Data leakage incidents: Threat Hunter security research experts analyze and verify samples of data leakage intelligence, eliminate historical false data, and confirm valid data leakage incidents;

Through in-depth analysis, Threat Hunter learned about the so-called "multiple borrowing" data among threat actors. Its core content mainly covers the repayment performance and overdue records of loan users. In the current credit risk management scenario, "multiple lending" data plays a key role. It can reflect the borrower's "multiple lending" behavior, that is, the situation of users applying for or holding loans on different platforms. When this kind of data is illegally used, it will have a serious impact on the decision-making of credit institutions, which may lead to distortion of risk assessments. It may also lead to the leakage of users' personal privacy information and encounter targeted marketing or fraud.

(The leaked data captured by Threat Hunter contains user performance information)

3.1.2 A credit risk management industry chain with "loan record information" data as the core has been formed

According to Threat Hunter's in-depth investigation and research, it was found that an underground credit risk management threat-actor industry chain with "loan record information" data as the core has been formed, and its operating model covers a series of illegal activities such as data theft, platform construction, data sales, and downstream targeted marketing and fraud.

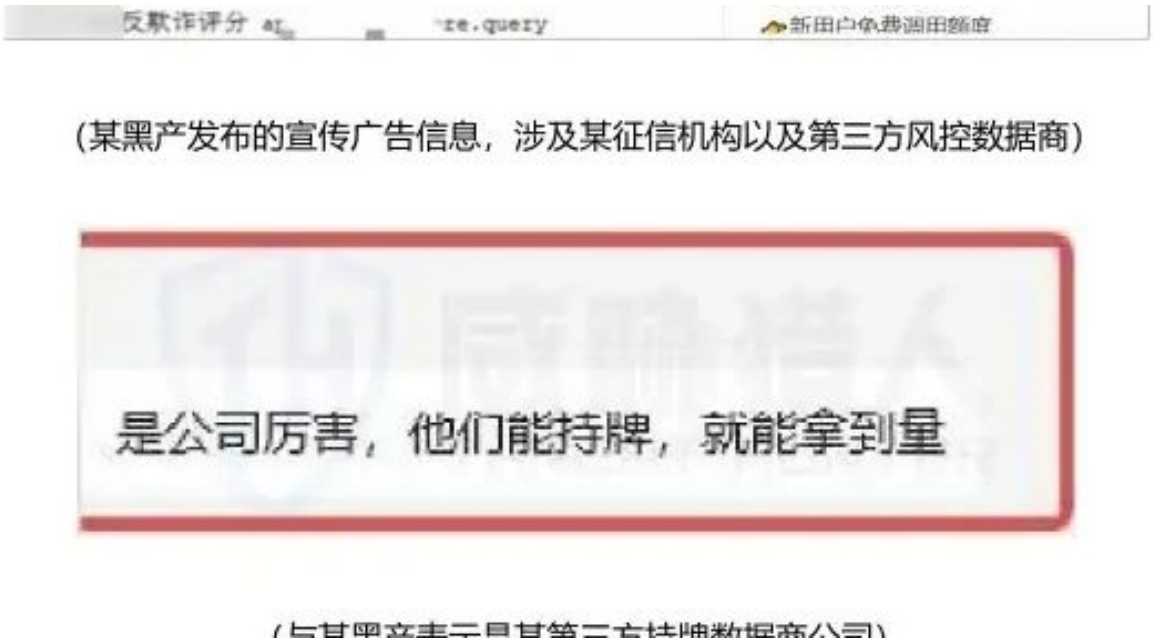
The specific industrial chain situation is as follows:

1. Upstream: The sources are mainly credit reporting agencies and third-party licensed risk-management data providers.

Through in-depth analysis, Threat Hunter learned about the so-called "multiple borrowing" data among threat actors. Its core content mainly covers the repayment performance and overdue records of loan users. In the current credit risk management scenario, "multiple lending" data plays a key role. It can reflect the borrower's "multiple lending" behavior, that is, the situation of users applying for or holding loans on different platforms. When this kind of data is illegally used, it will have a serious impact on the decision-making of credit institutions, which may lead to distortion of risk assessments. It may also lead to the leakage of users' personal privacy information and encounter targeted marketing or fraud.

At the same time, Threat Hunter conducted an in-depth analysis of the risk-management data query system provided by threat actors. All users' authorization letters involved a domestic credit agency.

(Promotional advertising information released by an threat actor, involving a credit reporting agency and a third-party risk-management data provider)

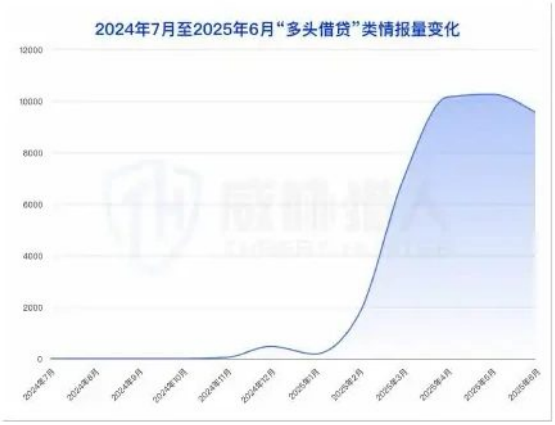


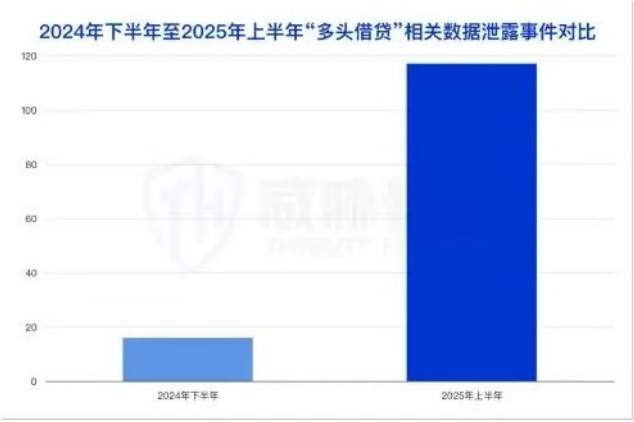
Citizens' multiple-lending data leaks were higher than in the second half of 2024, six times higher.

Source: Threat Hunter original report, page 27

English figure labels

1	Advertising information published by a black-sourced agency involving a letter caller and a third-party wind data dealer)
2	It's a good company. They hold cards, they get numbers.





Citizens' multiple-lending data leaks were higher than in the second half of 2024, six times higher.

Source: Threat Hunter original report, page 25

English figure labels

1	Changes in the volume of intelligence in the category “multiple lending” from July 2024 to June 2025
2	Comparison of multiple lending incidents between the second half of 2024 and the first half of 2025
3	Late 2024
4	First half of 2025

(With some threat actors, it means it is a third-party licensed data provider company)

2. Midstream: spawning multiple risk-management data query service platforms and platform construction services

姓名	身份证	号码1	号码2	0：代表查无数据	最大履约金额	履约笔数	当前逾期机构数	睡眠机构数	当前履约机构	最近履约时间	异常还款机构	最大逾期金额	最长逾期天数	最近逾期时间
王			4	2	40	16	0	4	9	2025-01	0	NULL	NULL	NULL
韩			8	2	80	0 11	0	3	8	2025-02	0	NULL	NULL	NULL
刘			4	2	60	32	0	16	15	2025-02	0	NULL	NULL	NULL
王			1	2	10	00 14	0	6	8	2025-01	0	NULL	NULL	NULL
杨			0	2	40	22	0	4	14	2025-02	0	NULL	NULL	NULL
方			7	2	80	0 47	0	31	31	2025-02	0	NULL	NULL	NULL
高			2	2	80	0 21	0	9	14	2025-02	0	NULL	NULL	NULL
段			8	2	10	00 43	0	8	15	2025-01	0	NULL	NULL	NULL
谷			6	2	10	00 160	0	27	59	2025-02	0	NULL	NULL	NULL
关			7	3	60	33	0	11	11	2025-01	0	NULL	NULL	NULL
杜			4	2	60	10	0	8	9	2025-02	0	NULL	NULL	NULL
郭			3	2	10	00 33	0	9	14	2025-02	0	NULL	NULL	NULL
郭			5	2	10	00 46	0	18	28	2025-02	0	NULL	NULL	NULL
郭			2	2	80	0 79	0	23	28	2025-02	0	NULL	NULL	NULL
郭			9	2	10	00 35	0	5	16	2025-02	0	NULL	NULL	NULL
郭			2	2	10	00 19	0	7	14	2025-02	0	NULL	NULL	NULL
韩			9	2	80	0 8	0	4	6	2025-01	0	NULL	NULL	NULL
韩			5	2	10	00 130	0	41	48	2025-02	0	NULL	NULL	NULL
郝			2	2	10	00 30	0	17	20	2025-02	0	NULL	NULL	NULL
何			6	2	40	30	0	6	15	2025-02	0	NULL	NULL	NULL
何			8	2	40	7	0	0	6	2025-02	0	NULL	NULL	NULL

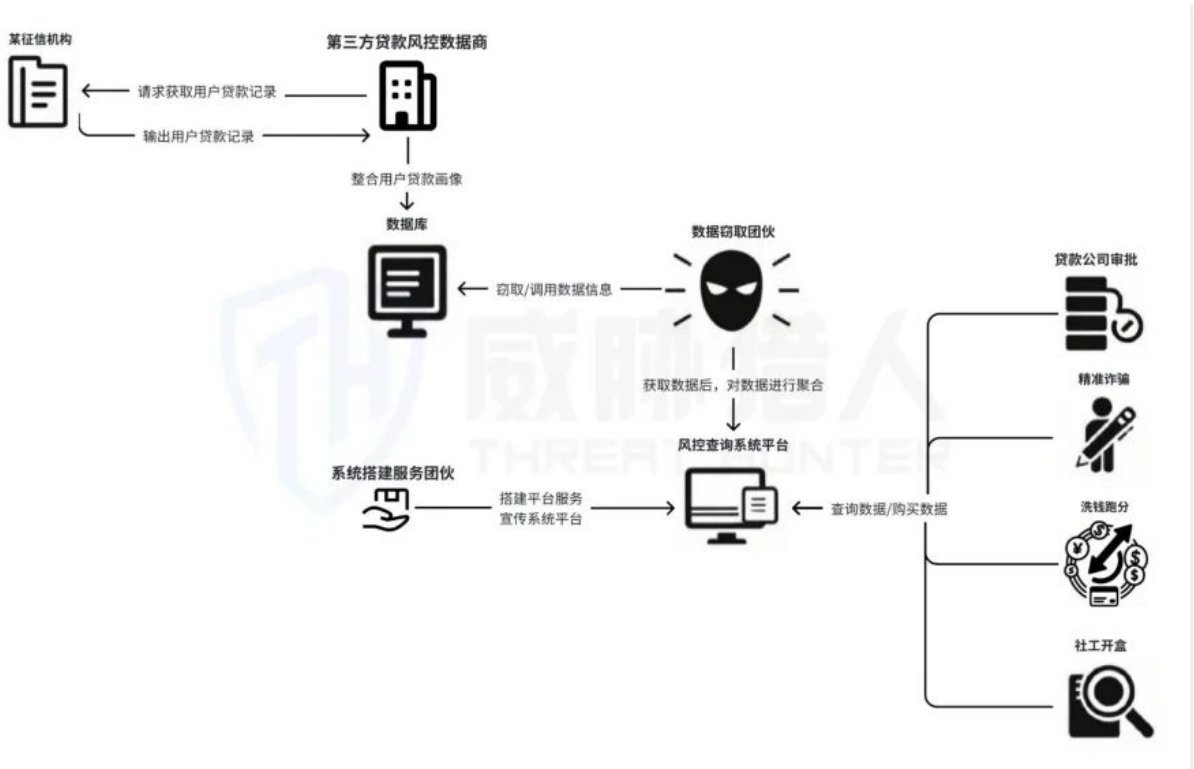
The leak sample included performance fields such as the number of loans, the number of current overdue institutions and the most recent overdue period; identity information was dissensitized.

Source: Threat Hunter original report, page 26

English figure labels

1	ID Se
2	Number 2.

Threat Hunter observed that due to the influence of "multiple borrowing" data, a large number of threat actors have appeared to promote risk-management data query system services, or directly sell user information data on overdue loans. These data query system services usually cover a variety of data query and verification functions such as "multiple lending" and "three-factor verification". Typical platform systems observed by Threat Hunter include "Fu* fraud controls Query", "Yi* fraud controls System", "Xin* fraud controls Query System", etc.



Data theft, wind search platforms and downstream loan approvals, precision fraud and social openings form underground chains.

Source: Threat Hunter original report, page 26

English figure labels

1	Some kind of letter agency.
2	Third-party loan winding data dealer
3	Request for user loan log I
4	= exit user loan record one.
5	User loan portrait
6	Database
7	Loan company approval
8	Once the data is available, the data are aggregated
9	That's a lie.
10	Wind Query System platform
11	System-building service groups
12	It means building a platform.
13	Money laundering
14	Social workers start

(The picture above shows the promotion of the risk-management data query system provided by threat actors)

At the same time, Threat Hunter also noticed that on social platforms such as WeChat, there are a large number of threat actors propaganda that can assist mid- and downstream threat actor

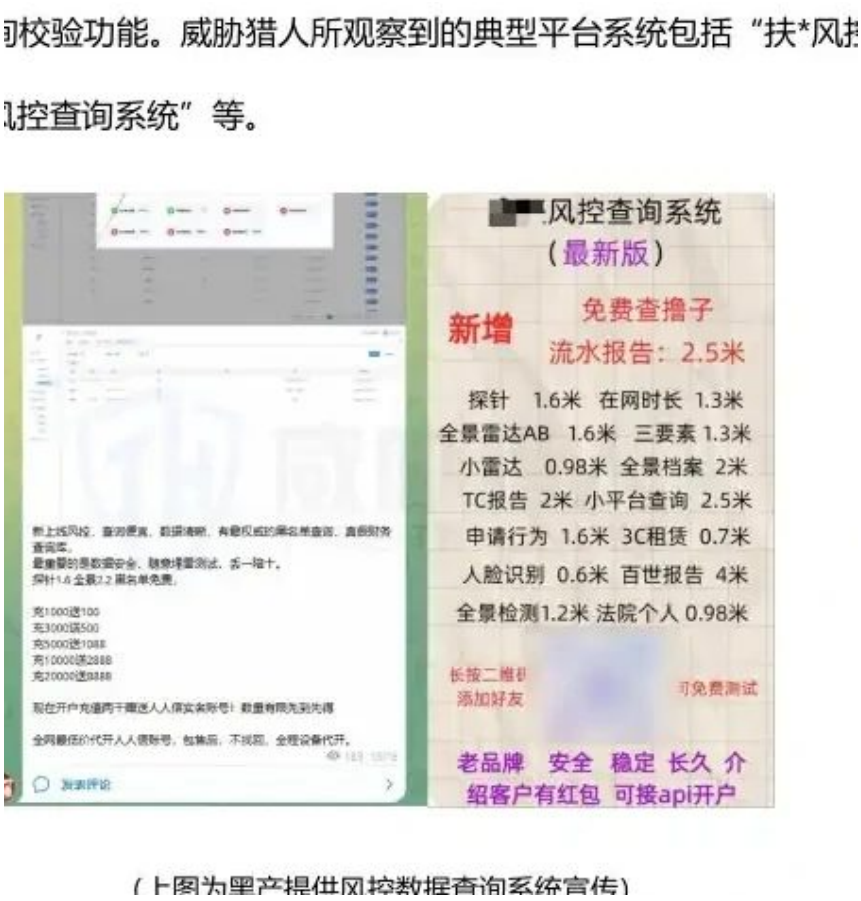
groups to build corresponding malicious activity platforms, such as "financial guarantee system", "leasing system", "fraud-control system", "credit inquiry system", "IOU inquiry system" and other types. These systems usually claim to have comprehensive functions and perfect fraud controls, support "one-stop services" such as overdue credit reporting, and notarization of property rights, and provide "full-process accompaniment and traffic support."

(The picture shows cybercriminal groups’s promotional content for platform construction services)

3. Downstream: Facilitate the upgrading of illegal and criminal activities such as targeted marketing, fraud, and money laundering

According to Threat Hunter’s observation, the downstream groups that receive and use such user loan qualification information records mainly focus on the following types:

1. Finance: mainly refers to the loan approval personnel of small and medium-sized loan platforms. They use these illegal data to query the qualifications of users.



（上图为黑产提供风控数据查询系统宣传）

A credit-control industry chain centred on data such as “borrowing record information” has developed

Source: Threat Hunter original report, page 28

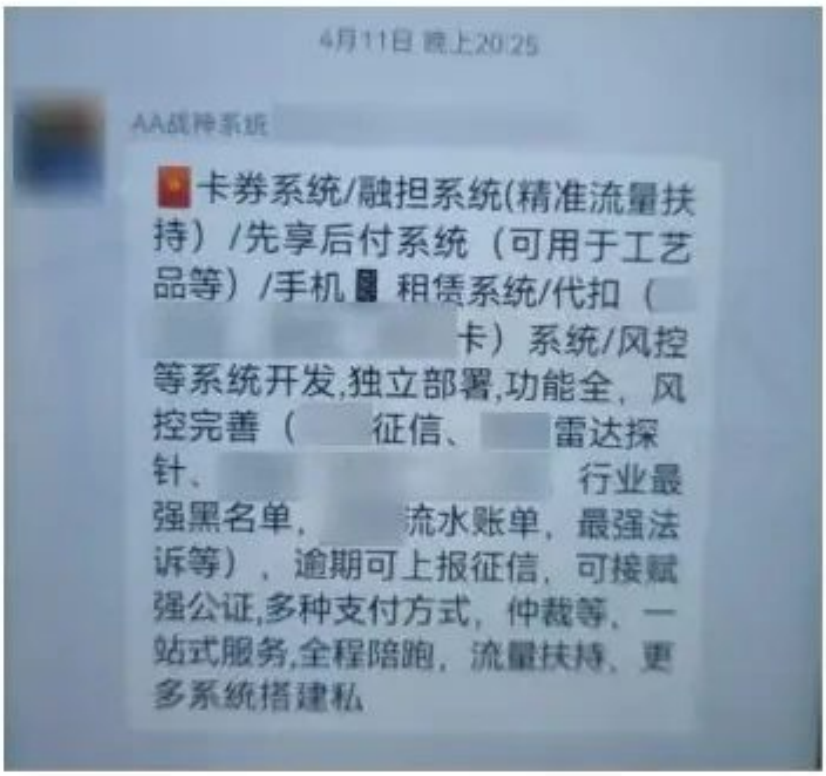
English figure labels

1	Check function. A typical platform system observed by a threat to hunters includes "Aft"*
2	Wind Query System
3	One...
4	Water flow report: 2.52
5	It's 1.6 meters long on the net.
6	AB 1.6 m "Three elements 1.3 m"
7	"0.98 m panorama file2"
8	TORE 2-metre small platform query 2.5 meters
9	Request for action 1.6 m3C lease 0.73
10	S452 free of charge.
11	AMIR 0.6 meters report 4 meters.
12	Panoramic test 1.2 m for individual court members 0.98 m
13	Old brand secure KAD.

Conduct comprehensive review and approval, or screen out target group users for targeted marketing;

2. Score running personnel: Mainly money launderers. After obtaining the data, they use their bank cards to conduct illegal activities by gaining the trust of users.

Fund flow, the so-called "score running" behavior;



（图为黑产团伙发布平台搭建服务宣传内容）

A credit-control industry chain centred on data such as “borrowing record information” has developed

Source: Threat Hunter original report, page 29

English figure labels

1	April 11th.
2	Carnet system/cleavage system (precision flow support)
3	Hold / buy-in systems (available for process)
4	(c) Systems/wind control
5	Wait for system development, stand-alone deployment, full functionality, wind.
6	Control Perfect
7	Industry
8	The black list.
9	Water bills, the strongest.
10	Notarized, multiple methods of payment, arbitration, etc.,
11	Station eye service, running around, traffic support, more.
12	Multi-system-based construction

3. Fraudsters: carry out "fish killing" (or "shark") behavior, mainly through telecommunications fraud (including loan fraud, impersonation

Public Security Bureau, Procuratorate, etc.) carry out precise fraud on users and use illegally obtained data to increase the success rate of fraud.

4. File checkers: In the data transaction file check scenario, there is a business that provides this kind of targeted inquiry on the credit status of individuals who open boxes, mainly

It calls the upstream data query by providing the user's name + ID card + phone number information, and returns the corresponding credit report information.

(The picture on the left shows the midstream threat actors indicating that the data is suitable for money laundering, fraud and other malicious activity behaviors. The picture on the right shows the query output of a personal credit report)

Appendix: Definitions of related slang words

Threat Hunter has conducted in-depth research and tracking of risk information related to "multiple borrowing". The following is the common slang terms used by threat actors related to "probes" to explain finance: Also known as "cw", it actually refers to loan sharks/private lending platform personnel.

Rongdan: Also known as "Rongdan", "Rongdan", "RD", Rongdan refers to a series of online loan platforms. This series is mainly composed of many small or micro online loan apps. The application process of this type of platform is simple and the pass rate is high. Therefore, "Rongdan material" actually refers to the user information data of small online lending platforms.

IOU: Also known as JT, it actually refers to the type of loan sharking or private loan, which will sign an "IOU" or electronic signature with the borrower, and "IOU material" actually refers to the user information data of the "IOU" signed by private lending or loan sharking.

Anti-aircraft guns: refers to loan sharking platforms or institutions, and anti-aircraft guns materials refer to user information data that make loans on loan sharking platforms.

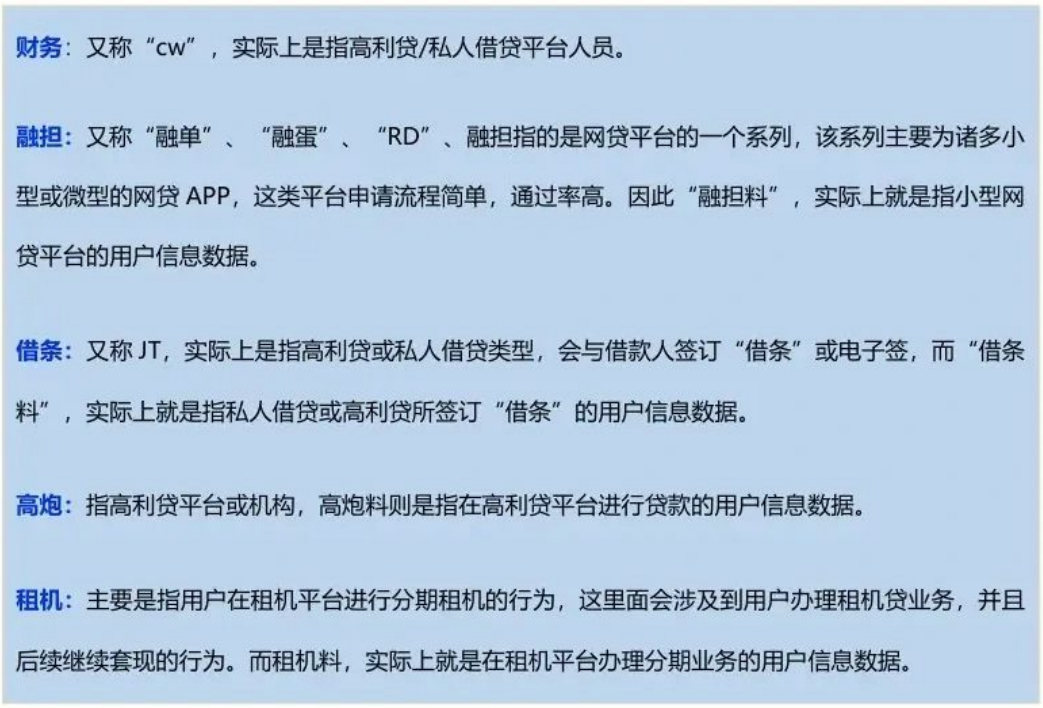
Appendix: Interpretation of relevant black phrases (Chart 1)

Source: Threat Hunter original report, page 30

English figure labels

1	SHE+ Cell phone
2	Validation of civil decisions in cyber data
3	No arrears, no complaints and no poverty applications.
4	Stable return receipt.

威胁猎人针对“多头借贷”相关风险情报进行了深度调研与跟踪，以下是与“探针”相关的黑产常用黑话词汇释义



Appendix: Interpretation of relevant black words (Chart 2)

Source: Threat Hunter original report, page 30

English figure labels

1	Threat Hunter to carry out in-depth research and follow-up on risk information related to multiple lending.
2	Commonly used terminological interpretations
3	Finance: MER "cw", in practice, refers to loan/private lending platform personnel.
4	RD', burden is a series of web-based lending platforms, mainly small
5	Type or micro-based web-based app, such as a simple application process and high pass rate. So, "breed" is actually a small net.
6	User information data for loan platforms.
7	Borrowing: Also referred to as tasting, which in fact refers to the type of loan loan or private lending that is “loaned” or electronic signature with the borrower and “loaned”
8	In practice, this refers to user information data on “loan notes” signed by private lending or usury.
9	Artillery: refers to a loan platform or institution, while artillery is used to refer to user information data on loans made on loan platforms.
10	il: primarily refers to the conduct of the user in the leasing platform, which involves the user in the leasing of the aircraft, and
11	Follow-up action continues. The lease of aircraft is, in fact, the user information data for a phased operation on the leased platform.

Renting: Mainly refers to the behavior of users renting machines in installments on the rental platform, which will involve users handling the rental business and continuing to cash out. The rental information is actually the user information data used for installment business on the rental platform.

Gold: The full name is Gold Mall. It is similar to the data on renting and cashing out. It is actually some platforms that can support the purchase of gold and repay it in installments. They are usually small platforms. The gold mall materials are the user information data of cashing out on these platforms.

E-Card/Card Voucher: Similar to the situation of rental aircraft and gold malls, some platforms that support the purchase of E-cards or card-voucher red envelopes and allow installment repayment are generally small platforms, and E-card materials are user information data for cashing out purchases on these platforms.

3.2 Bank “scan QR code application” loan information leakage trend and industry ecology analysis

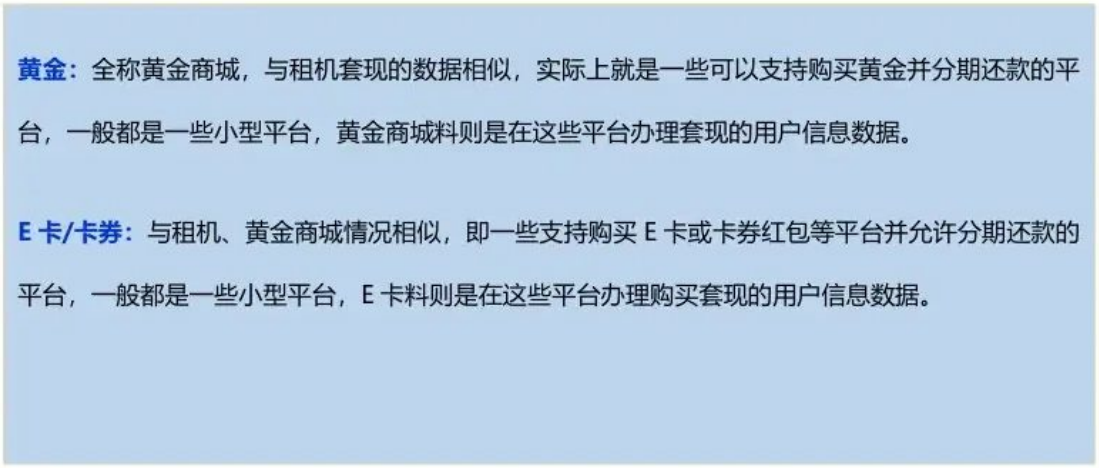
3.2.1 Bank “scan QR code application” loan information leakage incidents have increased significantly compared with the second half of 2024, with an increase of more than 4 times

Threat Hunter's continuous monitoring found that among the leaked data captured in the first half of 2025, there was another type of loan information leakage incident called "bank code scanning application materials", with a total of 111 cases, compared with 89 new cases in the second half of 2024, an increase of 404.55%.

Bank code scanning application: refers to information data for users to apply for loan business by scanning the loan activity QR code provided by the bank account manager.

Through in-depth analysis, Threat Hunter learned about the so-called "scan code application overnight" data among threat actors, which mainly focuses on bank "loan" business. It mainly includes information such as the phone number of the loan user, city area, and loan application approval results; at the same time, according to the screening of the bank loan platform provided by threat actors, there are more than 80 bank loan businesses, basically local banks or commercial banks.

(The picture on the left shows the leaked data format, and the picture on the right shows threat actors officially launching the “scan QR code overnight application” data product)



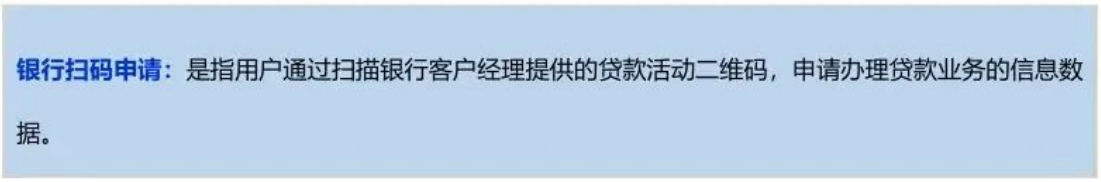
The leaking of bank's “sweep application” loan information increased significantly, by more than four times, compared to the second half of 2024 (Chart 1)

Source: Threat Hunter original report, page 31

English figure labels

1	Gold: Full-name gold mall, similar to the data available on leased aircraft, is actually a flat amount that can support the purchase of gold and be repaid in instalments
2	The stations, which are usually small platforms, are used to generate user information data.
3	E-cards/cards: Similar to leasing machines, gold malls, some that support the purchase of platforms such as E-cards or coupons and are allowed to pay in instalments
4	Platforms, usually small platforms.
5	E-cards are used to purchase off-the-shelf user information data on these platforms.

请科”的贷款信息泄露事件，共计 111 起，相较于 2024 年下半年新增 89 起，环比同达 404.55%。



The leaking of bank's “scanning application” loan information was significantly higher than in the second half of 2024 and more than four times higher (figure 2)

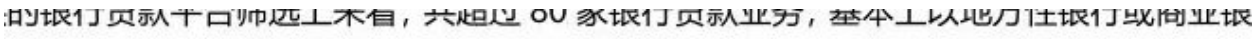
Source: Threat Hunter original report, page 31

English figure labels

1	From four to six.
2	Bank scanned applications: refers to the number of users applying for loan operations by scanning the two-dimensional code of loan activity provided by the bank ' s client manager

3.2.2 Bank “scan QR code application” loan information leaked: third-party financial technology company marketing tools become

The core risk point is related to more than 80 banking institutions. Threat Hunter analyzed and traced the bank QR codes involved in the leaked data and found that they all pointed to the "xx Marketing Assistant" platform developed by the same well-known financial technology service provider. Based on the list of bank loan platforms released by threat actors, it can be confirmed that more than 80 banking institutions are affected.



手机号	贷款平台	province	city	姓名
1.815E+10		安徽	合肥	
1.816E+10		安徽	合肥	
1.776E+10		安徽	合肥	
1.776E+10		安徽	合肥	
1.309E+10		安徽	合肥	
1.308E+10		安徽	合肥	
1.586E+10		安徽	合肥	汪
1.788E+10		安徽	合肥	
1.331E+10		安徽	合肥	许
1.396E+10		安徽	合肥	
1.526E+10		安徽	合肥	董
1.866E+10		安徽	合肥	张
1.361E+10		安徽	合肥	王
1.538E+10		安徽	合肥	仇
1.334E+10		安徽	合肥	王
1.387E+10		安徽	合肥	彭
1.596E+10		安徽	合肥	陈
1.591E+10		安徽	合肥	

The leaking of bank's “scanning application” loan information was much higher than in the second half of 2024 and more than four times higher.

Source: Threat Hunter original report, page 32

English figure labels

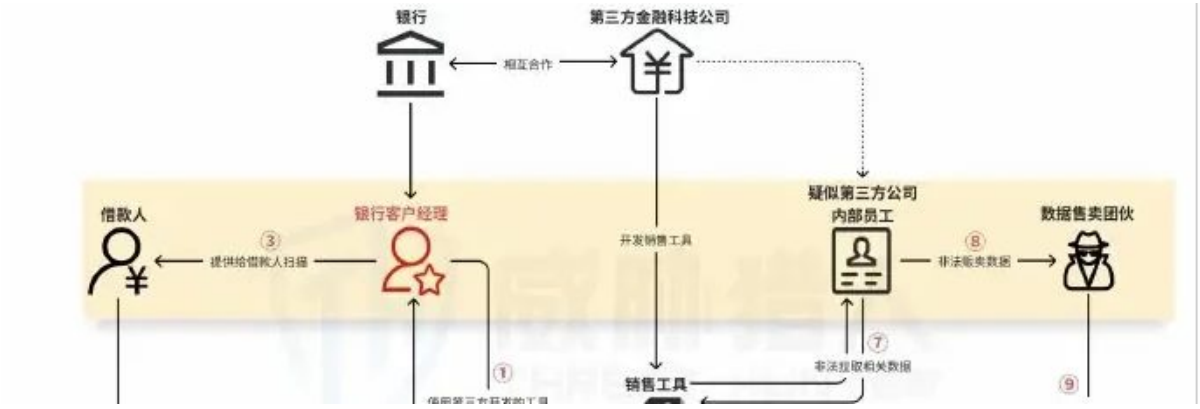
1	J.J. A.A. 4a. 6 ISN ALT
2	Anhui.
3	Yeah.
4	Fatty.
5	□ One □
6	It's fat.

(Flow chart of bank loan application information leakage)

Based on the fact that this type of related incident involves multiple banks, Threat Hunter conducted an in-depth restoration of the specific details and found:

1. In the process of applying for a loan, the user scans the QR code of the loan business activity provided by the bank account manager;

2. The QR code information for this type of bank loan business carries the customer manager information to jump to the bank’s official mini program;



Disclosure of bank's “sweep application” loan information: third-party financial technology company marketing tools

Source: Threat Hunter original report, page 33

English figure labels

1	Third-party financial technology companies
2	One-one.
3	Suspected third-party companies
4	Internal staff
5	Data sales group

3. Then the user operates on the specific loan business of the bank’s official applet and submits a loan application;

Threat Hunter learned that the loan QR code information provided by the account manager was actually produced through a sales tool developed by a third-party financial technology company. (Because the tool page is relatively sensitive, it will not be shown in detail here)

Threat Hunter analyzed this third-party financial technology company and found that the company not only provides application system software development for banks, but also provides intelligent fraud-control strategies. Provide different fraud-control strategies for loan users with different qualifications to cooperate with bank account managers for follow-up. It mainly provides business digitization for banks and promotes the development of bank loan business. After a user submits a loan application in the bank's official mini program, the bank will synchronize the user's relevant information to the sales tool to facilitate performance statistics and follow-up by the bank's account manager. At the same time, it also brings the risk of data leakage.

(threat actors publish information on materials required for users to apply on different bank loan platforms, as well as differences in the amount of data on different platforms in different cities and regions)

After a user submits a loan application in the bank's official mini program, the bank will synchronize the user's relevant information to the sales tool to facilitate performance statistics and follow-up by the bank's account manager. At the same time, it also brings the risk of data leakage.

According to Threat Hunter's follow-up and analysis of the information released by threat actors, it was found that when this type of incident began to be publicized, threat actors claimed that the data came from "insiders", that is, internal employees leaked it. Considering that more than 80 banking institutions are involved in the above, the probability of leakage by internal employees of 80 banking institutions is extremely low, and it is initially inferred that they are internal employees of third-party financial technology companies.

According to research by Threat Hunter, after such information and data are leaked to the illegal data trading market, they are mainly used to assist loan companies in targeted marketing. At the same time, according to the feedback from threat actors after marketing, the effect is very good, with a success rate of up to 20%, which also proves the authenticity of such data.

Risks and Hazards:

Customer churn and revenue loss: High-intention customers are contacted by competitors (loan assistance companies) on the day after application, offering alternative products with lower interest rates or faster approvals, which directly leads to the loss of potential customers of the bank and the loss of predictable interest income and intermediate business income.

Disclosure of bank's “sweep application” loan information: third-party financial technology company marketing tools

Source: Threat Hunter original report, page 35

English figure labels

1	Six.
2	One.

Brand reputation damage: Data leakage has seriously damaged users' trust in the bank's data security capabilities, especially in the core business of lending, and will have a long-term negative impact on the bank's brand. "Regulatory compliance risk: Such incidents have constituted a serious leak of personal financial information and violated the "Personal Information Protection

Law" and other relevant regulations. Banks, as data processors, will face the risk of high fines and regulatory accountability.

Threat Hunter data breach risk intelligence service

4. Threat Hunter data leakage risk intelligence service

To sum up, the data leakage risk landscape remains severe in the first half of 2025, the overall incident volume continues to run at a high level, the industrial chain is highly mature and has strong "self-healing capabilities"; platform crackdowns are difficult to fundamentally curb market activity.

Faced with such a severe situation, enterprises need to comprehensively improve their ability to identify and respond to risks, understand the details of risk events, including verifying the authenticity of risks, promptly trace the source, handle removal and follow up on potential risks, and enhance the timeliness of data leakage risk monitoring and early warning, etc.

In this regard, Threat Hunter provides targeted solutions:

Threat Hunter data leakage risk monitoring service, through real-time monitoring and in-depth mining of multi-channel intelligence across the entire network, and based on the risk authenticity verification engine and manual data verification, provides 7x24-hour real-time warning of data leakage risks, and links emergency response mechanisms to minimize harm and losses.

1. Network-wide intelligence monitoring and mining: covering dark web, anonymous group chat, network disk library, code hosting platform and other channels, from different dimensions

Continue to improve the comprehensiveness of channel coverage, including the continuous discovery and update of new channels, special mining of deep intelligence sources (Deep Source), and multi-lingual channel coverage.

2. Accurate early warning of data leakage risks: Based on the monitored transaction data of threat actors, the risk authenticity verification engine + manual data verification

Certification services provide comprehensive credibility assessment results to help enterprises accurately perceive risks and handle risks in a timely manner.

1 Risk authenticity verification engine: Verify risk authenticity based on three elements: "source confidence factor, three-factor matching factor, and historical coincidence factor";

2. Manual data verification service: further help enterprises accurately perceive risks through secondary verification, active verification and other methods.

3. "7×24" emergency response: Establish a DRRC risk emergency response center to monitor enterprise-related risk information around the clock,

Audit and early warning, providing "7×24" sample acquisition, intelligence mining, assistance in traceability, processing and removal services, etc., while also providing monthly data leakage risk monitoring reports and typical risk event analysis results.

Company official website: www.threathunter.cn Cooperation email: Marketing@threathunter.cn

IV. TRANSMITTING TRADITIONAL INDUSTRIAL SERVICES FOR TRANSMITTING TRADITIONAL DATA (Figure 1)

Source: Threat Hunter original report, page 39

English figure labels

1	DRRC professional team provides 7*24-hour emergency response service
2	Chongqing, Shenzhen, two DRRRC professional teams, provide 7'24,365 days of full emergency response
3	Validation of early warning
4	Monthly report
5	We'll take care of it.

IV. TRANSMITTING TRADITIONAL INDUSTRIAL SERVICES FOR TRANSFER DIGITAL DATA (Chart 2)

Source: Threat Hunter original report, page 39

English figure labels

1	Threat Hunter to establish a well-developed system of management of risk intelligence services, providing 7'24-hour professional services to businesses.
2	Human intelligence deterrent team structure
3	Data source operating team
4	Data Analysis Team
5	DRRC Emergency Response Services Team
6	Service quality management team