THREAT HUNTER RESEARCH

# 2025 Data Breach Risk Landscape Report

A 2025 landscape of verified data exposure, changing illegal-trading channels and emerging financial and messaging risks.

Original publication: 2026-01-26
Research team: Threat Hunter Research Team
Source report: 48 pages

# Original report text

This text version is reconstructed based on the 48-page original PDF, retaining the report narrative, chapters and research scope; the cover, repeated 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

Data breaches will continue to occur at a high level in 2025. threat actors have comprehensively upgraded their organizational forms, attack paths, and data transaction methods, and high-value financial data has become the core target. Based on the continuous monitoring and analysis of data leakage incidents throughout the year, Threat Hunter released the "2025 Data Breach Risk Landscape Report", which systematically analyzes data leakage trends, scenario changes and illegal data transaction links throughout the year, and comprehensively reflects the overall domestic data leakage risk landscape in 2025.

务支持。截至目前，公司已为金融、政务、物流、互联网、科技、零售等行业的 300 多家客户提供安全服务，覆盖 85%头部互联网企业，每年帮助客户减少数十亿资金损失。


**Original report charts, processes and cases**

Source: Threat Hunter original report, page 2

Summary of key points in the report:

1. Data leakage incidents continue to be at a high level, with the banking industry’s data leakage risk ranking first for three consecutive years:

A total of 41,644 effective data breaches were detected in 2025, a year-on-year increase of 10.83%. The risk of data leakage in the banking industry has ranked first for three consecutive years. Among the top five industries with leakage incidents, the pan-financial sector (banking, consumer finance, payment, securities) occupies four seats, indicating that the focus of threat actors' attacks is on capital flow data with high realizable value.

2. The threat actors organization is moving toward "federalization", interoperability of resources, and multiple blackmail attacks:

In 2025, threat actors showed an obvious trend of organizational integration, such as the emergence of the SLH Alliance (composed of Scattered Spider, Lapsus$, and ShinyHunters). Attack methods are systematically shifting from traditional vulnerability exploitation to voice phishing (Vishing)

Supply chain attacks driven by identity abuse and malicious OAuth integrations.

3. The illegal trading market showed great resilience, and traffic migrated rapidly after the collapse of the leading forum:

Although global law enforcement agencies have repeatedly cracked down on the leading darknet forum BreachForums (BF) in 2025, the traffic of threat actors has not disappeared, but has rapidly migrated to alternative platforms such as D**s and anonymous group chats. The illegal data trading market has strong adaptability and self-repair capabilities.

4. High-value financial data is refined and split, and algorithm models improve monetization efficiency:

Financial data transactions accounted for more than 50% of the data leakage incidents involving threat actors, in which loan information was highly refined into various product forms such as "finance application", "bank code scan", "lease materials" and so on. At the same time, threat actors began to introduce AI big data recognition and algorithm models to clean, quality control and profile segmentation of the original data to maintain high prices and high conversion rates.

5. New trend in SMS data leakage risk, 106 expansion code has become a new leakage entrance.

The 106 expansion code data leakage involves multiple industries and affects more than 420 companies. In addition, threat actors circumvent the company's traceability and evidence collection through artificial splicing and unified formats.

Data breach risk landscape 2025

# 1. Overview of data breach risks in 2025

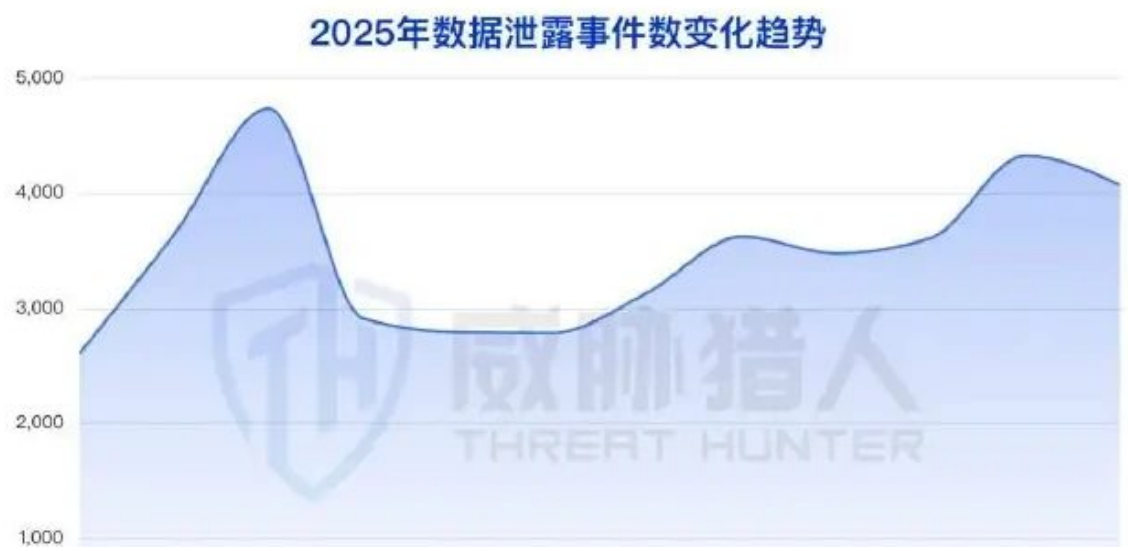
## 1.1 A total of 41,644 data breaches occurred in 2025, which is 41,644 cases compared with 2024.

A year-on-year increase of 10.83%. Threat Hunter data leakage risk monitoring platform data shows that from January to December 2025, the entire network monitored 767 million pieces of intelligence about data leakage. Based on the Threat Hunter authenticity verification engine and DRRC professional manual analysis, a total of 41,644 valid data leakage incidents were verified, involving a total of 2,120 companies in key industries such as finance, e-commerce, and express delivery.

The annual data in this report does not include some overseas and unidentified corporate entities' data leakage incidents. The statistical caliber has converged compared with the first half of the year, and the changes in relevant indicators are mainly caused by this.

As shown in the figure above, the magnitude of data breach events in 2005 fluctuated to varying degrees in Q1, Q2, and Q4. The main reasons are as follows:

- February-March 2025: The activity of illegal data trading gangs monitored by Threat Hunter increased, and the number of gangs increased by 116.96% compared with January, driving the increase in data leakage incidents.




**The total number of data leaks in 2025 was 41644 compared to the full year of 2024**

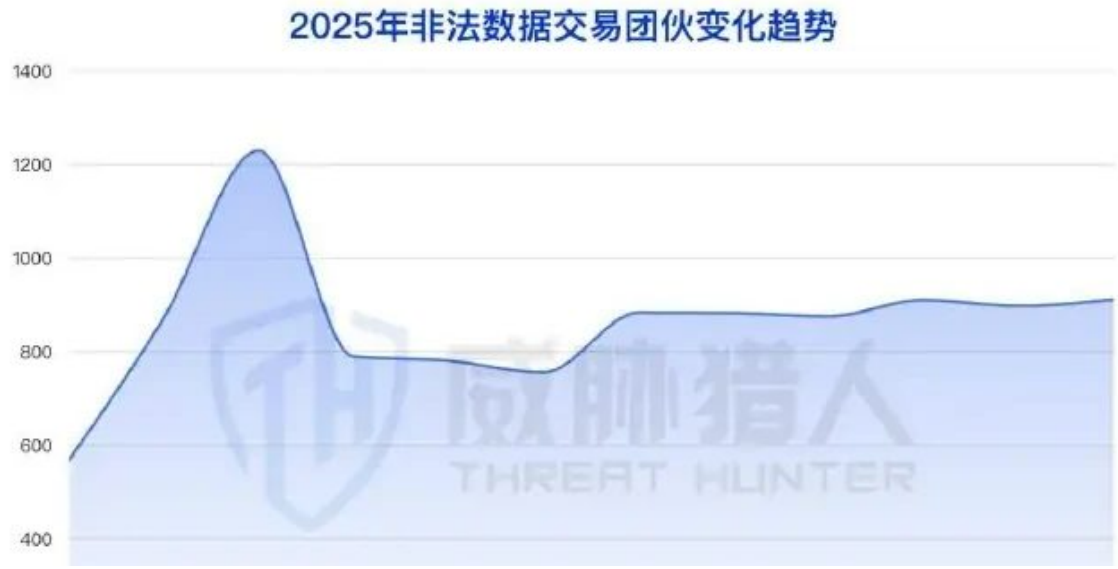
Source: Threat Hunter original report, page 7

- April 2025: Threat Hunter detected a significant decrease in the number of data leakage incidents. 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 a large number of illegal data transaction group chats being blocked; the number of data leakage incidents fell briefly.
- November 2025:: Affected by the concentrated promotion of the e-commerce shopping festival, a large number of leaked data related to the e-commerce industry appeared in leading dark web forums; the number of incidents related to dark web channels in November increased by 173.95% compared with October, becoming an important factor in pushing up the number of data leakage incidents in November.

## 1.2 The banking industry has ranked first in data leakage risk for three consecutive years, and the software application industry has ranked among the top 10 for the first time.

### 1.2.1 Risks in the financial industry are leading in a "faulty" manner

In 2025, the areas hardest hit by data breaches will further concentrate on capital-intensive industries. Data leakage incidents in the banking industry remain at the top of the list. Compared with 2024, the consumer finance industry has overtaken the e-commerce industry and jumped to second place. At the same time, the rankings of the payment and securities industries have moved significantly forward, entering the Top 4 and Top 5 respectively. The "pan-financial" sector occupies four of the top five high-risk industries, indicating that threat actors have focused their attacks on credit and capital flow-related data with high realizable value.




**The total number of data leaks in 2025 was 41644 compared to the full year of 2024**

Source: Threat Hunter original report, page 8

## 1.2.2 The intelligence on “strong access” to local life has dropped significantly, and software applications have replaced local life as a new target.

According to Threat Hunter monitoring, the "forced login" file checking data leakage incidents that were relatively active in the local life industry in 2024 dropped significantly in 2025, with the number of related incidents declining by 61.38% year-on-year; the focus of attacks by upstream illegal data acquirers began to shift, focusing more on mobile user behavior data with dynamic value, such as in-app interaction behaviors, location and trajectory information, etc.

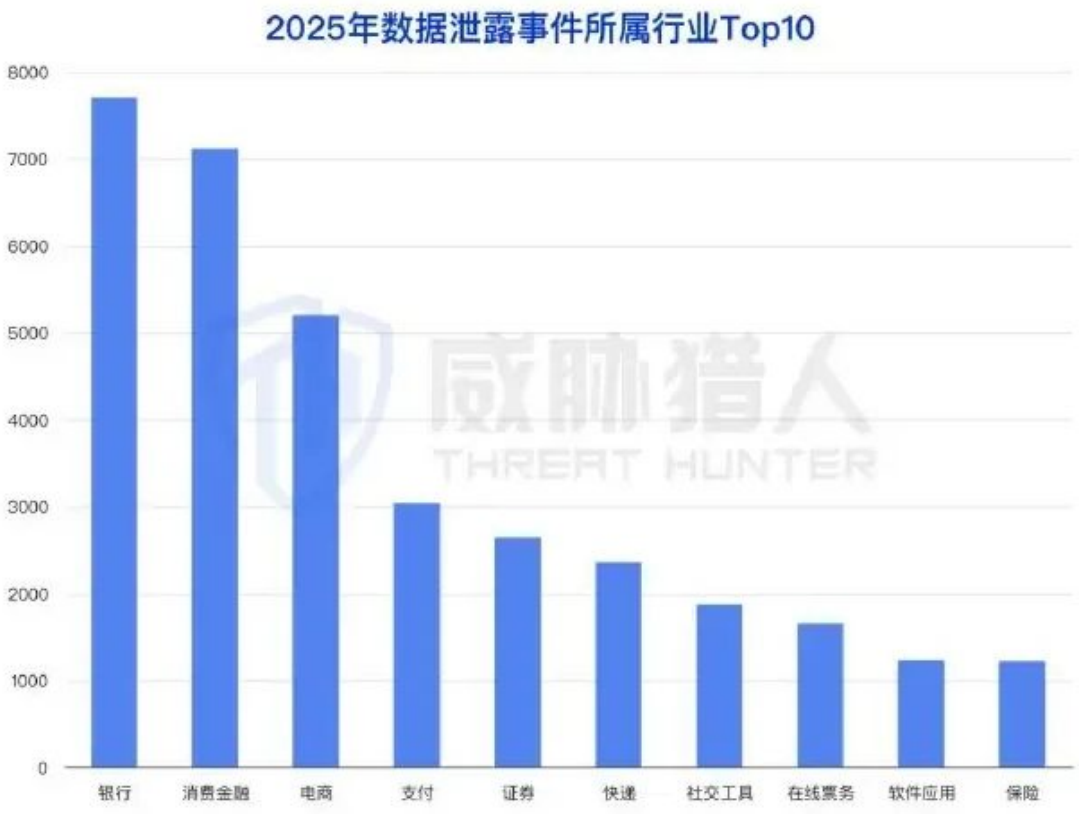
## 1.3 Overview of data leakage channels

According to Threat Hunter 2025 monitoring platform data statistics, anonymous group chats and dark web are still the main channels for data leakage, accounting for 88.77% of the total. The entire illegal data trading market shows a highly concentrated trend.

ApiTools: refers to API tool station/interface documentation station/online debugging and other platforms

Data breach risk landscape 2025

# 2. Changing trends of illegal data trading scenarios in 2025



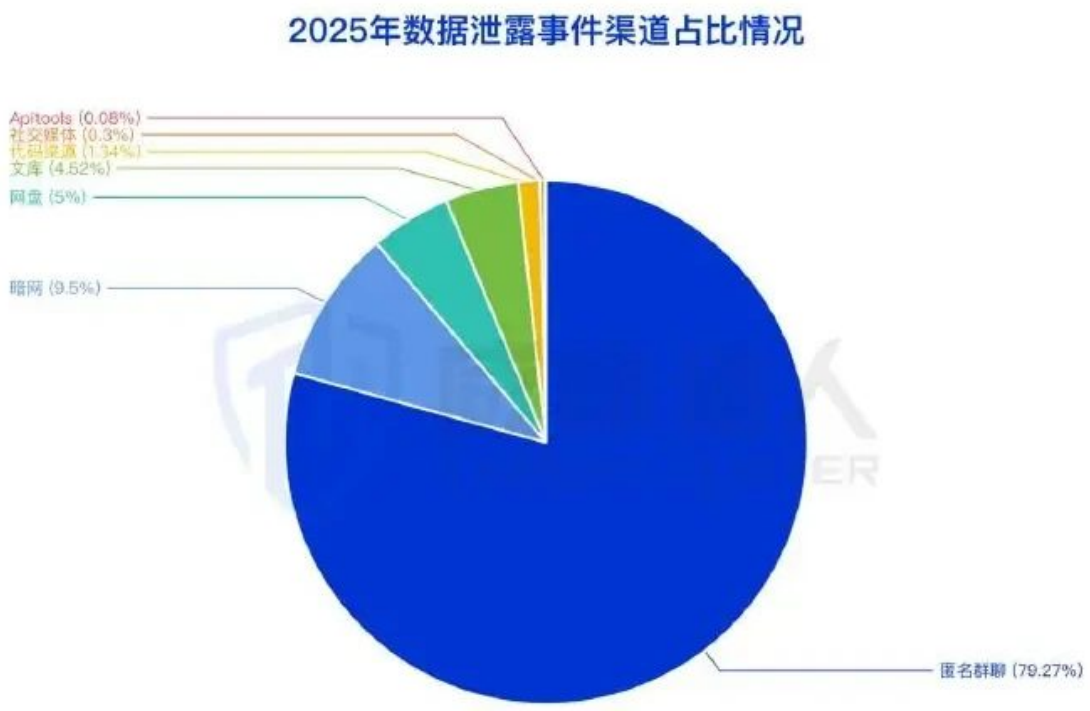

**Local life's "Johnden" intelligence has dropped dramatically, and software applications have replaced local life as a new target. Points**

Source: Threat Hunter original report, page 10

## 2.1 Blackmail gangs are moving towards federalization

### 2.1.1 From "fighting individually" to "organizational integration": the emergence of Scattered Lapsu$ Hunters

In the past few years, the upstream chain of data leakage has increasingly taken the form of "division of roles and on-demand collaboration": from intrusion to data theft and extortion, different links are usually completed by different groups or individuals, and transactions and collaboration are mainly completed through darknet forums and intermediaries (IABs, RaaS operators, affiliates, and data brokers work independently).




**Overview of data leak channels**

Source: Threat Hunter original report, page 11

- IAB (Initial Access Broker): IAB is mainly responsible for obtaining and reselling the initial access rights into the target system or network environment; including account credentials, VPN/RDP/SSO sessions, and established internal access points, providing a starting point for subsequent attack activities.
- RaaS operator (Ransomware-as-a-Service operator): RaaS operator provides ransomware tools, attack infrastructure, and sharing mechanism in a platform-based manner, recruits and manages agents (Affiliates) to implement intrusion, encryption, and extortion behaviors, and serves as the organization and dispatching center for attack capabilities.
- Affiliate (Raas agent/executor): Affiliate is the role responsible for "implementation execution" in the RaaS ecosystem. It usually enters the victim environment after obtaining or purchasing initial access, completes penetration expansion, data theft/external transmission and encrypted delivery, and shares revenue with it according to the rules of the RaaS operator.
- Data Broker: Data broker is the role of reselling data; transaction objects include database exports, internal documents, customer or employee information, mailbox contents and various access tokens, etc., providing a data basis for fraud, extortion or resale and realization.

Its basic ransomware collaboration operation link is as follows:

This pattern has changed significantly in 2025, and extortion gangs have begun to move toward federalization.

On August 8, 2025, a Telegram channel called "Scattered Lapsu$ Hunters – The ComHQ SCATTERED SP1D3R HUNTERS" was launched, officially announcing the cooperation of three well-known cybercriminal organizations.

The alliance is composed of the following three major groups:

- Scattered Spider
- Lapsus$
- ShinyHunters This is a cybercriminal group motivated by economic interests and centered on social engineering and identity abuse. Its operating model is the Federated federal model; it is regarded by the research community as an important signal that cybercrime has entered the "federalization".

Federated cybercrime model: refers to the fact that multiple relatively independent criminal groups do not need unified command, but operate externally under a common brand; they share/reuse some resources (such as leakage channels, social engineering scripts, infrastructure, and pressure processes) on demand to expand their influence and monetize in the form of collaboration.

## 2.1.2 Changes in attack strategy after integration

After SLH officially merged in early August 2025, in just over 4 months, it has publicly claimed to have attacked more than 300 companies and stolen hundreds of millions of data assets, involving many heavyweight targets, including Salesforce, CrowdStrike, Red Hat, etc.

The most significant change after its merger is the change in attack strategies: social engineering and supply chain attacks are systematically replacing traditional vulnerability attacks.

1. Identity and permission abuse: high-privilege account utilization driven by voice phishing

- Jaguar Land Rover (JLR) blackmail incident (August–September 2025)

By using a voice phishing scam to impersonate an internal employee to gain help desk support (either to reset or grant permissions), SLH compromised high-privileged administrator accounts and used those accounts to access and deploy ransomware against every aspect of Jaguar's business, from CAD and engineering software to payment tracking to customer car deliveries. As a result, JLR's global IT network was taken offline and many factories were shut down for several weeks. It was called "one of the most serious cyber attacks in British history" by the media. Later, its extortion gang mocked Jaguar Land Rover in the Telegram channel. After announcing the IT security breach of India's Tata Motors, the stock price began to fall slightly. Subsequently, more data sample information and project documents were released.

This incident presents a typical crypto-ransomware model: shutting down IT systems □ halting production □ causing a direct and quantifiable blow to the core business.

2. Authorization and Trust Abuse: Voice Phishing Drives Malicious Oauth Integrated Supply Chain Attacks

OAuth is an "authorization mechanism" that allows third-party applications to access your data according to agreed permissions without handing over your account and password.

Salesforce and Salesloft ransomware incident (October 2025)

In a massive SLH attack targeting Salesforce customers, according to the attackers:

联邦式（Federated）网络犯罪模式：指多个相对独立的犯罪团体不必统一指挥，而以共同品牌对外行动；按需共享/复用部分资源（如泄露渠道、社工剧本、基础设施与施压流程），以协作形式扩大影响与变现。

**Changes in post-join attack strategy (Chart 1)**

Source: Threat Hunter original report, page 15

嘲讽捷豹路虎在宣布印度塔塔汽车的 IT 安全漏洞后，股价开始出现小幅下跌。随后又公布了更多的数据样例信息以及项目文档。


**Changes in post-merger attack tactics (Chart 2)**

Source: Threat Hunter original report, page 15

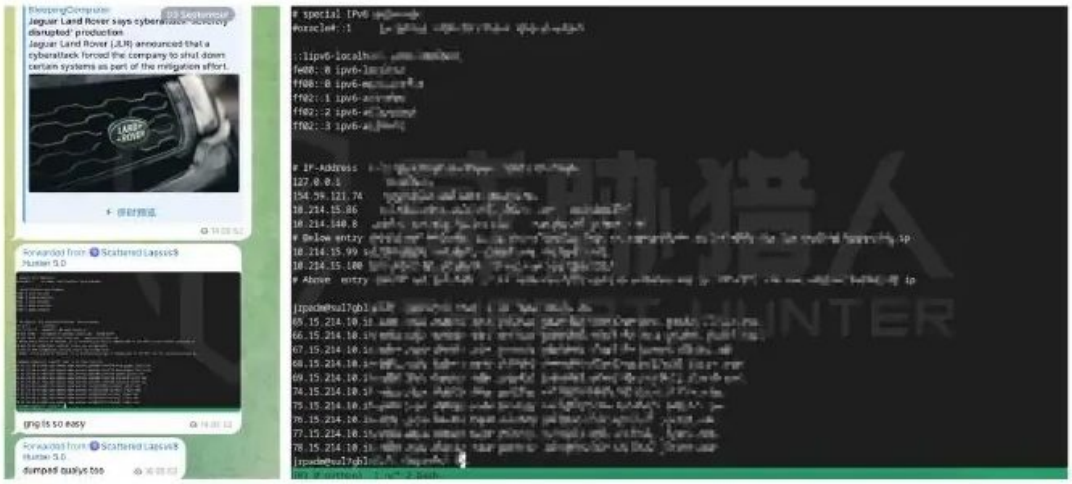
- About 760 Salesforce tenants were compromised
- 1.5 billion records were stolen This attack can be divided into two types of actions:

One type is a voice phishing attack that targets Salesforce customers directly. Attackers impersonate official support or operations personnel over the phone and induce enterprise users to connect so-called "data loader" applications to their Salesforce tenants. The application appears to be a normal data management tool, but is actually a malicious OAuth application controlled by the attacker. Once the user completes authorization, the attacker can continue to export customer data on a large scale within the scope of legitimate API permissions.

The other type shows obvious characteristics of supply chain attacks. The attacker first compromised the GitHub account of a Salesloft developer through phishing methods, then penetrated his AWS environment and stole access tokens. Since Salesloft's official integrations (such as Drift) are widely deployed in environments such as Salesforce and Google Workspace, attackers can use these OAuth tokens to access a large number of downstream customer systems as "legitimate integrations" and simultaneously steal data. The attack path then spread further laterally into Gainsight, impacting hundreds of additional Salesforce instances.

(Pictured is a screenshot shared by a member of the channel, depicting an operator running an automated voice phishing tool and abusing Google Voice to amplify the scale of a social engineering attack.)

该事件呈现的是典型的加密勒索模式：通过关闭 IT 系统 → 停摆生产 → 对核心业务形成直接、可量化打击。



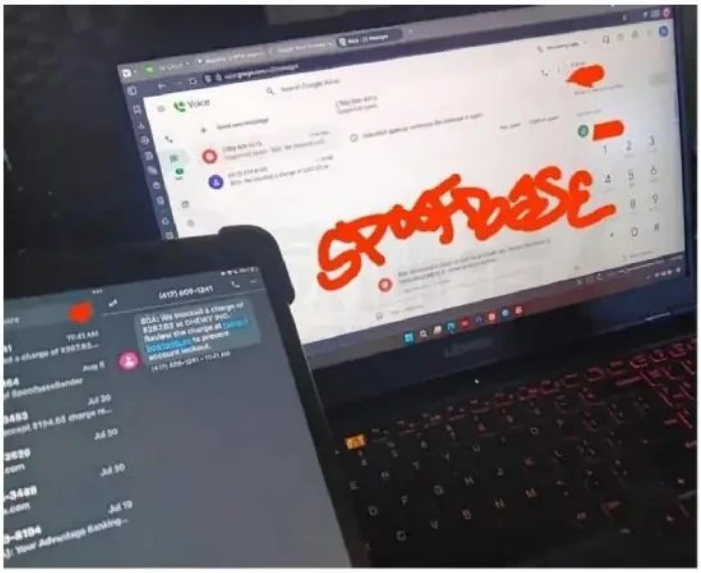

**Change of attack strategy after integration**

Source: Threat Hunter original report, page 16

## 2.2 The destruction of dark web forums and the migration of threat actors' traffic

In 2025, global law enforcement agencies launched multiple rounds and multi-dimensional attacks against the leading darknet forum BreachForums (BF).

另一类则体现出明显的供应链攻击特征。攻击者首先通过钓鱼手段入侵 Salesloft 一名开发者的 GitHub 账号，进而渗透其 AWS 环境并窃取访问令牌。由于 Salesloft 的官方集成（如 Drift）被广泛部署于 Salesforce 与 Google Workspace 等环境中，攻击者得以利用这些 OAuth 令牌，以“合法集成”的身份访问大量下游客户系统，并同步窃取数据。随后，攻击路径进一步横向扩散至 Gainsight，额外影响数百个 Salesforce 实例。




(图为频道中一位成员分享的屏幕截图)

**Change of attack strategy after integration**

Source: Threat Hunter original report, page 17

This series of actions not only severely damaged the platform, but also triggered a large-scale migration of threat actors.

## 2.2.1 Timeline of "Law Enforcement Strike" against BF Forum:

- Platform shutdown (April): On April 15, 2025, the BF forum was suddenly shut down. According to Threat Hunter monitoring data, the number of active illegal trading gangs on the platform plummeted from about 166 in April to zero in May.
- Judicial verdict (September): On September 16, the founder of BF was commuted to 3 years in prison by the US Department of Justice, establishing the results of the crackdown from a judicial perspective.
- Comprehensive seizure (October): On October 9-10, U.S. law enforcement agencies and France officially took over the BF clearnet domain name, and its Tor site was immediately taken offline.
- Statement from the operator (mid-October): The extortion gang ShinyHunters released a PGP signed message on Telegram, admitting that the BF backend server was seized and the database backup was destroyed, and reluctantly announced that "the forum era is over, and new forums that will appear subsequently should be regarded as honeypots."

( ShinyHunters publishes PGP signed message on Telegram)

## 2.2.2 The collapse of the BF forum did not lead to the demise of illegal transactions. threat actors moved to new platforms and continued to conduct malicious activity.

According to the trend chart monitored by Threat Hunter, as the overall activity of the BF platform has declined rapidly since April and is close to zero in May, the traffic and transaction demand of threat actors originally concentrated on the BF platform have not disappeared, but have rapidly migrated to multiple alternative darknet forums.

- Represented by the D**s platform, its activity has increased significantly since May, entered a high-growth range in June, and reached its annual peak in August-September, showing its ability to quickly accept the traffic and transaction needs of threat actors. Although the overall activity of the platform has declined after October, its operating level is still significantly higher than at the beginning of the year, indicating that the relevant demand for malicious purposes has been precipitated in alternative platforms, and a new trading "chassis" has gradually formed.

- 近言方声明（10 月中旬）：勒索团伙 ShinyHunters 在 Telegram 发布 PGP 签名消息，承认 BF 后端服务器被扣押且数据库备份被破坏，无奈宣布“论坛时代结束 ，后续出现的新论坛应视为蜜罐”。

（ShinyHunters 在 Telegram 发布 PGP 签名消息）

**"Law Enforcement Strike" Time for the BF Forum Line**

Source: Threat Hunter original report, page 18

Judging from the recovery situation of BF itself, Threat Hunter’s continuous monitoring data for the illegal BF gang shows:

From September to November, BF was in a state of zero for a long time and showed no signs of effective recovery. Until November 18, it was monitored that a new domain name that was highly similar to BF was registered. After GridinSoft website reputation analysis, the domain name was

marked as low trust and accompanied by a blacklist risk signal. Based on the fact that BF has publicly warned "be wary of clone sites and honeypot risks" many times in history, Threat Hunter determined that the new domain name has high risks of phishing, fraud or honeypot sites, and does not have the trustworthy characteristics of a stable trading platform.

After entering December, sporadic signs of activity from suspected BF clone sites were detected, further reflecting that some participants are still trying to restore or reuse the "BF Platform" as a trading entrance. However, due to concerns about "honeypot/phishing", its user return is more likely to be a small-scale test or low-frequency participation in the wait-and-see stage.

Based on the data for the whole year of 2025, the cybercrime ecosystem market shows strong ecological resilience: when leading platforms such as BF were continuously attacked, user and transaction demand did not disappear, but quickly migrated to existing/emerging alternative forums such as D**s, and maintained operation together with more decentralized channels (such as anonymous group chats).

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.

Data Breach Trading Market Research New Trends in 2025

# 3. New Trends in Data Breach Trading Market Research in 2025


**The collapse of the Forum has not led to the demise of the illegal trade and the diversion of cybercriminal groups to new platforms continues to cause corruption.**

Source: Threat Hunter original report, page 19

## 3.1 Financial, customized collection and social media data transactions are highly active, with financial transaction data accounting for over 50%

In the illegal data trading ecosystem, groups such as public groups play the role of "guarantors" in the threat actors chain. As the core hub of threat actors' transactions, these groups have accumulated massive transaction performance records, objectively reflecting the underground market's true demand for data and capital flows.

From January to December 2025, the Threat Hunter intelligence operations team continued to monitor public data trading groups on the Telegram platform, covering a total of 1,209 active data trading groups and capturing nearly 36,000 pieces of data transaction-related intelligence. The monitoring scope covers multiple industries such as loans, online shopping, stocks, logistics, e-commerce, and social tools.

From the perspective of transaction data types and their proportions, the data transaction types in the public group in 2025 will mainly focus on five major categories: financial data, customized collection data, social media data, logistics data and e-commerce data.

1. Financial user data is still the "hard currency" of the cybercrime ecosystem market due to its high monetization value. Loan user information has the greatest demand

It is booming, covering multiple segments such as online consumer finance loans, bank loans, corporate loans and loan supermarkets, and continues to dominate the market.

2. Customized data collection: The demand side shows a trend of "shifting from general to precise". Practitioners of threat actors no longer rely on common library sources;

Publish customized crawling and cleaning requirements for specific targets (such as specific official accounts, apps, and specific URL paths) to obtain more timely and accurate data.

3. Social/social media data: The collection targets are highly concentrated on domestic mainstream social software and short video content ecology. Among them, real-time interaction in the live broadcast room

Dynamic data and public account fan portraits have become key trading objects, reflecting the high attention of threat actors to private domain traffic and instant conversion.

4. Logistics data: Transactions focus on "gift list" logistics information and precise logistics data on high-net-worth female consumer groups.

5. E-commerce data: Domestic e-commerce data mainly consists of audience data and mainstream information on the "Black Five" sensitive products (weight loss, height gain, medical treatment, etc.)

The composition of shopping behavior data on e-commerce platforms.

Among them, financial transaction data accounts for more than 50%. Combining the results of the hot word map analysis of public group data transactions from 2024 to 2025 (high-frequency keywords include "loan", "provident fund", "insurance", "lease", etc.), it can be found that financial loan data has ranked first in transaction demand for two consecutive years. Based on the above monitoring results, Threat Hunter speculates that loan-related data leakage risks remained one of the major security challenges facing financial companies in 2026.

Further analysis from the transaction structure level shows that financial online loan data has been highly refined and split in the circulation process of threat actors, forming a variety of data product forms for different threat actors, such as "leasing machines", "financial guarantees", "finance applications", "IOUs", "incoming items", "multiple loans", etc., to adapt to the actual needs of different fraud scenarios and operation chains.

"Renting": refers to the user's behavior of renting an aircraft in installments on the rental platform, which involves the user's handling of the rental and loan business. "Aircraft rental information" refers to the user information data used by the rental platform to handle installment business.

"Rongdan": refers to a series of online loan platforms, mainly small or micro online loan apps. The application process is simple and the pass rate is high. "Rongdan material" refers to user information data of small online lending platforms.

企业面临的主要安全挑战之一。

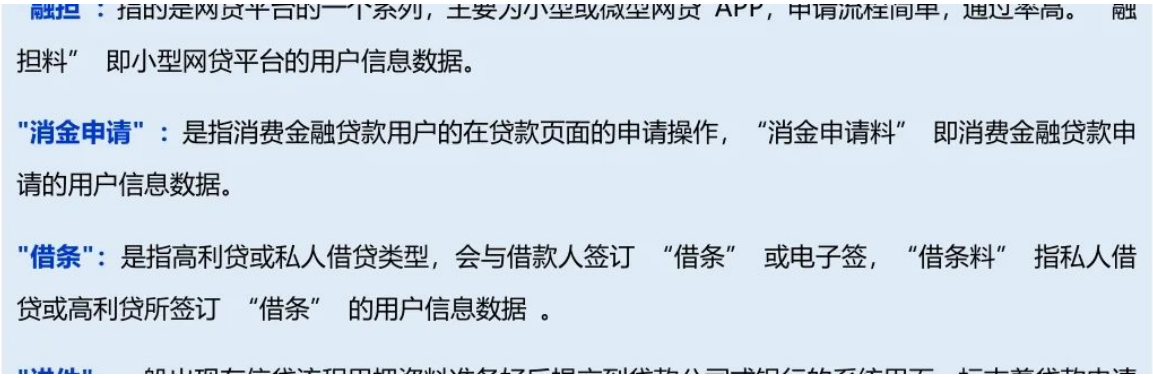

**Financial, customised collection and social media data transactions are highly active, with over 50 per cent of financial transactions**

Source: Threat Hunter original report, page 23

"Consumption finance application": refers to the application operation of consumer finance loan users on the loan page. "Consumption finance application materials" refers to the user information data of consumer finance loan application.


**Figure 1**

Source: Threat Hunter original report, page 24


融担 ：指的是网贷平台的一个系列，主要为小型或微型网贷 APP，申请流程简单，通过率高。 融担料” 即小型网贷平台的用户信息数据。

"消金申请" ：是指消费金融贷款用户的在贷款页面的申请操作，“消金申请料” 即消费金融贷款申请的用户信息数据。

"借条"：是指高利贷或私人借贷类型，会与借款人签订 “借条” 或电子签，“借条料” 指私人借贷或高利贷所签订 “借条” 的用户信息数据 。

**Figure 2**

Source: Threat Hunter original report, page 24

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

"Incoming documents": Generally occurs in the credit process, where the information is prepared and submitted to the loan company or bank's system, marking the official start of the loan application. "Incoming material" refers to the information submitted by the user for loan entry during the credit process.

"Multiple lending": refers to the borrower using the same set of real materials to apply for loans from multiple banks or private institutions at the same time to fill the funding gap.

In addition, in the field of credit risk management, "multiple borrowing" also refers to a fraud-control mechanism that specifically detects borrowers' "multiple borrowing" behavior, as well as the recorded information data of borrowers' long borrowings.

"Gao Pao": loan sharking platform or institution, "Gao Pao data" refers to the information data of users who make loans on the loan sharking platform.

## 3.2 Consumer loan user information leakage incidents continue to increase, and new leakage methods are diversified

Threat Hunter monitoring shows that illegal data trading incidents in the consumer finance industry showed a phased upward trend in time distribution in 2025.

From the beginning of the year to the first half of the year, the number of related incidents was generally at a low level and grew slowly; after entering the second half of the year, the number of incidents increased significantly, and reached a high point for the whole year from October to November.

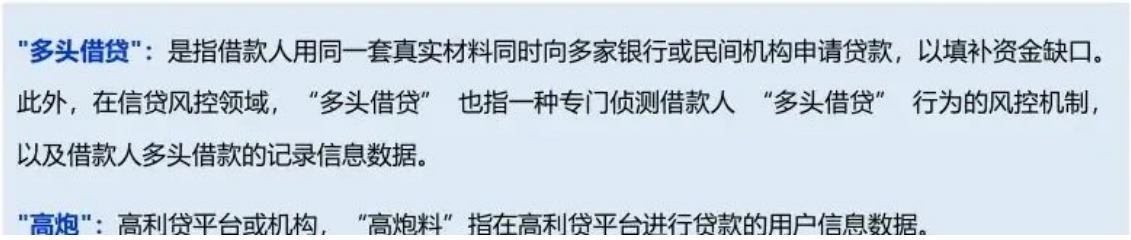
After in-depth analysis, Threat Hunter operators found that the increase in illegal consumer finance data transactions is mainly concentrated in several emerging data types.

In the list of "hot-selling data types" mentioned in the threat actors channel, data types such as "consumer loan application", "bank scan code" and "multiple loans" appear frequently. Especially the data of “Consumption Fund Application”;

Taking the hot-selling list updated weekly by an threat actors channel as an example, this type of data product has continued to rank among the top-selling products from August 2025 to December 2025, showing that it has formed a stable and active trading demand in the illegal data trading market. At the same time, usage feedback from downstream malicious activity scenarios also reflects the high value of this type of data in terms of authenticity and usability.

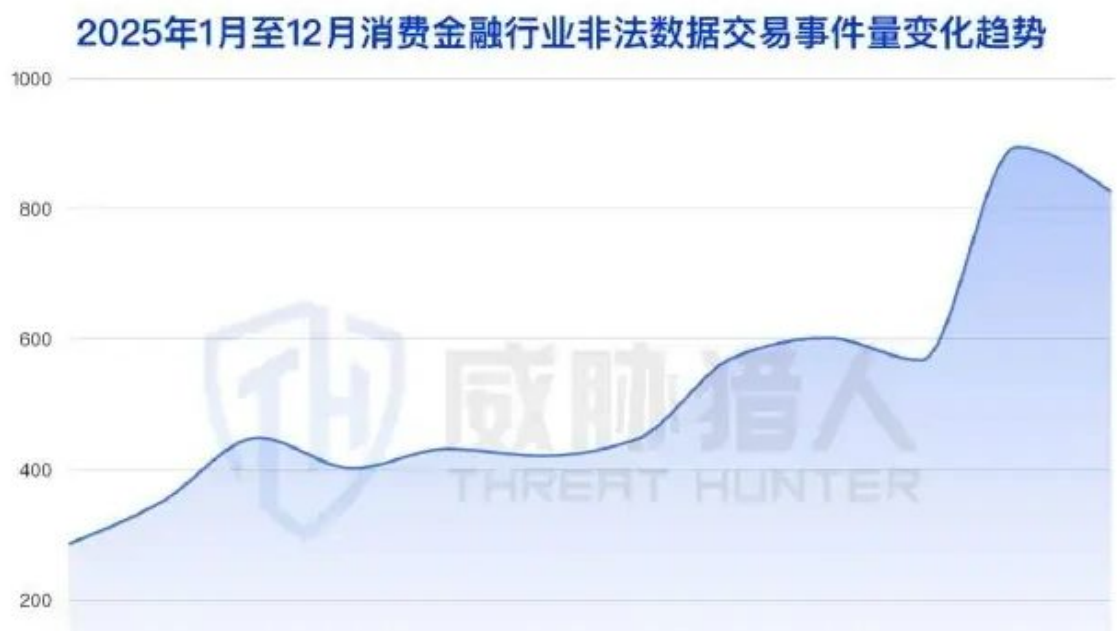
(In the hot-selling list of data types updated every week on the channel of an threat actors group, "consumer money application" data has long ranked first)

(Downstream malicious activity effect feedback reflects the authenticity of the data)




**There has been a steady increase in the incidence of information leaks from users of liquidating loans and the diversification of new types of leakage (Chart 1)**

Source: Threat Hunter original report, page 25




**There has been a steady increase in the incidence of leaks of information from users of liquidating loans and the diversification of new types of leakage (Chart 2)**

Source: Threat Hunter original report, page 25

## 3.2.1 “Consumer Financing Application” Risk Trends and Industry Ecology Analysis

### 3.2.1.1 Consumer loan application data leakage incidents continue to rise. In December, the number of incidents exceeded 600, accounting for 50% of illegal loan data transactions that month.

70%.

卖位列热销 Top，显示其已在非法数据交易市场中形成稳定且活跃的交易需求。同时，从下游作场景中的使用反馈也从侧面反映出该类数据在真实性与可用性方面具有较高价值。



（某黑产团伙频道每周更新的数据类型热销榜单中，“消金申请”数据长期高居第一）

**There has been a steady increase in the incidence of information leaks from users of liquidating loans and the diversification of new types of leakage (Chart 1)**

Source: Threat Hunter original report, page 26


**There has been a steady increase in the incidence of leaks of information from users of liquidating loans and the diversification of new types of leakage (Chart 2)**

Source: Threat Hunter original report, page 26

Threat Hunter monitoring found that "finance application" data first appeared in some illegal data trading channels at the end of May 2025. After about two months of tentative circulation by threat actors, it entered the large-scale dissemination stage at the end of July 2025 and was intensively promoted by multi-party data trading intermediaries. By December 2025, it reached a peak, accounting for 70% of illegal loan data transactions that month.

At the same time, judging from the changes in transactions and demand, the transaction volume of "finance application" data is highly consistent with the trend of purchase volume, and will simultaneously show explosive growth in the second half of the year.

According to Threat Hunter’s observation, the leaked “Consumer Fund Application” data mainly contains the following sample format fields:

User phone number, platform name, name, region, and status information of successful loan application. Name information is not included in all samples. Threat Hunter further followed up and learned that the name information appearing in some samples did not come from the original leaked data, but was artificially added by threat actors through data cleaning, splicing, or supplementary processing to improve the "usability" and transaction value of the data.

(The picture on the left shows the consumer finance application data format, and the picture on the right shows the feedback from threat actors that the name field was added for cleaning)

## 3.2.1.2 "Consumer Financing Application" product data is continuously iterated, involving most domestic consumer finance and loan platforms


**Discharge applications leaking data continues to rise, with over 600 incidents in December, accounting for illegal data transactions in the lending category of the month**

Source: Threat Hunter original report, page 27

Threat Hunter operators conducted an in-depth analysis of the "Consumption Fund Application" and found that the product data is mainly divided into four stages, namely the testing stage (May-June), official launch (July-August), refined operation (September-October), and AI model improvement stage (November). The following is the specific product development timeline.

(Consumption finance application product development timeline)

- Testing phase: (end of May - June)


**Discharge application data leaks continued to rise, with over 600 incidents in December, accounting for illegal data transactions in the lending category of the month (Chart 1)**

Source: Threat Hunter original report, page 28


**The incidence of data leaks from liquidation applications continued to rise, with over 600 incidents in December, accounting for illegal data transactions in the type of loans made during the month (Chart 2)**

Source: Threat Hunter original report, page 28

As early as the end of May 2025, threat actors first proposed a clear "consumer finance application" product. The data type involves some consumer finance platforms and bank loan platforms. The data timeliness is overnight (T+1). It does not support designated platforms, but it can support screening of users' regions. It only involves 24 licensed consumer finance institutions and bank loan products.

- Officially launched: (July-August)

In early July, new corporate loan type data was added, which is no longer limited to C-side loan demand users, and supplemented the information data of B-side or small and micro business owners; at the same time, it sorted out the behavioral characteristics of some users who applied on multiple loan platforms in a short period of time, and marked them as customers in urgent need of funds for downstream buyers to carry out precise malicious activity, involving 27 consumer finance/loan platforms.

(The picture shows that after threat actors officially launched consumer finance products, they added multi-platform tag features and model optimization)

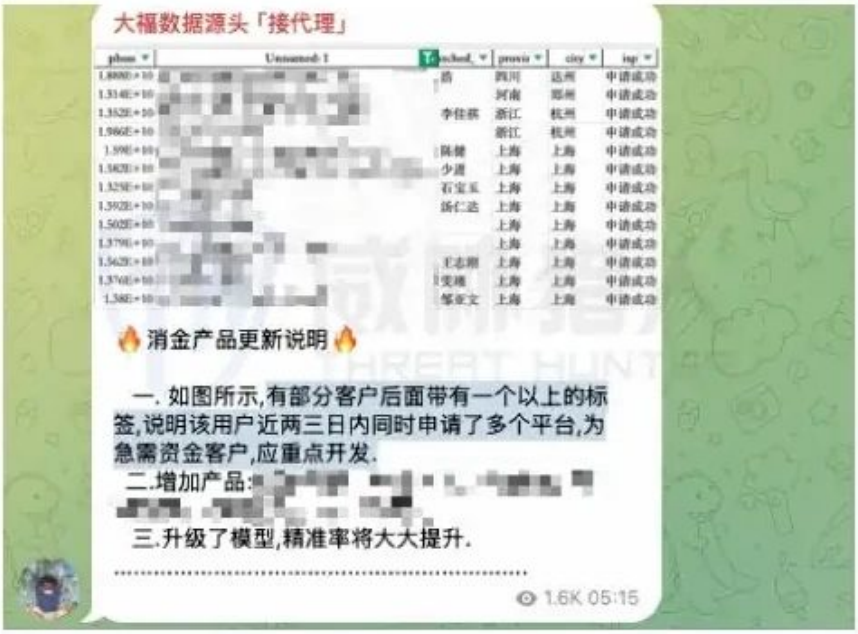
- Refined operation: (September-October)

Different types of platforms, such as licensed consumer finance institutions, bank loans, online loan platforms, and corporate loans, are divided and dismantled to meet the needs of different downstream loan intermediaries (capitals) for profiling malicious users; at the same time, the data

type involves a total of 40 consumer finance/loan platforms, supporting the screening of specific platforms.

(The picture shows the platform list carefully compiled by threat actors)

；同时梳理出部分用户在短时间内在多个贷款平台申请的行为特征，标记为急游购买者进行精准作恶，涉及消金/贷款平台达 27 家。




（图为黑产正式上线消金产品后，补充了多平台标签特征以及模型优化）

**The data on “exemption application” products continue to evolve, involving the vast majority of the country's eliminations, loan platforms**

Source: Threat Hunter original report, page 30

- Data intermediary threat actors use algorithm models to clean original data and improve data value (November)

In early November, illegal data trading threat actors reported that the volume of "consumer loan application" data transactions had reached a peak, causing the server memory to reach its limit, and targeted optimization and cleanup was carried out; involving up to 60 platforms for consumer loan, bank products, online loan products, and corporate loan products. At the end of November, AI big data recognition was introduced, shifting from pure data sales to "data cleaning + quality control", trying to maintain high data prices and high conversion rates by eliminating inferior user data.

(threat actors continue to optimize and upgrade the consumer finance application model)

Downstream malicious activity: After threat actors obtain the data, they will conduct targeted post-loan marketing for malicious purposes. Threat Hunter monitoring found that after threat actors obtain "consumer application" data, they mainly use it for highly targeted post-loan marketing. This type of malicious activity usually revolves around users who have "submitted loan applications" and implements misleading traffic and product promotion by pretending to be official or partner identities.

The following are two cases detected by Threat Hunter:


**The data on “exemption application” products continue to evolve, involving the vast majority of the country's eliminations, loan platforms**

Source: Threat Hunter original report, page 31

Case 1:

Judging from the "consumer finance sales test rhetoric" released by a data trading intermediary monitored by Threat Hunter, this rhetoric mainly involves pretending to be an account manager who has a cooperative relationship with the target consumer finance platform, contacting users who have submitted loan applications by phone, claiming that the user's loan or related business has been transferred to the user's responsibility, and then guiding the user to change loan products or accept other loan business promotions.

Case 2:

Judging from the content of the script that Threat Hunter obtained from a certain loan telemarketing group, this type of script mainly communicates with users by pretending to be staff of the customer follow-up department (or return visit department) of consumer loan platforms, such as loan qualification confirmation, and after gaining the user's trust, guides them to physical stores to promote other loan products.

## 3.3 Bank “scan QR code application” loan information leakage incidents continue to rise, and third-party financial technology company marketing tools have become a core risk point

### 3.3.1 Bank “scan QR code application” loan information leakage incidents continue to increase, reaching the peak in Q3 of 2025

In the first half of 2025, Threat Hunter monitoring found that a sharp increase in "bank scan code application" type events was captured (an increase of 404.55% compared to the second half of 2024), and the peak of this type of event intelligence occurred in Q3 of 2025, with a total of 274 bank "scan code scan application" type data leakage incidents discovered.


**The data on “exemption application” products continue to evolve, involving the vast majority of the country's eliminations, loan platforms**

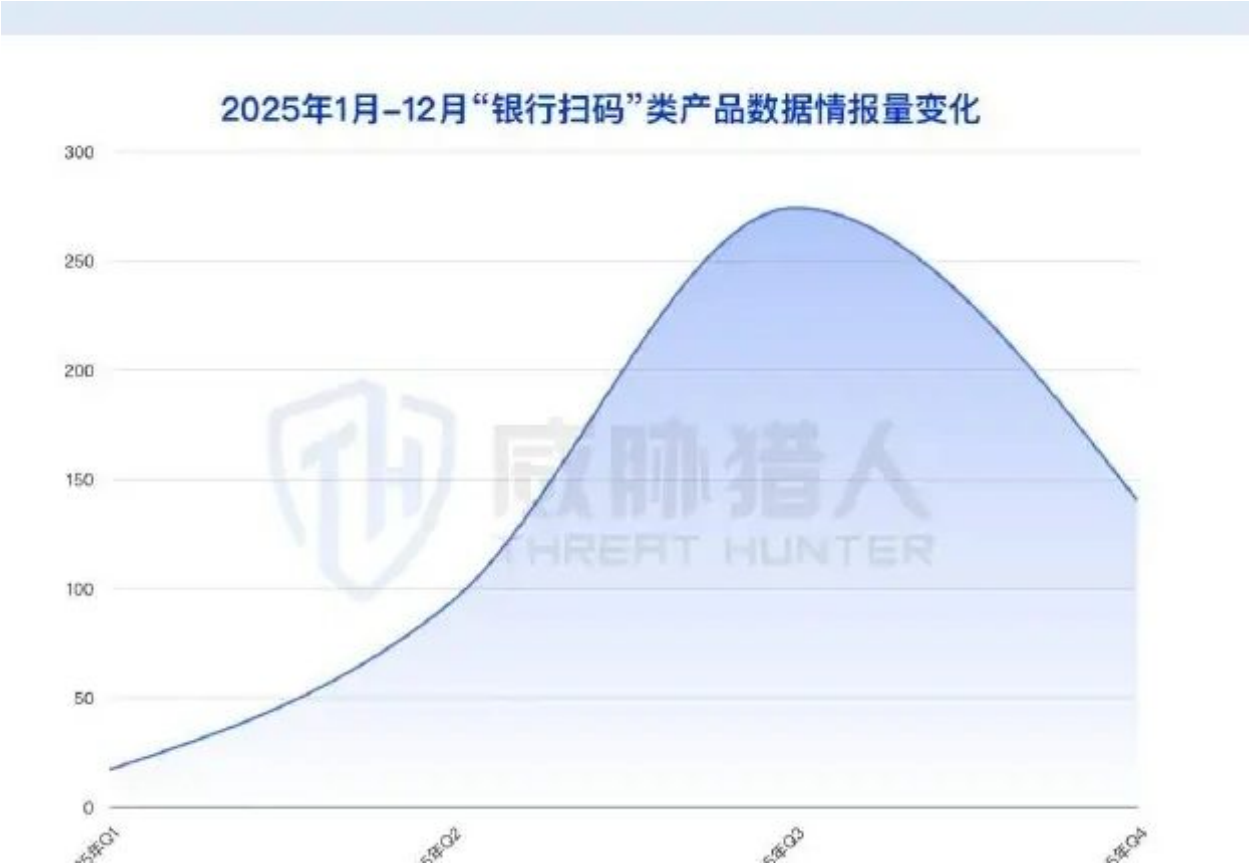
Source: Threat Hunter original report, page 32

After entering the fourth quarter of 2025, the number of bank “scan QR code application” incidents has declined. The main reason for the decline is that due to the influence of the new hot-selling product "Consumption Fund Application", more downstream criminal gangs have switched to purchasing "Consumption Fund Application" data, resulting in a decrease in "bank code scanning" incidents.

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.

In-depth analysis by Threat Hunter operators found that the “scan QR code application overnight” data referred to by threat actors is mainly concentrated in 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, a total of more than 80 bank loan businesses are involved, basically local banks or commercial banks.




**The leak of bank's “sweep application” loan information continued to rise, reaching its peak in 2025.**

Source: Threat Hunter original report, page 33

(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)

## 3.3.2 The marketing tools of third-party financial technology companies have become a core risk point and are associated with more than 80 banking institutions.

Threat Hunter conducted a traceability analysis of the bank QR codes involved in the leaked data and found that the relevant clues pointed to the "XX Marketing Assistant" platform developed by the same well-known financial technology service provider. Further cross-verification combined with the list of bank loan platforms circulated in illegal data trading channels in June 2025, it can be confirmed that the potential impact of this incident exceeds 80 banking institutions.

- If you want to know whether your banking institution is on the list, please contact Threat Hunter.

(Flow chart of bank loan application information leakage)

The relevant business process operations are as follows:

Bank loan business is usually handled through an exclusive event QR code provided by the account manager (the QR code carries information about the account manager). After scanning the code,

the user jumps to the bank's official mini program and completes the application operation on the corresponding loan business page.

Further analysis found that the above-mentioned loan business QR code provided by the account manager was not directly generated by the bank system, but was produced and distributed through a marketing and 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).

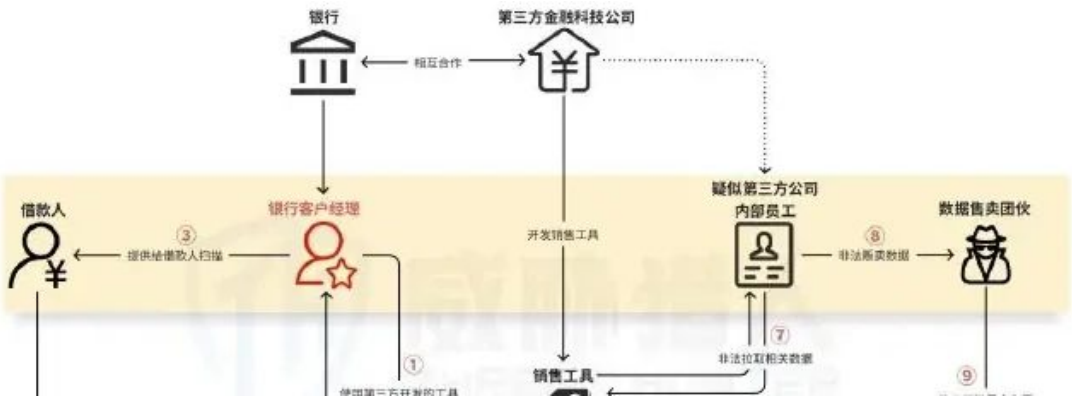
Threat Hunter followed up and analyzed the information released by threat actors and found that when this type of incident began to be publicized, threat actors claimed that the data came from "insiders", that is, internal employees leaked it. Considering that more than 80 banking institutions are involved 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.

To verify this judgment, Threat Hunter analyzed the business model of the third-party financial technology company and found that the company not only provides application system software development services for banks, but also provides supporting intelligent fraud-control strategy support. Relevant fraud-control strategies are usually configured based on the qualification differences of loan users and are used to assist bank account managers in customer screening and follow-up. In actual operation, when a user submits a loan application in the bank's official applet, the relevant user information will be synchronized to the above-mentioned sales tool platform for account managers' performance statistics and customer management.

Although this mechanism is reasonable in terms of business efficiency, in the context of cross-system data synchronization and multi-agency reuse, it also objectively expands the circulation links and exposure scope of user data, thereby increasing the potential risk of data abuse or 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)

At the same time, feedback from threat actors shows that after such information is leaked to the illegal data trading market, it is mainly used to assist loan companies in targeted marketing. 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.




**Third-party financial technology company marketing tools became core risk points, linked to 80 banking institutions**

Source: Threat Hunter original report, page 35

## 3.3.3 The range of data types continues to increase, and threat actors use AI models to segment the original data.


**Third-party financial technology company marketing tools became core risk points, linked to 80 banking institutions**

Source: Threat Hunter original report, page 36

According to Threat Hunter's continuous tracking of this type of illegal data transactions, after entering the second half of 2025, this type of data transactions showed two significant trends:

First, the coverage of data types continues to expand, and second, threat actors have begun to introduce algorithmic models to conduct refined portraits and dismantling of original data to improve the usability and monetization efficiency of data.

1) The range of data types continues to expand:

New post-loan user data was added in July 2025, which will no longer be limited to the original users who scan the QR code to apply;

In November 2025, new credit card application data was added, which is no longer limited to ordinary users who scan the QR code to apply for loans;

Supports multiple large banks, no longer limited to original local banks or commercial banks;

2) The dimensions of user portraits continue to be refined:

Model recognition optimization is introduced to conduct in-depth analysis of user portraits, and customized screening can be carried out according to the needs of downstream malicious activity

actors; such as user gender, age, device type, residence time after scanning, and other detailed label information content.

## 3.4 New trend in SMS data leakage risk, 106 expansion code has become a new leakage entrance

### 3.4.1 106 expansion code data leakage involves multiple industries, affecting more than 420 companies

In recent years, with the implementation of SMS "logo authentication", more and more corporate SMS messages will display brand names and logos on users' mobile phones, greatly improving user recognition. But it has also become a key anchor for threat actors to identify users of specific platforms.

In May 2025, a new type of user text message leakage risk began to quietly emerge in the circle of threat actors - "106 expansion code anti-hijacking".

It reached its peak in September this year, with more than 2,400 pieces of overall risk intelligence, involving more than 420 enterprise platforms, covering finance (consumer finance, banking, securities), e-commerce, travel, life services and other industries.

106 expansion code: refers to the number used by enterprises to send notifications to users through the SMS channel of communication service providers. It usually starts with 106, and the subsequent expansion numbers represent specific channel providers and service applications.

106 expansion code anti-hijacking: It is a new SMS data stealing method discovered by Threat Hunter. threat actors extract the expansion code from the 106 SMS number, reversely query the user information (such as phone number, city and platform name) who received such SMS, and then package and sell it or use it for precise malicious activity. This type of behavior abuses the SMS compliance mechanism of communication service providers and has constituted a serious data security risk.

The following is a sample of data captured by Threat Hunter:

- If you need to confirm whether your company's user data is on the list, please contact Threat Hunter (the picture on the left shows the leaked data format, and the picture on the right shows threat actors officially launching the "expansion code" SMS data product)

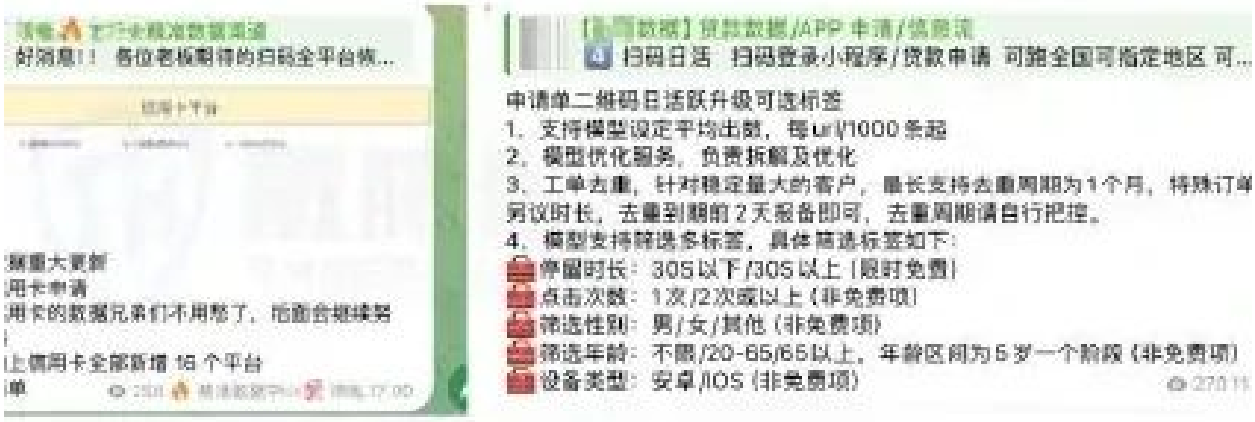
Panoramic view of the threat actors transaction chain: From communication service companies to the black market, Threat Hunter conducted research and analysis on the methods of data leakage, and restored the complete threat actors transaction path of "106 extension code anti-hijacking":

Upstream resource provider: Generate query tasks based on downstream data requirements, and ultimately provide information such as user phone number, region, and platform. The upstream resource provider provides the queried data to the data intermediary, and the data intermediary then delivers it to the downstream malicious activity gang. The entire process, from the bill of lading to the resource provider, to running the data and delivering the data, generally only takes three days.

Midstream data intermediary: integrates the data needs of downstream malicious activity gangs and submits them to upstream resource providers;

进行深入分析，可根据下游作恶黑产需求进行定制化筛选

言停留时间等细化标签信息内容。




**106. Outreach data leaks involved multiple industries affecting over 420 enterprises (Chart 1)**

Source: Threat Hunter original report, page 38

**106 拓展码：**指的是企业通过通信服务商的短信通道向用户发送通知所使用的号码，一般以 106 开头，其后的拓展数字则代表具体的通道商和服务应用。

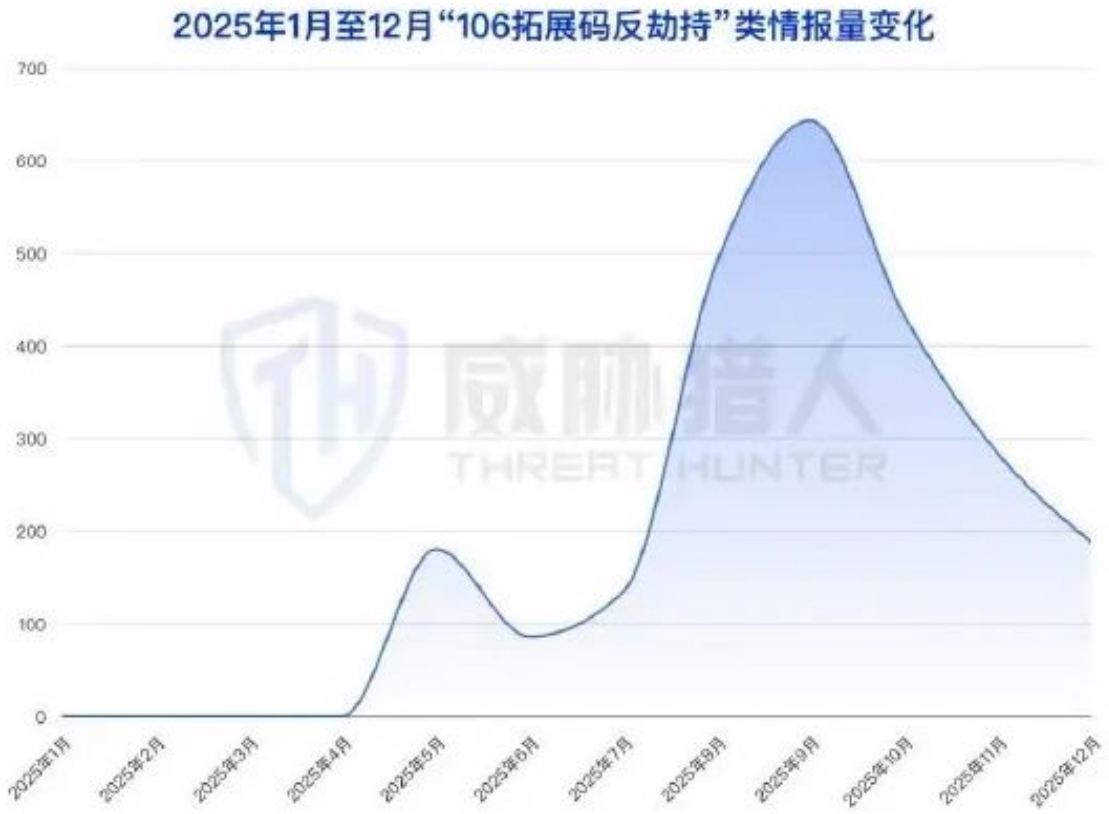
**106 拓展码反劫持：**是威胁猎人发现的一种新型的短信数据窃取手法，黑产从 106 短信号码中提取出拓展码，反向查询收到此类短信的用户信息（如手机号、城市和平台名称），进而打包售卖或用于精准作恶。这类行为滥用了通信服务商的短信合规机制，已构成严重的数据安全风险。

**106. Outreach data leaks involved multiple industries, affecting over 420 businesses (Chart 2)**

Source: Threat Hunter original report, page 38

Downstream malicious activity gangs: For example, loan assistance gangs register target platform accounts through specific operator mobile phone cards, obtain bound text message content and 106 expansion code information, organize data requirements (such as provinces, cities, etc.) based on the expansion code information, and then deliver them to midstream data intermediaries;

It is worth noting that the data extracted by downstream malicious activity gangs must carry the 106 extension code authenticated by the SMS logo. If the 106 extension code does not pass the SMS logo authentication, the user information cannot be matched.




**106. Outreach data leaks involved multiple industries affecting over 420 enterprises (Chart 1)**

Source: Threat Hunter original report, page 39


**106. Outreach data leaks involved multiple industries, affecting over 420 businesses (Chart 2)**

Source: Threat Hunter original report, page 39

Scope of influence:

1. SMS type dimension: platform account registration, verification code, loan application, overdue reminder, repayment SMS, payment SMS, etc.

Type

2. Industry dimension: finance (consumer finance, banking, securities), e-commerce, travel, life services and other industries

3. City dimension: Chengdu, Hangzhou, Chongqing, Suzhou, Wuhan, Xi'an, Nanjing, Changsha, Tianjin, Zhengzhou, Dongguan, Wuxi,

Ningbo, Qingdao, Hefei, Beijing, Shanghai, Guangzhou, Shenzhen, Fuzhou, Nanning, Jinan, Fuzhou, Foshan, Kunming, Shenyang, Harbin, Nanchang, Nantong, Guiyang, Lanzhou, Taiyuan, Changchun, Rizhao, Ningbo, Wenzhou

4. Time dimension: Testing began as early as May 13, 2025; it was officially promoted in the illegal data trading market on May 16.

Involving 350 companies, it affects 19 cities; starting from July 2, it is not limited to numbers starting with 106, and supports SMS users sent to numbers starting with 95 or 96; on August 6, the scale of the impact expanded to 420 companies, affecting users in 36 cities across the country.

(timeline)

(The picture on the left shows threat actors promoting this data type. The picture on the right shows threat actors saying on July 2 that they are not limited to data starting with 106)

In the illegal data trading market, data intermediaries threat actors have made it clear that such product data can be used to facilitate loan marketing and conduct malicious activity; at the same time, based on the industry classification of platforms provided by threat actors, nearly half of the platforms are loan business platforms (consumer finance, banking industry).


**106. Outreach data leaks involved multiple industries affecting over 420 businesses**

Source: Threat Hunter original report, page 41

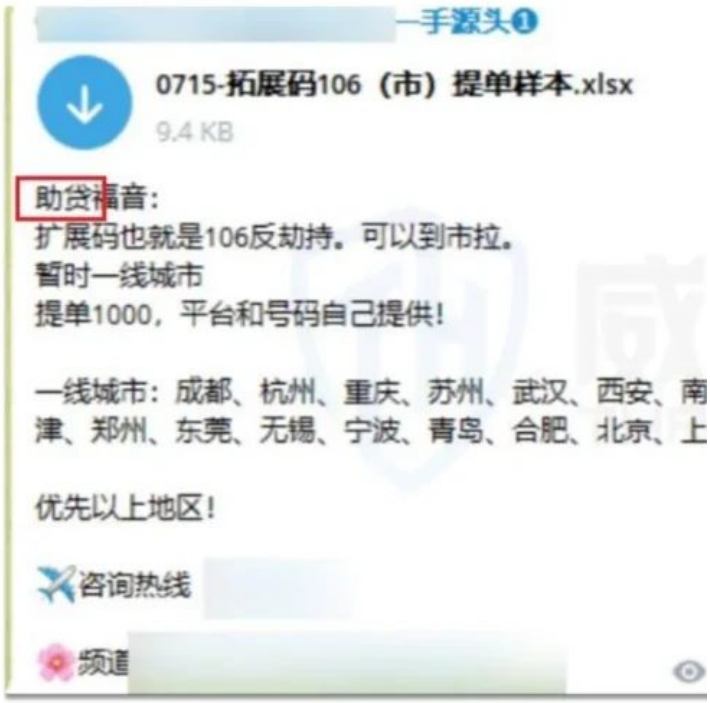
(The picture on the left shows the promotion of threat actors for loan assistance groups, and the picture on the right shows the classification of platform types provided by threat actors)

(时间线)


**SMS Extension Data Trading Chain (Chart 1)**

Source: Threat Hunter original report, page 42

合黑产提供的平台行业归属划分来看，有接近一半平台




**SMS Extension Data Trading Chain (Chart 2)**

Source: Threat Hunter original report, page 42

## 3.4.2 The fight against SMS leakage and traceability continues to escalate. threat actors make it more difficult for enterprises to collect evidence by modifying the original format of data.

In November 2025, Threat Hunter monitoring discovered that the SMS information of users from multiple different financial institutions was leaked simultaneously in the illegal data trading market. In the relevant leaked samples, the content of the text messages is highly consistent, generally showing general expressions such as "You successfully repaid the loan on xxx, please log in to the xxx app for details."

However, in actual business, different financial institutions usually do not use completely consistent text message templates. Multiple institutions using completely consistent text message content at the same time does not conform to normal business logic, and there are obvious abnormalities.

Threat Hunter further analyzed and followed up on relevant samples and found that some threat actors clearly stated during the transaction process that such SMS data was not the original content, but was regenerated through manual splicing and unified format. Its common expression is "Your repayment in the xxx time period has been successful!", and the content of the text message is exactly the same on different platforms (what threat actors call "mixed platforms").

The main purpose of this operation is to weaken the characteristics of SMS templates and avoid the traceability and forensic analysis of regulatory authorities and enterprises based on content templates.

(threat actors explain the text message format issue)

该操作的主要目的，在于削弱短信模板特征，规避监管部门及企业基于内容模板的溯源与取证分析。


**SMS leaks continue to escalate, cybercrime increases the difficulty of obtaining evidence by modifying the original data format**

Source: Threat Hunter original report, page 43

Threat Hunter recommends:

The above situation shows that the risk of SMS data leakage is showing a development trend of de-templating and de-platform characterization. It is difficult to effectively cover the current risk form simply relying on SMS content or template characteristics for identification and traceability. Some illegal data trading behaviors deliberately avoid identification mechanisms based on text templates by uniformly reconstructing text message content, weakening platform differences, and significantly increasing the difficulty of enterprises in the evidence collection and positioning stages.

In this context, when dealing with risks related to text message leakage, companies should not only rely on whether the text message content matches their own templates as the basis for judgment, but should move the focus of verification to the user-business relationship itself, focusing on whether the phone number involved is a registered user of the platform, whether there are real business interaction records, and whether its behavior track matches the normal business process. By changing from "content characteristics" to "relationship and behavior characteristics", we can more accurately identify real leakage risks and avoid misjudgment or omission of key risk signals.

Threat Hunter data breach risk intelligence service

# 4. Threat Hunter data leakage risk intelligence service

In 2025, the risk of data leakage will enter the deep water zone of "high normalization". Throughout the year, the cybercrime ecosystem chain has evolved to a very high degree of maturity and organizational resilience. Its unique "self-healing mechanism" makes it difficult for single-dimensional platform crackdowns to reach the root cause, resulting in a continued high number of risk events and leakage activities that remain highly active despite suppression. At the same time, threat actors continue to escalate their fight against the source of leaks, modifying original data information, etc., adding layers of resistance to corporate/regulatory unit traceability.

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 companies 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.

Note: The data information provided in this report is estimated and analyzed by Threat Hunter based on large sample data sampling and collection, small sample survey, external intelligence data collection, data model prediction and other research methods. Due to the limitations of any data sources and technical methods in the field of statistical analysis, the data information estimated and analyzed based on the above methods are for reference only.


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

Source: Threat Hunter original report, page 47


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

Source: Threat Hunter original report, page 47