THREAT HUNTER RESEARCH

# H1 2024 Credit Fraud Risk Report

A half-year study of fraudulent intermediaries, document manipulation and organized risk across the credit lifecycle.

Original publication: 2024-07-24
Research team: Threat Hunter Research Team
Source report: 29 pages

# Original report text

This text version is reconstructed based on the 29-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.

# Preface

Under the influence of current factors such as increased employment pressure and unstable income, the "debt tide" is intensifying. More and more people are falling into debt difficulties, and the demand for borrowing has increased significantly. Some people are unable to apply for loans normally due to problems such as unqualified qualifications, and can only borrow money through "non-standard means" such as false statements; some people do not hesitate to abandon their credit reports and become "professional debtors." Data from the China Enforcement Information Disclosure Network shows that as of July 24, 2024, there were as many as 8.38 million people subject to execution for dishonesty in our country, many of whom are "professional debtors" and "non-standard lenders."




**A national court-enforcement website lists 8,389,384 people as credit defaulters (data as of 24 July 2024)**

Source: Threat Hunter original report, page 3. Original image retained; numbered translations added by Threat Hunter.

## Figure guide

| | |
|---|---|
| 1 | Enforcement data |
| 2 | Credit-default penalties |
| 3 | Online auctions |
| 4 | Enforcement cases |
| 5 | Note |
| 6 | Earlier cumulative figures included people already removed from the defaulter list and repeat listings of the same person; figures now exclude both, to show the current number of defaulters. |
| 7 | Defaulters currently listed |
| 8 | Data as of 24 July 2024 |

Recently, Threat Hunter released the "Credit Fraud Risk Landscape Report for the First Half of 2024". Based on long-term investigations and research on the credit fraud industry chain, combined with various behavioral data of threat actors and intermediaries, it strives to accurately and objectively display the current criminal processes and behavior patterns of credit fraud cybercrime ecosystem.

Related noun definitions:

1. AB loan: AB loan is a kind of loan fraud, also known as on-lending, loan assistance, arbitrage loan, and worldly loan. Among them, A

He is a person in need of funds but has a poor credit report and cannot directly obtain a loan, while B is a person with good credit report and is induced by the intermediary and A to provide guarantee or credit enhancement for A. In fact, the loan funds are used by A, and B becomes the final lender without knowing it and assumes the debt and repayment responsibility.

2. Debt restructuring: refers to threat actors intermediaries helping target customers pay off debts and maintain credit records through "pre-stage advances", etc.

It is qualified to apply for a higher amount of "credit loan", and the debt restructuring mainly involves provident fund loans.

3. Non-standard loans: refers to customers who cannot meet the standard conditions for loans from conventional financial institutions, but their overall qualifications are pretty good, threat actors

The intermediary uses packaging materials, beautified data, relationships, etc. to help customers successfully obtain loans.

4. Professional debt: refers to those who have no loan qualifications at all (such as pure white, novice, small flower, low education level) or qualifications.

People with low quality and willingness to take on debt apply for large bank loans through the qualification package of threat actors. Professional debtors aim to obtain high profits and have no intention of repaying debts.

5. Technology enhancement: This mainly refers to the use of technology by threat actors to optimize credit assessment or improve credit scores, thereby improving credit quality.

The credit limit is mainly targeted at corporate loans that have channels to increase their credit limit.

6. Real estate scenarios: refers to loan scenarios related to real estate, such as home purchase mortgage loans, real estate mortgage loans, real estate mortgage loans, etc.

Loan scenarios such as business loans and real estate renovation loans.

7. Over-loaning: refers to the use of unconventional means to make one's credit limit exceed the loan limit specified by the financial institution, such as through high-rating

Usury loans apply for mortgages and mortgages that are much higher than the value of the property itself.

8. “Three Guarantees”: In the debt-bearing business, threat actors will advance funds in the early stage to cover the debt-bearing customers’ train tickets and air tickets to the cities designated by threat actors.

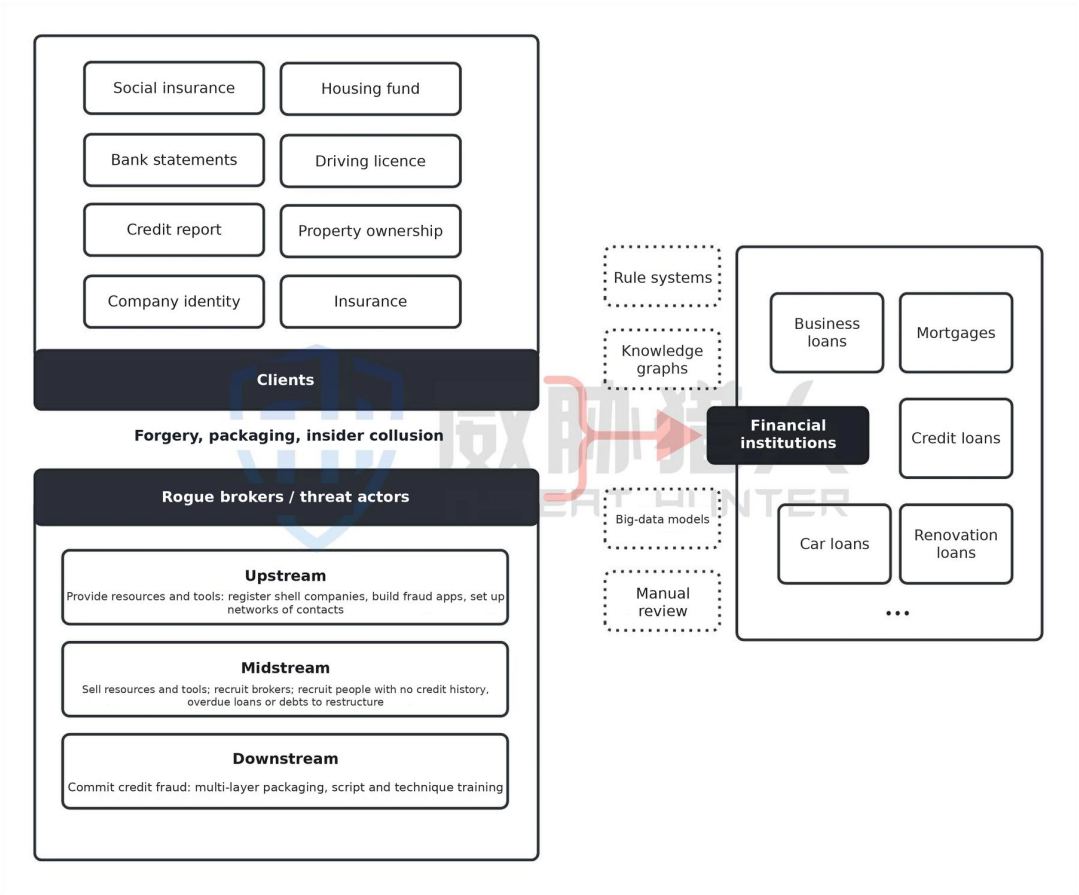
Expenses and room and board expenses during the operation period are called "three guarantees" by threat actors. In fact, threat actors will deduct the corresponding "three guarantees" expenses during settlement.

Credit fraud industry chain and crime process

# 1. Credit fraud industry chain and crime process

## 1.1 Overview of the credit fraud industry chain

In recent years, the division of labor in the financial credit fraud industry chain has become increasingly clear and large-scale. Each link in the upstream, middle and downstream sectors performs their own duties and maximizes the use of resources to defraud large loans from banks and financial institutions. The roles and responsibilities of each link are as follows:




**The credit fraud chain: rogue brokers and threat actors forge and package client credentials to defeat lenders' risk controls**

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

The upstream link provides resources and tools by registering shell companies, developing fraudulent applications, and building relationships;

The midstream link reorganizes debt by selling these resource tools, recruiting intermediaries, and recruiting white credit users or overdue customers;

The downstream link focuses on implementing credit fraud and conducting multi-dimensional identity packaging and speaking skills training.

Threat Hunter's in-depth research found that banks and other financial institutions are faced with fraud risks in all aspects of the loan scenario. malicious activity tactics are emerging in different stages before, during, and after the loan, resulting in different types of credit fraud such as professional debtor fraud, falsification of non-standard loan materials, negotiated repayment, and

credit repair agency services, and have formed large-scale and standardized fraud processes and techniques.

| Stage | Step | Fraud type | Description |
|---|---|---|---|
| **Pre-loan** | Application | Professional debt-carrier fraud | Threat actors recruit people who are poor, want quick money or urgently need cash and have no or thin credit history; after packaging, they take on debt for pay, combining credit, mortgage, renovation, car and business loans. |
| | | Fake documents | Identity packaging, forged paper and electronic documents, fake bank statements, etc. |
| | | Cashing out | Loan funds are cashed out through physical or virtual goods, e.g. car-loan cash-outs. |
| | | Debt restructuring | Rogue brokers advance funds to clear the debts of highly indebted employees of well-regarded employers, nurture their credit records and apply for several new loans. |
| | | Insider collusion | Staff at banks or lending platforms collude with outsiders in return for kickbacks. |
| | | AB loans | A needs a loan; a broker persuades A to bring in an acquaintance B as guarantor or credit enhancer, and B becomes the actual borrower. |
| | | Loan laundering | Money launderers pay people to apply for loans; the loan money is moved to laundering accounts via stablecoins, and the launderers repay the loans with dirty money. |
| | Review | Script coaching | Clients are trained and coached on what to say to evade risk review or answer offline risk questions, raising approval rates. |
| | Payout | Unauthorized deductions | When brokers handle a loan, they use auto-debit software to take fees from the client, to charge more or stop the client walking away. |
| **In-loan** | Application | Illicit limit increases | Credit limits are raised by abnormal means, such as technical tricks or fake income data. |
| **Post-loan** | Collection | Credit-card interest freeze and instalments | Debt-optimization agents coach or act for clients in negotiating with card centres, or complaining, to demand an interest freeze and repayment plan. |
| | | Loan repayment extensions | Debt-optimization agents coach or act for clients in negotiating with lenders, or complaining, to demand extended repayment. |
| | | Credit-card interest and fee refunds | Debt-optimization agents coach or act for clients in negotiating with card centres, or complaining, to demand refunds of interest and fees. |
| | | Loan interest and fee refunds | Debt-optimization agents coach or act for clients in negotiating with lenders, or complaining, to demand refunds of interest and fees. |
| | Settlement | Credit-record repair | Threat actors restore clients' credit records through complaints and credit-report disputes. |

**Credit fraud types and how they work, by loan stage**

Source: Threat Hunter original report, page 7. Redrawn in English from the original figure.

## 1.2 threat actors operate business processes

There are endless fraud techniques in different lending scenarios, and each operating process has its own characteristics. Fraudulent behavior exists in mortgage loans, credit, car loans, corporate loans and other loan scenarios, and the risk of overdue is extremely high, for example:

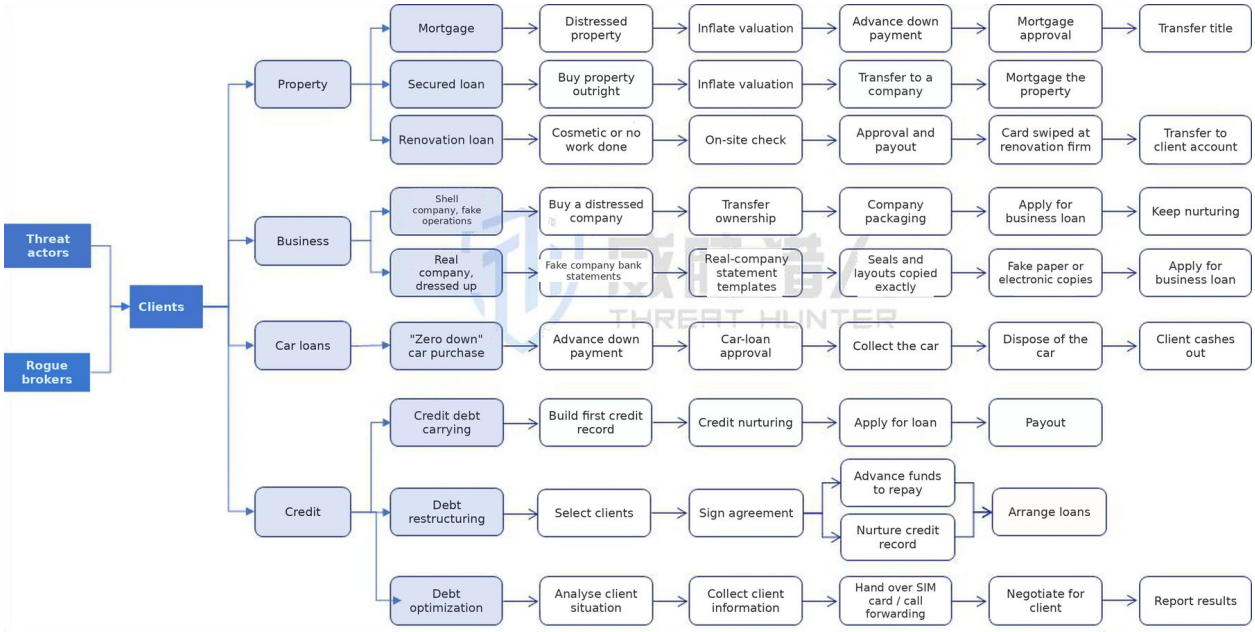
In the housing loan scenario, based on the unreal demand for home purchase, threat actors advance the down payment, apply for a super online mortgage mortgage loan, or advance the entire amount to the customer to purchase a house, thereby applying for a high-value housing loan, and then apply for multiple fake repair loans;

In the credit scenario, threat actors use intermediaries to repay loans, artificially improve credit scores, reorganize debts, or use internal relationships to enable people who do not have loan qualifications to obtain large credit loans;

In the car loan scenario, threat actors obtain high-priced car loans by advancing down payments to purchase cars, and after taking delivery of the car, they work with local car dealers to dispose of the vehicle and cash out;

In the corporate loan scenario, the debtor can apply for a large corporate loan by traffic manipulation up the company's business flow, issuing invoices and paying taxes for corporate packaging and maintenance.

The specific processes involved are as follows:




**How threat actors and rogue brokers run fraud across property, business, car and credit loans**

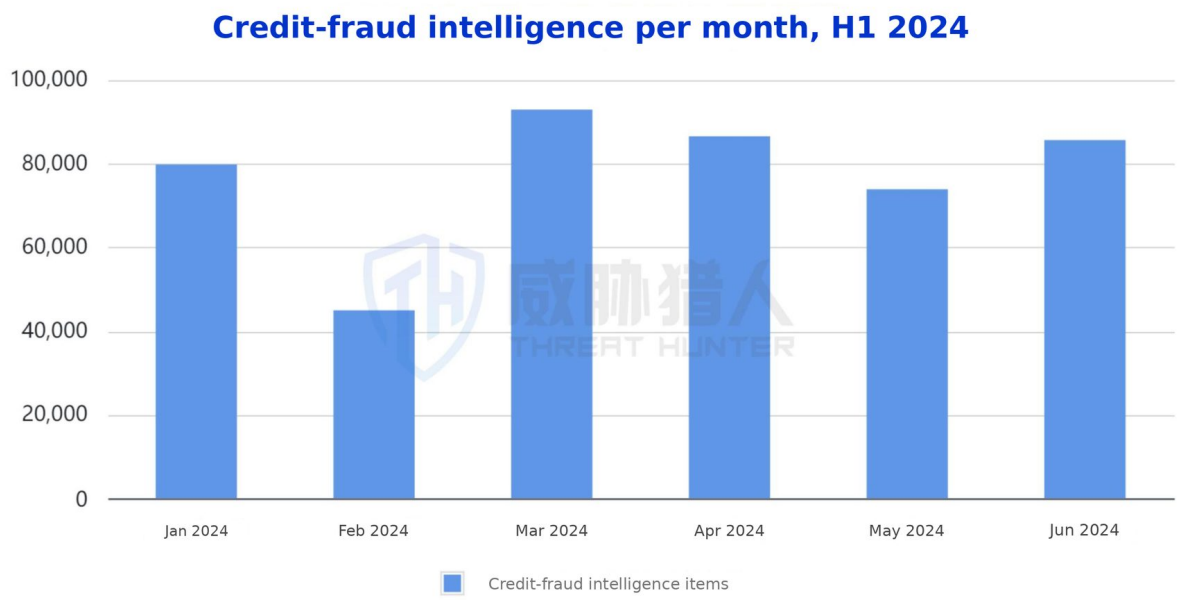
Source: Threat Hunter original report, page 8. Original figure with Chinese text replaced by English.

Credit fraud risk landscape in the first half of 2024 Credit fraud risk landscape in the first half of 2024

# 2. Credit fraud risk landscape in the first half of 2024

## 2.1 In the first half of 2024, there were 460,000 pieces of credit fraud attack intelligence, and 2,700 active malicious activity groups were detected.

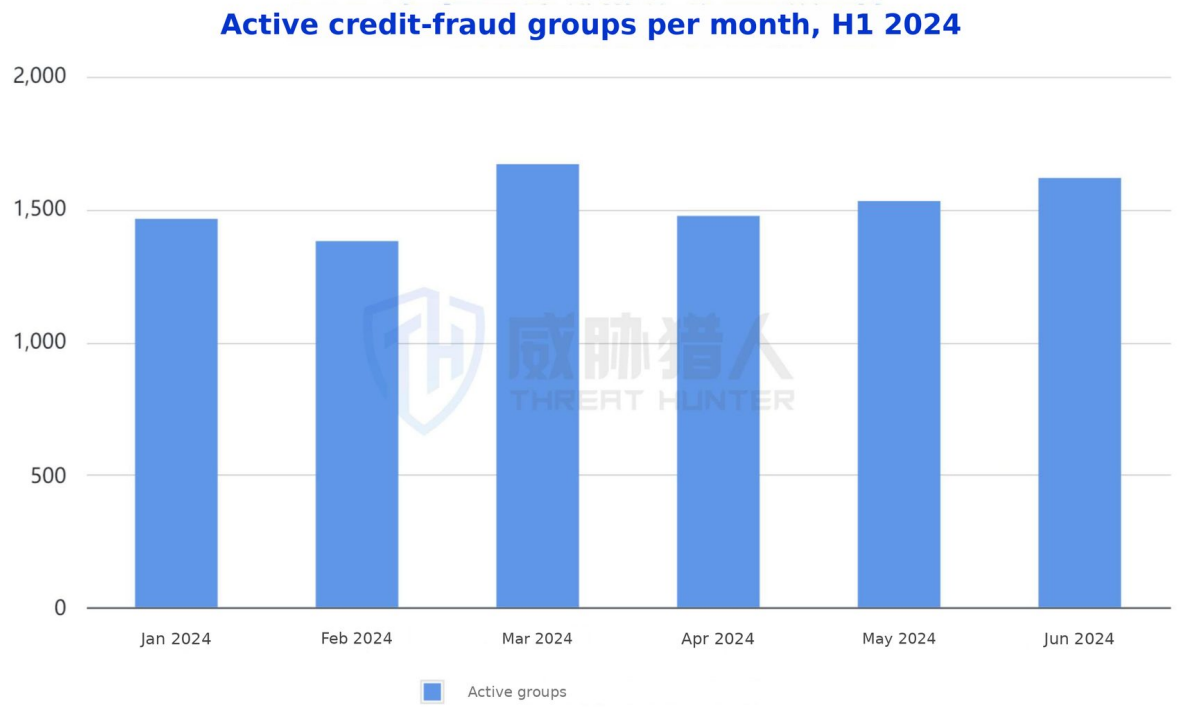
In the first half of 2024, Threat Hunter captured a total of 460,000 pieces of credit fraud attack intelligence, monitored 2,700 active malicious activity social groups, and involved 14,000 malicious activity threat actors.




**Credit-fraud intelligence captured per month, January–June 2024**

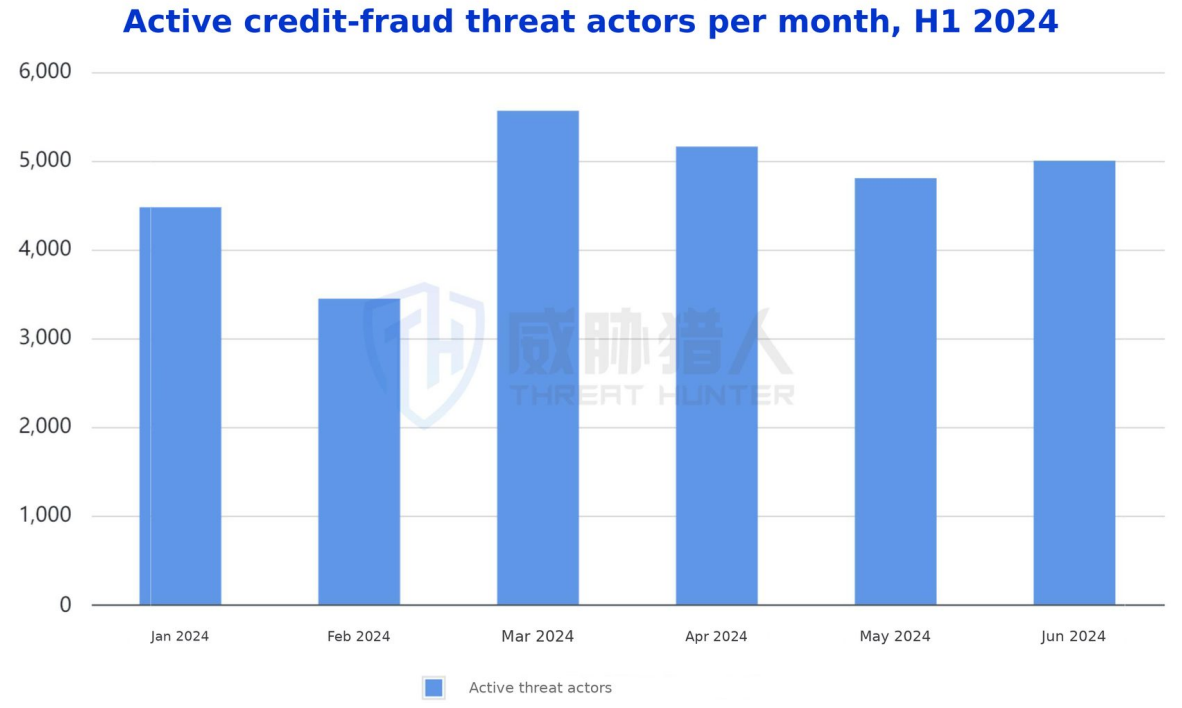
Source: Threat Hunter original report, page 10. Original figure with Chinese text replaced by English.

In the first half of 2024, the number of monthly credit fraud perpetrator groups and threat actors was generally relatively stable. Among them, the number of perpetrator groups increased slightly every month, and there was an increasing trend from April to June 2024.




**Active credit-fraud groups per month, January–June 2024**

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

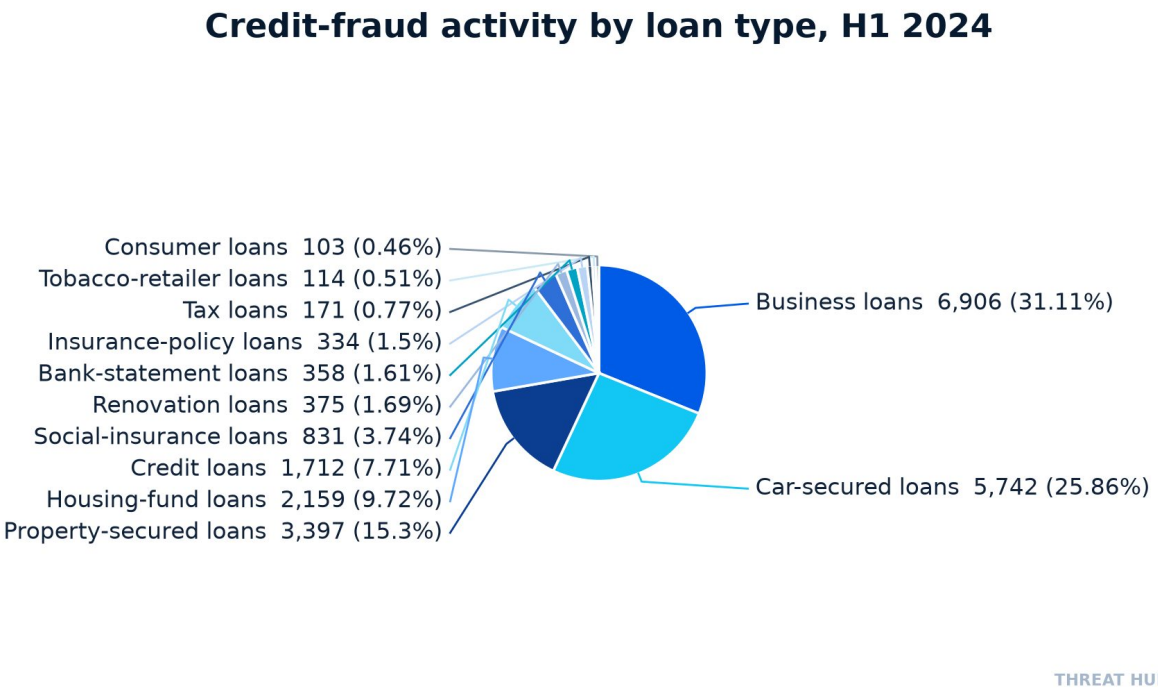



**Active credit-fraud threat actors per month, January–June 2024**

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

## 2.2 Among the loan categories subject to credit fraud, the most popular ones are: corporate loans, car loans, and housing loans.

From the perspective of credit fraud loan categories, the top five loan categories with the most popular credit fraud in 2024 are: corporate loans, car mortgage loans, housing mortgage loans, provident fund loans and credit loans.

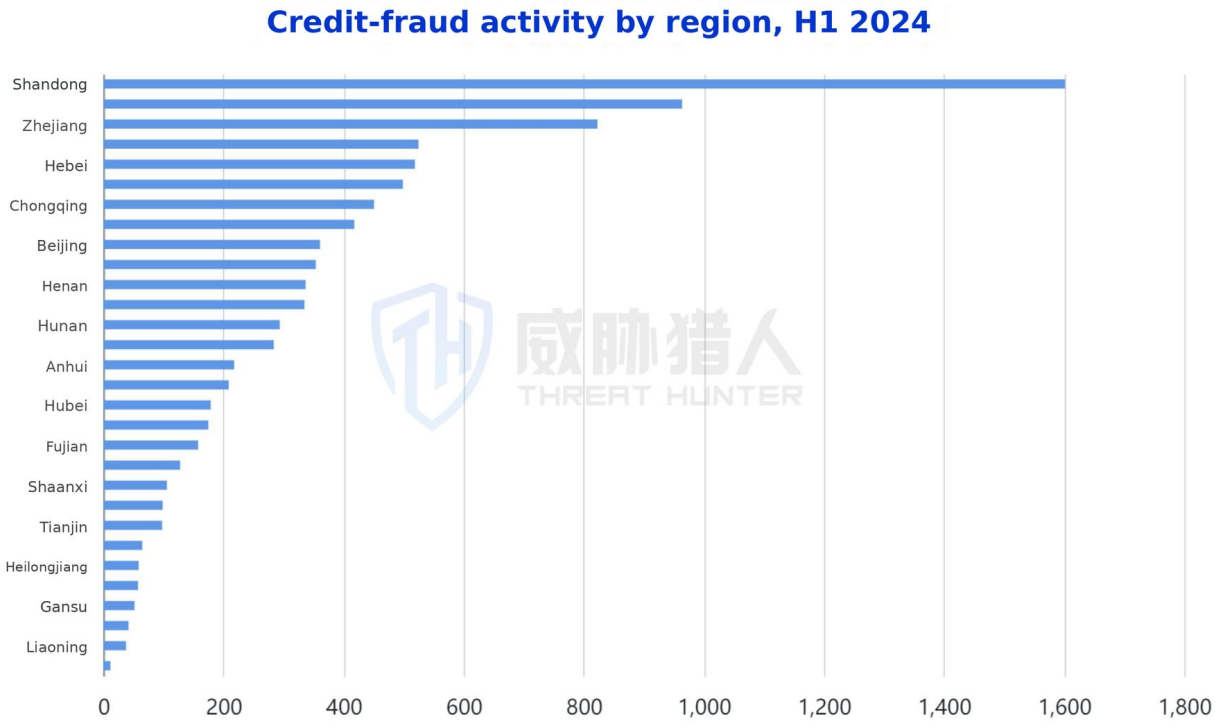



**Credit-fraud activity by loan type, H1 2024: business loans 31.11%, car-secured loans 25.86%, property-secured loans 15.3%**

Source: Threat Hunter original report, page 11. Redrawn in English from the original figure.

## 2.3 Provinces with the highest incidence of credit fraud in the first half of 2024: Shandong, Zhejiang, and Hebei

From the perspective of geographical distribution, the top five regions with the most popular credit fraud areas in the first half of 2024 are: Shandong, Zhejiang, Hebei, Chongqing, and Beijing.



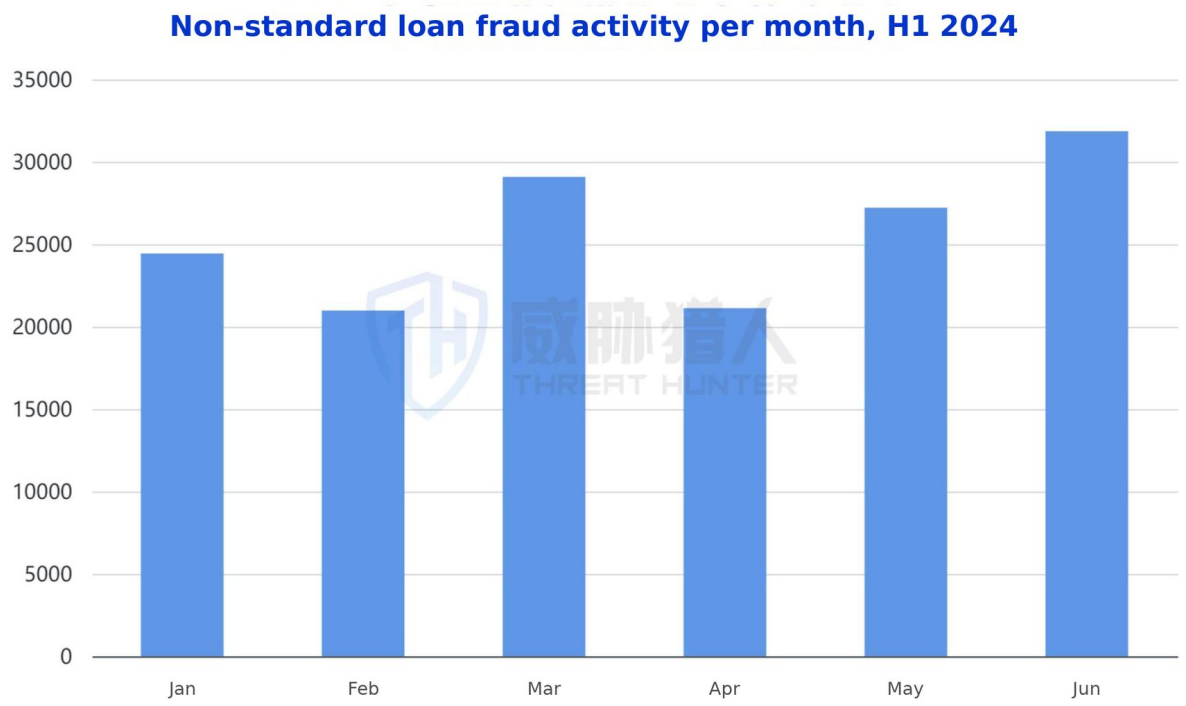

**Credit-fraud activity by region, H1 2024: Shandong, Zhejiang and Hebei lead**

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

## 2.4 The popularity of non-standard loans will continue to grow in the first half of 2024, with the topic popularity increasing by nearly 10% compared with the second half of 2023

Non-standard loans: Refers to the fraudulent behavior of customers who have good overall qualifications but cannot fully meet the conventional standard conditions for loans from financial institutions. threat actors use packaging materials, beautified data, relationships, etc. to help customers successfully obtain loans.

In the second half of 2023, the number of discussions on non-standard related topics reached 140,780. In the first half of 2024, the total popularity of non-standard topics was 154,685, with a growth rate of 9.9%.




**Non-standard loan fraud activity per month, H1 2024**

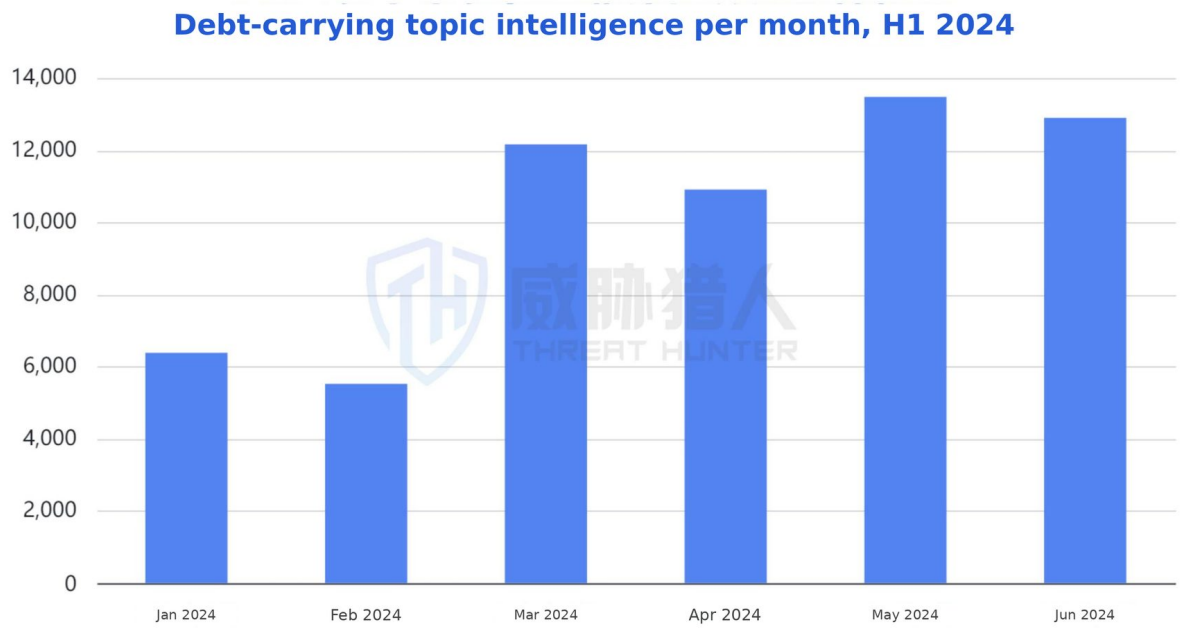
Source: Threat Hunter original report, page 13. Original figure with Chinese text replaced by English.

Under the influence of the economic downturn in recent years, enterprises, operators, and individuals have generally faced difficulties such as reduced income and high debt, which has caused

The existing qualifications of some enterprises, operators and individuals do not meet the loan requirements of financial institutions. threat actors and intermediaries commit fraud through false flow sheets (individuals and enterprises), technology quota increases, car financing cash out, fake renovation loan cash out, rent-to-purchase cash out, etc., and use false materials and false demands to pass the approval and quota increase system, making non-standard businesses continue to be active.

## 2.5 In the first half of 2024, the popularity of "recruitment of debtors" continues to rise. The provinces with the highest popularity are: Guangdong, Zhejiang, and Chongqing

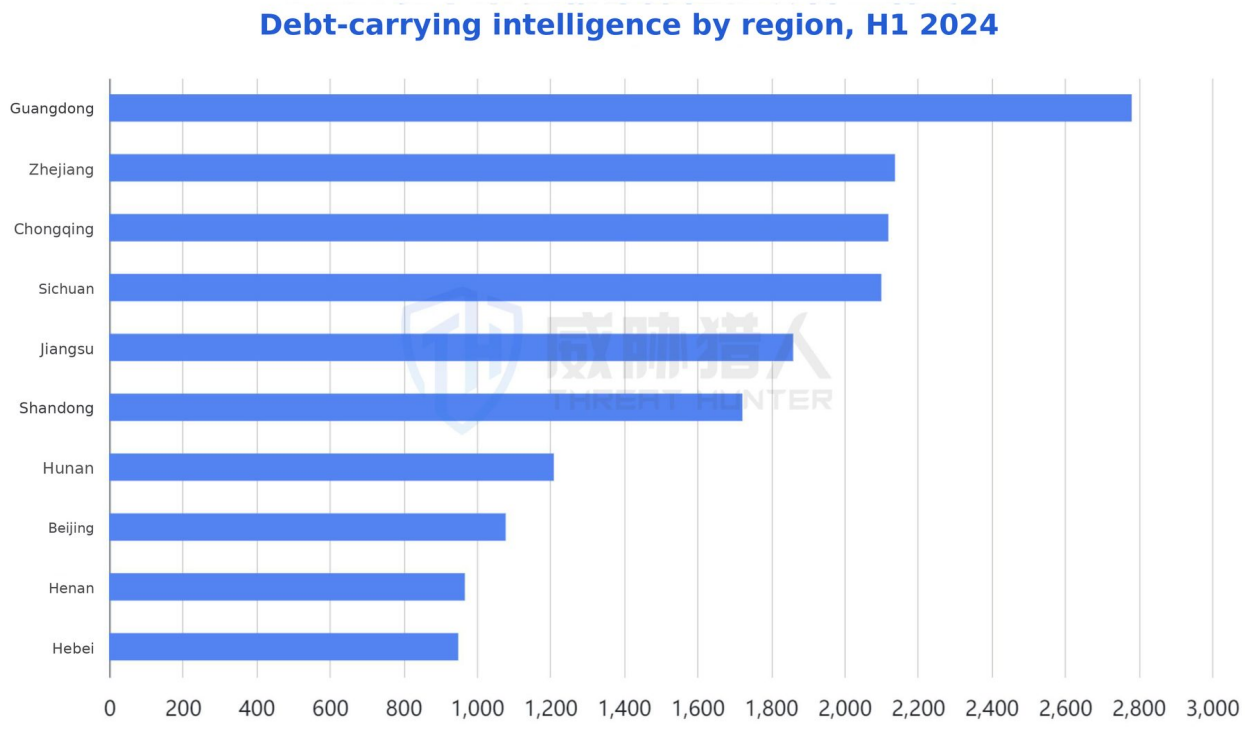
Judging from the amount of data related to threat actors recruiting debtors monitored by Threat Hunter in the first half of 2024, the popularity of threat actors recruiting debtors is generally on the rise in 2024.




**Debt-carrying topic intelligence per month, H1 2024**

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

The five most popular provinces for debt incurrence in the first half of 2024 are: Guangdong, Zhejiang, Chongqing, Sichuan, and Jiangsu. Among them, the topic of "recruiting debt holders" in Guangdong Province is far more popular than other provinces.




**Debt-carrying intelligence by region, H1 2024: Guangdong, Zhejiang and Chongqing lead**

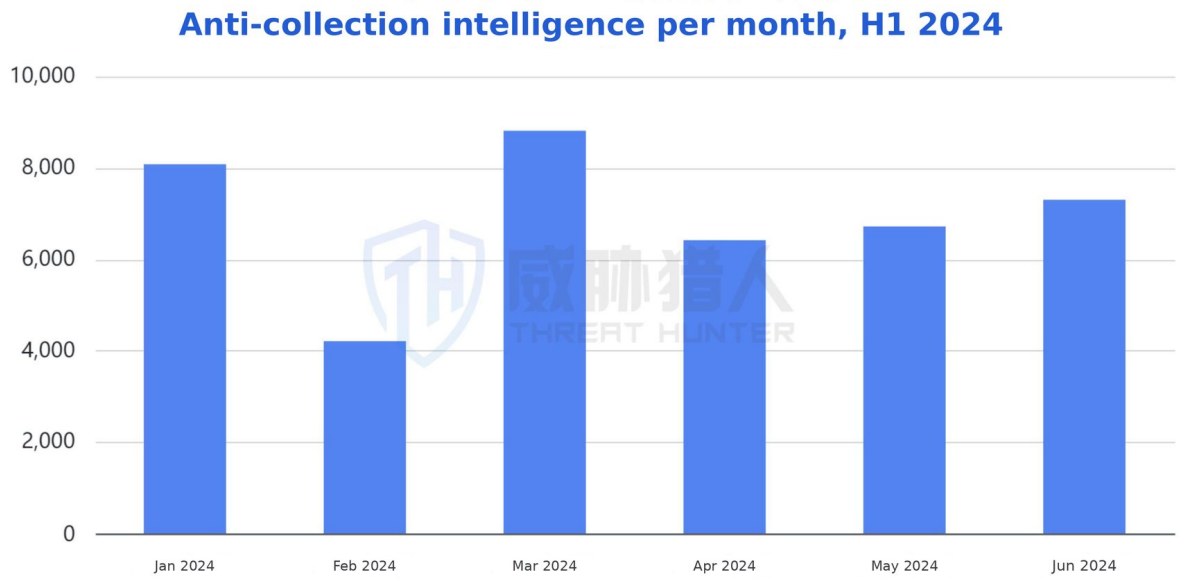
Source: Threat Hunter original report, page 14. Original figure with Chinese text replaced by English.

## 2.6 The demand for anti-collection business will continue to rise in the first half of 2024, and there were a large demand for "negotiated repayment of overdue small loans" and "credit repair"

Counter-collection mainly means that in order to cope with the collection of overdue loans, the debtor uses various means to fight or avoid the collection behavior of financial institutions, including obtaining interest exemptions, deferment/installment repayment, elimination of overdue records, etc., and thereby making profits.

The main demand scenarios for anti-collection include post-loan related agency services such as "credit card installments, interest suspension and pending accounts, credit deferred repayments, interest refunds, mortgage extensions, credit report repairs". After threat actors receive a counter-collection order from a debtor, they usually ask the debtor to mail a personal phone card or set up a call transfer. The so-called legal staff of the intermediary will negotiate and communicate on behalf of the debtor, and ultimately achieve the goals of interest reduction and exemption and deferment/installment repayment. Threat Hunter continues to monitor anti-collection related risk intelligence, 2024

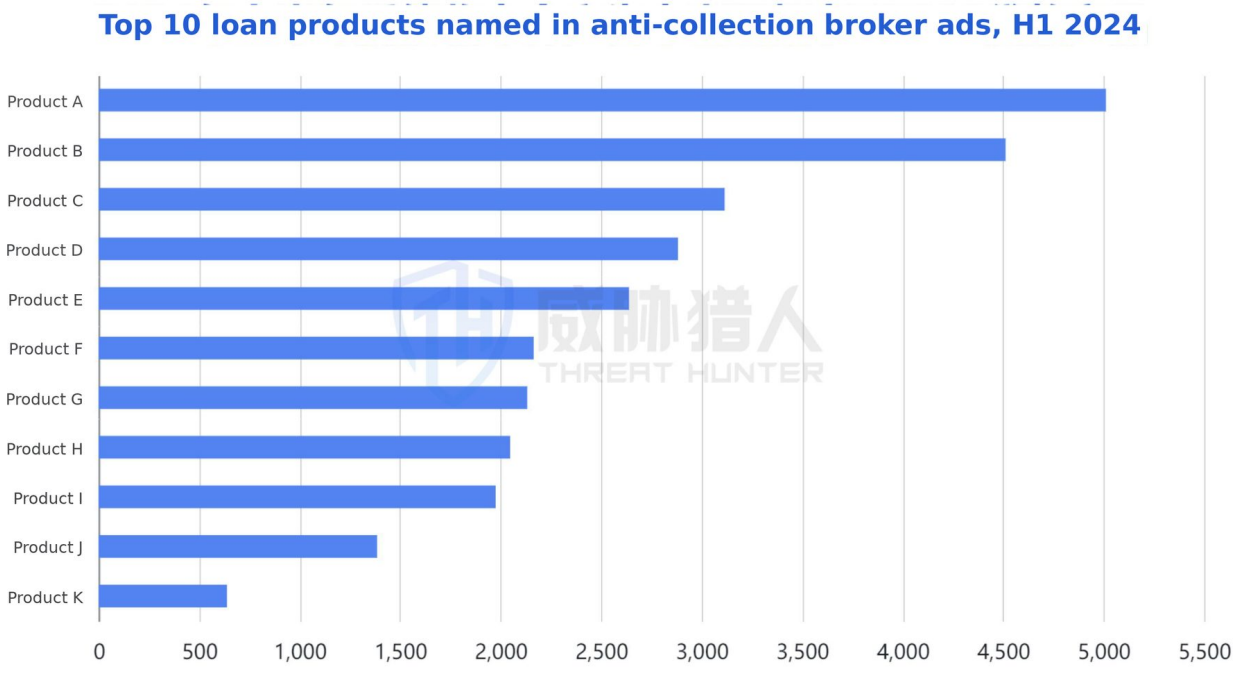
The trend in the quantity of anti-collection related intelligence in the first half of the year is as follows:




**Anti-collection intelligence per month, H1 2024**

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

Threat Hunter further analyzed the 10 most mentioned loan products in anti-collection intermediary advertisements in the first half of 2024 and found that the popular "negotiated repayment of small loans overdue" and "credit repair" are in high demand.




**Loan products most often named in anti-collection broker ads, H1 2024 (product names are masked in the original; the original chart shows 11 bars under a "Top 10" title)**

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

Typical credit fraud techniques and risk analysis Typical credit fraud techniques and risk analysis

# 3. Typical credit fraud techniques and risk analysis

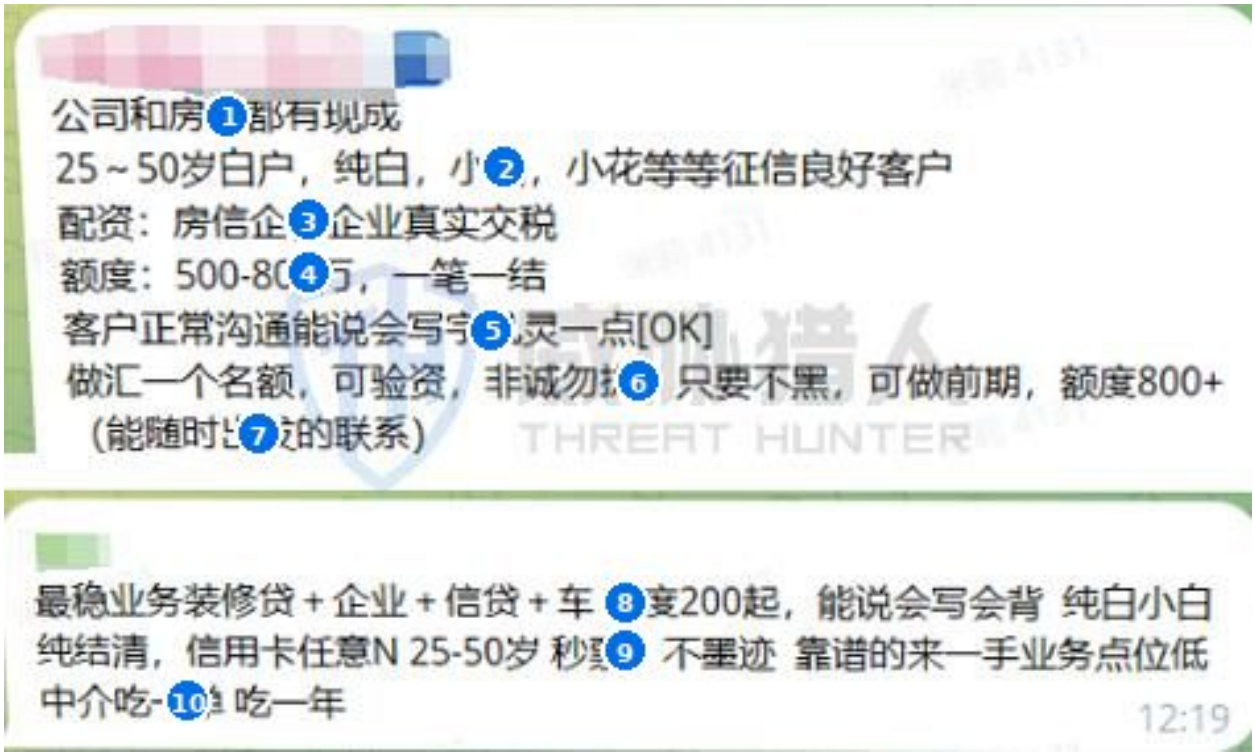
## 3.1 Professional Debt Carrying: Package the qualifications of debtors and obtain millions of loans such as housing loans/enterprise loans

### 3.1.1 Operation method

Threat Hunter research found that the target group of threat actors intermediaries is generally "people with low education, clean credit, 25-55 years old, who can speak and write and are willing to cooperate, want to make quick money or are extremely short of money." threat actors intermediaries usually promote and recruit through threat actors group chats, Moments, various social platforms and short video platforms.

After identifying the target debtors, cybercriminal groups will gather qualified people who are willing to take on debts to the loan fraud area and live there for a long time to implement the "three guarantees" policy. They will then package the identities and materials of the debtors to make qualification preparations for subsequent fraudulent "housing loans, credit loans, corporate loans, car loans", etc.

The following is the advertising information posted by threat actors intercepted on an encrypted messaging app:




**A debt-carrier recruitment ad intercepted on an encrypted messaging app**

Source: Threat Hunter original report, page 17. Original image retained; numbered translations added by Threat Hunter.

## Figure guide

| | |
|---|---|
| 1 | Company and property ready-made |
| 2 | Clients aged 25–50 with no or thin credit history and good credit |
| 3 | Package: mortgage + credit + business loans; company pays real taxes |
| 4 | Amount: CNY 5–8 million, settled per deal |
| 5 | Client must communicate normally, read and write, and be quick-witted |
| 6 | One slot open; funds can be verified; serious enquiries only; anyone not blacklisted; early stage possible; amount 8 million+ |
| 7 | (contacts who can leave at any time) |
| 8 | Most reliable: renovation + business + credit + car loans from 2 million; clients who can speak, write and memorise; no or thin credit history |
| 9 | All loans repaid; any credit card; aged 25–50; instant approval; not blacklisted; reliable people only; first-hand deals; low commission |
| 10 | A broker lives for a year off one deal |

In order to avoid bank fraud controls and related departments' crackdowns and ensure maximization of interests, relevant threat actors have made the identity packaging and material forgery of debtors more realistic. threat actors gangs target those who have clean credit records and are in urgent need of large amounts of funds but have no ability to repay. They package various false identities such as "workers, household heads, business owners", etc., as credit enhancement conditions for applying for loans, such as paying real social security, provident funds, transferred properties/enterprises, etc. to debtors.

In the end, the debtor's false identity and forged qualifications were used to carry out one-stop large loans of "housing loans, credit loans, business loans, and car loans" to obtain high-value loans from banks. The total amount of fraudulent loans by a debtor can reach about 10 million or even higher, but the actual amount obtained is 40-50% of the total amount of debt, or even less. The specific process is as follows:

1. Apply for a personal credit loan: After determining the debtor, threat actors will apply for a personal credit loan for the debtor based on the debtor's situation.

Loans serve as upfront capital, and this part of the funds is often used as one of the packaging costs for subsequent housing company loans;

2. Apply for housing loans and renovation loans: Based on unreal demand for home purchases, threat actors advance funds to pay the down payment, and transfer low-priced non-performing properties to high prices.

At the same time, they fabricate false high-value transaction contracts to raise the appraisal price, thereby obtaining high-value housing loans. Then, about a month after the mortgage is disbursed, threat actors will apply for 2-3 decoration loans for the debtor to earn profits from the decoration loans. The amount of the housing loan and decoration loan ranges from 300,000 to 1 million.

3. Handle corporate loans: threat actors intermediary transfer bad companies purchased at low prices to the debtor, making the debtor a corporate legal person.

By providing the debtor with company records, issuing invoices and paying taxes, the company is packaged and maintained, and the "five flows into one" of logistics, capital flow, information flow, contract flow, and bill flow are achieved, making the company appear to be operating normally. The maintenance period ranges from 3 to 9 months. threat actors can generally obtain corporate loans ranging from 4 million to 10 million from a debtor, and the debtor can get 40% to 50% of the loan amount;

Fast Enterprise: It has been found that threat actors can circumvent bank access rules through invisible transfers (banks cannot judge the actual changes of enterprises through industrial and commercial information), and can quickly raise funds and fraudulent loans in 20-45 days. This method of threat actors is called "Quick Enterprise";

Slow Enterprise: threat actors truly change business information, maintain it for 3-6 months, and then start financing and fraudulent loans. threat actors are called "Slow Enterprise".

4. Apply for car loans: threat actors advance the down payment to the debtor, and cooperate with local car dealers to match the debtor with high-priced car loans (usually

For first-hand new cars), after picking up the car, the vehicle will be disposed of and cashed out. A debtor can apply for multiple car loans, and the total loan amount can be up to 2 million. After the car dealer excludes down payment, vehicle purchase fee, depreciation fee, license fee and other related expenses, the amount obtained by the debtor is 40% to 60% of the total car loan.

## 3.1.2 Risk Analysis

threat actors gather low-income people who do not have the qualifications for large loans and apply for the "House Credit Enterprise Automobile" large loan debt business by packaging their qualifications. In order to avoid being classified as fraud, threat actors often give debtors normal repayments ranging from 6 months to 2 years, and then directly ignore the overdue payments.

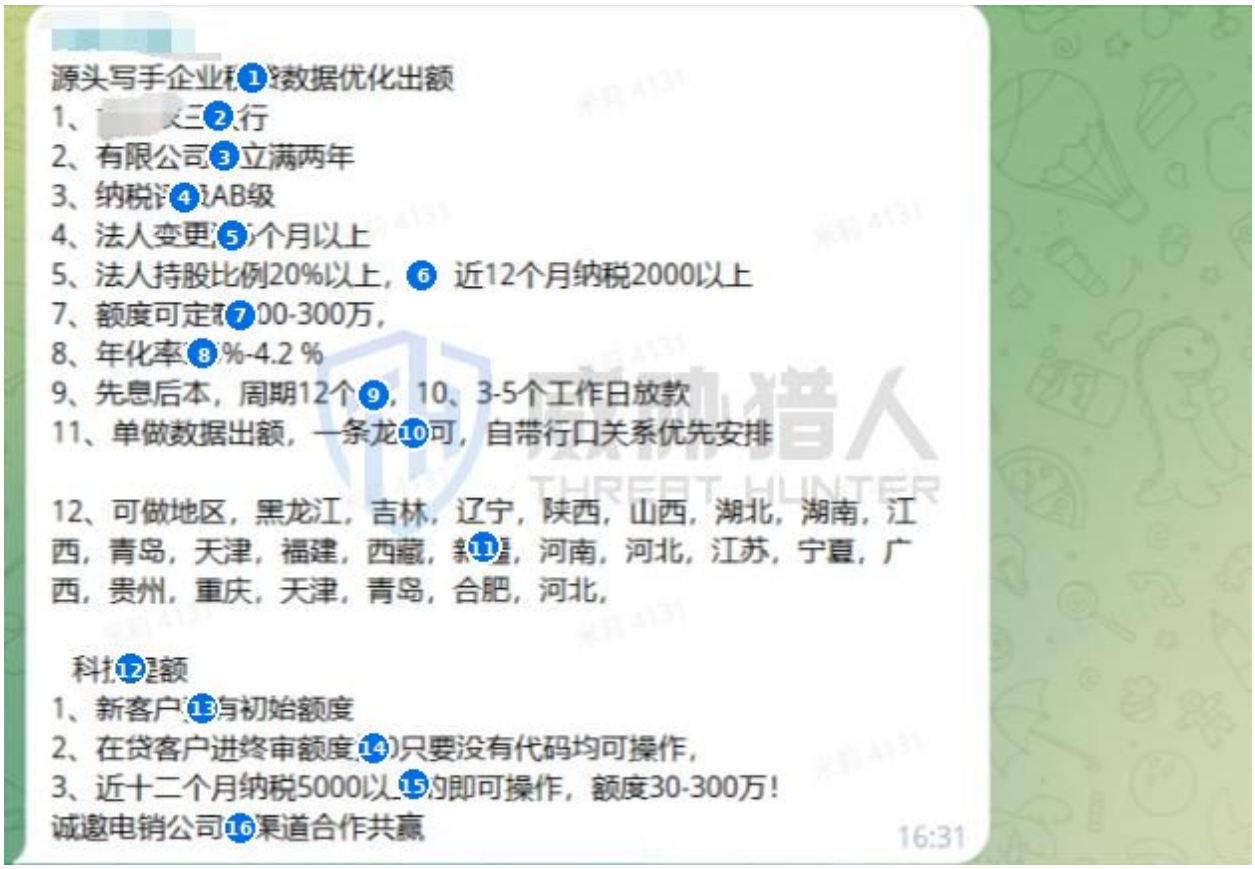
For the debtor, the profit amount is 40% to 50% of the total loan amount, or even less. The debtor does not have the ability to repay the loan in full, and will be classified as a dishonest executor and face the risk of legal sanctions; for the lending financial institution, this type of loan directly becomes a non-performing asset, increasing the internal non-performing rate, and ultimately the lending institution bears all losses.

## 3.2 Technology quota increase: “Technology” quota increase by adjusting tax data, increasing the risk of malicious fraud for banking institutions

### 3.2.1 Operation method

Technology limit increase mainly refers to the use of technology by threat actors to optimize credit evaluation or improve credit scores, thereby increasing credit limits, mainly for corporate loans that have channels to increase credit limits.

Threat Hunter's monitoring found that some threat actors released advertisements on different channels to increase the credit limit of different loans such as corporate loans. threat actors stated that they provide credit limit increase services to various intermediary companies, telemarketing companies, and individual customers. As long as the corporate loan has an initial limit and has a limit increase channel, the credit limit can be increased. The following are the technology limit increase advertisements monitored by Threat Hunter on an encrypted messaging app:




**A "tech limit increase" ad offering to unlock business tax loans by altering tax data**

Source: Threat Hunter original report, page 20. Original image retained; numbered translations added by Threat Hunter.

## Figure guide

| | |
|---|---|
| 1 | Direct source: tax-data optimization to unlock business tax loans |
| 2 | 1. ... the three largest banks |
| 3 | 2. Limited company registered for two years |
| 4 | 3. Tax rating A or B |
| 5 | 4. Legal representative changed at least 6 months ago |
| 6 | 5. Legal representative holds over 20%; 6. Tax paid over 2,000 in the last 12 months |
| 7 | 7. Custom amount CNY 1–3 million |
| 8 | 8. Annual rate 3.6%–4.2% |
| 9 | 9. Interest first, principal at maturity; 12-month term; 10. Paid out in 3–5 working days |
| 10 | 11. Data-only limit unlock or full service; clients with their own bank contacts get priority |
| 11 | 12. Regions served: Heilongjiang, Jilin, Liaoning, Shaanxi, Shanxi, Hubei, Hunan, Jiangxi, Qingdao, Tianjin, Fujian, Tibet, Xinjiang, Henan, Hebei, Jiangsu, Ningxia, Guangxi, Guizhou, Chongqing, Hefei |
| 12 | Tech limit increase |
| 13 | 1. New clients need an existing credit line |
| 14 | 2. Clients with loans whose final-review limit is 0 can be processed if they carry no rejection code |
| 15 | 3. Tax over 5,000 in the last 12 months qualifies; amount CNY 0.3–3 million |
| 16 | Telemarketing firms and channels welcome to partner |

Further research by Threat Hunter found that before carrying out technological quota increases, in line with the principle of "forging iron requires one's own hard work", threat actors intermediaries need to confirm whether the basic situation of corporate customers meets the basic quota and access conditions for bank loans, and handle the quota increase services for customers through online and offline methods. Online mainly involves intermediaries signing electronic agreements with customers, while offline handling mainly involves customers signing intermediary service contracts with intermediary companies and conducting face-to-face processing.

The main operating procedures for technology quota increase are as follows:

1. threat actors ask for customer loan account information and log in to the customer loan account to verify the customer's situation, mainly for enterprises.

Modify tax data based on business information. Different companies and banks have different requirements, and the actual operation will also be different.

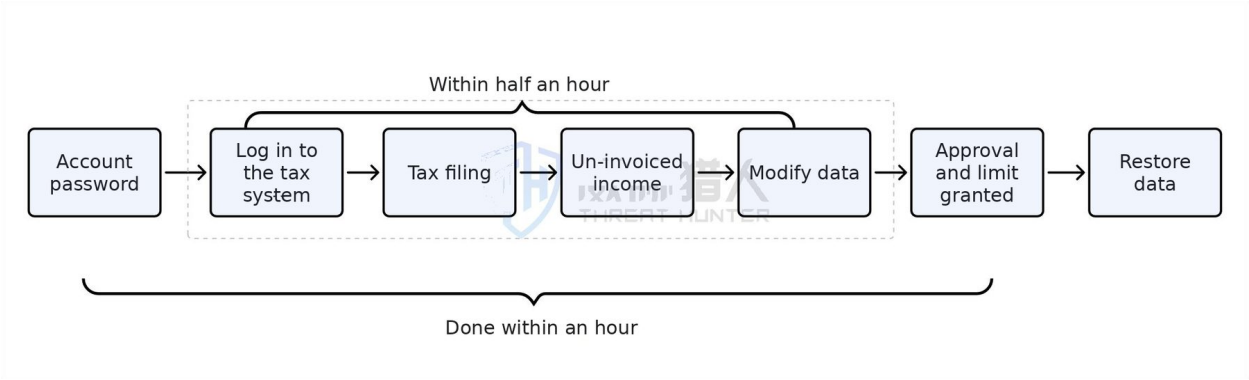
2. The threat actors intermediary can "correct the declaration" according to the rules of the company's tax return, ask for the customer's tax account password, and log in

Record the customer's tax account and enter the login verification code. The login path is: Log in to the account - enter the verification code - I want to do taxes - declare and pay - correct the declaration - non-invoicing income - modify the data.

3. After checking the customer’s tax information, modify the data of the customer’s non-invoiced income section according to the tax data to satisfy the bank.

Amount increase request. It only takes half an hour to modify the data. After the client successfully applies for an increase, the intermediary can log in to the client's tax system to restore the original data to avoid affecting business operations and incurring more tax costs.

The following is the operation process for modifying tax data:




**Steps to alter tax data for a credit-limit increase, completed within an hour**

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

## 3.2.2 Risk Analysis

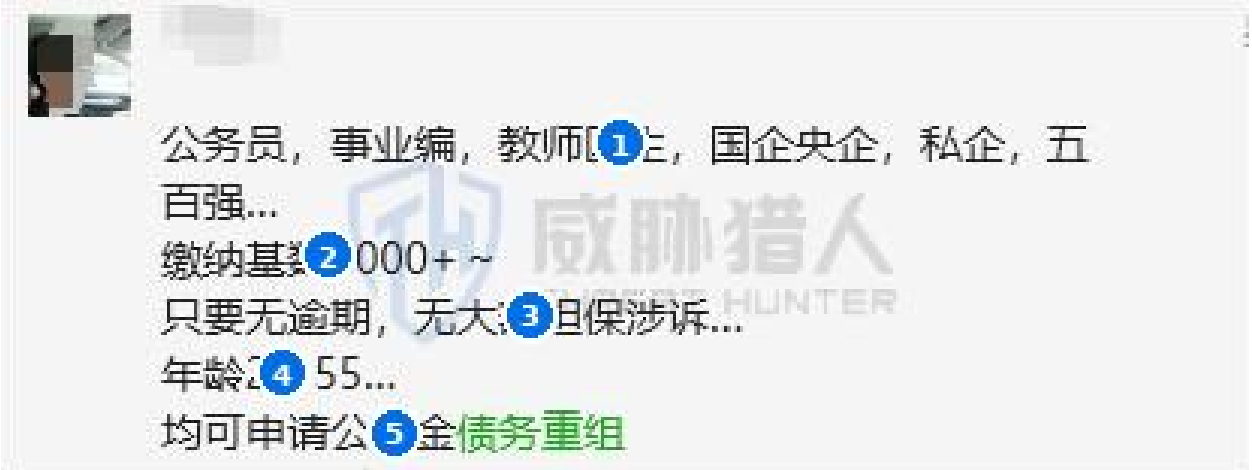
Under the premise that the tax system data is consistent with the ticketing system data, threat actors intermediary modify the unticketed income data in the tax system to increase the overall business sales of the company, so that the turnover reaches the target amount, thereby easily increasing the amount.

Through false data, companies that do not have the qualifications to increase their quotas can obtain higher quotas and charge business owners related fees. This will increase corporate borrowing costs and will also bring uncontrollable fraud risks to banks.

## 3.3 Debt restructuring: threat actors "pre-advance funds" to help customers pay off debts, thereby obtaining large credit loans

"Debt restructuring" refers to threat actors intermediaries helping target customers pay off their debts and maintain their credit through "pre-stage advances", etc., so that they are eligible to apply for higher amounts of "credit loans". Debt restructuring mainly involves provident fund loans.

Threat Hunter's research found that, unlike white debtors, those who undergo "debt restructuring" are usually high-quality employees with stable jobs such as civil servants, doctors, teachers, and employees of listed companies. Such customers often have extremely high debts and can no longer obtain bank loans on their own. They urgently need to obtain large loans to relieve financial pressure.




**A "debt restructuring" ad targeting employees with housing-fund contributions**

Source: Threat Hunter original report, page 22. Original image retained; numbered translations added by Threat Hunter.

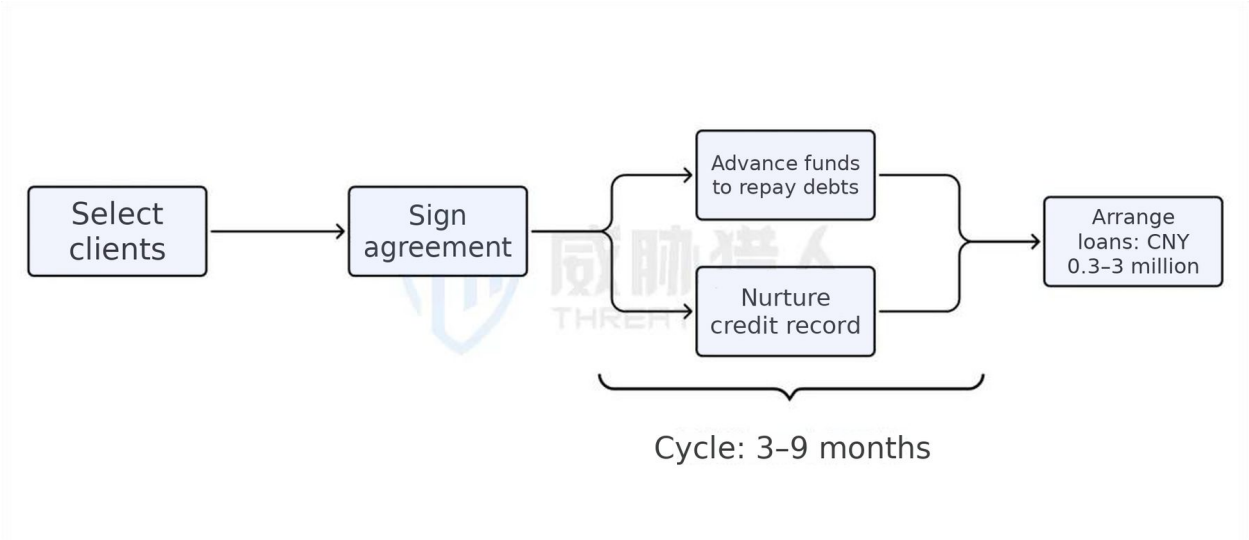
### Figure guide

| | |
|---|---|
| 1 | Civil servants, public-institution staff, teachers, doctors, state-owned and central enterprises, private firms, top 500 companies ... |
| 2 | Contribution base over 3,000 |
| 3 | No overdue loans, no large guarantees or litigation ... |
| 4 | Age 22–55 ... |
| 5 | All can apply for housing-fund debt restructuring |

After the threat actors intermediary helps the debtor advance funds to pay off the debt, he will apply for a qualified provident fund loan. Generally, he will handle multiple bank loans in a short period of time. The target customer is the main beneficiary. After the loan is completed, the threat actors intermediary will charge a high handling fee ranging from 20% to 30%. After the debt restructuring is completed, the customer is burdened with a higher loan amount and also has to bear high handling fees from threat actors, resulting in extremely high borrowing costs and extremely high overdue risks.

## 3.3.1 Operation method

The main operating procedures of threat actors intermediary for debt restructuring are as follows:




**Debt-restructuring process: select clients, sign an agreement, advance funds and nurture the credit record for 3–9 months, then arrange loans of CNY 0.3–3 million**

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

1. Selected customers

threat actors intermediaries review customer qualifications and debt situations to ensure that after "debt restructuring" the liabilities are offset and the profits achieved meet the expectations of both parties. Take the customer's debt situation as an example. For example, if the customer has a debt of 500,000 yuan, and after evaluation it is found that a loan of 1 million yuan can be obtained through debt restructuring, the threat actors intermediary will choose to accept the order and sign a corresponding contract with the customer.

2. Advance repayment

After selecting the target customers, threat actors advance the funds and repay the money for the customers. In order to avoid bank fraud controls (such as repayment accounts, login equipment, etc.), threat actors will transfer the repayment amount to the customer, allowing the customer to directly operate the repayment. The intermediary will charge a certain advance fee, which generally ranges from 5% to 15% of the repayment amount.

3. Maintenance credit report

The repayment period of the advance is also the time for the customer to maintain their credit report. The period for maintaining their credit report ranges from 3 to 9 months. The length of time depends on the customer's credit report. The better the credit report, the shorter the maintenance time, and vice versa.

4. Apply for a loan

After several months of credit investigation and maintenance, threat actors will apply for provident fund loans that meet the customer's qualifications. Generally, they will handle multiple bank loans in a short period of time, with loan amounts ranging from 300,000 to 3 million. During the financing stage, the intermediary will charge a client agency fee, which generally ranges from 5% to 18% of the financing amount.

### 3.3.2 Risk Analysis

Whether it is an individual customer or a financial institution, "debt restructuring" carries a high risk of fraud. For individual customers, they need to bear the interest on advance funds and subsequent financing service fees. These costs are extremely high, and they will need to bear higher liabilities in the future, and there is a risk of high repayment pressure or even overdue payment. In addition, after threat actors advance funds and repay them, they cannot guarantee that customers will get a 100% successful loan. If they are unable to apply for a bank loan later, the interest on advances provided by threat actors is much higher than the loan interest, and they will fall into the loan sharking scheme.

For subsequent lending financial institutions, individuals who do not have loan qualifications can obtain larger loan amounts from banks in disguised form after debt restructuring, directly assuming the overdue risk of customers.

## 3.4 AB loan: threat actors use other people’s credit reports to commit loan fraud and transfer the lending risk to a third party

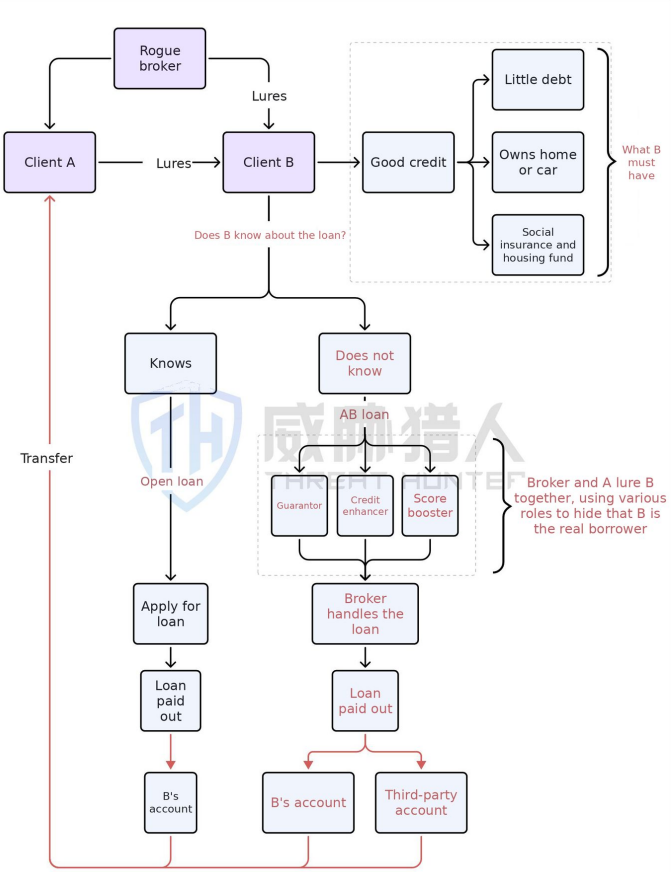
AB loan is a kind of loan fraud, also known as re-lending, loan assistance, arbitrage, and worldly loans. A is a person in need of funds but has poor credit and cannot directly obtain a loan, while B is a person with good credit and is induced to provide guarantee for A or serve as a loan applicant. In fact, the loan funds are used by A, and B becomes the final lender without knowing it, assuming the debt and repayment responsibility.

In recent years, illegal loan incidents of AB Loans have emerged one after another. Regulatory agencies have taken relevant measures, launched special governance actions against illegal loan intermediaries, and rectified and cracked down on offline illegal loan intermediaries in many places. In the first half of 2024, the popularity of AB loan fraud by threat actors has only increased. Threat Hunter visited AB loan companies through on-site research and objectively restored AB loan operating techniques and behavior patterns.

### 3.4.1 Operation method

Although AB Loan is suspected of violating laws and regulations, some threat actors intermediaries still take risks and find customer A through threat-actor groups, Moments and other social platforms and short video platforms, or even through telemarketing (customer A here often has financial needs but does not have loan qualifications).

The main operation process of threat actors intermediary to carry out AB loan fraud is as follows:




**How AB-loan fraud works: a broker and client A lure client B into becoming the real borrower**

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

1. The black intermediary provides false approval result information to client A, promising that it can “do it,” “can approve it,” and “guaranteed payment.”

After a series of lobbying and guidance, target customer B with loan qualifications is provided;

2. Client A joins forces with threat actors to make B believe that the lender is A, and deceives B into acting as a guarantor, credit extender, credit scorer, etc.

A successfully finances, and finally B becomes the actual lender without knowing it;

3. After the loan amount is transferred to B’s account or third-party account, threat actors use various reasons, such as A’s poor qualifications and the need for entrustment.

For payment, the money must be transferred to the guarantor's account, account B needs to be used, etc., and the loan amount from account B is transferred to account A, ultimately completing the fraud.

There is another situation here: clear loan. Different from AB loan, Ming loan means that customer B applies for a bank or institutional loan to customer A with the knowledge of customer AB. In this process, in order to avoid legal punishment, threat actors usually lobby A to get B to agree to help A by being merciful or giving B a certain amount of benefits. In the process, the intermediary will also add fuel to the fire.

### 3.4.1 Risk Analysis

Whether it is AB loan or "Ming loan", there is a huge risk of fraud. For customer A and threat actors, using illegal behaviors to deceive others and harm the interests of others is a serious fraud and faces severe legal sanctions and crackdowns; for customer B, if A fails to repay on time, B will become the actual debtor and need to bear the risk of debt overdue, and even become a dishonest executor; for financial institutions such as banks, A has no loan qualifications but becomes the actual borrower, and even has no ability or willingness to repay. As a borrower, you may not get a penny, but you become the ultimate debtor, with a lower willingness to repay, and banks and other financial institutions bear the final risk.

## Conclusion

## 4. Write at the end

The confrontation with threat actor groups such as financial fraud is dynamic and continuous. With the help of external accurate risk intelligence, major corporate institutions can proactively perceive risks related to credit fraud, understand credit fraud risk types, distribution trends, etc., carry out targeted identification and prevention based on effective data, and rely on the active defense ability of timely perception of risks to further contribute to the safe and stable development of financial digitalization.