THREAT HUNTER RESEARCH

Professional Debt Assumption Risk in Financial Fraud

An investigation into professional debt-assumption schemes, combined lending and the challenge of verifying borrower intent.

Original publication: 2024-04-26
Research team: Threat Hunter Research Team
Source report: 26 pages

Original report text

This text version is reconstructed based on the 26-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.

Preface

"As long as your credit record is clean, an annual salary of one million is not a dream. It can easily help you achieve financial freedom." When you see such an advertisement, you may think it is a phone scam, but in fact it is an unscrupulous intermediary recruiting "professional debtors" in financial fraud under the guise of "helping people take on debts and getting paid millions".

Professional debtors are often people with clean credit records who are in urgent need of large amounts of funds but have no ability to repay. By falsely packaging their personal assets and obtaining high-value loans from banks, these people can earn dozens or even millions of high profits.

The price he paid was to completely abandon his credit record, and even be listed as a defaulter by the court, and he has since become a desperado in financial fraud.

Under the temptation of huge interests, more and more people are joining the army of financial fraud and debt-bearing. Data from the China Enforcement Information Disclosure Network shows that as of April 22, 2024, the number of people subject to enforcement for dishonesty in our country reached 8.33 million. Among these 8.33 million, there are many "professional debtors".

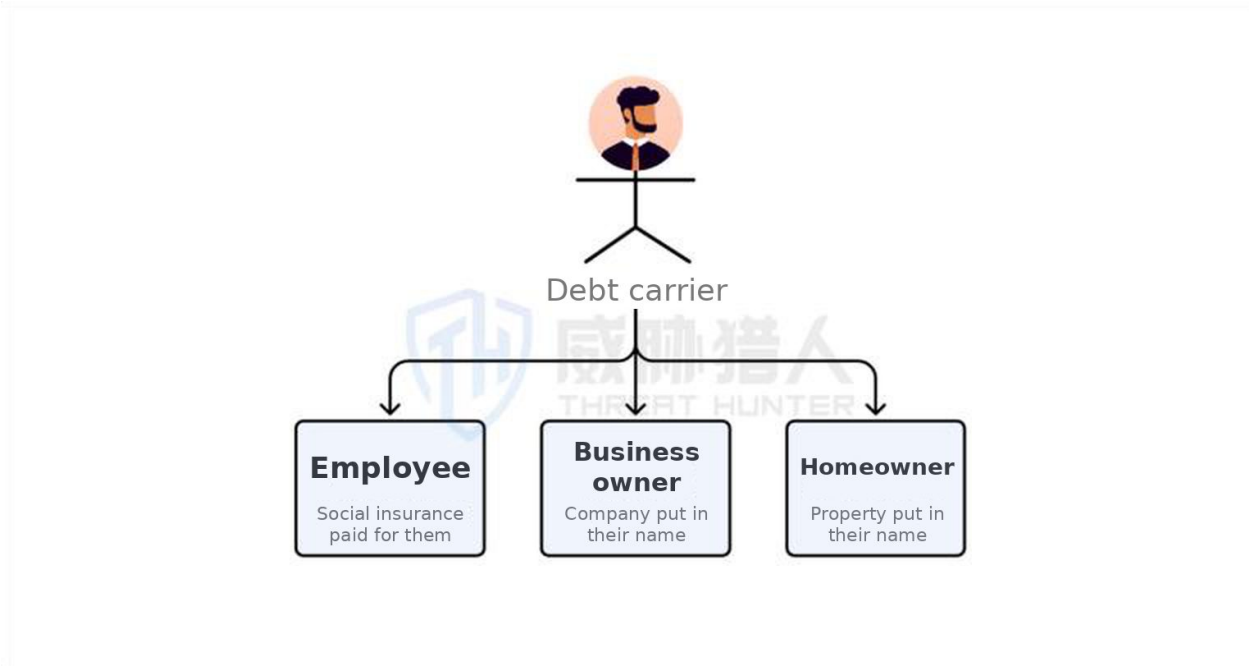
Threat Hunter conducts in-depth research on debt-trading techniques such as "white debtor combination loan debt" and "debt restructuring debt" in financial fraud. Combined with the distribution of debt-related data, it objectively presents professional debt-taking techniques, processes and risk trends in financial fraud, providing a reference for accurate fraud controls of banks and other financial institutions.

Analysis of the Debt Incurrence Process of Portfolio Loans

1. Analysis of portfolio loan debt incurring process

1. Identity packaging of the debtor of the white household

In order to avoid bank fraud controls, enable the debtor to obtain the maximum loan amount from banks and other institutions, and ensure maximum benefits, threat actors will package the debtor with various false identities such as "worker, household head, business owner", etc., as credit enhancement conditions for applying for a loan, such as paying local social security and provident fund to the debtor, transferring real estate/enterprise, fictitious local activity track of the debtor (to avoid restrictions caused by applications in other places), etc.



Identities that intermediaries build for a debt carrier with no credit history: employee, business owner and homeowner

Source: Threat Hunter original report, page 5. Original figure with Chinese text replaced by English.

1.1 Work status

After identifying the debtor, threat actors will first find a "job" for the debtor in a different place and pay social security, provident fund, etc. to make the debtor appear to be living in the local area and provide a good personal qualification basis for subsequent application for a series of loans.

1.2 Identity of head of household

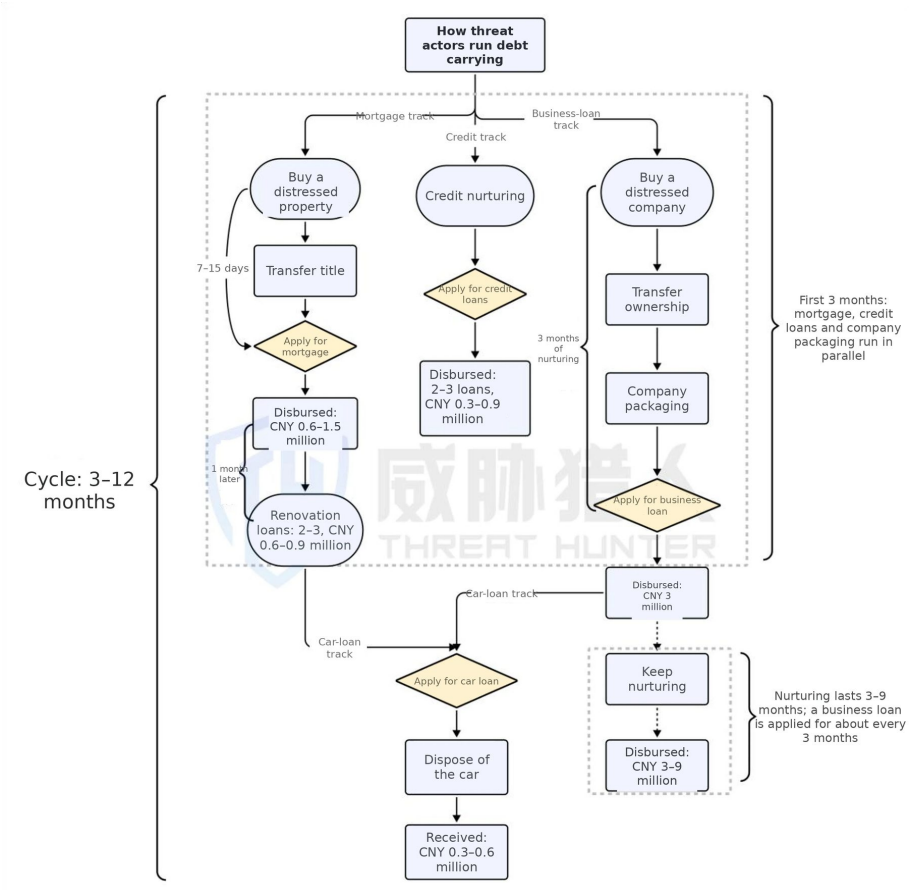
In order to facilitate the smooth subsequent application for mortgage loans, threat actors will transfer the bad property to the debtor and make him the owner of the property. threat actors use special channels to buy "bad packages" on the market at low prices, that is, a combination of "bad real estate + bad companies", and transfer existing houses and companies.

1.3 Business owner identity

In order to apply for a corporate loan, threat actors intermediary will transfer the company to the debtor to make it a legal person. In order to lend a higher amount of corporate loans to banks and other institutions, threat actors intermediary will convert the target enterprise from a general enterprise to a tax grade AB or high-tech enterprise, and use national incentive policies to package the debtor into a business owner with unique enterprise qualifications, thereby obtaining a higher amount of loans. In addition, threat actors will also provide professional training and packaging for some debtors on behavior, conversation, dressing, etc., to make such debtors look more like "businessmen."

2. Portfolio loan debt operation process

After a series of packaging preparations in the early stage, threat actors began to use the various qualifications of the debtor to carry out one-stop large-scale financing of "housing loans, credit loans, corporate loans, car loans". It is understood that the total amount of fraudulent loans by a debtor ranges from 5 to 20 million, and the actual amount received is 40%-60% of the total debt. The specific operation process is as follows:



How threat actors run combined-loan debt carrying: mortgage, credit, business-loan and car-loan tracks over a 3–12-month cycle

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

2.1 Transferring real estate: threat actors transfer properties bought at low prices to debtors at high prices, while fabricating false high-value transactions

The contract inflates the appraised value.

2.2 Apply for mortgages and credit loans: threat actors help debtors apply for mortgages and teach them how to deal with bank approvals and mortgage approvals

About a month after recovering, I applied for 2-3 renovation loans, and at the same time applied for personal credit loans for the debtors. After the mortgage and credit loans were received, part of them was given to the debtors, part was given to the black intermediaries as commissions, and the remaining part was used as repayment amount and subsequent operating cost funds.

2.3 Transferring companies: threat actors transfer bad companies bought at low prices to debtors. This process is often synchronized with the mortgage loan.

operation.

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".

2.4 Packaging company materials: threat actors intermediaries carry out corporate packaging and maintenance by traffic manipulation corporate statements, issuing invoices and paying taxes for debtors.

To make the company appear to have normal transaction operations and related tax data, the maintenance period is usually 3 months. The longer the period, the higher the total loan amount.

2.5 Applying for corporate loans: After the corporate packaging meets the bank application conditions, the threat actors intermediary will use a house in the name of the debtor as a credit enhancement

Conditions: Apply for a corporate loan for a debtor. Before applying for a loan, you need to record three videos of the debtor walking, writing, and reading aloud and send them to bank personnel for review. After passing the review, the debtor completes the corporate loan according to the skills and coping skills trained by threat actors.

2.6 Applying for car loans: threat actors cooperate with local car dealers to match high-priced car loans to debtors, and the car dealers eliminate down payments and vehicles.

Purchase fees, depreciation fees, registration fees, insurance premiums and other related expenses, the amount received by the debtor is about 50% of the car loan.

In this fraudulent loan operation, all links, from threat actors to debtors, to real estate agencies, loan agencies, and car dealers, worked closely together to create a huge scam of borrowing debts and defrauding loans. In the end, mortgage loans, car loans, credit loans, corporate loans and other loans were all passed on to debtors, while participants in other links made huge profits.

It is worth noting that "credit loans" are a type of loan that threat actors will inevitably involve in the process of incurring debts, and their methods of arbitrage are also very diverse. In addition to obtaining credit loans through the above-mentioned method of "packaging white debtors", many

threat actors use "debt restructuring" techniques to obtain high-amount credit loans. Threat Hunter conducted further research on the fraudulent loan process of "debt restructuring".

Analysis of Debt Restructuring and Debt Incurrence Process

2. Analysis of Debt Restructuring and Debt Incurrence Process

"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.

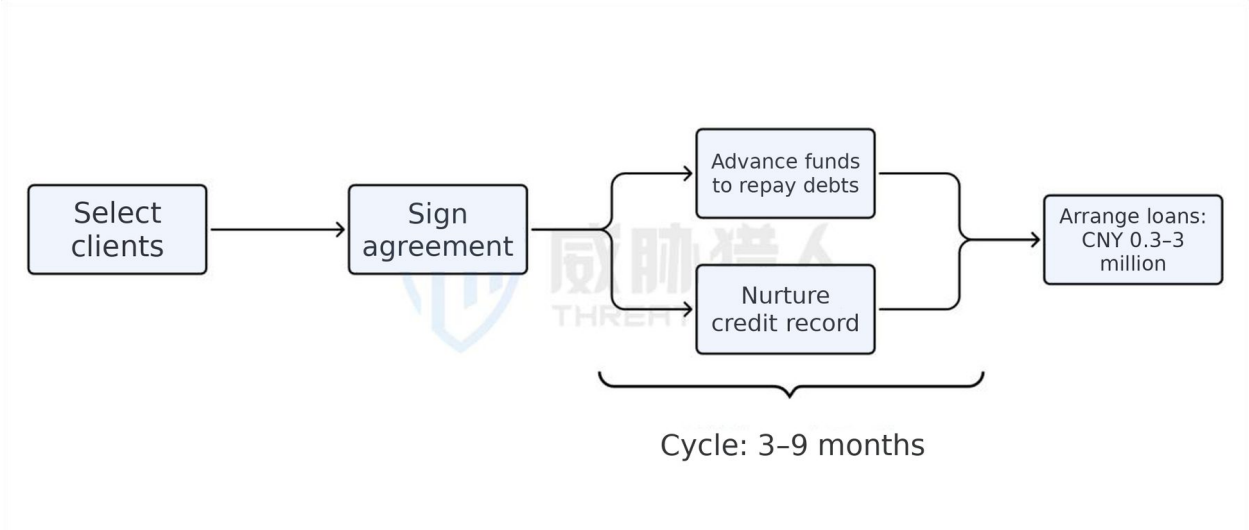
1. Target customers for debt restructuring

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.

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.

2. Debt restructuring and debt operation process

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, with loan amounts ranging from 300,000 to 3 million. 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%. The specific process is 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 10. Original figure with Chinese text replaced by English.

2.1 Selected Customers

threat actors intermediaries review customer qualifications and debt situations to ensure that the profits obtained after "debt restructuring" 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, it is found after evaluation that a loan of 1 million yuan can be obtained through debt restructuring. This ensures that while the debt is offset, the profits obtained by both parties meet expectations. The threat actors intermediary will choose to accept the order and sign a corresponding contract with the customer.

2.2 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 controlss (such as repayment accounts, login devices, etc.), threat actors will transfer the repayment amount to the customer, allowing the customer to directly operate the repayment. During the advance stage, the intermediary will charge a certain advance fee, which generally ranges from 5% to 15% of the repayment amount. The repayment method is gradual. Generally, the customer's historical debt will be settled within 3-9 months based on the customer's credit report.

2.3 Control customers

In the early advance and repayment stage, in order to prevent customers from refusing to accept their debts, threat actors will accurately grasp the customer's home address, workplace and other personal information, and arrange dedicated personnel to track the customer's situation; at the same time, in order to ensure the stability of the customer's credit report, threat actors intermediaries do not allow customers to apply for any other loans during this period. Such customers are generally high-quality unit groups. In order to avoid negative information affecting work, their cooperation is usually high.

2.4 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.

2.5 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.

Whether it is portfolio loan debt or debt restructuring, it is essentially a financial fraud. The main risk of debt is borne by the debtor, who will face a series of irreparable consequences such as fines and criminal liability. Threat Hunter conducted statistical analysis on the intelligence data of threat actors recruiting debtors in the first quarter of 2024, and further objectively presented the trend

changes in communication channels, geographical distribution, quota range and other dimensions of threat actors' debt-taking and loan fraud.

2.1

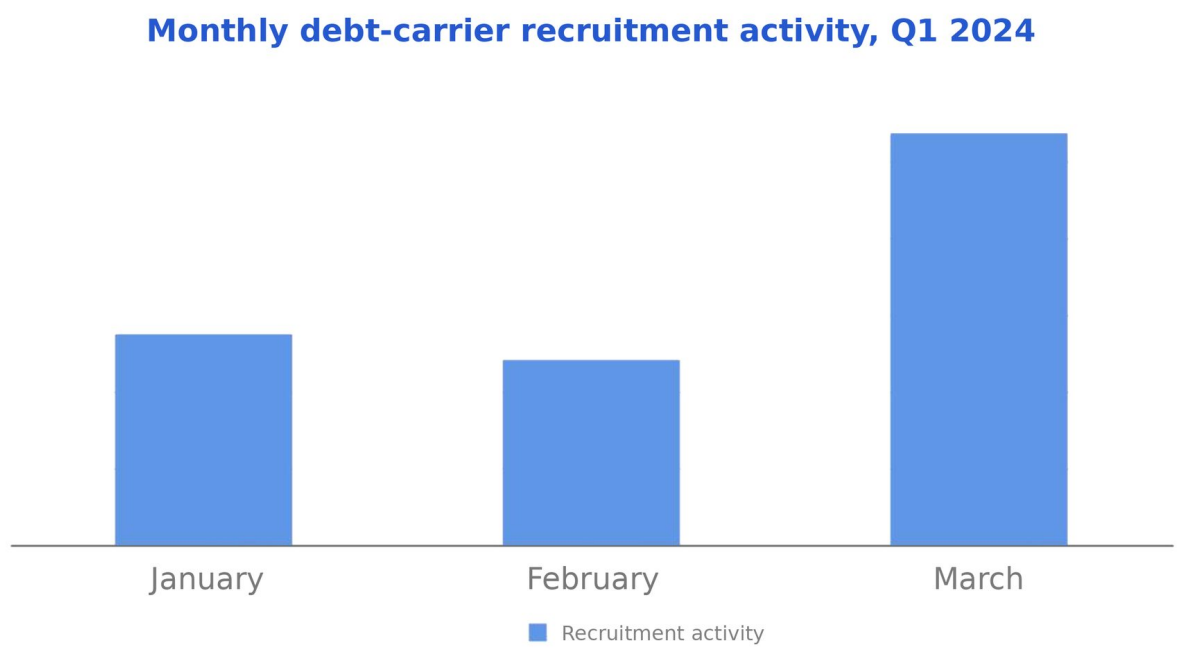
Distribution trend of debt data

3. Distribution trend of debt data

Based on the analysis of debt intelligence data in the first quarter of 2024, Threat Hunter found that the popularity of debt in financial fraud is still on the rise, and there are clusters in some areas. The specific situation is as follows:

1. The popularity of debt-taking will not decrease in the first quarter of 2024, and the popularity of debt-taking increased significantly in March

Judging from the amount of debt intelligence data monitored by Threat Hunter in the first quarter of 2024, the popularity of threat actors recruiting debtors continued to rise every month in 2024. The popularity of promotion increased significantly in March, and the amount of debt intelligence data in March increased by 120% compared with February.



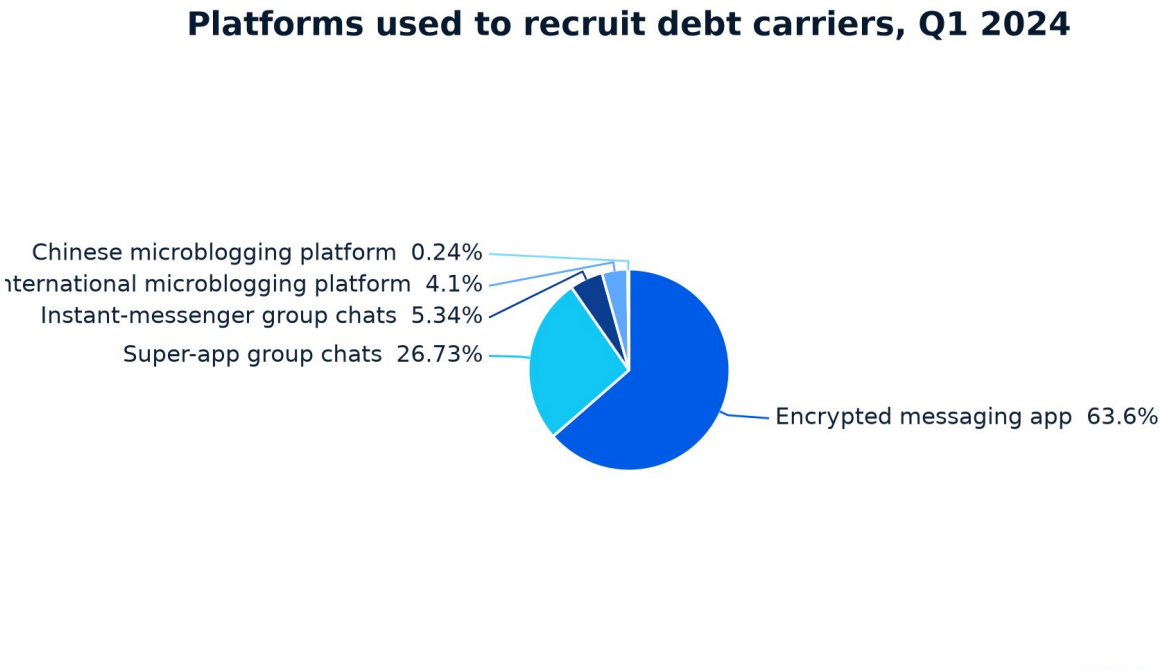
Debt-carrier recruitment activity rose in Q1 2024; March was up 120% on February. The original chart has no value axis, so bar heights show relative activity only.

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

2. An encrypted messaging app has become the main channel for threat actors to recruit debtors and communicate, accounting for up to

64%

Threat Hunter's research found that threat actors mainly publish recruitment advertisements and communicate online through mainstream social platforms. The content of the advertisements involves debtor conditions, loan types, debt amounts, amounts received by debtors, etc. Debt intelligence data from an encrypted messaging app accounted for as much as 64%, becoming the main channel for threat actors to recruit debtors and communicate.



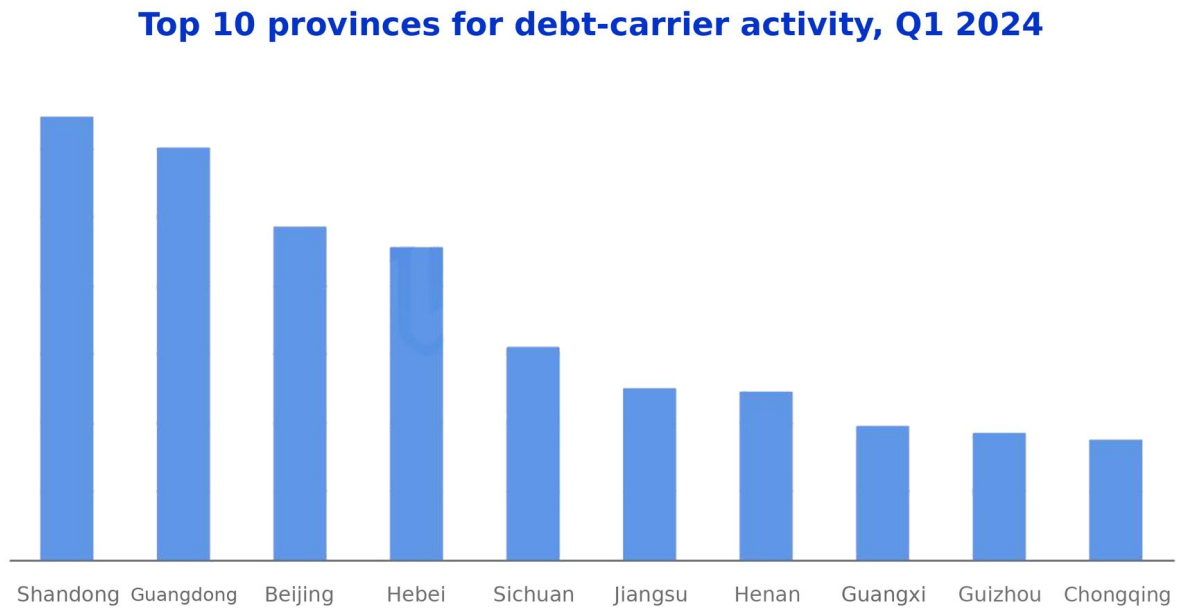
Platforms used to recruit and talk to debt carriers, Q1 2024: an encrypted messaging app accounts for 63.6%

Source: Threat Hunter original report, page 15. Redrawn in English from the original figure.

3. Distribution of provinces and cities where debt data comes from

3.1 The three provinces with the highest debt load in the first quarter of 2024: Shandong, Guangdong, and Beijing

Threat Hunter used intelligence technology to obtain the source provinces of debt data and found that the three provinces of Shandong, Guangdong, and Beijing (including municipalities directly under the Central Government) have a high degree of debt indebtedness. The top 10 provinces where debt data comes from in the first quarter of 2024 are as shown in the figure below:

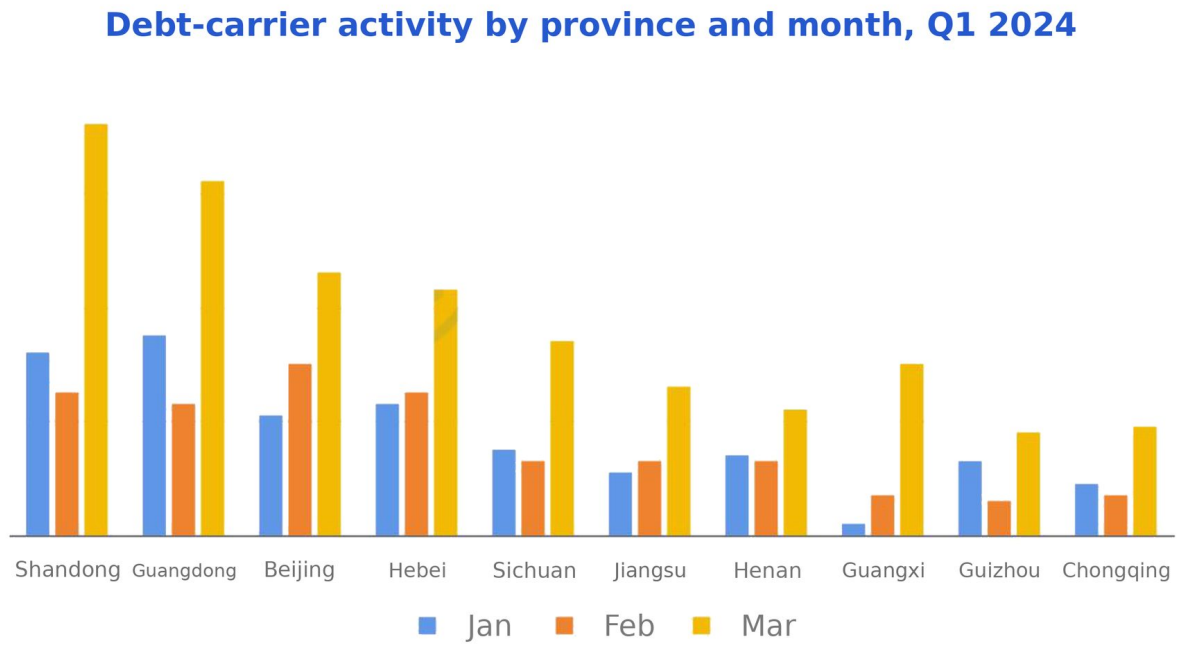


Top 10 provinces for debt-carrier activity in Q1 2024: Shandong, Guangdong and Beijing lead. The original chart has no value axis, so bar heights show relative activity only.

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

3.2 In March 2024, the three provinces of Guangxi, Sichuan, and Chongqing saw a significant increase in debt incurrence

As mentioned above, the popularity of threat actors recruiting debtors increased significantly in March 2024. Threat Hunter research and statistics found that the popularity of debtors in the three provinces of Guangxi, Sichuan, and Chongqing increased significantly in March 2024, mainly reflected in the increase in the number of threat actors gangs.

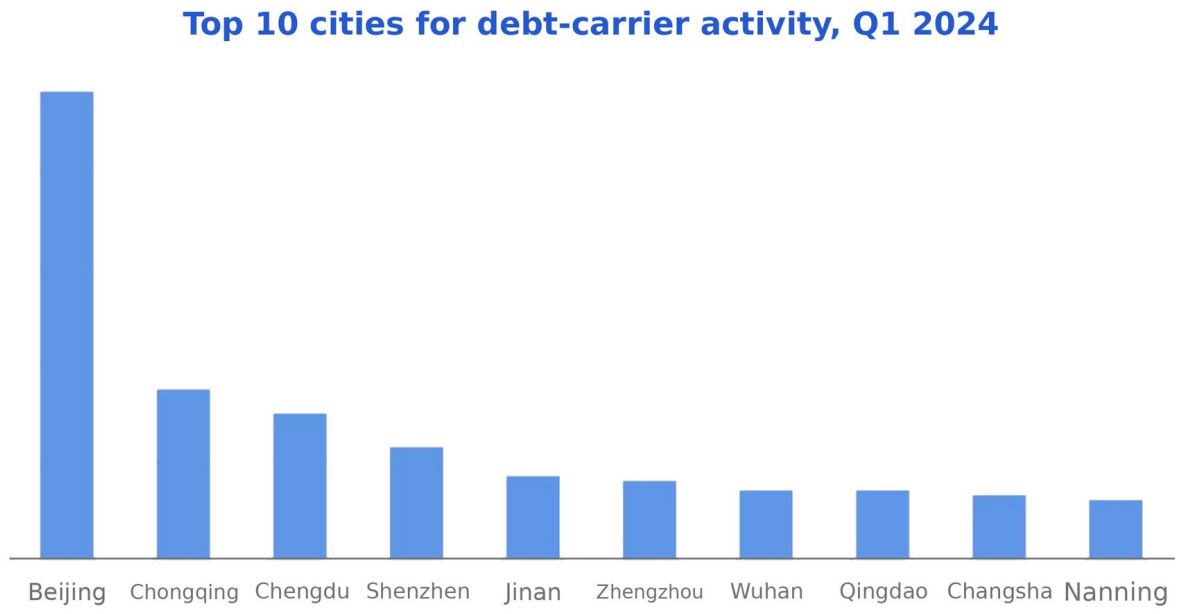


Debt-carrier activity by province and month, Q1 2024: Guangxi, Sichuan and Chongqing rose sharply in March. The original chart has no value axis, so bar heights show relative activity only.

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

3.3 The three cities with the highest debt burden in the first quarter of 2024: Beijing, Chongqing, and Chengdu

Judging from the city distribution of debt incurring data, the three cities with the highest debt incurring intensity in the first quarter of 2024 are Beijing, Chongqing, and Chengdu. Among them, Beijing's debt incurring intensity is much higher than other cities.



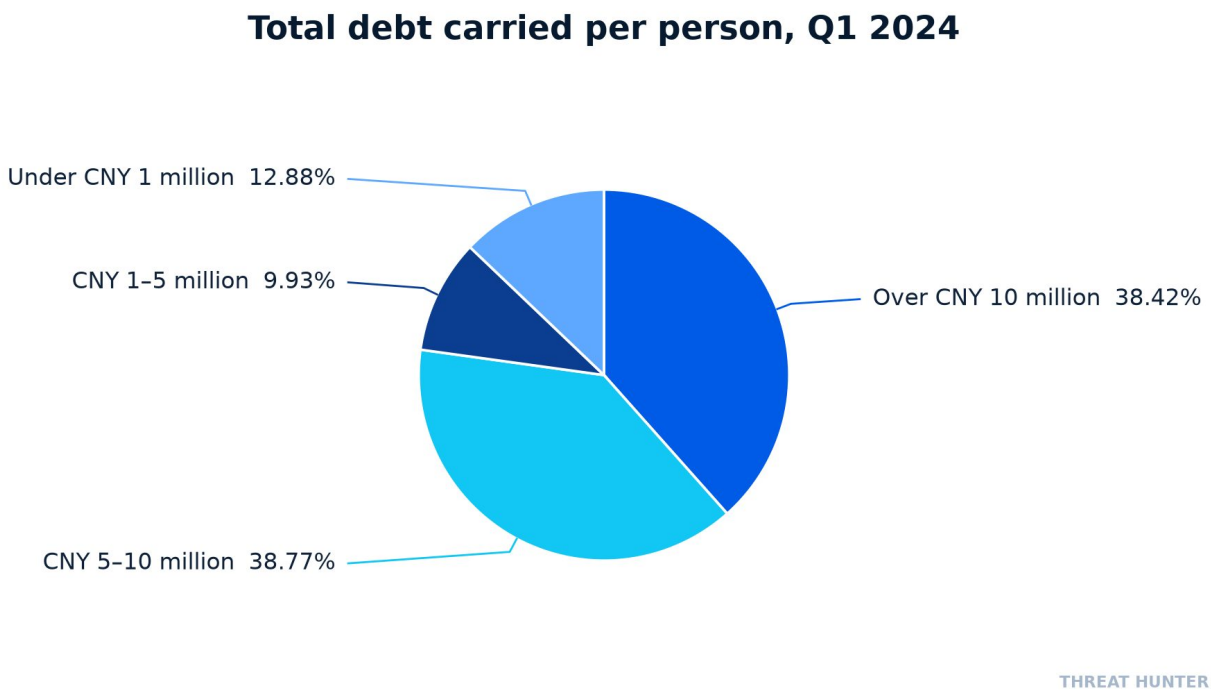
Top 10 cities for debt-carrier activity in Q1 2024: Beijing is far ahead, followed by Chongqing and Chengdu. The original chart has no value axis, so bar heights show relative activity only.

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

4. Distribution of total debt amount

4.1 The debt amount is mainly large-amount loans of more than 5 million yuan, and the proportion of more than 10 million yuan accounts for 38%

Threat Hunter analyzed the distribution of the total debt limit and found that the debt limit is mainly large loans of more than 5 million yuan. The total debt limit of a single debtor is more than 5 million yuan, accounting for about 77%. Among them, the total debt limit is more than 10 million yuan, accounting for 38%, and the total debt limit is between 5 million and 10 million yuan, accounting for about 39%.



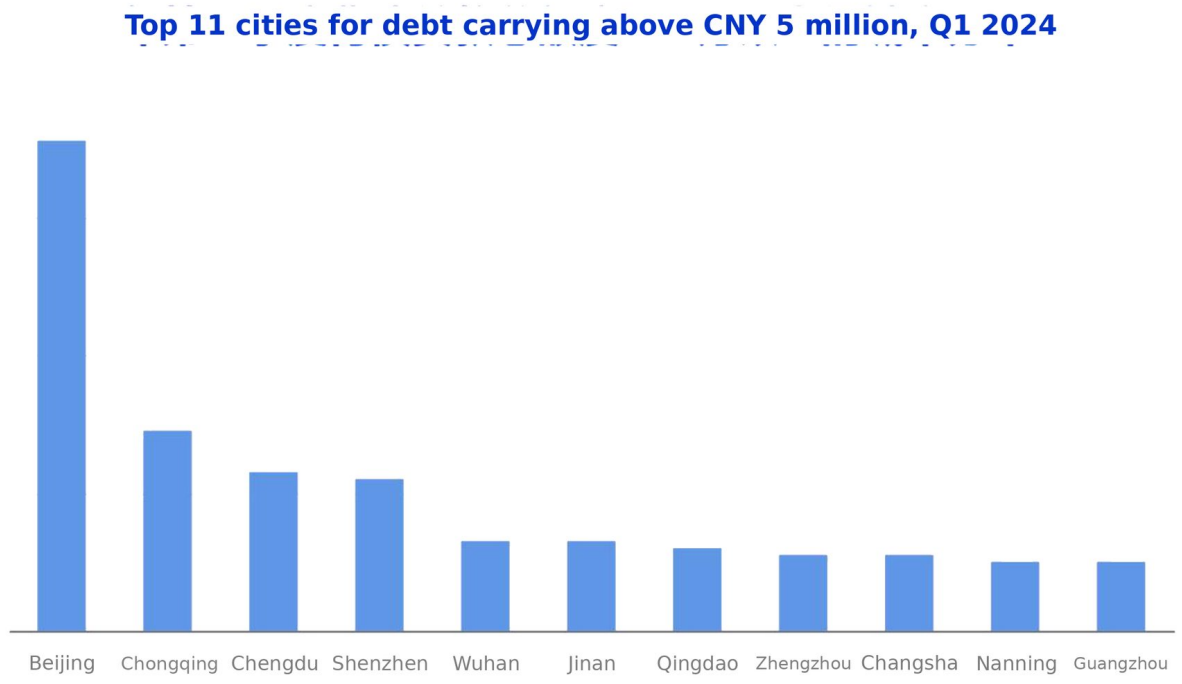
Total debt carried per person, Q1 2024: 77% of debt carriers take on more than CNY 5 million

Source: Threat Hunter original report, page 18. Redrawn in English from the original figure.

4.2 Judging from the city distribution of large-amount debt data, Beijing has the highest popularity for large-amount debts

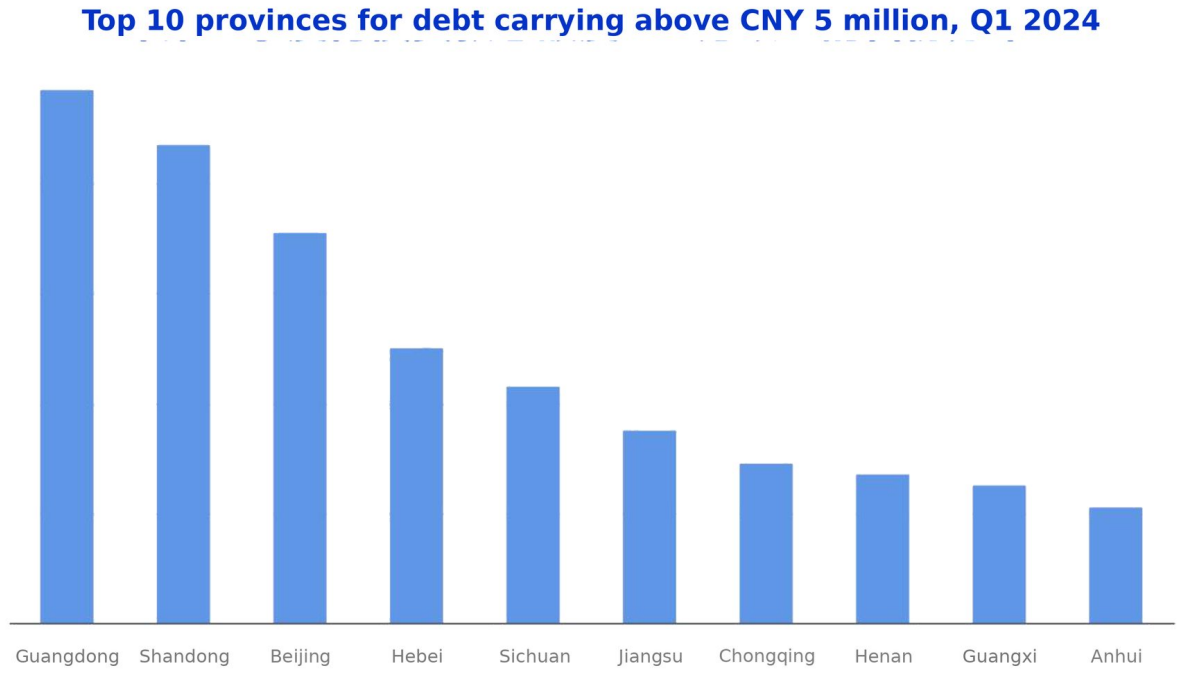
From the perspective of city data distribution, among the top 11 cities with a total debt of more than 5 million, Beijing is much more popular for large-amount debts than other cities, becoming the city with the highest popularity for large-amount debts, followed by Chongqing and Chengdu. From the perspective of provincial data distribution, among the top ten provinces (including municipalities) with a total debt amount of more than 5 million, Guangdong Province, Shandong Province, and Beijing City rank among the top three.

Note: The "large amount of debt" here refers to a debt amount of more than 5 million.



Top 11 cities for large-sum debt carrying (over CNY 5 million) in Q1 2024: Beijing leads, followed by Chongqing and Chengdu. The original chart has no value axis, so bar heights show relative activity only.

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



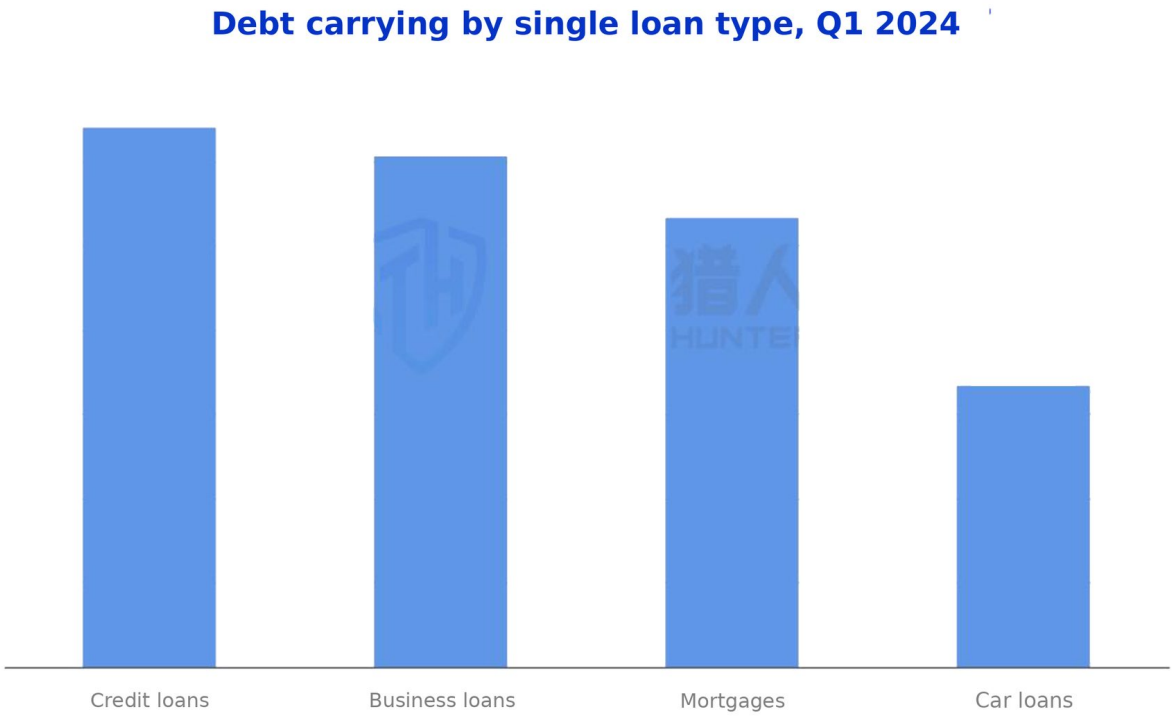
Top 10 provinces for large-sum debt carrying (over CNY 5 million) in Q1 2024: Guangdong, Shandong and Beijing lead. The original chart has no value axis, so bar heights show relative activity only.

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

5. Distribution of debtor loan types

5.1 Among the main loan types of debtors, credit loans and enterprise loans are more prominent.

The main types of loans on the market include credit loans, enterprise loans, housing loans, car loans, etc. Through analysis of individual loan types, it was found that in the first quarter of 2024, credit loans and enterprise loans were more prominent among the main loan types of debtors.



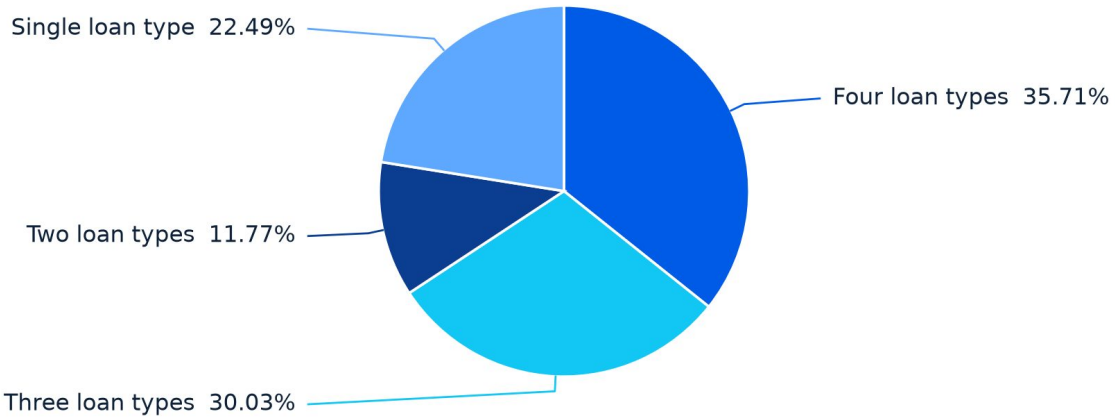
Debt carrying by loan type in Q1 2024: credit loans and business loans stand out. The original chart has no value axis, so bar heights show relative activity only.

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

5. 2 Among different types of portfolio loans, portfolio loans of more than two types account for the largest proportion, accounting for 78%.

threat actors carry out combined loans through "mortgage loans, credit loans, corporate loans, and car loans". The four types of combined loans of "housing, credit, enterprise and automobile" account for the highest proportion, reaching 36%. From the figure below, the proportion of combined loans of more than two types is as high as 78%. It can be seen that in order to maximize the loan amount and squeeze out the value of the debtor, it has become a trend to use "combination loans" to maximize profits in the debt-bearing business.

Loan combinations used by debt carriers, Q1 2024

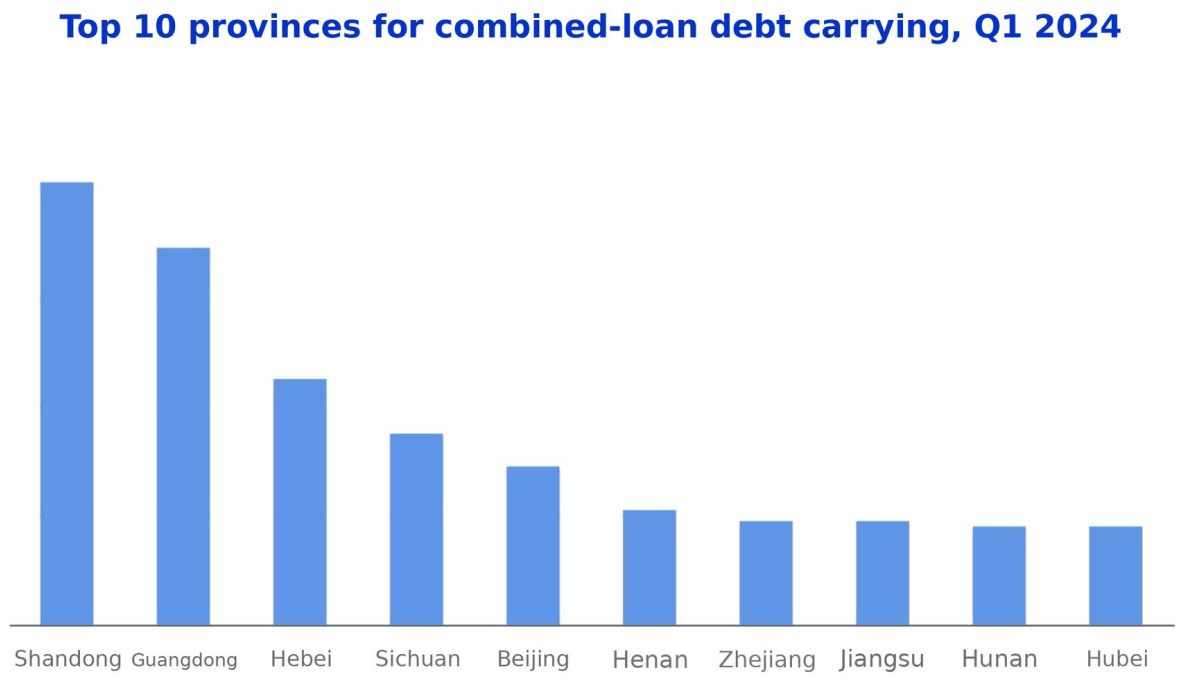


THREAT HUNTER

Loan combinations used by debt carriers, Q1 2024: combinations of two or more loan types make up 78%

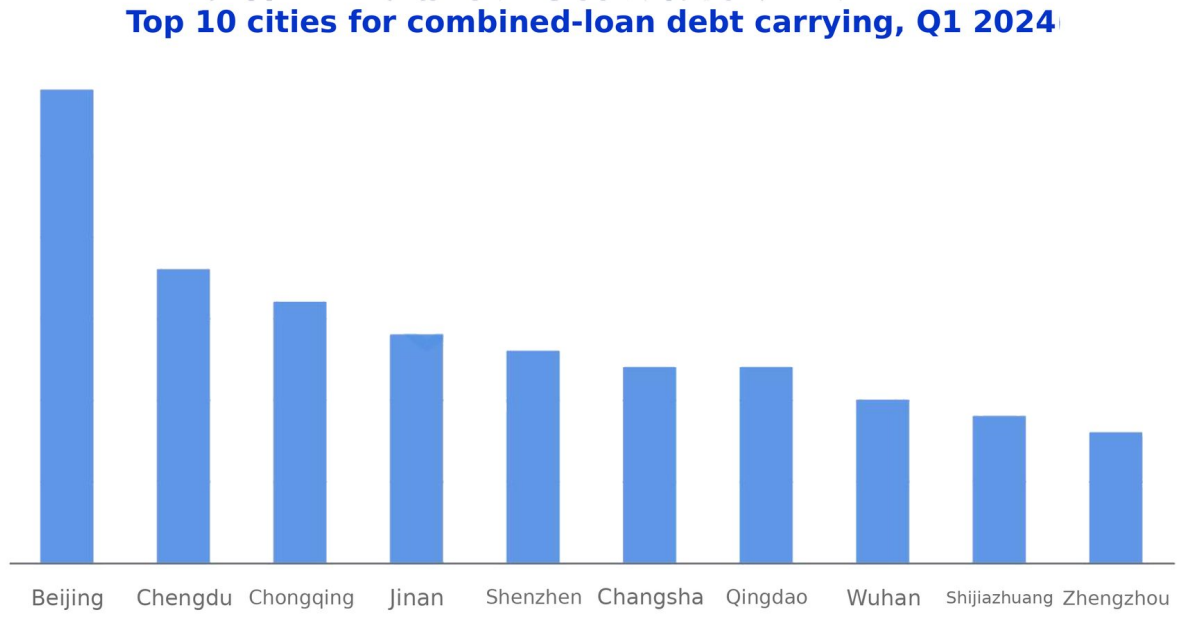
Source: Threat Hunter original report, page 21. Redrawn in English from the original figure.

Threat Hunter conducts a specific analysis of combined loans of type 2 and above. From the perspective of provincial data distribution, Shandong and Guangdong are the most popular for using "combination loans" to carry debt. From the perspective of city data distribution, Beijing is far more popular than other cities.



Top 10 provinces for combined-loan debt carrying in Q1 2024: Shandong and Guangdong lead. The original chart has no value axis, so bar heights show relative activity only.

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

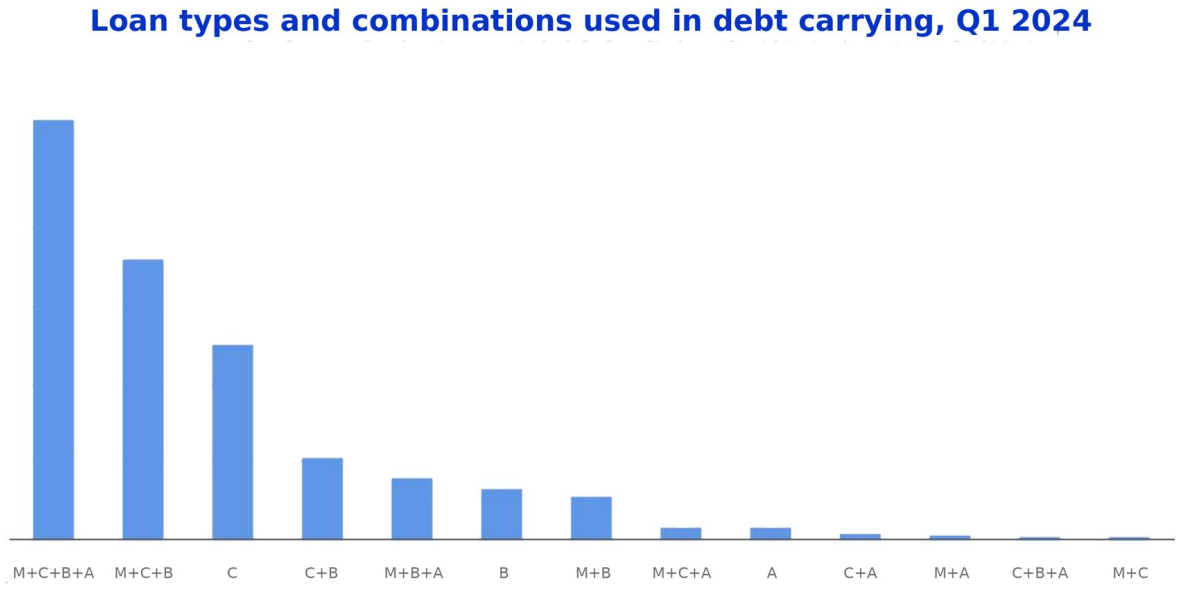


Top 10 cities for combined-loan debt carrying in Q1 2024: Beijing is far ahead of other cities. The original chart has no value axis, so bar heights show relative activity only.

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

5.3 Among the loan types of different combinations, the two combinations of “housing credit enterprise automobile” and “housing credit enterprise” account for the most loans, accounting for up to 60%

Threat Hunter conducted an overall statistical analysis on various loan combinations such as single loans and portfolio loans and found that the two portfolio loans of "housing credit enterprise and automobile" and "housing credit enterprise" accounted for as much as 60%. The four types of loan combinations of "House Credit, Enterprise Automotive" account for the highest proportion, which further proves that the current "one-stop" debt-taking and loan-defrauding methods of threat actors have gradually matured.



Loan types and combinations used in debt carrying, Q1 2024 (M = mortgage, C = credit loan, B = business loan, A = car loan): mortgage + credit + business + car and mortgage + credit + business together account for 60%. The original chart has no value axis, so bar heights show relative activity only.

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

Trend summary

In the first quarter of 2024, the amount of intelligence data related to the recruitment of debtors by threat actors continues to increase. The current situation of debt-taking and loan fraud in financial fraud is still severe. Timely attention to debt-taking and loan fraud and the monitoring and prevention of potential risks have become a major challenge for companies in finance and other industries.

Judging from the debt-taking methods and data trends of threat actors in the first quarter of 2024, companies need to focus on the following issues:

1. The popularity of debt-taking and loan fraud continued in the first quarter of 2024, and the popularity increased significantly in March

In the first quarter of 2024, the monthly popularity of threat actors recruiting debtors continued to rise, and its promotion popularity increased significantly in March. The amount of intelligence data on threat actors recruiting debtors increased by 120% in March compared with February.

2. The three provinces (including municipalities) with the highest debt load in the first quarter of 2024: Shandong, Guangdong, and Beijing

Jing Threat Hunter used intelligence technology to obtain the source provinces of debt data and found that Shandong, Guangdong, and Beijing (including municipalities directly under the Central Government) have a relatively high level of debt debt. The three cities with the highest debt load: Beijing, Chongqing, and Chengdu.

3. The debt limit is mainly large-amount loans of more than 5 million yuan, with 38% of debts exceeding 10 million yuan.

Threat Hunter analyzed the distribution of the total debt limit and found that about 77% of individual debtors have a total debt limit of more than 5 million, of which 38% have a total debt limit of more than 10 million, and about 39% have a total debt limit of 5 million to 10 million.

4. The proportion of combined loans of more than 2 types is as high as 78%. In the debt-bearing business, "combination loans" are used to realize

Profit maximization has now become a trend. Among the main loan types for debtors in the first quarter of 2024, credit loans and enterprise loans are more prominent. Among the types of portfolio loans, the proportion of portfolio loans of more than two types is as high as 78%.

5. "Debt restructuring" can obtain credit loans of up to more than 3 million yuan, which has become a key issue for financial institutions.

One of the debt-taking methods is that threat actors intermediaries can obtain up to 600,000 personal credit loans by "packaging white debtors", while threat actors can obtain up to 3 million credit loans by taking on debts through "debt restructuring" ("debt restructuring" enables customers to qualify for higher credit loans). Due to the higher amount of credit loans, debt restructuring has gradually become one of the debt-taking methods that financial institutions need to focus on.

The confrontation with groups of threat actors such as financial fraud is dynamic and continuous. With the help of external accurate risk intelligence, major enterprises and institutions can proactively perceive risks, understand risk attributes, types, distribution trends, etc., conduct 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.

number of events