THREAT HUNTER RESEARCH

H1 2024 Data Breach Risk Report

A half-year analysis of data-breach incidents, the criminal groups behind them and their convergence with downstream fraud.

Original publication: 2024-07-04
Research team: Threat Hunter Research Team
Source report: 36 pages

Original report text

This text version is reconstructed based on the 36-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

In the era of the rapidly emerging digital economy, data is the core asset and important strategic resource of enterprises. While it is growing at a rapid pace, the data risks behind it are also rising. The increasingly complex data leakage situation has become a serious obstacle to the digital development of enterprises.

Threat Hunter's "Data Breach Risk Landscape Report for the First Half of 2024" conducts a detailed analysis of the data asset leakage risk profile and threat-actor data trading market in the first half of 2024. Combined with typical industry cases, it presents a multi-dimensional panoramic view of the domestic data leakage situation in the first half of 2024:

1. In the first half of 2024, 16,011 effective data leakage incidents were monitored, analyzed and verified across the entire network, which is higher than the number in the second half of 2023.

An increase of 59.58%, a total of 9539 cases;

2. Among the 34,000 threat actors gangs monitored in the first half of 2024, analysis has verified that the threat actors involved in real data leakage incidents

There are 1,973 gangs in total, an increase of 984 from the second half of 2023, nearly doubling.

3. From the perspective of industry distribution, data breaches in the first half of 2024 involved 85 industries, with the number of data breaches in the Top 5

The industries are banking, e-commerce, consumer finance, insurance, and express delivery;

4. From the perspective of region, age, gender and other dimensions, the regions with the largest number of data breaches in the first half of 2024 are: Zhejiang

Jiangsu, Sichuan, and Guangdong; the highest proportion of people aged 35-54 is 62%; the highest proportion of women is 64%.

5. Research on the threat-actor data trading market found that fraud activities using built-in smartphone video calls increased in the first half of 2024.

In the first half of the year, there were as many as 1,237 related risk events involving the "iOS" field in the leaked data, an increase of 8 times compared with the second half of 2023.

Related noun definitions:

1. DRRC: Threat Hunter established two DRRC digital risk emergency response centers in Shenzhen and Chongqing, bringing together 30+ security experts

Operation experts provide 7×24-hour emergency response services to enterprises;

2. Authenticity verification engine: through the extraction and comparison of personal elements of different file types, and in the image OCR results

Extract and verify the elements to effectively identify whether the image content contains forged data/historical leaked data;

3. Data leakage intelligence: Threat Hunter captured “unauthorized personal/organizational sensitive information through encrypted messaging groups, dark web and other channels”

"Publicly traded or used" intelligence information may include historical data, duplicate data, etc., and is often of huge magnitude;

4. Data leakage incidents: Threat Hunter security research experts analyze, verify and troubleshoot data leakage intelligence samples, etc.

Remove historical false data and confirm valid data leakage incidents;

5. Citizen personal information: refers to citizens’ personal identity information, including but not limited to name, ID number, date of birth, phone number, etc.

Phone number, home address, bank account information, etc.;

6. Historical personal information: refers to personal information that has been leaked before this data leakage incident, a lot of historical personal information

Collected and integrated into a social engineering library by threat actors;

7. Darknet: refers to a hidden network that ordinary netizens cannot search and access through conventional means. They need to use some specific software.

Configuration or authorization is required to log in;

8. Private group: A group that can only be entered through an invitation link/administrator's approval. Generally, outsiders cannot monitor or enter.

The group chat.

9. Historical data events: threat actors integrate leaked real information and reuse it for transactions. Usually threat actors will

Perform refined processing of data to supplement the integrity of data fields, thereby increasing data value and profitability;

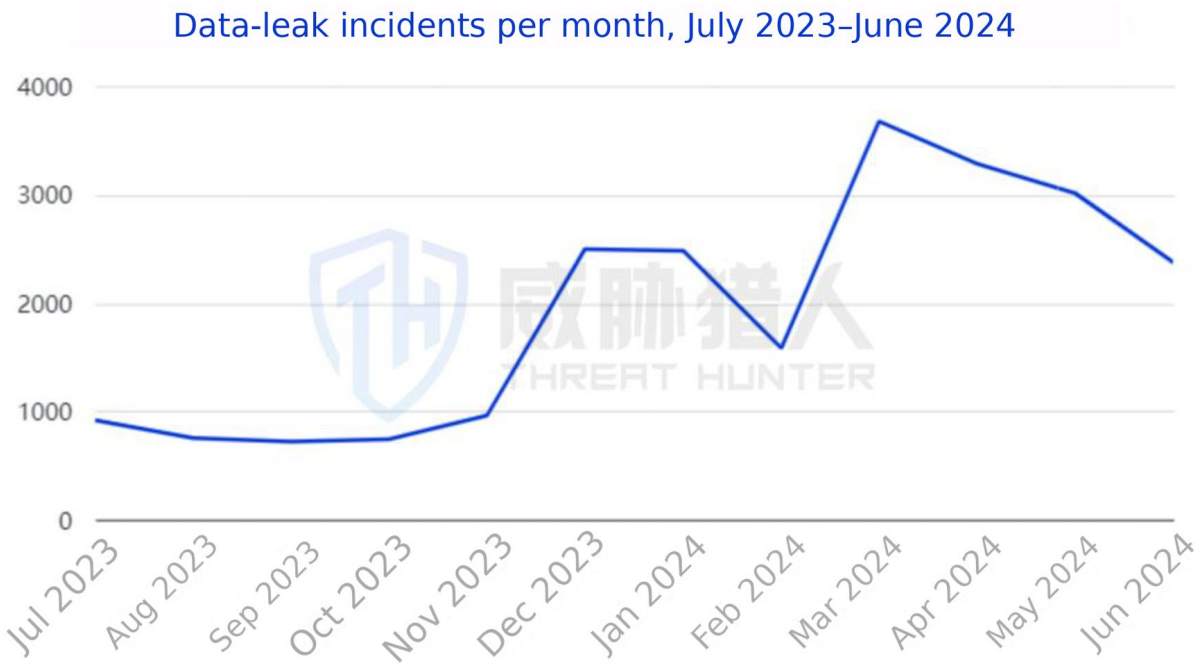
10. Fake data incident: An incident in which threat actors use forged fake data for transactions.

Data breach risk overview in the first half of 2024

1. Overview of data breach risks in the first half of 2024

1.1 In the first half of 2024, there were a total of 16,011 data breaches, which was higher than that in the second half of 2023.

Annual growth of 59.58% According to data from the Threat Hunter data leakage risk monitoring platform, among the 110 million pieces of intelligence monitored across the entire network in the first half of 2024 (January to June), there were a total of 16,011 valid data leakage incidents based on the authenticity verification engine and DRRC manual analysis, an increase of 59.58% from the second half of 2023, to 9,539 cases.

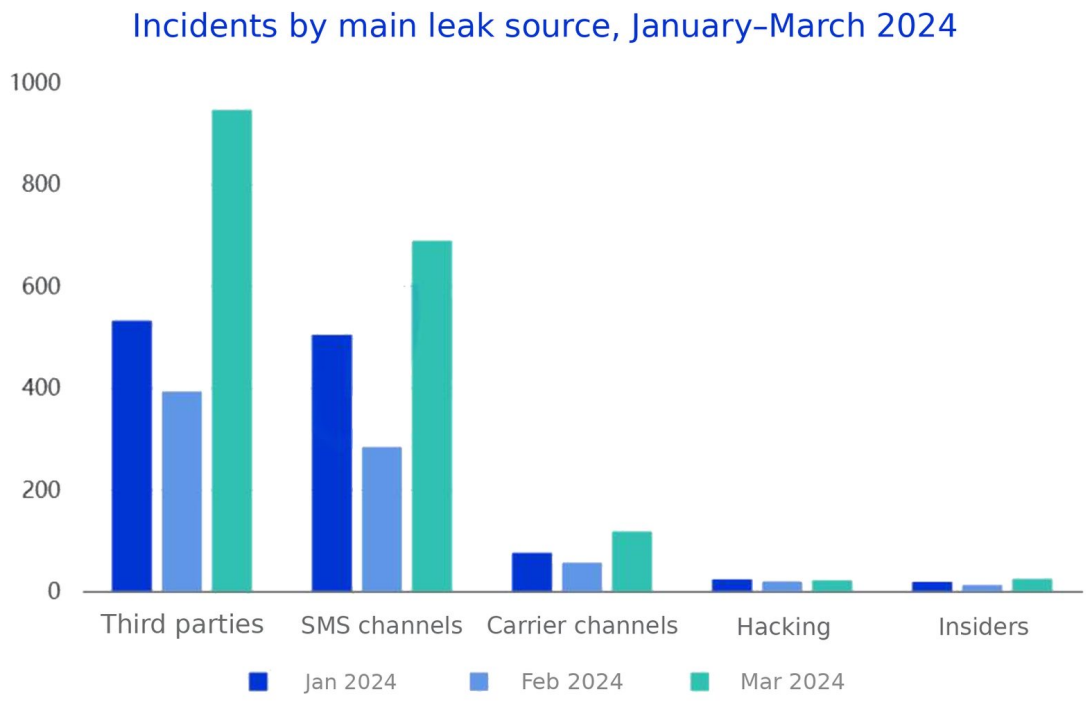


Data-leak incidents per month, July 2023–June 2024: a sharp fall in February 2024, then a rise

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

Threat Hunter found that the number of data breaches dropped significantly in February 2024, down 36% from January 2024 (898 cases). Further analysis revealed that it was mainly due to the following two aspects:

(1) From the perspective of the source of data leakage, the number of data leakage incidents caused by different reasons such as third-party leakage and SMS channel leakage all declined in February 2024. It can be seen that it was mainly affected by the slowdown in trading behavior caused by the holiday of threat actors during the Spring Festival.



Incidents by main leak source, January–March 2024: all five sources dip in February

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

The top causes of data breaches in the first half of 2024 include:

Leakage of SMS channels: With the development of the SMS sending and receiving business over the years, SMS channel providers have begun to obtain higher orders by lowering prices. For example, they will reach transactions with the SMS sender (Party A) at a price lower than the market standard, and their profit margins will be much reduced. Therefore, they will obtain more profits internally by illegally selling SMS information data.

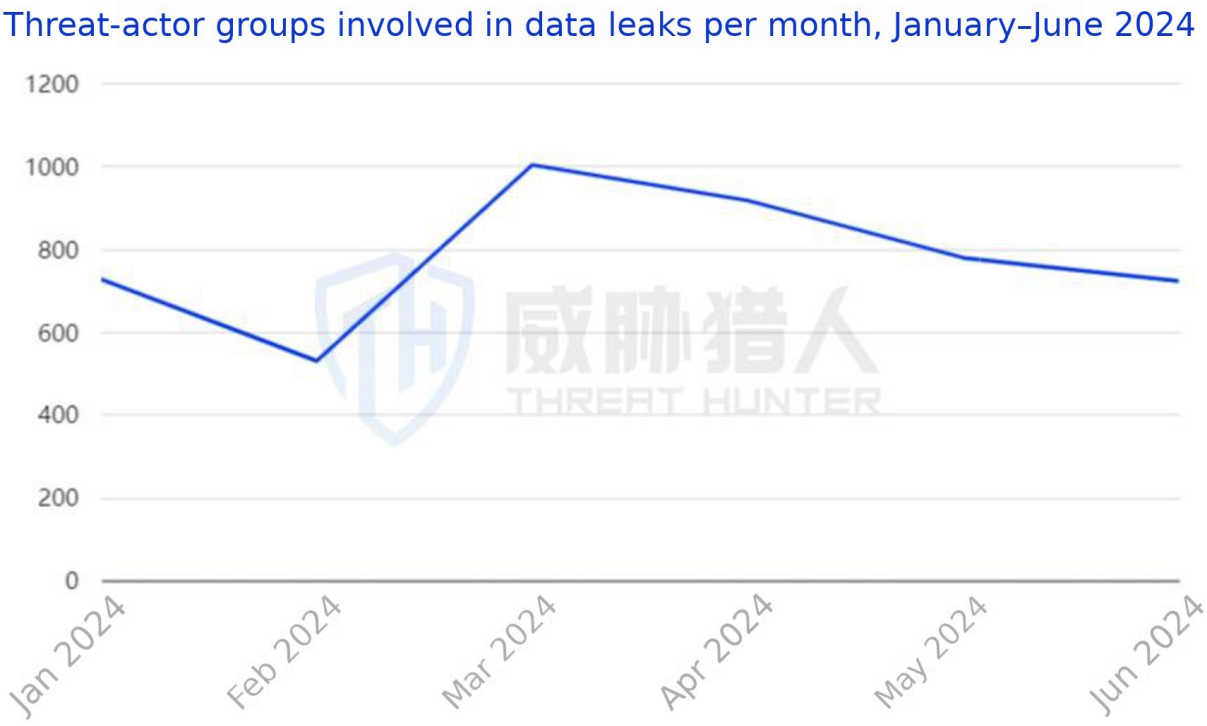
Operator channel: threat actors obtain information such as access data of specified web pages, installation data of specified applications, receiving and sending data of specified text messages, etc. through channels such as operator insiders or illegal agents;

Insider leaks: Internal employees of the company, driven by interests, use methods such as data export and manual photography to obtain sensitive customer information and then sell it;

Hacker attack: External hackers use crawlers, scanning, penetration and other methods to attack corporate systems and network assets, and exploit corporate network vulnerabilities to steal data on a large scale;

Third-party leakage: A third party that has a cooperative relationship with an enterprise has the authority to access certain sensitive data of the enterprise. However, due to irregular management and other issues, these sensitive data are leaked to threat actors through the third party;

(2) Judging from the number of threat actor groups that sell data (intermediaries), the number of illegal data trading threat actor groups dropped in February 2024.

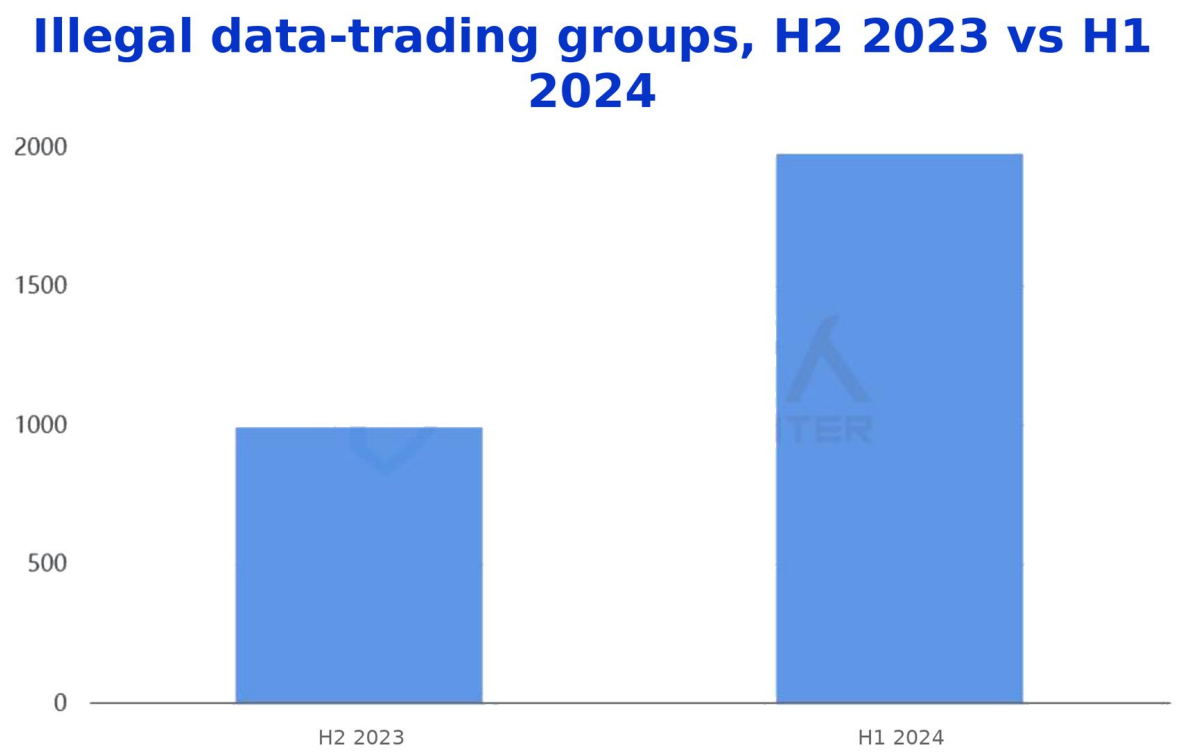


Threat-actor groups involved in data leaks per month, January–June 2024

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

1.2 1,973 illegal data trading threat-actor groups were detected, nearly double the number in the second half of 2023

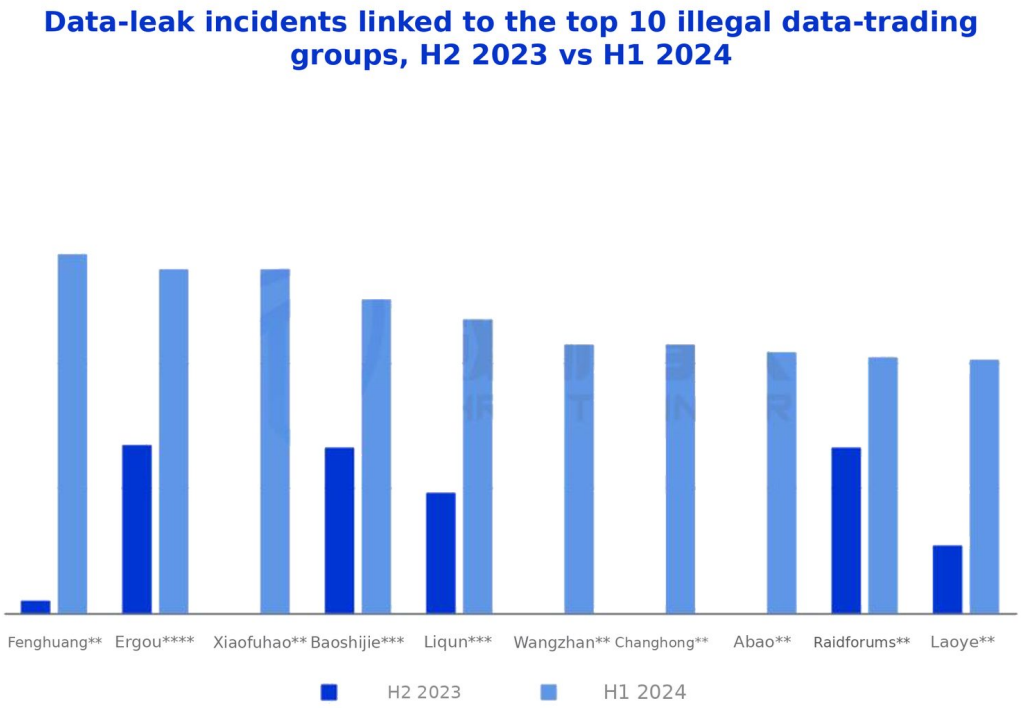
Threat Hunter conducted an in-depth analysis of illegal data trading gangs. From January to June 2024, it monitored 34,000 threat actor gangs. The analysis verified that there were a total of 1,973 threat actor gangs involved in real data leaks, an increase of 984 compared with the second half of 2023, an increase of nearly double.



Illegal data-trading groups, H2 2023 vs H1 2024: nearly double

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

Research on the top 10 illegal data trading threat-actor groups found that the total number of data leakage risk events associated with each group in the first half of 2024 was higher than that in the second half of 2023. It can be seen that the overall activity of illegal data trading groups continues to increase and illegal trading behaviors are more frequent. At the same time, new large-scale threat-actor groups continue to join (such as Xiao Fuhao, Abao, etc.), making the situation of illegal data transactions by threat actors through Telegaram more severe.

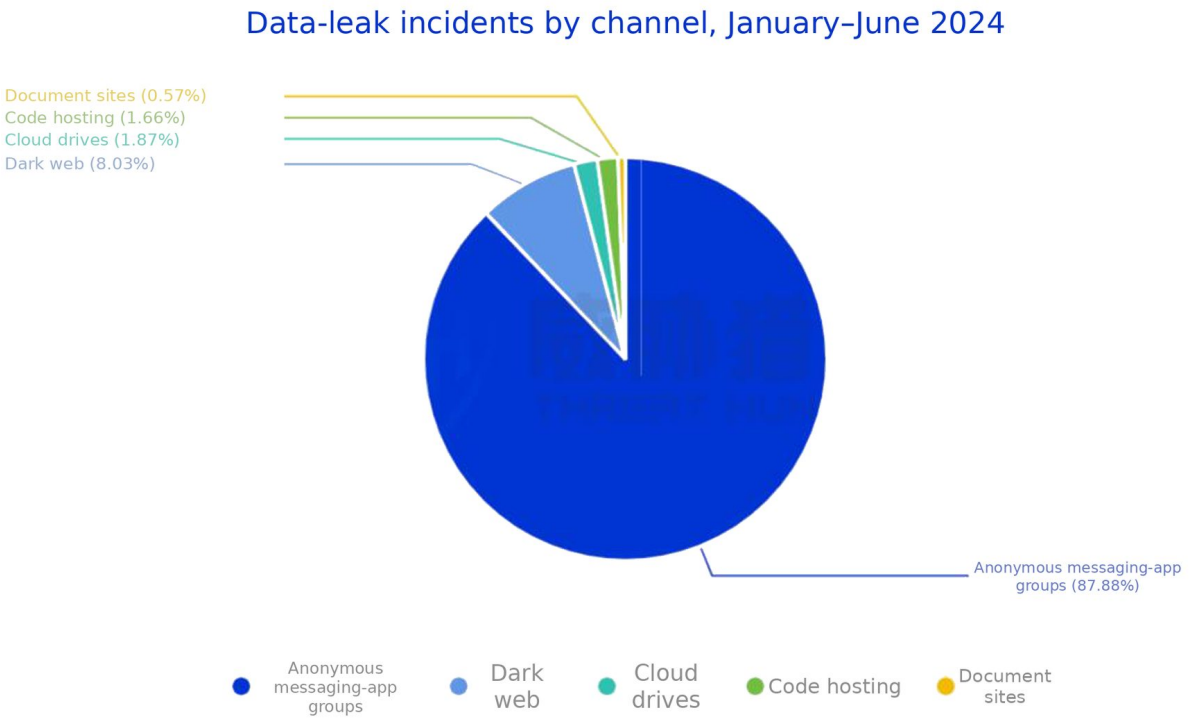


Data-leak incidents linked to the top 10 illegal data-trading groups, H2 2023 vs H1 2024 (names masked as in the original)

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

1.3 Encrypted messaging apps and the dark web are still active, accounting for 95% of data leakage channels

Among the data breaches monitored by Threat Hunter in the first half of 2024, more than 95% occurred on a major encrypted messaging app and the dark web, of which 87% were concentrated on that messaging app.



Data-leak incidents by channel, January–June 2024: anonymous groups on encrypted messaging apps account for 87.88%

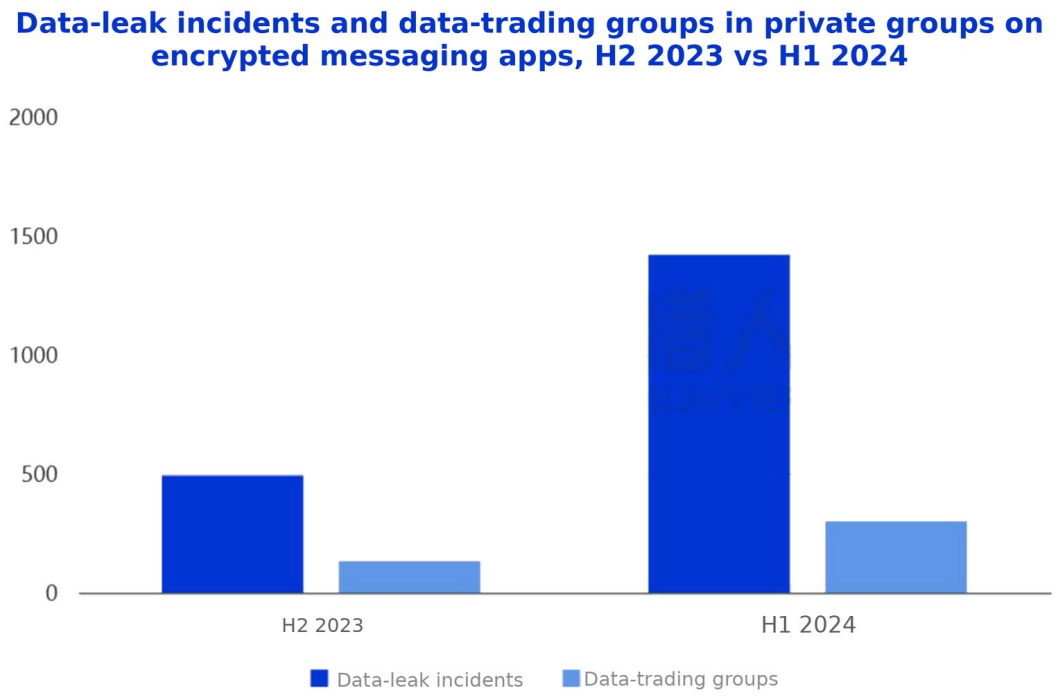
Source: Threat Hunter original report, page 9. Original figure with Chinese text replaced by English.

1.3.1 “Private groups” on the messaging app captured more than 1,400 risk events, an increase of nearly 2 times compared with the second half of 2023

Since 2023, most groups of threat actors have begun to turn to private domain groups for transactions, and data trading groups have also anonymously hidden their account information. The channel/group chat with the most risk events detected on the messaging app is the private domain group. In the first half of 2024, Threat Hunter discovered more than 1,400 risk events in private domain groups, an increase of nearly 2 times compared with the second half of 2023.

Private group: A group that can only be entered through an invitation link/administrator's consent. Generally, outsiders cannot monitor or enter the group chat. The group has administrators who regularly clean the group member list, filtering out people with low credibility such as advertisements, robots, second-hand dealers, and intermediaries to a certain extent. The quality of the group content is closer to the source of real data leaks.

In the first half of 2024, the number of "private groups" on the messaging app has grown rapidly. threat actors gangs communicate with buyers through encrypted messages, passwords, and private chats in the "private groups", making illegal transactions by threat actors more difficult to detect by regulatory agencies.



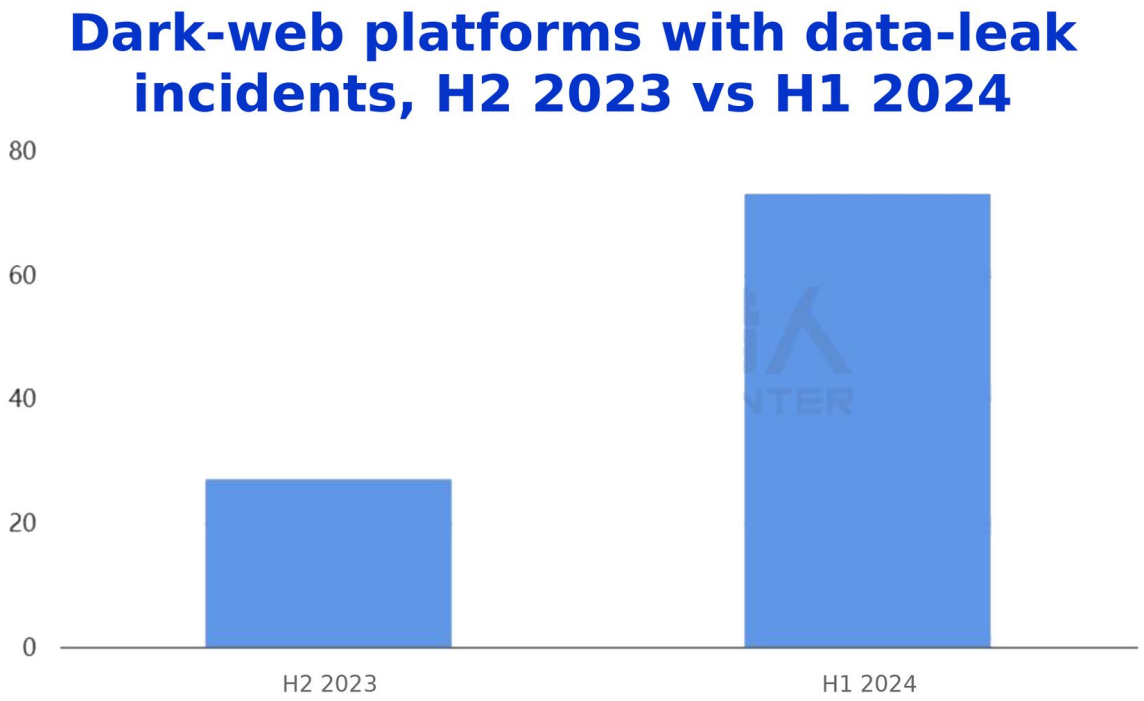
Data-leak incidents and data-trading groups in private groups on encrypted messaging apps, H2 2023 vs H1 2024

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

1.3.2 The number of darknet platforms in the first half of 2024 increased by 46 compared with the second half of 2023

As one of the mainstream channels for illegal data transactions by threat actors, the rapid growth of the number of darknet platforms also reflects the continuous increase in the activity of the darknet, providing more new covert channels for illegal data transactions by threat actors.

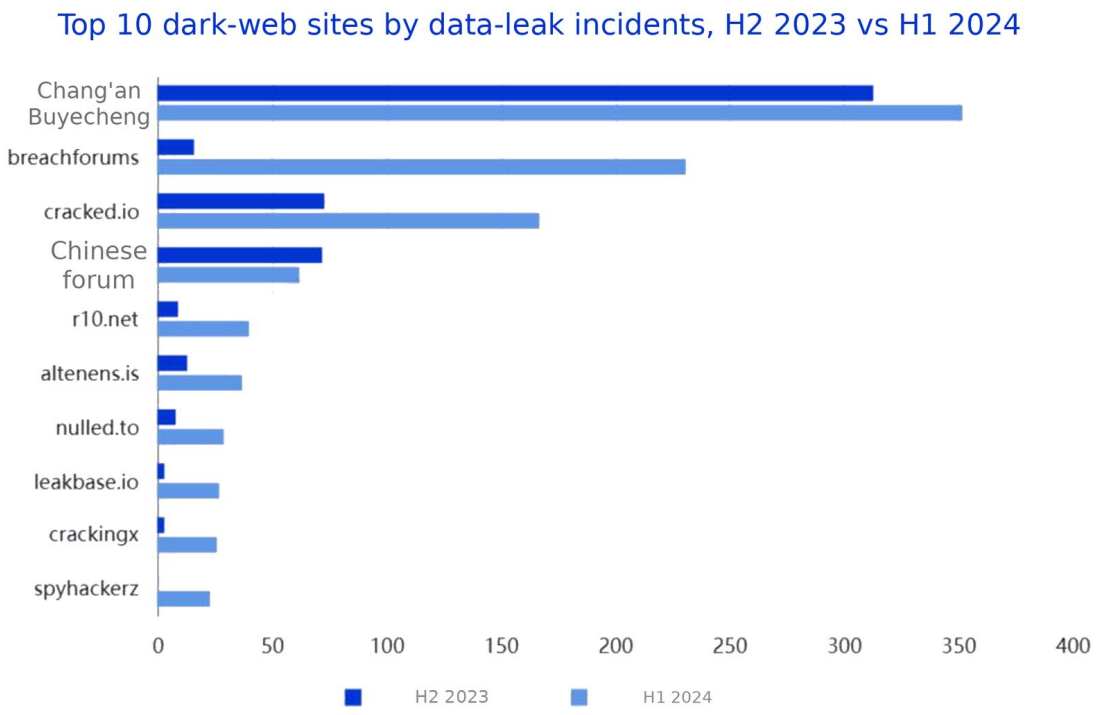
In the first half of 2024, Threat Hunter discovered a total of 1,229 data breaches in dark web channels, involving a total of 73 websites (such as spyhackerz, crackingx, etc.), an increase of 46 websites compared with the second half of 2023.



Dark-web platforms with data-leak incidents, H2 2023 vs H1 2024

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

Based on the Top 10 darknet websites with the highest number of data leakage incidents, Threat Hunter discovered a total of 994 data leakage incidents, accounting for more than 80% of the total number of darknet data leakage incidents captured, mainly concentrated in Chang'an Evernight City, breachforums and cracked.

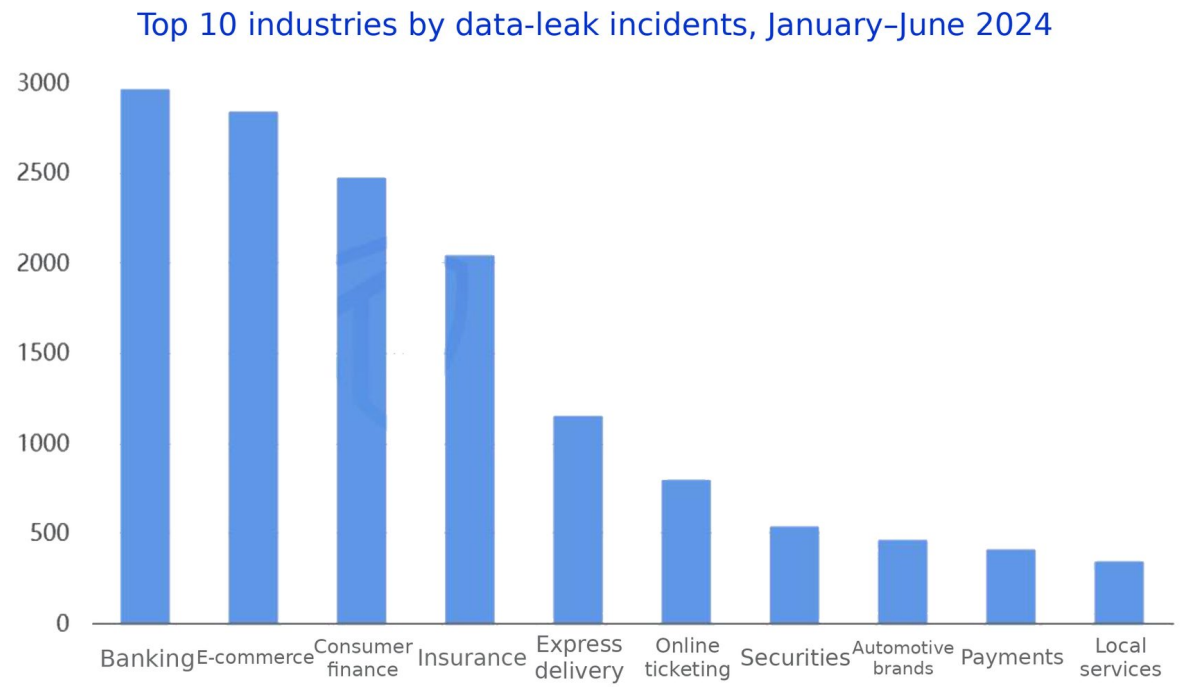


Top 10 dark-web sites by data-leak incidents, H2 2023 vs H1 2024

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

1.4 Banking, e-commerce, and consumer finance have become the top three industries with the number of data breach incidents, and banking incidents ranked first with 2,961 incidents.

From the perspective of industry distribution, data breaches in the first half of 2024 involved 85 industries and 1,524 companies. The top five industries with the number of data breaches were banking, e-commerce, consumer finance, insurance, and express delivery. Among them, the number of data breaches in the banking industry was as high as 2,961, making it the industry with the largest number of data breaches.



Top 10 industries by data-leak incidents, January–June 2024: banking leads

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

The changes in the rankings of the top 10 industries in the first half of 2024 are as follows:

Industry	Rank, H2 2023	Rank, H1 2024	Change
Banking	2	1	Up 1
E-commerce	5	2	Up 3
Consumer finance	1	3	Down 2
Insurance	4	4	No change
Express delivery	3	5	Down 2
Online ticketing	7	6	Up 1
Securities	8	7	Up 1
Automotive brands	9	8	Up 1
Payments	6	9	Down 3
Local services	15	10	Up 5

Top 10 industries by data-leak incidents: rank in H2 2023, rank in H1 2024 and change

Source: Threat Hunter original report, page 13. Table re-typeset in English from the original.

The top industries for data leakage are mainly the finance and e-commerce industries. Data leakage incidents in the financial industry are mainly reflected in the reselling of customer information by banks, consumer finance, insurance and other companies. They are usually used by downstream threat actor groups for targeted marketing and fraud. Because they involve a large

amount of high-value user data and are close to the transaction link, they have become the hardest hit area for personal information leakage.

In recent years, online shopping has developed even more vigorously. According to the "Statistical Report on China's Internet Development" released in March 2024, as of December 2023, the number of online shopping users in China reached 915 million, accounting for 83.8% of the total Internet users.

With the continued and steady growth of online shopping, e-commerce platforms have generated a massive amount of shopping orders and logistics information. Due to their large exposure, these shopping orders and logistics information have become key targets of threat actor groups and are also used for marketing or fraud.

At the same time, among the "Top Ten Most Frequent Types of Telecom Network Fraud" recently announced by the Ministry of Public Security, 10 common types of telecom network fraud, such as fraudulent bill rebates, fake online investment and financial management, fake shopping services, fake reseller logistics customer service, and fake credit reporting, accounted for nearly 88.4% of the cases.

Among them, rebate fraud is the type of fraud with the largest number of cases and the most losses. Fake online investment and financial management fraud cases have the largest losses. The number of cases of fake shopping service fraud has increased significantly and ranks third. Financial and e-commerce user groups are the victims of such fraud cases.

1.5 In the first half of 2024, there were a total of 9 incidents involving tens of millions of data leaks, mainly involving citizens’ three-factor information and online shopping data.

In the first half of 2024, Threat Hunter monitored a total of 9 incidents in which the amount of data leaked reached tens of millions, of which the highest amount of leaked data reached 1.2 billion. After multiple in-depth analysis and verification by Threat Hunter, it was found that the leaked data in this incident was mainly integrated and spliced by the publisher (based on many previous large-scale domestic data leaks), and was not a recent leak.

The leaked data information mainly includes three elements of citizens’ personal information (name, phone number, ID card), followed by online shopping and e-commerce data, and finally financial data (bank and loan information). Judging from the leakage channels, it is mainly concentrated in well-known dark networks such as breachforums, Chang'an Evernight City, cc2crd, and anonymous group chats.

Analysis of data leakage fields and crowd portraits in the first half of 2024

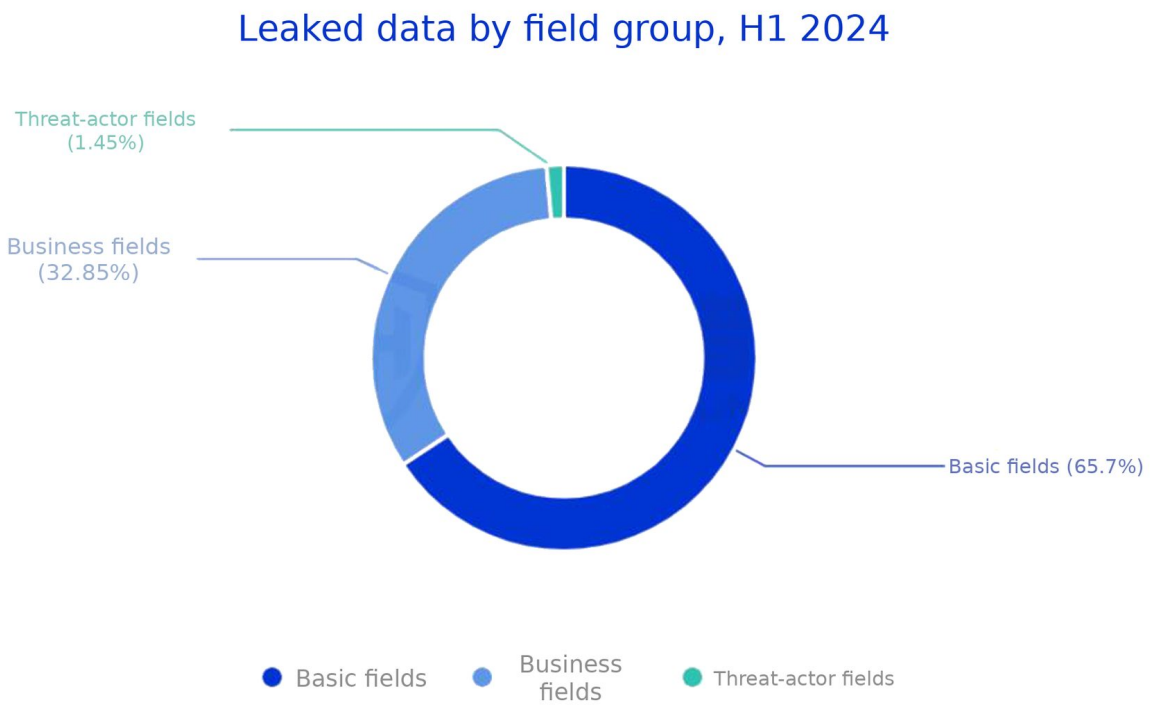
2. Analysis of data leakage fields and crowd portraits in the first half of 2024

2.1 Analysis of data leakage fields in the first half of 2024: basic fields account for 65.7%

Threat Hunter's survey and statistics on leaked fields found that data leakage fields mainly include basic fields, business fields, threat actors definition fields and other types. Basic fields account for the highest proportion, reaching 65.7%, and name, phone number, and ID number account for the highest proportion among basic fields.

The value of leaked data is closely related to the specific fields it contains. Downstream threat actors can construct complete citizen portraits through "full format" data fields and conduct targeted malicious activity, making the overall success rate and revenue of malicious activity higher.

"Full-format" data is a professional and general vocabulary used by threat actors to describe the field format contained in the data. It usually refers to basic field information such as ID card, name, and phone number, plus business field information related to different industries. Taking the insurance industry as an example, full-format information in the insurance industry usually includes ID card, name, phone number, insurance amount, insurance type, etc.



Leaked data by field group, H1 2024: basic fields account for 65.7%

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

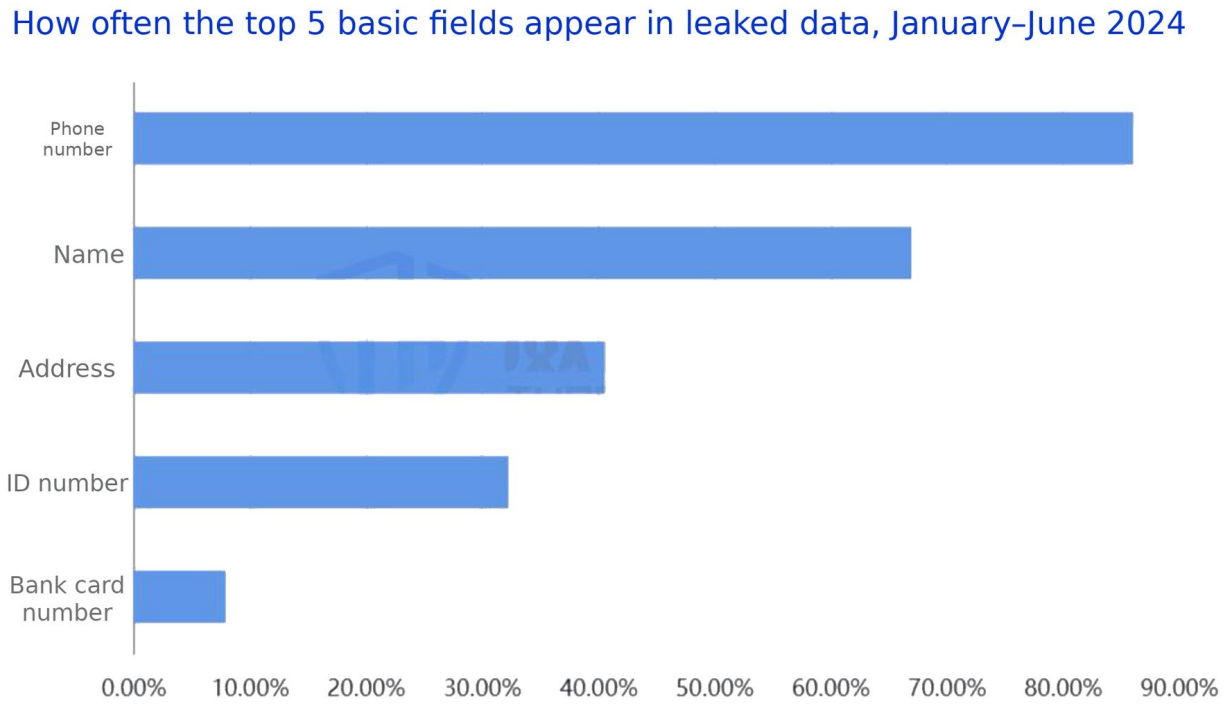
Basic fields: mainly refers to basic personal information, including name, phone number, ID number, bank card number, geographical location, detailed address, etc.;

Business field: mainly refers to business-related information, including platform name, insurance type, brand, courier number, airline, flight number, etc.;

Fields defined by threat actors: mainly refer to the fields defined after data cleaning by cybercriminal groups, such as: verification ID, device information (iOS/Android), affiliated operator, etc. (Verification ID is mainly used by threat actors to mark data to prevent secondary trafficking);

2.1.1 The frequency of "phone number" in the leaked basic fields is as high as 86%

Threat Hunter's investigation and statistics on leaked fields found that data leakage fields mainly include basic fields, business fields, threat actors definition fields and other types. Basic fields account for the highest proportion, reaching 65.7%. As one of the important basic data fields, phone numbers are an indispensable data resource for threat actors to conduct malicious activity. They are frequently used by downstream marketing/fraud gangs to send text messages, telemarketing, etc. to related phone numbers to further carry out illegal malicious activity acts. From January to June 2024, there were more than 15,000 citizen information leaks, and more than 86% of the leaked information fields contained "phone number".



How often the top 5 basic fields appear in leaked data, January–June 2024: phone number leads

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

Threat Hunter security operations staff investigated and learned that some upstream threat-actor groups can only obtain the "phone number" field due to limited technical means. The threat-actor groups will use a variety of methods to splice personal information and complete data field information, thereby increasing the value of the data.

2.1.2 "Bank" accounts for the highest proportion among the leaked business fields, among which the "bank card number" field accounts for up to 57%

After statistical analysis, the "banking" industry accounts for the highest proportion of the leaked business fields. Further analysis found that the most frequently appearing business field information in the leaked data in the banking industry is "bank card number", which accounts for up to 10% of all business fields in the banking industry.

57.08%.

The frequency of occurrence of bank data top 3 business fields are as follows:

Field	Share of appearances
Bank card number	57.08%
Transaction amount	25.99%
Transaction time	21.11%

Top 3 business fields in leaked banking data

Source: Threat Hunter original report, page 18. Table re-typeset in English from the original.

2.1.3 In the custom fields of threat actors, the "low-frequency harassment" and "verification ID" fields appeared for the first time in January 2024.

Threat Hunter analyzed the leaked data and found that in January 2024, fields such as "low-frequency harassment" and "verification ID" appeared for the first time in fields customized by threat actors. Research and analysis of related fields found that:

1 threat actors improve the success rate of fraud through "low-frequency filtering and cleaning" of data, and a total of 52 related incidents have been discovered. Threat Hunter found that starting from January 2024, "low-frequency harassment" field content began to appear in leaked data fields at a high frequency. In the first half of 2024, a total of 52 risk events of this type were discovered.



13	贾	3307	52 女	1970	金华	DP2024280	2024/2/25 15:4	低频骚扰
15	邱	3326	20 女	1979	浙江	DP2024221	2024/1/22 18:0	低频骚扰
15	刘	3325	92 男	1960	丽水	DP2024260	2024/1/21 1:15	低频骚扰
13	徐	3210	21 男	1969	江苏	DP2024274	2024/1/10 20:5	低频骚扰
13	蒋	3210	52 男	1968	江苏	DP2024282	2024/2/20 7:22	低频骚扰
13	王	3301	1 女	1971	河南	DP2024218	2024/2/20 16:4	低频骚扰
18	楼	3301	22 女	1968	杭州	DP2024253	2024/1/7 17:49	低频骚扰
13	刘	3201	3 男	1973	江苏	DP2024247	2024/2/22 12:1	低频骚扰
13	庞	3210	32 男	1953	江苏	DP2024285	2024/1/17 10:5	低频骚扰
15	周	3206	52 男	1977	江苏	DP2024231	2024/1/4 8:57	低频骚扰
13	侯	3208	71 男	1968	连云港	DP2024215	2024/1/22 19:4	低频骚扰
13	陈	3307	91 女	1983	绍兴	DP2024299	2024/2/9 1:11	低频骚扰
13	赵	3306	00 女	1975	浙江	DP2024280	2024/2/15 19:0	低频骚扰
18	郭	3208	70 男	1976	天津	DP2024209	2024/1/4 16:18	低频骚扰
15	周	3307	51 女	1989	浙江	DP2024250	2024/2/28 9:27	低频骚扰

Sample of "low-frequency harassment" data: phone numbers that receive few nuisance calls

Source: Threat Hunter original report, page 19. Original image retained; numbered translations added by Threat Hunter.

Figure guide

1	Columns, left to right: phone number (partly blurred), surname, ID-number prefix (rest blurred), gender, birth year, city or province, batch code with date and time, and the tag "low-frequency harassment"
2	Every row carries the tag "low-frequency harassment"; places include Xuzhou, Jinhua, Zhejiang, Lishui, Jiangsu, Henan, Hangzhou, Lianyungang, Shaoxing and Tianjin

(low frequency data sample form)

Threat Hunter further communicated with threat actors who released relevant data and learned that threat actors define this type of data as low-frequency harassment data. "Low-frequency filtering and cleaning" mainly means that when data sellers screen data, they will analyze the frequency of harassment of ordinary user phone numbers, thereby filtering out user phone numbers with low harassment rates, that is, user phone numbers that usually receive fewer harassing calls and are less resistant to answering strange calls.

For this type of phone number, criminal gangs can achieve a higher user answer rate when conducting marketing promotions or fraud, and can better gain the trust of users for precise promotion, greatly improving the success rate of fraud.



A data seller explains "low-frequency harassment" data to a buyer

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

Figure guide

1	File: "Low-frequency harassment, female data.xlsx" (10.7 KB)
2	Buyer: "What does low-frequency mean?" Seller: "High connection rate, low harassment rate." Buyer: "So the numbers connect well, but the final success rate is low?" Seller: "These numbers are harassed less often, so people are more likely to pick up."
3	Buyer: "How do you know these numbers are harassed less often? This is new to us and we plan to buy some, but we need to understand your method." Seller: "It also goes through software that checks how often a phone is harassed." Seller: "Price per record: 1.6."
4	Buyer: "Roughly how does the software check?" Seller: "The software screens the harassment rate, brother."

2 threat actors used the "verification ID" identification verification to locate data sources with higher credibility, and a total of 37 related incidents were discovered. In January 2024, Threat Hunter found that the "verification ID" field appeared frequently in the leaked data fields. In the first half of 2024, a total of 37 risk events of this type were discovered.



Sample of leaked insurance data with a "verification ID" field

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

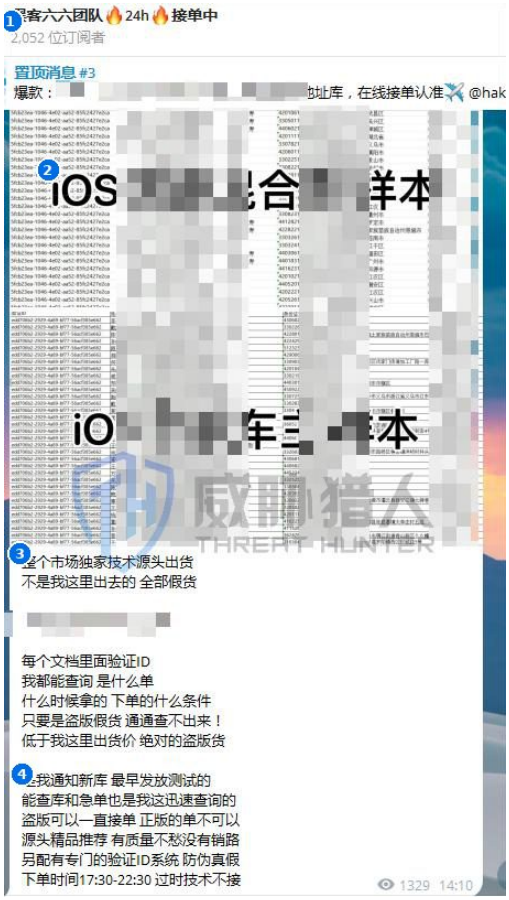
Figure guide

1	Column headers, left to right: verification ID, (blurred column), name, phone number, insurance type, company, ID number, address, carrier
2	Insurance types: annuity, life, health and accident insurance; every row carries the same verification ID

(Verify ID field class data)

In-depth investigation revealed that the "verification ID" is actually an identification made by illegal data trading threat actors gangs in order to verify the authenticity of the data and prevent the data from being re-sold by intermediaries. Downstream data purchasing gangs can verify the authenticity of the data through the data verification system provided by them.

Secondary sales and multiple sales of data are common in illegal data trading markets. Threat Hunter research found that on average, the same data sample is sold by at least 2 threat-actor groups, and the same data sample is sold by up to 433 threat-actor groups. There is a mixture of old and new real and fake data in the threat actors trading market. The ID verification method can to a certain extent help the downstream threat-actor groups that purchase data to effectively find data with higher credibility.



A data seller says its verification-ID system proves which data is genuine

Source: Threat Hunter original report, page 21. Original image retained; numbered translations added by Threat Hunter.

Figure guide

1	Channel: "Hacker Liuliu Team, 24h, taking orders" (2,052 subscribers). Pinned message: "Best seller: ... address database; for online orders, look for @hak..."
2	Sample files overlaid with "iOS ... mixed ... sample" and "iOS ... car ... sample" (partly blurred)
3	"The only technical source on the whole market; anything not shipped by me is fake. I can look up the verification ID in every file: what order it was, when it was taken and on what terms. Pirated copies cannot be traced at all! Anything cheaper than my price is definitely pirated."
4	"I announce new databases and hand out the earliest test data; database checks and urgent orders are also looked up quickly here. Pirated data can be ordered any time; genuine data cannot. Quality source data sells itself. A dedicated verification-ID system tells genuine from fake. Orders 17:30–22:30 only."



A second seller offers verification-ID lookups for insurance data

Source: Threat Hunter original report, page 21. Original image retained; numbered translations added by Threat Hunter.

Figure guide

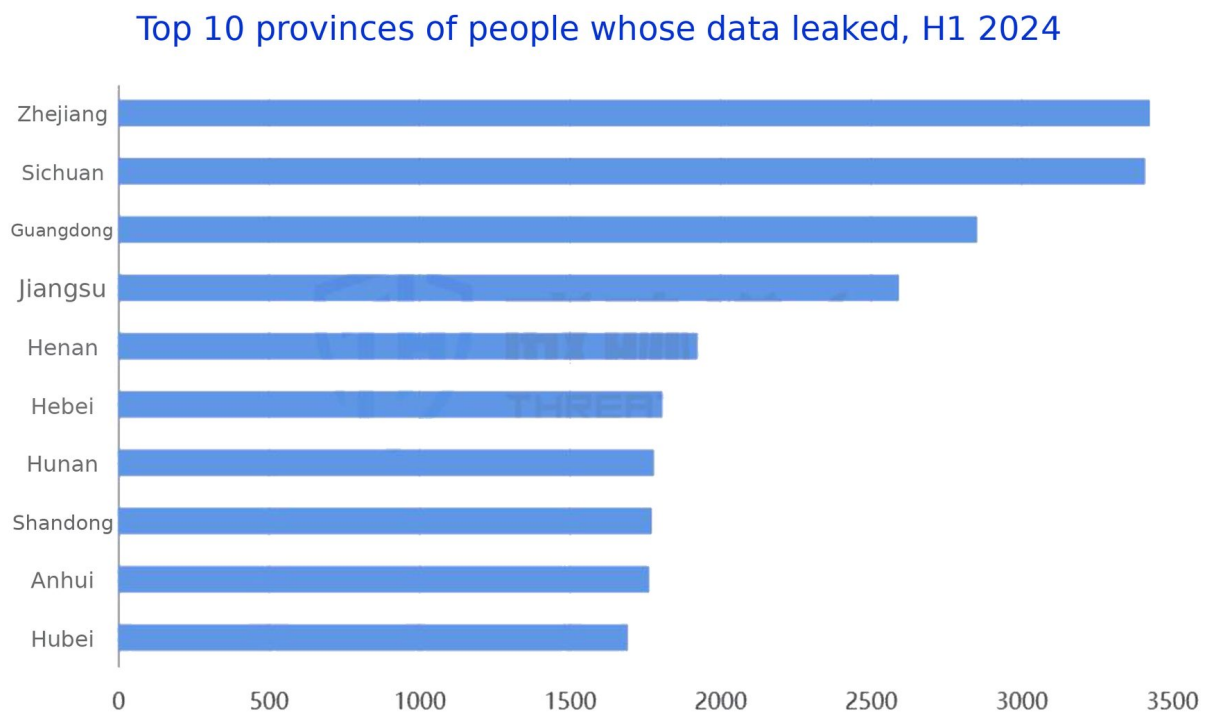
1	Channel: "HK all-industry data" (1,427 subscribers). Pinned: "App web extraction, SDK, DPI, SMS hijacking; contact us if needed: loans, shopping, data"
2	Reply to a verification-ID query (6 May): "No such verification ID; please contact the sales staff"
3	Second reply: "The verification ID refers to: 2024-05-04, standard insurance, Chongqing, 1963–1967, 1,000"
4	"Mixed insurance, life insurance, annuity insurance. The whole market is full of 1:1 copies; only I sell genuine insurance data. Brothers, bring your verification ID and check."

(Verify the explanation of ID field by threat actors)

2.2 Analysis of data leakage crowd portraits in the first half of 2024

2.2.1 Regional distribution of data breaches in 2024 top 3: Zhejiang, Sichuan, Guangdong

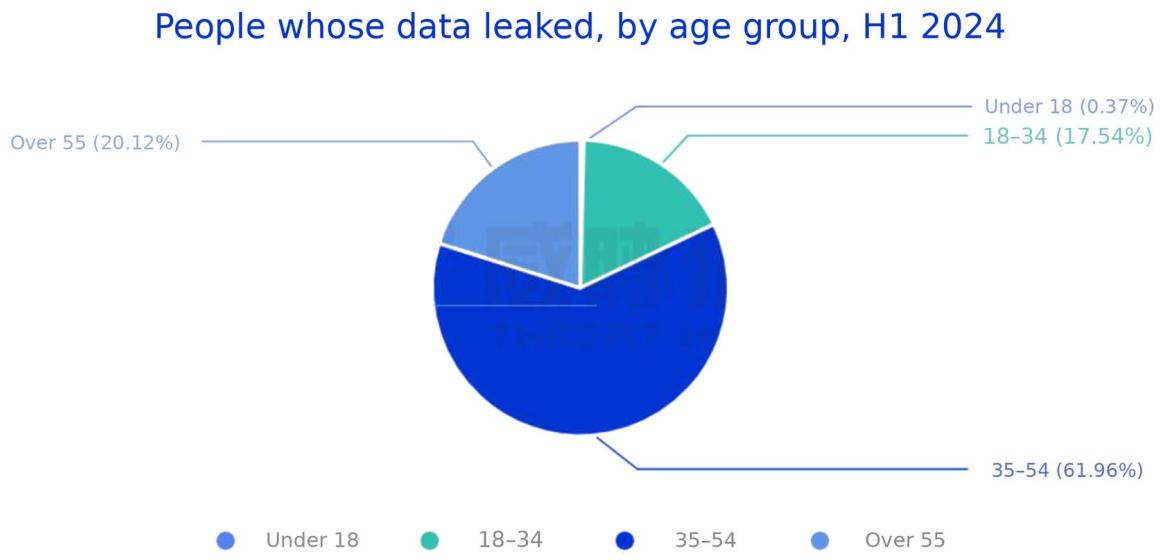
Threat Hunter analyzes information related to data leakage groups across the industry. From a regional perspective, the top 3 regions with the largest number of data leakage groups are: Zhejiang, Sichuan, and Guangdong.



Top 10 provinces of people whose data leaked, H1 2024: Zhejiang, Sichuan and Guangdong lead

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

2.2.2 Age distribution of data breaches in 2024: 35-54 year olds account for 62%



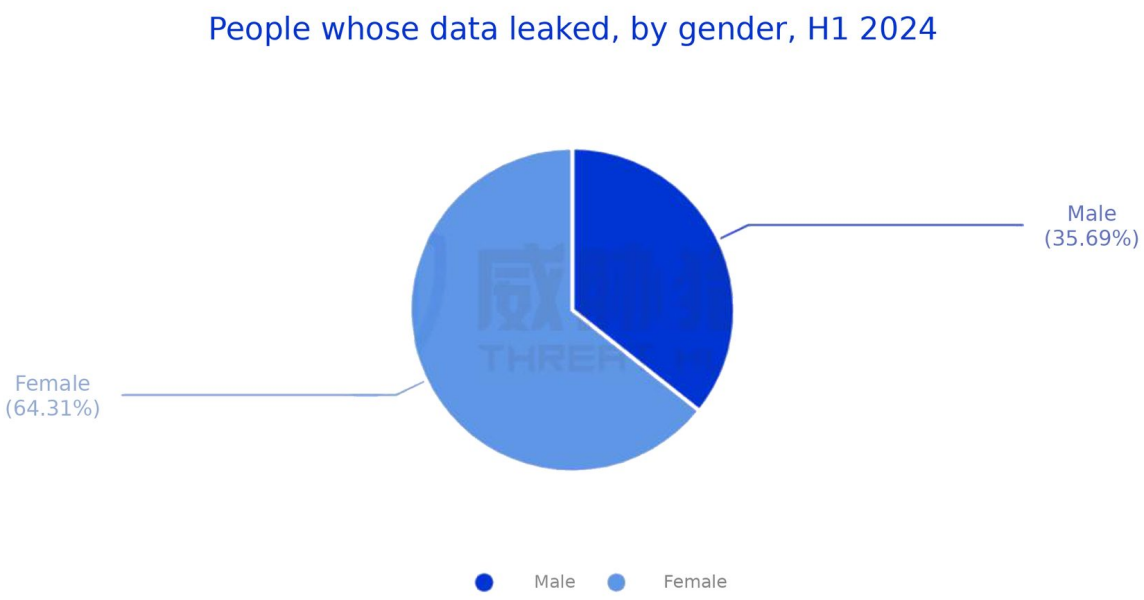
People whose data leaked, by age group, H1 2024: those aged 35–54 make up 61.96%

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

Definition of distribution by age group (for reference):

Minors: Under 18 years old Youth stage: 18-34 years old Middle-aged stage: 35-54 years old Old stage: Over 55 years old (retirement age)

2.2.3 Gender distribution of data breaches in 2024: women account for a larger proportion, reaching 64%

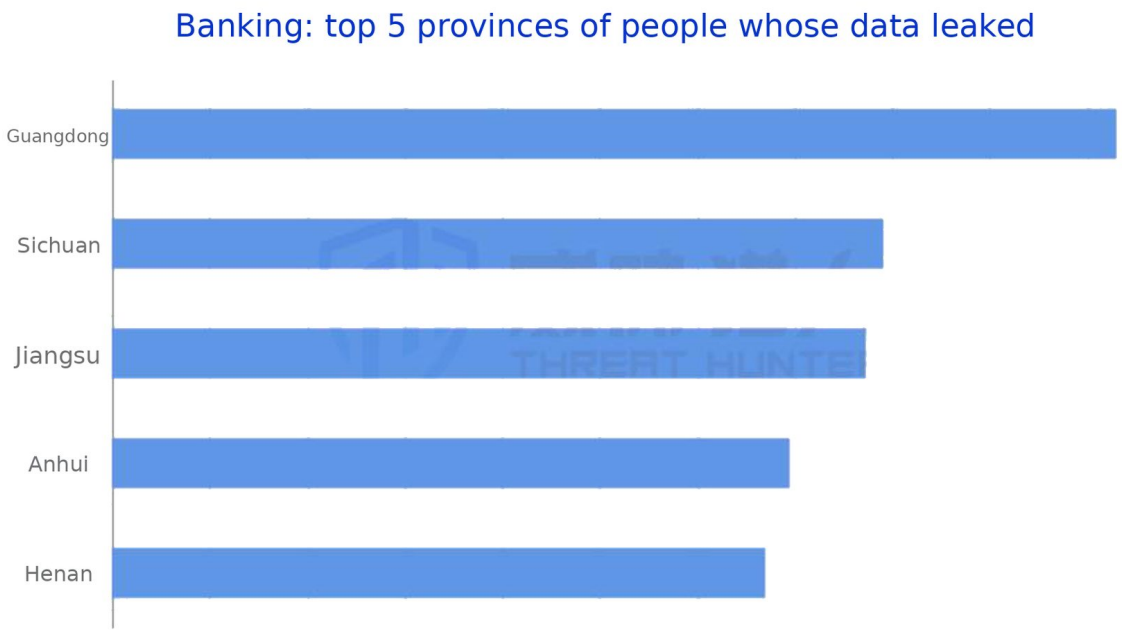


People whose data leaked, by gender, H1 2024: women make up 64.31%

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

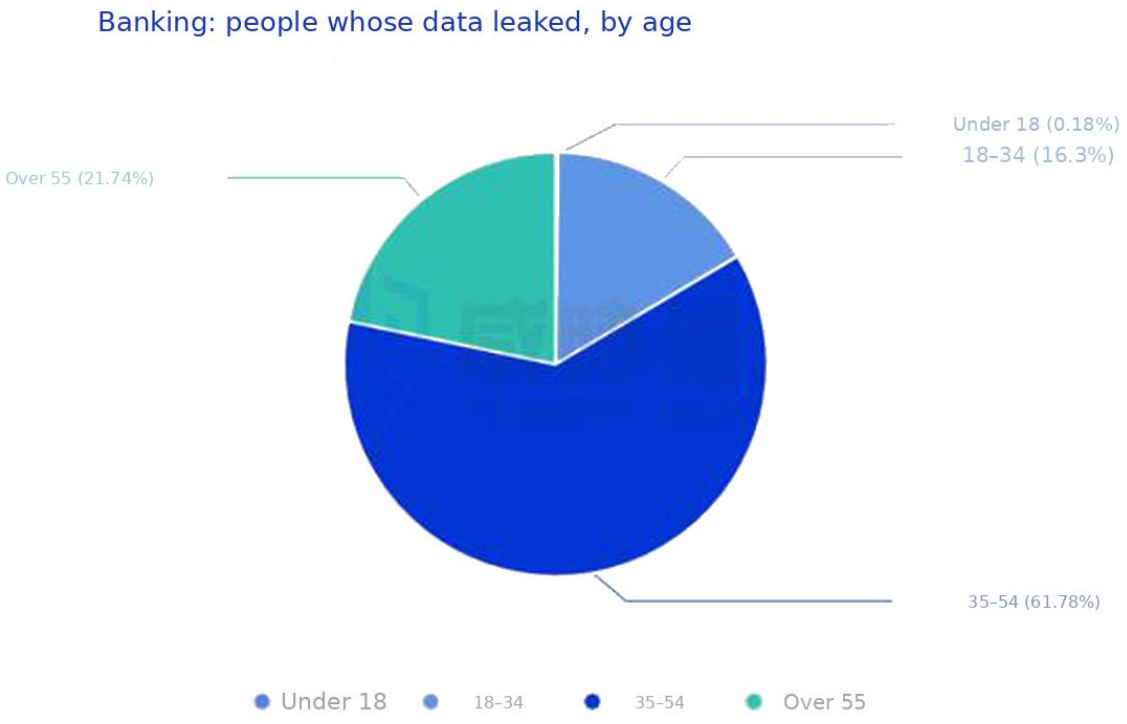
2.2.4 top 3 industry (banking, e-commerce, consumer finance) crowd portrait analysis 1 Portrait of people involved in bank data leakage

Threat Hunter analyzed information related to bank data leakage groups. The regions with the largest number of data leakage groups are: Guangdong, Sichuan, Jiangsu, Anhui, and Henan. The age of the leaked people is mainly 35-54 years old, accounting for 61.78% of the data leaked people, and women account for 66.42%.



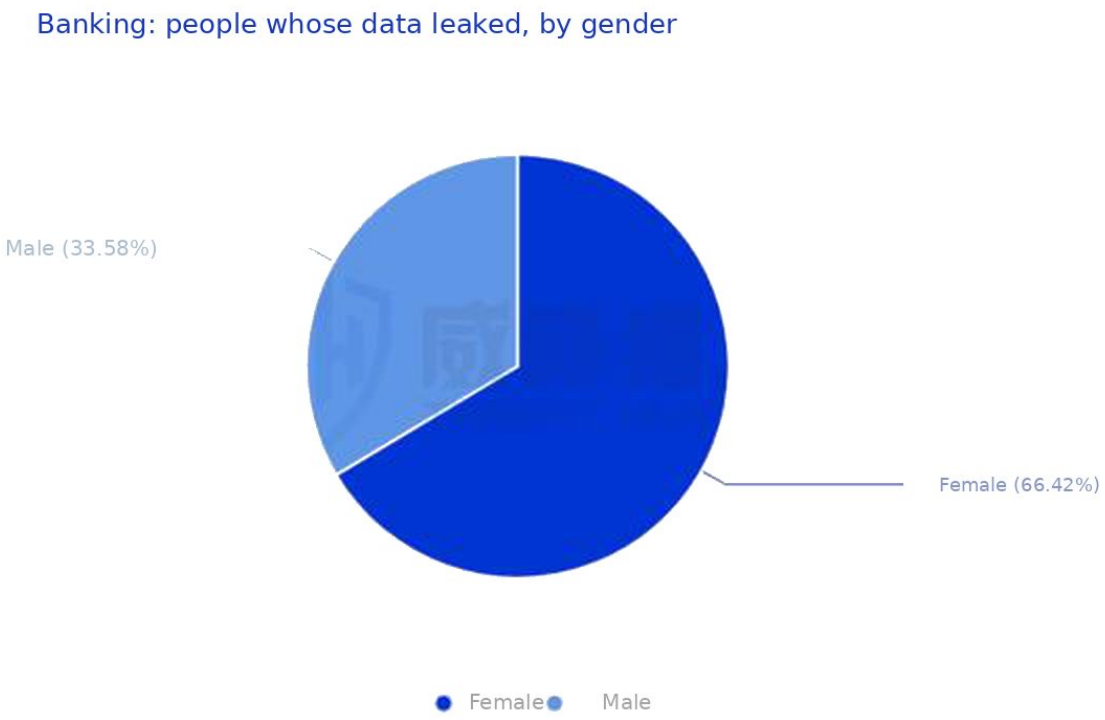
Banking: top 5 provinces of people whose data leaked

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



Banking: people whose data leaked, by age

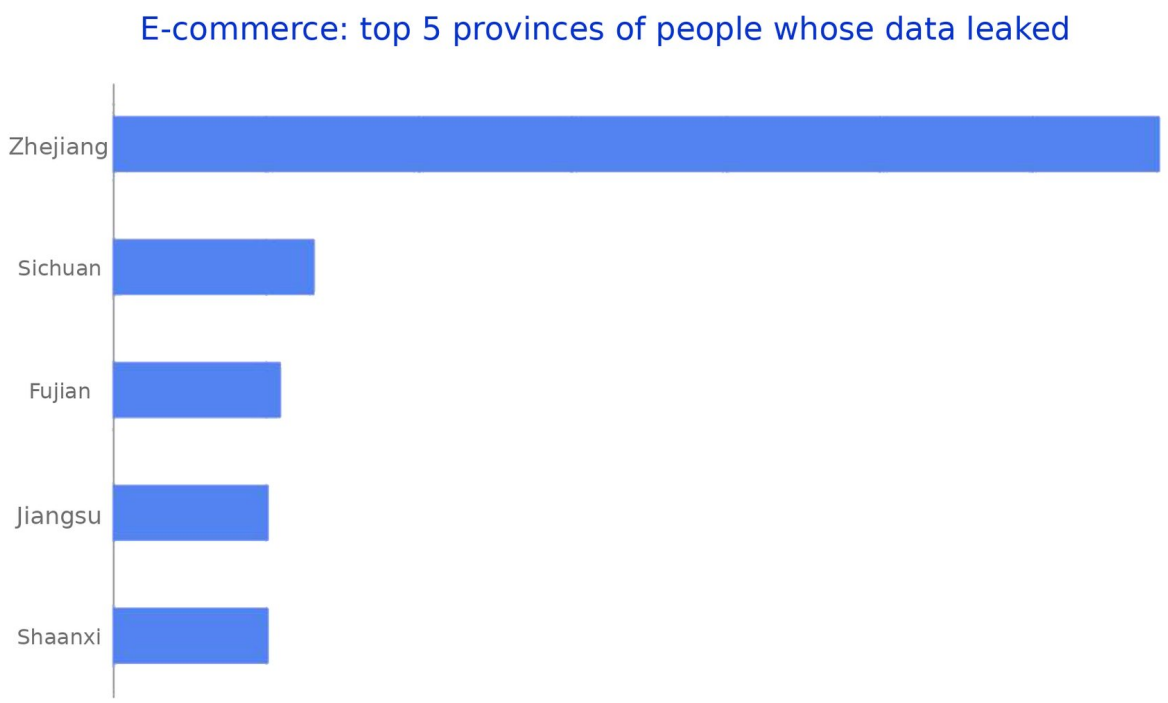
Source: Threat Hunter original report, page 24. Original figure with Chinese text replaced by English.



Banking: people whose data leaked, by gender

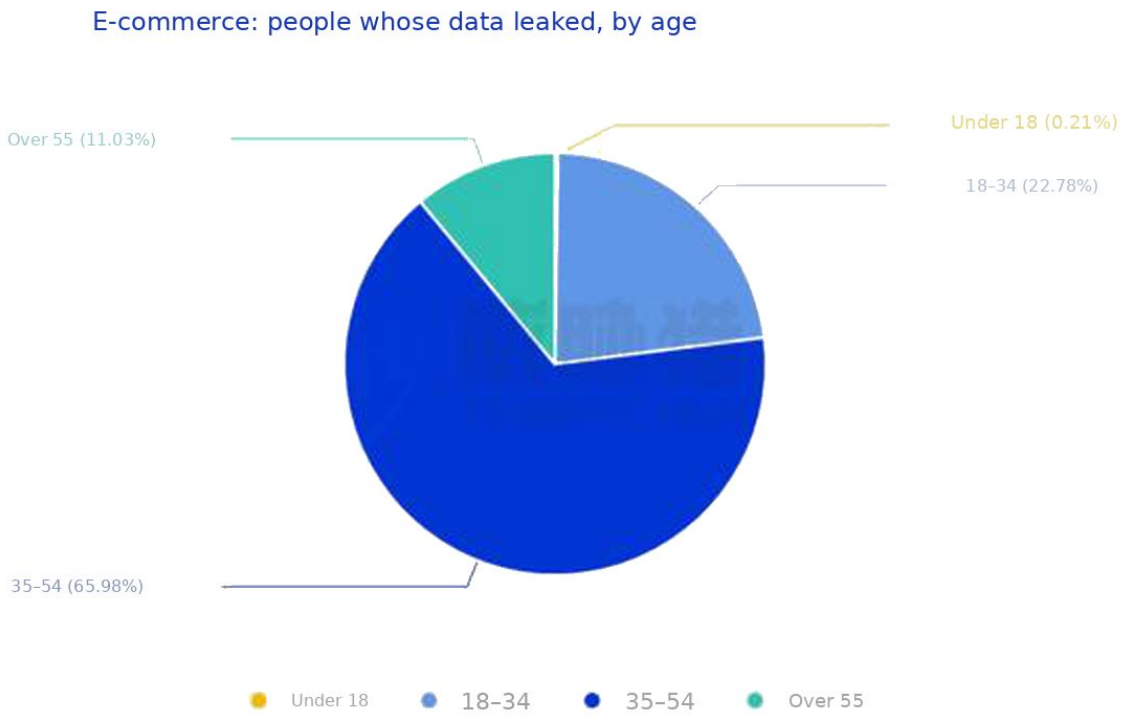
Source: Threat Hunter original report, page 24. Original figure with Chinese text replaced by English.

2. Portraits of e-commerce data leakage personnel. Threat Hunter analyzes information related to e-commerce data leakage groups. The regions with the largest number of data leakage groups are: Zhejiang, Sichuan, Fujian, Jiangsu, and Shaanxi. The age of the leaked people is mainly 35-54 years old, accounting for 65.98% of the e-commerce data leaked people, and women account for 68.25%.



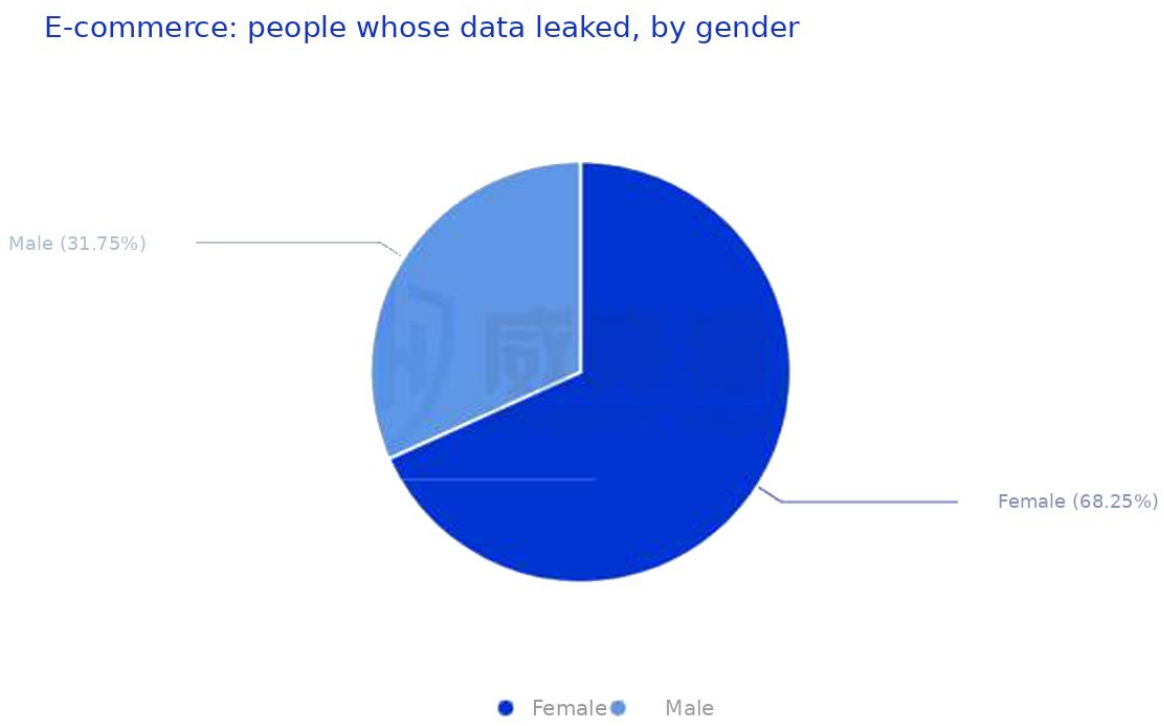
E-commerce: top 5 provinces of people whose data leaked

Source: Threat Hunter original report, page 24. Original figure with Chinese text replaced by English.



E-commerce: people whose data leaked, by age

Source: Threat Hunter original report, page 24. Original figure with Chinese text replaced by English.

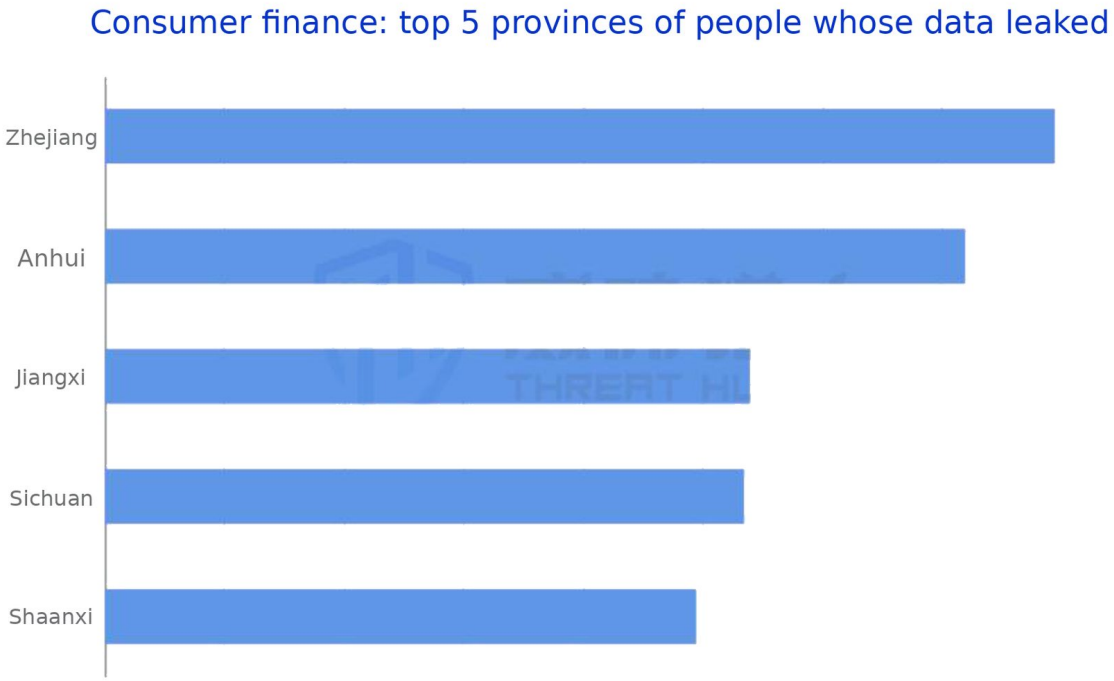


E-commerce: people whose data leaked, by gender

Source: Threat Hunter original report, page 24. Original figure with Chinese text replaced by English.

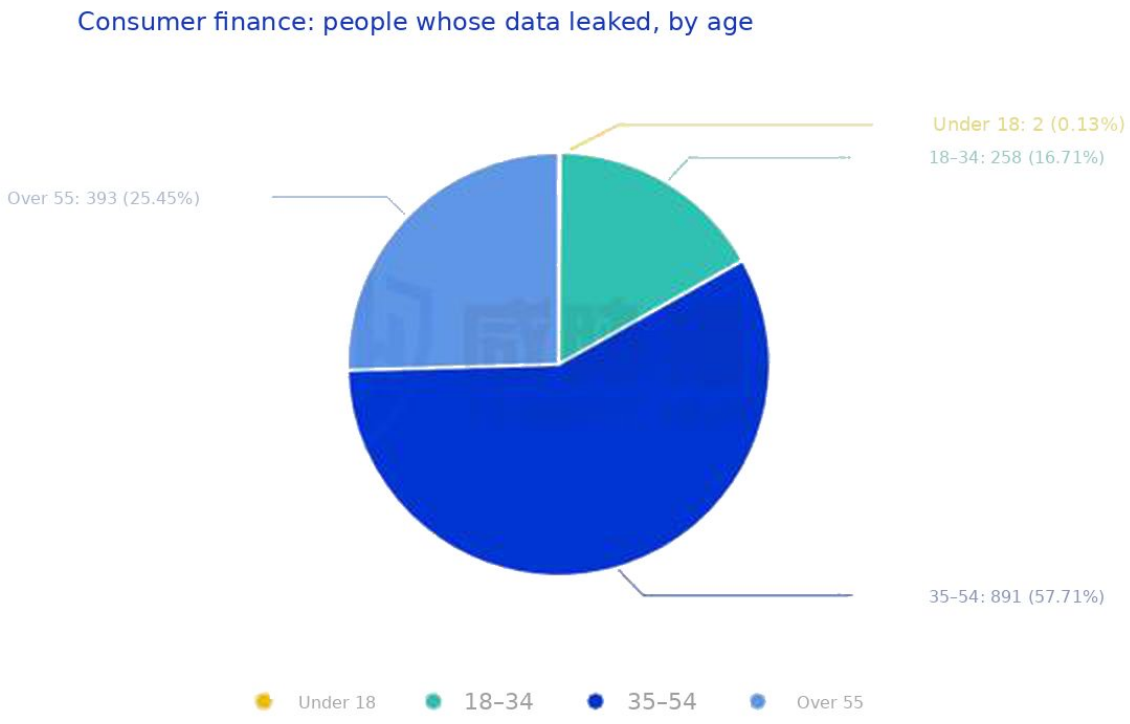
3. Portraits of people with consumer financial data leaks. Threat Hunter analyzes information related to people with consumer financial data leaks. The areas with the largest number of people with data leaks are:

Zhejiang, Anhui, Jiangxi, Sichuan, and Shaanxi. The age of the leaked people is mainly 35-54 years old, accounting for 57.71% of the people whose consumer financial data was leaked, and women accounted for 52.46%.



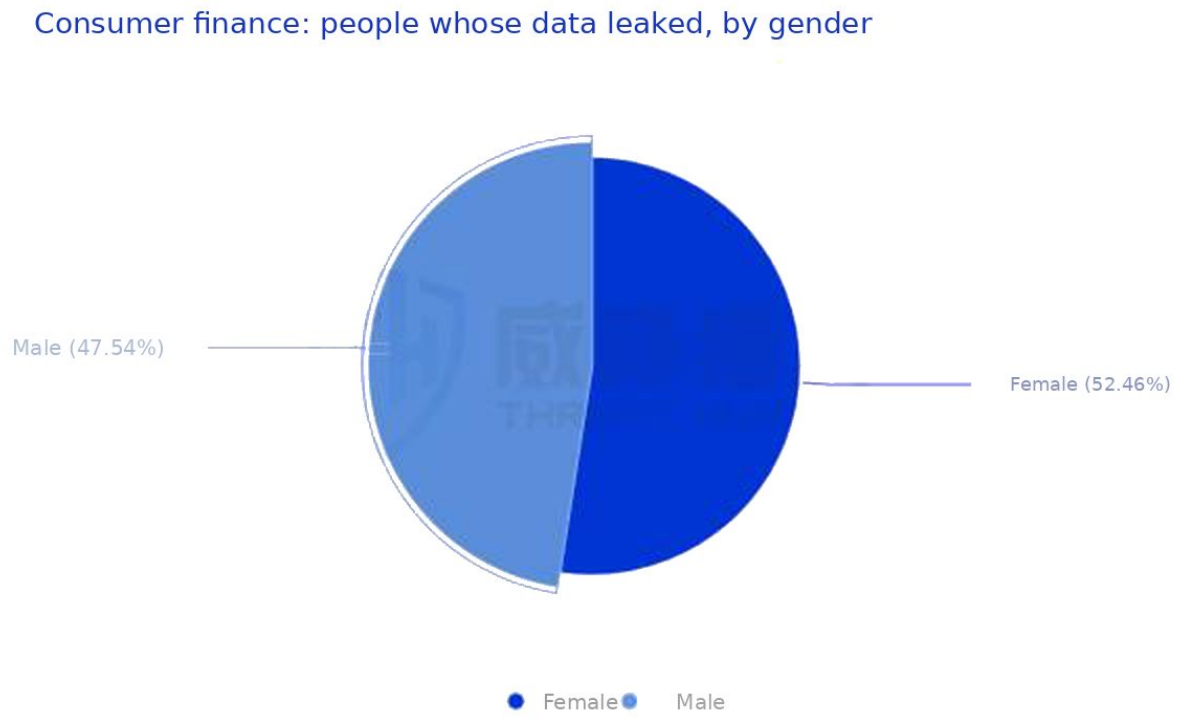
Consumer finance: top 5 provinces of people whose data leaked

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



Consumer finance: people whose data leaked, by age

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



Consumer finance: people whose data leaked, by gender

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

Research on the threat-actor data trading market in the first half of 2024

3. Research on the threat-actor data trading market in the first half of 2024

3.1 In the first half of 2024, there were many fraudulent activities using built-in video calls, the word "iOS"

There were a total of 1,237 risk events related to the segment, an increase of 8 times compared with the second half of 2023. Threat Hunter security researchers found that in the data leaked in the first half of 2024, the frequency of "device information" field information gradually increased, especially the "iOS" data field. Judging from the chat records between the underground data trafficking gang and downstream data buyers, the data buyers mentioned the screening requirements for "iOS" device data many times in their repurchase requirements for data.



0		订单号	姓名	身份证号	手机号	出生日期	年份	性别	保障到期	投保日期	公司分部	设备信息
9	险创建订单	34	34 石	211	195	10/27/81	1981	女	2/2/24 23	2/3/23 0:	辽宁省分公司辽阳中心支公	iOS
9	保险创建订单	90	60 潘	232	360	9/25/71	1971	女	4/25/24 2	4/26/23 0	黑龙江省分公司绥化中心支公	iOS
9	保险创建订单	11	932 胡	230	458	5/3/71	1971	女	7/25/24 2	7/26/23 0	黑龙江省分公司伊春中心支公	iOS
9	保险创建订单	65	266 衣	210	097	8/20/80	1980	女	4/24/24 2	4/25/23 0	辽宁省分公司大连中心支公司	iOS
9	保险创建订单	60	41 王	220	008	7/5/75	1975	女	10/4/24 2	10/5/23 0	吉林省分公司吉林中心支公司	iOS
9	保险创建订单	81	814 邢	210	332	9/24/70	1970	女	4/16/24 2	4/17/23 0	辽宁省分公司抚顺中心支公司	iOS
9	保险创建订单	25	835 朱	239	543	10/25/79	1979	女	2/21/24 2	2/22/23 0	黑龙江省分公司富锦中心支公	iOS
9	保险创建订单	12	805 王	230	578	10/3/67	1967	女	7/14/24 2	7/15/23 0	黑龙江省分公司鸡西中心支公	iOS
9	保险创建订单	84	635 吕	220	707	7/26/75	1975	女	8/25/24 2	8/26/23 0	吉林省分公司长春中心支公司	iOS
9	保险创建订单	77	904 顾	210	135	2/16/73	1973	女	1/6/24 23	1/7/23 0:	辽宁省分公司抚顺中心支公司	iOS
9	保险创建订单	55	674 单	211	210	6/25/69	1969	女	7/5/24 23	7/6/23 0:	辽宁省分公司朝阳中心支公司	iOS
9	保险创建订单	31	817 杨	211	083	5/14/70	1970	女	12/11/24	12/12/23	辽宁省分公司铁岭中心支公司	iOS
9	保险创建订单	92	821 牛	210	235	11/14/73	1973	女	4/14/24 2	4/15/23 0	辽宁省分公司抚顺中心支公司	iOS
9	保险创建订单	97	39 李	232	398	7/19/73	1973	女	6/12/24 2	6/13/23 0	黑龙江省分公司松花江中心	iOS
9	保险创建订单	96	11 曲	220	511	8/16/79	1979	女	3/12/24 2	3/13/23 0	吉林省分公司四平中心支公司	iOS
9	保险创建订单	80	928 姚	230	583	3/11/78	1978	女	7/1/24 23	7/2/23 0:	黑龙江省分公司鸡西中心支公	iOS
9	保险创建订单	49	584 杜	230	334	10/1/69	1969	女	12/26/24	12/27/23	黑龙江省分公司齐齐哈尔中心	iOS
9	保险创建订单	84	44 李	220	111	2/1/76	1976	女	11/4/24 2	11/5/23 0	吉林省分公司长春中心支公司	iOS

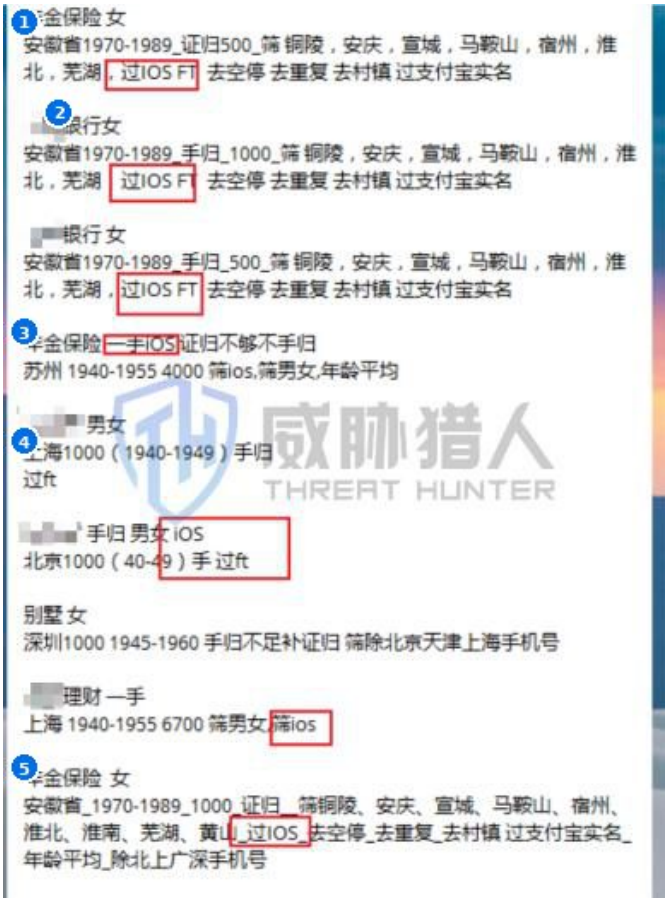
Leaked insurance order data captured by Threat Hunter, with a device-information field

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

Figure guide

1	Column headers: (status), order number, name, ID number, phone number, date of birth, year, gender, coverage expiry, policy date, company branch, device information
2	Every row reads "Insurance order created"; branches are provincial and city branches in Liaoning, Heilongjiang and Jilin
3	Device information column: every row reads "iOS"

(The leaked data captured by Threat Hunter contains device information)



Buyers' data orders that require numbers able to "pass iOS FT"

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

Figure guide

1	"Annuity insurance, female: Anhui, born 1970–1989, ID-located, 500, filtered to Tongling, Anqing, Xuancheng, Ma'anshan, Suzhou, Huaibei and Wuhu; must pass iOS FT (boxed); remove dead numbers and duplicates, remove villages and towns, must pass a payment app's real-name check"
2	Two bank requests, female, on the same terms (Anhui, 1970–1989, phone-located, 1,000 and 500), each requiring "pass iOS FT"
3	"Annuity insurance, first-hand iOS (boxed), ID-located, or phone-located if not enough: Suzhou, 1940–1955, 4,000, filter iOS, male and female, mixed ages"
4	Further requests: Shanghai 1,000 (1940–1949), phone-located, pass FT; Beijing 1,000 (1940–1949), phone-located, iOS, pass FT (boxed); Shenzhen villa owners 1,000 (1945–1960); Shanghai first-hand wealth management, 1940–1955, 6,700, filter iOS (boxed)
5	"Annuity insurance, female: Anhui, 1970–1989, 1,000, ID-located, filtered to listed cities, pass iOS (boxed), remove dead numbers and duplicates, remove villages and towns, pass a payment app's real-name check; mixed ages; exclude numbers from Beijing, Shanghai, Guangzhou and Shenzhen"



A buyer orders leaked life-insurance data that must "pass FT + iOS"

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

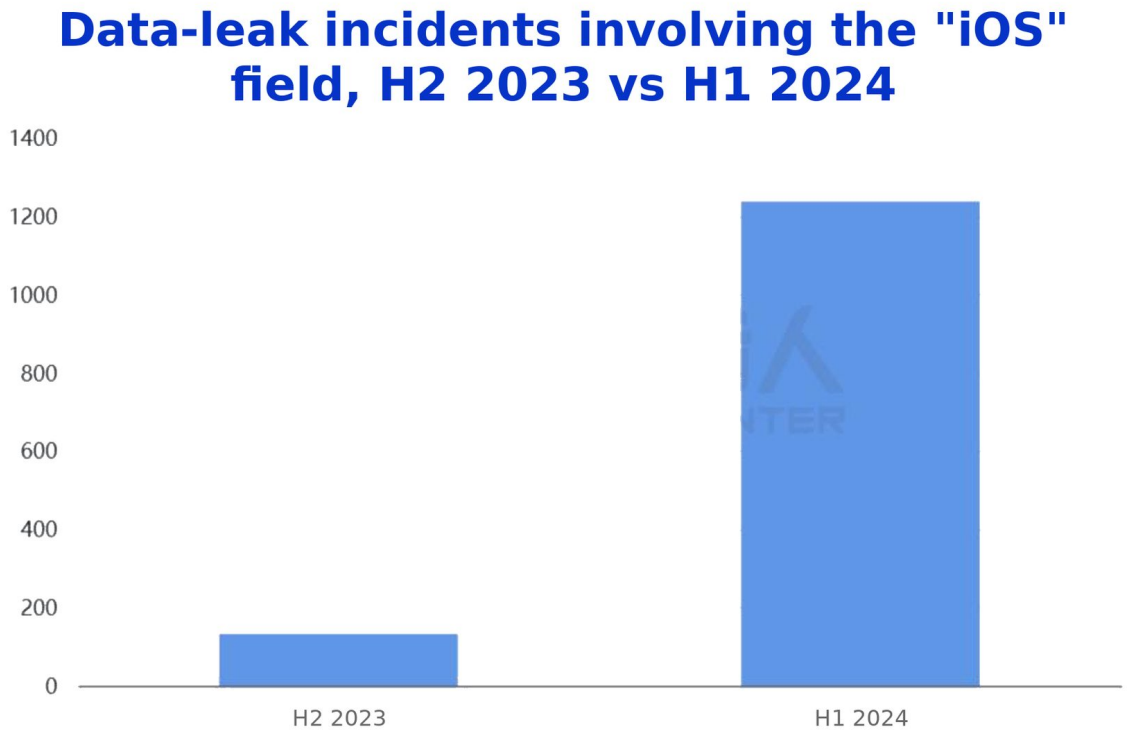
Figure guide

1	Buyer: "Life insurance, iOS, Shandong, Henan, Guangdong, Guizhou, Jiangsu, Jiangxi and Hunan, mixed, 5,000, male, born 1965/1975, must pass FT + iOS" (sent twice)
2	Buyer: "Can you handle it?" Seller: "No problem." Seller: "How was yesterday's feedback?" Buyer: "Not bad."

(Feedback from downstream criminal gangs and data sellers must pass iOS, FT, etc.)

Threat Hunter statistics found that in the first half of 2024, there were as many as 1,237 related risk events containing the "iOS" field in the leaked data, an increase of 8 times compared with the second half of 2023.

As the national public security organs intensify their crackdown on traditional phone fraud, operator supervision strengthens, and built-in video calling becomes more and more popular, criminals begin to focus on the video-calling function and try to use this function to commit fraud. The substantial increase in "iOS" data fields and the communication and verification by threat actors further prove that the current situation of using built-in video calls for fraud has made the development of the upstream data cleaning industry chain more rampant.



Data-leak incidents involving the "iOS" field, H2 2023 vs H1 2024

Source: Threat Hunter original report, page 28. Original figure with Chinese text replaced by English.

Since 2024, Threat Hunter has discovered that many fraudsters pretend to be "financial platform customer service", "National Credit Center staff" and other identities, use a built-in video-calling function to call users of a major smartphone brand, and defraud on the grounds that "millions of dollars in medical insurance need to be closed", "there are outstanding loans that need to be processed", etc., telling mobile phone users that if they do not cancel, they will be forcibly deducted, or their personal credit will be damaged, thereby tricking mobile phone users into transferring relevant funds to designated accounts, causing huge losses to the victims.

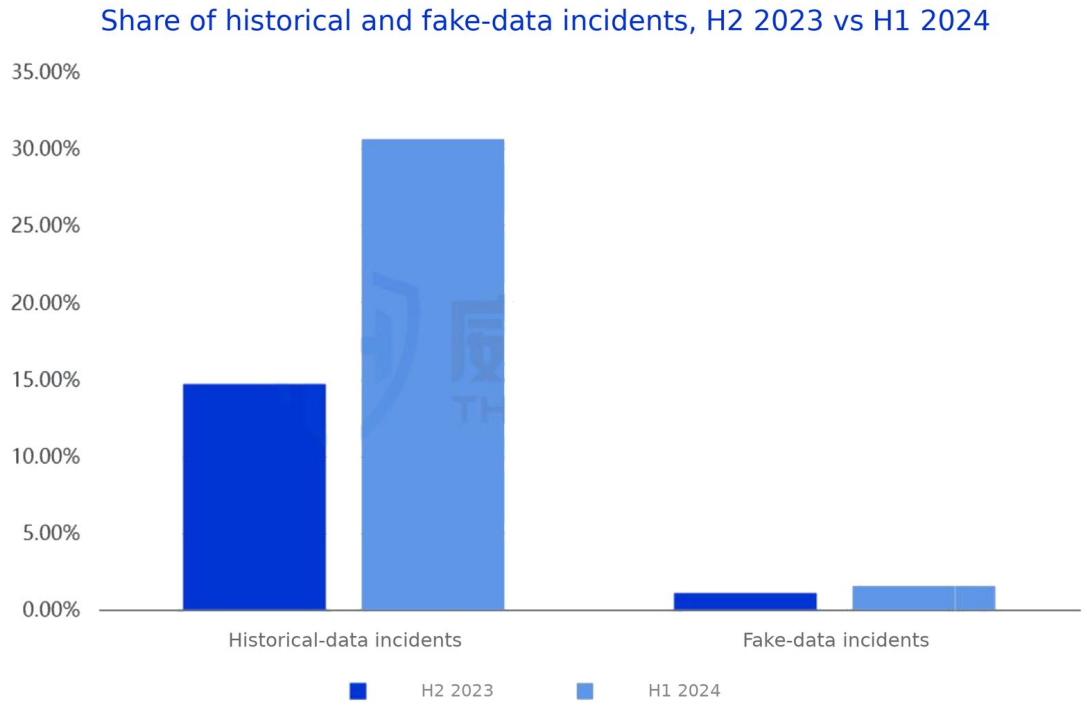
3.2 Among data breaches in the first half of 2024, 30% will include historical data

Historical data events: Threat Hunter identifies events that contain old data in data samples released by threat actors through matching verification with past leaked data;

False data incident: Threat Hunter matches and verifies the three elements contained in the data sample and identifies incidents of false data forged by threat actors;

Based on the optimization of the data authenticity verification engine, Threat Hunter effectively identifies the proportion of incidents that contain historical data in sample data leakage incidents. After sampling analysis, it was found that 30.60% of data leakage incidents in the threat actors trading market in the first half of 2024 contained historical data, that is, 3 out of 10 illegal data transactions were the sale of historical data, an increase of 15.93% from the second half of 2023.

It can be seen that many threat actors in the data trading market have repeatedly made profits by selling historical data, forging data, splicing data, etc. The behavior is even more serious.



Share of historical and fake-data incidents, H2 2023 vs H1 2024

Source: Threat Hunter original report, page 29. Original figure with Chinese text replaced by English.

3.3 In the first half of 2024, there were a total of 657 "file checking" information incidents, and the number of incidents showed a rapid upward trend.

It is not uncommon for threat actors to search their files through encrypted messaging apps and other channels. For example, through a phone number, all identity information related to the phone number can be queried, such as address, bank card number, assets under the name, etc.

File checking: refers to providing investigation or related data extraction services for designated personnel’s information files.

Common file checking services include: trajectory (person trajectory, vehicle trajectory), property in the name (card in the name, car in the name, house in the name), express delivery business (express delivery address, logistics information), personal information (marriage, household registration, social security), etc.



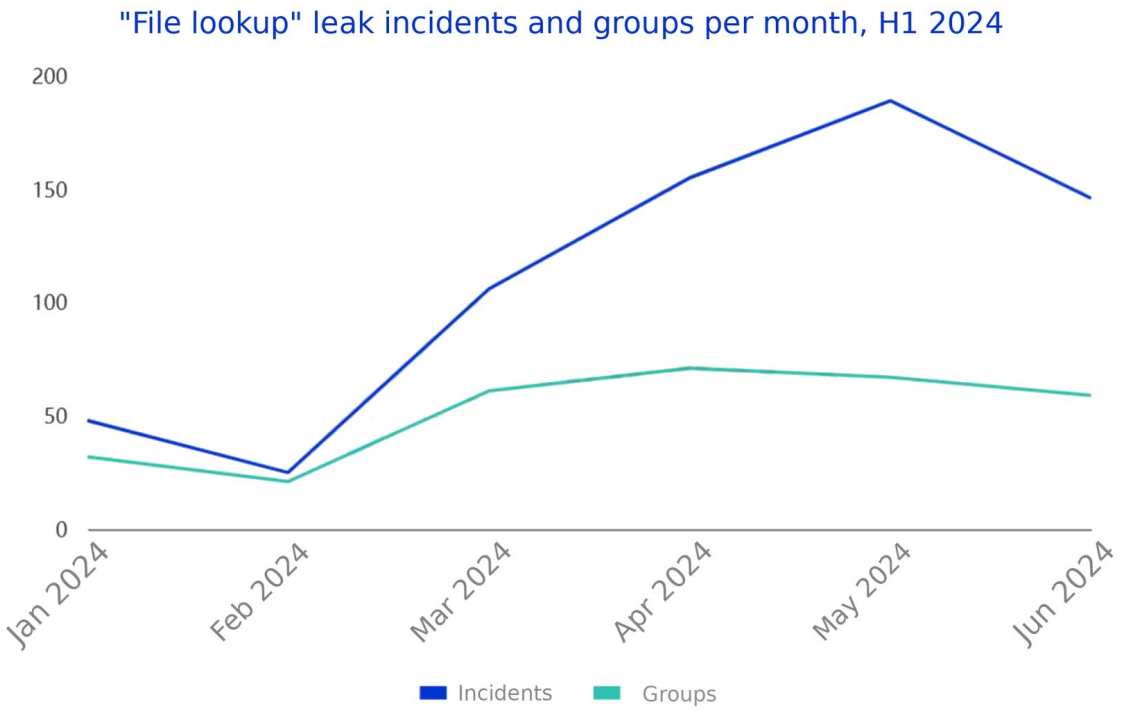
A messaging-app channel advertising "file lookup" services

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

Figure guide

1	Channel name: "... crime records, hotel stays and co-residents, bank statements, vehicle tracks, phone location" (1,493 subscribers)
2	Pinned: "One deal, a choice for life"
3	Services: tracking (people, vehicles, location, phone, flight and train records, entry and exit); phone-owner checks on all three carriers and a payment app; public-network checks (find a person from partial details, vehicles in a name, passports, criminal records, defaulters); assets in a name (bank cards, homes, vehicles); bank services (ID from a bank card, card balance, any bank statement); vehicle files, mortgages and tracks; express delivery (partly blurred); other: marriage, household registration, social insurance employer, frequently used numbers, ID lookup, criminal records of a whole household, statements, medical records. "Contact a salesperson for any of the above"

Among the data breaches discovered in the first half of 2024, Threat Hunter found a total of 657 "archive" information leaks, accounting for 4.10% of the overall data breaches. Judging from the monthly change trend, the number of related risk events related to file checking is on the rise, and the number of related threat actor groups is also increasing. To a certain extent, this reflects that illegal gains through file searches are more common, and the profits behind them are more substantial.

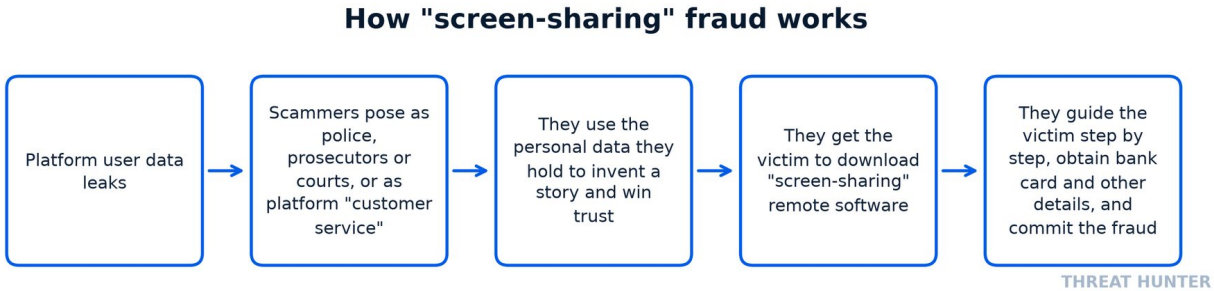


"File lookup" leak incidents and groups per month, H1 2024: both rise

Source: Threat Hunter original report, page 31. Original figure with Chinese text replaced by English.

3.4 There is a high incidence of fraud using “shared screen”. In the first half of 2024, 25 types of “shared screen” remote software were monitored

In the first half of 2024, "screen sharing" fraud occurred frequently. Scammers obtained passengers' personal information and flight information through some illegal channels, pretended to be airline staff, and notified flight delays or cancellations through text messages or phone calls. Through some specific words, victims are guided to download apps with screen sharing functions for reasons such as "refund" and "claim settlement", and then use the user information obtained in the screen sharing state to commit fraud. The specific process is as follows:



How "screen-sharing" fraud works, in five steps

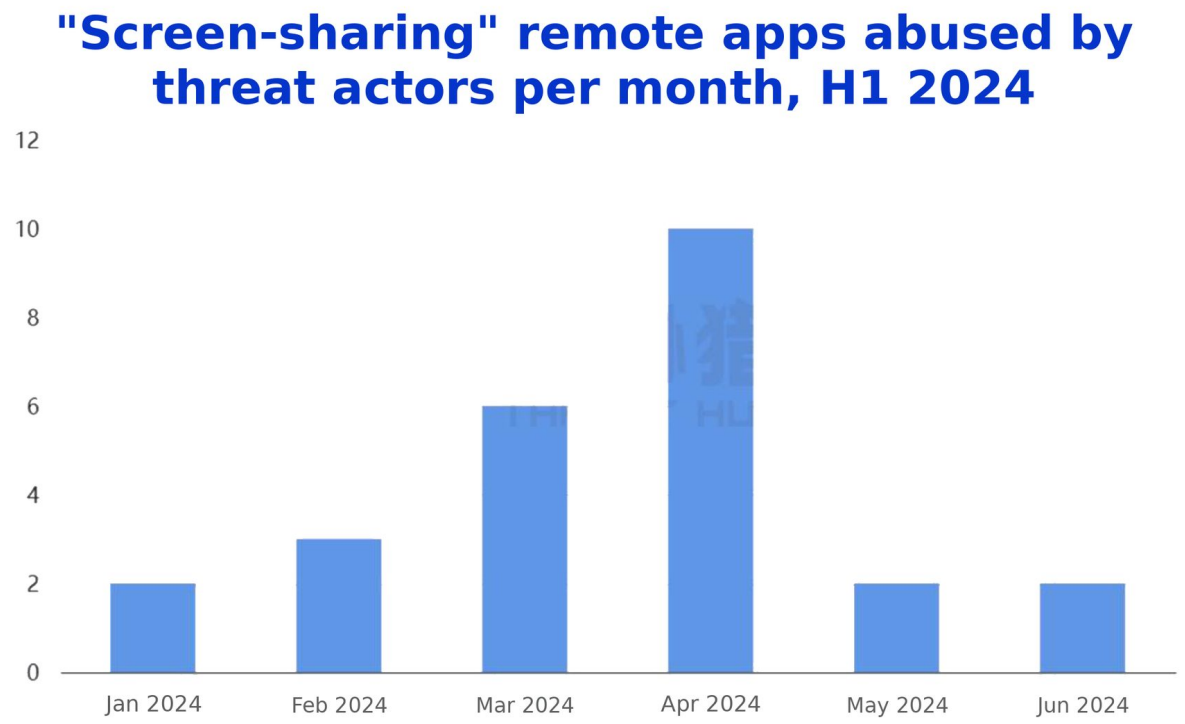
Source: Threat Hunter original report, page 31. Redrawn in English from the original figure.

Give a real case:

Li received a call from an unknown person, pretending to be the "customer service" of an airline, telling him that his flight needed to be changed and compensation would be provided, and asked him to click on an online meeting link to start screen sharing. Since the other party could accurately tell his flight information, Li believed it and performed screen sharing in accordance with his request.

At this time, the scammer took advantage of this function to obtain Li's personal information, and asked Li to provide his bank card number, password, mobile phone verification code and other information on the pretext of identity authentication and unbinding his bank card, and performed facial recognition. In the end, all 30,000 yuan in Li's bank card was transferred away by the other party.

Further research found that there are endless scams using "screen sharing" and "screen sharing" remote software is rapidly updated. According to statistics from the Threat Hunter risk intelligence platform, in the first half of 2024 alone, 25 types of "sharing screen" remote software were discovered that were maliciously exploited by threat actors, such as the common "Chanlian Cloud", "Vymeet" and so on.



"Screen-sharing" remote apps abused by threat actors per month, H1 2024

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

Conclusion

4. Conclusion

Judging from the current status of data leakage risks in the first half of 2024, enterprises need to focus on the following issues:

1. “The number of effective data leakage incidents” and “the number of threat actors trading groups” continue to rise, and the risk of data leakage

The situation is not optimistic. In the first half of 2024 (January to June), a total of 16,011 effective data leakage incidents were monitored and verified across the entire network, an increase of 59.58% from the second half of 2023. In addition, a total of 1,973 threat actor groups involved in data transactions were monitored, an increase of 984 from the second half of 2023 (nearly doubled). The overall activity of illegal data trading groups on encrypted messaging apps continues to rise.

2. Banking, e-commerce, consumer finance and other industries are still at a high level of data leakage, with bank data leakage incidents 2876

Ranked first in the first half of 2024, data breaches involved 85 industries and 1,489 companies. The top five industries with the number of data breaches were banking, e-commerce, consumer finance, insurance, and express delivery. Among them, the number of data breaches in the banking industry was as high as 2,876, making it the industry with the largest number of data breaches.

3. Regional distribution of data breaches in 2024 top 3: Zhejiang, Sichuan, Guangdong

From a regional perspective, the regions with the largest number of data breaches in the first half of 2024 are: Zhejiang, Sichuan, and Guangdong; from an age perspective, 35-54 year olds accounted for 62%; from a gender perspective, women accounted for 64%.

In response to the above 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 tracing their sources, handling delisting and following up on potential risks, and enhancing the timeliness of data leakage risk monitoring and early warning, etc.

In this regard, Threat Hunter proposed a targeted solution:

1. Network-wide intelligence monitoring and mining: covering dark web, anonymous group chat, network disk library, code hosting platform and other channels, never

The same dimension continues to improve the comprehensiveness of channel coverage, including the continuous discovery and update of new channels, special mining of deep intelligence sources (DeepSource), 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 services provide comprehensive credibility assessment results to help enterprises accurately perceive risks and handle risks in a timely manner:

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

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

3. "7×24" emergency response: In October 2023, two major emergency response centers will be established in Shenzhen and Chongqing, and

After-sales service centers have been established in Shanghai, Chongqing, Beijing and other places to conduct round-the-clock monitoring, review and early warning of enterprise-related risk information, and provide services such as "7×24" sample acquisition, intelligence mining, assistance in traceability, disposal and removal, and monthly data leakage risk monitoring reports, as well as analysis results of typical risk events.