THREAT HUNTER RESEARCH

H1 2024 Insurance Data Breach Risk Report

A half-year assessment of insurance-sector data exposure, the channels involved and the resulting governance priorities.

Original publication: 2024-07-15
Research team: Threat Hunter Research Team
Source report: 34 pages

Original report text

This text version is reconstructed based on the 34-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

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

As one of the three pillar industries of the financial industry, the insurance industry involves a large number of high-net-worth individuals, has high data conversion efficiency and strong monetization capabilities, and is a key target of cybercriminal attacks. Data from the "Data Breach Risk Landscape Report for the First Half of 2024" recently released by Threat Hunter shows that 2,039 data breaches occurred in the insurance industry in the first half of 2024, ranking fourth in the industry.

Once a data leak occurs, or the data is not promptly controlled after the leak, the data will be used by the cybercrime ecosystem for large-scale transactions and malicious activity deeds, seriously damaging the interests of platform customers. Financial institutions such as insurance companies will not only suffer customer complaints, but also face punishment from regulatory authorities, damaging their economy and brand reputation.

Threat Hunter has long been committed to in-depth exploration and research of the cybercrime ecosystem chain and data leakage risks. The report will discuss the main characteristics and development of data asset leakage in the insurance industry together with peers.

Related noun definitions:

1. DRRC: Threat Hunter established DRRC Digital Risk Emergency Response Center in Shenzhen and Chongqing, bringing together 30+ security operations

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 anonymous group chats, the 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 information and confirm valid data leakage incidents;

5. Dark web: 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;

6. Citizen’s 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.;

7. 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;

8. 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;

9. Fake data incident: threat actors use forged fake data for transactions;

10. 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, but

Due to problems such as irregular management, these sensitive data are leaked to threat actors through third parties;

11. Leakage of SMS channels: With the development of SMS sending and receiving services over the years, SMS channel providers have begun to lower prices.

In order to obtain higher orders, for example, a transaction will be reached with the SMS sender (Party A) at a price lower than the market standard, and the profit margin will be much lower, so internally, the SMS information data will be illegally sold to obtain more revenue.

12. Operator channel: threat actors obtain the access data of designated web pages through channels such as operator insiders or illegal agents.

Installation data of specified applications, receiving and sending data of specified text messages and other information;

13. Insider leaks: Internal employees of the company, driven by interests, use methods such as data export and manual photography to obtain customer information.

User sensitive information is then sold;

14. Hacker attacks: External hackers use crawlers, scans, penetrations, etc. to attack corporate systems and network assets, taking advantage of corporate

Industrial network vulnerabilities steal data on a large scale;

15. Basic fields: mainly refers to basic personal information, including personal information (name, phone number, ID number, date of birth

Date, gender, age, email address, specific place of residence, education, etc.), property information (income, license plate number, car brand, number type, car price, etc.), family information (marriage status, family relationships, etc.), work information (enterprise unit, occupation, etc.);

16. Business field: mainly refers to information related to insurance business, including insurance type (type of insurance), insurance date, guarantee period,

Insurance amount, policy number, policy form, policy purpose, insurance liability, payment form, platform name, order number, order payment status, order payment amount, order source, etc.;

17. threat-actor-defined fields: In order to improve the value and efficiency of threat-actor data transactions, threat actors will clean and define the data.

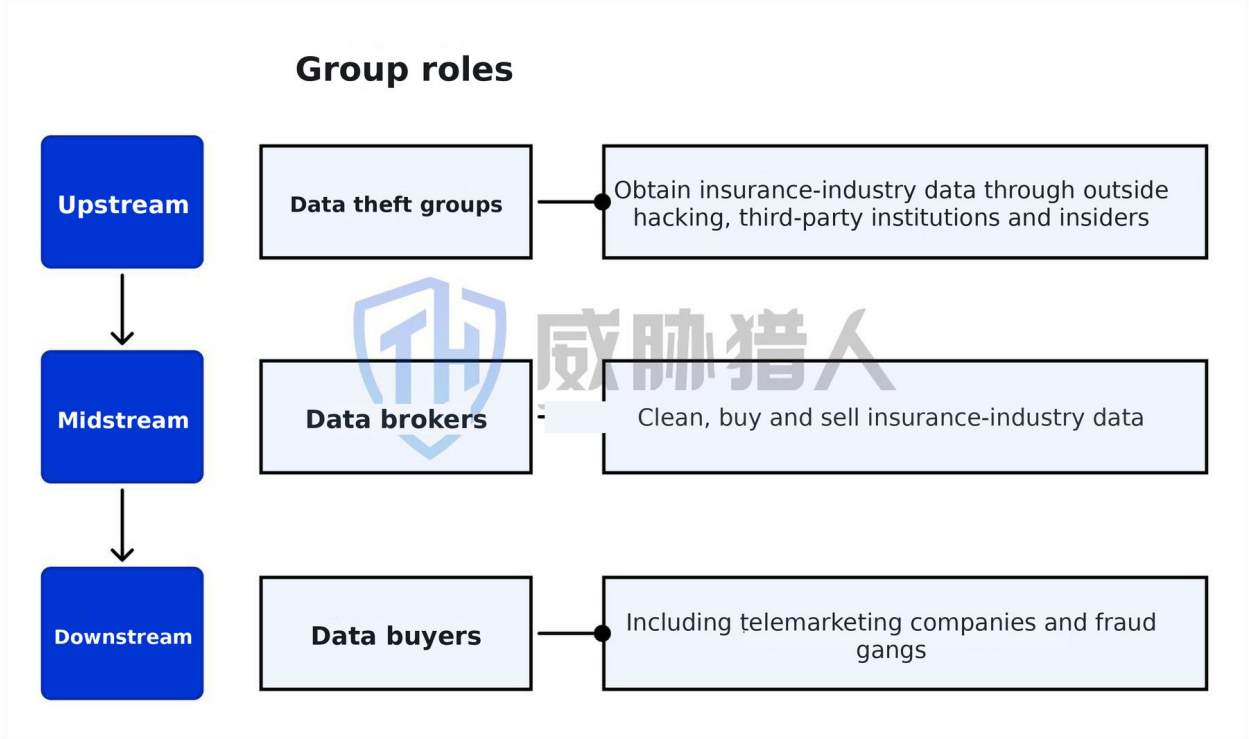
Such as: verification ID, device information (iOS/Android), operator, etc. (Verification ID is mainly used by threat actors to mark the data to prevent secondary trafficking). Mark them to prevent them from being sold again).

Secondary sale).

Introduction to the fraud network of data leakage in the insurance industry

1. Introduction to the fraud network of data leakage in the insurance industry

Threat Hunter conducted in-depth research on the data leakage industry chain in the insurance industry and found that the industry chain surrounding data asset leakage and reselling is currently quite mature and is divided into upstream, middle and downstream based on a clear division of labor and positioning.



The insurance data leak chain: theft groups upstream, data brokers in the middle, buyers downstream

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

Upstream: Data theft groups include company insiders, hackers, operators, operators' third-party agents, SMS channel service providers, etc. These individuals are specifically responsible for

finding ways to obtain and steal data from both inside and outside the insurance organization. At a time when data is becoming more and more valuable, huge profits and extremely low crime costs drive upstream data thieves to be willing to take risks.

Note: The following will analyze the platforms that have been attacked and data leakage channels in the insurance industry. See Chapter 2 for details.

Midstream: Most data middlemen are active on the dark web, encrypted messaging apps, threat-actor forums and other platforms. These people publish posts on different platforms.

Sub-sales data, and is responsible for classifying and cleaning the data to meet the various needs of downstream customers.

Note: The following will analyze underground transaction channels, data fields, etc. that have leaked data in the insurance industry. See Chapter 2 for details.

Downstream: Data buyers include telemarketing companies, fraud gangs, etc. People who purchase data usually use it for targeted marketing and fraud. After use, the data may be resold or exchanged with other illegal parties. In recent years, there has been an increasing demand for refined data, such as data for insurance customers, claims users, and high-net-worth individuals. This data is used for more precise marketing and fraud activities, with a success rate far higher than traditional methods. For example, insurance customer data is used to promote new insurance products, or claims user data is used to commit insurance claims fraud. Changes in downstream demand prompt upstream and midstream illegal personnel to use various technical means to collect user data, classify the data according to demand, and then sell it.

Threat Hunter sorted out fraud incidents related to the insurance industry from May 2023 to May 2024. Fraud incidents occurred on average every month, and fraud incidents related to the insurance industry occurred frequently. According to past fraud cases related to the insurance industry, it can be seen that leaked personal information is the main basic element for the occurrence of fraud in the insurance industry: electronic fraud gangs can use leaked personal information and insurance-related data to tailor scripts and rhetoric to carry out false claims, identity theft, insurance fraud and other activities.

Month	Headline	What happened
May 2023	Posing as insurer staff	Using "policy dividends" as a pretext, they tricked consumers into surrendering policies and buying other investment products.
Jun 2023	Posing as insurer staff	Xiaoyun (alias), who works at a company in Yushan, told the county anti-fraud centre she had been cheated of more than 17,000 yuan under the pretext of "cancelling an insurance account".
Jul 2023	New scam reported in many places	Exploiting victims' unfamiliarity with "million-yuan medical insurance", fraudsters claimed the service would be charged monthly unless cancelled, and tricked victims into transferring money.
Aug 2023	Posing as insurer customer service	At about noon on 5 August, Ms Li of Hangzhou got a call from someone claiming to be from an internet company's insurance agency: "Your messaging app has million-yuan cover that deducts a 20,000-yuan fee each year", and she was asked to pay a handling fee.
Sep 2023	Beware the "million-yuan cover" scam	Fraudsters posed as staff of a million-yuan property insurance product and used policy surrender as a pretext.
Oct 2023	"Million-yuan cover" scams rampant	Fraud using the closing of "million-yuan cover" as a pretext.
Nov 2023	Lost 810,000 yuan trying to cancel "insurance"	A woman fell for a new "insurance" scam by fake customer service; police stopped further losses in time.
Dec 2023	Posing as insurer customer service	Ms Zhang got a call from fake insurer customer service and filled in a fake survey with her personal details; lured by a fake prize, she paid 3,000 yuan in "tax" before realising it was a scam.
Jan 2024	Posing as insurance customer service	Ms He rushed to a police station after a text said more than 4,700 yuan had left her bank card, though she had not made the transfer or shared her card password.
Feb 2024	Fake insurance, real theft	Ms Lü got a call from fake insurance customer service who stated her personal details; worried about her money, she moved more than 490,000 yuan to the "safe account" provided.
Mar 2024	Woman hit by "million-yuan insurance" scam	Police in Chengguan, Lanzhou, solved a scam that used the expiry refund of "million-yuan insurance" as a pretext, recovering the victim's full loss of 105,830 yuan.
Apr 2024	Expiring million-yuan medical cover scams rampant	Mr Zou got a call from fake insurance customer service and was led to a fake website, where he topped up, bought shopping cards and took a loan through an online platform, losing more than 130,000 yuan.
May 2024	Woman caught in "million-yuan cover" scam	Police in Jinfeng district, while promoting anti-fraud awareness, spotted and stopped a scam in the name of "million-yuan medical insurance", recovering 9,600 yuan.

Insurance-themed fraud cases reported in the news, May 2023 to May 2024

Source: Threat Hunter original report, page 8. Table re-typeset in English from the original.

The fraud process is roughly as follows:

Step	What happens
1	An insurer's data is leaked
2	Fraudsters pose as customer service
3	Claiming the user accidentally signed up for insurance and offering to help close the order, they state the user's ID, personal and policy details to win trust
4	They have the user turn on screen sharing, 'verify' with a password red envelope, and transfer the money to the fraudster's bank card

How fraudsters use leaked insurance data to pose as customer service and take victims' money

Source: Threat Hunter original report, page 9. Redrawn in English from the original figure.

The framework of fraud rhetoric is as follows:



A fraud call-centre script tutorial shared in a group chat: "help the client close accidentally opened insurance"

Source: Threat Hunter original report, page 9. Original image retained; numbered translations added by Threat Hunter.

Figure guide

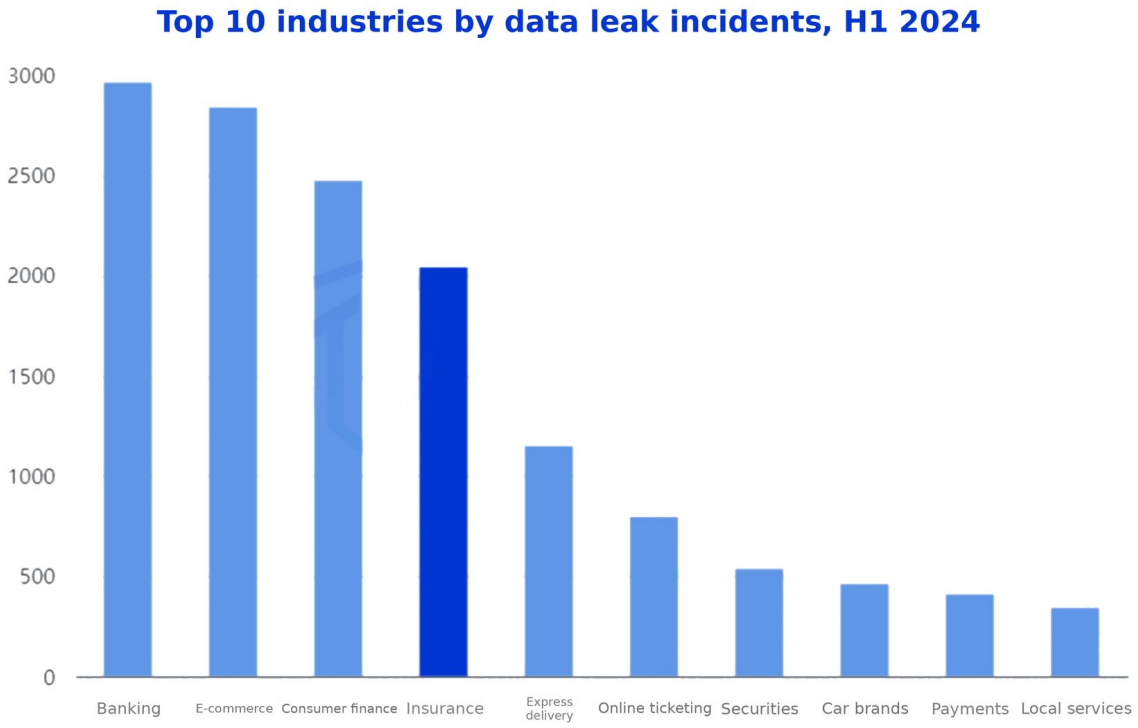
1	Call-centre script tutorial
2	Many people say our script is too long
3	Probably because I didn't organise it well
4	It looks long, but just master the basic framework
5	Our goal is an outcome, not just reading out a script
6	Framework: the client "accidentally signed up" for insurance; take them to look at the policy and see if it can be closed
7	Help close it
8	When closing, have the client repeat what they will tell the bank staff
9	The script can be shortened, but the framework stays
10	It all revolves around this; remember three points
11	Usually, once you reach the closing step, you can lead the client on

Overview of data breach risks in the insurance industry in the first half of 2024

2. Overview of data breach risks in the insurance industry in the first half of 2024

2.1 In the first half of 2024, there were 2,039 data breaches in the insurance industry, involving 80 insurance institutions

In the first half of 2024, Threat Hunter monitored 110 million pieces of intelligence across the entire network. Based on the authenticity verification engine and DRRC manual analysis, there were a total of 16,011 valid data leakage incidents, involving 85 industries, of which the insurance industry ranked fourth with a total of 2,039 incidents, an average of about 340 incidents per month, involving 80 insurance institutions.



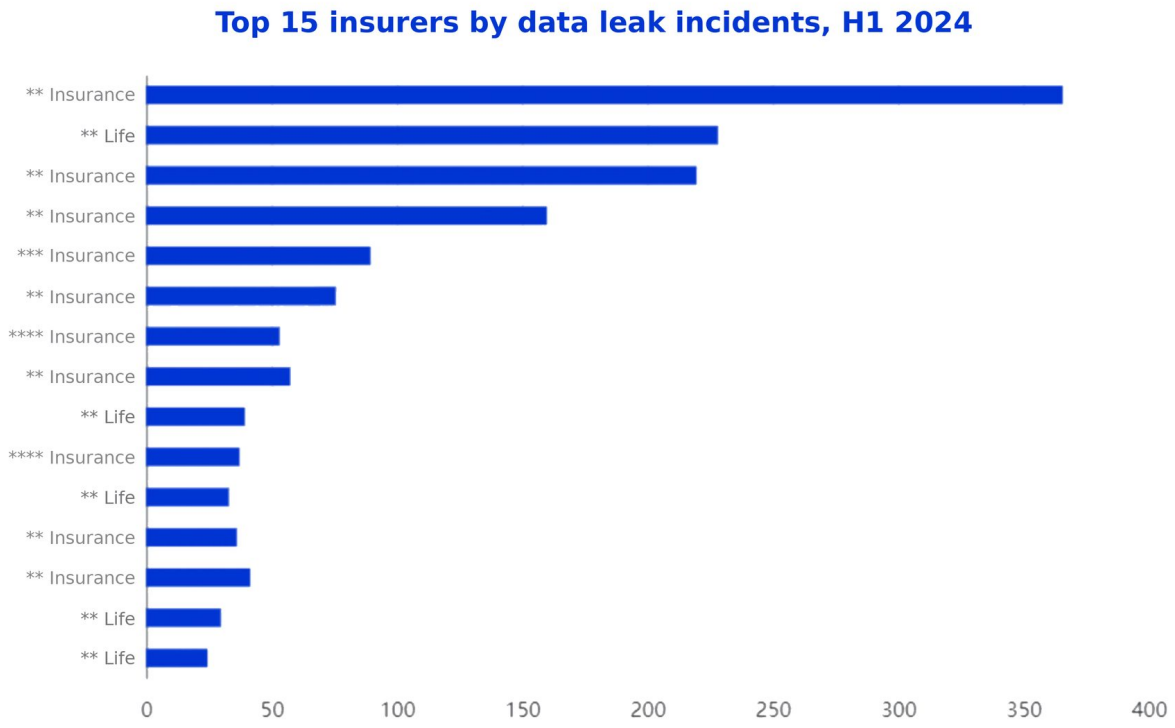
Top 10 industries by data leak incidents in H1 2024: insurance ranks fourth

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

2.2 Large domestic insurance institutions are the main targets of threat actors, accounting for more than 50% of data leakage incidents

Threat Hunter intelligence researchers further analyzed the 15 insurance institutions with the most data breaches in the first half of the year and found that the data breaches involved in these 15 insurance institutions accounted for nearly 80% of the total data breaches in the entire insurance industry, among which the top 5

Institutional data breaches account for more than 50%.

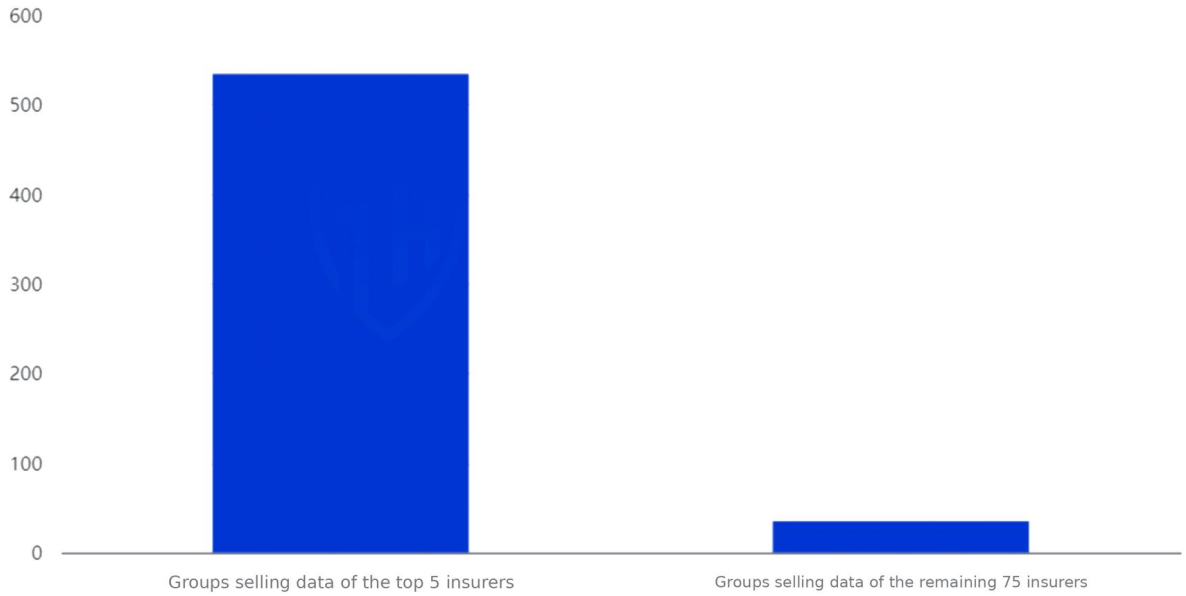


Top 15 insurers by data leak incidents, H1 2024 (names masked in the original)

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

Further analysis of the data trading situation of the Top5 institutions and threat actors shows that the Top5 are all insurance institutions of the top ten domestic insurance brands, with large institutional scales, large user groups on the platform, and large amounts of user data. From the perspective of threat actors trading gangs, there are 569 threat actors gangs that illegally sell insurance institution data, of which 534 are threat actors gangs that sell the data of the Top5 institutions, which far exceeds the number of threat actor gangs that sell the data of other institutions. It can be seen that the Top 5 insurance institutions are the main targets of threat actors.

Threat-actor groups selling data of the top 5 insurers vs the remaining 75 insurers, H1 2024

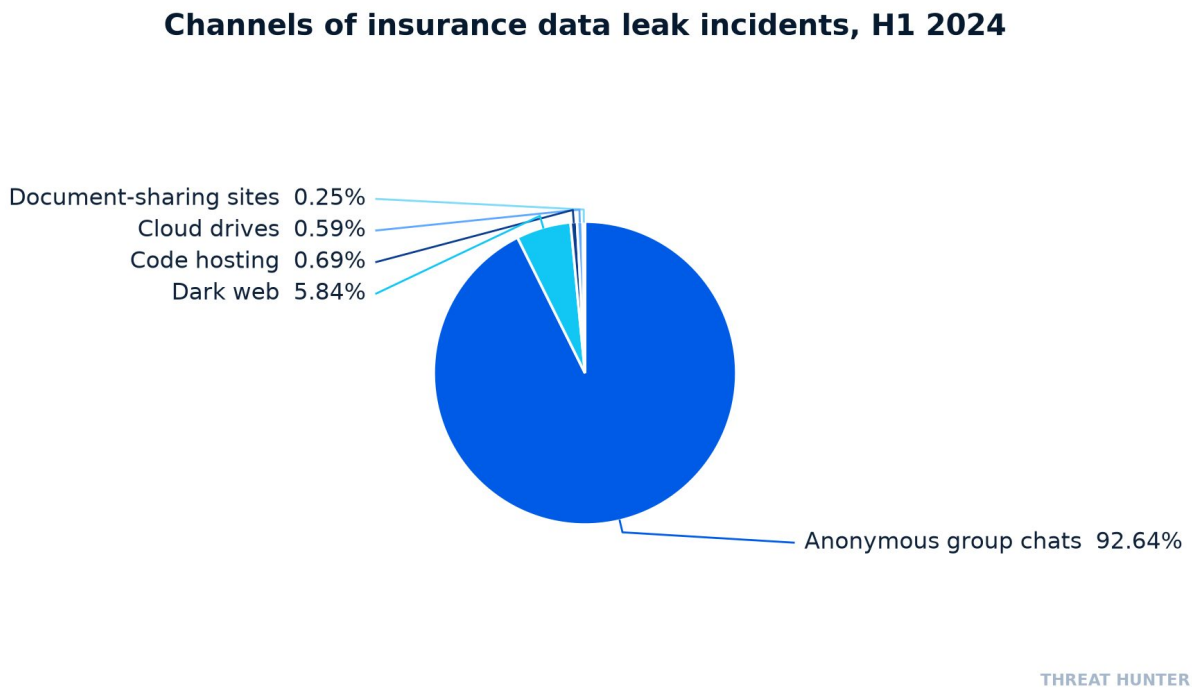


Threat-actor groups selling data of the top 5 insurers far outnumber those selling data of the other 75 insurers

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

2.3 Anonymous group chats and darknet channels are the main transaction channels for illegal data transactions, accounting for more than 98%

Threat Hunter analyzed the transaction channels of data leakage in the insurance industry and found that anonymous group chats on an encrypted messaging app and the darknet accounted for



Channels of insurance data leak incidents, H1 2024: anonymous group chats 92.64%, dark web 5.84%

Source: Threat Hunter original report, page 13. Redrawn in English from the original figure.

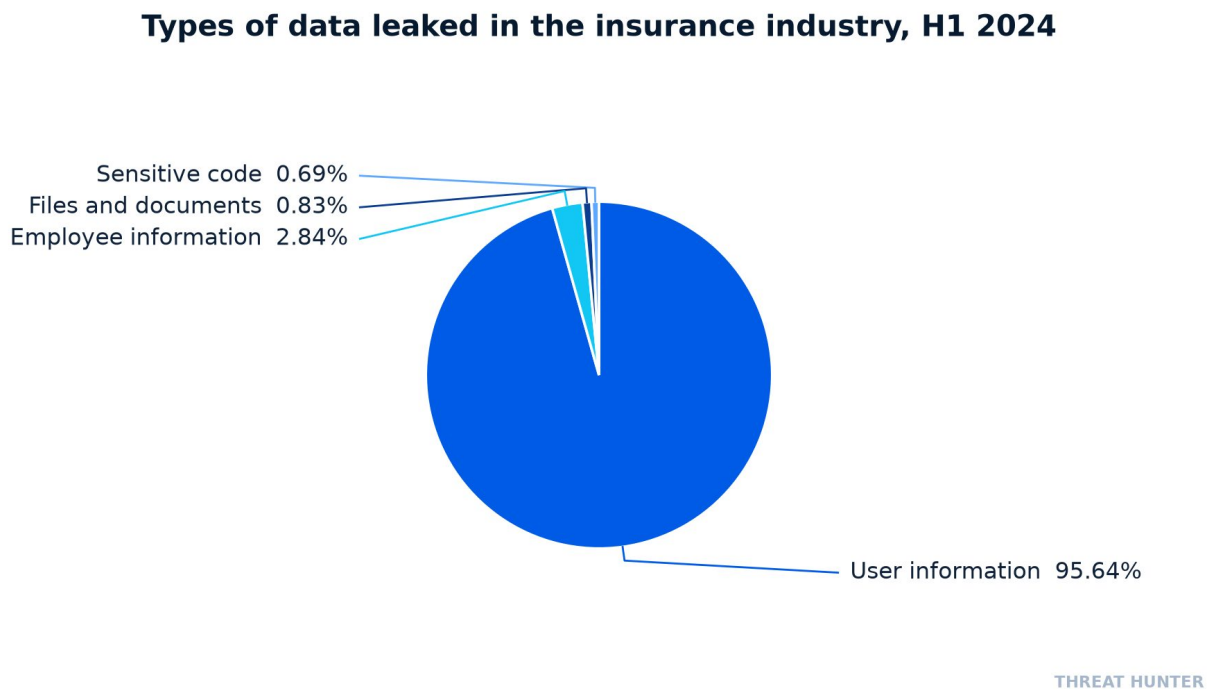
98.47%, is the main channel for threat actors to conduct illegal data transactions, which is consistent with the illegal data transaction channels in the entire industry in the first half of 2024.

The distribution is basically the same.

2.4 The type of data leaked in the insurance industry is mainly user information, accounting for over 95%

Threat Hunter analyzed the data information leaked in the insurance industry and found that user information accounted for as much as 10% of the leaked data.

95. 64%, which is the main type of illegal data transactions.



Types of data leaked in the insurance industry, H1 2024: user information 95.64%

Source: Threat Hunter original report, page 14. Redrawn in English from the original figure.

User information: personal information of platform users, including name, phone number, ID number, insurance-related information, health information, property information, etc.;

Employee information: personal information and professional information of company employees, including employee name, phone number, ID card, professional position and other information;

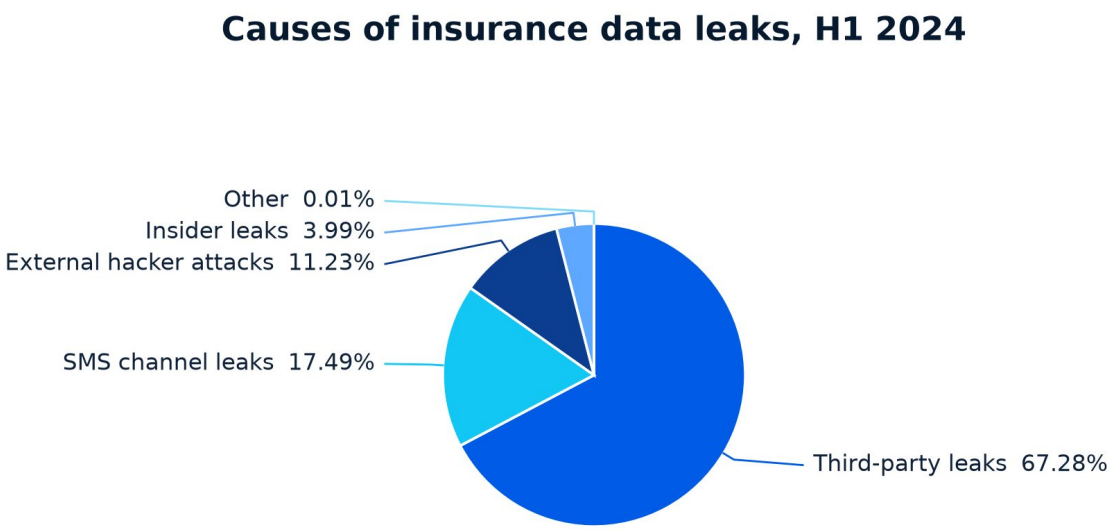
Sensitive documents: Sensitive documents and information within the enterprise, including internal confidential documents, contract documents, product drawings and other information;

Sensitive code: It is sensitive code information within the enterprise, including source code information, API interface keys, environment configuration, domain name and other information.

Note: In order to further understand the details of the leaked user information, Threat Hunter analyzed the leaked data fields. See Chapter 3 for details.

2.5 The leaked data in the insurance industry mainly comes from third-party leaks, followed by SMS channel leaks

Threat Hunter analyzed the sources of data leaks in the insurance industry. Data leaks caused by third parties were the main reason, accounting for 67.28%, followed by SMS channel leaks, accounting for 17.39%, external hacker attacks accounting for 11.23%, and internal employee leaks 3.99%.



Causes of insurance data leaks, H1 2024: third-party leaks 67.28%, SMS channel leaks 17.49%

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

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;

Leakage of SMS channels: With the development of 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 a deal with the SMS sender (Party A) at a price lower than the market standard, and its profit margin

It is much lower, so internally, more revenue will be obtained by illegally selling SMS message data.

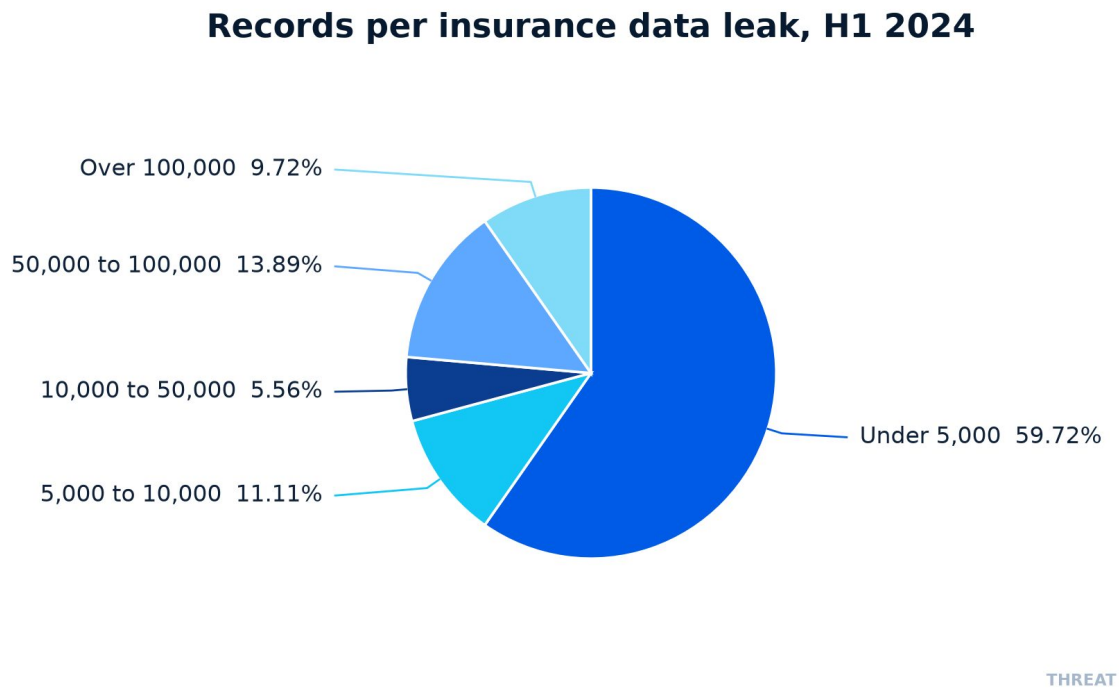
Operator channel: threat actors obtain information such as access data of specified web pages, installation data of specified applications, receiving and sending data of specified text messages, etc. through channels such as operator insiders or illegal agents;

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.

2.6 The amount of data leaked in a single incident is mostly small-scale, with nearly 60% of data leaked under 5,000 items.

In the first half of 2024, most of the data transactions of threat actors in the insurance industry captured by Threat Hunter were small-scale transactions of less than 5,000, accounting for 59.72%.



Size of single insurance data leaks, H1 2024: 59.72% involved fewer than 5,000 records

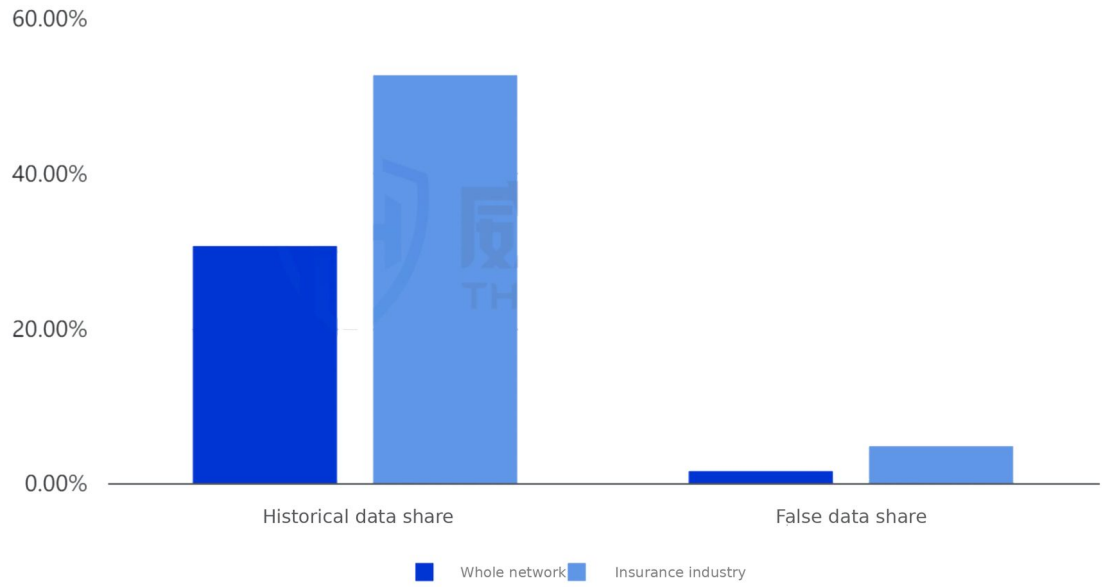
Source: Threat Hunter original report, page 16. Redrawn in English from the original figure.

Although the overall data transactions are mainly small-scale data transactions, there are also many single leaks of more than 100,000 pieces of data, with up to 700,000 pieces of data. Further analysis shows that this incident is a major data leakage incident in an insurance institution in 2022.

2.7 The proportion of historical data and false data among the data traded by threat actors in the insurance industry far exceeds the level of the entire network

Threat Hunter conducted an authenticity verification analysis on the data traded by threat actors in the insurance industry and found that the proportion of false data and historical data far exceeded the overall level of the entire network:

Share of historical and false data: whole network vs insurance industry, H1 2024



Historical and false data shares among traded data: whole network vs insurance industry, H1 2024

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

Analyzing from the perspective of historical data, 52.67% of the leaked insurance data is historical leaked data, which exceeds 30.60% of the historical data of the entire network;

Analyzing from the perspective of data authenticity, 4.76% of the leaked insurance data is false and mismatched information data, exceeding the 1.54% proportion of false data in the entire network.

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 events: Threat Hunter matches and verifies the three elements contained in the data sample and identifies false data events forged by threat actors.

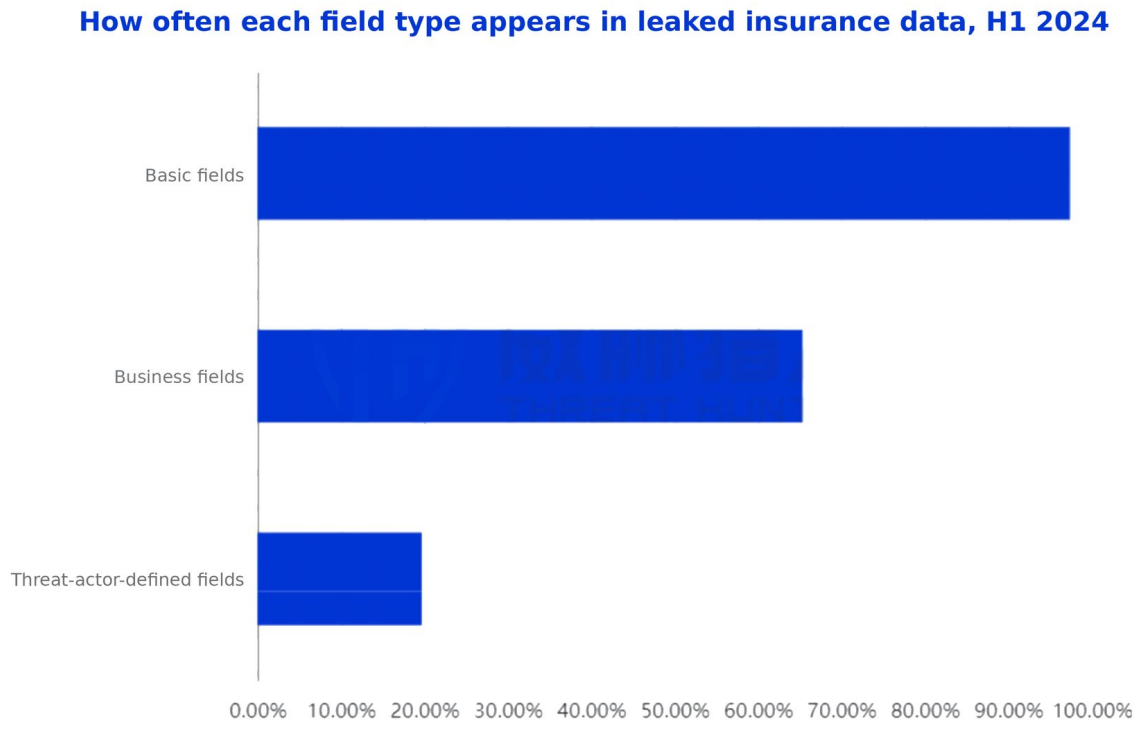
The Threat Hunter authenticity verification engine will conduct credibility assessment and preliminary verification of risk intelligence based on the historical overlap of data samples, three-factor matching, and source confidence, helping enterprises identify false data, historical data, and irrelevant data released by threat actors, and improve the accuracy and credibility of event warnings.

Analysis of data leakage fields and crowd portraits in the insurance industry

3. Analysis of data leakage fields and crowd portraits in the insurance industry

3.1 Nearly 98% of the data contains basic personal information, and 20% of the data contains custom tags for threat actors

Threat Hunter's statistical analysis of leaked data fields in the insurance industry found that data fields mainly include basic fields, business fields, and threat actors' defined fields. 97.40% of the data contains basic fields, and 65.35% of the data contains business fields. It is worth noting that threat actors' custom fields reached 19.71%. In order to improve the value and efficiency of threat actors' data transactions, threat actors will clean the data and customize labels.



Field types in leaked insurance data, H1 2024: nearly 98% contain basic personal fields

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

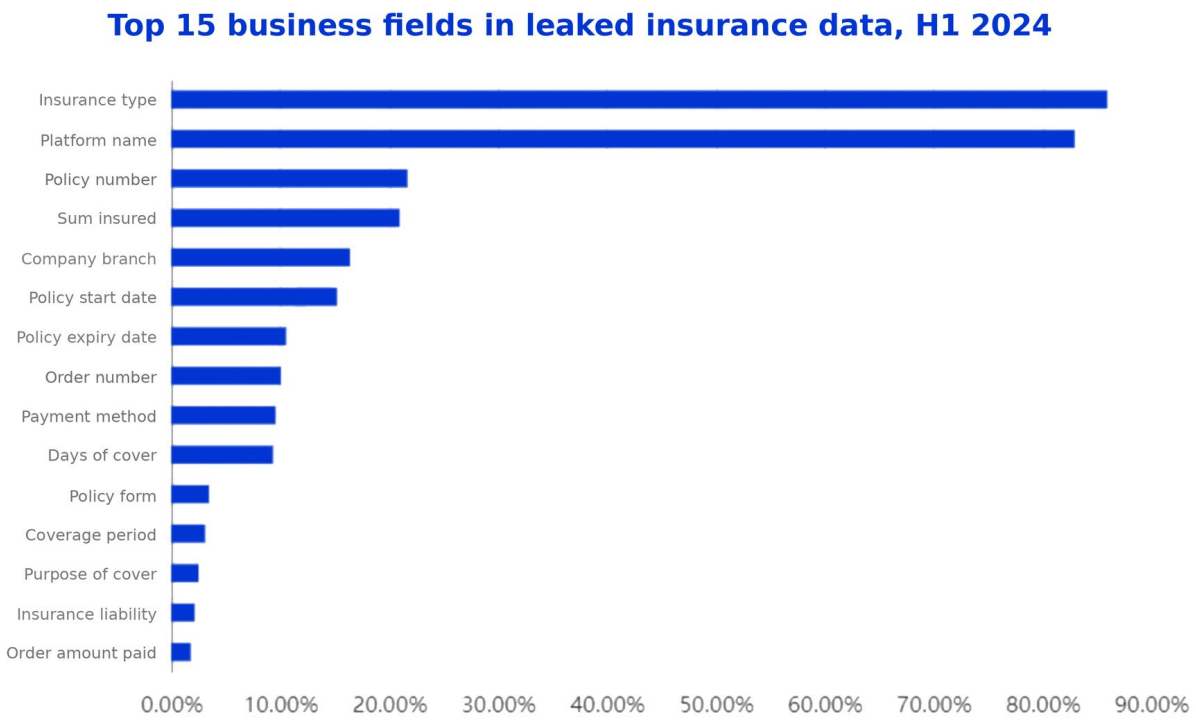
Basic fields: Mainly refers to basic personal information, including personal information (name, phone number, ID number, date of birth, gender, age, email, specific place of residence, education, etc.), property information (income, license plate number, car brand, number type, car price, etc.), family information (marriage status, family relationships, etc.), work information (enterprise unit, occupation, etc.);

Business fields: mainly refers to information related to insurance business, including insurance type (type of insurance), insurance date, guarantee period, insurance amount, policy number, policy form, policy purpose, insurance liability, payment form, platform name, order number, order payment status, order payment amount, order source, etc.;

threat-actor-defined fields: Mainly refers to the fields defined by cybercriminal groups after data cleaning, such as: verification ID, device information (iOS/Android), mobile carrier, etc. (Verification ID is mainly used by threat actors to mark data to prevent secondary trafficking).

3.2 The insurance business fields that appear most frequently are “insurance type” and “platform name”

Threat Hunter analyzed the insurance business information fields and found that fields such as "insurance type", "platform name", "policy number", and "insured amount" appear more frequently. Among them, "insurance type" has the highest frequency, up to 85.97%, followed by "platform name", up to 82.97%. This data is very specific. Once the fraud gang obtains this data, it can accurately grasp the insurance status of users of insurance institutions and commit fraud.

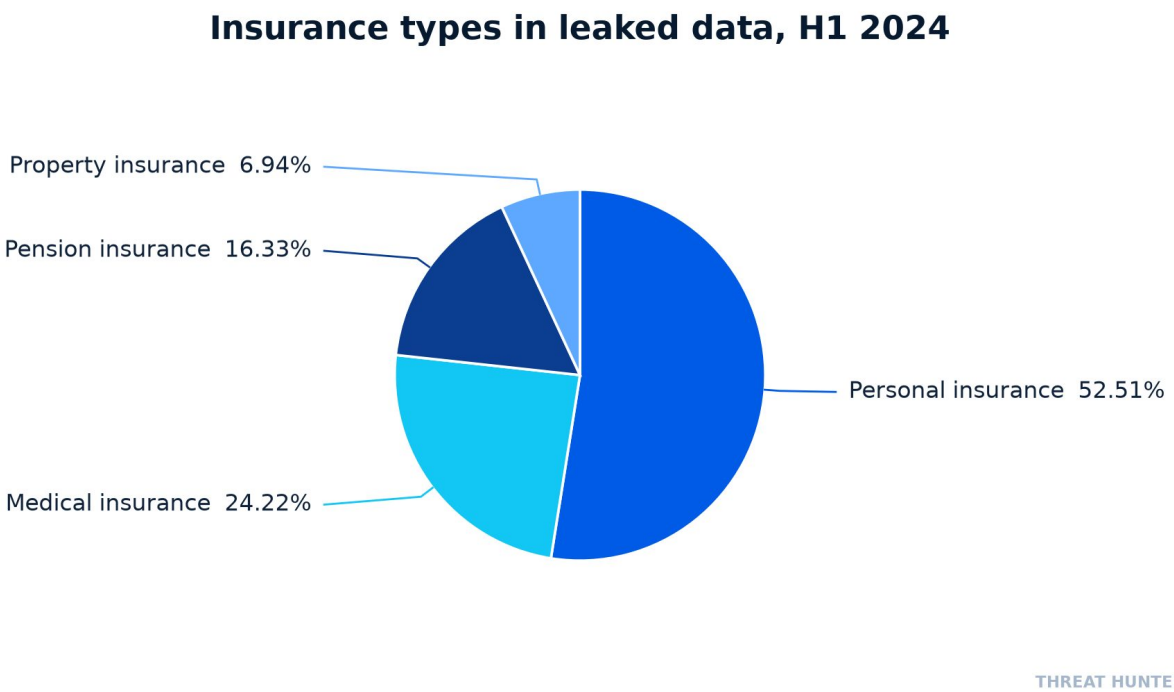


Top 15 business fields in leaked insurance data, H1 2024: insurance type and platform name lead

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

3.3 "Personal insurance" accounts for the highest proportion among "Insurance Types", with "life insurance" and "annuity insurance" being the most common

Threat Hunter analyzed "insurance type" and found that the leaked insurance industry data mainly involved products such as "personal insurance", "medical insurance", "pension insurance" and "property insurance", among which "personal insurance" accounted for the highest proportion, reaching 52.51%.



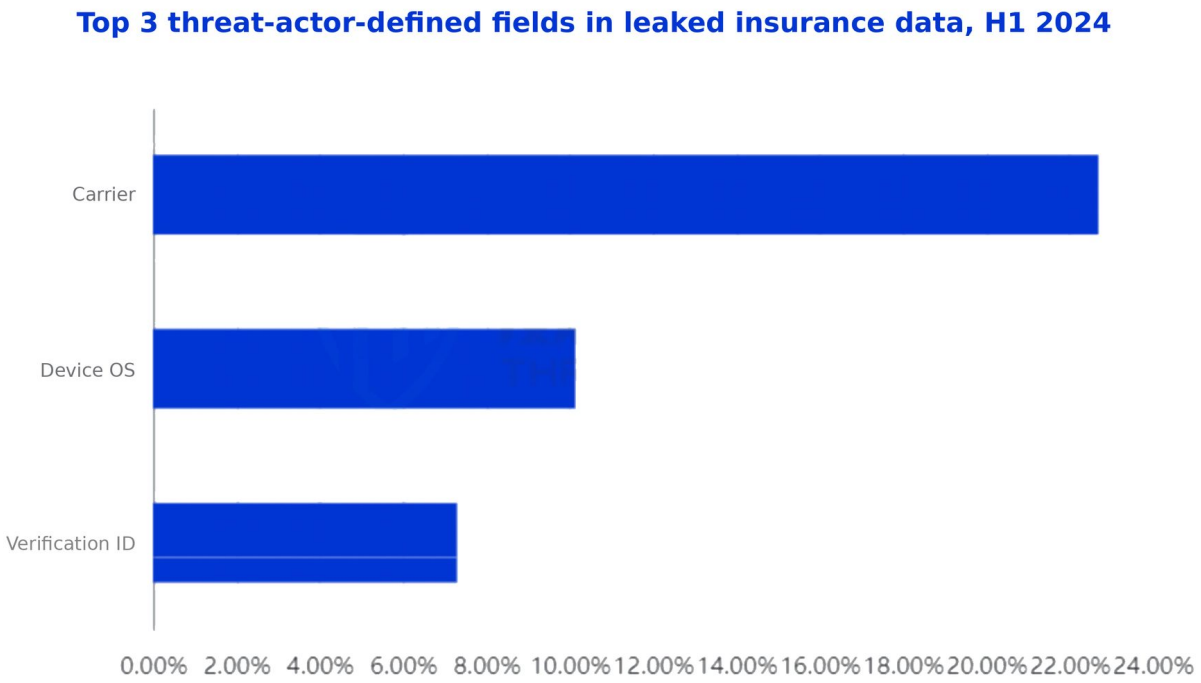
Insurance types in leaked data, H1 2024: personal insurance 52.51%

Source: Threat Hunter original report, page 22. Redrawn in English from the original figure.

Further analysis found that among the "personal insurance" products, "life insurance" and "annuity insurance" are the majority.

3.4 Fraud gangs carry out precise fraud on insurance platform users through the "iOS" field tag

In order to improve the value and efficiency of threat-actor data transactions, cybercriminal groups will clean the data and customize labels. In the first half of 2024, a large number of fields defined by threat actors appeared in the leaked data, with "operator", "device system", "verification ID", etc. appearing most frequently:



Top 3 threat-actor-defined fields in leaked insurance data, H1 2024: carrier, device OS and verification ID

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

It is worth noting that there is a large amount of data labeled "iOS" in the "device system". Judging from the chat records between the underground data trafficking actors group and downstream data buyers, the downstream data buyers repeatedly mentioned the screening requirements for "iOS" device data in their repurchase requirements for data.

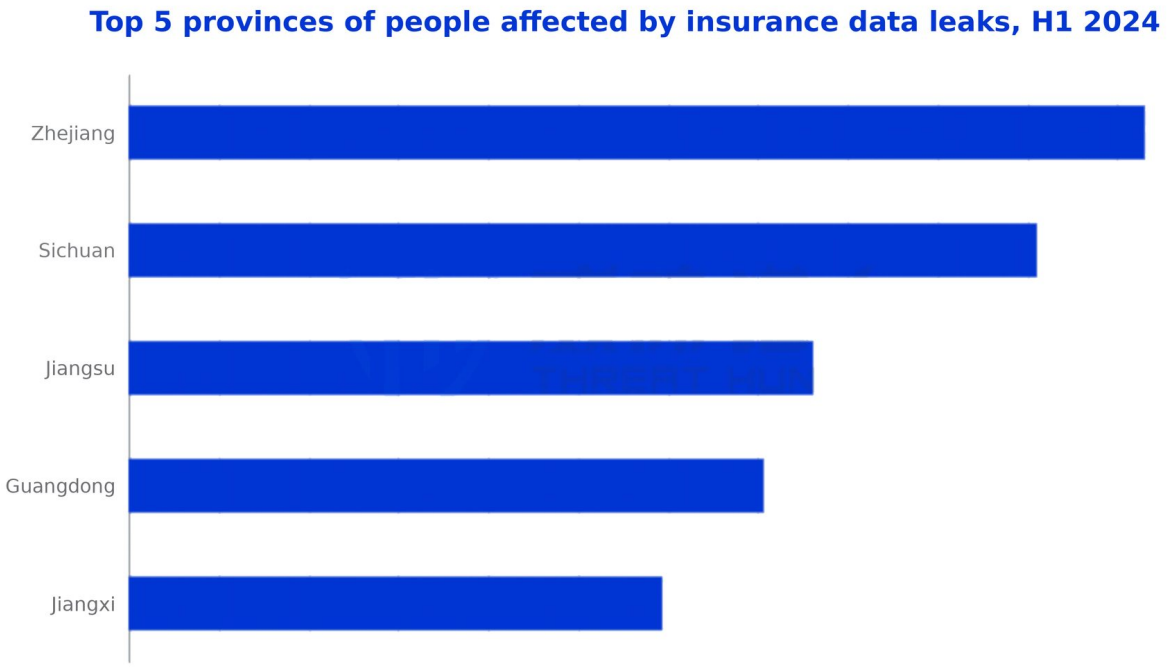
It was mentioned in Threat Hunter's "Data Breach Risk Landscape Report for the First Half of 2024" that fraudsters used a built-in video-call function to commit fraud by filtering out "iOS" user information. Since 2024, Threat Hunter has discovered that many fraudsters have pretended to be "financial platform customer service", "National Credit Information Center staff" and other identities to use this video-call function to call iOS phone users and defrauds them on the grounds that "million-dollar medical insurance needs to be closed", "there are unpaid loans that need to be processed", etc., and informs mobile phone users that if they do not cancel, they will be forced to deduct money, 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.

Take a real event as an example:

On March 19, the victim, Mr. Lin, received a video call through the built-in video-call function from an unknown number. The other party said that he had purchased "million-dollar medical insurance" online. The monthly payment standard was 800 yuan, and the annual fee was 9,600 yuan. If you do not go through the cancellation procedures, the payment will continue to be deducted. Believing it to be true, the victim Lin went through the cancellation procedures as required by the other party. He was guided to send a red envelope with a password to a designated account on a mobile payment app, and was defrauded of more than 300,000 yuan.

3.5 The data leakage user groups in the insurance industry are mainly concentrated in Zhejiang, Sichuan and other places, and are mainly middle-aged women.

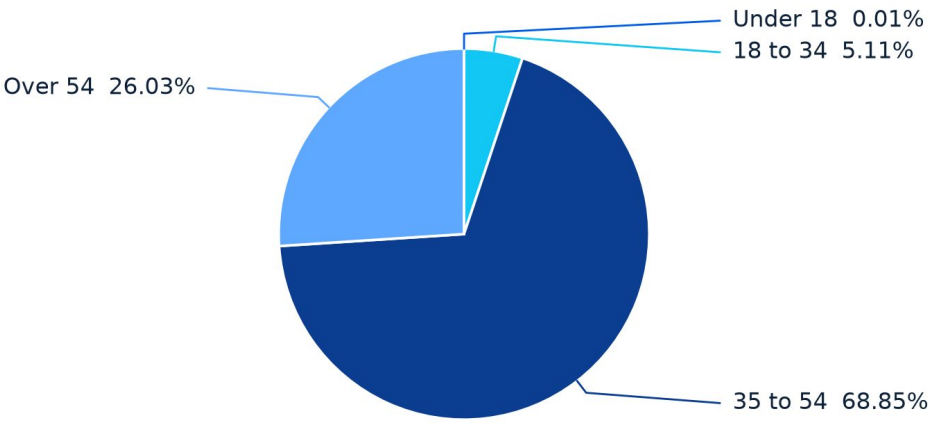
Threat Hunter conducted a sampling analysis of portraits of people whose data was leaked in the insurance industry and found that the victim groups of data leaks in the insurance industry are mainly concentrated in Zhejiang, Sichuan, Jiangsu and other places; in terms of age distribution, people between 35 and 54 years old accounted for the largest proportion, reaching 68.85%; in terms of gender distribution, women accounted for 78.44%, far exceeding the 21.56% of men.



Top 5 provinces of people affected by insurance data leaks, H1 2024: Zhejiang and Sichuan lead

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

Age of people affected by insurance data leaks, H1 2024

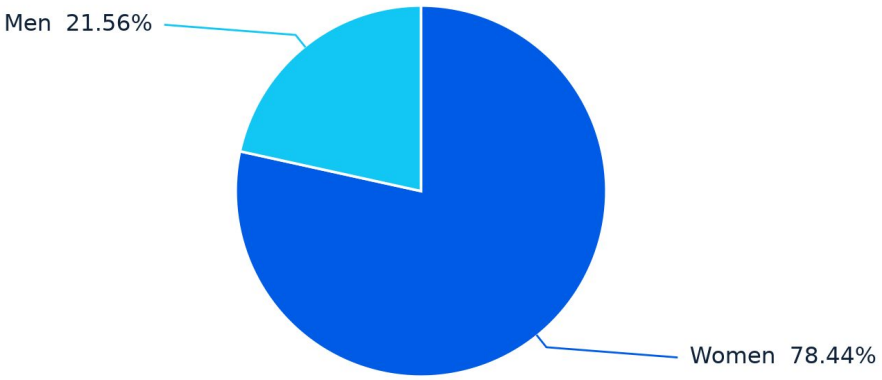


THREAT HUNTER

Age of people affected by insurance data leaks, H1 2024: 35 to 54 accounts for 68.85%

Source: Threat Hunter original report, page 25. Redrawn in English from the original figure.

Gender of people affected by insurance data leaks, H1 2024



THREAT HUNTER

Gender of people affected by insurance data leaks, H1 2024: women 78.44%

Source: Threat Hunter original report, page 25. Redrawn in English from the original figure.

Analysis of typical data breach incidents in the insurance industry Analysis of typical data breach incidents in the insurance industry

4. Analysis of typical data leakage incidents in the insurance industry

4.1 Due to insufficient third-party security control, a large amount of sensitive data in the insurance industry was leaked

In order to improve the efficiency of business development and service quality, insurance institutions often introduce third-party cooperation agents. Many third-party cooperation agents are small and medium-sized enterprises that put "business first" and invest relatively little in security construction. Moreover, their business involves a large number of customers' sensitive data, making them easy targets for attacks by threat actors.

Threat Hunter's monitoring intelligence analysis on the anonymous chat platform channel found that a large amount of sensitive data in the insurance industry is being traded. The leaked data fields not only contain the user's personal information, but also contain the user's specific insurance information (insurance type, insurance amount, insurance period, etc.), and involve multiple insurance companies.

Data sample is as follows:



Sample of leaked policy data from several insurers, attributed to a third-party leak

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

Figure guide

1	Plan name (personal accident cover, outpatient medical)
2	ID document type: ID card
3	Gender
4	City: Shanghai
5	Insurance

Analysis process:

Threat Hunter found that the data fields leaked by such data samples were relatively complete, including not only personal information, but also insurance information.

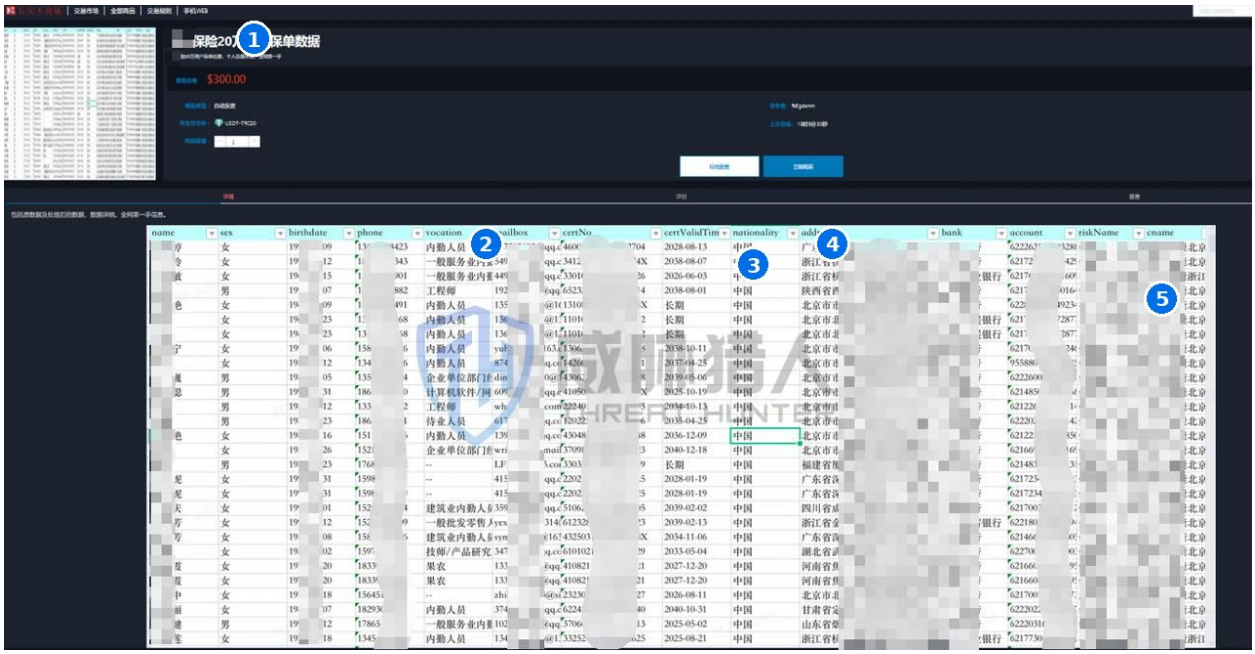
At the same time, multiple insurance institutions are involved, so Threat Hunter initially determined that the leak was caused by a third party related to cooperation with multiple insurance institutions.

4.2 The API organization of an insurance institution was hacked, and the policy information of 200,000 users was leaked

As the level of network security in various industries continues to improve, it is becoming more and more difficult for hackers to invade and obtain backend permissions. Therefore, many hackers target API interfaces with security flaws and steal data through data traversal attacks and other methods.

Threat Hunter's monitoring intelligence analysis on darknet platform channels found that the policy information data of 200,000 users of a domestic insurance institution was sold by threat actors for $300. The leaked data samples not only included basic information such as user names and phone numbers, but also the user's job position, home address, bank card and other information.

Data sample is as follows:



A dark-web listing offers policy data of 200,000 users of an insurer for US$300

Source: Threat Hunter original report, page 28. Original image retained; numbered translations added by Threat Hunter.

Figure guide

1	Policy data of 200,000 users of an insurer
2	Occupation (e.g. office staff, engineer)
3	Nationality: China
4	Address (province and city)
5	City

The analysis process is as follows:

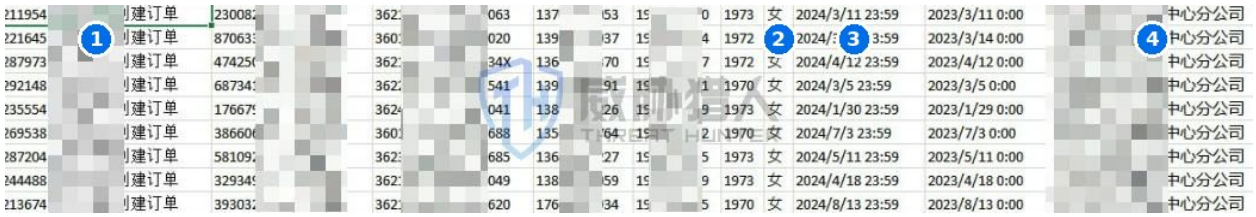
According to the information provided by the dark web post, the insurance data sold by the other party only involves a certain domestic insurance institution, which is highly targeted; at the same time, the leaked data fields are relatively complete and involve multiple sensitive fields. Therefore, combining the above two points, threat hunting

People initially judged that it was suspected to be caused by an external hacker attack on the insurance institution.

4.3 Suspected "insiders" in insurance institutions illegally obtain user data and profit

Threat Hunter's monitoring intelligence analysis on anonymous chat platform channels found that threat actors are selling user information data of a domestic insurance institution. The following is the data sample information provided.

Data sample:



Sample of policy data suspected to have been taken by an insurer's insiders

Source: Threat Hunter original report, page 29. Original image retained; numbered translations added by Threat Hunter.

Figure guide

1	Order created
2	Gender
3	Policy dates
4	Branch office

Analysis process:

Threat Hunter analyzed that the data sample not only contains the user's personal information, but also includes the establishment status of the insurance institution and the status of the insurance institution's branches within the enterprise.

Therefore, Threat Hunter initially determined that it was suspected that internal employees of the insurance institution used internal channels to illegally obtain data and then sold it to the data trading market.

4.4 Suspected security risks in SMS channels lead to data leakage in insurance institutions

Threat Hunter's monitoring intelligence analysis on anonymous chat platform channels found that there are threat actors selling SMS information data of insurance agency users. The following is the data sample information provided.

Data sample:



Sample of SMS records leaked through an SMS channel, including policy notification texts

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

Figure guide

1	Gender
2	Province
3	City
4	SMS text: "Policy effective notice: Dear ..."

Analysis process:

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 message data.

The source of SMS data leakage comes from the SMS channel, which is generally a third-party service. It itself has the risk of penetration or information leakage, leading to data leakage within the third-party service.

Threat Hunter analyzed the leaked data samples and found that the leaked data contained the content of user text messages, and the security protection of the SMS delivery interface of the company's own platform was relatively complete. Therefore, it was initially determined that the suspected leak channel was caused by the SMS channel.

Conclusion

5. Conclusion

Data breaches in the insurance industry in the first half of 2024 are not optimistic. From the perspective of data leakage risk status in the insurance industry, companies need to focus on the following issues:

1. The number of data breaches in the insurance industry in the first half of 2024 was 2,039, involving 80 insurance institutions

In the first half of 2024, there were a total of 16,011 data breaches across the entire network, with the insurance industry ranking fourth with a total of 2,039 incidents, an average of about 340 incidents per month, involving 80 insurance institutions.

2. Large insurance institutions are the main targets of threat actors, accounting for more than 50% of data breaches.

In the first half of 2024, the Top 5 are all insurance institutions of the top ten domestic insurance brands. They have large institutional scales, large platform user groups, and large amounts of user data. There are 534 threat actor groups selling the data of the Top 5 insurance institutions (a total of 569 threat actor groups illegally selling insurance company information data).

3. Third-party leakage and SMS channel leakage are the main reasons for data leakage in insurance institutions.

Different from previous years, as insurance institutions increasingly strengthen data protection and pay attention to the data security management of internal systems, traditional data leaks caused by insider leaks, penetration and dragging, etc. are gradually decreasing. Improper data access control by partners, SMS channel leaks and other methods have become the current mainstream. In 2024, the proportion of data leaks in the insurance industry caused by third parties will be as high as 67.28%, and data leaks caused by SMS channels accounted for 17.39%.

4. “Personal insurance” accounts for the highest proportion among “Insurance Types”, with “life insurance” and “annuity insurance” being the most common.

Among the data leaked in the insurance industry in the first half of 2024, data involving "personal insurance" accounted for the highest proportion, reaching 52.51%;

Further analysis found that among the "personal insurance" products, "life insurance" and "annuity insurance" are the majority.

5. The proportion of false data and historical data in the data traded by threat actors in the insurance industry far exceeds the level of the entire network.

Among the insurance data leaked in the first half of 2024, 52.67% were historical leaked data, accounting for 30.60% of the historical data of the entire network; 4.76% were false mismatched information data, accounting for 1.54% of the false data of the entire network.

6. The data leakage user groups in the insurance industry are mainly concentrated in Zhejiang, Sichuan and other places, and are mainly middle-aged women.

From a regional perspective, the regions with the largest number of data breaches in the insurance industry in the first half of 2024 are: Zhejiang, Sichuan and other places; from an age perspective, 35-54 year olds accounted for 68.85%; from a gender perspective, women accounted for 78.44%.

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.