THREAT HUNTER RESEARCH

2024 Data Breach Risk Landscape Report

A 2024 landscape of verified data exposure, illegal trading chains and the practical requirements for verification and response.

Original publication: 2025-01-12
Research team: Threat Hunter Research Team
Source report: 42 pages

Original report text

This text version is reconstructed based on the 42-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.

About Threat Hunter

Threat Hunter was founded in 2017 and helps organizations identify and respond to business fraud, external digital risk, and API security threats. Its work combines cybercrime intelligence, risk data, product platforms, and specialist services.

The company provides mature and diverse products and services focusing on risk scenarios such as business fraud, data leakage, phishing and counterfeiting, and API attacks that different industries face in the process of digital development. It has been selected as a representative vendor in Gartner's technology maturity curve report and IDC's threat intelligence field for many times.

Headquartered in Shenzhen, Threat Hunter also operates offices in Beijing, Shanghai, and Chongqing, with Digital Risk Response Centers in Shenzhen and Chongqing. The company supports customers in China, Europe, the United States, South America, and Southeast Asia.

Preface

In the wave of the digital age, data has become a key element of the core competitiveness of enterprises. However, the risk of data leakage is like the sword of Damocles, hanging over the heads of various industries. In 2024, data breaches will occur frequently, affecting many companies and seriously threatening user privacy and corporate interests.

Threat Hunter's "2024 Data Breach Risk Landscape Report" conducts a multi-dimensional analysis of the domestic enterprise data asset leakage risk profile and illegal data transaction industry chain in 2024, and objectively presents a panoramic view of the domestic data leakage risk landscape in 2024.

Summary of key points in the report:

1. The risk landscape of data leakage remained severe in 2024, and many companies in multiple industries have data leakage risks.

Throughout 2024, 37,575 effective data breaches were monitored, involving 2,598 companies, covering many key industries such as finance, e-commerce, express delivery, automobiles, and local life.

2. The banking industry once again topped the list of data breach risks, and local life entered the top ten for the first time.

The number of data breaches in the banking industry reached 6,333 in 2024, ranking first for two consecutive years. Data security control in the financial industry is urgent. Data breaches in the

local life industry jumped from Top14 in 2023 to Top10. A total of more than 700 incidents were discovered in 2024. The new leakage type "forced login" is the main driver.

3. Anonymous group chats and the dark web are still the main leakage channels, and risk events in libraries and network disks have doubled.

In 2024, anonymous group chats and dark web will still be the main channels for data leakage, accounting for 90.83% of the total; the number of risk events in library and network disk channels has doubled, reaching 2,714 cases.

4. "Private domain group" and "guarantee" models are developing rapidly, and illegal data transactions are more hidden and "standardized"

In 2024, the "private domain group" and "guarantee" models have developed rapidly. A total of 4,193 data leakage risk incidents have been discovered in private domain groups, the number of threat actor groups has exceeded 500, and more than half of the "private domain groups" are operated by guarantee agencies.

5. Privileged accounts have become a weapon for attackers, and ATO risks continue to grow.

ATO risks will continue to grow in 2024, with more than 4.7 million employee accounts leaked in just one week, involving 210,000 companies in multiple industries such as social networking, e-commerce, finance, and short videos.

6. The rise of new data leakage "forced login" and "decryption", involving e-commerce, takeout, express delivery and other industries

In 2024, the "file checking" model developed rapidly, and two new data leakage methods, "decryption" and "forced login", emerged. "Qiangden" has appeared since June, first appearing on the e-commerce giant platform, and then spreading to multiple platforms such as takeout and express delivery; "Decryption" was born by threat actors to crack privacy forms. In the past year, related data leakage incidents have been on the rise.

7. Risk events related to the "iOS" field have declined, and demand for illegal data transactions related to "poverty alleviation" has increased.

A phone maker's crackdown on fraud through its built-in video calls has resulted in a decrease in risk events in the "iOS" field, with a decrease of 59.90% in the second half compared to the first half;

At the same time, the demand for illegal data transactions related to "poverty alleviation" has increased.

Disclaimer: The data information provided by Threat Hunter is estimated and analyzed based on large sample data sampling collection, small sample survey, data model prediction and other research methods. As any data source and technical method in the field of statistical analysis have limitations, Threat Hunter is no exception. The data information estimated and analyzed by Threat Hunter based on the above methods are for reference only. Threat Hunter does not make any guarantees about the accuracy, completeness, applicability and non-infringement of the above data information. Threat Hunter has nothing to do with any legal consequences caused by any action taken by any organization or individual citing or based on the above data information. Any relevant disputes or legal liabilities arising therefrom shall be borne by the perpetrators.

Overview of domestic data breach risks in 2024

1. Overview of domestic data breach risks in 2024

1.1 In 2024, 37,575 data leakage incidents were monitored, involving 2,598 companies in finance, e-commerce, express delivery and other industries.

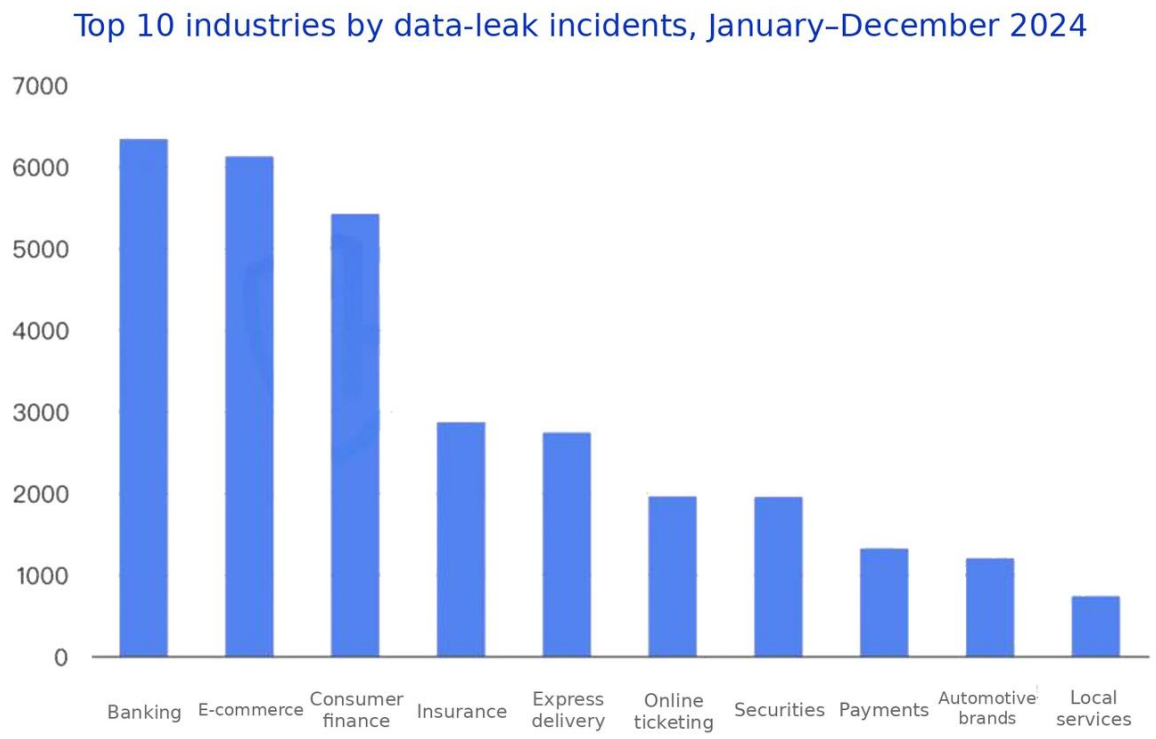
Data from the Threat Hunter data leakage risk monitoring platform shows that from January to December 2024, the entire network monitored 303 million pieces of intelligence about data leaks. Based on the Threat Hunter authenticity verification engine and DRRC professional manual analysis, a total of 37,575 effective data leakage incidents were verified, involving 2,598 companies in finance, e-commerce, express delivery and other industries.

Threat Hunter found that the number of data breaches dropped significantly in February 2024 (down 36% from January 2024, a total of 898 cases), and increased significantly in November (up 29.48% from October 2024, a total of 1,096 cases). Further analysis from the source of the data leakage revealed that the main reasons are as follows:

In February 2024, the number of data breaches caused by different reasons such as third-party leaks and SMS channel leaks all declined. It can be seen that the sharp decline in data breaches in February 2024 was mainly affected by the slowdown in transactions caused by the holiday of threat actors during the Spring Festival.

In November 2024, the activity of illegal data trading gangs increased. The number of gangs increased by 156 illegal data trading gangs compared with October. This increase led to a significant increase in the number of data leakage incidents across the network in November.

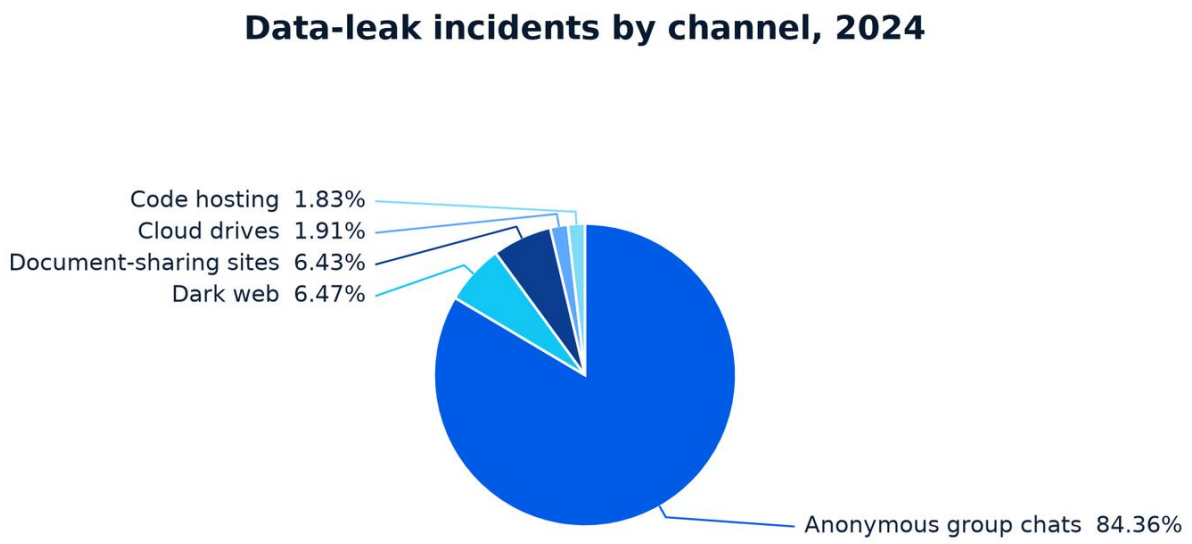
1.2 The risk of data leakage in the banking industry ranks first for two consecutive years, and local life enters the top ten for the first time



Top 10 industries by data-leak incidents in 2024: banking ranks first for the second year running

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

From the perspective of industry distribution, 88 industries were involved in data breaches from January to December 2024. The top five industries are banking, e-commerce, consumer finance, insurance and express delivery. Among them, the number of data breaches in the banking industry was as high as 6,333, making it the industry with the largest number of data breaches for two consecutive years.



Data-leak incidents by channel, 2024: anonymous group chats account for 84.36%

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

In addition, the industry ranking of data breach incidents in the local life industry this year has increased compared with 2023, rising from the previous Top14 to the Top10. Data shows that more than 700 data breaches were discovered in the local life industry in 2024, a sharp increase from 2023

7. 22 times.

Further analysis found that the reason for the sharp increase in local life data leakage is the new type of leakage "forced login".

Forced login: refers to the use of technical means to force login to a user's account and obtain the private information in the user's account.

Local life: mainly refers to service platforms that provide takeout, catering, movie tickets, grocery shopping and other services closely related to life.

Note: For further information on "Forced Login" please see Chapter 2.2.

1.3 Anonymous group chats and dark web are still the main channels for data leakage, and incidents on library and network disk channels have doubled.

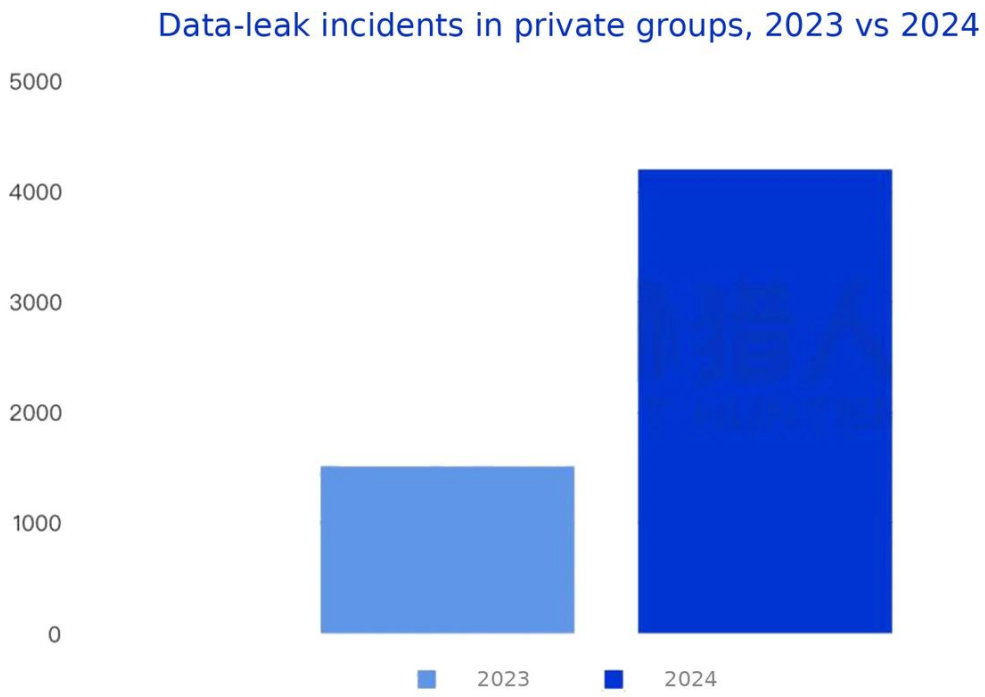
Threat Hunter statistics show that the main channels for data leakage in 2024 will still be anonymous group chats and the dark web, accounting for as high as 90.83%.

It is worth noting that in 2024, there were 2,714 risk incidents involving library and network disk leaks, accounting for 7.34% of all channel incidents, a significant increase compared to last year.

It is worth mentioning that since June 2024, the Threat Hunter data leakage risk monitoring platform has introduced large language model technology, using the intelligent screening and

massive data analysis capabilities of the large model, combined with the verification and judgment of the Threat Hunter DRRC professional team, to greatly improve the efficiency of risk file review and risk event detection capabilities from library and network disk channels.

1.4 "Private domain group" and "guarantee" models develop rapidly, and illegal data transactions become more hidden and standardized



Data-leak incidents in private groups, 2023 vs 2024

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

As the scale and complexity of illegal data transactions intensifies, more and more groups of threat actors tend to choose private domain environments for transactions, making transactions more concealed, organized, and standardized.

Threat Hunter statistics show that in 2024, a total of 4,193 data leakage risk incidents were discovered in "private groups" on an encrypted messaging app, an increase of 2.70 times compared with 2023. The number of threat actor groups in the "private group" exceeded 500, which was 2.88 times that 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.

Threat Hunter intelligence personnel further analyzed the data leakage incidents in the "private domain group" and cybercriminal groups and found:

1) The threat actors gang communicates with buyers through encrypted messages, passwords, and private chats in the "private domain group," making illegal transactions by threat actors more difficult to detect by regulatory agencies.

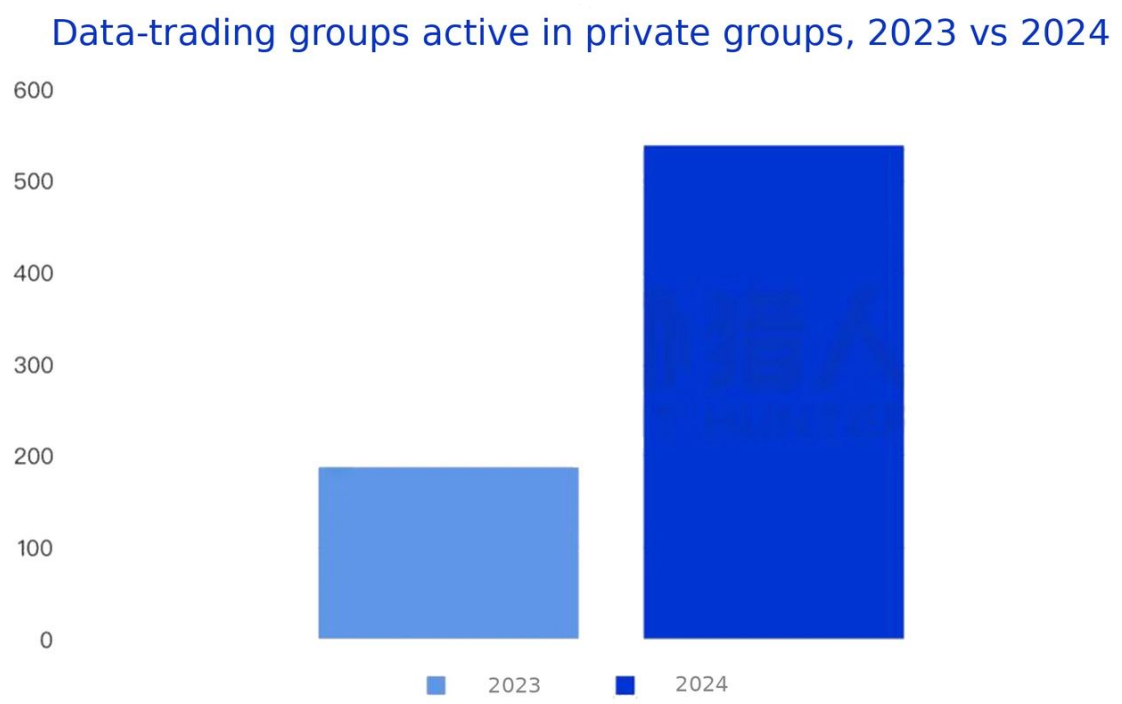
2) More than half of the “private domain groups” are operated by guarantee agencies.

Guarantee agency: plays the role of "middleman" in illegal data transactions, responsible for verifying the qualifications of both parties to the transaction, supervising the transaction process and ensuring the smooth completion of the transaction. This model improves the trust of both parties to the transaction, makes the illegal data transaction process more "standardized", and ensures the smooth progress of illegal data transactions to a certain extent.

Threat Hunter further analyzed the guarantee gangs and found that among the many guarantee gangs currently, the top three guarantee gangs are "Haowang Guarantee" (formerly Huiwang Guarantee), "Xinbi Guarantee" and "Chunjiang Guarantee". Among them, "Haowang Guarantee" occupies a dominant position among the guarantee groups, accounting for 94.34% of the illegal data transaction incidents guaranteed by it. It can be described as "the largest one".

It is worth noting that in order to avoid regulatory crackdowns, "Original Huiwang Guarantee" was officially renamed "Haowang Guarantee" on October 19, 2024.

1.5 A total of 4,034 data breaches were caused by ransomware attacks, involving manufacturing, finance, real estate and other industries



Data-trading groups active in private groups, 2023 vs 2024

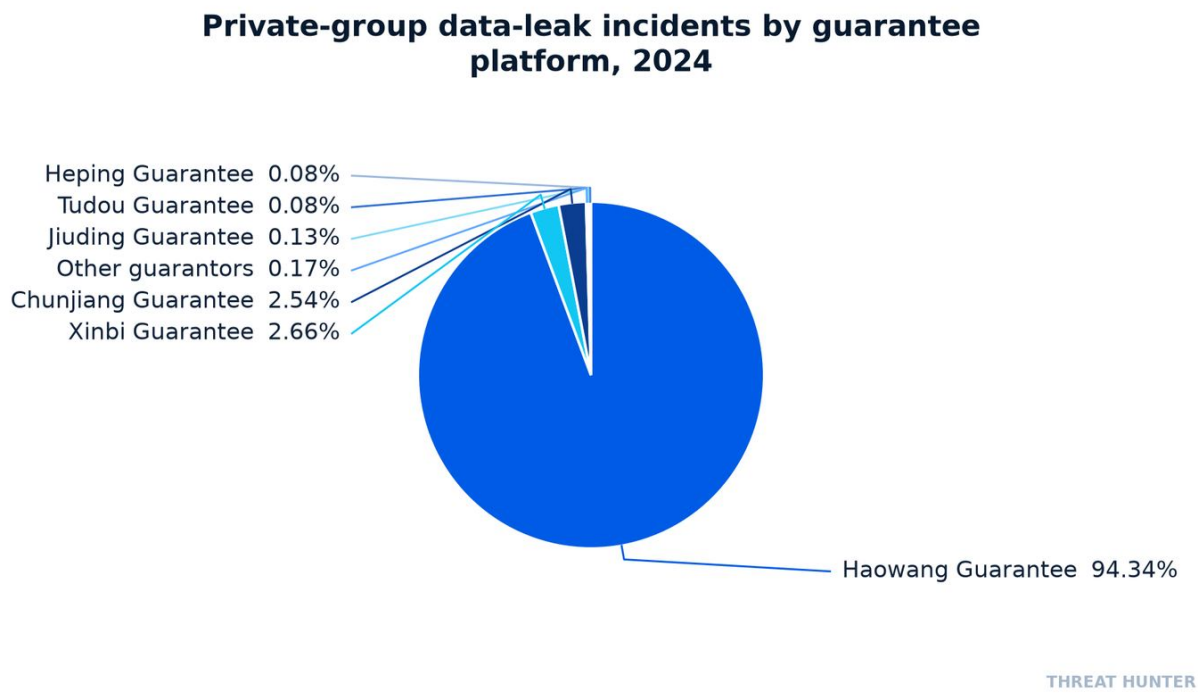
Source: Threat Hunter original report, page 11. Original figure with Chinese text replaced by English.

In 2024, Threat Hunter captured a total of 4,034 data breaches caused by ransomware attacks, involving multiple industries around the world. The top three industries were manufacturing, finance, and real estate.

1.6 Privileged accounts have become a weapon for attackers, and ATO risks continue to grow

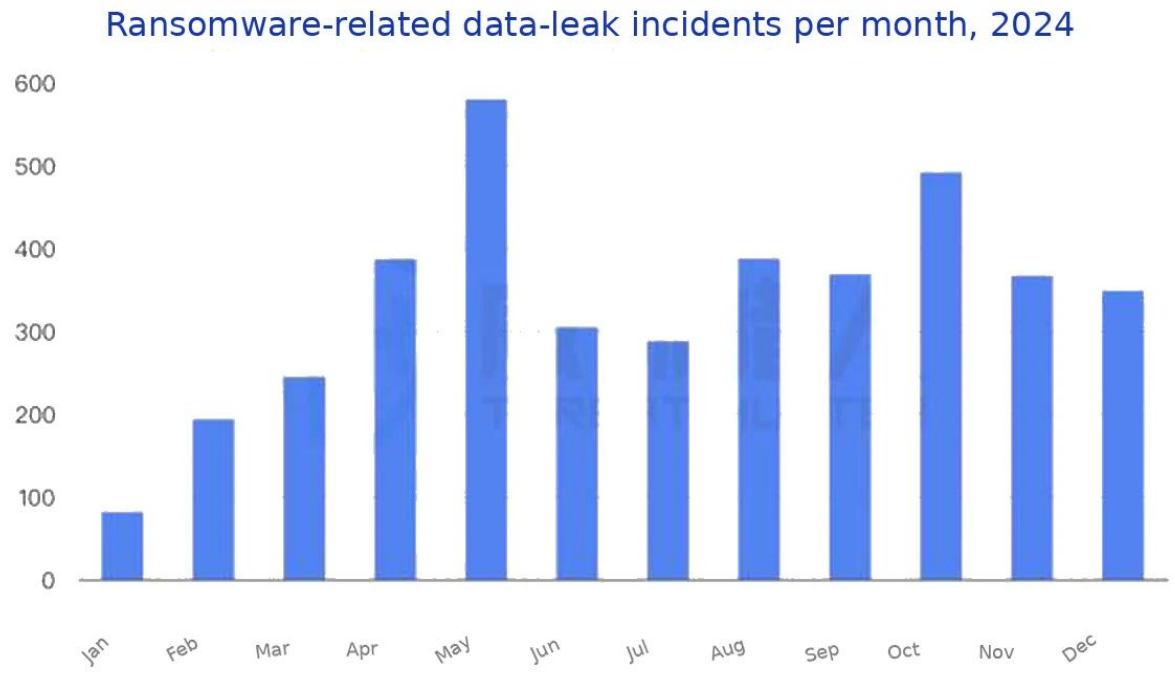
Note: In view of the particularity of privileged account leakage incidents, Threat Hunter will directly communicate with cooperative customers after capturing relevant intelligence, so such incidents are not included in the total data leakage incident statistics of this report.

Privileged Account: refers to an account with special permissions, usually with advanced access rights to the system, network or data, such as an enterprise employee account. Privileged accounts have the characteristics of high authority, scattered distribution, and large number. They are distributed in various application systems such as business systems, applications, databases, and network equipment. Once the account is taken over (Account Takeover, ATO), it may lead to the leakage of sensitive data resources, business interruption, and other consequences.



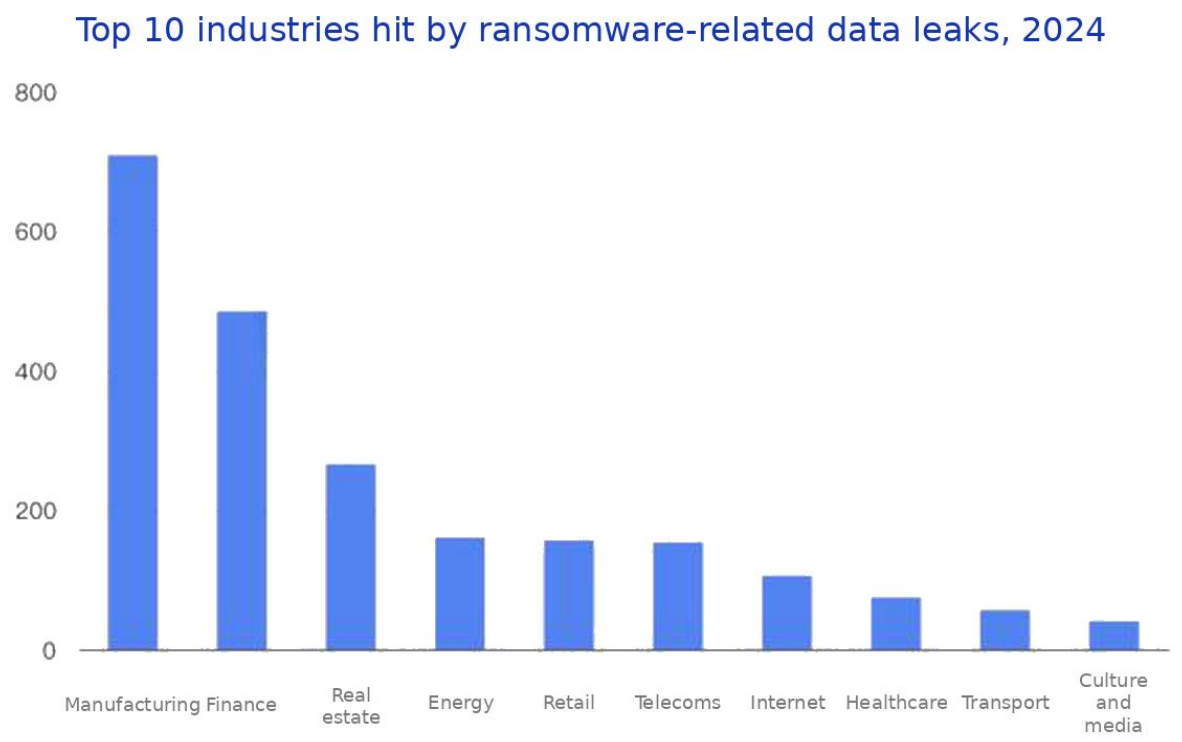
Private-group data-leak incidents by guarantee platform, 2024: Haowang Guarantee accounts for 94.34%

Source: Threat Hunter original report, page 12. Redrawn in English from the original figure.



Ransomware-related data-leak incidents per month, 2024

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



Top 10 industries hit by ransomware-related data leaks, 2024

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

For groups of threat actors, instead of penetrating layers of protection to steal data, it is better to steal accounts directly, move laterally through the intranet, exploit the lack of control methods of privileged accounts to break into authorized accounts, and finally use privileged account permissions to maliciously damage the system.

In recent years, risk incidents caused by improper control or theft of account permissions have been increasing year by year. The latest "2024 Threat Intelligence Index Report" released by IBM X-Force stated that the number of attackers using stolen credentials to access valid accounts increased by 71% compared with last year, accounting for 30% of all risk incidents that X-Force responded to in 2023, and tied with phishing as the number one infection vector.

1.6.1 Over 4.7 million employee accounts were leaked in just one week, involving 210,000 companies in social networking, e-commerce and other industries

The Threat Hunter ATO intelligence service continues to monitor the risk of corporate account leakage. In just one week, it detected that the number of leaked corporate employee accounts exceeded 4.7 million, involving nearly 210,000 companies in social networking, e-commerce, finance, short video and other industries.

Note: The statistical period of the statistical chart data is from February to December 2024.

1.6.2 Third-party office collaboration tools such as CRM and video-meeting software are high-risk areas for account leakage

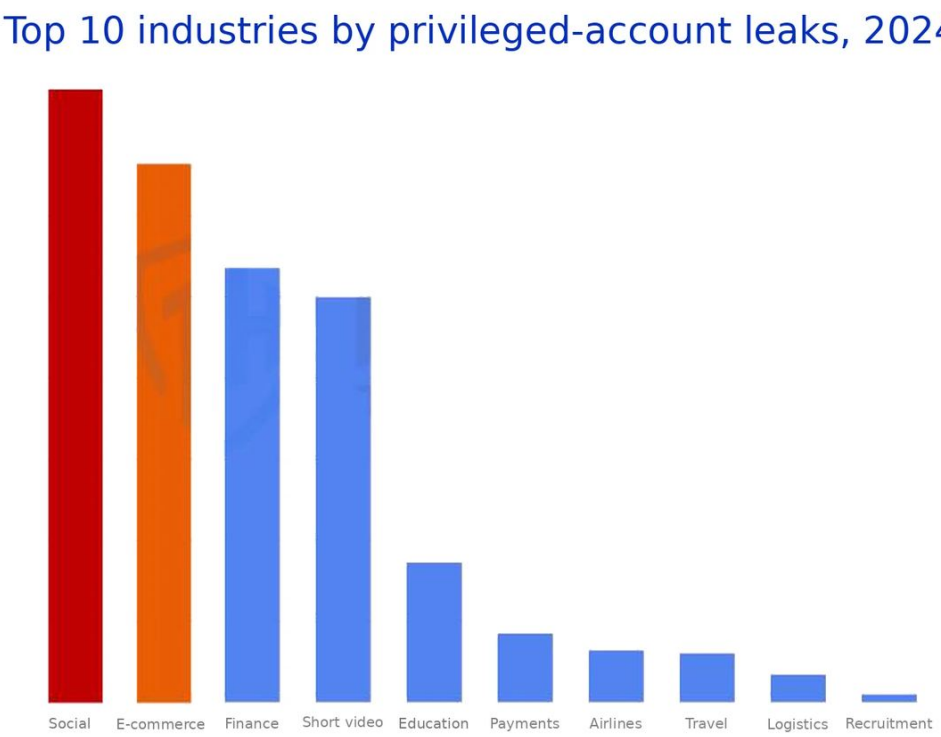
Threat Hunter intelligence personnel further analyzed the leaked corporate account information and found that the leaked accounts have a large number of external software accounts, with one customer relationship management (CRM) platform having the largest number, followed by a second CRM platform and a video-conferencing service.

There is a large amount of sensitive account data on these platforms, including but not limited to user identity information, corporate secrets, customer information, financial information, communication content, etc. Once the security defense line of these data is breached and the account is maliciously taken over, it will bring a series of serious problems to enterprises and users.

Note: The statistical period of the statistical chart data is from February to December 2024.

1.6.3 Internal systems of enterprises generally face the risk of account leakage, mainly corporate email, recruitment system, unified login system, etc.

In addition to enterprise external software account information, enterprise internal systems, such as corporate email, recruitment, unified login, document systems, etc., have experienced varying degrees of account leakage. These systems involve internal corporate communications, business processes, etc., and carry a large amount of sensitive data and key information. Once an employee's account is maliciously taken over, it is like opening a gap in the company's door, giving attackers the opportunity to snoop, steal or even tamper with these sensitive data, thereby causing losses to the company.



Top 10 industries by privileged-account leaks, 2024

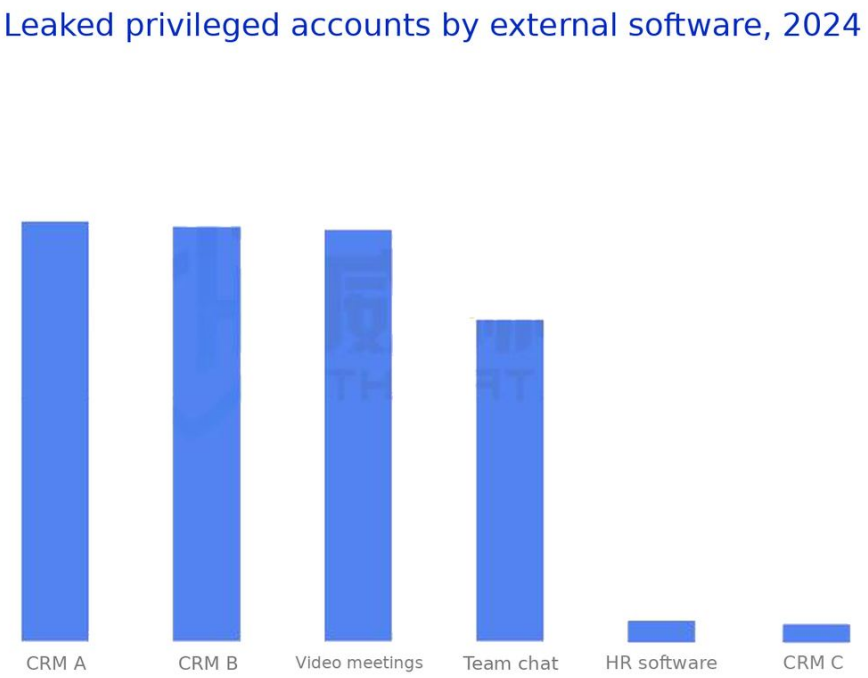
Source: Threat Hunter original report, page 14. Original figure with Chinese text replaced by English.

Note: The statistical period of the statistical chart data is from February to December 2024.

Analysis of illegal data trading industry chain in 2024

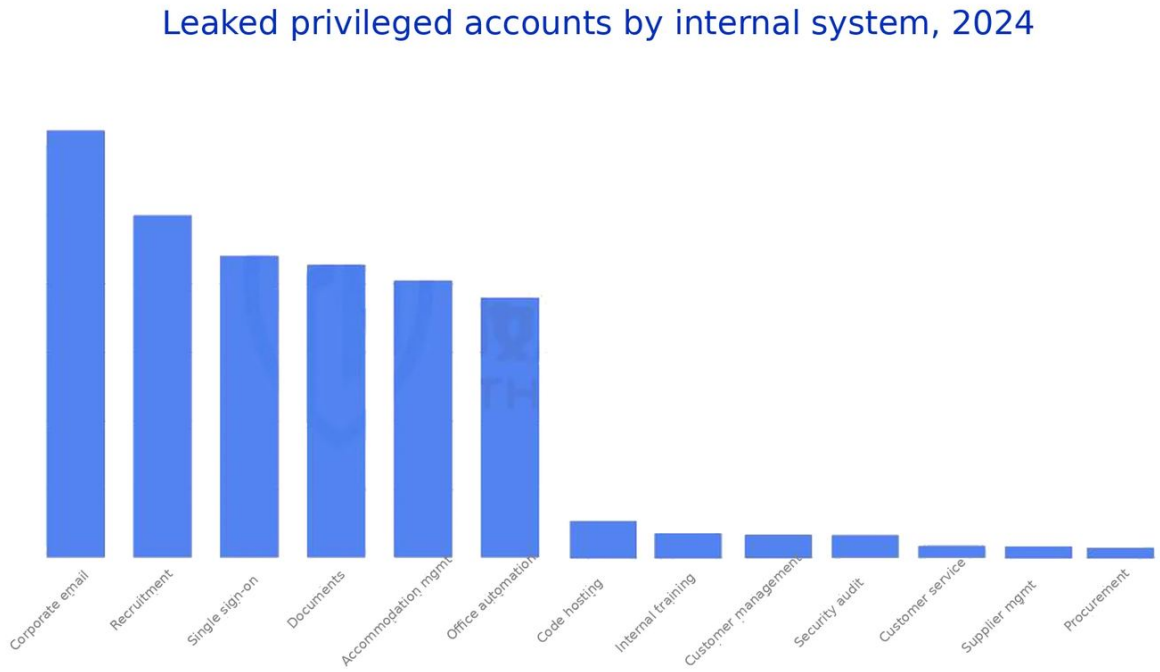
2. Analysis of illegal data trading industry chain in 2024

Since the development of the Internet fraud network, the illegal data trading industry surrounding the leakage and reselling of data assets has developed quite maturely. Based on the division of labor and positioning of different roles, the upstream, middle and downstream industries have evolved:



Leaked privileged accounts by external software, 2024: CRM platforms lead, followed by video-meeting software

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



Leaked privileged accounts by internal system, 2024

Source: Threat Hunter original report, page 15. 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 specialize in finding ways to obtain and steal data from both inside and outside companies. 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.

Midstream: Data middlemen are mostly active on the dark web, threat actors forums, encrypted messaging apps and other platforms. These people post sales data on different platforms and are responsible for classifying and cleaning the data to meet the various needs of customers.

Downstream: data buyers

Including telemarketing companies, fraud gangs, etc. People who buy data often 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. 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 research found that in 2024, there were some new changes in the illegal data trading industry chain in the upstream, midstream, and downstream:

2.1 The number of "file checking" leaks increased rapidly in 2024, involving data from e-commerce, takeout, social networking, express delivery and other industries

In recent years, Threat Hunter has been paying attention to the frequent "file checking" data leaks in the middle reaches of the illegal data trading industry chain. 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 cybercriminal groups that can provide the information files of designated persons. For example, through a phone number, the identity information related to this phone number can be queried, such as address, bank card number, assets under the name, etc. File checking services include query services, decryption services, forced login services, etc.

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), online shopping orders, express delivery business (express delivery address, logistics information), personal information (marriage, household registration, social security), etc.

Threat Hunter intelligence data shows that the trend of data leakage related to "file checking" is on the rise in 2024, with more than 3,200 risk incidents throughout the year, and the leaked information involves e-commerce shopping information, takeout delivery information, social accounts, express delivery information, bank statements, etc.

2.2 The emergence of a new type of data leakage, "Forced Login", involving leading platforms in e-commerce, takeout, express delivery and other industries

Threat Hunter discovered a new type of file check in 2024 - "forced entry". The leaked information mainly involves users' online shopping orders, takeout delivery orders, travel taxi orders, express delivery order information, etc., covering leading platforms in multiple industries such as e-commerce, express delivery, local life services (mainly the takeout industry) and travel services.

Since June 2024, methods of obtaining data through "forced login" have begun to appear, and by the end of December, there had been more than 6,600 cases. Initially, it was mainly concentrated on the leading e-commerce platform, and then gradually spread to multiple platforms such as takeout and express delivery.

Forced login: refers to the cybercrime ecosystem using a variety of complex techniques to forcefully log into the user's platform account, obtain sensitive information such as specific orders placed under the account, and then provide this information to downstream data buyers. When midstream data is sold, the sales advertisement will be marked with [forced login].

So, where did the “forced login” data come from?

Threat Hunter intelligence personnel further dug and analyzed "Qiang Deng" and found that the main modus operandi of the upstream gang against "Qiang Deng" was as follows:

1. Information acquisition: First, the attacker obtains the user’s ID number and ID number through other channels (such as file checking or social engineering database) through the phone number.

ID photos and other information.

2. Bypass verification: Then, use the obtained ID photo to generate an AI video or simulated face to bypass the platform’s video verification loop.

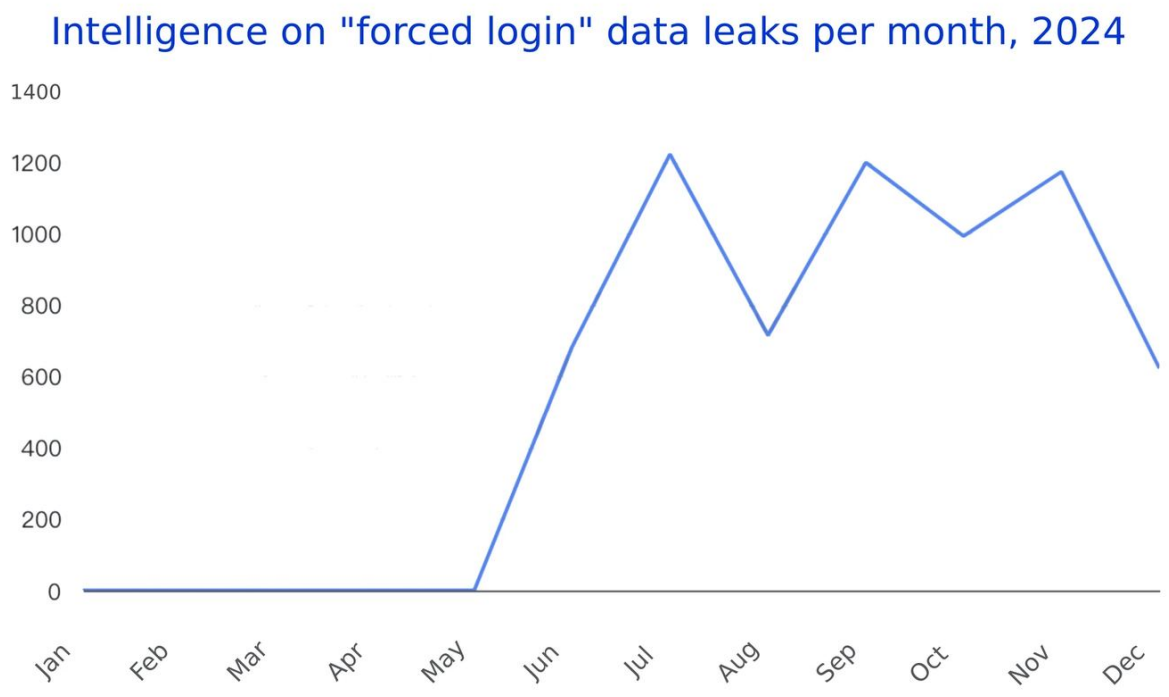
section.

3. Forced login: Finally, use the platform’s interface such as forgotten password or password retrieval to bypass the platform’s verification mechanism and force login.

The user's account number is used to obtain sensitive information such as the order content in the account.

After the upstream gangs obtain order information from e-commerce, takeout, express delivery, travel services and other industries through "forced posting", the midstream gangs then publish sales advertisements in various anonymous group chats, social media, etc. to attract more downstream demand groups.

2.3 With the rise of “decryption” services in the logistics industry, related data leakage incidents have gradually increased in the past year.



Intelligence on "forced login" data leaks per month, 2024: a new leak method on front-line e-commerce platforms

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

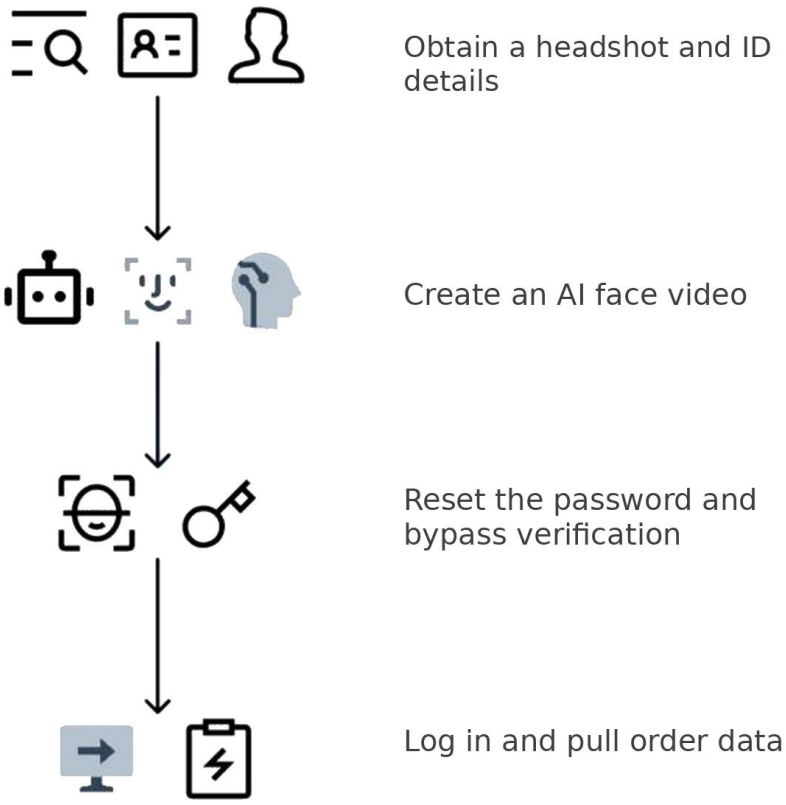
In recent years, "privacy mask" technology has been continuously developed to protect the security of personal information by hiding users' real phone numbers. In the past year, with the strengthening of supervision in the logistics industry and the joint efforts of enterprises, the promotion of privacy forms has effectively reduced the leakage of express delivery forms. Overall

The governance effect is obvious (see the picture below). But criminal tactics continue to evolve. In 2024, threat actors launched a new file checking service - "decryption" to crack the privacy form. In the past year, "decryption" related data leakage incidents have gradually increased.

Order decryption is mainly done through "express delivery number + virtual number (or phone number coded in the first three and last four)" to obtain the complete phone number.

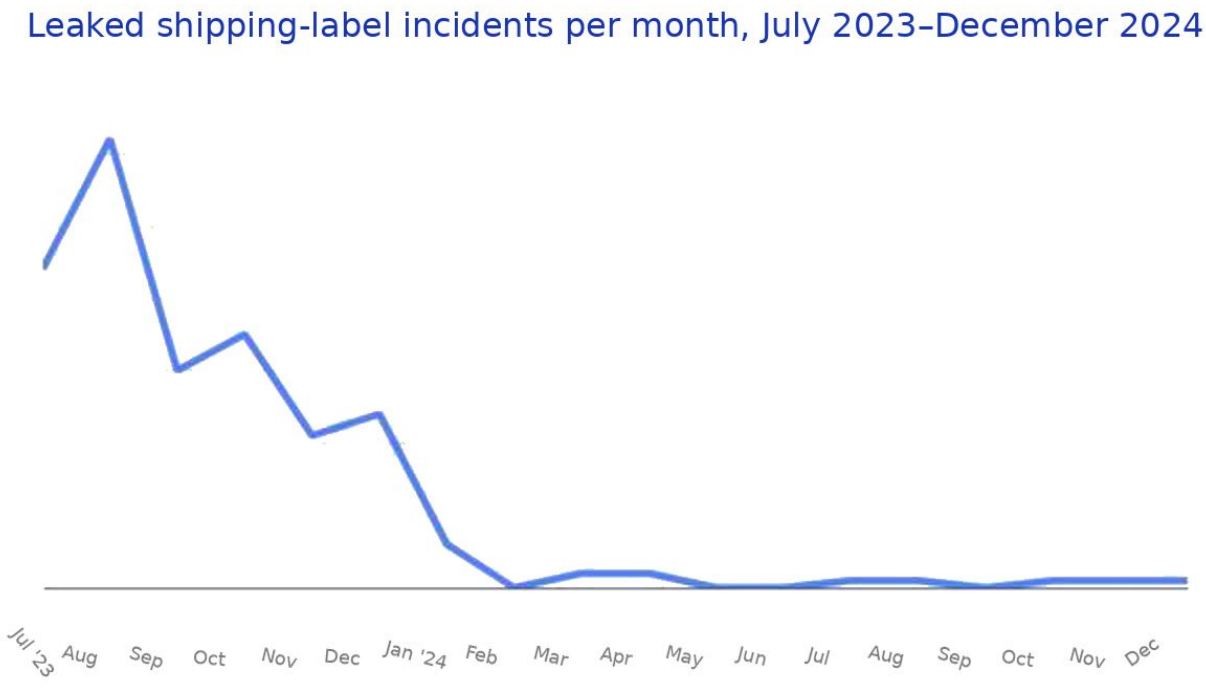
[Extended information] File checking in the logistics industry is mainly divided into query type and decryption type:

Threat Hunter noticed that the price of decryption services is much lower than the price of query services. It calculated the median price of query and service events captured every month:



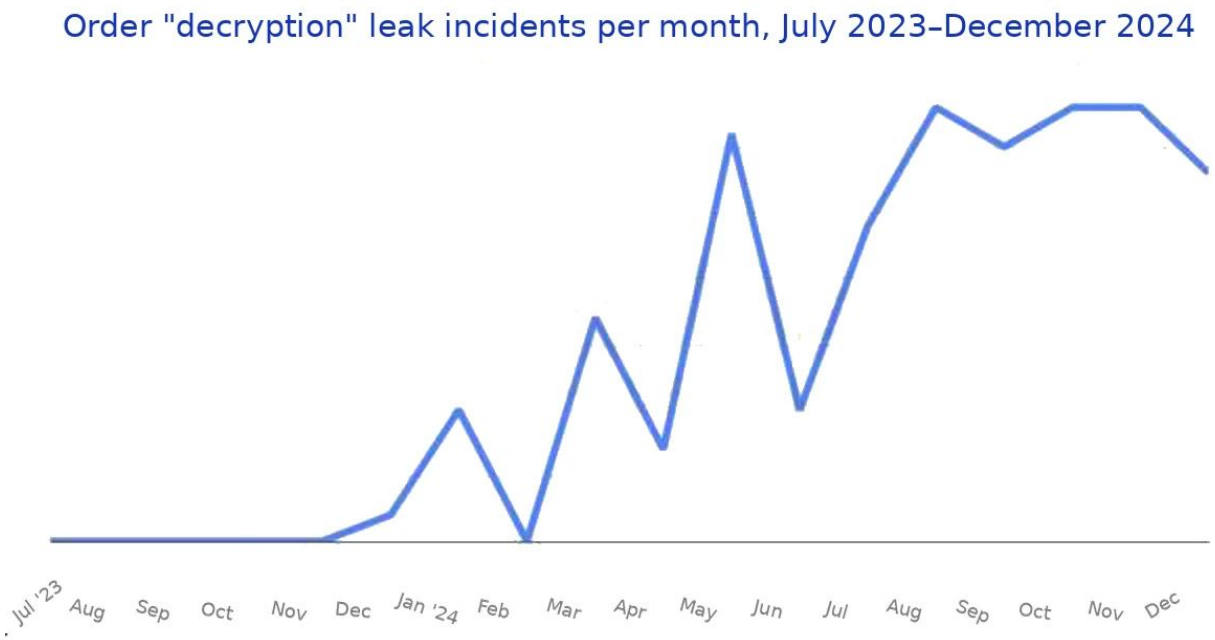
How the "forced login" method works: from a victim's ID photo to their order data

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



Leaked shipping-label incidents per month, July 2023–December 2024

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



Order "decryption" leak incidents per month, July 2023–December 2024: a steady rise as shipping labels became harder to obtain

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

1. The median price of query services is between 75 and 435 yuan, among which the price of querying information such as the delivery address through a phone number is higher.

Mainly affected by service complexity and risk.

2. The median price of decryption services is only about 4 yuan, with the highest price being 7.5 yuan and the lowest price being 2 yuan. The decryption service belongs to distributed query, mainly

For e-commerce merchants.

2.4 There is strong downstream demand for loan, online shopping, stock, recruitment and other data

From January to December 2024, Threat Hunter captured nearly a thousand pieces of precise purchasing data information from various threat-actor channels, involving loan, online shopping, stock, recruitment, express delivery and other data. Among them, the demand for user information in the loan category is the strongest, including user information in multiple subcategories such as consumer finance online loans, bank loans, corporate loans, and loan supermarkets.

Purchasing data: refers to downstream telecom fraud or marketing groups publishing their purchase demand information for specific types of data in threat-actor channels.

Threat Hunter further analyzes the purchasing data information and purchasing personnel:

From the perspective of purchase data types, it mainly includes three major categories: financial data, logistics and express data, and recruitment data. Financial data mainly targets foreign shareholders and virtual currency investors; logistics and express delivery data focuses on order information of large express delivery companies, and there is the possibility of insiders participating in reselling; recruitment and job search data mainly involves mainstream recruitment platforms, and threat actors are generally used for telemarketing and fraud.

Judging from the regions targeted by purchase data, India and Vietnam are the hardest hit areas. The data for buying in India mainly involves financial data needs such as stocks and securities; the types of data for buying in Vietnam are more diverse, including information on government officials, Vietnamese living abroad, students and other groups.

2024 Illegal Data Trading Market Research



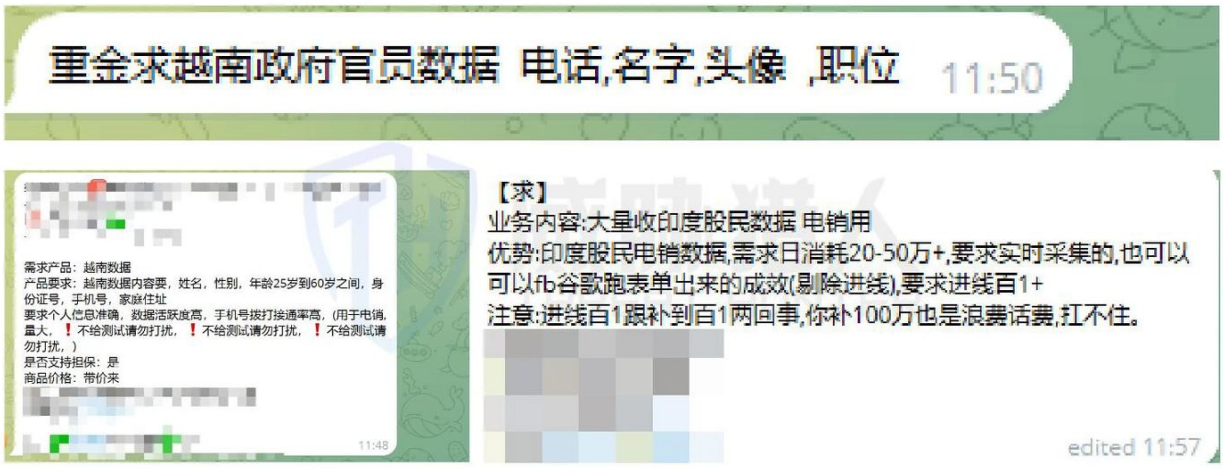
Top 5 data types threat actors sought to buy, 2024: loan data leads

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



Hot keywords in threat actors' data requests, 2024

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



Threat actors' requests to buy data: Vietnamese government staff contacts and Indian stock-investor data for telemarketing

Source: Threat Hunter original report, page 25. Original image retained.

3. Research on illegal data trading market in 2024

3.1 A total of 496 risk events related to the "iOS" field were discovered in the second half of the year, which was higher than that in the first half.

Threat Hunter research found that from the second half of 2023 to the first quarter of 2024, the "iOS" field increased in the leaked data fields. Judging from the chat records between the data trafficking threat actors group and downstream data buyers, downstream data buyers repeatedly mentioned the screening requirements for "iOS" device data in their repurchase requirements for data.

However, starting from April, the risk events related to the "iOS" field have shown a downward trend, and the number in the second half of 2024 decreased compared with the first half of the year.

Reported share: 59.90%

Threat Hunter intelligence personnel further analyzed the reasons for the decline in the second half of the year. The decline in "iOS" related data in the second half of the year was mainly due to the phone maker's introduction of measures against fraud through its built-in video calls.

In March 2024, the phone maker upgraded the iOS system to iOS 17.4.1, launching a feature that rejects incoming video calls from unfamiliar numbers, and pushed iOS 17.5 in May, which enhanced the video-call function. After testing, Threat Hunter intelligence personnel confirmed that this feature has enabled the rejection of unknown calls.

(threat actors posted the phone maker's official notice on rejecting video calls from unknown numbers in an anonymous group chat)

Threat Hunter discovered during public opinion monitoring in May that some fraud groups operating outside China, especially in northern Myanmar, were unable to continue using this method to commit fraud due to the video-call updates. It was initially determined that this was the phone maker's official crackdown on such illegal activities.



A notice posted in an anonymous group chat: the phone maker's update lets users reject video calls from unknown numbers

Source: Threat Hunter original report, page 28. Original image retained.



Fraud operators report that built-in video calls no longer get through from northern Myanmar after the update

Source: Threat Hunter original report, page 28. Original image retained.

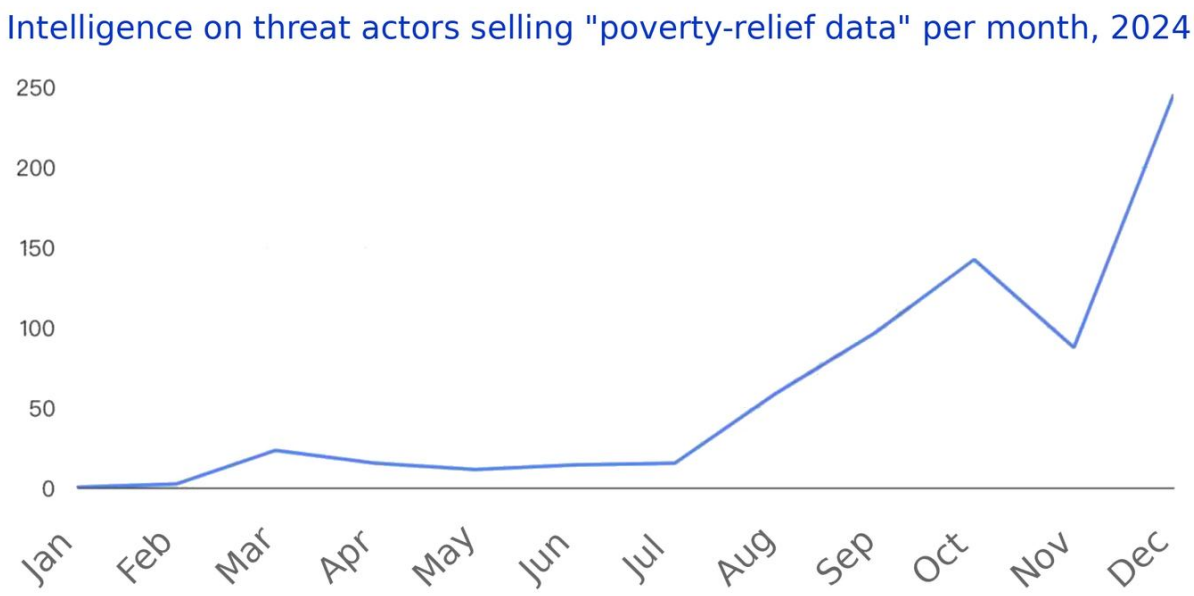
At the same time, Threat Hunter noticed that cybercriminal groups responsible for data cleaning and selling in the illegal data trading market suggested that the fraud gangs use "conventional" methods to conduct fraud (that is, using phone numbers to commit fraud) in order to cope with the video-call crackdown.

3.2 The number of “poverty alleviation” related data risk intelligence has increased significantly, and the demand for purchasing “poverty alleviation materials” has increased month by month.



A data seller advises fraud groups to switch to ordinary phone calls after the video-call crackdown

Source: Threat Hunter original report, page 29. Original image retained.



Intelligence on threat actors selling "poverty-relief data" per month, 2024

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

Intelligence data from the Threat Hunter data leakage risk monitoring platform shows that the number of illegal data transaction intelligence related to "poverty alleviation" has increased significantly in 2024, especially in the fourth quarter.

Poverty alleviation materials: Personal information or data related to poverty alleviation subsidy objects in illegal data transactions. After these data are illegally obtained by threat actors, they are usually resold to third parties for targeted fraud, money laundering and other illegal activities.

Through in-depth research on all aspects of the illegal data trading industry chain, Threat Hunter intelligence personnel found that the "poverty alleviation materials" peddled in the illegal trading market include funds from the fund app, manual poverty alleviation powder, etc.

Fund Disk app: Refers to threat actors gangs obtaining the personal information of “investors” by collecting data on fund disks related to some “investment projects”. These investors generally have bank cards and sell them to downstream groups to conduct fraudulent card score runs.

Human-operated promotion-abuse accounts: refers to groups of threat actors manually collecting personal information of poverty alleviation targets on a large scale through social media and other channels.

Data cleaning gangs and trafficking gangs will screen the above data by age, region, activity, etc., and then sell it to downstream gangs for precise fraud, score-based money laundering, and recruitment as "debtors" to commit loan fraud, etc.

Case: In October 2024, Threat Hunter captured a data leakage incident related to an "instant-messaging poverty alleviation sample". The leaked sample fields included contact information (phone number, instant-messaging account number), personal identity information (name, gender, age), detailed address (specific to

Street and address), economic information (annual income 45,000 yuan), behavioral attributes (online device status), and labels such as "high activity".

It is worth noting that in addition to midstream gangs selling "poverty alleviation materials" in the trading market, in the second half of 2024, there was a significant increase in information on downstream gangs purchasing "poverty alleviation materials", increasing month by month, and the proportion was higher than the information on selling "poverty alleviation materials".

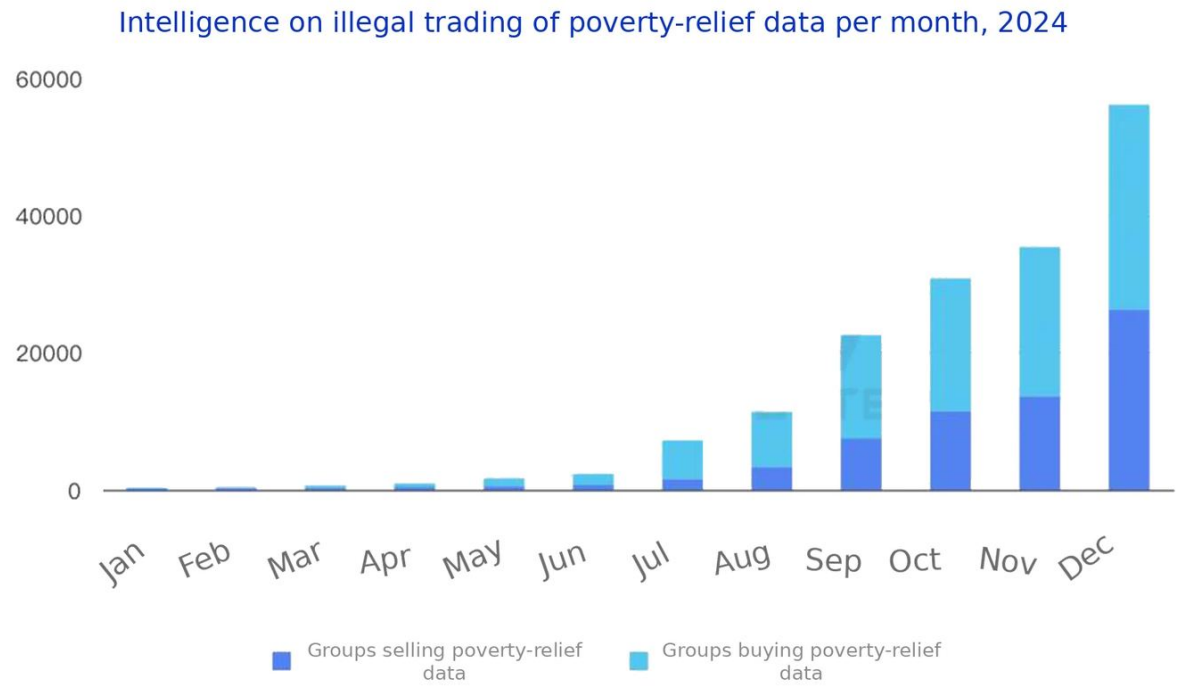


A threat actor sells data on members of fraudulent investment schemes, with a sample of leaked records

Source: Threat Hunter original report, page 30. Original image retained.

As downstream demand continues to grow, upstream and midstream groups are bound to do their best to obtain more "poverty alleviation material" data in order to meet this demand. This may lead to a large amount of personal information related to "poverty alleviation" flowing into the illegal trading market. This phenomenon deserves great attention from relevant institutions and platforms.

3.3 Hidden risks behind the bull market: Investment-related data breach risk trends rose significantly in 2024



Intelligence on illegal trading of poverty-relief data per month, 2024: buyers outnumber sellers in the second half

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

3.3.1 Shareholder data leakage and fraud attacks

During the bull market, stock market activities are frequent, investor participation increases, and investor data risk exposure also increases. Once the security protection of investment platforms or financial services websites is insufficient, the risk of investor data leakage may also increase with the activity of the stock market.

Data from the Threat Hunter data leakage risk monitoring platform shows that as the market heats up, the amount of risk intelligence about investor data in the illegal data trading market has increased significantly, especially during the peak of the bull market in the second half of the year and the end of the year.

Threat Hunter further analyzed the intelligence data and found that the main investor data involved in the illegal data trading market include investment advisory data, stock diagnosis data, securities data and capital allocation data, with the price of each piece of data ranging from 0.6 to 0.8 yuan.

Stockholder data leakage and fraud attack process:

Partial explanation of the fraud attack process:

1. Fraudulent gangs illegally obtain a large amount of personal data and financial information of shareholders through cybercrime ecosystem channels, including names, contact information, investment information, etc.

investment habits, etc., and at the same time forge investment and financial management websites or apps;

2. The fraud gang adds victims and induces them to visit fake websites or apps;

3. Once investors are deceived and visit a fake website or app, they are tricked into providing personal account information;

4. The fraud gang uses the personal account information provided by the victim to log in to the real financial management platform and steal the victim's funds.

3.3.2 Cryptocurrency investment data leakage and fraud attacks

Similarly, the new bull market for virtual currencies in the second half of 2024 seems to have also brought about an increase in risk intelligence related to cryptocurrency. Judging from the advertisements released by threat actors, this wave of popularity is mainly due to the fact that well-known cryptocurrency exchanges have suffered credential stuffing attacks.

Cryptocurrency data leakage and fraud attack process:

Partial explanation of the fraud attack process:

1. The fraud gang forges a virtual currency investment platform for subsequent use by fraud victims (investors);



A threat actor sells cryptocurrency investor data

Source: Threat Hunter original report, page 34. Original image retained.

2. The fraud gang establishes contact with the victims through social media and guides them to register and use the virtual currency investment platform.

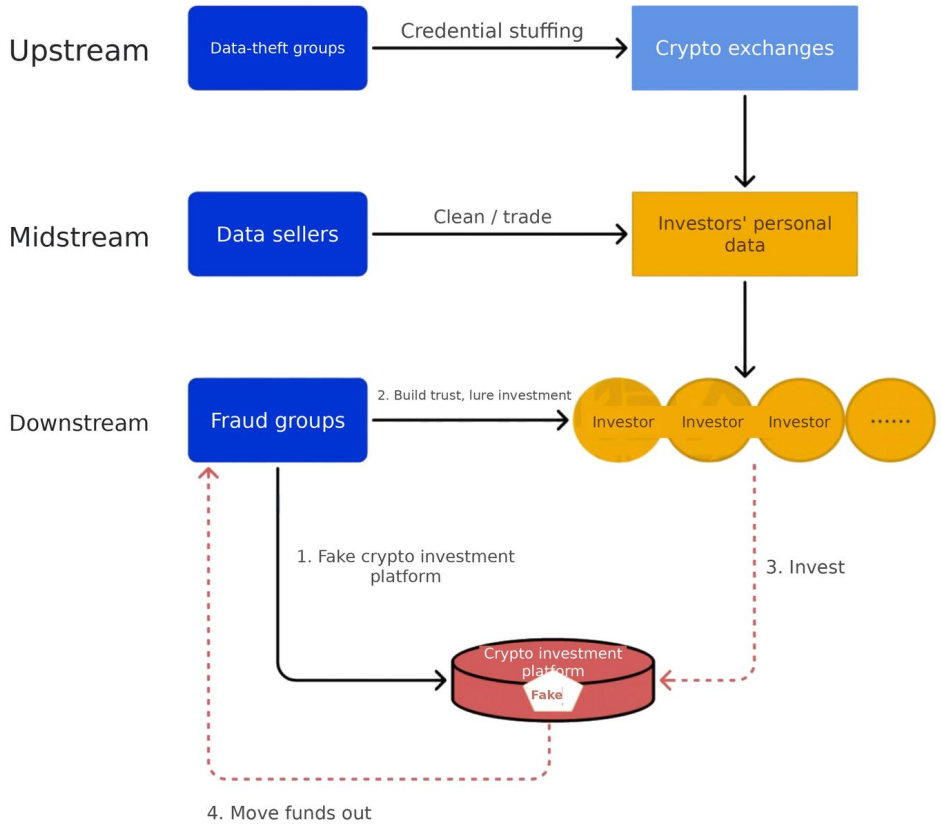
Scammers will also play roles such as "big brother in the currency circle" to further gain the victim's trust;

3. The victim invests money into the platform faked by the fraud gang. In the process, the fraud gang will manipulate the user's investment results on the platform's backend.

For example, by attracting them to continue investing by offering small returns, in fact the funds have been transferred away by the fraud gang;

4. Once the victim realizes that he has been deceived, the scammer will immediately cut off all contact information, such as blocking the victim, making it impossible to recover losses.

Threat Hunter data breach risk intelligence service



How crypto investor data leaks feed investment fraud: from credential stuffing to fake investment platforms

Source: Threat Hunter original report, page 35. Original figure with Chinese text replaced by English.

4. Threat Hunter data leakage risk intelligence service

To sum up, the risk of data leakage showed an unprecedented serious situation in 2024, involving many industries and a large number of enterprises, posing a huge threat to user privacy and corporate interests. Faced with such a severe situation, enterprises need to comprehensively improve their ability to identify and respond to risks, understand the details of risk events, including verifying the authenticity of risks, promptly trace the source, handle removal and follow up on potential risks, and enhance the timeliness of data leakage risk monitoring and early warning, etc.

In this regard, Threat Hunter provides targeted solutions:

Threat Hunter data leakage risk monitoring service, through real-time monitoring and in-depth mining of multi-channel intelligence across the entire network, and based on the risk authenticity verification engine and manual data verification, provides 7x24-hour real-time warning of data leakage risks, and links emergency response mechanisms to minimize harm and losses.

1. Network-wide intelligence monitoring and mining: covering dark web, anonymous group chat, network disk library, code hosting platform and other channels, from different dimensions

Continue to improve the comprehensiveness of channel coverage, including the continuous discovery and update of new channels, special mining of deep intelligence sources (Deep Source), and multi-lingual channel coverage.

2. Accurate early warning of data leakage risks: Based on the monitored transaction data of threat actors, the risk authenticity verification engine + manual data verification

Certification services provide comprehensive credibility assessment results to help 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: Establish a DRRC risk emergency response center to monitor enterprise-related risk information around the clock,

Audit and early warning, providing "7×24" sample acquisition, intelligence mining, assistance in traceability, processing and removal services, etc., while also providing monthly data leakage risk monitoring reports and typical risk event analysis results.

Explanation of terms related to data leakage

5. Explanation of terms related to data leakage

DRRC: Digital Risk Emergency Response Center. Threat Hunter has established two DRRCs in Shenzhen and Chongqing, bringing together 30+ security operation experts to provide 7×24-hour emergency response services to enterprises.

Authenticity verification engine: Through the extraction and comparison of personal elements of different file types, as well as the extraction and verification of elements in the image OCR results, it can effectively identify whether the image content contains forged data/historical leaked data.

Data leakage intelligence: Threat Hunter captures intelligence information about "sensitive information of unauthorized individuals or organizations being publicly traded or used" through TG groups, dark web and other channels, including data sales advertisements, data purchase information, unverified false information/historical data/duplicate data, etc., which are often of huge magnitude.

Data leakage incidents: Threat Hunter security research experts analyze and verify samples of data leakage intelligence, eliminate historical and false incidents, and confirm real and effective data leakage incidents.

Historical data events: threat actors integrate leaked real information and reuse it for transactions. Usually threat actors will refine the data and supplement the integrity of the data fields, thereby increasing the value of the data and profit margins.

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

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.

Guarantee agency: plays the role of "middleman" in illegal data transactions, responsible for verifying the qualifications of both parties to the transaction, supervising the transaction process and ensuring the smooth completion of the transaction. This model improves the trust of both parties to the transaction, makes the illegal data transaction process more "standardized", and ensures the smooth progress of illegal data transactions to a certain extent.

File checking: refers to cybercriminal groups that can provide the information files of designated persons. For example, through a phone number, the identity information related to this phone number can be queried, such as address, bank card number, assets under the name, etc. File checking services include query services, decryption services, forced login services, etc.

Forced login: refers to the use of technical means to force login to a user's account and obtain the private information in the user's account.

Privileged Account: refers to an account with special permissions, usually with advanced access rights to the system, network or data, such as an enterprise employee account.

Purchasing data: refers to downstream telecom fraud or marketing groups publishing their purchase demand information for specific types of data in threat-actor channels.

Poverty alleviation materials: Personal information or data related to poverty alleviation subsidy objects in illegal data transactions. After these data are illegally obtained by threat actors, they are usually resold to third parties for targeted fraud, money laundering and other illegal activities.

Fund plate app data collection: refers to threat actors gangs obtaining the personal information of "investors" through data collection of fund plates related to some "investment projects". These investors generally have bank cards and sell them to downstream gangs to conduct fraudulent card score runs.

Human-operated promotion-abuse accounts: refers to groups of threat actors manually collecting personal information of poverty alleviation targets on a large scale through social media and other channels.

Company official website: www.threathunter.cn Cooperation email: Marketing@threathunter.cn