THREAT HUNTER RESEARCH

Q1 2023 Data Asset Exposure Report

A first-quarter assessment of data-asset exposure, with particular attention to financial-sector risk and protection priorities.

Original publication: 2023-04-14
Research team: Threat Hunter Research Team
Source report: 25 pages

Original report text

This text version is reconstructed based on the 25-page original PDF, retaining the report narrative, chapters and research scope; the cover, duplicate table of contents and purely decorative pages are not repeated. Localized figures are placed in context throughout this web edition, with the original PDF retained for reference.

Preface

Nearly 1,000 data breaches occurred in Q1 of 2023, involving 1,204 companies and 38 industries. The data transactions of threat actors are mainly concentrated on more hidden and convenient anonymous social platforms. It is worth mentioning that leaks through SMS channels, although the proportion is not high, have a great impact. Only one incident involved more than 1,000 companies.

In recent years, laws and regulations related to national data security and personal information protection have been promulgated and gradually refined. In the 2022 national-level offensive and defensive drills, new attack and defense points for data leakage have been added, indicating that data security protection has gradually moved from regulatory implementation to specific offensive and defensive practices.

The "State Council Government Work Report" in March this year once again emphasized the importance of data security. For enterprises, data leakage will not only be subject to regulatory and legal penalties, but may also suffer property and reputation losses.

Q1 Users of financial companies have experienced an increase in phishing and counterfeit telecommunications fraud cases. One of the important reasons is that fraudsters carry out precise fraud through phishing and counterfeit websites based on leaked user information data. Therefore, timely monitoring of data leakage risks and good data security construction are important issues on the road to enterprise development.

Threat Hunter has released the "2023 Q1 Data Asset Leakage Analysis Report". The report contains detailed situation analysis, noteworthy cases and attack and defense suggestions. It is hoped that this report will provide inspiration and suggestions for enterprise data security construction and data leakage prevention.

Data breach risk profile

1. Overview of data leakage risks in Q1 2023

1. Captured nearly 1,000 data breaches involving 1,204 companies

In Q1 of 2023, the Threat Hunter intelligence platform monitored and verified 987 effective data breaches. After the epidemic, threat actors became more active. Compared with Q1 of 2022, the number of data breaches in this quarter increased by 42%, involving as many as 1,204 companies. January is the Spring Festival period, and the vast majority of threat actors are on vacation, so the number of incidents is relatively small. By February and March, threat actors gradually "come on duty", and the number of risk incidents is also increasing month by month.

Threat Hunter further researched the incident publishers and found that two threat actors published 244 data leakage incidents in Q1. Judging from the past release information, they mainly

targeted the logistics industry and speculated that they should cooperate with couriers from many express delivery companies across the country.

2. The anonymous social software Telegram is the main data trading platform, mostly for second-hand resale data.

According to Threat Hunter monitoring channels, data leakage channels in Q1 of 2023 are mainly concentrated in four channels: Telegram, Github, darknet, and network disk. Among them, the anonymous social software Telegram has become an ideal platform for data trading and dissemination of illegal information due to the privacy and convenience of information transmission, accounting for as high as 82%. According to Threat Hunter, people with first-hand data will find agents to promote and trade data to protect their own safety, so most of the disseminated data is second-hand resale data.

3. Data leaks occur in all walks of life, including logistics, finance, e-commerce, etc.

From the perspective of industry distribution, data breaches in Q1 of 2023 spread across all walks of life, involving 38 industries, including logistics, finance, e-commerce, aviation, recruitment, education, tourism and other industries.

4. Artificial photography and leakage by partners are the main reasons for leakage, involving sales, express delivery, etc.

Judging from the causes of leaks, human-photographed information accounted for the largest proportion of data leaks this quarter, up to 42%. Further research found that it was mainly concentrated in the logistics industry, involving the leakage of bill information in sales, warehousing, express delivery and other links; leaks from partners ranked second, accounting for 34%. Attackers often attack small and medium-sized enterprises in the supply chain. Such enterprises have low or no security cost investment and are easy to be breached. It is difficult to guarantee the data security of the companies they cooperate with.

What deserves attention is the leakage of internal security flaws and the leakage of text messages. Although the proportions are not high, 10% and 7% respectively, the scope of impact is large, especially the leakage of text messages. Threat Hunter captured a text message leak incident on March 15, 2023: 1,000+ companies were involved, and the number of leaked text messages from one company was as high as 100 million+, which were sold by threat actors on Telegram.

Safety advice:

1) Purchase formal SMS channels;

2) Add differentiated identification to the text messages of different channels. When a data leakage occurs, the problematic text message channel can be quickly located.

Insights into data leakage risks in the financial lending industry

2. Insights into data leakage risks in the financial lending industry

Threat Hunter's 2022 Data Asset Breach Report shows that the number of data breaches in the lending industry accounts for 38% of the total number of data breaches in the financial industry, ranking first. By Q1 of 2023, this value has soared to 51%, and the Threat Hunter intelligence platform has monitored a total of 91 related incidents, far more than other financial sub-sectors.

Threat Hunter researchers further analyzed the reasons and found that the financial lending industry has the largest proportion of leaks through third-party software services (such as SDK) and SMS channels. The data leaked through these two reasons basically only have phone numbers, and it is difficult to obtain detailed information such as names. However, intentional threat actors can query specific user information such as names, addresses, ID cards, etc. through social engineering libraries, historical leak information, and other channels. In addition, the real-time nature of the leaked data is relatively high, and there is a huge market in the field of threat actors.

Regarding the data leaked in the financial lending industry, threat actors are mostly used for fraud:

With temptations such as low interest rates and quick disbursement, users are guided to borrow money from other platforms, and fraud is committed by "freezing the loan on the grounds that the personal information is entered incorrectly, and a deposit must be paid before it can be unfrozen"; or pretending to be platform customer service, using "account violation, cancellation, etc. excuses" to require users to pay fees to commit fraud. The more personal information data threat actors obtain about users, the higher the likelihood that users will be convinced that it is customer service, and the higher the success rate of committing fraud.

Recently, the Threat Hunter intelligence platform captured a security incident on Telegram in which threat actors sold user information of an online lending platform. There are 1-2,000 messages per day. The fields involved include names, phone numbers, payment time and amounts, etc., which are very likely to be used by threat actors for fraud.

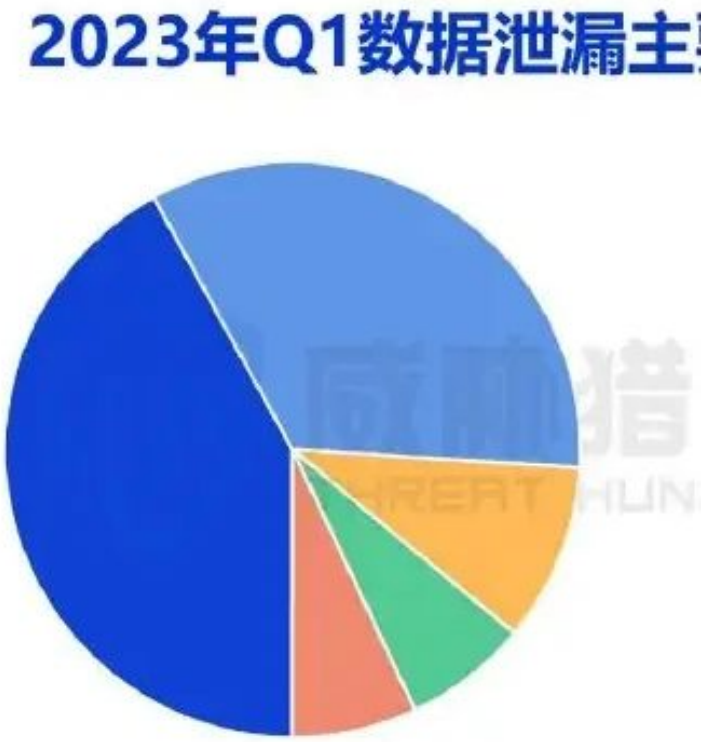
After an internal investigation of the online lending platform, the cause of the data leak was determined to be an unauthorized vulnerability in the Spring Boot Actuator. The API leaked the connection information of the database. The database also supports public network connections, and hackers can steal data by directly connecting to the database.

I. 2023 Q1 Data leakage risk profile

Source: Threat Hunter original report, page 7

Enterprises need to monitor application status. Spring Boot has built-in monitoring function Actuator. When Spring Boot Actuator is not configured properly, attackers can easily obtain sensitive information of the application by accessing the default built-in API:

- In versions below Actuator 1.5.x, all APIs are directly accessible without authorization by default, which poses huge security risks;



I. 2023 Q1 Data leakage risk profile

Source: Threat Hunter original report, page 8

- In versions 1.5.x and above, only /health and /info, two APIs that usually do not leak sensitive information, can be accessed by default. However, if the configuration is improper and APIs such as /env and /heapdump are configured to be accessible without authorization, it may also cause security risks.

Safety advice:

1) Try to use the latest versions of applications and systems;

2) Sensitive applications and systems such as databases are not exposed to the public network, or IP whitelists are restricted.

Data leakage case

3. Data breach cases worthy of attention in Q1 2023

1. Employee information leakage case

- The computers of employees of the big data platform were attacked by the Stealer log virus Trojan, causing data leakage. On March 1, 2023, Threat Hunter discovered that threat actors were selling data on a certain big data platform on the dark web, including 50W+ pieces of data in Json format involving names, phone numbers, departments and other fields. Based on the analysis of information released by threat actors in the past, Threat Hunter intelligence researchers found that most of the data is obtained from databases, covering a wide range of countries and industries, and is most likely obtained through weak passwords or unauthorized methods in databases such as MongoDB and MySQL.

After analysis and source tracing by Threat Hunter intelligence experts, it was found that the data leakage incident was caused by the Stealer log. Stealer log refers to: a log file that records sensitive information stolen from a computer by viruses and Trojans. The files contain private data such as account passwords and cookies for various software/browser saves/enterprise backend systems/FTP/databases, etc., which can lead to security incidents such as leakage of corporate secrets and customer information.

The cause was that a virus Trojan had entered the employee's personal computer, and the PostgreSQL database connected to the company was recorded in the Stealer log. Since the database can be accessed from the public network, threat actors can directly connect to the database to steal it. Below, threat actors show the PostgreSQL database connection information they stole. At the same time, threat actors said they also cracked the hashes of 9 other users in the database. Simply changing the leaked account password cannot solve the problem.

The threat actors started acting in 2019, and employees' personal computers were attacked by virus Trojans in 2021. It was not until the threat actors sold relevant data in 2023 that the problem was exposed, which ultimately led to the data leakage.

Safety advice:

1) Change the database connection address, set up an IP whitelist, restrict accessible IPs, or put the database on the intranet so that it is not exposed to the public network;

Reasons for data leakage in the financial and borrowing sector

Source: Threat Hunter original report, page 10

2) The user hash has been cracked, change the password as soon as possible to prevent password spray attacks;

3) Require internal employees to change their passwords regularly.

- The bidding platform API returned too much sensitive employee information and was attacked by threat actors. The Threat Hunter intelligence system detected that the API interface of a bidding platform was being attacked by threat actors because the interface returned too much sensitive information. threat actors can directly attack the API to obtain the clear text names, ID cards, phone numbers, addresses, passwords and other information of the company's employees. Although the leaked passwords are md5 encrypted, the clear text passwords can still be restored.

II. DISTRIBUTION OF RISK IN THE FINANCE AND LABORING SECTOR

Source: Threat Hunter original report, page 11

At the same time, the company's OA system is exposed to the public network, and threat actors can even directly log in to the OA system through the account and password leaked through the interface, steal internal information of the company, or perform other malicious acts.

Safety advice:

1) Confirm whether the fields returned by the API interface will be used in the business logic, and delete the returned redundant fields;

2) Inform employees to change their passwords and check whether the internal system has been invaded.

2. User information leakage cases

- There is an API override vulnerability in the gym, and members’ phone numbers are crawled. Threat Hunter researchers have observed that there is an override vulnerability in the API of a fitness platform. Uploading user_id will return the corresponding user’s phone number. The user_id seems to be non-traversable, unpredictable, and difficult to exploit.

Threat Hunter researchers observed that another API interface of the gym returned 100 user_ids, as shown in the following figure:

Through analysis, it was found that the ciphertext user_id is preceded by B_BBKOs, and the plaintext userid is preceded by 155. This shows that the user_id is generated according to rules. threat actors can generate the ciphertext user_id by themselves, achieving unauthorized access to any user's phone number.

Safety advice:

1) The API interface needs to be authenticated so that members can enter the system to operate, reducing exposure;

2) When querying sensitive data, if the query parameter contains a field of id type, use a string that cannot be traversed or predicted;

3) Verify whether the object of querying sensitive data is the current user. If not, the query will not be performed.

- There are vulnerabilities in the insurance agency supplier, and the data of the cooperating party A has been leaked. Recently, Threat Hunter discovered when analyzing the honeypot traffic

that many insurance agency companies have API vulnerabilities, which is very likely to leak the user data of the cooperating party A.

Take insurance agency A as an example:

In order to promote the insurance business to Party A, insurance agency A launched activities such as “Complete personal information and receive insurance”. Although the page displays desensitized personal user information, Threat Hunter analysis found that the insurance agency only displayed it on the front end.

Desensitization is done when displaying, and the API interface returns plain text data. Moreover, this vulnerability has been exploited by threat actors, and it is expected that up to 30 million+ user data will be leaked.

The defective API obtains personal sensitive information by passing in encryptStr, which is obtained through another defective API interface. threat actors can obtain the encryptStr of different users by traversing the parameters in the URL, and then request the above interface to obtain the personal information of different users.

Safety advice:

1) When transmitting sensitive data with partners, the data must be encrypted, data export permissions must be increased, to avoid exposure during the transmission process, and internal reviews must be conducted;

2) Require partners to require protection, encryption, desensitization, etc. in accordance with personal protection laws. At the same time, they must understand the specific data transmission process to avoid data leakage to other platforms or platforms with weak protection;

3) Capture the real-time dynamics of the data trading market in a timely manner, analyze the leakage incidents involving the company based on relevant clues, and determine the leakage link.

Whether the object of the data is the current user, if not, it will not be queried.

- Express waybill information leaked, threat actors sold it for 0.9 yuan a piece. Threat Hunter detected that there are threat actors on Telegram selling the waybill information data of a certain express delivery. The fields include the waybill number, product type, recipient address, phone number, name, delivery person's name, etc. 50,000+ pieces of data can be provided in a day, and the price is 0.9 yuan a piece.

After obtaining authorization from the express delivery platform, Threat Hunter launched an investigation. Through watermarked screenshots of the backend disclosed by threat actors, it was determined that the data leakage was caused by the failure of the resigned employee's account permissions to be recovered in time. At present, the express delivery platform has withdrawn the permissions of resigned employees and reported it to the police. The threat actors who stole the data have been arrested and imprisoned.

Safety advice:

1) Recover the accounts and permissions of resigned employees in a timely manner;

2) The backend system is not open to public network access and requires VPN to access, or restricts IP whitelisting;

3) Limit access to sensitive data to only a few accounts that really need it.

3. Code information leakage cases

- An enterprise’s code was leaked on Github due to an employee’s

Recently, Twitter's code leak on Github triggered heated discussions across the Internet. In addition, Threat Hunter intelligence also monitored a Github leak incident. After tracing the source, it was found that the log file uploaded by an employee to Github contained SQL statements that inserted into the user table, thus leaking the administrator account password. After obtaining the account password, threat actors directly logged into the management backend, which ultimately led to serious consequences such as data leakage and even system permission failure.

Safety advice:

For information leaks caused by employee errors in pushing code to GitHub, Threat Hunter security experts recommend:

1) Remove the code immediately: Remove the code from GitHub immediately to stop the impact of information leakage as soon as possible;

2) Analyze the degree of leakage: Assess the degree and scope of information leakage, including the data that may be leaked, the number of people who have accessed the data, etc.

3) Strengthen security awareness education: Strengthen employee security awareness education and improve their awareness of the importance and protection of code security;

4) Regular review: Regularly review the code base and promptly repair loopholes or problems when they are discovered to prevent similar problems from happening again.

4. Sensitive document leakage cases

Q1 Data leaks of concern

Source: Threat Hunter original report, page 15

- Sensitive files of many companies have been leaked, involving confidential files, servers and other information. Telegram and the dark web are high-risk areas for sensitive file data leaks. In addition, network disks, libraries, online documents and other channels may also leak corporate sensitive information. Recently, the Threat Hunter intelligence platform has detected that sensitive information of many companies has been leaked online. Here are two cases.

Case 1: A bank's confidential loan business documents were leaked in a library, which not only affects the bank's reputation, but may also lead to the bank's legal liability for violating regulations. In addition, cybercriminal groups can also use leaked confidential documents to commit illegal acts, such as copying the documents and pretending to be a bank employee to commit fraud.

Case 2: A company's internal online documents were leaked. The leaked fields included detailed server information, app information, company information on Alipay and other platforms, and even exposed specific login accounts and passwords. If this information is discovered by threat actors, threat actors can directly log in to the account password and commit malicious acts such as stealing confidential documents.

Safety advice:

1) Inform employees of the importance of data protection, and guide employees to learn the company's data security policy and network security knowledge;

2) Use a secure file sharing platform, such as encrypted cloud storage or private file server;

3) Implement access control measures, for example: employees use VPN to connect to the company network to access sensitive files;

4) Conduct regular security audits and vulnerability scans to ensure the security of the network and system, and remediate problems immediately if problems are discovered;

5) Establish a security response plan to respond to data leaks and security incidents.

Data protection measures and recommendations

4. Data protection measures and suggestions

External: Data leakage risk monitoring Enterprise data assets are diversified and increasingly valuable, involving user information, employee information, sensitive files, business codes, etc. Digitization has brought about a greater exposure to data, making early perception of possible data leakage risks increasingly important. Threat Hunter data leakage monitoring intelligence comprehensively monitors threat actors' data transaction channels and outsourcing channels for sensitive files and codes, helping enterprises to promptly perceive, trace sources early and defend against potential data leakage risks, and avoid large-scale data leaks that affect the normal development of business.

Internal: Strengthen API security construction. Enterprises should strengthen API security construction on the basis of "business priority". Through the API security management and control platform, comprehensively sort out open APIs, flowing sensitive data and access accounts, and achieve timely monitoring of abnormal access risks to sensitive data.

Threat Hunter's API security management and control platform comprehensively sorts out the enterprise's APIs, sensitive data and access accounts, evaluates design flaws such as unauthorized access to API assets, excessive exposure of sensitive data, etc., and promptly identifies risks such as data crawling and abnormal account data access based on threat actors attack intelligence, eliminating the risk of data leakage from the root cause.

Only by combining internal asset security with external threat intelligence monitoring can enterprises respond to data leakage risks efficiently and effectively, and move quickly and steadily on the road to digital construction and innovative development.

Sources of data leakage and industry distribution in the first quarter

Source: Threat Hunter original report, page 6