THREAT HUNTER RESEARCH

API Security Governance: Assets, Authorization and Business Risk

A governance-focused report on dynamic API assets, authorization, data minimization and abuse of business logic.

Original publication: 2023-02-09
Research team: Threat Hunter Research Team
Source report: 39 pages

Original report text

This text version is reconstructed based on the 39-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 recent years, the wave of digitalization has intertwined with the epidemic, and the "fast forward button" has been pressed on the online transformation of corporate business. Under the trend of digitalization and onlineization, API interfaces, as an important channel for application connection and data transmission, are showing a large-scale growth trend. The imbalance between the growth rate of API applications and their security development has made them the first choice for malicious attacks. The battle between attack and defense around API security has become increasingly fierce.

Threat Hunter has long been committed to the research of API security, focusing on various cybercrime ecosystem intelligence against API attacks across the entire network.

The "2022 API Security Research Report" shows that API security has become one of the most severe network security challenges facing enterprises today:

1. The average number of APIs attacked every month in 2022 exceeded 210,000, among which the "promotion abuse" scenario is the most common among API attacks.

Accounting for the largest proportion of major scenarios, financial and government platforms have become important targets for threat actors to attack APIs and steal data;

2. In 2022, many API attacks caused by improper API security protection occurred in various industries such as the Internet, government affairs, and finance.

Attacks and data leakage incidents: For example, the business API of the online government platform was attacked by threat actors, and citizens' private data was crawled; social platforms faced a large number of account scanning, credential stuffing and other attacks, and a large number of user accounts were sold by threat actors and used for pornography, gambling, fraud and other traffic promotion.

Threat Hunter's "2022 API Security Research Report" is based on API attack risks captured by the Karma intelligence platform. It analyzes the API security status and attack trends in the past year, sorts out the more common API security flaws and API attack methods in 2022, and gives corresponding defense suggestions based on API security cases.

API security risk profile

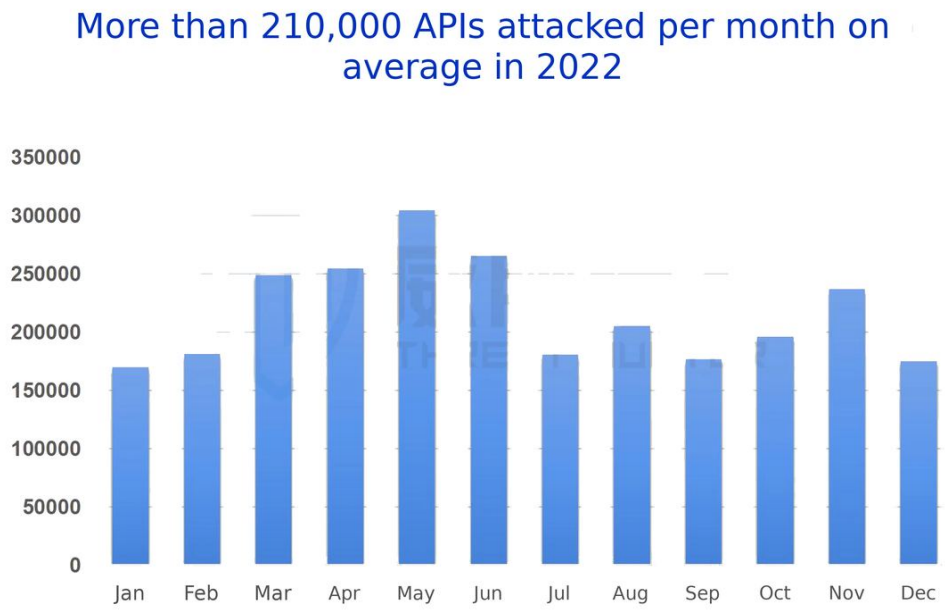
1. Overview of API security risks in 2022

1. The average number of APIs attacked every month in 2022 exceeded 210,000

Judging from the attack traffic captured by the Threat Hunter Karma intelligence platform, the average number of APIs attacked per month throughout 2022 exceeded 210,000. The number of

APIs attacked reached a peak in the second quarter (April-June), with the average number of monthly attacks exceeding 270,000.

Figure: Number of APIs attacked from January to December 2022



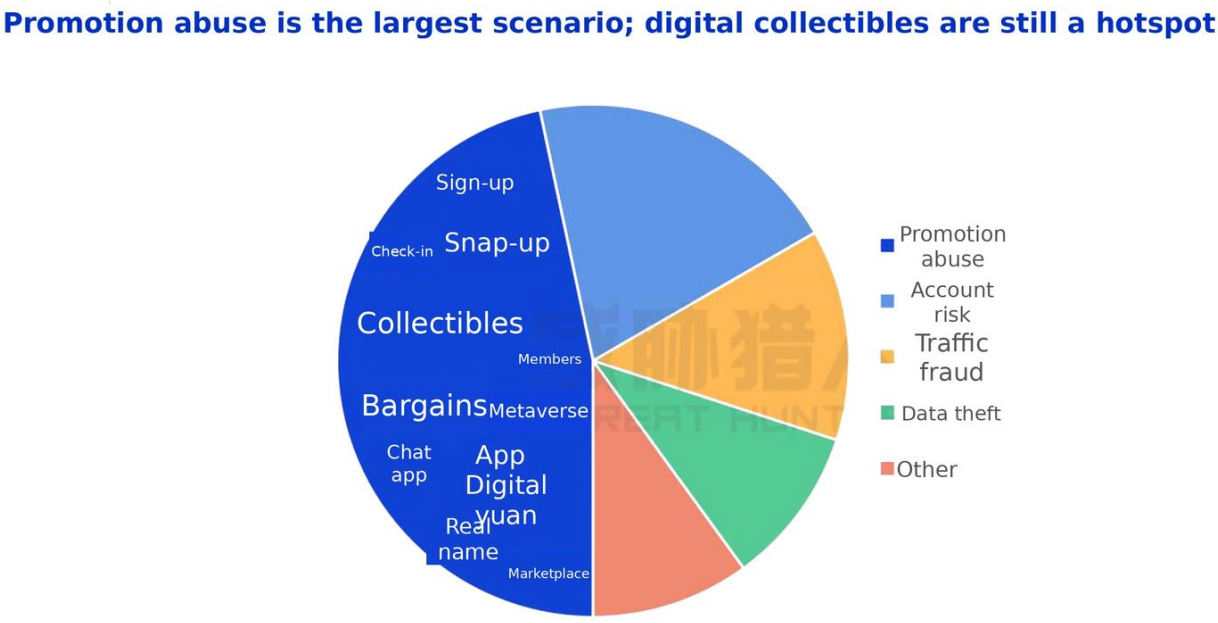
Number of APIs attacked per month in 2022: more than 210,000 on average

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

2. API attacks are mainly concentrated in four major scenarios, with promotion abuse scenarios accounting for the largest proportion.

Judging from the scenarios where APIs are attacked, they are mainly concentrated in four major scenarios: promotion abuse, account risk, data theft, and traffic fraud. Among them, the number of attacks in promotion abuse scenarios accounts for nearly half of the total number of attacks. In addition, a series of account risk issues such as fake accounts and account theft account for up to 20%, becoming the second most common API attack scenario.

Figure: Proportion of common scenarios of API attacks

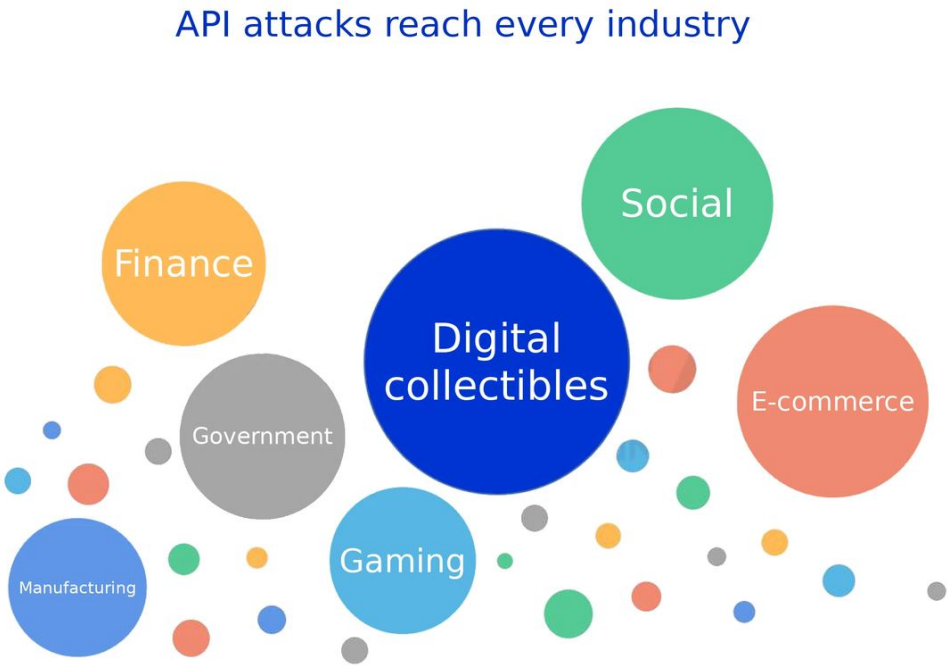


Share of API attack scenarios: promotion abuse is the largest, and digital collectibles remain a hotspot

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

3. API attacks occur in all walks of life. Financial and government platforms are threat actors attacking APIs and stealing

Top Targets of the Data Map: Top Industries for API Attacks in 2022



API attacks reach every industry, led by digital collectibles

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

Judging from the industry distribution data of API attacks in 2022, the most popular one is the digital collection industry. Beginning in early 2022, attacks by threat actors targeting digital collection activity interfaces surged rapidly and reached a peak in Q2 2022.

It is worth noting that by analyzing API attack traffic in 2022, the Threat Hunter intelligence research team found that multiple financial and government platforms have suffered large-scale attacks. threat actors illegally crawled a large amount of sensitive data involving citizen privacy, financial business processing, etc. through APIs with security flaws on financial or government platforms.

threat actors can obtain high profits by selling user data in the financial industry, including but not limited to selling it to intermediaries to "precisely" attract customers, selling it to criminals to commit fraud, etc.; the API interface of the government affairs platform carries a large amount of citizen privacy data, such as ID cards, addresses, medical insurance and social security and other sensitive information, and is also the target of crazy attacks by threat actors.

In addition, API interfaces in gaming, social networking, e-commerce, manufacturing and other industries have also been subject to large-scale attacks by threat actors, as shown below:

Games: The main scenario where API interfaces in the game industry are attacked is account risk. threat actors have long launched account scanning, credential stuffing, and brute force attacks on interfaces such as registration, login, and password retrieval, stealing player accounts and virtual assets. The scale of network-wide attacks targeting some popular games has reached hundreds of millions.

Social: The main scenario where social platform API interfaces are attacked is traffic fraud. threat actors create false readings, likes, comments, etc. by attacking the business interface of the platform. Internet trolls can use this to control public opinion, and traffic gangs can use this to divert traffic to online crimes such as gambling and fraud.

E-commerce: E-commerce platforms are faced with traffic fraud problems such as marketing cheats, merchants' traffic manipulation orders, and scalpers rushing to buy. Especially during e-commerce festivals such as Double 11 and Double 22 every year, as well as during the rush for popular commodities such as masks and antigens during the epidemic, the API interfaces of various platforms are often subject to large-scale attacks by threat actors.

Manufacturing: Traditional manufacturing industries such as automobiles and home appliances will further deepen their digital transformation in 2022, and their online business API interfaces have also been targeted by threat actors, resulting in security issues such as promotion abuse and data theft.

API security flaw analysis

2. Analysis of API security flaws in 2022

API attacks occur frequently, and the root cause is still the security flaws in APIs. Based on the 2022 traffic audit results of the API security management and control platform, Threat Hunter sorted out the five major API security flaws that enterprises need to pay attention to from the three dimensions of harm, exploitability, and universality.

Five API security flaws to watch in 2022

Flaw type	Harm	Exploitability	Prevalence
Unauthorized access	Very high	High	High
Weak passwords allowed	High	High	High
Excessive exposure of sensitive data	High	High	Medium
Unreasonable error messages	Medium-high	Medium-high	High
Unreasonable security configuration	Very high	High	Medium

Five API security flaws to watch in 2022, rated by harm, exploitability and prevalence

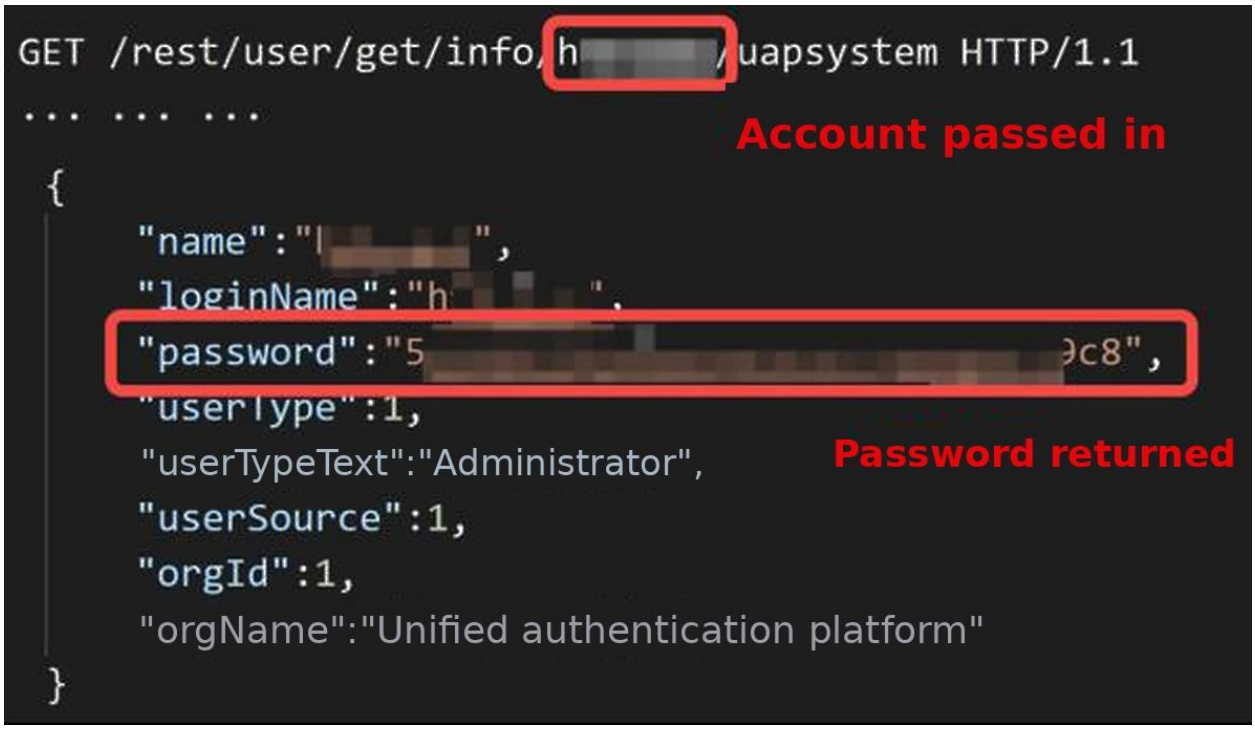
Source: Threat Hunter original report, page 10. Table re-typeset in English from the original.

Note: Very High>High>Medium High>Medium

1. Unauthorized access

Judging from the audit results in 2022, "unauthorized access" is still one of the most harmful API security flaws. The API has unauthorized access flaws that may lead to system permissions being compromised. Threat Hunter intelligence researchers discovered an API interface of a company's internal system in Q1 of 2022. This interface opened access to the external network and did not require any authorization for access. The password of the account can be obtained by passing in any account.

This is a very serious security vulnerability. Once attacked, the attacker can easily obtain the administrator's account password and gain the highest authority of the system.



An unauthorized API returns the administrator account and its password when an account is passed in

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

The flaw could also lead to large-scale data theft. Threat Hunter conducted a security assessment on the API interfaces of 48 banks' credit card services in Q3 of 2022, and found that at least 20 banks' API interfaces have unauthorized access flaws: without authorization, the credit card processing information of any user can be queried, and threat actors gangs also used this flaw to launch large-scale automated attacks on the API interfaces of many banks, stealing user private information in batches.

Safety advice:

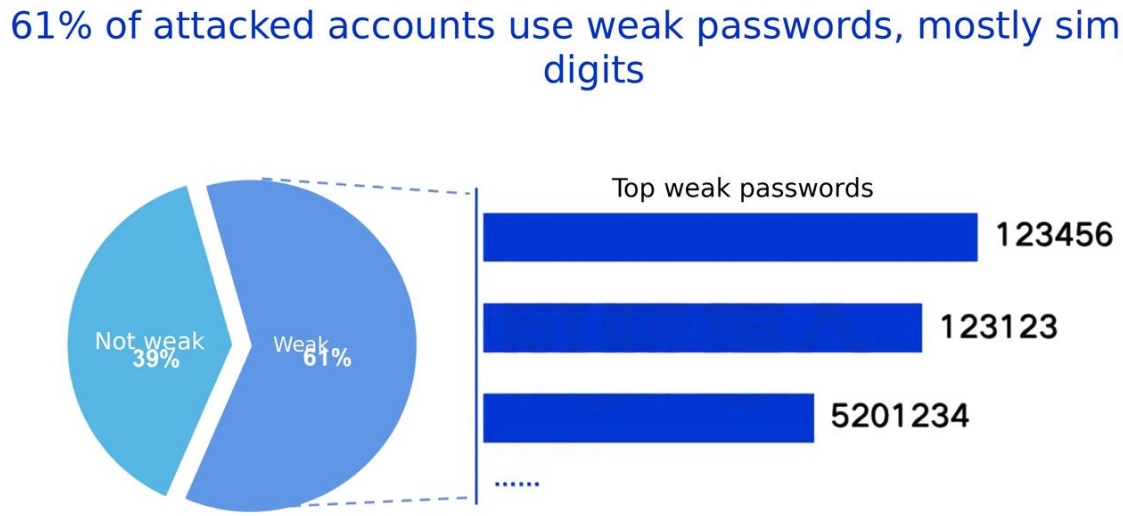
1) Unless the resources are completely open to the outside world, access must be authorized by default, especially access to user resources or restricted resources;

2) Strictly control access to API interfaces that do not require authorization through whitelisting.

2. Allow weak passwords

"Allowing weak passwords" is a flaw that is very harmful, common, and exploitable. It is one of the main methods used by threat actors to steal accounts. Although many security development specifications mention that password settings need to meet a certain level of strength, judging from the overall situation in 2022, there are still many API interfaces, and even some login interfaces in the management backend, that have the defect of allowing weak passwords.

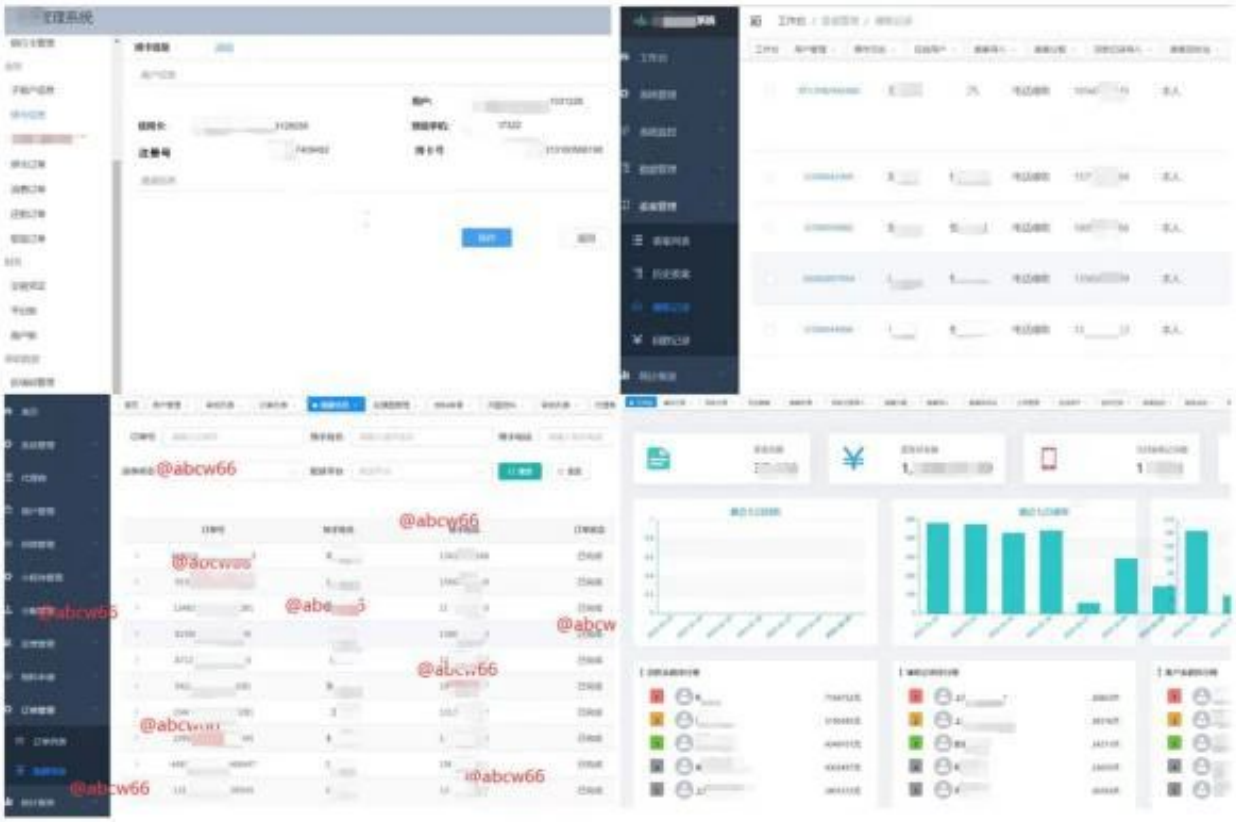
The API interface has a flaw that allows weak passwords, which can easily lead to serious account risks. Take a certain gaming platform as an example. Due to weak password flaws, the platform has been subject to long-term credential stuffing and brute force attacks by threat actors. More than 61% of the accounts successfully stolen by threat actors have weak passwords, and the top ones are some very simple pure number combinations.



61% of attacked accounts used weak passwords, mostly simple digits

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

This flaw in the backend API interface may cause system permissions to be compromised. In a data leakage incident, Threat Hunter intelligence researchers repeatedly discovered screenshots of the management backend circulated by criminals. It was initially determined that the attacker exploited weak password flaws to break out the account and password for logging into the backend.



A back-end system reached through a weak password exposes user data

Source: Threat Hunter original report, page 13. Original image retained.

Safety advice:

1) Check password complexity in user registration, login, password reset and other scenarios. It is recommended that the password length be no less than 8 characters and contain uppercase and lowercase letters, numbers and special symbols;

2) The password is not allowed to be set to account number, email address, birthday and other related information;

3) For high-privilege accounts, it is recommended to introduce a mechanism to force password changes within a period of time.

3. Excessive exposure of sensitive data

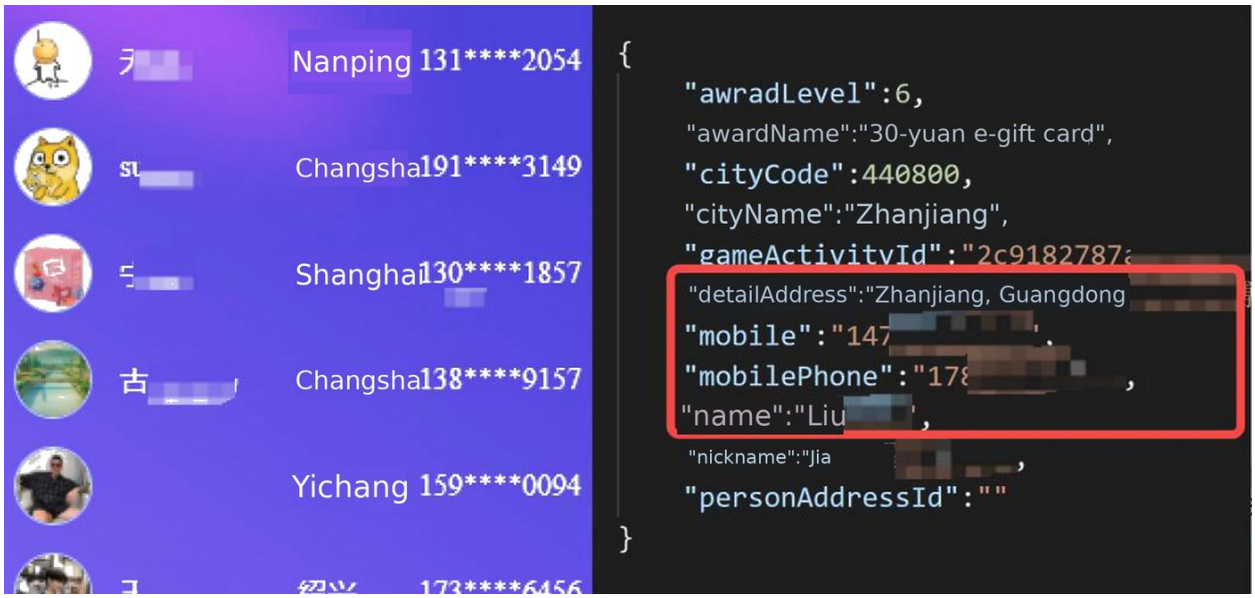
"Excessive exposure of sensitive data" means that the API interface does not impose any restrictions or filters and returns sensitive data stored in the backend to the frontend. Once attacked by threat actors, it will cause serious data leakage problems.

Research by the Threat Hunter Intelligence Laboratory found that APIs with defects in excessive exposure of sensitive data often appear on corporate information disclosure pages. Although the page only displays necessary information and desensitized information, the API interface behind it returns a large amount of unnecessary plaintext sensitive data. Some API interfaces return hundreds or even thousands of user sensitive data at a time.

Take the marketing activities of an Internet company as an example:

On the winning announcement page of an Internet company's marketing campaign, only the avatar, nickname, city and desensitized phone number of the winning user were displayed, but the

API interface returned a lot of sensitive data that was not displayed on the page, including the real name of the winner, shipping address, plain text phone number, etc. The announced winning information can be viewed by anyone, and can easily be obtained and used by criminals.



A winners' page API returns full phone numbers and addresses that the page itself hides

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

Another real-life example of overexposure of sensitive data via APIs:

On the supplier disclosure page of the official website of a digital transformation enterprise, only the supplier's company name, company picture, business license and other basic information are displayed. However, the API interface returns a lot of very sensitive personal privacy data that does not need to be disclosed, including the supplier's legal person's ID number, phone number, emergency contact, etc. After these sensitive data are stolen by criminals, it will not only endanger the personal security of the supplier's legal person, but also bring resistance and blow to the digital transformation of the enterprise.



A supplier disclosure API returns ID numbers, ID card photos, phone numbers and emergency contacts

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

Safety advice:

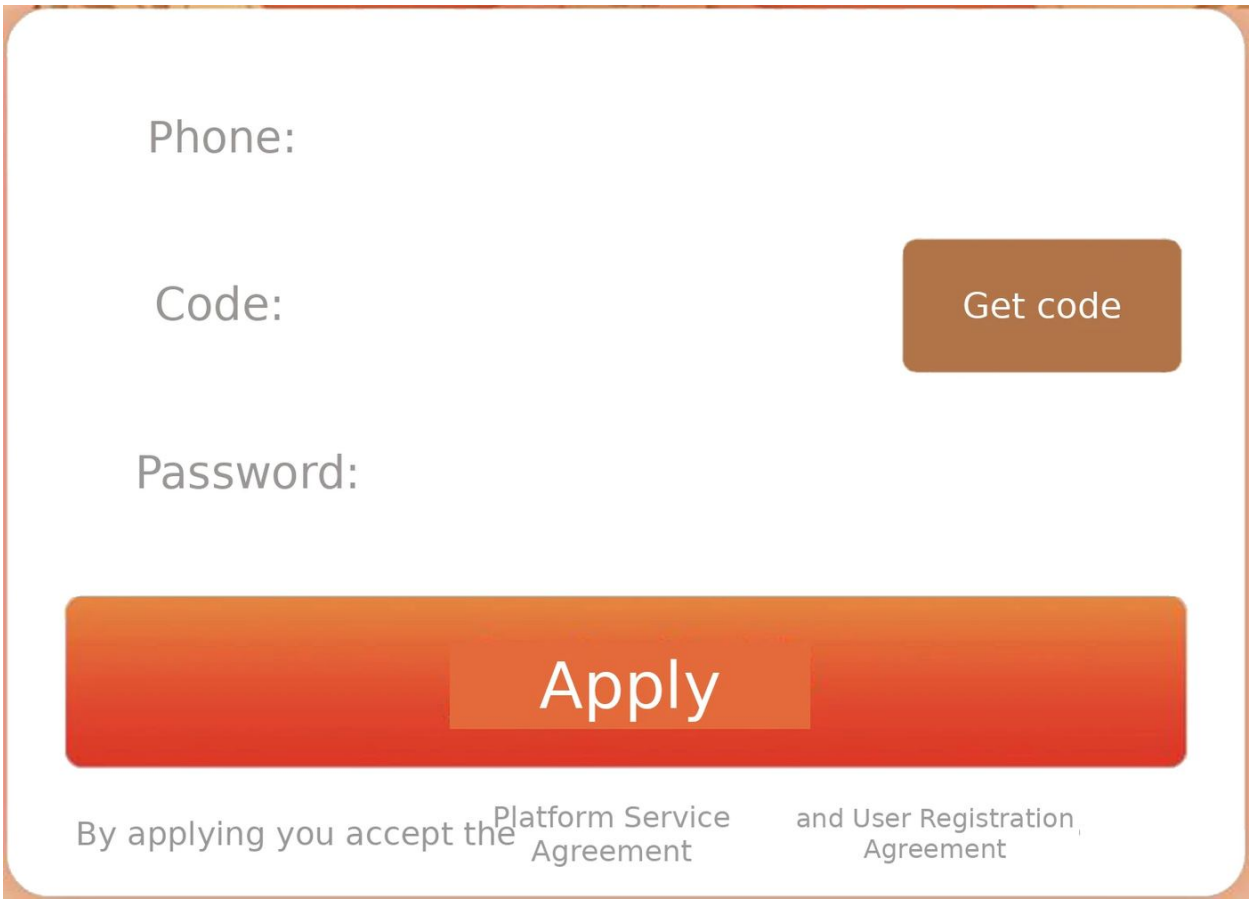
The API interface must strictly filter the sensitive data returned to the front end and only return the data required by the front end.

4. The error message is unreasonable

"Unreasonable error message" refers to the error message returned by the API interface, which may inadvertently expose sensitive data such as the user's registered account, phone number, and email address. Judging from the audit results in 2022, unreasonable error prompts are still widely used by threat actors in account scanning attacks. Threat Hunter intelligence researchers discovered that the API interfaces of multiple financial lending platforms were attacked by threat actors gangs, resulting in the leakage of a large number of phone numbers of users on the platform.

Take the API attack on a certain financial lending platform as an example:

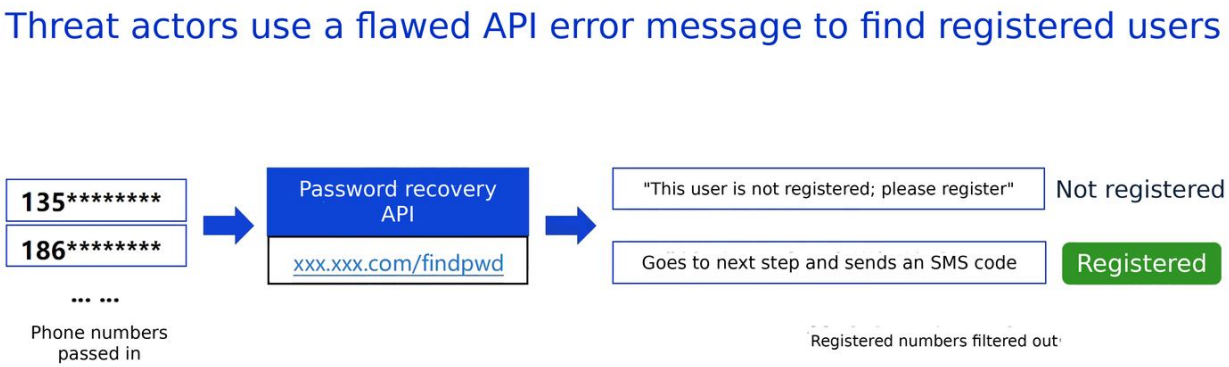
Threat Hunter intelligence researchers analyzed the attack traffic and found that when users initiate a loan application, they will be guided to fill in their phone number to register. After clicking to apply, the front end will return different prompts to the user based on the value returned by the interface (as shown below).



The loan application page: phone number, SMS code and password

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

Many attackers take advantage of this to carry out account scanning attacks, passing in different phone numbers in the interface parameters, and then filtering through the interface return value (True/False), thereby obtaining the phone numbers of a large number of platform registered users. In batch attacks, there are API interfaces with unreasonable error prompts. If the attack cannot be discovered and blocked in time, threat actors can completely traverse the 11-digit phone numbers and obtain the registered phone numbers of all users of the platform.



Threat actors use an unreasonable error message on the password recovery API to sort registered from unregistered numbers

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

Safety advice:

1) Fuzzify the error message for login, registration, verification code sending, password retrieval and other interfaces, such as returning "the username or password is incorrect";

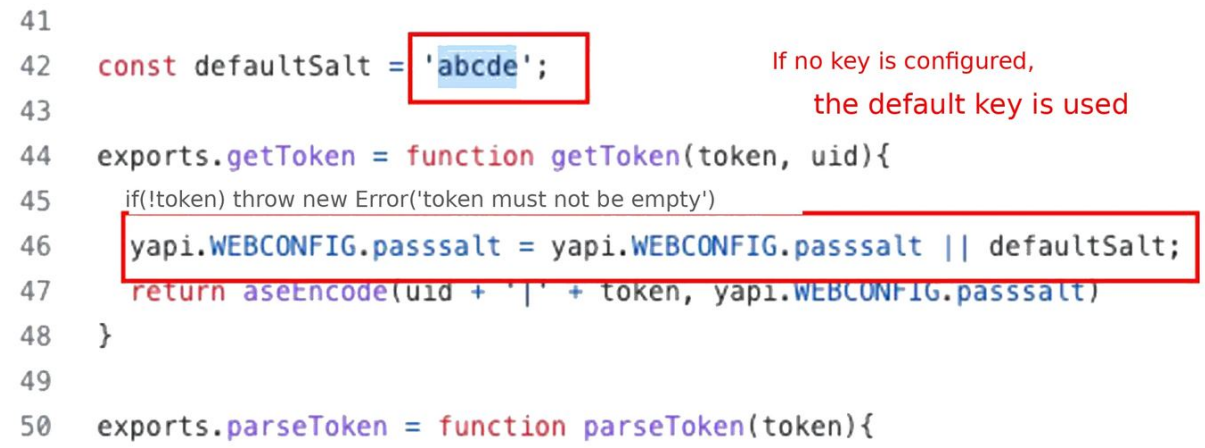
2) For the above interfaces, strengthen monitoring of abnormal behaviors such as excessive call volume and high call frequency.

5. Unreasonable security configuration

"Unreasonable security configuration" refers to problems such as the negligence of development or operation and maintenance personnel, which leads to the exposure of API interfaces that should not be made public, the use of older versions of API interfaces with vulnerabilities, or the use of default passwords or keys for interface access.

In 2022, Threat Hunter conducted a security audit on the back-end components and services of some enterprises. Judging from the audit results, the defect of unreasonable security configuration is widespread, and there are many serious security configuration errors such as Spring Boot Actuator and Elasticsearch configuration errors.

It is understood that in November 2022, a widely used open-source API management platform exposed a high-risk vulnerability in executing arbitrary commands. One of the important reasons is that the default key is used, which allows the attacker to successfully obtain system permissions, as shown in the figure:



The API management platform falls back to a default key when none is configured

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

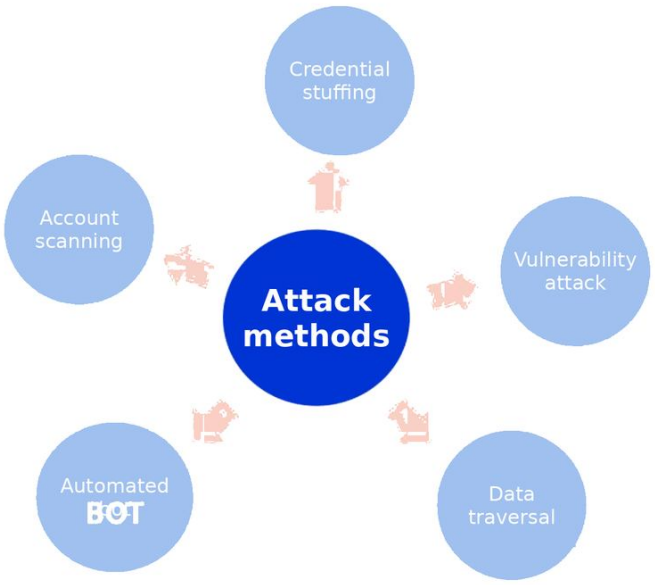
Safety advice:

1) Comprehensively check the version of the components/services used and try to upgrade to the latest version;

2) Comprehensively check whether the configuration is correct to avoid components/services exposing unauthorized access to APIs and avoid using default passwords or keys.

Analysis of API attack methods

3. Analysis of API attack methods in 2022



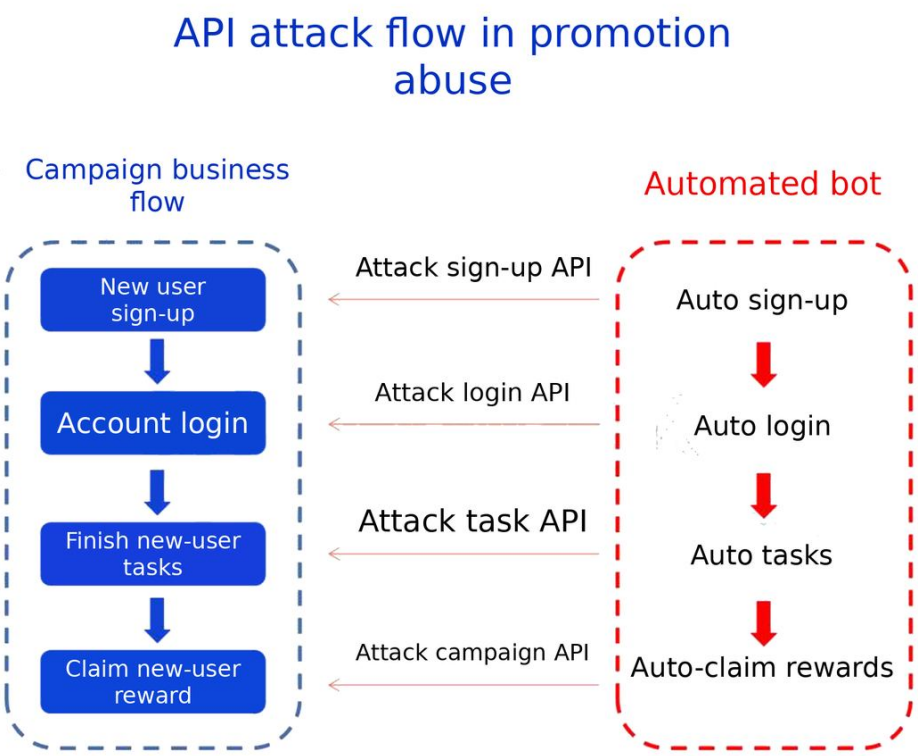
The main API attack methods in 2022

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

1. Automated BOT

"Automated BOT" is one of the most common API attack methods in 2022, mainly appearing in promotion abuse and traffic fraud scenarios. threat actors simulate human-operated operations through automated scripts and other methods, forge complete business processes, and then attack multiple API interfaces according to the real business access sequence.

Take API attacks in marketing fraud scenarios as an example:



API attack flow in promotion abuse: bots hit each API of a new-user campaign

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

Professional threat actors often have rich experience in offensive and defensive confrontations. The automated BOT attacks they launch will not show obvious abnormalities in traffic and behavior, making it difficult to identify whether they are human participants or robots. Therefore, for automated BOT attack methods, we need to distinguish it from normal user requests from massive interface access data.

Automated BOT attacks mainly include the following identification dimensions:

Main dimensions for identifying automated bot attacks

Dimension	Experienced bot attacks	How they evade defences
UA	No clustering	Random forged user agents that match the device
IP	No clustering	Switch IP addresses through dynamic proxies or dial-up IPs
Device	No clustering	Change device parameters with device-spoofing tools
Behaviour	Request parameters and order identical to a real user	Capture and crack traffic to obtain the API request parameters and order

Main dimensions for identifying automated bot attacks

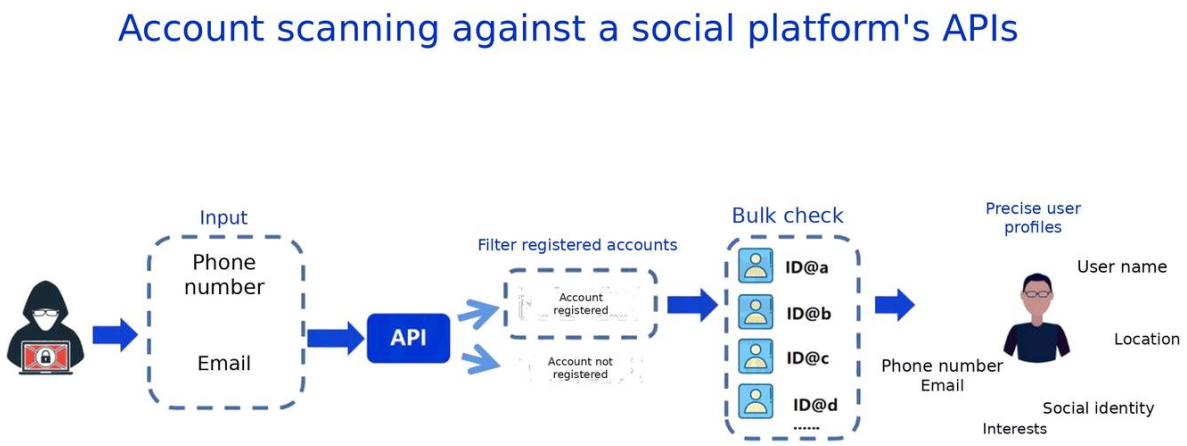
Source: Threat Hunter original report, page 20. Table re-typeset in English from the original.

2. Account scanning attack

"Account scanning attack" means that cybercriminal groups targets API interfaces such as "registration, login, and password retrieval" and uses the return values □□of registration, login and other interfaces, such as "account already exists" or "account does not exist" to determine whether an account (user name, email, phone number, etc.) has been registered on the platform.

By traversing the 11-digit phone numbers, cybercriminal groups can filter out the phone numbers of all registered users on the platform. Once these data are sold on the black market, the owners of the phone numbers will suffer from telemarketing harassment or even phone fraud.

It is mentioned in the API security flaw analysis that if the interface has flaws with unreasonable error prompts, it is likely to be attacked by threat actors.

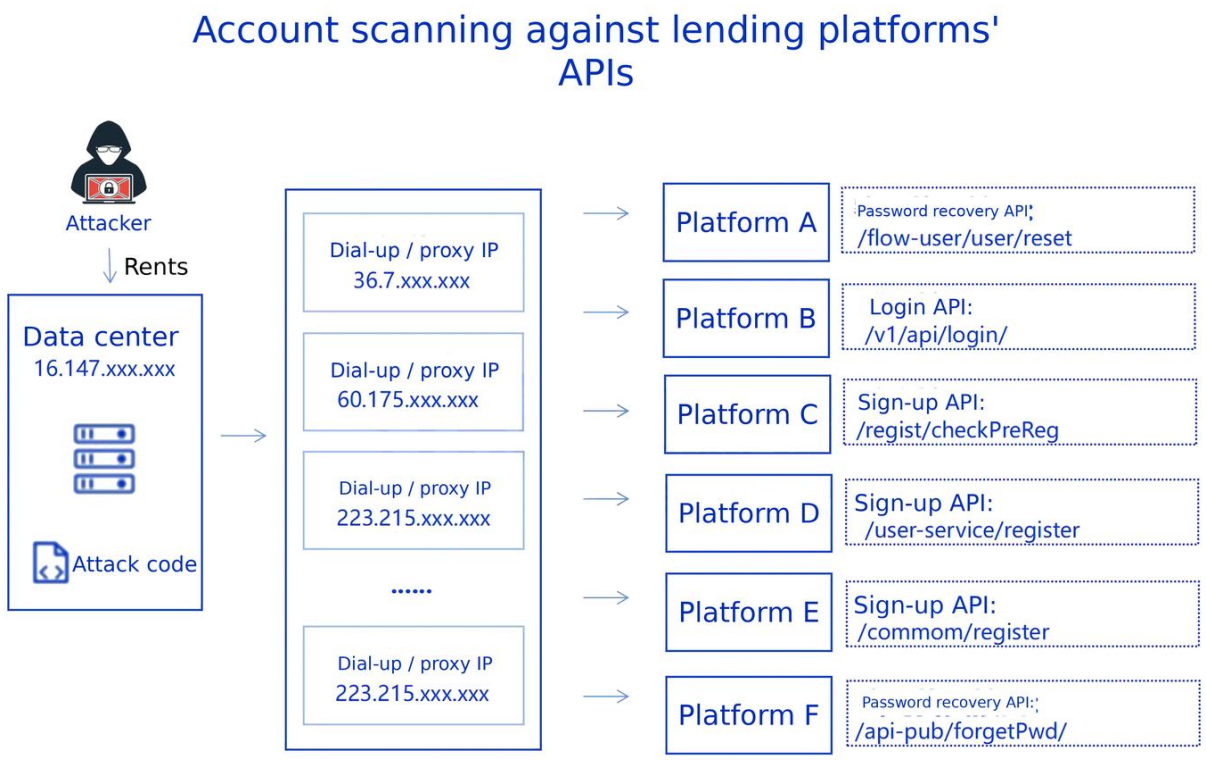


Account scanning against a social platform's APIs builds precise user profiles

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

The financial industry is a key industry for account scanning attacks. On the one hand, these data will be sold to financial intermediaries or promoters of other platforms for "targeted marketing" and "accurate customer acquisition"; on the other hand, these data will also be sold to fraud gangs to implement precision fraud. The most typical routine is to confirm that the victim has borrowed money from a certain financial platform, and then call to induce the victim to transfer money to a bank account controlled by criminals in the name of "margin", "service fee", "handling fee", etc.

The Threat Hunter Karma intelligence platform captured multiple account scanning attacks targeting the API interfaces of financial lending platforms in 2022, and conducted a detailed analysis of the attack process of one of the more active threat-actor groups. The gang first rented a server in an IDC computer room in China, deployed the attack code on the server, and then launched a large-scale automated attack on the API interfaces of multiple platforms, as shown in the figure below:



Account scanning against lending platforms' APIs from rented data-center servers through dial-up and proxy IPs

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

In order to obtain as much user data as possible, the gang will frequently attack these interfaces. At the same time, in order to avoid being discovered, the gang frequently switches IPs through dynamic proxies and speed dials obtained from the threat actors resource platform. More than 35% of the IPs even launch only one attack. Judging from the actual attack results, none of the platforms under attack can identify or block the attack, and the attack success rate reaches 100%.

3. Credential stuffing attack

"Credential stuffing attack" refers to a group of threat actors targeting the login interface or other interfaces, submitting a large number of leaked username/password combinations in batches through some automated tools, and recording the combinations that can successfully log in, thereby stealing the account and taking over its permissions.

The gaming industry is a key industry for credential stuffing attacks. After threat actors successfully steal accounts through credential stuffing attacks, they usually log in to the account to check the player's account level, assets, equipment and other information (account sharing). If the account does not have secondary verification, threat actors will transfer gold coins and other assets and equipment in a very short time, and even break down equipment that cannot be transferred (account washing), which not only causes property damage to players.

The loss also caused damage to the reputation and ecology of the game platform. In addition, Threat Hunter researchers found that some large social platforms have also encountered credential stuffing attacks many times.

In order to reduce the risk of credential stuffing attacks, many companies have strict security restrictions on login interfaces. But as the saying goes, "defensive controls must continue to evolve", professional threat actors will adopt targeted attack strategies:

1. In order to avoid being discovered, the attack group carries out low-frequency credential stuffing attacks on the login interface. For example, an attack is launched only once every 3-4 minutes on average.

Because it is difficult to detect, it can maintain long-term attacks;

2. In order to improve the efficiency of credential stuffing attacks, the attack group will combine account scanning attacks and first screen out registered accounts through account scanning.

Registered accounts further launch credential stuffing attacks;

3. In order to further improve the attack efficiency, threat actors conduct API asset detection through path scanning and other methods to find old login interfaces.

Attacks are carried out through interfaces. Old interfaces may lack security restrictions due to lack of maintenance and are more susceptible to attacks.

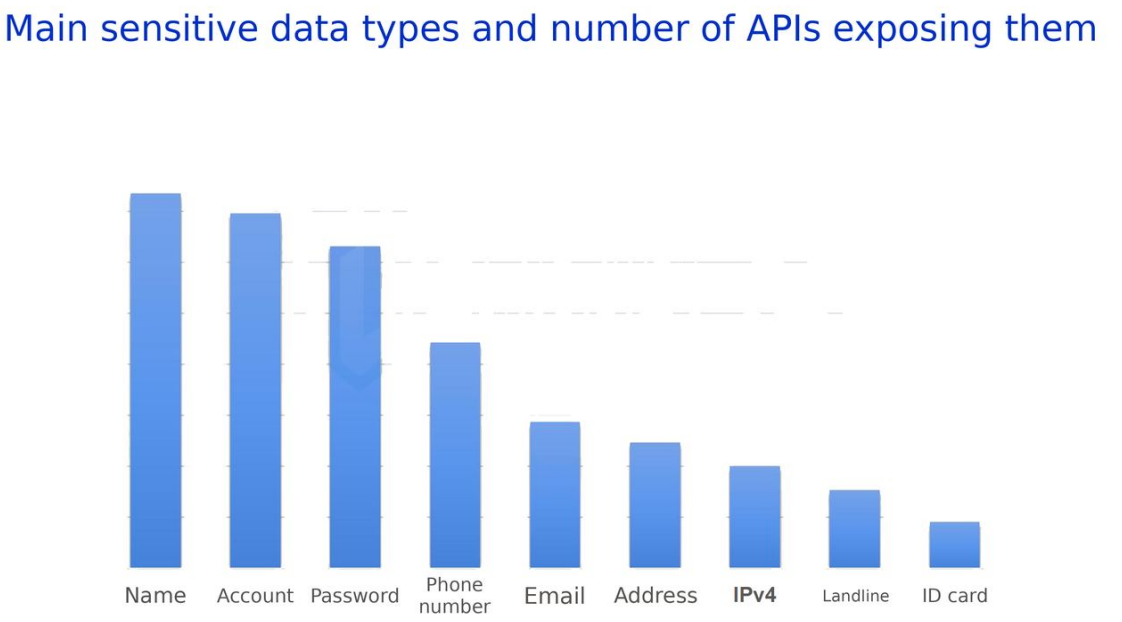
4. Data traversal attack

"Data traversal attacks" usually target API interfaces with "unauthorized access defects" or "excessive access defects". threat actors attack these API interfaces to steal user data or business data of the platform in batches. Data traversal attacks have gradually become one of the important causes of data leakage incidents.

Government affairs platforms are a key industry for data traversal attacks. In order to improve business processing efficiency and service experience, local government agencies have launched online government services. However, many business API interfaces have become key targets for cybercriminals due to security flaws.

Data traversal attacks on government platforms became more rampant in 2022. The Threat Hunter Intelligence Laboratory once discovered a large-scale cybercriminal group that illegally stole data. After investigation, it was found that the group developed dozens of automated attack tools and exploited security flaws in the API interfaces of government platforms to illegally steal citizens' private data on a large scale through data traversal attacks.

By conducting data traversal attacks on API interfaces, threat actors steal the main types of sensitive data as follows:



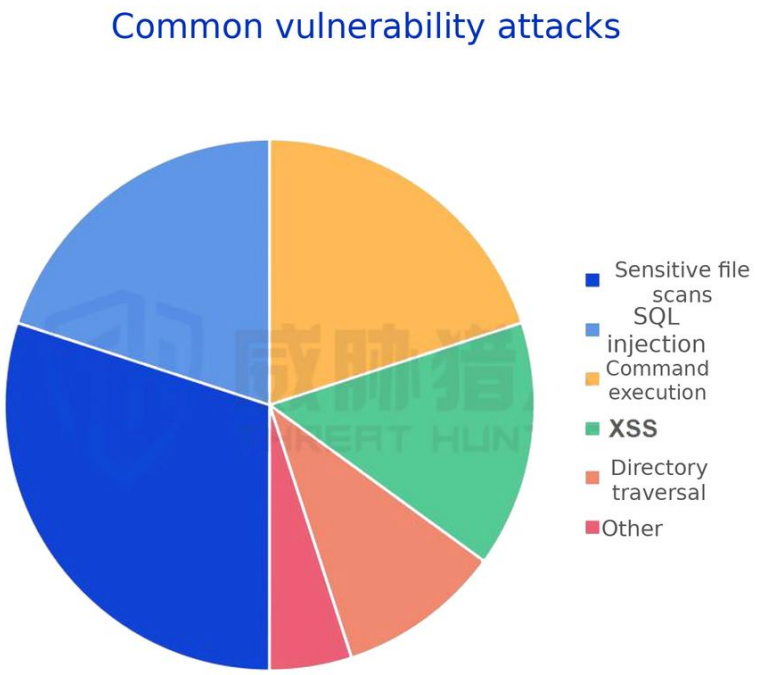
Main types of sensitive data stolen through data traversal and the number of APIs exposing each

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

5. Vulnerability attacks

"Vulnerability attacks" usually refer to some common web vulnerabilities such as "SQL injection vulnerabilities, command execution vulnerabilities", which are used to attack API interfaces. In 2022, Threat Hunter intelligence researchers conducted an audit study on the traffic of some enterprises and found that vulnerabilities such as "sensitive file scanning, SQL injection, command execution, XSS, and directory traversal" occurred more frequently.

There are a large number of vulnerability attacks launched by scanners every day on the Internet. During attack and defense drills, "vulnerability attacks" are an important "killer weapon" for attackers. Attackers initiate scans through vulnerability scanners and quickly find vulnerabilities in target assets. Due to the large number of scans, it is difficult for security equipment to achieve accurate alarms, and it is easy to generate a large number of false alarms. Therefore, the defender needs to locate the vulnerability point, perceive the risk in a timely manner and take defensive measures to prevent the risk from further expansion.

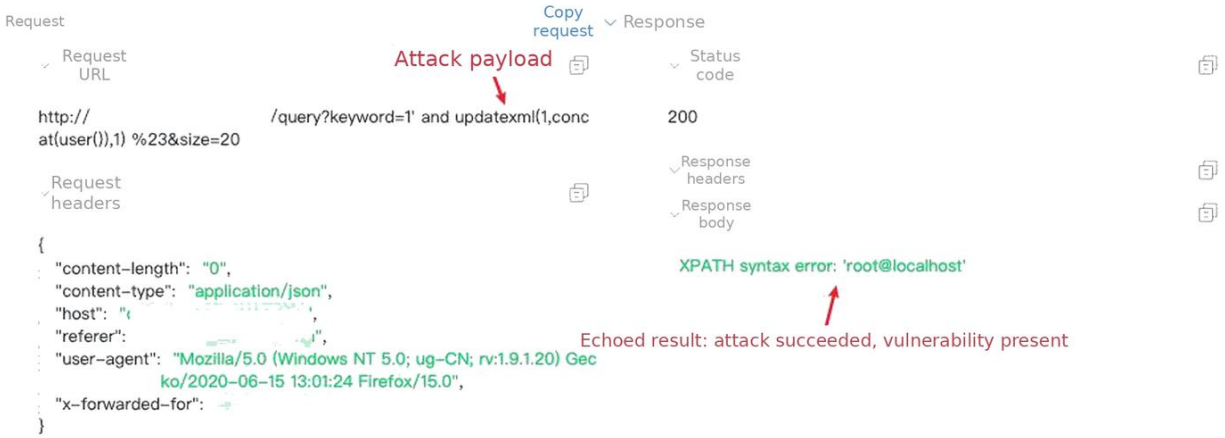


Common vulnerability attacks: sensitive file scans, SQL injection, command execution, XSS and directory traversal

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

Take the more classic "SQL injection" as an example:

Combining HTTP requests and responses, we can analyze whether some SQL injection vulnerabilities are successfully attacked. If there are functions such as updatexml() in the request parameters, and there are keywords such as "XPATH syntax error" in the response body, it can basically be determined that SQL error injection is being performed and the attack has been successful.



A request and response showing that an SQL injection succeeded

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

API attack cases

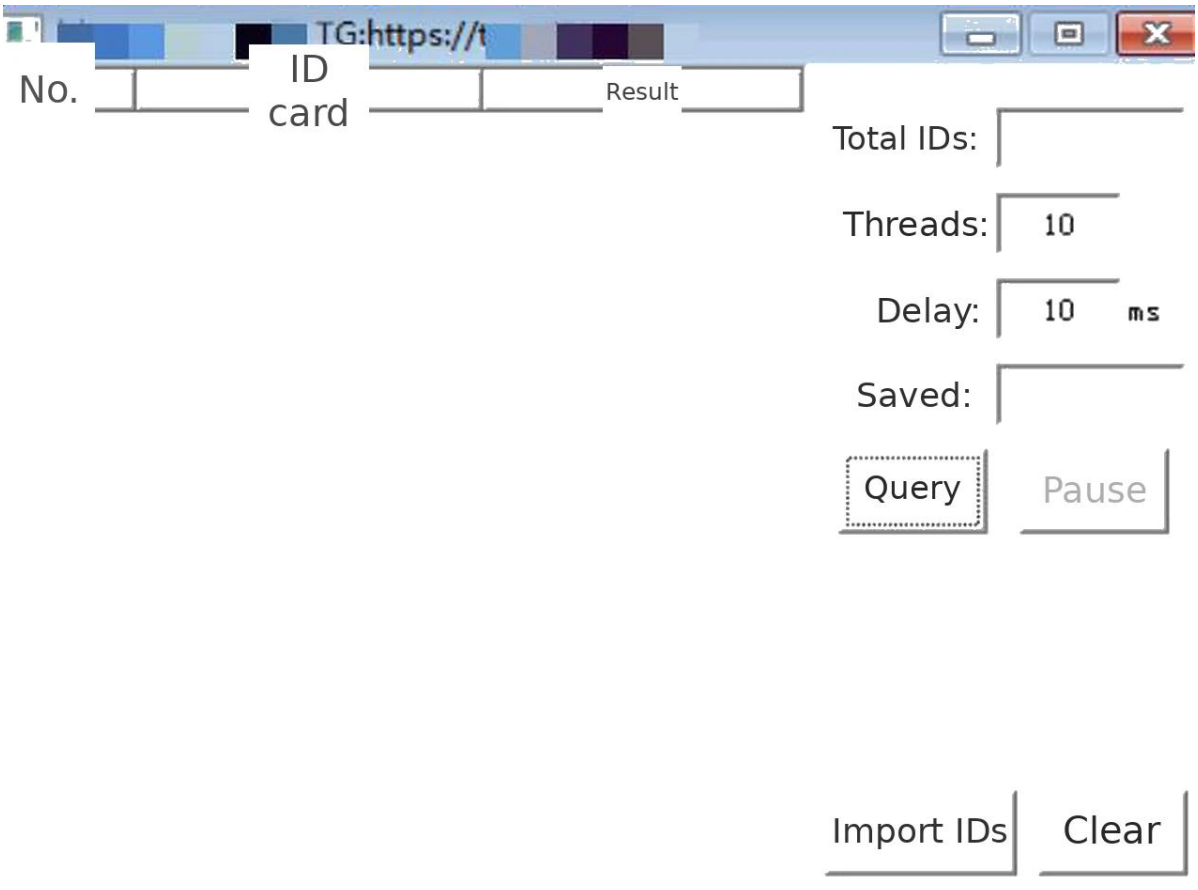
4. API attack cases worthy of attention in 2022

1. The business API of the online government platform was attacked by threat actors, and citizens' private data was crawled

Online government affairs bring great convenience to the general public, but behind online government affairs are often associated with a large amount of citizen privacy data. Data access restrictions, identity authorization, etc. need to be carefully designed and strictly reviewed. The exposure of a large number of APIs on the Internet undoubtedly increases the risk of citizen privacy data leakage.

Real-life examples of attackers exploiting APIs to obtain sensitive data:

In September 2022, the Threat Hunter Karma intelligence platform captured an automated attack tool called "**Name Certificate". The attacker used this tool to attack the data query API interface of an online government affairs platform in Guangdong, traversing and crawling the platform's user information.



The attack tool queries ID numbers in bulk against the government platform

Source: Threat Hunter original report, page 27. Original figure with Chinese text replaced by English.

Threat Hunter researchers analyzed the attack tools and found from the reproduced attack code that the attacker only needs to construct the ID card parameters in the function and can query the basic information of any user without any authorization, including the citizen's name, ID card, marriage certificate, child birth certificate, household registration book, social security card, real estate rights, etc.

```
    # Get the document list for a given ID number
    resp = requests.post(url, data = postPattern.encode("utf-8"),
headers=headers, verify=False)
    print(resp.text)
    if resp.text == "[]":
        print("No result found")
        return
    j = json.loads(resp.text)
    for index in range(len(j)):
        fileId = j[index]["fileId"]
        if fileId == None:
            continue
        getLicenseFileStream(fileId,idCard)
        time.sleep(5)
```

Reproduced attack code that fetches the document list for a given ID number

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

Attackers will continue to scan and discover security vulnerabilities in system APIs, use a large number of dynamic proxy IPs, and use automated tools to crawl sensitive data, which can easily lead to large-scale data leaks. The recurring API attack code is as follows:

Examples of crawled sensitive information are as follows:

JSON ▾ No wrap Copy

```
    "fileName": "Resident ID card",
      "licenseCode": "440000201802******",
      "type": "0",
      "materialUnid": "",
      "fileId":
"440000201802******_100208101_1144060631507697******111187000",
      "licenseItemCode": "100208***"
  },
  {
      "fileName": "Guangdong household register",
      "licenseCode": "440000201902******",
      "type": "0",
      "materialUnid": "",
      "fileId":
"440000201902******_100210301_1144060631507697******111187000",
      "licenseItemCode": "100210***"
  }
]
```

Example of crawled data: resident ID card and household register files with ID numbers

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

Safety advice:

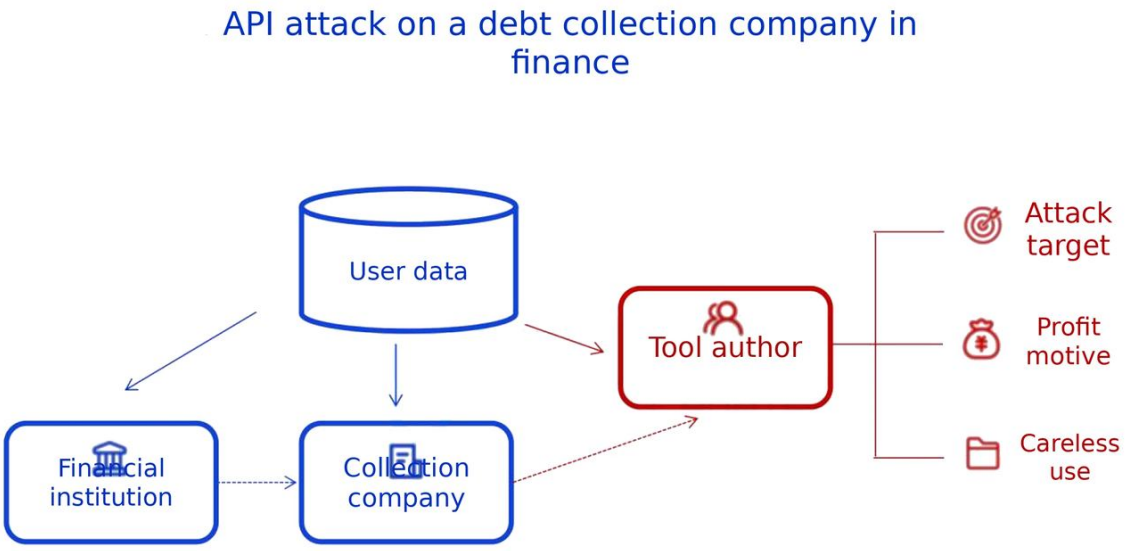
1) The interface for querying information on the government affairs platform is limited to only logged-in users, and the user's personal information can only be found when the ID card bound to the current user is consistent with the ID card being queried;

2) If it is unavoidable to query the user's personal information directly through the ID card, it is recommended that the interface should not be exposed to the Internet, only allow intranet access, limit the access rights of personnel, and keep log records.

2. API security risks exist in third-party cooperation in the financial industry, and many financial institutions are facing data

Leakage risk In order to reduce the risk of overdue debts from borrowers, financial institutions often entrust third-party companies to collect debts, and open the authority of their own debt collection systems to debt collection companies. At the same time, the borrower's ID card, phone number, address, contact person, loan amount and other data will be handed over to the third-party debt collection company. How to ensure data security has become an unavoidable issue for financial institutions.

Take the API attack incident of a collection company in the financial industry as an example:



API attack on a debt collection company working for financial institutions

Source: Threat Hunter original report, page 30. Original figure with Chinese text replaced by English.

In 2022, the Threat Hunter Karma intelligence platform monitored a collection company developing automated "collection assistance tools" through external tool authors, involving multiple financial institutions. After research and analysis, it was found that the "collection assistance tool" can bypass the collection system and gain access to user data and download customer data in batches by forging "API interface for pulling data" requests, without being affected by system access rights and operation restrictions.

Taking a certain tool as an example, the "Collection Assistance Tool" can directly obtain the borrower's name, ID card, loan amount, address and other data when accessing the following interface, and also supports downloading the data to the local.

API accessed by the tool	Purpose	Data returned
https://cs.xxx.com:8080/ajax/case/list.json	Pull the loan list	data.count: number of loans data[i].caseNo: loan number data[i].debtorName: borrower name
https://cs.xxx.com:8080/ajax/case/detail/info.js	Get borrower details	data.baseInfo.overdueAmount: overdue amount data.baseInfo.overdueDays: days overdue data.userInfo.certificateNo: ID number data.userInfo.workUnit: employer data.userInfo.unitAddress: address ...

APIs called by a "collection helper" tool and the borrower data they return

Source: Threat Hunter original report, page 30. Table re-typeset in English from the original.

On the one hand, employees of collection companies can log in to the system and view the information of borrowers, making it easier for potential insiders to steal data in batches; on the other hand, tool authors who have gained access to data will also become one of the targets of attackers, expanding data exposure and bringing new data leakage risks to financial institutions.

Safety advice:

1) During the process of API asset sorting and API defect detection, API interfaces that transmit business-sensitive data or user-sensitive data must undergo complete security audits and strict security restrictions to avoid defects such as unauthorized access and unauthorized access;

2) Intelligence-based API risk identification capabilities, extract behavioral patterns such as API request characteristics initiated by "collection assistance tools", and promptly discover abnormal flows of sensitive data and account violations;

3) The financial industry needs to strengthen the security governance of cooperative collection companies: The 2022 network-wide attack and defense drills have added a new dimension of data acquisition, including "obtaining sensitive data information through supply chain companies." Collection companies, as suppliers of collection services for financial institutions, are also supply chain companies and will become key attack targets in the future.

3. Internet social platforms are subject to credential stuffing attacks, and selling accounts are used for traffic promotion.

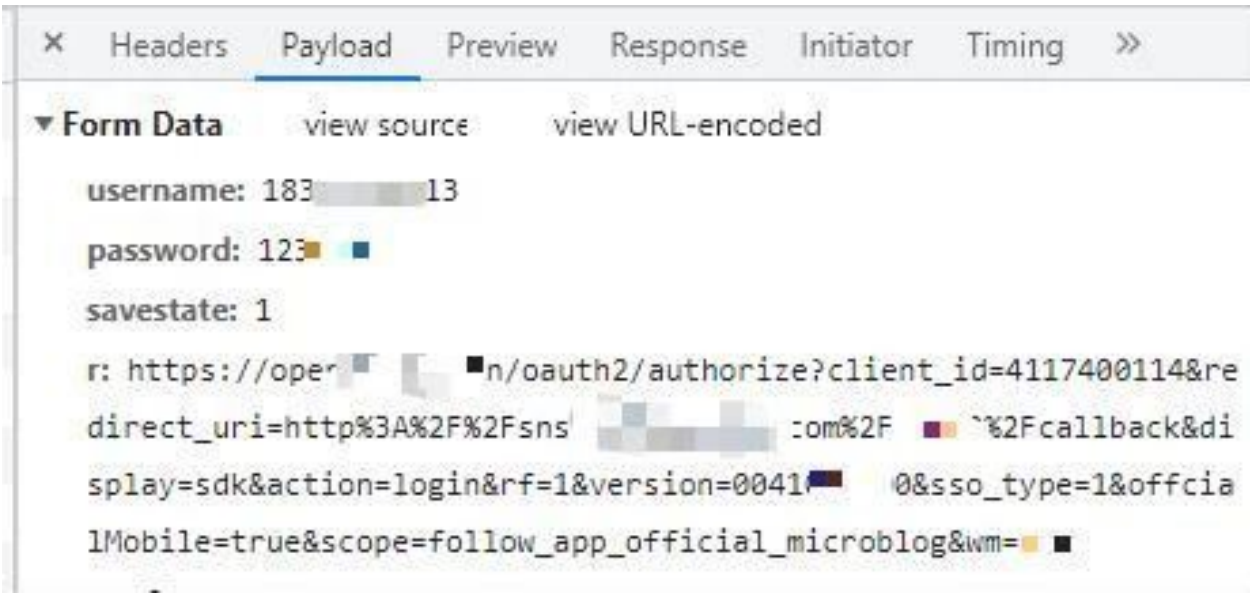
In 2022, the Threat Hunter Karma intelligence platform detected a large number of account scanning, credential stuffing and other attacks on social platforms, many of which involved groups of professional threat actors. Some large social platforms have been repeatedly attacked due to problems with their API interfaces, and account security incidents have occurred one after another.

Take the credential stuffing attack on a large social platform as an example:

In August 2022, the Threat Hunter Karma intelligence platform monitored that attackers launched a credential stuffing attack on a large domestic social platform and successfully stole the account passwords of many platform users. These account passwords are used by attackers to sell and profit, and are mainly used for pornography, gambling, fraud and traffic promotion, etc. Since most of them are accounts used by normal users for a long time and are not fake accounts registered in batches by threat actors, this increases the difficulty of platform governance.

From the attack traffic captured by the Threat Hunter honeypot, it was found that from August to October 2022, attackers used proxy IPs to launch attacks on the login API of a social platform more than 5 million times in total, stealing thousands of accounts. Through further analysis, it was found that the social platform has multiple login API interfaces. As shown in the figure below, the account

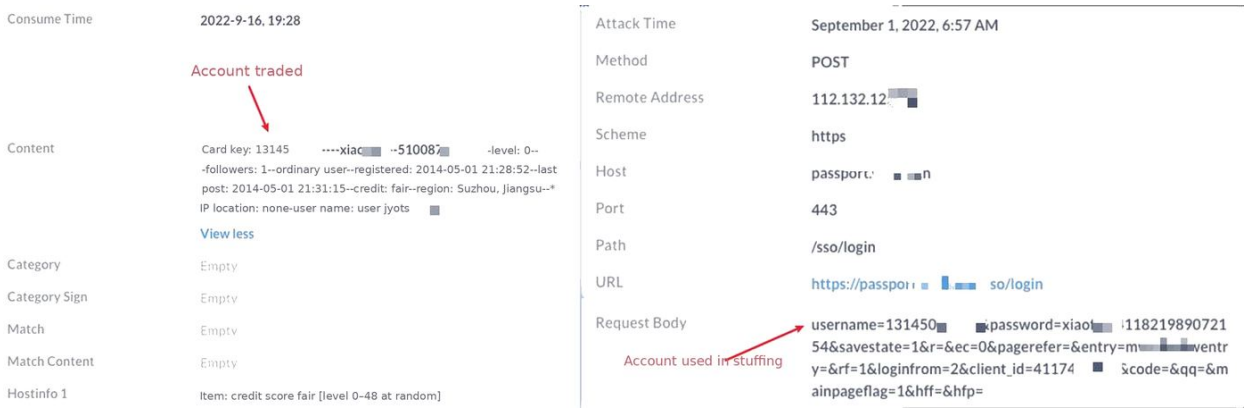
and password parameters in some login API interfaces are not encrypted and are transmitted in plain text. These login API interfaces have also become the main targets of credential stuffing attacks launched by threat actors.



Some login APIs send the account and password in clear text

Source: Threat Hunter original report, page 32. Original image retained.

From September to October 2022, the Threat Hunter Karma intelligence platform captured a total of more than 3,000 social accounts traded by threat actors through the card issuance platform. Through statistical research on the behavior of account sellers, it was found that the accounts captured by threat actors traded could be successfully matched with credential stuffing traffic, further confirming the behavior of threat actors stealing social accounts for transactions.



Accounts traded by threat actors match the accounts seen in credential-stuffing traffic

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

Safety advice:

1) Using the unified login API, unified management of login portals can be achieved, the attack surface can be reduced, security policies can be centrally controlled, and risks can be responded to in a timely manner;

2) The account number and password used to log in to the API must be encrypted before transmission, and the verification of strong and weak passwords must be strengthened;

3) Use human-machine identification such as verification codes. Although attackers will use CAPTCHA-solving services to bypass it, the continuously strengthened verification code strategies will increase the attacker's attack threshold.

4. There are loopholes in the API interface of the smart parking platform, and car owner information leaks occur frequently.

In recent years, the "smart parking" platform has been booming. After the parking lot is connected to the "smart parking" system, car owners can check and pay online by scanning the car with their mobile phone and entering the license plate number. While the smart parking platform brings convenience to the majority of car owners, business security issues are also gradually exposed.

A real case of an attacker using the "query API interface" to obtain the privacy of car owners:

Threat Hunter intelligence researchers discovered persistent attacks on multiple "smart parking" systems in the traffic monitored by honeypots. The attacked "smart parking platforms" basically cover most parking lots accessible to citizens. Through analysis, they found that the payment query API interfaces of these smart parking platforms all have "unauthorized access vulnerabilities", and attackers used this vulnerability to crawl a large amount of user parking information.

Smart parking apps attacked in several provinces and cities (partial list)

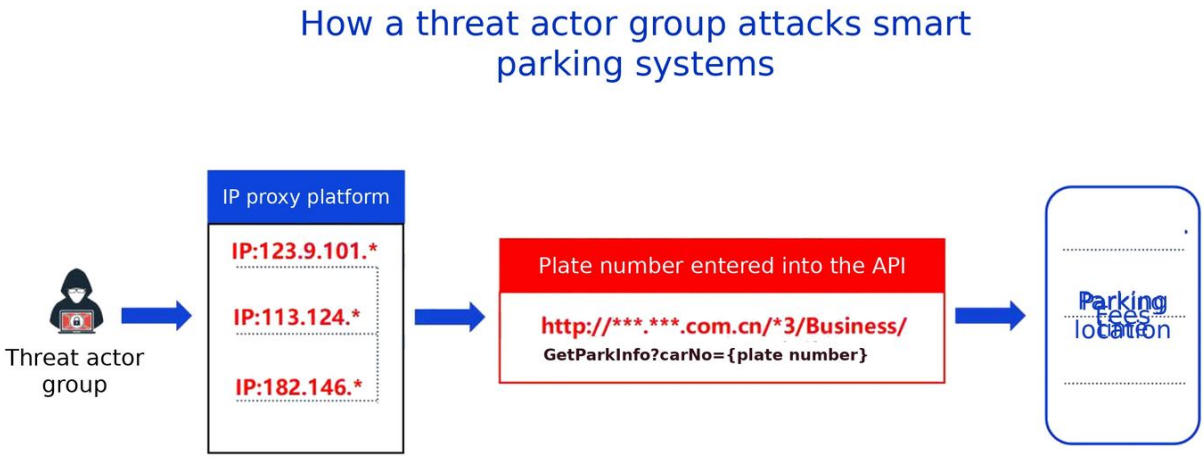
Tool	Company	Attacked API
A[redacted].exe	Shenzhen [redacted] Co., Ltd.	http://mops.[redacted]com.cn/v3/Bussiness/GetParkInfo
Re[redacted].exe	Guangxi [redacted] Technology Co., Ltd.	https://plate-[redacted]/plate
EP[redacted]a.exe	Shenzhen [redacted] Co., Ltd.	https://api.a[redacted]/gateway
Ha[redacted].exe	Beijing [redacted] Technology Co., Ltd.	http://www[redacted]/v1/api/parking/lookup?licence_plate
J[redacted].exe	Shenzhen [redacted] Holdings Co., Ltd.	https://s[redacted]com.cn/core-gateway/order/carno/pay/index
L[redacted].exe	Lanzhou [redacted] Operations Co., Ltd.	https://[redacted].com/parking_orders/wx_get_car_orders
T[redacted].exe	Wuhan [redacted] Technology Co., Ltd.	https://mpapi.[redacted]/kesb_req
X[redacted].exe	Zhejiang [redacted] Technology Co., Ltd.	https://u.[redacted]/parkingLot/getCurrentChargeBill
Yi[redacted].exe	Guangdong [redacted] Technology Holdings Co., Ltd.	https://wxy[redacted].xin/user/charge/charge/parkingCharge.do

Smart parking apps attacked in several provinces and cities (partial list)

Source: Threat Hunter original report, page 34. Table re-typeset in English from the original.

For further verification, Threat Hunter intelligence researchers analyzed one of the attacked smart parking platforms and found that threat actors obtained a large number of IPs through the IP proxy platform and conducted frequent and batch attacks on the query API interface of the smart parking platform.

The threat actors gang used this API flaw to input a license plate number arbitrarily, and without the authorization of the car owner, can query the vehicle's parking information for each period in the system, including entry time, entry location, entry photos and other information. While figuring out the driving trajectory of any vehicle, it can also "follow the clues" to obtain the owner's home address, phone number, work unit and other more private data.

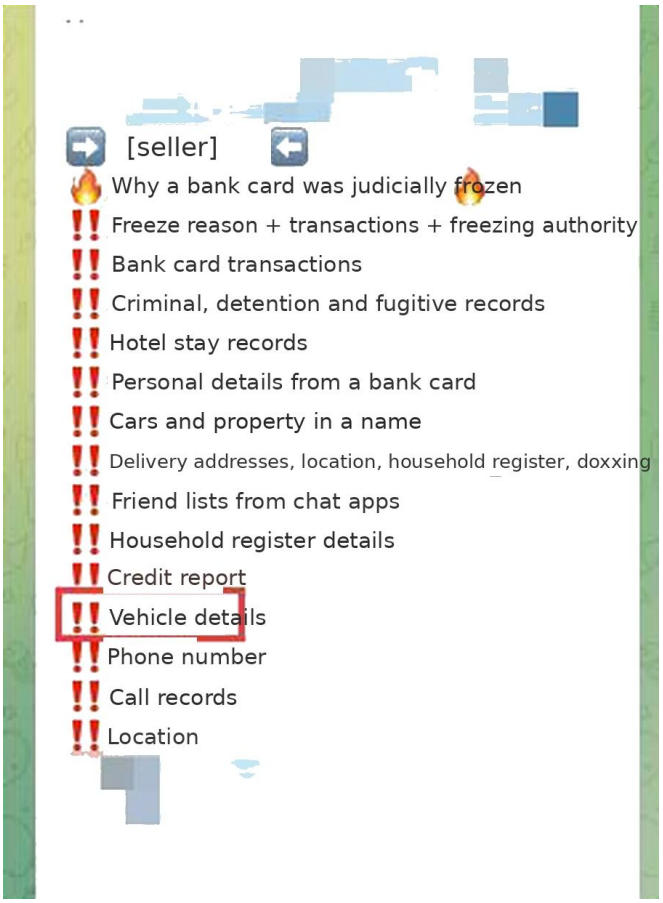


How a threat actor group attacks smart parking systems

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

threat actors make profits by selling information or providing location services through relevant channels. Car owners' information may be used for various purposes, ranging from having their accounts stolen to forging identities for loans, posing a threat to citizens' property security.

The Threat Hunter Intelligence Laboratory discovered that a group of threat actors provided vehicle information query services in an instant-messaging group:



A threat actor offers lookups including vehicle details and location

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

Safety advice:

1) The information interface that restricts vehicle parking requires identity verification first, such as binding a messaging-app account, phone number, etc. before querying;

2) Limit the frequency of interface queries. For example, no more than 2 license plate numbers can be queried for a single identity in a short period of time.

In the process of digital transformation and development, the actual problems faced by enterprises in network security management are far more than this, and the API attacks they encounter are also more complex and changeable. For enterprises, once a data leak occurs, they not only face economic losses and reputational losses, but also face legal risks and even more severe penalties. Combining API attack cases in different industries/scenarios, it can be seen that enterprises need to strengthen their own security construction, especially for API security construction.

Security advice

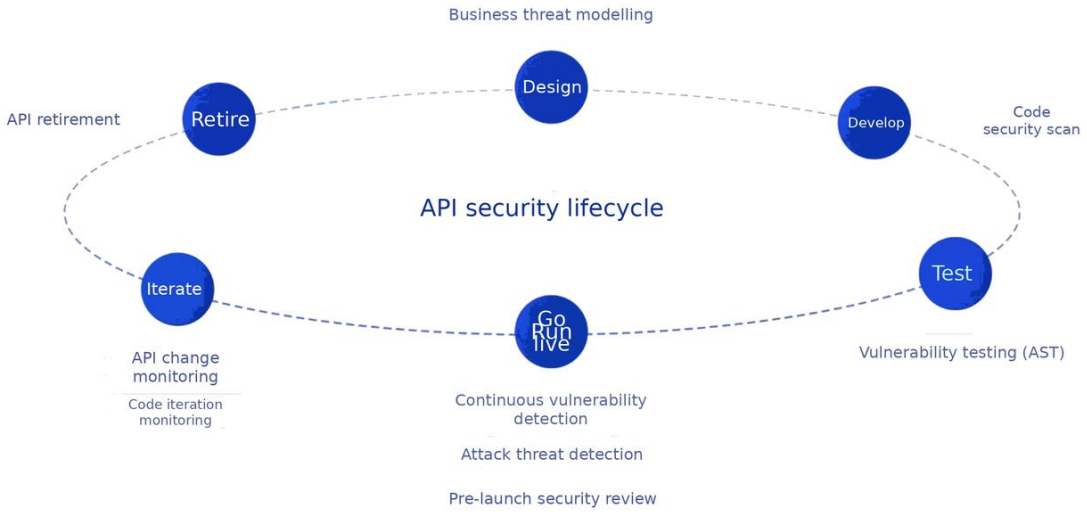
5. Safety Suggestions

In the face of constantly changing internal and external API attacks, how should enterprises identify the key to API security construction? Threat Hunter believes that "business first" is the prerequisite for enterprise development, and the enterprise's overall security construction should follow:

First, prioritize business; second, address visibility; third, achieve overall controllability.

On the basis of "business priority", Threat Hunter security experts recommend starting from the production operations stage of the API and conducting an overall combing of the online API and the data assets flowing on the API based on intelligence. The top priority is to achieve visibility of all API assets and flowing sensitive data, and then conduct continuous API defect assessment and attack threat awareness to achieve controllable API risks. From a business security perspective, this is also a prerequisite for the healthy development of enterprises.

Then, by shifting the security left, the perspective will shift to the design, development, testing and other stages before the API goes online, so as to better realize the full life cycle management of the API. In the process, combined with the summary of security practices after going online, it can be more targeted and avoid blind investment.

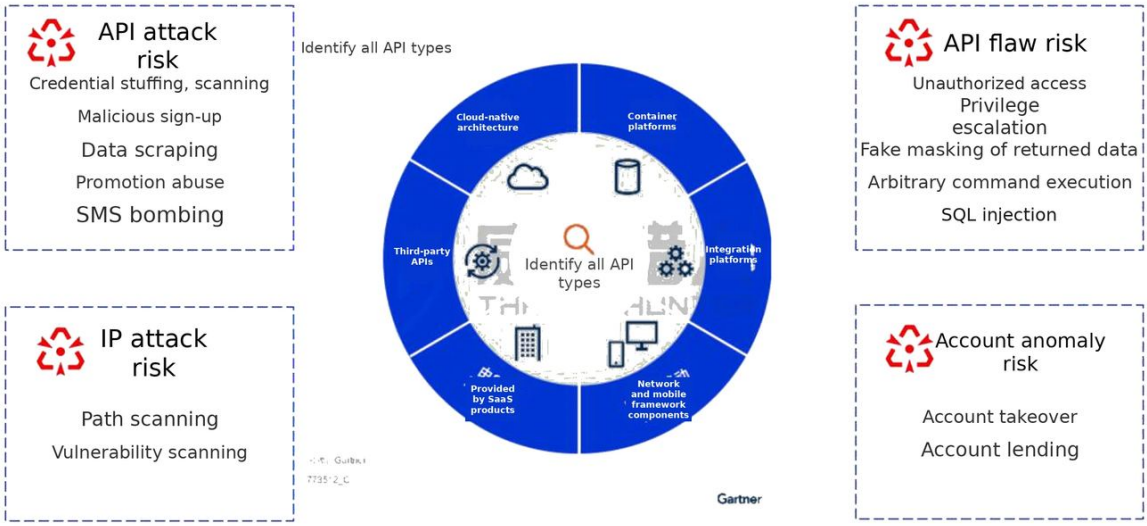


The API security lifecycle: security checks at each stage from design to retirement

Source: Threat Hunter original report, page 37. Original figure with Chinese text replaced by English.

According to research by a major cloud provider, companies with high API security maturity are far ahead in digital transformation compared to companies with low maturity. Clearly, technology leaders have realized the value that APIs bring, and API security ultimately needs to be part of an overall end-to-end security strategy.

API-centred, multi-dimensional risk discovery

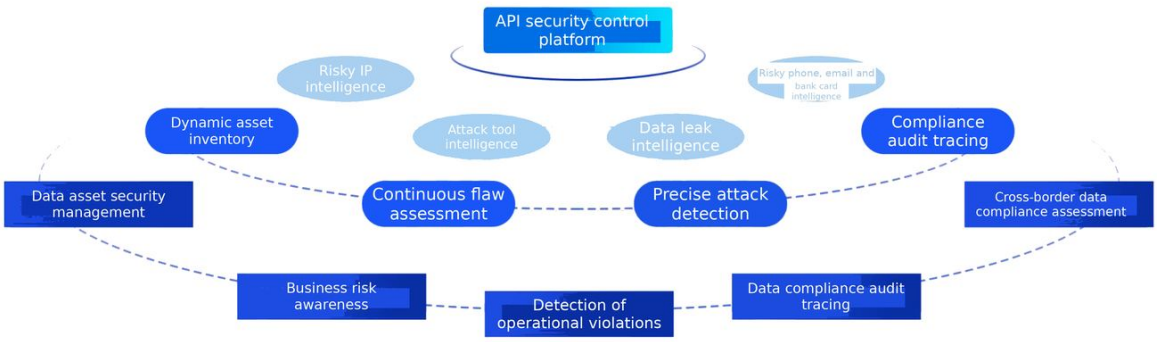


API-centred, multi-dimensional risk discovery

Source: Threat Hunter original report, page 38. Original figure with Chinese text replaced by English.

The Threat Hunter API security management and control platform fully integrates attack defense capabilities with AI intelligent data analysis capabilities. It builds a behavioral baseline for API access based on "intelligence" and is not affected by AI traffic fluctuations. It can quickly determine risk attack events on APIs, help enterprises comprehensively sort out API assets, prevent discovery and block API attacks, improve the response speed of risk events, prevent the leakage of mobile sensitive data, better protect the business and data security of enterprises, and build the cornerstone of digital security with intelligence.

Intelligence-driven API security control platform



Intelligence-driven API security control platform

Source: Threat Hunter original report, page 38. Original figure with Chinese text replaced by English.