The Internal Workings of the Chinese Cybercrime Ecosystem

spycloud.com/blog/deep-dive-chinese-cybercrime-ecosystem/

Kyla Cardona

October 18, 2024

“The data you leave on the internet knows you better than your mother.”
– A quote from a China-based blog on social engineering databases (SGK)
As we reported in a previous post about China-based threat actor TTPs, Chinese-language criminal actors have unique methods of data collection and aggregation that can give them extremely detailed pictures of individual targets. These actors offer data collection as a service, and then sell the exfiltrated data to competitors, hackers, data vendors, and the black market for further exfiltration and cyberattacks.

In this blog, we’ll take a deeper dive into the techniques China-based threat actors refer to as SDK and DPI, which they use to primarily target the mobile application supply chain and collect “fresh” data directly from the source. Additionally, we’ll take a closer look at SGKs, which house the exfiltrated data from the SDK and DPI collection methods as well as other hacked databases and can be queried to find detailed information about Chinese residents.

How Chinese-language actors advertise illicit data collection services

In our research, we have uncovered a range of different keywords that these actors use to advertise their data collection services on X, Telegram, and clearnet websites.

Terms used synonymously with SDK, DPI, and SGK

English Terms	Chinese Characters
First-hand data	一手数据
Primary data/First-hand data resources	一手数据资源
Fresh data	新鲜数据
Accurate data	精准数据
Real-time data	实时数据
Operator data	运营商数据
Operator big data	运营商大数据
Big data customer acquisition	大数据获客
Three network data	三网数据
Industry-wide data	全行业数据
Domestic data	国内数据
Online shopping data	网购数据
Human Flesh Search	查人 人肉搜索

These terms are used by China-based actors to sell breached data and hacking services, such as Distributed Denial-of-Service (DDoS) attacks, SMS hijacking, and DNS hijacking.

Vendors that advertise operator-related data services also appear to include marketing services that operate in a gray area, between legitimate services authorized by statute and those which would be best described as criminal in nature. These ‘marketing services’ that engage in illicit data collection in Chinese-speaking criminal communities share some similarities with Western pay-per-install (PPI) networks, which are popular services for malware distribution.

Breaking down the top Chinese-language actor TTPs

Let’s dive into the technical analysis of these TTPs:

- SDK

DPI

- SGK

SDK data collection method

In our last blog on Chinese cybercrime, we provided an overview of how Chinese actors are using Software Development Kits (SDKs) to steal massive amounts of user data that they can resell in criminal marketplaces.

▶

A quick recap on SDKs

The data collected and exfiltrated through the SDK method are mainly domestic (to China) personally identifiable information (PII) that includes full names, phone numbers, genders, ages, and location information. However, it varies based on the type of app, its intended audience, and other factors.

The information collected, extracted, and sold from the SDK exfiltration method may also include online behavior records (such as frequently used apps or visited websites), the users' contacts, and the user's personal account information from other applications installed on the mobile device. Criminals use this data for a variety of cyber attacks, especially online shopping and financial fraud.

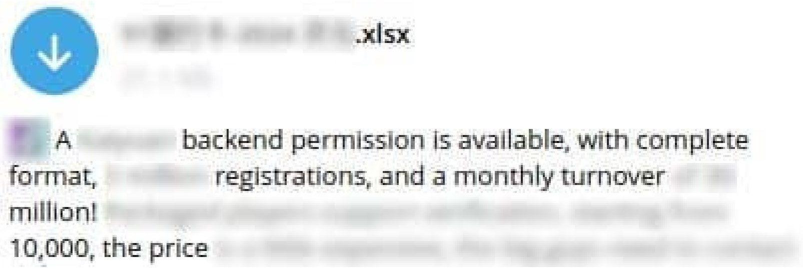
Threat actors usually post a list of the SDKs they have direct access to, which they refer to as a 'library.' For example:

Table 1: Example SDK Library

Alipay
Kuaishou Express
China Construction Bank
Postal Savings Bank of China
Douyin Express
Meituan
Ping An Guarantee, Personal Loan, Auto Finance
WeChat Business Bank
Everbright Futures
Guangzhou Futures
Chongqing Credit Loan

Table 1 shows a list of applications that China-based threat actors claim to have backend access to.

Based on the sheer breadth of persistent access that these malicious actors claim to have, we assess with moderate confidence that some of these actors are likely tainting and repackaging open source SDKs to add in vulnerable or malicious components. By repackaging popular development tools with their own malicious code, these actors are targeting the mobile application supply chain as a vector to harvest data from mobile end users.



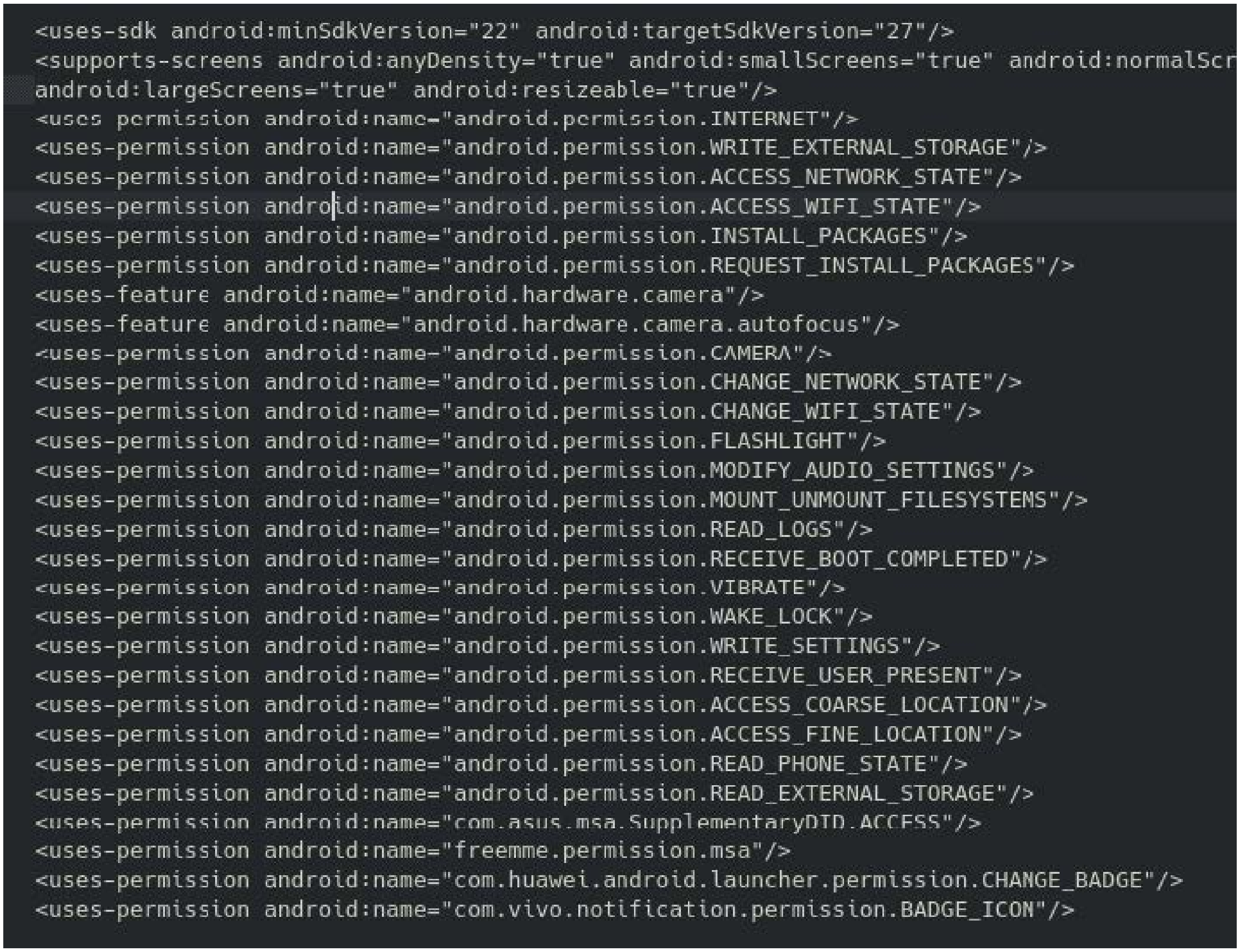
[redacted].xlsx

[redacted]

[redacted] A [redacted] backend permission is available, with complete
format, [redacted] registrations, and a monthly turnover [redacted]
million! [redacted]
10,000, the price [redacted]

Figure 1: A China-based threat actor providing a data leak file and advertising that backend permissions are available and other high quality data features.[1]

SpyCloud Labs researchers have conducted a static analysis of applications and have observed excessive permissions as shown below in Figures 2, 3, and 4.



```
<uses-sdk android:minSdkVersion="22" android:targetSdkVersion="27"/>
<supports-screens android:anyDensity="true" android:smallScreens="true" android:normalScr
android:largeScreens="true" android:resizeable="true"/>
<uses-permission android:name="android.permission.INTERNET"/>
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
<uses-permission android:name="android.permission.INSTALL_PACKAGES"/>
<uses-permission android:name="android.permission.REQUEST_INSTALL_PACKAGES"/>
<uses-feature android:name="android.hardware.camera"/>
<uses-feature android:name="android.hardware.camera.autofocus"/>
<uses-permission android:name="android.permission.CAMERA"/>
<uses-permission android:name="android.permission.CHANGE_NETWORK_STATE"/>
<uses-permission android:name="android.permission.CHANGE_WIFI_STATE"/>
<uses-permission android:name="android.permission.FLASHLIGHT"/>
<uses-permission android:name="android.permission.MODIFY_AUDIO_SETTINGS"/>
<uses-permission android:name="android.permission.MOUNT_UNMOUNT_FILESYSTEMS"/>
<uses-permission android:name="android.permission.READ_LOGS"/>
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
<uses-permission android:name="android.permission.VIBRATE"/>
<uses-permission android:name="android.permission.WAKE_LOCK"/>
<uses-permission android:name="android.permission.WRITE_SETTINGS"/>
<uses-permission android:name="android.permission.RECEIVE_USER_PRESENT"/>
<uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
<uses-permission android:name="android.permission.READ_PHONE_STATE"/>
<uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
<uses-permission android:name="com.asus.msa.SupplementaryDID.ACCESS"/>
<uses-permission android:name="freemme.permission.msa"/>
<uses-permission android:name="com.huawei.android.launcher.permission.CHANGE_BADGE"/>
<uses-permission android:name="com.vivo.notification.permission.BADGE_ICON"/>
```

Figure 2

In this instance, an application that is mainly used for venue and activity management is requesting excessive permissions, as noted in the manifest file.

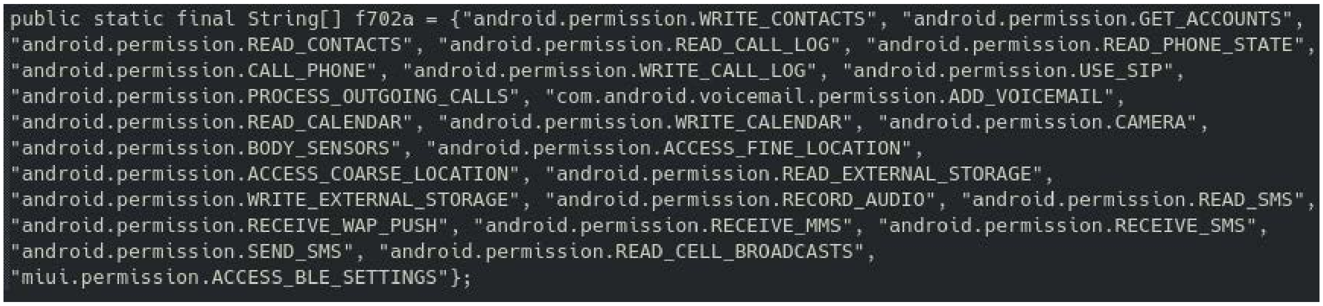
▶

These permissions include:

The same threat actor also shared data derived from an application made with this APK code, showing they were able to extract user information such as username, mobile information, login IP address, and registration IP address.

While these permissions may be essential for specific functionalities of the application and may be used individually based on the application's purpose, when combined, they can pose significant security risks.

The excessive permissions shown in Figure 3 and Figure 4 below are derived from an APK template shared between threat actors on a China-based hacker channel. The purpose of this APK is to provide pre-written base malicious code to hackers to embed in SDKs they develop.



```
public static final String[] f702a = {"android.permission.WRITE_CONTACTS", "android.permission.GET_ACCOUNTS",
"android.permission.READ_CONTACTS", "android.permission.READ_CALL_LOG", "android.permission.READ_PHONE_STATE",
"android.permission.CALL_PHONE", "android.permission.WRITE_CALL_LOG", "android.permission.USE_SIP",
"android.permission.PROCESS_OUTGOING_CALLS", "com.android.voicemail.permission.ADD_VOICEMAIL",
"android.permission.READ_CALENDAR", "android.permission.WRITE_CALENDAR", "android.permission.CAMERA",
"android.permission.BODY_SENSORS", "android.permission.ACCESS_FINE_LOCATION",
"android.permission.ACCESS_COARSE_LOCATION", "android.permission.READ_EXTERNAL_STORAGE",
"android.permission.WRITE_EXTERNAL_STORAGE", "android.permission.RECORD_AUDIO", "android.permission.READ_SMS",
"android.permission.RECEIVE_WAP_PUSH", "android.permission.RECEIVE_MMS", "android.permission.RECEIVE_SMS",
"android.permission.SEND_SMS", "android.permission.READ_CELL_BROADCASTS",
"miui.permission.ACCESS_BLE_SETTINGS"};
```

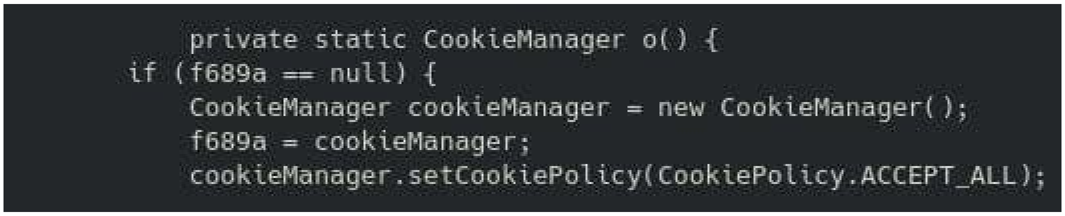
Figure 3: A sample of pre-written code designed to be embedded in SDKs to extract user data.

▶

The code in Figure 3 includes excessive permissions, as it provides access to:
Many of the permissions outlined in this template grant access to sensitive user data. When integrated into an application, these permissions could be used to collect and exfiltrate this information.

Moreover, access to personal data such as text messages, call logs, and contacts could be exploited by threat actors to track users, create and maintain highly accurate user profiles with behavioral data, and conduct phishing or other cyberattacks targeting the user's friends and family.

As previously mentioned, China-based threat actors claim that in China some applications require users to grant all requested permissions and those who decline are unable to use the application completely. Some companies justify this by claiming they may need the information in the future, even if it's not currently necessary. **However, it's crucial to remember that excessive permissions can pose significant security risks, increasing the potential for data collection, further exfiltration, and cyberattacks.**



```
        private static CookieManager o() {
    if (f689a == null) {
        CookieManager cookieManager = new CookieManager();
        f689a = cookieManager;
        cookieManager.setCookiePolicy(CookiePolicy.ACCEPT_ALL);
```

Figure 4: A sample of pre-written code designed to automatically accept all cookies on behalf of a user.

This code above sets the cookie policy of an application to accept all cookies. This raises security and privacy concerns, such as session hijacking, cross-site scripting, and data exfiltration:

- Session hijacking can occur if an application accepts all cookies indiscriminately. Injecting malicious cookies can lead to this type of cyberattack.

- Cross-site scripting can occur if an application accepts cookies without proper validation; a threat actor can inject malicious scripts to steal cookies and potentially exfiltrate data.

DPI (三网数据) data collection method

For China-based actors, DPI refers to more than just deep packet inspection – instead, it refers to a collaborative data collection method between China’s telecommunication operators, marketing companies, and malicious cyber threat actors and hackers.

DPI for these individuals and groups combines data aggregation, data enrichment, and data mining. This appears to take place through two main methods, which differ depending on whether or not the owners of a website or application consent to having this data collected from their users.

1. DPI data collection *with* user consent:

Some companies legally allow telecom companies to insert crawlers on their websites and capture visitor data for data collection and analysis. When this happens, marketing companies create user profiles (name, birthday, gender, region/location) for end users based on the IMEI and phone number they receive from the telecom operator.

User profiles generally include a person’s full name, date of birth, gender, email address, phone number, location, financial information, and internet behavior, such as frequently visited apps and websites. These profiles are made from behavioral modeling of a user’s online behavior.

2. DPI data collection *without* user consent:

When companies do not allow telecom operators to crawl their website, a more sophisticated and nefarious tactic is at play. Threat actors use insider access to telecommunications provider infrastructure to track when users visit certain webpages. When a customer approaches a criminal data seller to request data about users of an application or website that is not already listed on the TA’s SDK/DPI library, the actor will ask the customer to find the exact target URLs that they want to buy data for.

In our research into these groups, we found a step-by-step tutorial for these customers to show them how to extract their desired target URLs for mobile application traffic, as seen on Figure 5. In this tutorial, they use the Telerik Fiddler debugging tool for mobile applications to capture application web traffic and generate the exact URLs of the account creation and login pages of the targeted application. The malicious actors provide their customers with a Bill of Lading form that includes the target URLs, quantity of records, gender, location, and other fields to filter the data if desired by the customer. After this form is submitted to the sales agent, it is then submitted to the insider agent, who claims to have access to view the data traffic through network monitoring methods. The direct translation of how they refer to this traffic monitoring is inside the “screening” or “computer” room.

When the insider agents who allegedly work for telecom operators are informed of the target URLs, they proceed to collect visitor traffic on the URLs. However, they may be limited to observing the IMEI of the mobile phone number(s) that belong to their telecom company. The telecom companies are able to match IMEIs with user profiles of customers and their network IP addresses when they are accessing the internet.

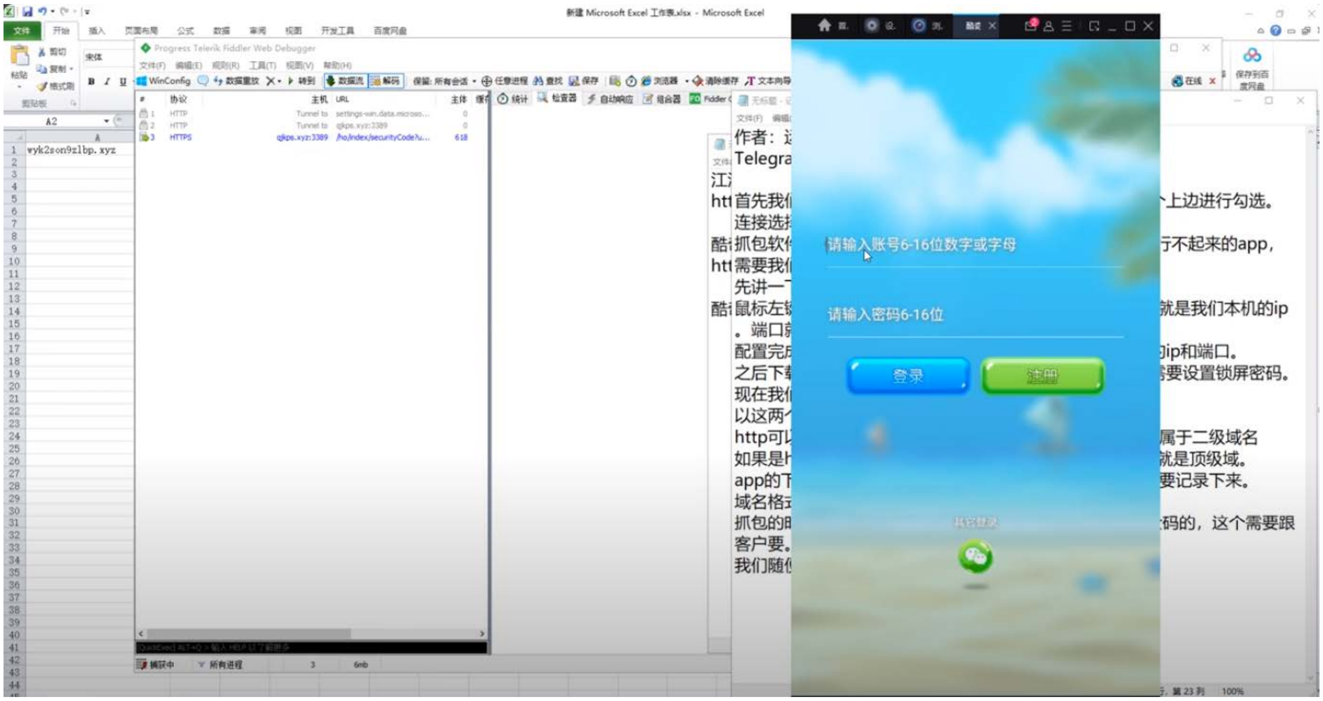
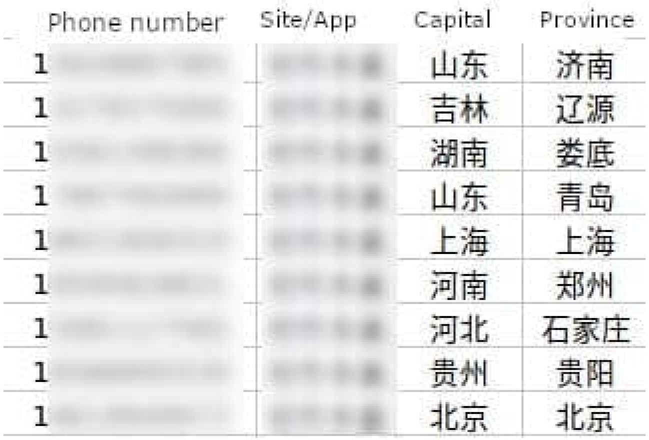

新建 Microsoft Excel 工作表.xlsx - Microsoft Excel
Progress Telerik Fiddler Web Debugger
wyk2son9zlbp.xyz
HTTPS
/ho/index/securityCode?u...
请输入账号6-16位数字或字母
请输入密码6-16位
登录
注册

Figure 5: A China-based Telegram actor's step-by-step tutorial on how to extract their desired target URL using Telerik Fiddler and Mumu.



Phone number	Site/App	Capital	Province
1[redacted]	[redacted]	山东	济南
1[redacted]	[redacted]	吉林	辽源
1[redacted]	[redacted]	湖南	娄底
1[redacted]	[redacted]	山东	青岛
1[redacted]	[redacted]	上海	上海
1[redacted]	[redacted]	河南	郑州
1[redacted]	[redacted]	河北	石家庄
1[redacted]	[redacted]	贵州	贵阳
1[redacted]	[redacted]	北京	北京

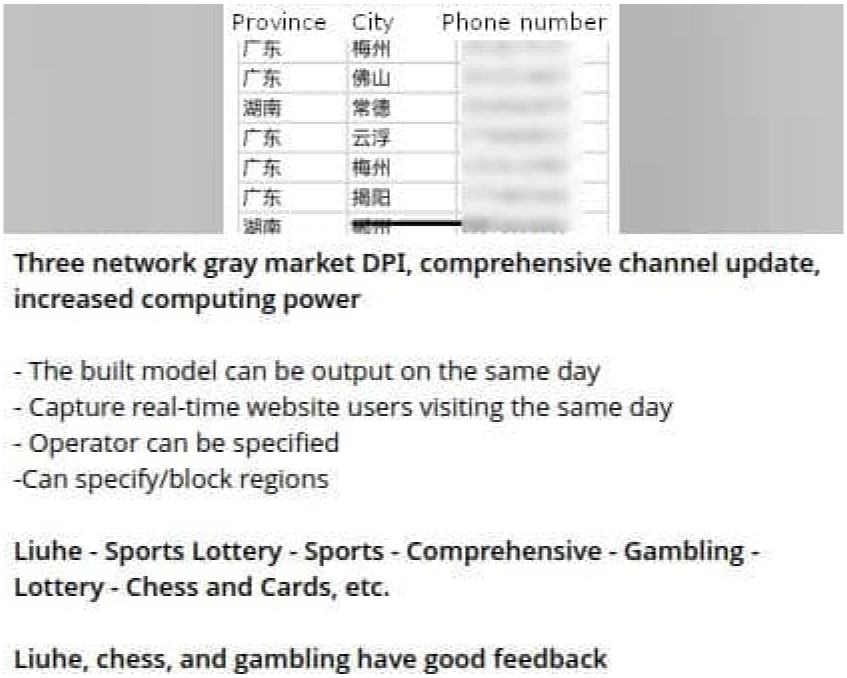
Figure 6: A sample of data extracted using the DPI method.

For example, let's say a Chinese citizen named Zhang Wei (张伟) who has a phone with the IMEI number XXXX is visiting example[.]com on September XX, 2024. The telecom operator can see that Zhang is visiting this website on their network traffic logs. To obtain additional information such as a user profile on Zhang, they are able to match the IMEI number to the associated mobile phone number. Marketing companies can then match the mobile phone number to a comprehensive user profile. Some data brokers also allegedly claim to have assistance from insiders for some mobile phone manufacturers. This assistance may come in the form of providing IMEI numbers and also having pre-installed and trojanized applications.

In short, mobile phone users' traffic is monitored by telecom companies. The telecom operators then communicate with marketing and third-party services to enrich the collected data based on a user's IMEI to build a more robust user portrait. If all other methods fail, malicious actors also offer their "penetration services" against targeted apps or websites.

These data brokers market their services to potential customers by claiming that if they don't give their sales staff highly detailed data on their clients, they are sending them into battle without equipping them with "swords to fight." [A] According to one data seller, "the integration of the three networks [China's telecom operators] and operator big data [marketing companies] will make it easier, cheaper, and more accurate to acquire customers, thereby increasing a company's sales." [B] Additionally, they flaunt that they are "always adding onto their data models," meaning that they are always adding more sources to their SDK/DPI 'libraries'. These data brokers will "establish models on the behaviors of users accessing or registering on websites, apps, receiving verification codes, and calling 400 numbers[2]," allowing their customers – both businesses marketing their products and social engineers trying to defraud users – to meet their goals.

The DPI data exfil method is referred to as highly timely, as orders can be processed the same day or by the next day and is also highly accurate because the data is collected via direct monitoring of users.



Province	City	Phone number
广东	梅州	[redacted]
广东	佛山	[redacted]
湖南	常德	[redacted]
广东	云浮	[redacted]
广东	梅州	[redacted]
广东	揭阳	[redacted]
湖南	~~郴州~~	[redacted]

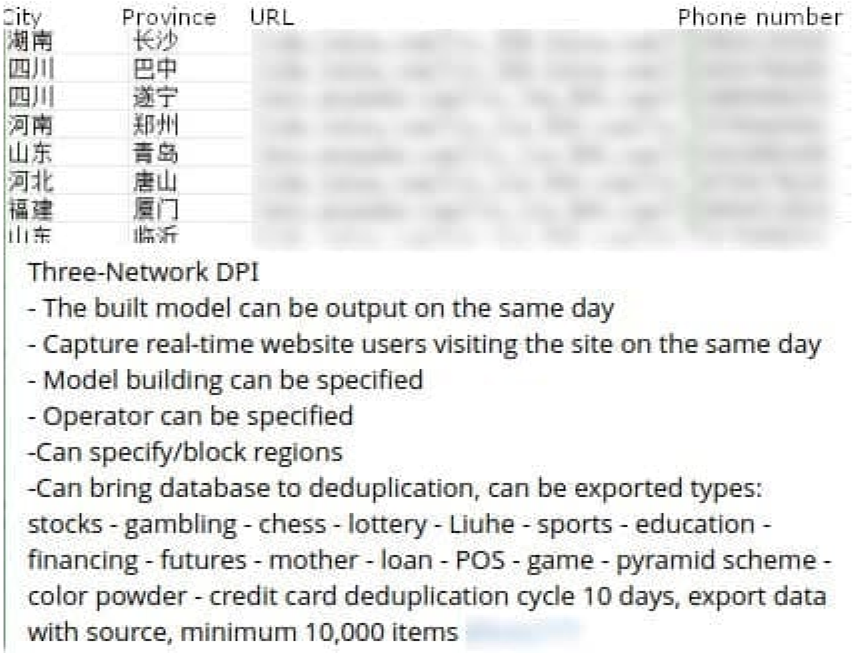
Three network gray market DPI, comprehensive channel update, increased computing power

- The built model can be output on the same day
- Capture real-time website users visiting the same day
- Operator can be specified
-Can specify/block regions

Liuhe - Sports Lottery - Sports - Comprehensive - Gambling - Lottery - Chess and Cards, etc.

Liuhe, chess, and gambling have good feedback

Figure 7 shows a China-based Telegram actor's data leak channel advertising DPI data for sale with high quality features of data extraction.[3]



City	Province	URL	Phone number
湖南	长沙	[redacted]	[redacted]
四川	巴中	[redacted]	[redacted]
四川	遂宁	[redacted]	[redacted]
河南	郑州	[redacted]	[redacted]
山东	青岛	[redacted]	[redacted]
河北	唐山	[redacted]	[redacted]
福建	厦门	[redacted]	[redacted]
山东	临沂	[redacted]	[redacted]

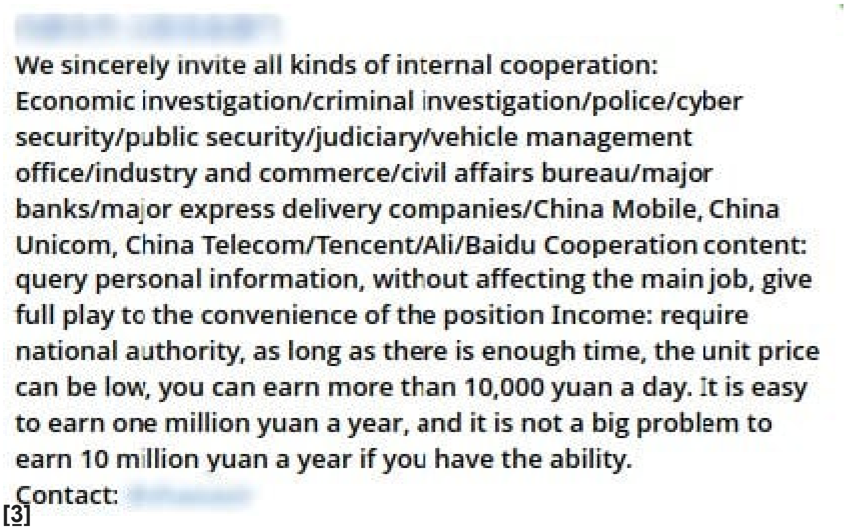
Three-Network DPI
- The built model can be output on the same day
- Capture real-time website users visiting the site on the same day
- Model building can be specified
- Operator can be specified
-Can specify/block regions
-Can bring database to deduplication, can be exported types: stocks - gambling - chess - lottery - Liuhe - sports - education - financing - futures - mother - loan - POS - game - pyramid scheme - color powder - credit card deduplication cycle 10 days, export data with source, minimum 10,000 items [redacted]

Figure 8 shows a China-based Telegram actor's data leak channel advertising DPI data for sale with high quality features of data extraction, deduplication, and industries that data can be extracted from. [3]

Recruiting techniques:

SpyCloud Labs analysts have also observed Chinese-language cybercriminal actors post public recruitment ads for 'internal cooperation' personnel as shown on Figure 9 and 10.

In one of these posts, an actor states that, their "most profitable projects include those with access to bank statements, judicial freezing, room sharing, WeChat, QQ, call records, those in the Public Security Bureau, and those who work in public banks," as seen on Figure 10. They claim to operate under a "professional gray monetization service, and distribute commissions earned from inquiries [orders] through virtual currency." They also promise to coach new 'internal cooperation personnel' through how to avoid risks of being caught as well as how to mix and withdraw virtual currency.

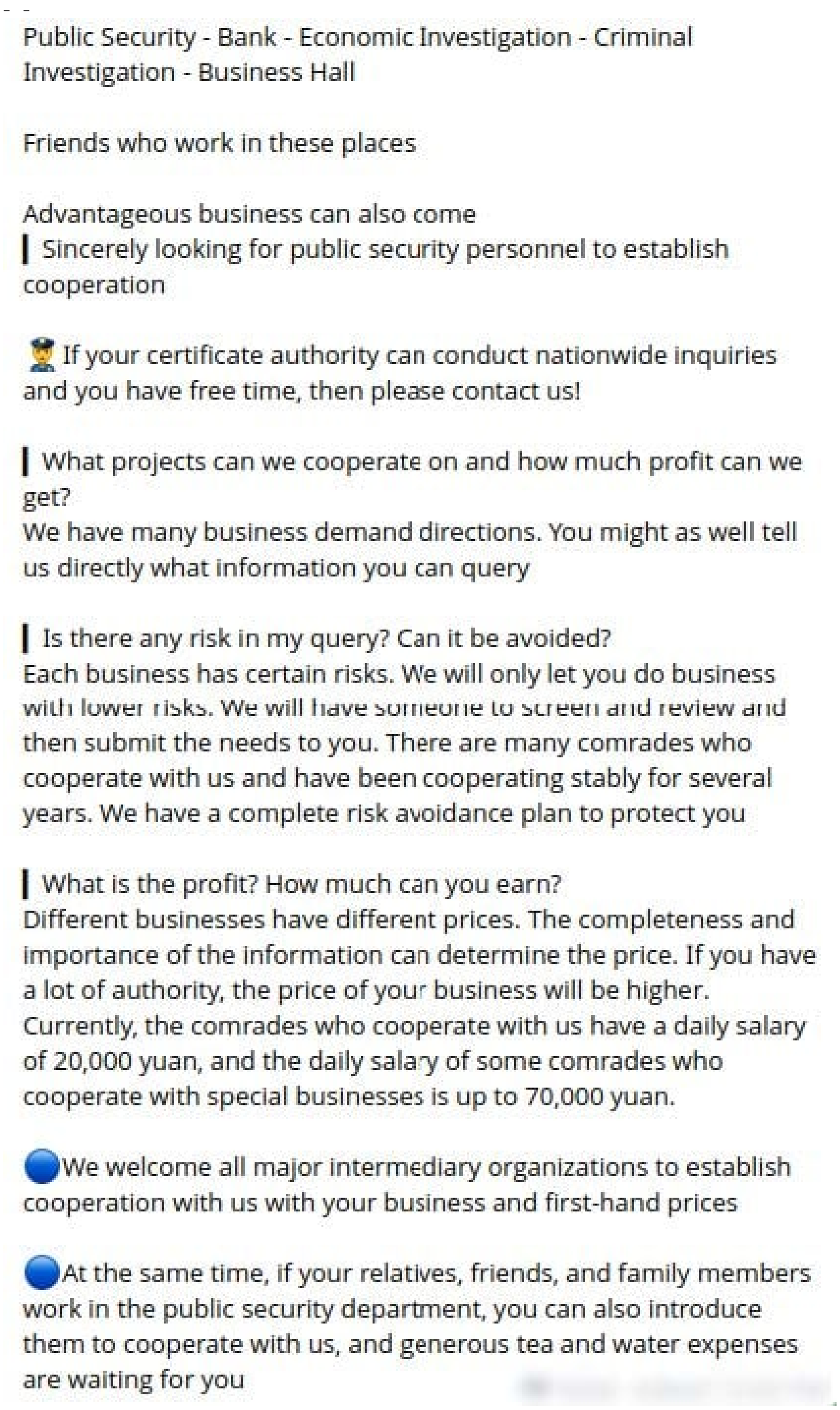


[redacted]

We sincerely invite all kinds of internal cooperation: Economic investigation/criminal investigation/police/cyber security/public security/judiciary/vehicle management office/industry and commerce/civil affairs bureau/major banks/major express delivery companies/China Mobile, China Unicom, China Telecom/Tencent/Ali/Baidu Cooperation content: query personal information, without affecting the main job, give full play to the convenience of the position Income: require national authority, as long as there is enough time, the unit price can be low, you can earn more than 10,000 yuan a day. It is easy to earn one million yuan a year, and it is not a big problem to earn 10 million yuan a year if you have the ability.

Contact: [redacted]

[3]



Public Security - Bank - Economic Investigation - Criminal Investigation - Business Hall

Friends who work in these places

Advantageous business can also come
▍Sincerely looking for public security personnel to establish cooperation

👮If your certificate authority can conduct nationwide inquiries and you have free time, then please contact us!

▍What projects can we cooperate on and how much profit can we get?
We have many business demand directions. You might as well tell us directly what information you can query

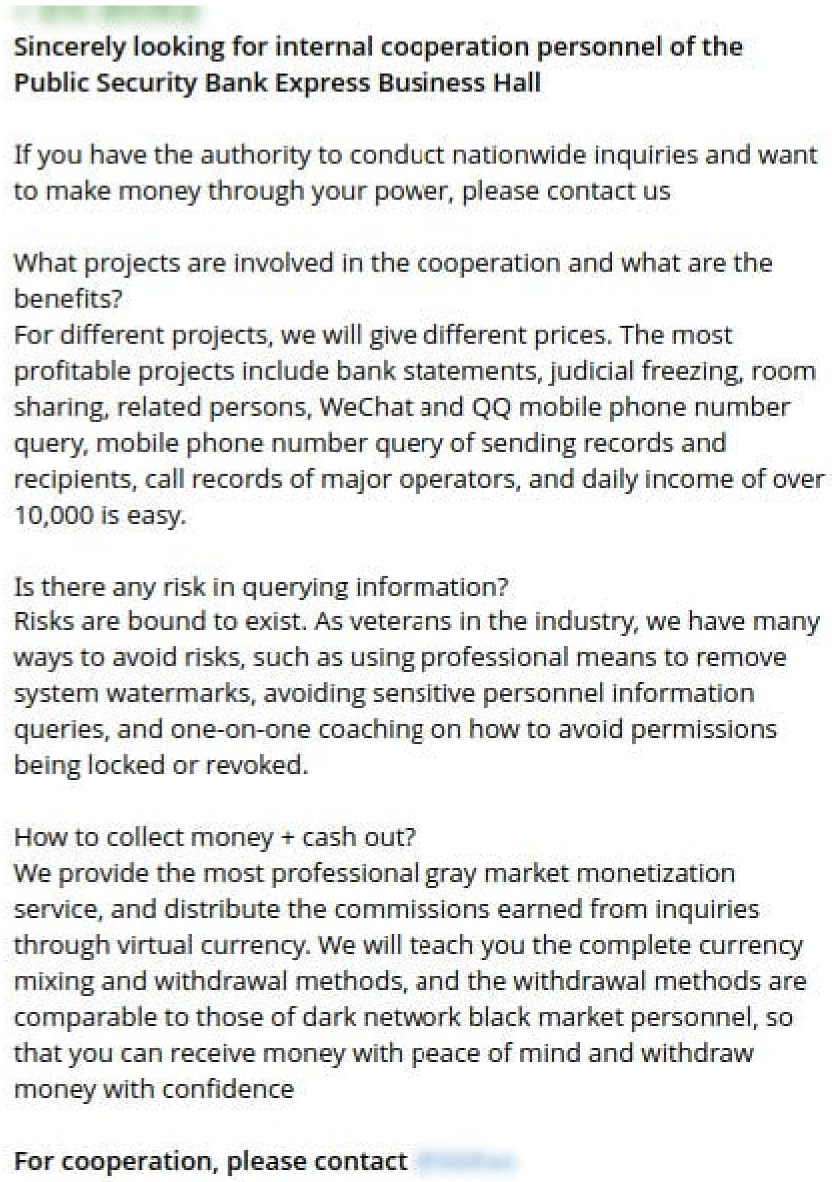
▍Is there any risk in my query? Can it be avoided?
Each business has certain risks. We will only let you do business with lower risks. We will have someone to screen and review and then submit the needs to you. There are many comrades who cooperate with us and have been cooperating stably for several years. We have a complete risk avoidance plan to protect you

▍What is the profit? How much can you earn?
Different businesses have different prices. The completeness and importance of the information can determine the price. If you have a lot of authority, the price of your business will be higher. Currently, the comrades who cooperate with us have a daily salary of 20,000 yuan, and the daily salary of some comrades who cooperate with special businesses is up to 70,000 yuan.

🔵We welcome all major intermediary organizations to establish cooperation with us with your business and first-hand prices

🔵At the same time, if your relatives, friends, and family members work in the public security department, you can also introduce them to cooperate with us, and generous tea and water expenses are waiting for you [redacted]

Figure 10 shows a China-based Telegram channel recruiting agents for the cybercrime industry. [3]



[redacted]

Sincerely looking for internal cooperation personnel of the Public Security Bank Express Business Hall

If you have the authority to conduct nationwide inquiries and want to make money through your power, please contact us

What projects are involved in the cooperation and what are the benefits?
For different projects, we will give different prices. The most profitable projects include bank statements, judicial freezing, room sharing, related persons, WeChat and QQ mobile phone number query, mobile phone number query of sending records and recipients, call records of major operators, and daily income of over 10,000 is easy.

Is there any risk in querying information?
Risks are bound to exist. As veterans in the industry, we have many ways to avoid risks, such as using professional means to remove system watermarks, avoiding sensitive personnel information queries, and one-on-one coaching on how to avoid permissions being locked or revoked.

How to collect money + cash out?
We provide the most professional gray market monetization service, and distribute the commissions earned from inquiries through virtual currency. We will teach you the complete currency mixing and withdrawal methods, and the withdrawal methods are comparable to those of dark network black market personnel, so that you can receive money with peace of mind and withdraw money with confidence

For cooperation, please contact [redacted]

Figure 11 shows A China-based Telegram channel recruiting agents for the cybercrime industry. [3]

Social Work Library (SGK 社工库)

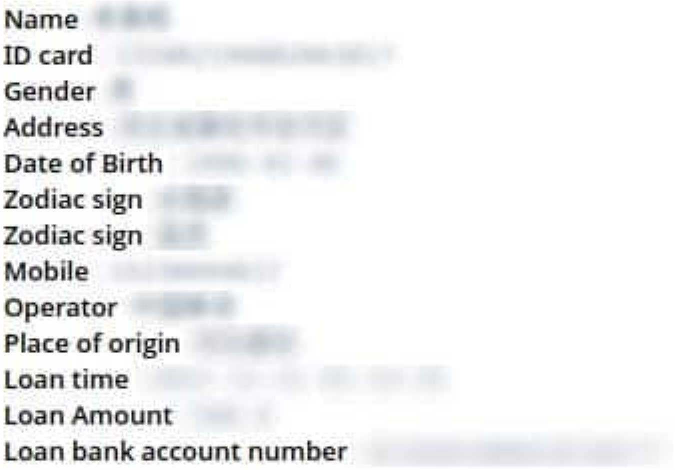
Social Work Library is referred to as *SGK* because the translation of the term is *‘Shègōng kù.’* It is also commonly referred to as a social engineering database, social worker database, and human flesh search.

This database is a repository of leaked PII, created by Chinese-language threat actors that compile hacked and leaked databases. Some are fully public, while others require engaging with an actor to gain access.

These libraries generally contain basic information on individuals such as their name, national ID number, and photo, and they may also contain additional PII like place(s) of residence, place(s) of work, business trips (past and future), place(s) of travel, income level, shopping habits, movies watched, restaurants visited, purchases made, and other behavioral data.

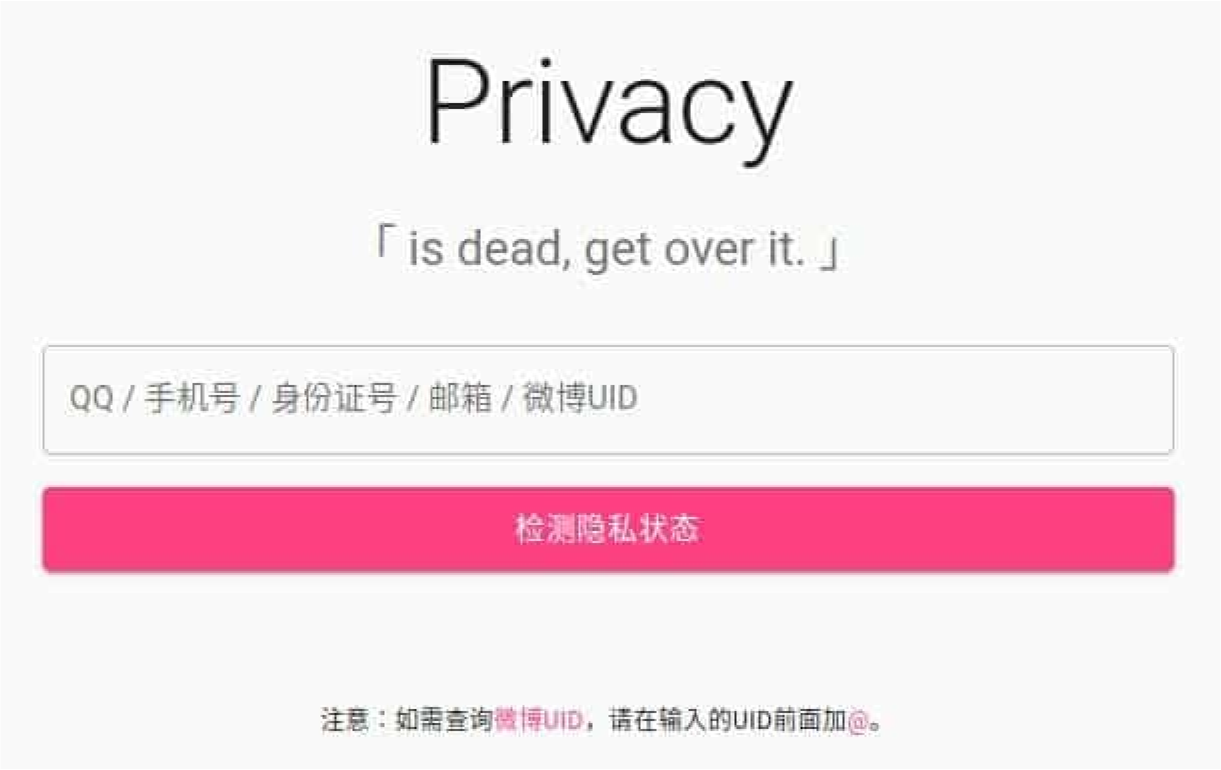
SGK libraries can paint a highly accurate “user portrait” for malicious actors, which enable them to create profiles on targets. These types of libraries are referred to as “social engineering” databases by threat actors because with the amount of fine detail found in these libraries, actors can more convincingly use social engineering methods to commit fraud, phishing, and other forms of cyberattacks targeting individuals and their employers.

The China-based actors host SGK libraries on clearnet websites and Telegram channels, and the data that can be found therein include, general PII, banking or other financial information, social media data, residency information, and travel and lodging information.



Name	[redacted]
ID card	[redacted]
Gender	[redacted]
Address	[redacted]
Date of Birth	[redacted]
Zodiac sign	[redacted]
Zodiac sign	[redacted]
Mobile	[redacted]
Operator	[redacted]
Place of origin	[redacted]
Loan time	[redacted]
Loan Amount	[redacted]
Loan bank account number	[redacted]

Figure 14 shows a China-based SGK query with detailed PII results. [3]

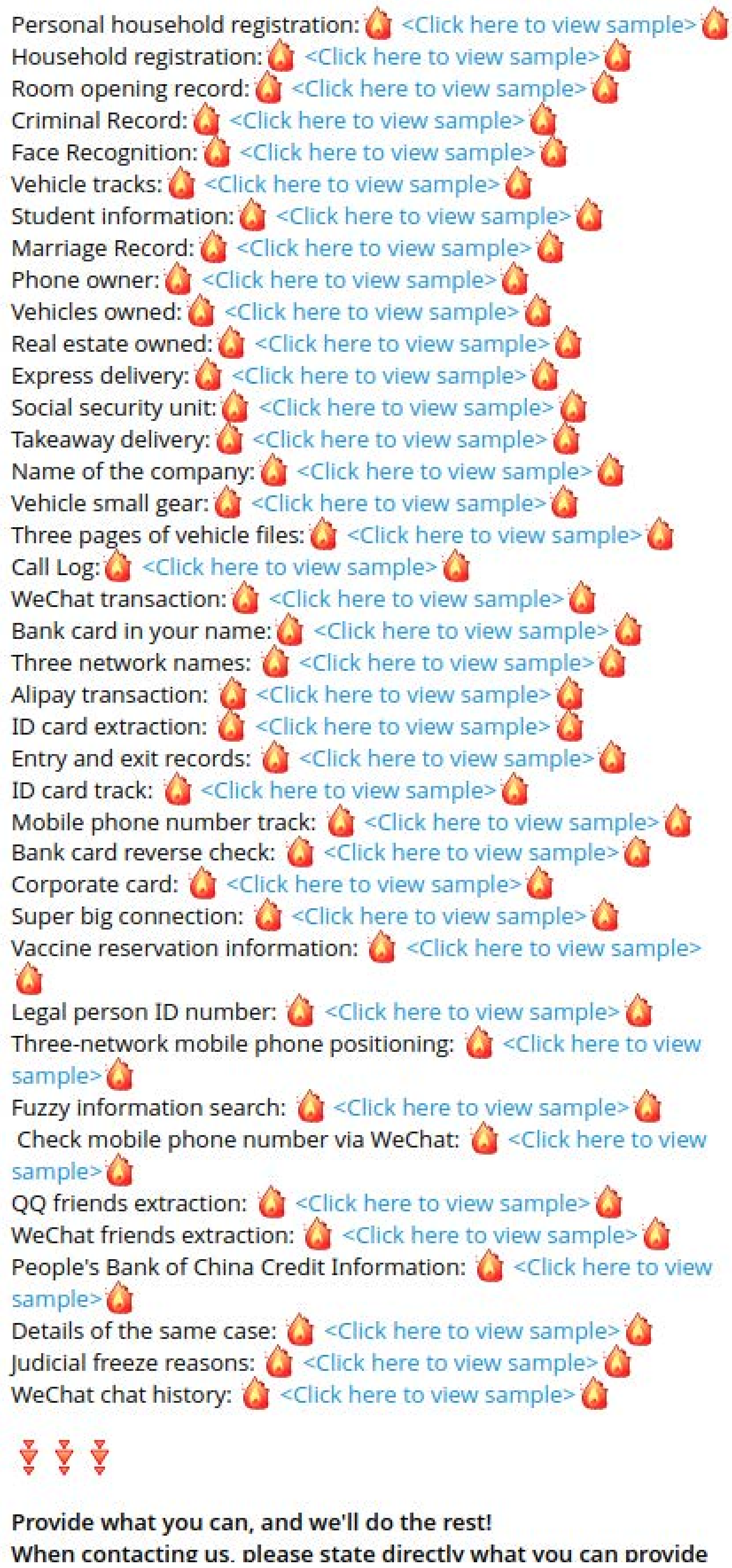


Privacy

「is dead, get over it.」

注意：如需查询微博UID，请在输入的UID前面加@。

Figure 12 shows an SGK clearnet website that can be queried through QQ numbers, mobile phone number, national ID number, email address, or Weibo ID.



Personal household registration:🔥 <Click here to view sample>🔥

Household registration:🔥 <Click here to view sample>🔥

Room opening record:🔥 <Click here to view sample>🔥

Criminal Record:🔥 <Click here to view sample>🔥

Face Recognition:🔥 <Click here to view sample>🔥

Vehicle tracks:🔥 <Click here to view sample>🔥

Student information:🔥 <Click here to view sample>🔥

Marriage Record:🔥 <Click here to view sample>🔥

Phone owner:🔥 <Click here to view sample>🔥

Vehicles owned:🔥 <Click here to view sample>🔥

Real estate owned:🔥 <Click here to view sample>🔥

Express delivery:🔥 <Click here to view sample>🔥

Social security unit:🔥 <Click here to view sample>🔥

Takeaway delivery:🔥 <Click here to view sample>🔥

Name of the company:🔥 <Click here to view sample>🔥

Vehicle small gear:🔥 <Click here to view sample>🔥

Three pages of vehicle files:🔥 <Click here to view sample>🔥

Call Log:🔥 <Click here to view sample>🔥

WeChat transaction:🔥 <Click here to view sample>🔥

Bank card in your name:🔥 <Click here to view sample>🔥

Three network names: 🔥 <Click here to view sample>🔥

Alipay transaction: 🔥 <Click here to view sample>🔥

ID card extraction: 🔥 <Click here to view sample>🔥

Entry and exit records: 🔥 <Click here to view sample>🔥

ID card track: 🔥 <Click here to view sample>🔥

Mobile phone number track: 🔥 <Click here to view sample>🔥

Bank card reverse check: 🔥 <Click here to view sample>🔥

Corporate card: 🔥 <Click here to view sample>🔥

Super big connection: 🔥 <Click here to view sample>🔥

Vaccine reservation information: 🔥 <Click here to view sample> 🔥

Legal person ID number: 🔥 <Click here to view sample>🔥

Three-network mobile phone positioning: 🔥 <Click here to view sample>🔥

Fuzzy information search: 🔥 <Click here to view sample>🔥

Check mobile phone number via WeChat: 🔥 <Click here to view sample>🔥

QQ friends extraction: 🔥 <Click here to view sample>🔥

WeChat friends extraction: 🔥 <Click here to view sample>🔥

People's Bank of China Credit Information: 🔥 <Click here to view sample>🔥

Details of the same case: 🔥 <Click here to view sample>🔥

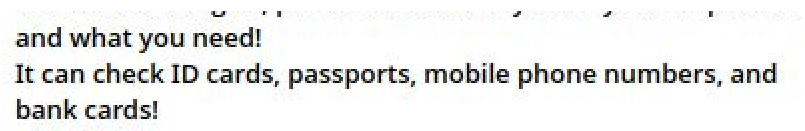
Judicial freeze reasons: 🔥 <Click here to view sample>🔥

WeChat chat history: 🔥 <Click here to view sample>🔥

⏬ ⏬ ⏬

Provide what you can, and we'll do the rest!

When contacting us, please state directly what you can provide



and what you need!
It can check ID cards, passports, mobile phone numbers, and bank cards!

[3]

Summary of research findings

The intricacy of Chinese cybercrime TTPs is both unique and highly effective for threat actors. Here are some of the things that set it apart and that should be kept on the security community's radar:

- **China-based threat actors are targeting the mobile application supply chain**. SpyCloud Labs researchers have observed excessive permissions in SDK applications being used to exfiltrate user data. These actors have constant uploads of library lists of SDKs they claim to have backend access to.

DPI is a collaborative data collection method involving several players. It combines the access of China's telecommunication providers with marketing companies and malicious cyber actors to collect, aggregate, and enrich PII data.

- **Chinese-language cyber actors are recruiting insiders**. They are constantly seeking to collaborate with and leverage the access of personnel from the Public Security Bureau and Public Banks for profitable projects in the gray/black market industry.

- **Stolen user profiles are highly accurate and can be queried through SGKs**. Due to the constant data collection through SDK and DPI methods, user profiles contain more than PII- they contain behavioral records that are perpetually updated and can be used by malicious actors to create profiles on their targets.

Our team at SpyCloud Labs continues to monitor the Chinese-language threat actor community and will provide new research as we uncover it in additional blogs.
Read more from SpyCloud Labs
See new research