THREAT HUNTER RESEARCH

Fraud Risks in China's Consumer Subsidy Program

A focused investigation into merchant abuse and transaction manipulation targeting China's consumer subsidy program.

Original publication: 2025-05-22
Research team: Threat Hunter Research Team
Source report: 19 pages

Original report text

This text version is reconstructed based on the 19-page original PDF, retaining the report narrative, chapters and research scope; the cover, duplicate table of contents and purely decorative pages are not repeated. Localized figures are placed in context throughout this web edition, with the original PDF retained for reference.

About Threat Hunter

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

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

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

01The cybercrime ecosystem chain under the supervision of “state subsidies”

02. Various roles in the national subsidy industry chain exploit the advantages of national subsidy

Benefit method analysis and case presentation

03. Conclusion

Directory

Preface

Starting from 2024, the national subsidy policy for the trade-in of consumer goods, hereinafter referred to as the "national subsidy" policy, will be fully implemented in the three major fields of automobiles, digital products, and home appliances to promote consumption upgrades, energy conservation, and emission reduction. The activity subsidies are significant, such as a 20,000 yuan subsidy for new energy vehicles and a 15% subsidy for digital products, covering multiple online e-commerce platforms and physical brand stores.

Behind the policy dividends, there are also behaviors of profiteering from subsidies; in order to prevent cybercrime ecosystem from taking profits from subsidies, the state and participating platforms (e-commerce, express delivery) have simultaneously launched a number of anti-scalper measures, including users needing to meet real-name purchase, purchase limit of 1 item, personal signature activation and other conditions, and through technical means such as qualification code binding, order invoice matching, SN code verification and signature, restricting cybercrime ecosystem and illegal users from obtaining off-site subsidy qualifications, and increasing their resale profit costs.

Despite this, some cybercrime ecosystem still bypass supervision and implement arbitrage through fine division of labor and role collaboration, forming a mature industrial chain, invading the preferential rights and interests of normal consumers on major platforms, and seriously damaging the fair ecology of the platform.

Threat Hunter is based on long-term investigations and research on the "consumer subsidy" industry chain, combined with relevant data, and strives to accurately and objectively demonstrate the current malicious activity status and behavior patterns of cybercriminal groups use of the "consumer subsidy" industry chain.

01The cybercrime ecosystem chain under the supervision of “state subsidies”

1.1 Overview of the industrial chain

Under the supervision of the "state-approved" policy, the Threat Hunter intelligence platform still detected cybercrime ecosystem profiting from state-approved vulnerabilities. cybercriminal groups use various methods such as illegal acceptance of joint couriers, resale of qualifications, illegal verification operations, counterfeit recycling orders for arbitrage, recruiting individuals to recycle national subsidy, and other methods to obtain the preferential state subsidy.

These techniques involve multiple roles, including cybercrime ecosystem, merchants and individual users, specifically involving fraud users, resale qualified users, merchants, agents, scalpers, couriers, etc. These roles cooperate with each other to bypass national subsidy areas and user supervision through purchasing, forwarding, activation, etc., forming a complex chain of interests.

The points and methods of profit-making through multi-role collaboration are as follows:

1.2 Digital home appliances have become the hardest hit area for sales of state-subsidized goods

Threat Hunter has compiled statistics on the types of products related to China's national consumer subsidy program sold in the cybercrime ecosystem trading market. The top product categories with the highest transaction popularity are: digital products, home appliances, and lifestyle products. Accounting for 59.11%, 28.95% and 11.07% respectively.

Digital and home appliance products have become the main target of cybercrime ecosystem reselling for profit due to their high unit prices and strong subsidies (the maximum subsidy is 1,000 yuan for digital products and 2,000 yuan for home appliances). In contrast, lifestyle products have little profit potential, and it is difficult to resell cars. At the same time, the demand for digital and home appliances is highly elastic and price-sensitive. National subsidies stimulate demand, and cybercriminal groups use low-price discounts and multiple discount qualifications to attract consumers to make profits.

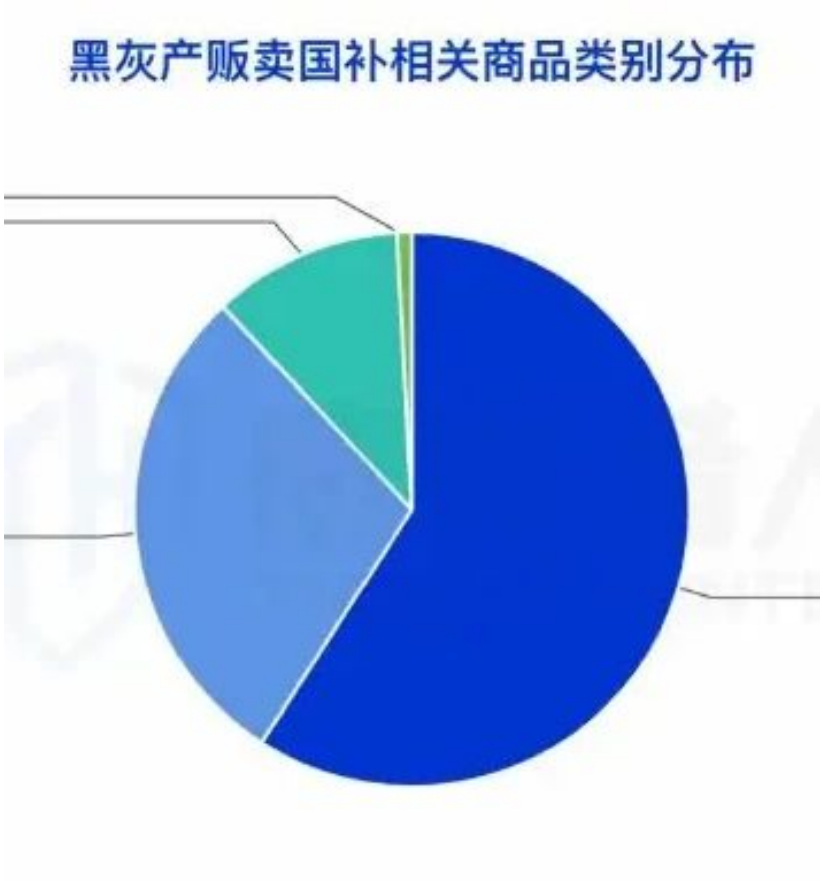
These factors work together to make digital and home appliances the hardest hit areas for cybercrime ecosystem arbitrage.

1.3 Main distribution areas of cybercrime ecosystem selling consumer subsidy products top 3: Guangzhou, Shanghai, Beijing

Threat Hunter researchers analyzed the registration locations of individual cybercrime ecosystem stores selling consumer subsidy products on major trading platforms and found that cybercrime ecosystem stores selling consumer subsidy products are mainly distributed in Guangzhou, Shanghai, Beijing, Shenzhen and other areas.

Digital household electricity products become areas of serious national commodity trafficking (figure 1)

Source: Threat Hunter original report, page 6



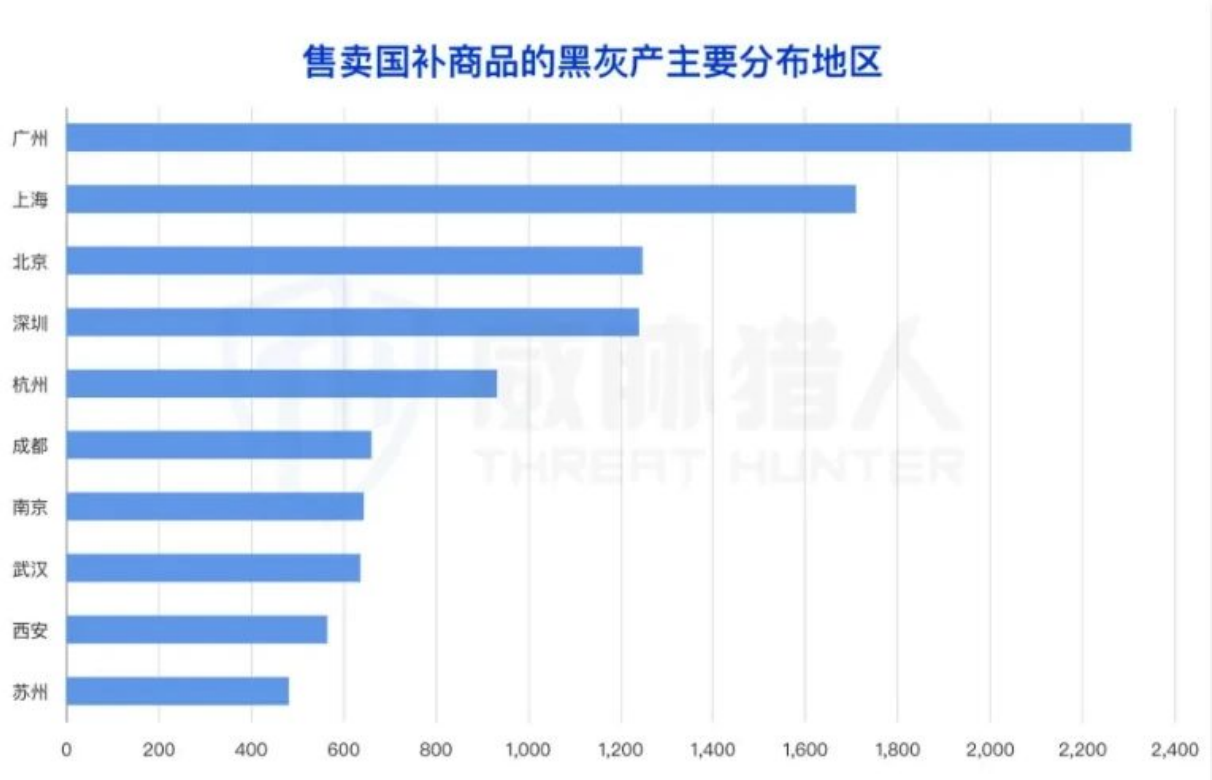
Digital household electricity products become areas of serious national commodity trafficking (figure 2)

Source: Threat Hunter original report, page 6

1.4 The main source channels for selling consumer subsidy products are the two leading domestic e-commerce platforms.

Note: The content of the following report has been desensitized (relevant e-commerce platforms are designated by A, B, C, etc.), and the "internal publication" version will be synchronized for customers who have cooperated. Threat Hunter collects statistics on the source and channel information of the consumer subsidy products sold by cybercrime ecosystem from the capture cycle sample data. Among them, 82.93% of the consumer subsidy products come from the two leading domestic e-commerce platforms.

1.5 cybercriminal groups publishes advertisements in forums and social media and then diverts traffic to the private domain to complete transactions



Source of national by-products and distribution of cybercriminal activity (Chart 1)

Source: Threat Hunter original report, page 7

Source of national by-products and distribution of cybercriminal activity (Chart 2)

Source: Threat Hunter original report, page 7

Threat Hunter monitored the discussion channels surrounding the risks related to “purchasing, forwarding, cashback, and recycling” of state subsidies. Forums and social media were the main active channels for threat actors; forum channels accounted for 52.45%, and social media channels accounted for 35.85%.

cybercriminal groups publishes advertisements in forums or social media, directing users to private domains for detailed exchanges and transactions.

Threat Hunter researchers further analyzed and found that the main reasons why forums and social media are the main active channels for cybercriminal groups are:

The portraits of users using forums and social media are highly overlapped with the target group of consumer subsidy products, and the form of information release is flexible and concealed, such as disguising it as a 'money-saving guide' or diverting traffic to private domains through QR codes, which can effectively avoid platform review.

cybercrime ecosystem products were diverted to private areas after the forum and the media advertised.

Source: Threat Hunter original report, page 8

At the same time, the forum’s old accounts, hot posts, and social media’s algorithm recommendations and the ‘big V’ effect also provide trust endorsement and dissemination convenience for these illegal information, greatly reducing the cost of cybercriminal groups' traffic and improving the recruitment success rate.

02 Analysis and case studies on the methods used by various actors in the state subsidy industry chain to obtain preferential state subsidy. Under such strict policy supervision, cybercriminal

groups can still exploit the "loopholes" of state subsidy. How do the various actors cooperate with each other to bypass the state subsidy supervision and successfully obtain state subsidy?

The following are typical behavior patterns of each role

2.1 Analysis of scalper group techniques

Threat Hunter research found that scalpers use social media to recruit users who are qualified to sell state subsidies, recycle the state subsidies, and allow couriers to collaborate to bypass supervision. They mainly use the following characteristics:

- Diversion and recruitment: cross-regional collaboration and supervision are difficult
- Cash on delivery: collaborative courier supervision is bypassed
- Temporary dispatch of orders to group chat and group settlement: high concealment

2.1.1 Scalpers summon users to collect China's national consumer subsidy programary products to share cases

Scalpers convene "trading national subsidy-qualified users" on social media, forums and other social platforms, divert traffic to a temporary WeChat group, and fill in the real names and phone numbers of the selling-qualified users in accordance with the scalpers' requirements. The delivery address is selected from the address database provided by the scalpers, and orders are placed via cash on delivery.

On the surface, this is a commonly used recycling method, but in fact, scalpers team up with the "consignee" - that is, the courier to illegally inspect and accept the equipment for express delivery, bypassing policy supervision and recycling the national subsidy. In order to avoid monitoring, scalpers divide order dispatch and settlement into groups, disbanding old groups within 1 to 2 days and reopening new groups to continue placing orders, which increases the difficulty of supervision.

After the scalper signs for the receipt, the order-receiving user enters the scalper-specific statement group chat and provides a screenshot of the signed receipt and the courier order number for settlement.

2.2 Analysis of merchant fraud techniques

Threat Hunter research found that under the national subsidy regulatory policy, some merchants will still cooperate with consumers to implement arbitrage even though they are aware of the violations. Merchants mainly profit from the following characteristics:

- Remote verification/false trade-in: taking advantage of policy loopholes to avoid supervision

Cows gather users for national commodity case sharing
Source: Threat Hunter original report, page 10

- Social media traffic: hashtag topic group traffic, high consumption rate, merchants assist fraud methods, generally divided into two situations: physical-store merchants and online dealers:

1) Physical merchants remotely activate someone other than themselves to increase product sales
2) Online dealers and agents fabricate the trade-in process to defraud double subsidies

2.2.1 Case sharing of merchants assisting users in fraud to obtain nationally supplemented products 1) Remote activation by merchants not in person

In accordance with the national subsidy supervision policy, the normal process of purchasing national subsidy in physical stores requires the purchaser to be present with his or her ID card information, and the store merchant will verify that the identity is consistent and the machine will be inspected and activated on the spot. However, some merchants remotely allow buyers to scan codes to activate the device through WeChat videos, and then deliver it to the purchasing user's address by express delivery. to bypass regulation

2) Agents take advantage of the triple discount of national subsidies. According to research, some online dealers use the "triple discount" to sell national subsidy products at low prices to increase sales and obtain double profits.

The "triple discount" for distributors includes:

1. Normal state subsidies for individual users

2. National subsidy trade-in subsidy discount

National commodity off-site activation links (Chart 1)

Source: Threat Hunter original report, page 12

National commodity offshore activation links (Chart 2)

Source: Threat Hunter original report, page 12

3. Agents provide platform coupons

In addition, some dealers cheat in the "trade-in" process and falsely recycle old products, allowing users to enjoy the subsidy without providing any old product recycling certificate when choosing the "trade-in" subsidy.

In addition, agents revealed that if users need to purchase products with national subsidy in other places, they can find "gunners" (i.e. users in remote areas with national subsidy and whose qualifications for national subsidy are idle) to place orders on their behalf, thereby bypassing the restriction of national subsidy IP regions. Users only need to click this operation and then complete the transaction through the agent channel.

2.3 Analysis of individual users' violation methods

Research by Threat Hunter intelligence staff found. In the scenario of "consumer subsidy fraud", more and more real users are making malicious profits by studying and using the "legitimate" rules of platform business. Among them, the following characteristics are mainly used to make profits:

- Couriers collaborate to "forward": taking advantage of policy loopholes to avoid supervision

Businesses assisting users in fraudulent national commodity case sharing 1)

Source: Threat Hunter original report, page 13

- Personal information purchasing on behalf of individuals: supervision is difficult

2.3.1 Case sharing of individual users selling/fraud to obtain national subsidy products 1) Users make profits by selling personal national subsidy qualifications

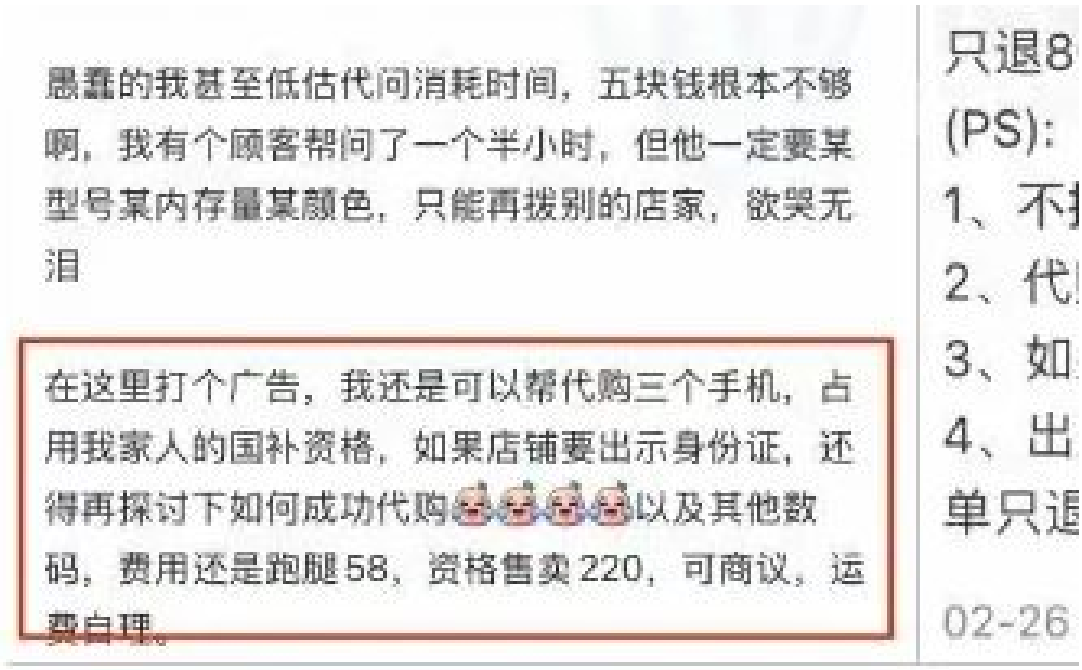
Some individual users publish recruitment information through active social platforms and resell their or their family members' qualifications for national subsidy in physical stores, placing orders for national subsidy equipment and verification equipment as themselves or their family members, and finally delivering them to the address of the person in need by mail. This will charge a certain qualification fee and legwork fees.

2) Users cooperate with couriers to "forward" to bypass supervision. In addition, in order to obtain multiple national subsidy discounts, some users actively participate in off-site subsidy arbitrage and provide identity information to cooperate with verification. They also communicated with the courier and forwarded the goods to bypass the country's regional restrictions on subsidy. Some users deliberately look for courier companies that can forward their shipments, and then use forwarding to bypass regional restrictions.

There is also a special participant in the industry chain of swindling state subsidies - the couriers in the area. As mentioned above, they play a key role in bypassing the regional restrictions on state subsidies. They are responsible for helping users activate products and assist users in forwarding, and finally deliver the goods to the real owner's address.

03 Conclusion During the implementation of the consumer subsidy policy, although the state and platforms have taken a number of anti-scalper measures, the cybercrime ecosystem still exploits loopholes to obtain subsidies through refined division of labor and collaboration, seriously damaging the fair market ecology.

Faced with this problem, all parties need to continue to update their understanding of cybercrime ecosystem malicious activity, and continuously strengthen supervision and technical means to better maintain a fair market environment and ensure that subsidy policies truly benefit consumers.



(a) Individual user trafficking/false enrichment sharing 1)

Source: Threat Hunter original report, page 16

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

(a) Individual users who sell/false goods to the State for profit (Chart 1)

Source: Threat Hunter original report, page 17

Individual users trafficking/false-seeking national commodity case sharing 1)

Source: Threat Hunter original report, page 17