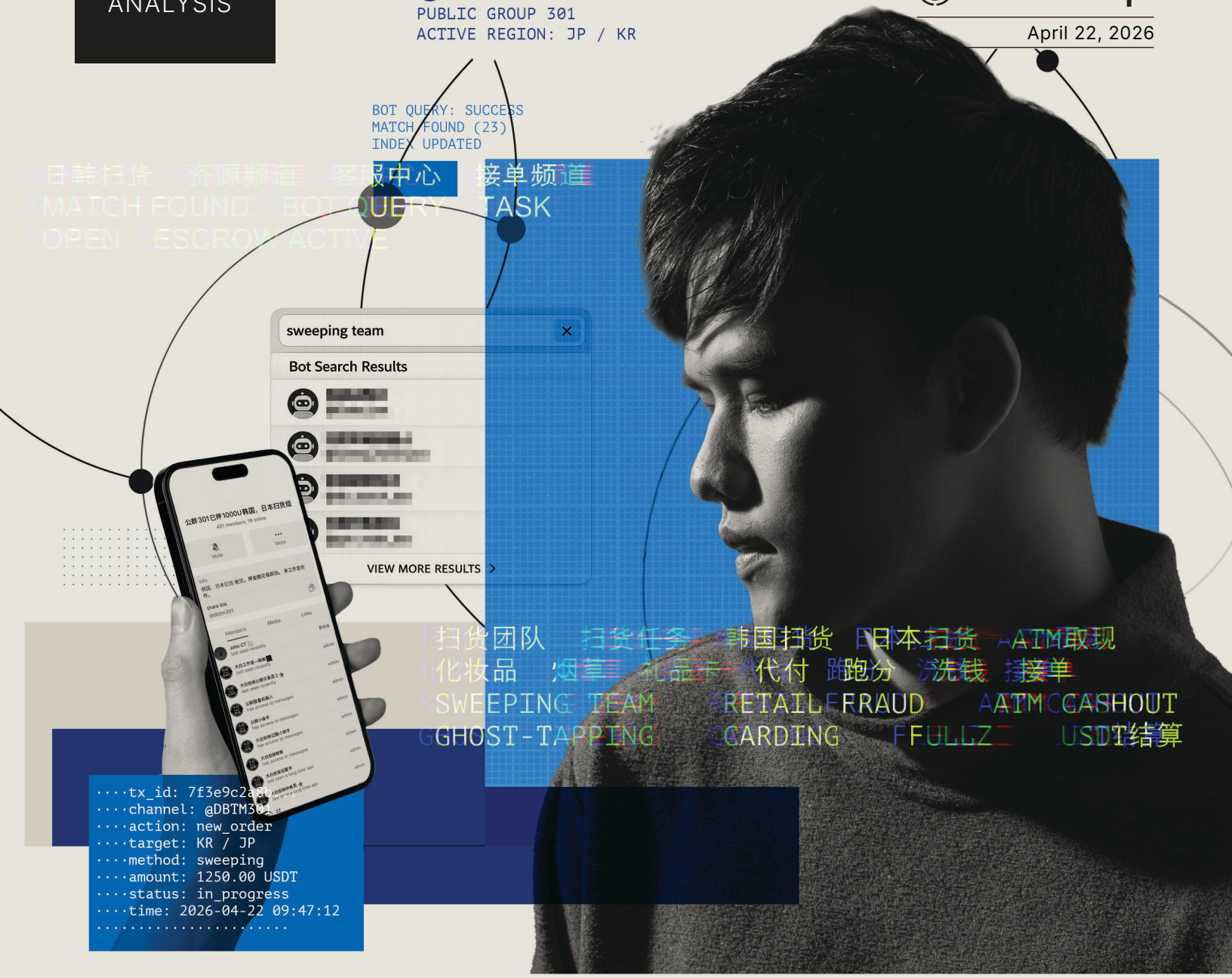
CYBER THREAT ANALYSIS

Recorded Future®

Insikt Group®

April 22, 2026



Evolution of Chinese-Language Guarantee Telegram Marketplaces

Guarantee marketplaces serve as conduits for Chinese-speaking threat groups with strong presences across multiple countries to coordinate and launch global-scale fraud and cybercriminal campaigns.

Dabai Guarantee uses bot and human customer support agents to redirect and match cybercriminal groups to the types of campaigns they wish to participate in, and to threat actors with similar activities.

Dabai Guarantee's Public Group 301 demonstrated its capability to coordinate different Chinese-speaking criminal groups for ghost-tapping operations in Japan and South Korea.

Executive Summary

Chinese-language, Telegram-based "guarantee" marketplaces are increasingly popular among Chinese-speaking criminal groups despite the widely publicized shutdown of Huione Guarantee in 2025. Although these guarantee marketplaces operate similarly to Huione Guarantee, they differ in their focus on particular aspects of cybercrime and in their targeting of specific geographies. To better understand these Chinese-language guarantee marketplaces, Insikt Group observed and analyzed another increasingly popular guarantee marketplace, dubbed Dabai Guarantee ("大白担保").

Given that guarantee marketplaces typically involve hundreds to thousands of public and private channels, this report outlines how Insikt Group analysts navigated through just one of the Telegram channels belonging to Dabai Guarantee's large infrastructure. The channel is known as Dabai Guarantee Public Group 301 (@DBTM301), and its main objective is to conduct "sweeping" operations (using illicit techniques to make purchases of physical goods at retailers or to withdraw and transact at country-specific ATMs) in South Korea and Japan. This report also includes the visible organizational structure of Dabai Guarantee Public Group 301, key rules, staff, and customer service functions.

This report primarily serves as an introduction to understanding how Chinese-language, Telegram-based guarantee marketplaces work and how to navigate them. It also includes interpretations of multiple criminal terminologies used by Chinese-speaking criminals, which are pivotal to understanding how Chinese cybercrime evolves over time. The cyber and fraud campaigns being promoted and launched on Dabai Guarantee and other similar guarantee marketplaces can negatively impact retail, banking, contactless payment providers, insurance companies, and individuals vulnerable to scam-related campaigns.

Key Findings

- Dabai Guarantee is a platform that enables multiple Chinese-speaking threat groups with strong presences across multiple countries to coordinate and launch global-scale fraud and cyber campaigns.
- Chinese-speaking syndicates are using Dabai Guarantee as a platform to facilitate campaigns involving financial and retail fraud, such as ATM withdrawal and ghost-tapping.
- Criminal groups participating in campaigns are often siloed, acting independently, and restricting the sharing of information, resources, and goals, thereby creating barriers to tracking their activities.
- Unlike conventional ghost-tapping campaigns that mainly target luxury businesses, "sweeping teams" typically purchase goods that are less expensive but still considered valuable to criminal groups and are relatively easy to transport (such as women's cosmetics and tobacco products), likely to avoid detection by law enforcement. The sweeping teams eventually resell them in other markets for cash.
- Dabai Guarantee's bot search function makes it easy for Chinese-speaking criminals to enter specific search terms and be matched with existing public groups running those campaigns.

Table of Contents

Background

Chinese-language guarantee marketplaces first emerged around 2021 with the launch of Huione Guarantee, serving as reliable alternatives to traditional dark web marketplaces accessible via the Tor network. Owners of traditional dark web marketplaces, such as Exchange Market and Chang'An Sleepless Night, have close to full control over advertisements and transactions. These guarantee marketplaces seek to eliminate distrust stemming from criminal groups scamming one another, dark web marketplaces shutting down, potential exit scams, and parties failing to honor terms that were previously agreed upon. Furthermore, guarantee marketplaces operate on publicly accessible Telegram channels by design; these public channels are meant to be found and appeal to a wider Chinese-speaking audience that uses Telegram, noting that most Chinese criminals still use Telegram rather than Tor for communication.

Guarantee marketplaces are often different from typical peer-to-peer (P2P) transactions between threat actors. Guarantee marketplaces are one-stop shops that handle and facilitate all cryptocurrency transactions (typically Tether/USDT) and mediation services between parties, whereas P2P transactions typically take place directly between users or through a third-party escrow service. The preferred cryptocurrency of Chinese-speaking threat actors is USDT, a stablecoin pegged to the US dollar that maintains anonymity. Stablecoins are a type of cryptocurrency designed to maintain a stable value by pegging themselves to reserve assets, most commonly the US dollar, to mitigate the volatility of cryptocurrencies like Bitcoin. According to Chainalysis's 2026 Crypto Crime Report, stablecoins have come to dominate the landscape of illicit transactions, accounting for 84% of all illicit transaction volume in 2025. Chinese cybercriminals prefer using stablecoins such as USDT due to their combination of price stability, ease of border transfer, and relative anonymity. USDT also helps Chinese cybercriminals bypass China's strict capital controls and traditional banking scrutiny to move money across borders.

In January 2025, Insikt Group published a report on the Chinese-language guarantee marketplace Huione Guarantee, "Huione Guarantee Serves as a One-Stop Shop for Chinese-Speaking Cybercriminals." The report described the activities facilitated by Huione Guarantee, which include investment fraud, money laundering, and various online scams. Despite Huione Guarantee's shutdown on May 13, 2025, Insikt Group observed that other guarantee marketplaces, such as Tudou and Xinbi, stepped in to fill the void left by Huione Guarantee's closure. According to Elliptic, Tudou Guarantee also shut down its operations in January 2026, after processing $12 billion in transactions. Even though Xinbi Guarantee was previously reported to have shut down, it has since been rebuilt and maintains a presence on Telegram as of this writing. Other, but not widely reported, active Chinese-language guarantee marketplaces operating on Telegram (besides Dabai Guarantee) are Yinuo, BoChuang, and Ouyi.

Guarantee marketplaces can also facilitate new attack vectors such as ghost-tapping. In July 2025, Insikt Group published a report titled "Ghost-Tapping and the Chinese Cybercriminal Retail Fraud Ecosystem," which details how Chinese-speaking cybercriminals and syndicates work together to

conduct retail fraud using near-field communications (NFC) relay tactics. As of February 2026, Insikt Group observed that Dabai Guarantee has emerged as a major player in Chinese-language cybercrime, with its Telegram-based infrastructure resembling that of Huione Guarantee and offering malicious services similar to those advertised on Huione Guarantee, which is now defunct.

Dabai Guarantee Overview

Dabai Guarantee is a Telegram-based marketplace, consisting of thousands of public and private Chinese-language Telegram groups, that operates in a manner similar to Huione, Tudou, and Xinbi guarantees; many of these services cater to "small to medium-sized clients." However, the operators of Dabai Guarantee do not maintain a clearnet website; they operate solely on Telegram, likely due to operational security (OPSEC) concerns. Operators of Dabai Guarantee likely chose not to have a clearnet website in light of Huione's "bad OPSEC" practices — Huione Guarantee's clearnet website made tracking much easier for law enforcement officials and researchers, which likely contributed to FinCEN sanctioning the organization in May 2025. The Dabai platform is populated with third-party vendors providing various services that facilitate cybercriminal and fraud activities, including money laundering methods and services, compromised social media and e-commerce accounts, SIM cards, personally identifiable information (PII), malware-as-a-service (MaaS), deepfake technology, know-your-customer (KYC) bypass services, and more.

Dabai Guarantee was likely founded in December 2024, based on its Telegram Channel's creation date. There are currently six known official main Telegram channels:

- "公群导航 @dabai" (@dabai_a): "Public Group for Navigation Purpose", 15,372 subscribers, as of this writing
- "大白担保大群" (@dabai_c): "Dabai Guarantee Big Group", 19,225 members, as of this writing
- "大白供需频道" (@dabaiyajing): "Dabai Supply and Demand Channel", 17,085 subscribers, as of this writing
- "大白担保规则" (@dabai_e): "Dabai Guarantee rules", 428 subscribers, as of this writing
- "大白担保客服人员名单" (@dabai_f): "Dabai customer service list", 527 subscribers, as of this writing
- "大白担保 @dabai" (@dabai): "Dabai Guarantee bot channel"

Dabai Guarantee's public navigation channel, 公群导航 @dabai, is used to direct threat actors to different private/public Telegram channels to coordinate and collaborate on campaigns targeting both Chinese-speaking and non-Chinese-speaking victims. Below is a list of the service categories offered on the public Telegram groups on Dabai Guarantee. Each category has subcategories for more specific services. Each public Telegram group has a unique group number, the amount of the deposit made to Dabai Guarantee in USDT, the handles of group administrators and customer service representatives, the transaction rules, and a dedicated cryptocurrency wallet. More information can be found in **Figure 1**. These specialized channels include the following:

- “海外钓鱼类” (“Overseas Phishing”) — Coordinate phishing campaigns against individuals residing outside of China
- “买卖类” (“Trading”) — Buy and sell gift cards, databases, SIM cards, social media burner accounts, IP addresses, and physical goods
- “引流类” (“Traffic generation methods”) — Overseas SMS blasts, Baidu promotions, chat scripts, and other services
- “承兑类” (“Acceptance methods”) — Payment methods accepted by merchants include Alipay, WeChat Pay, and cryptocurrencies
- “通道合作类” (“Cooperation Channels”) — Motorcade teams to conduct overseas operations such as collecting or making payments via cash and cryptocurrencies, and logistic operations to move physical goods
- “短视频类” (“Short Videos”) — Short Douyin videos for promotions
- “合作类” (“Cooperation”) — ID Loans, Apple IDs, courier delivery services, and burner mobile phones
- “服务类” (“Services”) — SMS verification, file lookup, and graphic design services
- “卡商类” (“Carding Merchants”) — Money laundering through bank cards and contactless cash withdrawal without cards
- “搭建类” (“Developers”) — Software and bot setup services, and Apple signing/server/VPN/domain setup services
- “其他类” (“Others”) — Other miscellaneous fraud services, social escort services, police impersonation, artificial intelligence (AI), and search engine optimization (SEO)-related services
- “游戏类公群” (“Gaming-related public groups”) — Online gambling and video games

Figure 1: *Dabai Guarantee's public navigation purpose Telegram channel "公群导航 @dabai", with listed categories (Source: Telegram)*

Dabai Guarantee's Rules (@dabai_e)

Dabai Guarantee's rules channel (@dabai_e) has posted rules to prevent impersonation of the marketplace and to prevent users from creating their own "public groups" that are not officially regulated by Dabai Guarantee's administrators. Some of the rules also showcase Dabai Guarantee's OPSEC measures to prevent scamming and impersonation. The original Chinese text is in **Appendix B.** The following are some key rules:

- Members are not allowed to create their own public group channel without Dabai Guarantee`s approval.
- Members are not allowed to have private dealings with other parties or platforms, as Dabai Guarantee only guarantees transactions conducted on its platform. Dabai Guarantee also does not provide assurances for transactions with the Public Group "boss" or any other administrator. This means that no individual should have any transactions with the boss directly and should instead use Dabai Guarantee's funds transfer mechanism.
- Individuals who initiate a chat session with you are 100% scammers; members are to block and refrain from chatting with them.
- The cryptocurrency address belonging to Dabai Guarantee is unique, and anyone sending other deposit addresses is a scammer.
- After members have staked their cryptocurrency as deposits, they are required to send Dabai Guarantee's leadership screenshots of the deposit to @dabai for verification and confirmation. Any losses resulting from failure to contact @dabai will be the member's responsibility.

Case Study: Public Group 301

Group Structure

For this report, we will use the Telegram channel "Public Group 301," which belongs to Dabai Guarantee, as a case study. This is not meant to be a comprehensive analysis of Dabai Guarantee's massive infrastructure and that of other Chinese-language guarantee marketplaces. It is difficult to accurately quantify how many "Public Group" channels and threat groups are on Dabai Guarantee, as the numbers tagged to Public Groups are not assigned in chronological order, resulting in a lack of visibility — unlike Huione Guarantee, which had a clearnet website that listed the Public Group channels to redirect threat actors. Although there are thousands of channels belonging to Dabai Guarantee alone, understanding Public Group 301's structure can at least provide insight into how threat actors use Dabai Guarantee in their campaigns.

In guarantee marketplaces, threat actors looking to launch campaigns typically deposit USDT to start a public Telegram group approved by Dabai Guarantee. This model ensures that criminal syndicates do not have to deal with other threat actors directly, but have Dabai Guarantee as a mediator. In the case of Dabai Guarantee's Public Group 301, affiliate threat groups do not have to engage directly with the group's leader, @J0hnNo1, and instead receive payments from Dabai Guarantee after the completion of

tasks required by @J0hnNo1. Guarantee marketplaces such as Huione, Tudou, Xinbi, and Dabai seek to eliminate the "lack of trust" among Chinese-speaking threat actors. These marketplaces are designed to become trusted platforms that foster coordination and cooperation between different Chinese-speaking criminal groups to achieve their objectives.

Insikt Group navigated through Public Group 301's Telegram infrastructure in order to identify the redirection flow. As shown in **Figure 1**, each category contains a hyperlink that redirects to other channels. From **Figure 1**, selecting category 5, sub-category 2 ("海外扫货车队", or "Overseas Goods Sweeping Team") redirected to a pinned message as seen in **Figure 2.** This message lists four different public channels ("公群") containing campaigns targeting the US, Canada, South Korea, and Japan.

Figure 2: *Selecting "海外扫货车队" (Overseas Goods Sweeping Team) redirects users to four different Telegram groups, where threat actors are seen discussing and showing off their financial crime-related achievements in countries such as the US, Canada, South Korea, and Japan (Source: Telegram)*

As seen in **Figure 2**, "公群" refers to unique Public Group channels for specific purposes or operations. Each public channel here contains a numerical group identifier and a "U" deposit amount, where "U" refers to USDT. For example, "公群935已押2000U" refers to Public Group Number 935, with 2,000 USDT already being deposited in Dabai Guarantee to start the campaign. The naming convention for these Public Groups is "dbtmxxx"; in this case, Public Group Number 935 will have the Telegram channel @dbtm935. When selecting the second option, "公群301已押1000U韩国，日本扫货组", which means Public Group Number 301, with 1,000 USDT already deposited to "sweep goods" in South Korea and Japan, the corresponding Telegram channel is @dbtm301.

Upon further investigation and analysis of the channel, Insikt Group assesses that "sweeping goods" refers to the use of illicit means, such as ghost-tapping, to purchase physical goods at physical retail stores (in this case, in South Korea and Japan). This activity also includes ATM cash withdrawals at Japanese or South Korean ATMs.

Key Personnel Involved in Public Group 301

The following terms are important for understanding the operations of criminals involved in Public Group 301, and the entire Dabai Guarantee infrastructure more broadly:

- **Boss ("群老板"):** The main coordinator overseeing a group's operations. These individuals are not directly related to Dabai Guarantee and operate more like customers, making use of Dabai Guarantee's infrastructure to lay out tasks and promising payouts in USDT upon completion. The boss will typically start a campaign by placing significant deposits into Dabai Guarantee's USDT cryptocurrency addresses ("上押地址") in order to get Dabai Guarantee's administrators to approve the creation of a Public Group channel. In Dabai Guarantee's Public Group 301 (@dbtm301), @J0hnNo1 is the boss of the channel. We observed that this threat actor intends to conduct ghost-tapping and fraud campaigns in Japan and South Korea, with the key objective of obtaining physical goods, cash, and funds through unauthorized transactions. Once the boss confirms receipt of the items and is satisfied with the outcome, they can ask Dabai Guarantee to release the payment to the criminals who participated in the requested task.
- **Channel Administrators ("管理员"):** Dabai Guarantee's personnel who act as intermediaries between the boss and other Chinese syndicates, ensuring that the boss gets the items and physical cash, while the Chinese syndicates are paid in USDT. These are the people who will process the payments. Channel administrators will also inspect video evidence provided by sweeping and "goods-receiving" teams and wait for confirmation from the boss that everything is satisfactory before releasing payments to the various Chinese-speaking criminal groups.
- **Chinese Syndicates ("犯罪组织")**: Teams in charge of providing the people ("mules") to form sweeping and goods-receiving teams. These syndicates will coordinate with the boss and receive payment in USDT after completing the required jobs.
- **Sweeping Teams ("扫货队")**: Personnel tasked by the boss or other administrators with obtaining physical goods or conducting ATM cash withdrawals, typically through illegal methods such as ghost-tapping or financial fraud, and to eventually transfer the goods to "goods receiving" teams.
- **Goods Receiving Teams ("收货队"):** Personnel tasked by either the boss or their respective Chinese syndicates with receiving goods from sweeping teams; the items will eventually have to reach the "goods inspection teams."
- **Goods Inspection Teams ("检货队")**: Personnel tasked with physically inspecting the goods and cash being delivered by the sweeping or goods-receiving teams, typically appointed by bosses. When the "goods receiving" team is appointed by the boss, it is also possible that the "goods receiving" and "goods inspection" teams are composed of the same personnel, each fulfilling multiple roles. These teams will inform the boss whether the physical goods are satisfactory, and

the boss will proceed to ask Dabai Guarantee to release the payment to the sweeping and goods-receiving teams.

Insikt Group assesses that individuals in the sweeping, goods receiving, and goods inspection teams act as mules, and these teams likely consist of Chinese-speaking tourists who can amass large quantities of physical goods and cash and exit the targeted countries as soon as possible. It is also likely that Chinese-speaking groups have members who are long-term residents of the countries targeted by the operations, such as South Korea and Japan.

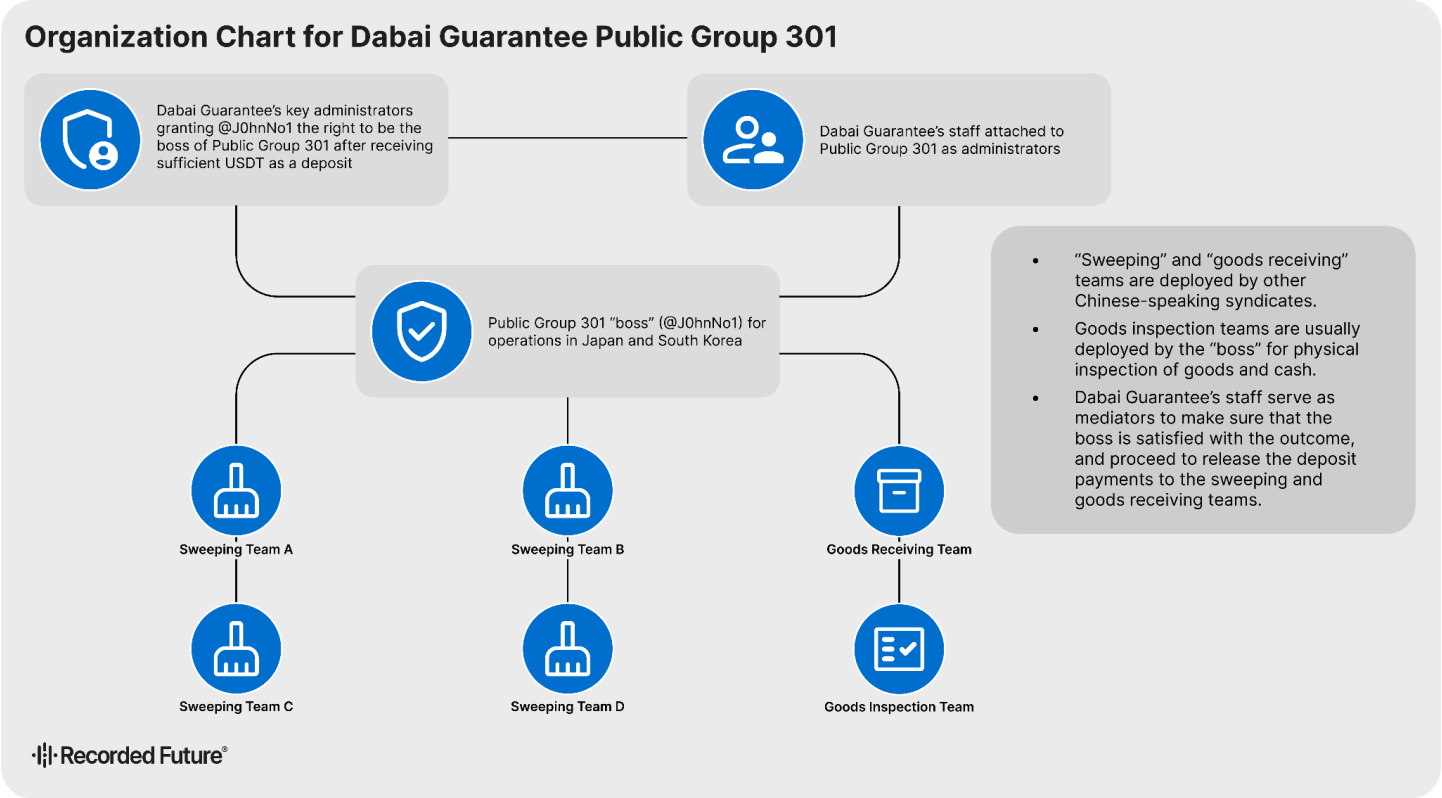


Figure 3: *Simplified illustration of Dabai Guarantee Public Group 301's structure (Source: Recorded Future Data)*

Figure 3 is a simplified illustration of Dabai Guarantee's Public Group 301's organizational structure. The barrier to entry for participating in "sweeping operations" is low, as participants just need to have the legal right to enter Japan or South Korea, pose as tourists, and follow the instructions given by the boss and other administrators. We estimate that there are likely more than a dozen sweeping teams linked to Dabai Guarantee operating in Japan and South Korea alone. Sweeping teams are likely assigned to obtain certain goods and cash in very specific areas and do not coordinate with one another because they are being deployed by different Chinese syndicates. This model suggests that operations are siloed, where teams act as independent, isolated units that restrict the sharing of information, resources, and goals.

Figure 4 shows the Telegram structure of Public Group 301, where @J0hnNo1 is the channel's boss. The channel is also composed of multiple Dabai Guarantee customer service staff, who serve as administrators. The original creator of the channel is @dbwb22; the Telegram account is no longer active, and @dbwb22 is no longer listed as one of Dabai Guarantee's official customer service agents.

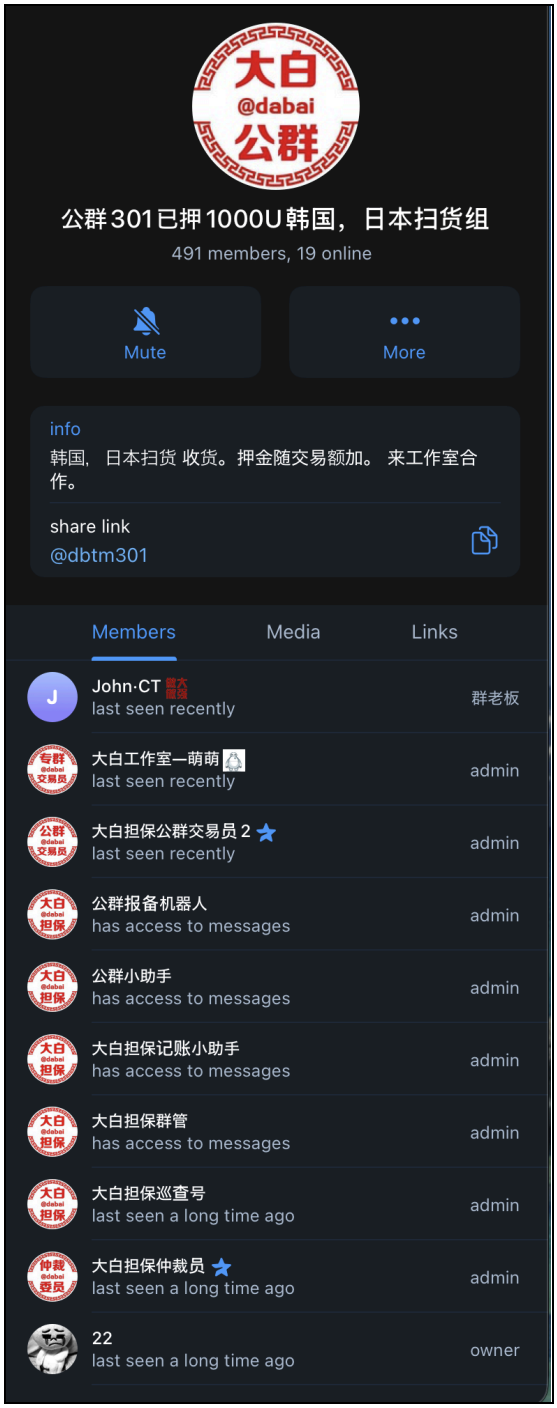


Figure 4: *List of key personnel in Dabai Guarantee's Public Group 301 (@dbtm301); @J0hnNo1 is listed as this group's public channel boss (Source: Telegram)*

The distribution of these teams significantly complicates efforts by researchers and law enforcement agencies to track and deter such criminal activities. For example, if members of "Sweeping Team A" are arrested for retail or financial fraud, law enforcement agencies will still need to locate the members of the "Goods Receiving Teams" and "Goods Inspection Teams" before they can even get close to decoding the identity of the boss, who is most likely coordinating operations from a location outside Japan or South Korea's jurisdiction, such as Cambodia or Myanmar. Additionally, these sweeping teams most likely consist of low-level mules who are considered "expendables" by their Chinese syndicate recruiters. The screenshots in **Figures 6, 7, 8, 9, and 10** illustrate the siloed operations conducted by different sweeping teams.

Figure 5 shows Dabai Guarantee customer service personnel @dbtm9 helping to set up public Telegram channel 301 on March 21, 2025, and serving as the channel's key administrator. This individual serves as a mediator to facilitate transactions and dealings between the boss and other threat actors. The total amount of USDT deposited on that date was 485 USDT; as of this writing, it has risen to 1,000 USDT. The purpose of this channel is to encourage other threat actors to cooperate by taking part in sweeping and goods-receiving operations in Japan and South Korea. In the conversation below, the boss stated that the deposit amount will increase in proportion to the transaction amount. Insikt Group assesses that this would mean the sum of deposit scales with the size of operations in Japan and South Korea.

Figure 5: *Screenshot of Public Group 301's (@dbtm301) administrator (@dbtm9) establishing a group for "sweeping goods" and "receiving goods" operations in South Korea and Japan*

Figure 6 shows that the boss is looking to recruit sweeping teams to conduct operations in Seoul, South Korea. The main objective is to purchase cosmetics, and once the goods have been delivered, the rewards will be "high." The final sentence uses the term "速度快", which means that the boss welcomes any sweeping team that can conduct and complete these operations quickly.

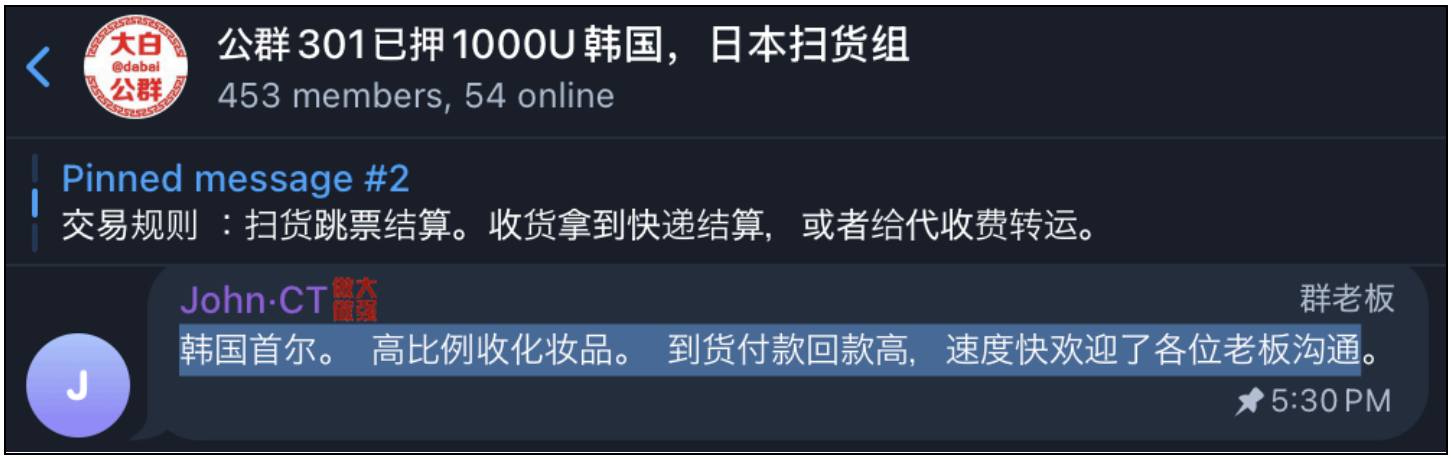


Figure 6: *Screenshot of Public Group 301 "boss" @J0hnNo1 recruiting sweeping teams to purchase cosmetics in Seoul, South Korea (Source: Telegram)*

Figure 7 features a sweeping team involved in purchasing tobacco-related products from the Terea brand at a CU store, a South Korean convenience store chain in Seoul, South Korea. It is clear that the boss has goods from specific brands they wish to obtain, and such goods may be resold for cash in other foreign markets at a later date, likely at a lower price to obtain hard currency as soon as possible. Insikt Group assesses that the items are very likely purchased using the ghost-tapping attack vector or through stolen payment card information. This reflects a shift from targeting luxury retailers to smaller-sized businesses, likely to avoid arousing suspicion from law enforcement authorities
.

Figure 7: *Public Group 301's boss @J0hnNo1 showing a CU receipt of tobacco sticks belonging to the Terea brand totaling 288,000 won, worth approximately $196 on March 25, 2025 (Source: Telegram)*

Figure 8 shows an Apple Store receipt listing unspecified Apple products totaling 499,600 yen (approximately $3,145.66, as of this writing). Public Group 301's boss @J0hnNo1 also stated, "Who said there are no large transactions in Japan? Just a single receipt amounted to 500,000 Yen." This is likely a post encouraging syndicates to send more sweeping teams to acquire as many Apple products as possible, while hinting that the rewards could be lucrative.

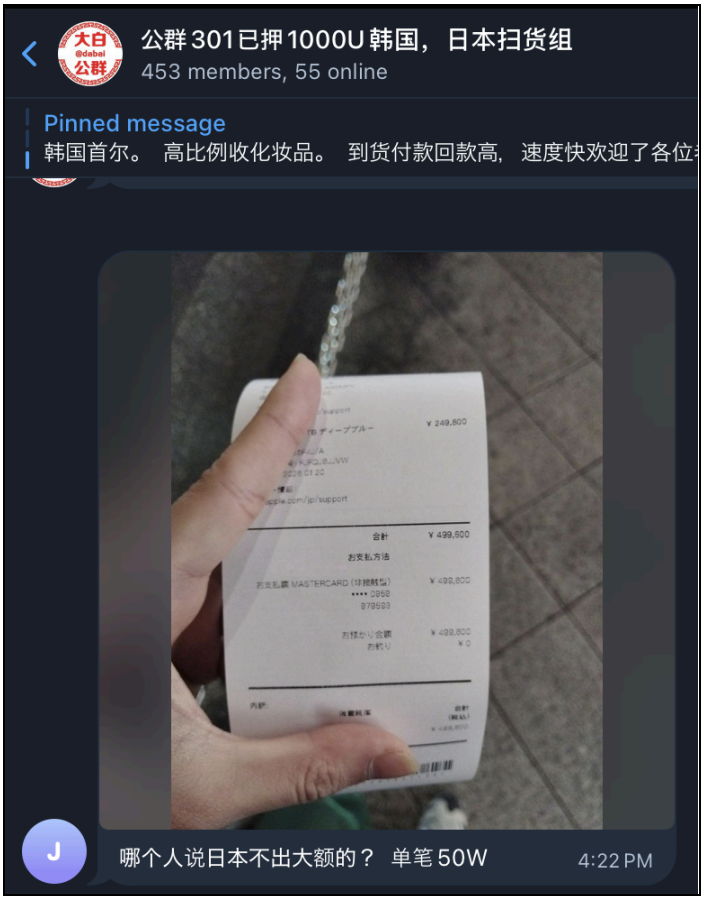


Figure 8: *Public Group 301's boss @J0hnNo1 showing an Apple store receipt of items totaling 499,600 yen, approximately $3,145.66 on December 28, 2025 (Source: Telegram)*

Figure 9 provides some evidence that Vietnamese individuals are also involved in sweeping operations. In the top-left corner of the iPhone in the image, the Vietnamese phrase "Không có SIM" means "No SIM card." This indicates that the person holding the phone is very likely a Vietnamese-speaking individual conducting unauthorized banking transactions using burner iPhones. Every single burner phone appears to be tagged with a label, which is very similar to the tactics, techniques, and procedures (TTPs) we documented in our Insikt Group report on ghost-tapping. It is also likely that this individual understands Japanese in addition to Chinese, as they were observed interacting with a Japanese banking application that displayed processed transactions. The transactions shown in the screenshot are dated between July 30, 2025, and August 28, 2025. The ability to use Japanese banking applications is an indicator that this individual is legally residing in Japan. In general, most Japanese banks require foreigners to close their bank accounts before leaving permanently; these regulations are implemented by major Japanese banks such as Shinsei Bank.

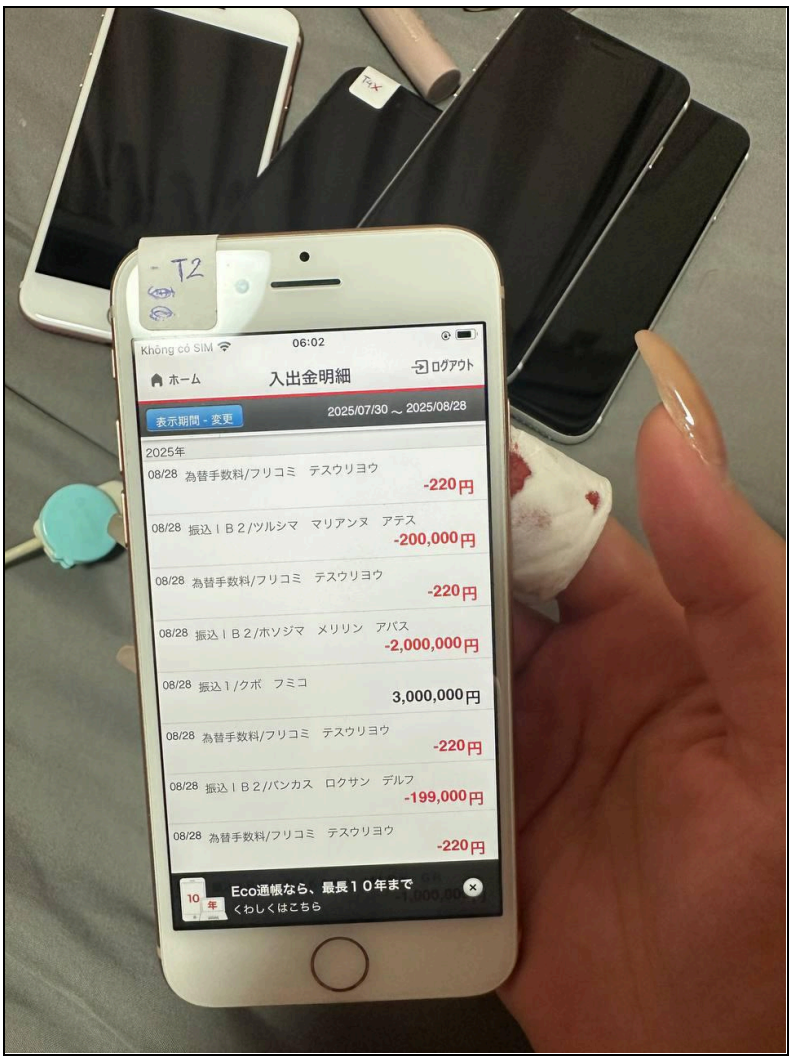


Figure 9: *Image posted by Public Group 301's boss @J0hnNo1 involving multiple unauthorized banking transactions from July 30, 2025, to August 2025. Insikt Group assesses that this is indicative of a ghost-tapping campaign targeting Japanese retail businesses involving multiple Apple burner iPhones on August 28, 2025 (Source: Telegram)*

Figure 10 shows what appears to be an ATM cash withdrawal or transfer attempt at a Japanese ATM at an unspecified bank. This screenshot is also likely shown as an example of what sweeping teams in charge of withdrawing and transferring cash are expected and required to do.

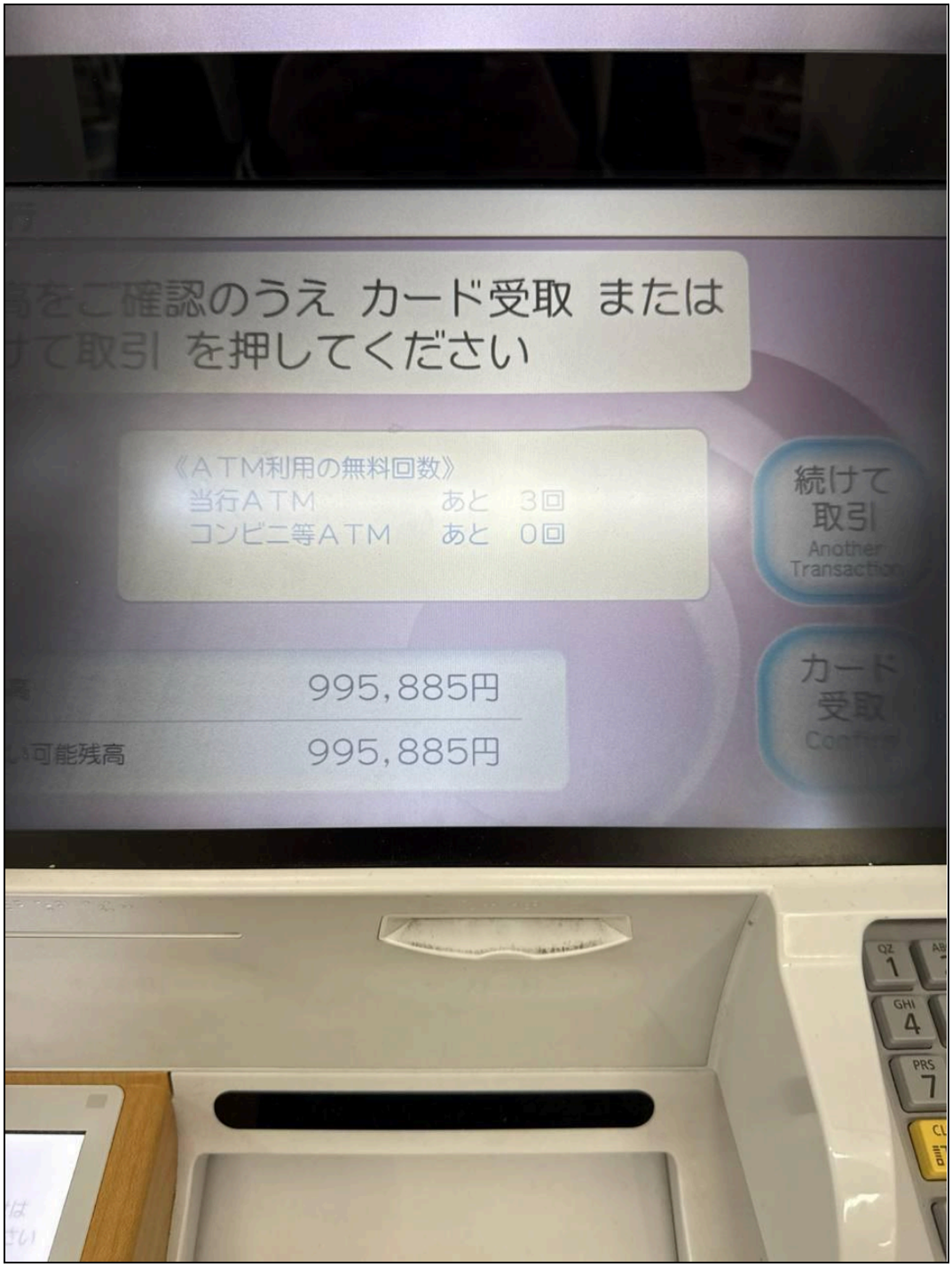


Figure 10: *Public Group 301's boss @J0hnNo1 posted an image of what Insikt Group assesses to be an ATM cash withdrawal/transfer using a Japanese ATM machine on April 23, 2025 (Source: Telegram)*

Figure 11 shows a cryptocurrency transaction of 10,629 USDT via the Tron (TRX) network to a sweeping team for the successful completion of the "mission." The boss @J0hnNo1 thanked the sweeping team coordinator without identifying them. The exact phrase used while posting the image was "感谢老板信任", which translates from Chinese to "Thank you boss for trusting me." Boss, in this context, refers to the Chinese syndicates that provide the sweeping teams for successful operations. In the entire Dabai Guarantee Public Group 301 channel, there were many screenshots of such cryptocurrency transactions being sent to teams that participated in sweeping operations. The boss redacts recipients' cryptocurrency wallet addresses to prevent law enforcement agencies from tracking them. The TRON wallet address used by Public Group 301 is TByDzGWCirpCABaUorkhz5eWhjyDdYWgSo, as shown in **Figure 11**; this wallet address has facilitated a total of 2,943 transactions as of this writing.

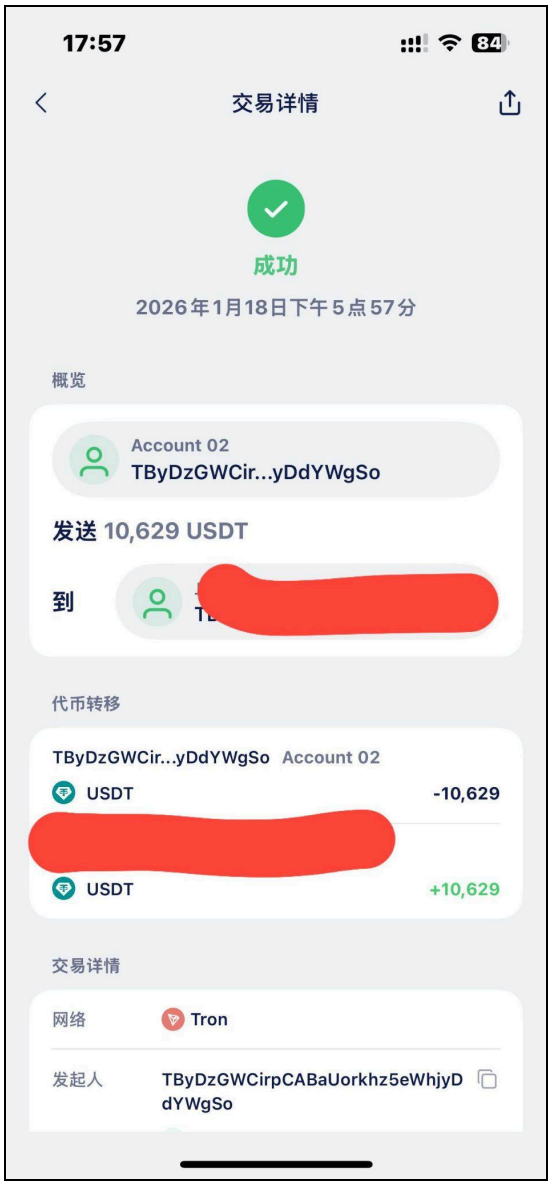


Figure 11: *Multiple screenshots involving USDT transactions are posted on the channel, likely for transparency and to reassure the sweeping teams (Source: Telegram)*

Dabai Guarantee's Staff and Customer Service Functions (@dabai_f)

Dabai Guarantee maintains a list of its official staff and customer service agents on its Telegram channel @dabai_f to facilitate the creation of Public Group channels and transactions. This system also helps prevent impersonation and scamming. Members are to contact customer service agents directly for any queries or concerns. The staff and customer service teams usually provide the functions[1] listed in **Tables 1 and 2**; the customer service agents are listed in **Figure 12** by their functions and Telegram handles.

Chinese Term	English Term	Explanation of Function	Telegram Moniker/Channel
大白公群	Main Dabai Public Group	Dabai Guarantee's directory, to help threat actors navigate through different aspects of cybercrime	@dabai_a
供求信息	Supply and demand information	A channel where Dabai Guarantee's administrators post advertisements on behalf of their customers (other threat actors)	@dabaiyajing
核心大群	Core group	A channel where other threat actors can post their own advertisements and URLs for their websites, as well as key contact information, such as Telegram monikers	@dabai_c
客服频道	Dabai Guarantee's official customer service channel	A channel for individuals to reach out to customer service officers who cater to different categories of cybercrime	@dabai_f
人工客服 @dabai 咨询、拉群、广告	Human customer service agents for consultation, group chat, and advertising	A bot channel that redirects individuals to human customer service agents for consultation, group chat, and advertising	@dabai
人工客服 @dabai 会员、解封、投诉	Human customer service agents for membership queries, unblocking	A bot channel that redirects individuals to human customer service agents for membership queries, unblocking accounts, and complaints	@dabai

[1] The Chinese terminologies were translated by an Insikt Group fluent Mandarin speaker; however, these terminologies are unique to Dabai Guarantee and are not uniform across the Chinese-language cybercriminal ecosystem.

Chinese Term	English Term	Explanation of Function	Telegram Moniker/Channel
	accounts, and complaints		
人工客服 @dabai 验群、丢失群恢复	Human customer service agents for group verification and lost group recovery	This is to prevent impersonation, such as threat actors starting their own Public Group that is not officially approved by Dabai Guarantee. There may be instances where Telegram deletes public channels for violating the terms of service, and the customer service team offers a service to restore them (This happened to Huione and Xinbi Guarantee; many of their channels were deleted by Telegram).	@dabai
人工客服 @dabai 纠纷仲裁、资源对接	Human customer service agents for dispute arbitration and resource matching	Customer service agents will attempt to resolve disputes between criminal groups when an unsatisfactory outcome is reached for one or more parties. They can also moderate disputes on transactions between buyers and sellers. Resource matching refers to customer service agents attempting to match criminal groups to certain existing groups that are already participating in specific campaigns. In addition, customer service agents can connect buyers with sellers of goods and services.	@dabai
24小时客服机器人	24-hour customer service bot		@dabai
公群报备机器人	Public Group reporting bot	A bot that assists members in reporting violations of the terms of service	@dbhwbb_BOT
公群记账机器人	Public Group accounting bot	A bot that can help to look up transactions, real-time USDT pricing in relation to Chinese Renminbi (RMB), and cryptocurrency wallet monitoring	@dbjz_bot
客服人员名单 (@dbtm0 - @dbtm10)	Customer service staff lists (@dbtm0 – @dbtm10) All customer service numbers come with a +888 virtual number. Any number without this is a scam.		@dbtm0 – @dbtm10

Chinese Term	English Term	Explanation of Function	Telegram Moniker/Channel
所有号标配 +888 虚拟号 没有一律骗子			

Table 1: *List of Dabai Guarantee's official staff and functions (Source: Telegram, Recorded Future)*

Chinese Term	English Term	Explanation of Function	Telegram Moniker/Channel
业务号（大白）	Business account (Dabai)	A business account belonging to a person called Dabai, with no specific function stated	@dbtm1
业务号（萌萌）	Business account ("Mengmeng" — Admin's moniker)	A business account belonging to a person called Mengmeng, with no specific function stated	@dbtm9
专群交易员	Specialist traders	A group of agents well-versed in certain types of trade to facilitate coordination and cooperation in the public channels	@dbtm0 @dbtm3 @dbtm4
公群交易员	Public Group traders	A group of agents who facilitate cryptocurrency transactions, receive deposits, and release payments to other criminal groups	@dbtm7 @dbtm8 @dbtm10
公群巡查号	Public Group patrol account	A group of agents who direct individuals to specific Public Group channels based on what they are looking for	@dbtm2
担保仲裁号	Guarantee arbitration number	A case reference number assigned by agents for any disputes between parties	@dbtm5
资源对接号	Resource docking number	A unique number is assigned to a case or transaction to track conversational and transaction records	@dbtm6

Table 2: *List of Dabai Guarantee's customer service agents (Source: Telegram, Recorded Future)*

Figure 12: *Dabai Guarantee customer service Telegram channel "大白担保客服人员名单" (@dabai_f) provides a list of customer service agents (Source: Telegram)*

Automated Bot System Directs Chinese Syndicates to Relevant Public Groups for Existing Campaigns

Insikt Group analyzed the public administrator bot @dbdbqg_bot to observe how a Dabai Guarantee user would be routed by the platform to participate in cybercriminal activities. To use this functionality, individuals must enter search terms in Mandarin. We used the terms 远程 (remote) and 数据 (data), which returned three and ten public channels, respectively. When querying for the term "远程" (remote), which typically refers to ghost-tapping campaigns involving NFC relay methods, three Public Group channels appeared as relevant results. When querying for the term "数据" (data), which typically refers to databases, ten Public Group channels specializing in datasets appeared in the results. In addition, using a country as a search term, such as 美国 (US), will also return results that show fraud or cyber campaigns targeting the US. This bot function demonstrates how easy it is for criminal groups to search for relevant groups, determine which campaigns they wish to participate in, and identify the types of datasets they are interested in procuring. **Table 3** shows the number of Public Group channels involved in fraud or cyber campaigns for the search terms; specific details are not listed due to certain global entities named in the Public Group channels belonging to Dabai Guarantee.

Figure 13: *Dabai Guarantee's public administrator bot @dbdbqg_bot has a search function that will return results relevant to the individual's search (Source: Recorded Future Data)*

Chinese Criminal Lingo and Corresponding English Meaning	Number of Channels Returned as Search Results	Explanation of Function	Telegram Channels
远程 (Remote)	3	Ghost-tapping/remote NFC-related payment card fraud involving point-of-sale (POS) terminals	@dbtm153 (64 members, 800 USDT deposit as of writing) @dbtm439 (49 members, 777 USDT deposit as of writing) @dbtm307 (268 members, 500 USDT deposit as of writing)
数据 (Data)	10	Threat actors buying and selling databases	@dbtm123 (519 members, 888 USDT deposit as of writing) @dbtm99 (49 members, 500 USDT deposit as of writing) @dbtm688 (151 members, 500 USDT deposit as of writing) @dbtm369 (65 members, 500 USDT deposit as of writing) @dbtm567 (80 members, 2,888 USDT deposit as of writing) @dbtm449 (177 members, 500 USDT deposit as of writing) @dbtm298 (145 members, 500 USDT deposit as of writing) @dbtm327 (89 members, 500 USDT deposit as of writing) @dbtm211 (836 members, 500 USDT deposit as of writing) @dbtm816 (851 members, 500 USDT deposit as of writing)
美国 (US)	2	Fraud or cyber campaigns targeting US entities	@dbtm322 (338 members, 500 USDT deposit as of writing) @dbtm932 (956 members, 500 USDT deposit as of writing)
钓鱼 (Phishing)	1	Phishing campaigns	@dbtm142 (234 members, 500 USDT deposit as of writing)
账号 (Account)	2	Burner accounts being used for fraud campaigns	@dbtm322 (338 members, 500 USDT deposit as of writing)

Chinese Criminal Lingo and Corresponding English Meaning	Number of Channels Returned as Search Results	Explanation of Function	Telegram Channels
			@dbtm425 (60 members, 500 USDT deposit as of writing)
银行 (Bank)	2	Fraud campaigns targeting or involving banks worldwide	@dbtm420 (117 members, 500 USDT deposit as of writing) @dbtm138 (50 members, 1,000 USDT deposit as of writing)

Table 3: *Search results of Dabai Guarantee's Public Group channels using their bot function (Source: Telegram, Recorded Future)*

Outlook

Even with guarantee marketplaces such as Huione Guarantee being shut down, many Chinese criminals are likely turning to these Telegram-based guarantee marketplaces to sell illicit goods and to offer their services. Guarantee marketplaces such as Dabai Guarantee have demonstrated their ability to coordinate operations in countries such as Japan, South Korea, Canada, and the US by using Chinese-speaking individuals who are traveling or residing in those geographies to conduct retail and financial fraud. Over time, Dabai Guarantee may be able to establish itself as a trusted escrow platform for Chinese syndicates to rely on, despite the growing competition from existing and new guarantee marketplaces. There is also a possibility that operators of other guarantee marketplaces could execute an exit scam, leading to a loss of trust in guarantee marketplaces as a whole among Chinese criminals.

Threat actors such as @J0hnNo1, the leader of Dabai Guarantee Public Group 301, seek to obtain physical goods and foreign currency through illegal means, giving specific instructions to different syndicates to complete their objectives. Such operations are scalable on demand and will become harder to track and disrupt over time due to the siloed nature of the sweeping and goods-receiving teams. This report showcases the activities and structure of a single group (Public Group 301), which is only one group among hundreds under Dabai Guarantee's decentralized and growing infrastructure. Ghost-tapping and ATM withdrawals are commonly used by Chinese-speaking criminals for money laundering, and we will likely continue to see more threat actors facilitating such financial and retail-related crime on multiple guarantee marketplaces.

Insikt Group assesses that Chinese syndicates will continue to recruit and deploy non-Chinese individuals with specific language skills to participate in campaigns, as exemplified by the Vietnamese individual mentioned in **Figure 9**.

Insikt Group assesses that guarantee marketplaces have solidified themselves as a major alternative to traditional Chinese-language dark web marketplaces. This decentralized model is becoming increasingly popular among the global Chinese-speaking criminal diaspora, enabling criminals without sophisticated skillsets to coordinate with syndicates and participate in operations that require physical elements.

Appendix A: Glossary of Terms

Chinese	Direct Translation	Definition with Relevant Context
公群	Public Group	Public Telegram channel/group facilitates a specific campaign, usually ending with a number; for example, 公群 1025 means Public Group 1025
飞机	Plane	Cryptocurrency
退押	Backing down	Withdrawal of funds from a Public Group
交易所地址	Transaction address	Cryptocurrency transaction wallet address
上押地址	Betting/Staking Address	Unique cryptocurrency addresses owned by Dabai Guarantee are usually listed in Public Groups. Threat actors who wish to launch a specific campaign must stake enough cryptocurrency as a deposit to create a Public Group channel; they will become the channel's "boss."
私下拉群做单	Privately soliciting orders	
拉黑	Blackmail	When an individual blocks someone who contacts them directly (Dabai Guarantee's staff will never initiate private chats with any individual)
拉群	Pull the crowd	Start a new public Telegram group and get people to join it so other criminal groups can participate in a new, specific campaign
扫货	Sweep goods	To obtain physical goods or conduct ATM cash withdrawals, typically through illegal methods such as ghost-tapping or financial fraud
收货	Receive goods	To receive goods, typically obtained by sweeping teams via illegal means
群老板	Group boss	Main coordinator to coordinate with other Chinese-speaking criminal groups for cyber and/or fraud campaigns; individuals who staked USDT to get approval to start a Public Group channel on Dabai Guarantee
冒充	Impersonate	Some scammers may impersonate group bosses or create Telegram groups with the intention of scamming other Chinese syndicates.
钱包监听	Wallet monitoring	To monitor cryptocurrency transactions in real time
实时U价	Real-time USDT value in relation to the Chinese Renminbi	

Appendix B: Key Rules Written in Mandarin

(Translation available on p. 7)

⚠交易注意事项⚠

1.进群交易请先看置顶里面的群规则，交易过程请严格按照交易规则进行，群内所有事情请联系群内交易员，私下交易或者其他地方交易，后果自负，大白担保只担保本群内的交易。

2.大白担保业务只担保我们的公群内已经报备过的交易，我们不为公群老板或者其他管理员个人做担保，公群群老板对自己的业务员负责，如果群内业务员违规操作，由公群老板负责。

3.禁止以公群名义私下拉群做单，禁止金额不透明，如被用户举报后果自负。

4.大白担保工作人员不会主动私聊你，主动私聊你的100%都是骗子，请直接拉黑。

5.大白担保的上押地址是唯一的,发其它上押地址的一定是骗子,请大家远离骗子。

6.客户上押后,请及时发送上押截图与我们 @dabai 核实确认,如长时间未找 @dabai 核实确认押金而造成的损失由自己负责。

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for customers, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Operations Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining precise, AI-driven analytics with the Intelligence Graph® populated by specialized threat data, Recorded Future enables cyber teams to see the complete picture, act with confidence, and get ahead of threats that matter before they impact your business. Headquartered in Boston with offices around the world, Recorded Future works with more than 1,900 businesses and government organizations across 80 countries.

Learn more at recordedfuture.com