CYBER THREAT ANALYSIS

Recorded Future®

By Insikt Group®

August 14, 2025

Ghost-Tapping and the Chinese Cybercriminal Retail Fraud Ecosystem

Ghost-tapping is a relatively new and popular attack vector for threat actors using near-field communication (NFC) relay tactics to commit retail fraud in person.

Ghost-tapping campaigns involve cybercriminals and syndicates that collaborate to harvest compromised payment card data and launder funds, respectively.

Ghost-tapping campaigns negatively impact retail, banking, contactless payment providers, and insurance companies by using unauthorized payment card transactions belonging to payment cardholders.

Executive Summary

Ghost-tapping is a relatively new and popular attack vector used mainly by Chinese-speaking threat actors who use near-field communication (NFC) relay tactics to commit retail fraud by using stolen payment card details linked to mobile payment services (such as Apple Pay and Google Pay). This technique allows these threat actors to provide mules with stolen payment card details linked to contactless payment systems in person to obtain physical goods, eventually transporting and reselling stolen goods for profit. Insikt Group analysts identified a key threat actor on Telegram, @webu8, advertising burner phones and ghost-tapping services to Chinese-speaking threat groups (hereafter referred to as syndicates) and engaged with threat actors involved in retail fraud campaigns. Even though Huione Guarantee, a Telegram-based criminal marketplace, announced it shut down its operations on May 13, 2025, we observed that cybercriminals and syndicates have since been using Huione Guarantee’s existing massive decentralized infrastructure on Telegram to conduct dealings. Chinese-speaking cybercriminals have also pivoted to Xinbi Guarantee and Tudou Guarantee platforms as one-stop shops to recruit ghost-tapping, transportation, reseller, and money laundering mules. We believe that established, Southeast Asia-based criminal groups that have been involved in scamming activities (romance, investment scam, and cryptomining, among others) since 2020 have begun and will continue to incorporate ghost-tapping campaigns into their activities for financial gains.

This report includes the key findings of our engagement with threat actors, analysis of video demonstrations showcasing ghost-tapping and contactless ATM withdrawals, open-source research, and law enforcement advisories to explain the Chinese ghost-tapping ecosystem. Insikt Group assesses that ghost-tapping campaigns are difficult to detect due to a lack of Know-Your-Customer (KYC) measures at retail stores and because syndicates can send mules claiming to be tourists to purchase physical goods and resell them for profit. These campaigns can negatively impact retail, banking, contactless payment providers, and insurance companies as a result of unauthorized payment card transactions belonging to payment cardholders. Although ghost-tapping campaigns have been widely reported in Singapore due to high-profile arrests, these campaigns can be conducted on a global scale.

Key Findings

- Chinese-speaking cybercriminals are using automation to add stolen payment card information to contactless payment wallets, selling burner phones, and providing an unspecified peripheral software capable of relaying payment card details to separate mobile devices to multiple Chinese-speaking criminal syndicates. Syndicates can also send burner phones back to these cybercriminals to recycle them for future retail fraud campaigns.
- Threat actors involved in ghost-tapping activities claim the technique can work worldwide, with some groups likely based in Cambodia and China. Through our engagements, we identified some threat actors that only operate domestically within China and other specific geographical locations such as Singapore, Malaysia, Thailand, and the Philippines.
- Many criminal groups are using ghost-tapping techniques to conduct ATM withdrawals and purchase luxury goods such as jewelry and mobile phones at retail stores. Once these goods have been purchased, threat actors resell them for cash on Telegram channels like Tudou Guarantee, Xinbi Guarantee, and Huione Guarantee.

Background

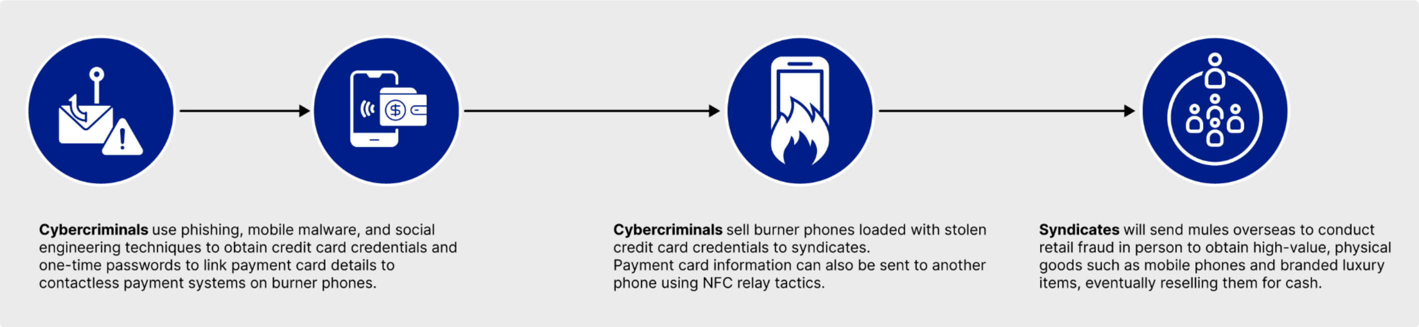
“Ghost Tap” is a term coined by Threat Fabric. It describes a tactic that threat actors use to cash out money after they have stolen credit card details linked to mobile payment services (such as Google Pay or Apple Pay). It also involves relaying NFC traffic, where cybercriminals phish or procure stolen payment cards and load them onto mobile wallets, which are then used for fraudulent transactions. Insikt Group defines ghost-tapping as NFC relay fraud; ghost-tapping involves criminals using mobile devices to relay payment information from a victim's card or device to a payment terminal without the victim's knowledge. Once the payment card information is stolen and loaded into mobile wallets, criminals can transmit an NFC signal containing payment card information to a different phone and scale the operation, which can greatly boost mobile wallet-related fraud.

Recorded Future’s Payment Fraud Intelligence team has published a report titled “Mobile Wallet, Phishing, and Scam Nexus Supports Globally Distributed Card Fraud.” The report’s findings show that NFC relay fraud is an emerging and effective attack method that allows cybercriminals to conduct unauthorized transactions using stolen payment card credentials. Threat actors leverage phishing campaigns and malware to compromise payment cards and intercept one-time passwords (OTPs), which are often essential for adding these cards to mobile wallets. By using open-source NFC relay tools, such as NFCGate, attackers can transmit or relay tokenized card data in real time to other mobile devices. This method allows threat groups based anywhere in the world to:

- Centrally manage phishing campaigns to compromise payment cards belonging to victims in foreign countries and fraudulently activate the cards on mobile wallets under their control
- Relay the NFC traffic of compromised payment cards provisioned on mobile wallets to money mules who conduct fraudulent, tap-to-pay card-present transactions in the victims’ countries

Ghost-tapping campaigns consist of cyber and physical elements that require cybercriminals and syndicates to collaborate for the scheme to succeed. These cybercriminals use phishing campaigns, mobile malware, and social engineering techniques to obtain payment card credentials and one-time passwords to link payment card credentials belonging to victims to contactless payment systems (such as Apple Pay and Google Pay) on burner phones. The cybercriminals will then proceed to sell the burner phones loaded with payment card information and develop proprietary software capable of relaying payment card data to Chinese-speaking syndicates for ghost-tapping campaigns. In essence, cybercriminals only fulfill the cyber spectrum of ghost-tapping campaigns.

Syndicates are well-established criminal groups looking to launder their illegally acquired gains through ghost-tapping campaigns. In ghost-tapping campaigns, the role of syndicates is to work closely with cybercriminals, hire mules to purchase physical goods using burner phones loaded with payment card credentials, and eventually resell the physical goods for cash. Syndicates are responsible for hiring mules, establishing their own contacts, and strengthening their networks and supply chains to launder money through ghost-tapping campaigns. Syndicates fulfill both the cyber and physical spectrum of ghost-tapping campaigns. In November 2024, The Straits Times reported that criminal syndicates from China have been setting up bases in countries such as the Philippines, Australia, and Singapore to launder their gains from illegal activities such as illegal online gambling and scam campaigns as early as 2016.



Cybercriminals use phishing, mobile malware, and social engineering techniques to obtain credit card credentials and one-time passwords to link payment card details to contactless payment systems on burner phones.

Cybercriminals sell burner phones loaded with stolen credit card credentials to syndicates.
Payment card information can also be sent to another phone using NFC relay tactics.

Syndicates will send mules overseas to conduct retail fraud in person to obtain high-value, physical goods such as mobile phones and branded luxury items, eventually reselling them for cash.

Figure 1: *Overview of ghost-tapping campaign involving mobile wallets; an additional proprietary software is required to relay NFC traffic containing payment card data to another mobile phone from the attacker's C2 infrastructure (Source: Recorded Future)*

According to a Threat Fabric report on ghost-tapping, the prerequisites for the tactic to be executed include a mobile device with NFC with stolen payment card data linked to a mobile payment system (most often iOS or Android), two mobile devices with NFCGate installed, and a server configured to relay the traffic. NFCGate is an Android application meant to capture, analyze, or modify NFC traffic. It can be used as a research tool to reverse engineer protocols or assess the security of protocols against traffic modifications.

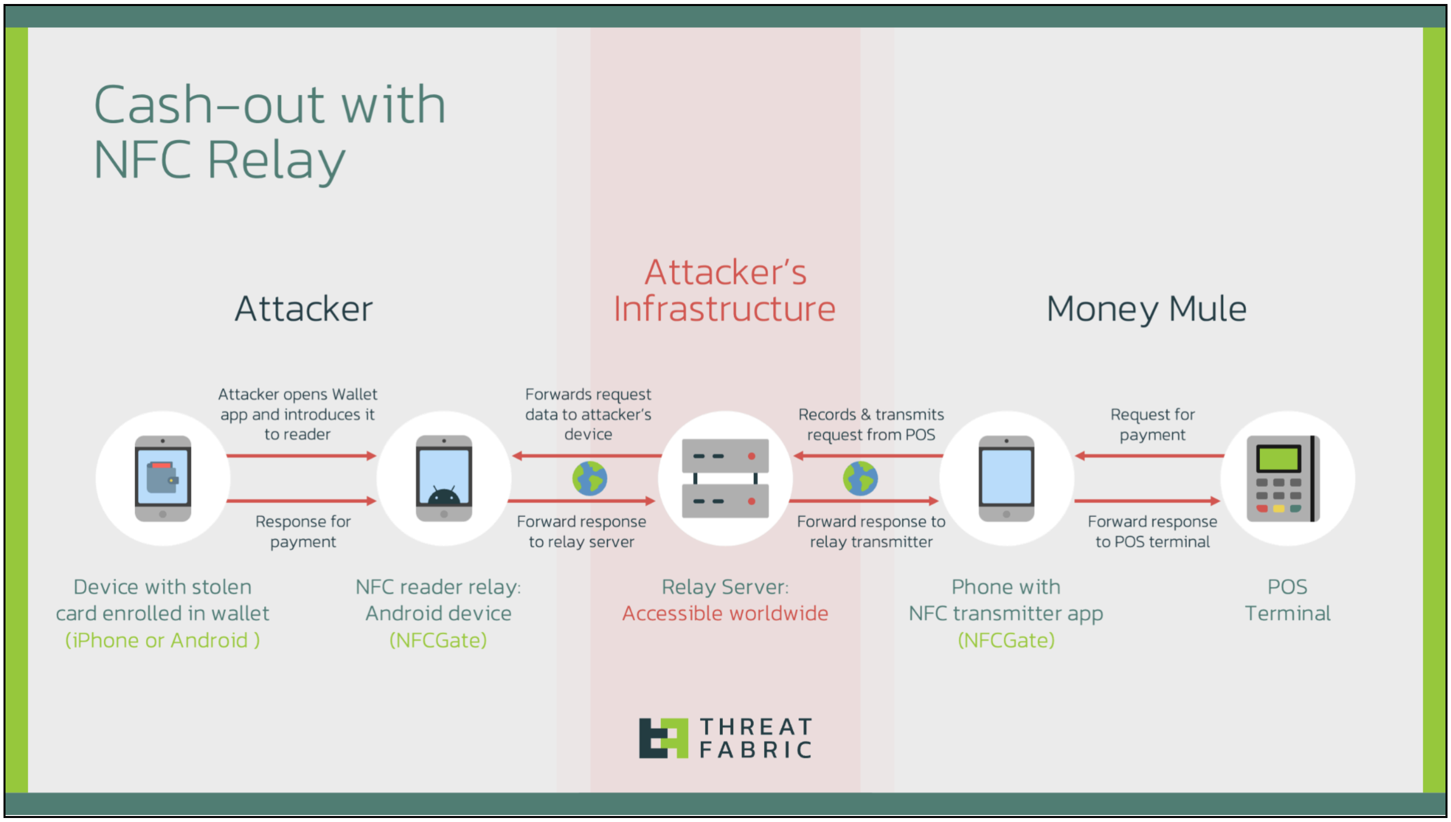

Cash-out with NFC Relay
Attacker
Attacker's Infrastructure
Money Mule
Attacker opens Wallet app and introduces it to reader
Response for payment
Forwards request data to attacker's device
Forward response to relay server
Records & transmits request from POS
Forward response to relay transmitter
Request for payment
Forward response to POS terminal
Device with stolen card enrolled in wallet (iPhone or Android)
NFC reader relay: Android device (NFCGate)
Relay Server: Accessible worldwide
Phone with NFC transmitter app (NFCGate)
POS Terminal
THREAT FABRIC

Figure 2: *Overview of the ghost-tapping technique (Source: Threat Fabric)*

According to the Singapore Police Force, between October 1 and December 2024, there were 656 reports of compromised payment cards involving mobile wallets, with losses amounting to at least $1.2 million SGD ($0.93 million USD). Of these cases, at least 502 reports involved compromised payment cards that were linked to Apple Pay. After successfully linking victims' credit card information to Apple Wallets, mules working for scam syndicates could make in-person purchases using NFC mobile payment methods to buy physical goods in-store, such as high-value electronic items or luxury goods.

In November 2024, The Straits Times reported about an emerging trend of foreign nationals being sent to Singapore by syndicates to commit payment card fraud at retail outlets across the country. Singaporean authorities also warned retailers about syndicates who has supposedly stolen the payment card details of victims through a series of online phishing scams. Stolen payment card details were then loaded onto an unspecified mobile application, which could be controlled remotely and used for contactless payments that work with point-of-sale (POS) terminals. Foreigners are believed to be recruited by transnational syndicates in their home countries via social messaging platforms and instructed to enter Singapore to buy items such as expensive mobile phones, electronic accessories, luxury goods, jewelry, and gold bars. Investigations from the Singapore Police Force revealed that mules recruited by Chinese syndicates also obtained images of fake Japanese passports to be used as proof of identity during the process of in-person purchases at retail stores, and credit card details had been unlawfully obtained through phishing. This case is most likely an example of ghost-tapping, as it involves payment card details loaded onto an unspecified mobile application that can be controlled remotely and used for contactless payments that work with point-of-sale (POS) terminals. The mobile application is most likely used for relaying NFC traffic involving payment card information from another device in real time.

We observed criminals buying and selling stolen goods on criminal sources, such as the Telegram marketplaces Huione Guarantee, Xinbi Guarantee, and Tudou Guarantee. There have been reports (1, 2) of similar cases using the same TTPs involving individuals belonging to different nationalities. While Chinese syndicates do not explicitly mention selling goods on e-commerce websites, criminals have been known to sell stolen goods on eBay (1), Carousell (1), and Mercari (1), among others. We assess with a high degree of confidence that Chinese syndicates are also selling goods bought with stolen payment card information on e-commerce platforms.

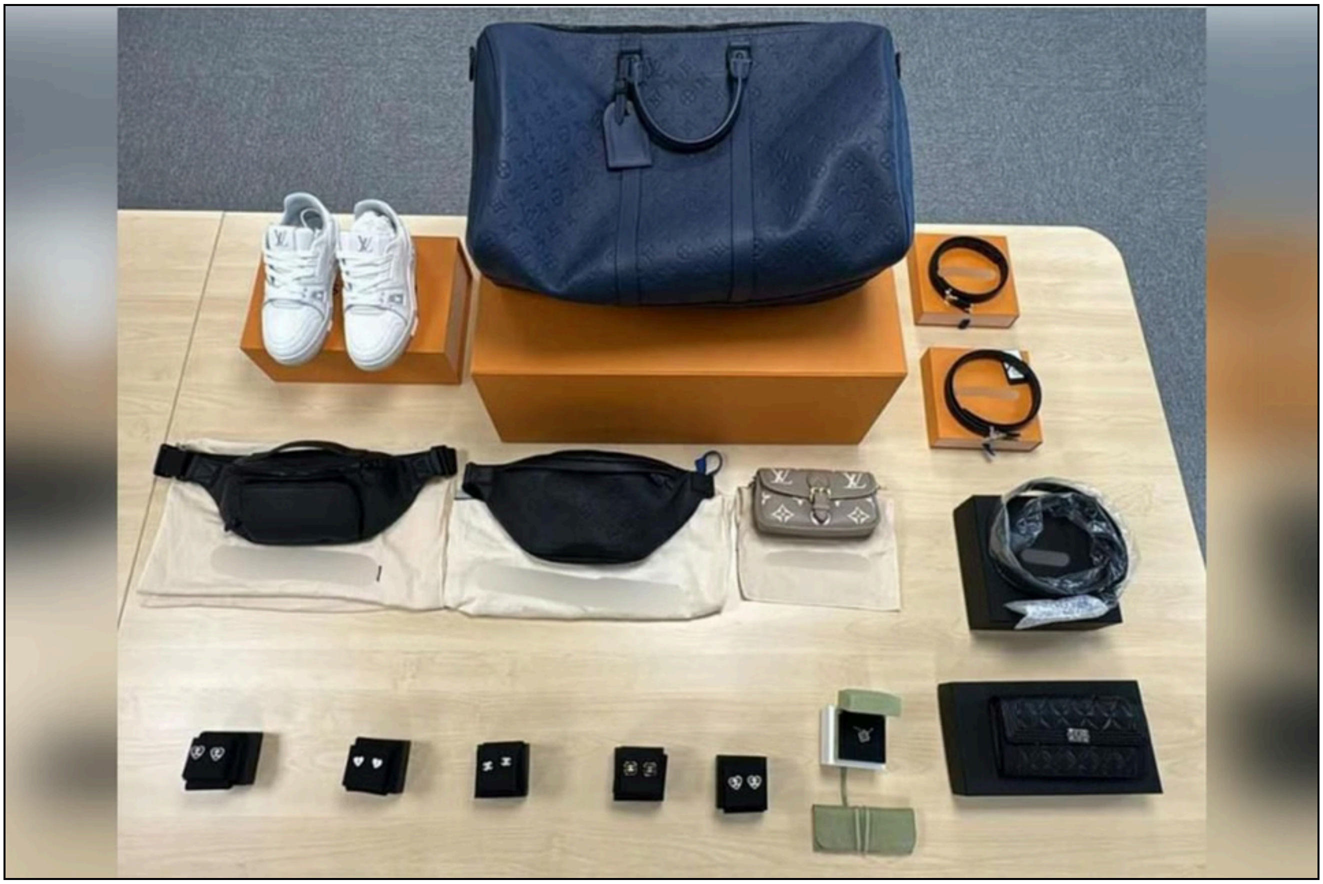


Figure 3: *Luxury goods purchased from various retail stores using ghost-tapping techniques (Source: The Straits Times, photo provided by the Singapore Police Force*)

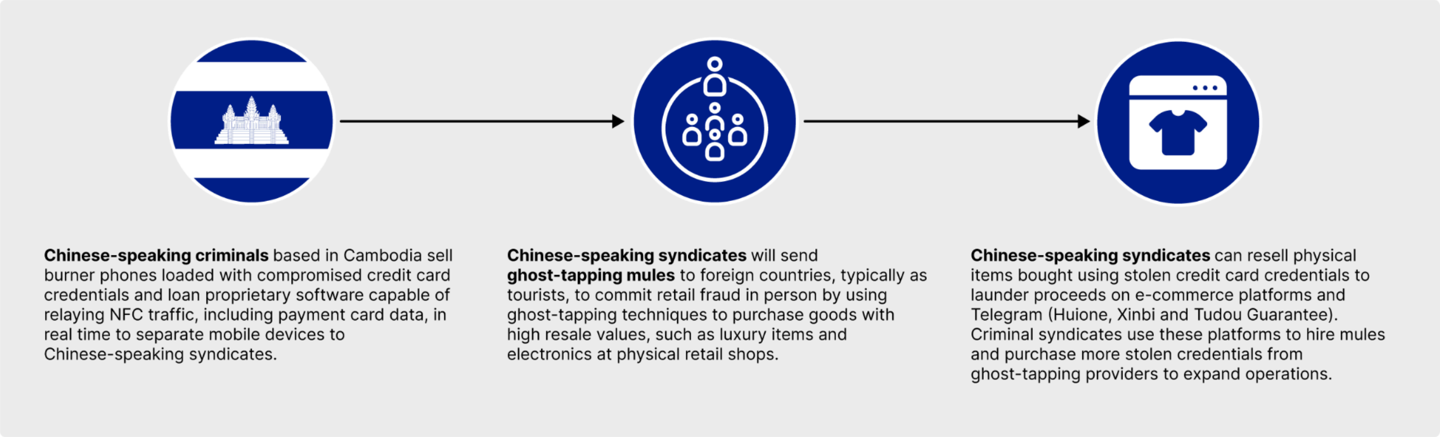
A Singapore Police Force advisory dated February 17, 2025, stated that scammers, who are likely based overseas, obtained card credentials belonging to victims through e-commerce-related phishing websites, including social media advertisements. The advisory states that after obtaining a victim's payment card credentials, a scammer would then add the card details to the Apple Wallet on their own device. An SMS one-time password (OTP) would be sent to the victim, who is then tricked into entering the OTP into the phishing website operated by the scammer, thereby giving the scammer access to the victim's payment card. After successfully taking over the victim's payment card, the scam syndicate would conspire with a money mule to make unauthorized transactions by connecting the mule's mobile device to the scammer's Apple Wallet. The money mule would then be able to make in-person purchases using the contactless payment method (NFC) to buy goods in-store. This police advisory is likely describing ghost-tapping, where there is a need to connect the mule's mobile device to mobile wallets controlled and operated by syndicates remotely.

In April 2025, two Chinese nationals were arrested for smuggling fifteen iPhones into Singapore from China; the individual and an accomplice were instructed by an unspecified syndicate to throw the phones into a trash can outside a local shopping mall. Insikt Group assesses with high confidence that the two individuals are likely transportation mules recruited by a Chinese-speaking syndicate, and the iPhones likely contain stolen payment card credentials that were already linked to Apple Pay. Once retrieved, the syndicate would have used the phones to activate ghost-tapping mules already residing within Singapore, who would then use them to buy physical goods in person. This case is an example of mobile wallet fraud, which involves burner phones loaded with stolen payment card information and does not require the use of NFC relay tactics.

Ghost-Tapping and the Criminal Ecosystem

Since 2024, Insikt Group has observed Chinese cybercriminals operating on Telegram-based escrow platforms, such as Huione Guarantee, Xinbi Guarantee, and Tudou Guarantee, to advertise criminal services and TTPs from general scamming to cryptomining. Through engagements with threat actors involved in different aspects of criminality, we learned that Chinese-speaking criminals involved in scamming-related activities are now adopting ghost-tapping into their attack vectors. We identified that ghost-tapping threat actors are based in Southeast Asian nations, specifically in Cambodia, and have been selling burner phones loaded with payment card credentials belonging to victims to multiple Chinese-speaking syndicates. A single ghost-tapping criminal group possesses the means and ability to provide essential items such as burner phones and loan proprietary software to multiple Chinese-speaking syndicates. This means that the existence of multiple ghost-tapping criminal groups would be able to facilitate a very large number of Chinese-speaking syndicates for many different ghost-tapping campaigns that target multiple businesses — specifically in the retail sector — globally.

In addition to advertising ghost-tapping services, we observed Chinese-speaking syndicates recruiting mules to conduct purchases on the three above-mentioned Telegram marketplaces. The syndicates will usually hire Chinese-speaking mules to conduct operations on their behalf, with mules traveling to foreign countries, such as Singapore, under the guise of tourists to purchase high-value physical goods such as gold, luxury items, and mobile phones. Chinese criminal syndicates will then resell the items on three Telegram marketplaces for cash.



Chinese-speaking criminals based in Cambodia sell burner phones loaded with compromised credit card credentials and loan proprietary software capable of relaying NFC traffic, including payment card data, in real time to separate mobile devices to Chinese-speaking syndicates.

Chinese-speaking syndicates will send **ghost-tapping mules** to foreign countries, typically as tourists, to commit retail fraud in person by using ghost-tapping techniques to purchase goods with high resale values, such as luxury items and electronics at physical retail shops.

Chinese-speaking syndicates can resell physical items bought using stolen credit card credentials to launder proceeds on e-commerce platforms and Telegram (Huione, Xinbi and Tudou Guarantee). Criminal syndicates use these platforms to hire mules and purchase more stolen credentials from ghost-tapping providers to expand operations.

Figure 4: *Overview of the ghost-tapping ecosystem showing how cybercriminals can facilitate ghost-tapping campaigns for multiple Chinese-speaking syndicates (Source: Recorded Future)*

Definition of Different Types of Threat Actors and Mules in the Ghost-Tapping Ecosystem

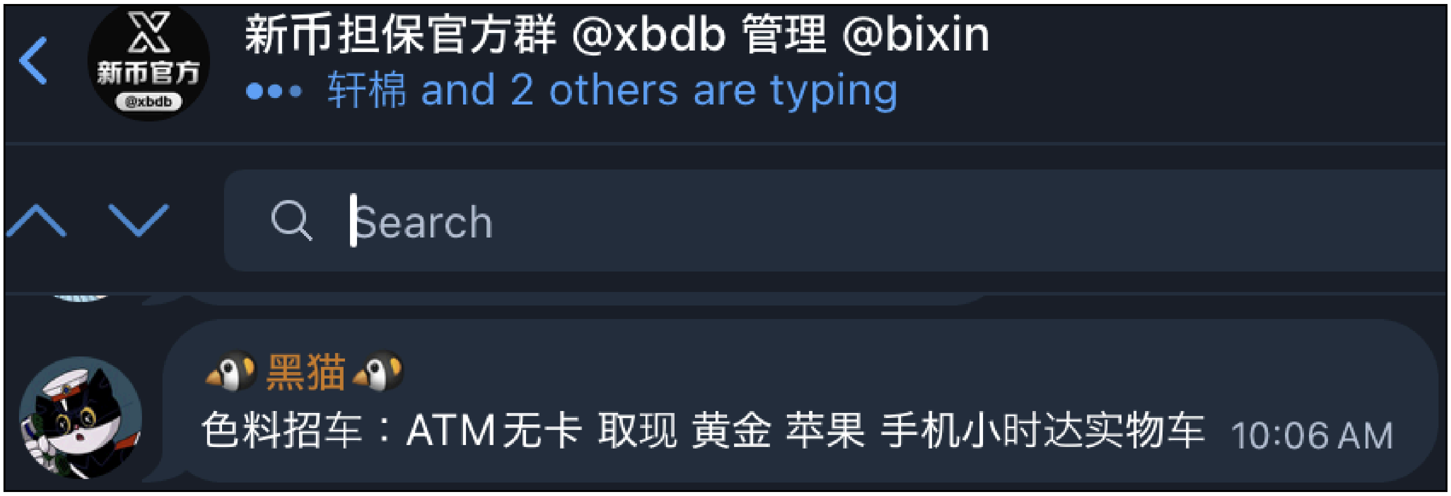
Through observations, threat actor engagements, and open-source intelligence (OSINT) reporting, Insikt Group defines different types of threat actors and their roles within ghost-tapping campaigns as follows:

- **Cybercriminal:** Obtains stolen payment card credentials and links them to contactless payment services such as Apple Pay and Google Pay. Cybercriminals develop software capable of relaying NFC traffic, including payment card data, in real time to other mobile devices, and they typically sell payment card information to syndicates looking to commit retail fraud via ghost-tapping campaigns. Additionally, cybercriminals sell burner phones loaded with stolen payment card credentials to syndicates to commit retail fraud.
- **Syndicate:** In charge of recruiting, training, and instructing different mules for specific purposes to ensure operational success. Chinese-speaking syndicate members typically use Telegram to recruit mules on Huione Guarantee, Xinbi Guarantee, and Tudou Guarantee platforms.
- **Ghost-Tapping Mule:** Conducts retail fraud using ghost-tapping techniques to obtain physical goods, including gold, luxury items, and mobile phones. Mules often enter other countries as tourists, purchase high-value items, and deliver the items to a transportation mule or the syndicate directly.
- **Transportation Mule:** Transports goods within and beyond borders to the desired destination of the syndicate that hired them.
- **Reseller Mule:** Sells items bought using stolen payment card credentials for Tether (USDT) on Huione Guarantee, Xinbi Guarantee, and Tudou Guarantee. We assess that such goods could also be transported and sold in different geographical regions for cash.
- **Money-Laundering Mule:** Transfers money back to bank accounts of syndicate members. The syndicates have been known to use Telegram as a platform to recruit money mules.

- **Buyer**: Chinese-speaking syndicate offering to buy physical goods such as gold, luxury items, and mobile phones in large quantities with cash on Huione Guarantee, Xinbi Guarantee, and Tudou Guarantee platforms.

We assess that cybercriminals may undertake multiple roles and work for multiple syndicates simultaneously due to threat actors constantly advertising for the need of 车队 (motorcade), which indicates there is a high demand for different types of mules to fulfill the objectives of syndicates, such as conducting contactless ATM withdrawals, purchasing physical goods using ghost-tapping techniques, transporting, reselling physical goods, and money-laundering operations.

On Xinbi Guarantee, we observed threat actors offering transportation services for physical goods that can be transported within and across borders for specific countries. For example, the threat actor "路飞" (@OPLuffy888) advertised express transportation services for physical goods on Xinbi Guarantee to transport goods within and beyond Malaysia, Singapore, Indonesia, and Thailand. We also observed "黑猫" (@llan19889) recruiting ATM withdrawal mules and ghost-tapping mules to purchase gold and Apple mobile devices.



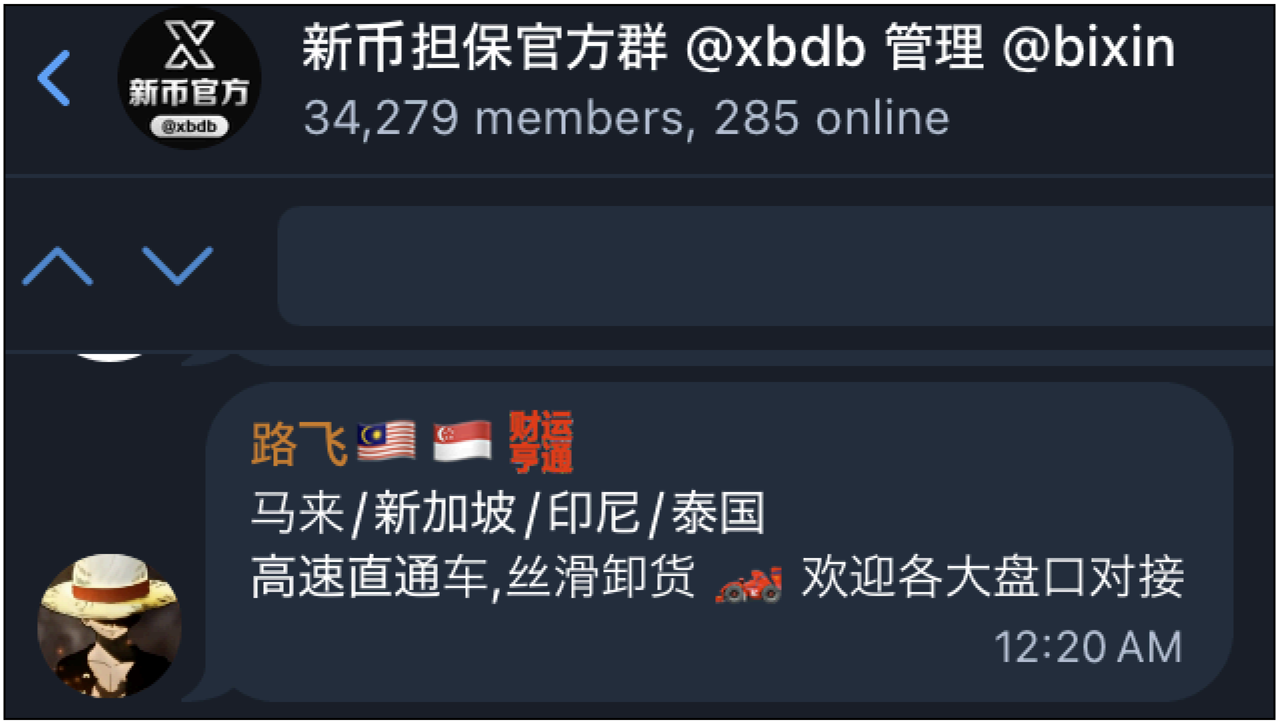
新币担保官方群 @xbdb 管理 @bixin

••• 轩棉 and 2 others are typing

🐧黑猫🐧

色料招车：ATM无卡 取现 黄金 苹果 手机小时达实物车 10:06 AM

Figure 5: *Threat actor 黑猫 (@llan19889) recruiting ATM withdrawal mules and ghost-tapping mules to purchase gold and Apple mobile devices (Source: Telegram)*



新币担保官方群 @xbdb 管理 @bixin

34,279 members, 285 online

路飞 🇲🇾 🇸🇬 财运亨通

马来/新加坡/印尼/泰国

高速直通车,丝滑卸货 🏎️ 欢迎各大盘口对接

12:20 AM

Figure 6: *Threat actor 路飞 (@OPLuffy888) advertising express transportation services for physical goods on Xinbi Guarantee to transport goods within and beyond Malaysia, Singapore, Indonesia, and Thailand (Source: Telegram)*

Huione Guarantee, Xinbi Guarantee, and Tudou Guarantee Facilitating Ghost-Tapping Campaigns

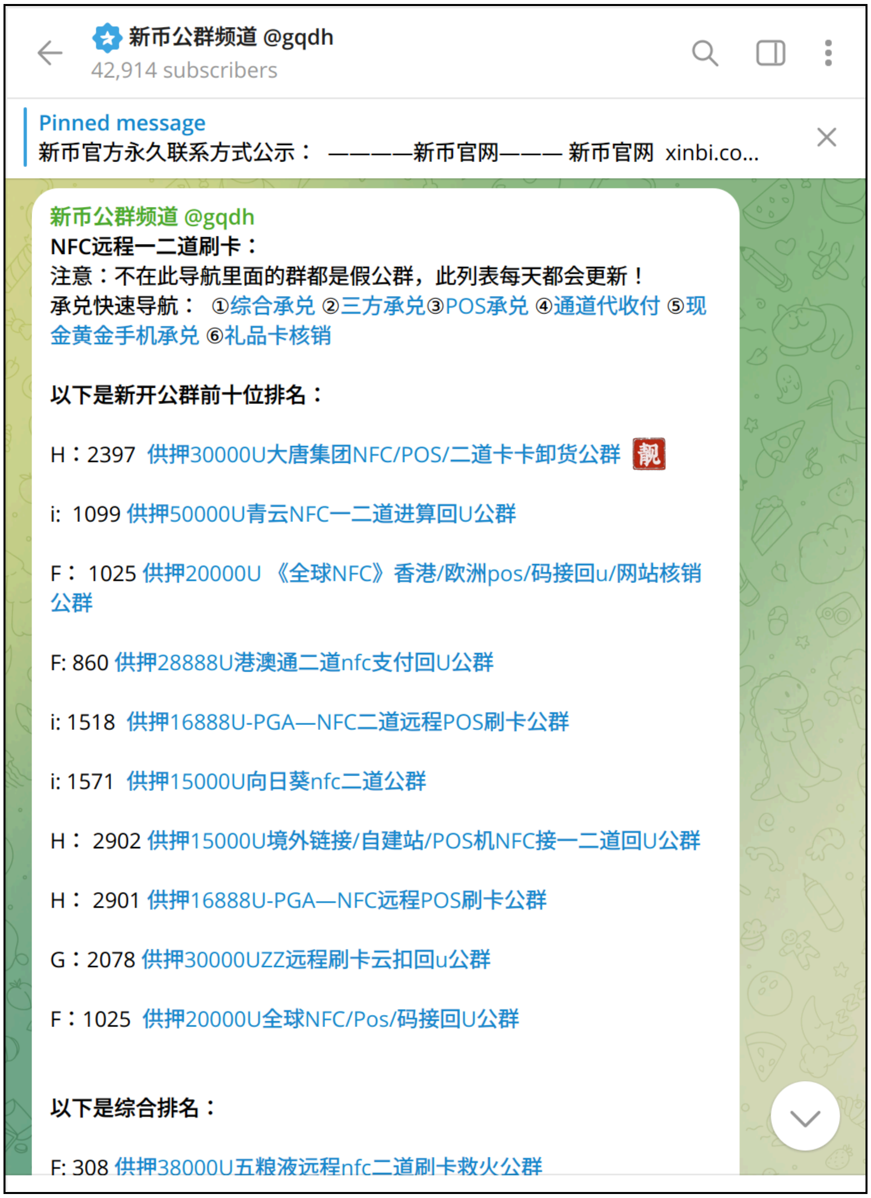
Huione Guarantee (@hwdb) is a Chinese-language clearnet website that operates under the Huione Group, a financial conglomerate based in Cambodia. Huione Guarantee serves as a platform for thousands of public and private Chinese-language Telegram groups that provide various services that enable cybercriminal activities, providing escrow services to Chinese-speaking cybercriminals. Elliptic reported that illicit cryptocurrency-based activities linked to Huione Group reached at least $24 billion. Threat actors advertised the sale of social media and e-commerce accounts, SIM cards, data containing personally identifiable information (PII), malware-as-a-service (MaaS), deepfake technology, KYC bypass services, money-laundering methods and services, and more. For more information about Huione Guarantee, please refer to the Insikt Group report "Huione Guarantee Serves as a One-Stop Shop for Chinese-Speaking Cybercriminals."

Despite Huione Guarantee announcing the shutdown of their operations on May 13, 2025, we observed cybercriminals continuing to use Huione Guarantee's vast infrastructure on Telegram to facilitate criminal activities and dealings. In addition, we observed cybercriminals pivoting to Xinbi Guarantee (@xbdb) and Tudou Guarantee (@tddb), two other Telegram-based marketplaces that function the same way as Huione Guarantee and serve as viable alternatives for Chinese-speaking cybercriminals to continue recruiting members for their cyber, fraud, and scamming campaigns. All deposits have to be made in USDT to a cryptocurrency wallet operated by Xinbi Guarantee and Tudou Guarantee's customer service representatives.

***Figure 7**: Xinbi Guarantee and Tudou Guarantee are platforms that provide escrow services similar to Huione Guarantee to facilitate the hiring of ghost-tapping, transportation, reseller, and money-laundering mules (Source: Recorded Future)*

We observed Chinese-speaking cybercriminals advertising first-hand (一道) and second-hand (二道) payment cards on all three Telegram marketplaces for ghost-tapping campaigns. 远程刷卡 refers to remote card swiping, and in this case, it refers to ghost-tapping operations. Cybercriminals typically use USDT to purchase these payment card details belonging to victims, and the cards are advertised to work globally, including with NFC and POS terminals.

In **Figure 8**, the administrator of Xinbi Guarantee was observed advertising multiple channels involved in ghost-tapping operations on the now-defunct Xinbi Guarantee's public community channel (新币公群频道; @gqdh). The administrator advertised more than ten different channels involved in ghost-tapping campaigns that include first- and second-hand payment cards, which indicates that multiple cybercriminal groups and Chinese-speaking syndicates are actively participating in such campaigns.



新币公群频道 @gqdh
42,914 subscribers

Pinned message
新币官方永久联系方式公示： ————新币官网——— 新币官网 xinbi.co...

新币公群频道 @gqdh
NFC远程一二道刷卡：
注意：不在此导航里面的群都是假公群，此列表每天都会更新！
承兑快速导航： ①综合承兑 ②三方承兑③POS承兑 ④通道代收付 ⑤现金黄金手机承兑 ⑥礼品卡核销

以下是新开公群前十位排名：

H：2397 供押30000U大唐集团NFC/POS/二道卡卡卸货公群 靚

i: 1099 供押50000U青云NFC一二道进算回U公群

F： 1025 供押20000U 《全球NFC》香港/欧洲pos/码接回u/网站核销公群

F: 860 供押28888U港澳通二道nfc支付回U公群

i: 1518 供押16888U-PGA—NFC二道远程POS刷卡公群

i: 1571 供押15000U向日葵nfc二道公群

H： 2902 供押15000U境外链接/自建站/POS机NFC接一二道回U公群

H： 2901 供押16888U-PGA—NFC远程POS刷卡公群

G：2078 供押30000UZZ远程刷卡云扣回u公群

F：1025 供押20000U全球NFC/Pos/码接回U公群

以下是综合排名：

F: 308 供押38000U五粮液远程nfc二道刷卡救火公群

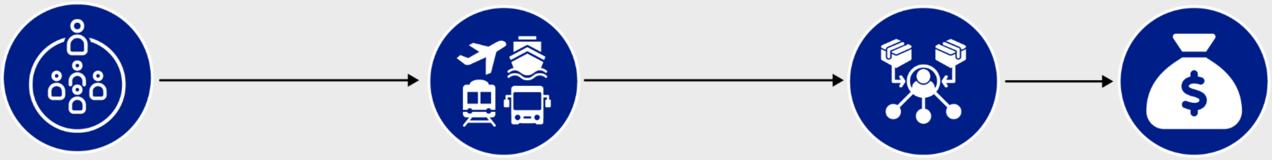
Figure 8*: An administrator of Xinbi Guarantee posting an advertisement about using first- and second-hand victim payment card credentials for ghost-tapping campaigns worldwide; the Telegram channel @gqdh, which used to be Xinbi Guarantee's public community Telegram channel, has been deleted by Telegram, likely due to a violation of use terms (Source: Telegram)*

Reselling of Goods to Launder Funds

On Huione Guarantee, Xinbi Guarantee, and Tudou Guarantee platforms, we observed threat actors offering to purchase and sell physical items obtained through illicit means in large quantities. Chinese-speaking syndicates typically do not specify how and where they obtained such physical items, but through our research, we believe there are two common methods: ghost-tapping campaigns and e-commerce fraud. The e-commerce method is considered more risky due to more digital and physical footprints, as key details such as online card payment details, physical addresses, and phone numbers are required. In comparison, ghost-tapping campaigns are much harder to detect by law enforcement agencies, and mules can travel to foreign countries and purchase physical goods on behalf of syndicates. These in-person transactions performed by mules grant syndicates the advantage of obtaining goods immediately and with greater control, often issuing specific instructions in real time to mules to deliver the goods to specific locations that could remain unknown to authorities for prolonged periods of time.

Due to the large number of advertisements regarding ghost-tapping campaigns and recruitment of mules to purchase physical goods using ghost-tapping techniques, all being discussed and advertised together on Huione Guarantee, Xinbi Guarantee, and Tudou Guarantees, coupled with OSINT articles and a Singapore Police Force advisory (1, 2, 3) detailing ghost-tapping crimes, we believe with a high degree of confidence that a large number of physical goods being sold on these Chinese cybercrime marketplaces are obtained through ghost-tapping techniques.

Based on advertisements on the three above-mentioned Telegram channels, **Figure 9** illustrates how physical goods get transported and resold for cash as part of money-laundering operations by Chinese-speaking syndicates. It is highly likely that Chinese-speaking syndicates involved in ghost-tapping campaigns will resell physical items bought with stolen payment card credentials for cash.



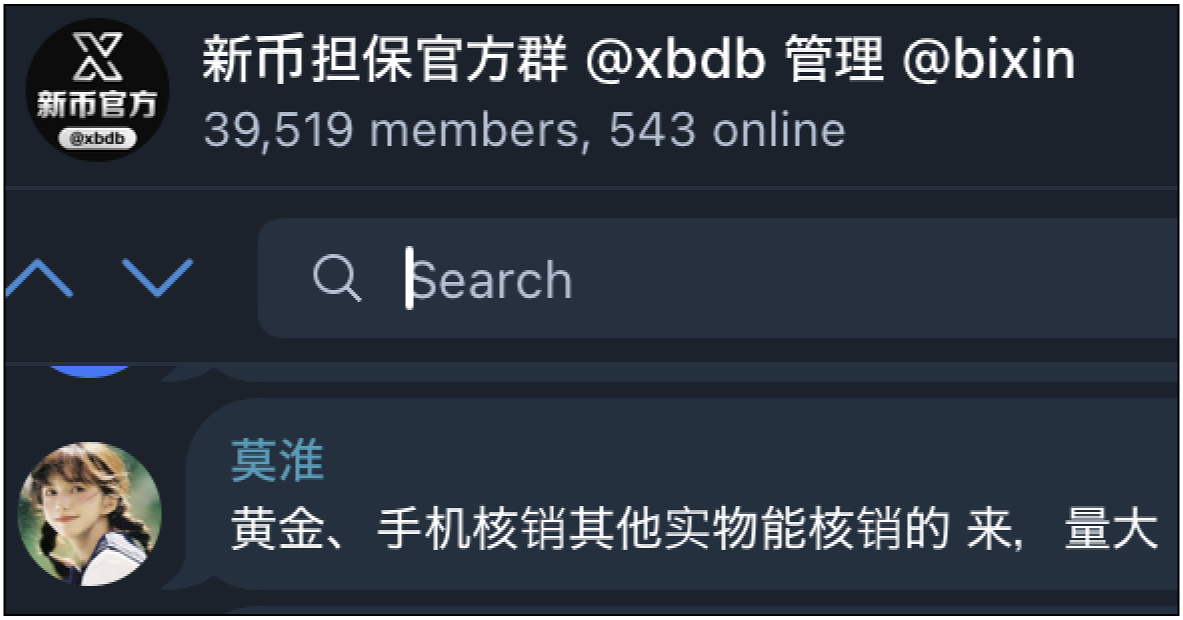
Ghost-tapping mules belonging to syndicates will pass physical goods bought with stolen credit card credentials to **transportation mules.**

Transportation mules will facilitate the transportation of physical goods bought with stolen payment card information to the syndicates' desired location. Chinese-speaking syndicates advertised gold, iPhones, and luxury goods for cash on Telegram marketplaces. Alternatively, we also observed syndicates hiring mules to resell physical items on these platforms.

Reseller mules are suspected to transfer proceeds to **money laundering mules** after selling stolen goods for cash proceeds. Money laundering mules will then transfer proceeds online back to the Chinese-speaking syndicates' bank accounts.

Figure 9*: How physical goods get transported and resold for USDT/cash as part of money laundering operations by Chinese-speaking syndicates (Source: Recorded Future)*

For example, we observed the threat actor “莫淮” (@eyDLBhqqotRXfJ) buying gold, mobile phones, and other physical goods that syndicates can offload in large quantities on Xinbi Guarantee.



新币担保官方群 @xbdb 管理 @bixin
39,519 members, 543 online

莫淮
黄金、手机核销其他实物能核销的 来，量大

Figure 10: *Threat actor 莫淮 (@eyDLBhqqotRXfJ) offering to buy gold, mobile phones, and other physical goods that can be offloaded by syndicates in large quantities on Xinbi Guarantee (Source: Telegram)*

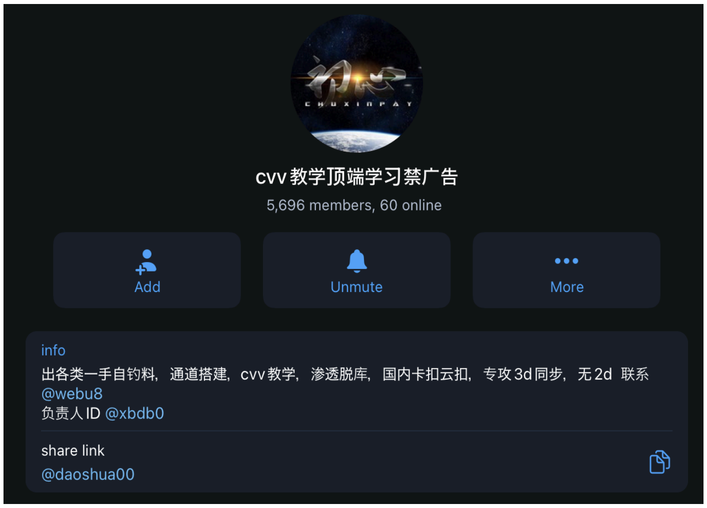
Threat Analysis and Engagements

Insikt Group conducted engagements with two Telegram monikers involved in different aspects of the ghost-tapping ecosystem: @webu8 (developer of proprietary software used in ghost-tapping) and @xingma888 (controller and recruiter of mules who purchase and resell luxury goods purchased through ghost-tapping). These engagements gave us valuable insights into the organization, structure, security measures, and TTPs used by these threat actors and their associates.

@webu8: Ghost-Tapping Software Developer

Background

Insikt Group discovered a public Chinese-language Telegram channel, cvv教学顶端学习禁广告 (@daoshua00), which has 5,695 members as of writing. This channel promotes ghost-tapping and carding-related services, as well as materials used in ghost-tapping campaigns, specifically first-hand phishing materials, penetration techniques, CVV tutorials, ATM card cloning, and exfiltration of databases. The administrators of this channel operate the Telegram handles @webu8 and @xbdb0. We note that @xbdb0 is similar to Xinbi Guarantee's Telegram channel (@xbdb), and through our engagement with @xbdb0, the threat actor claimed they have connections with Xinbi Guarantee. We observed the administrators posting photos and video demonstrations of ghost-tapping for syndicates interested in conducting ghost-tapping campaigns. The videos and photos mainly consisted of cash, multiple burner mobile phones with compromised payment cards linked to Apple Pay and Google Pay services, cloned payment cards, and POS terminals. Individuals were asked to contact @webu8 for more information. We engaged with @webu8 and managed to get information and the description of the software being used for ghost-tapping purposes.



cvv 教学顶端学习禁广告

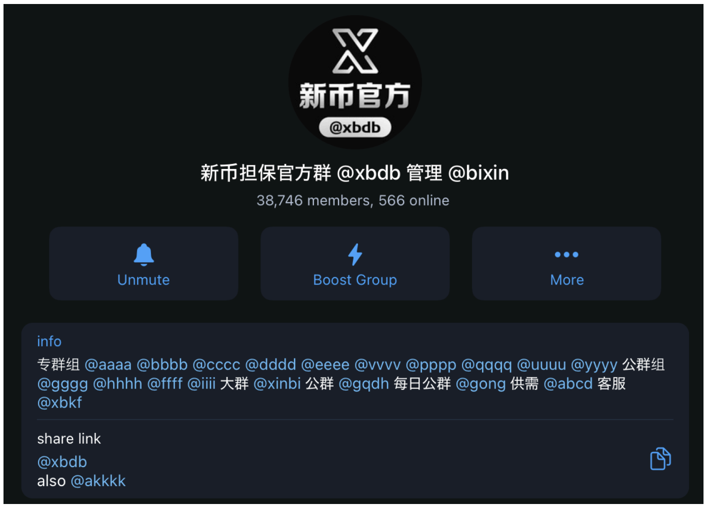
5,696 members, 60 online

info

出各类一手自钓料，通道搭建，cvv 教学，渗透脱库，国内卡扣云扣，专攻 3d 同步，无 2d 联系 @webu8
负责人 ID @xbdb0

share link

@daoshua00



新币担保官方群 @xbdb 管理 @bixin

38,746 members, 566 online

info

专群组 @aaaa @bbbb @cccc @dddd @eeee @vvvv @pppp @qqqq @uuuu @yyyy 公群组 @gggg @hhhh @ffff @iiii 大群 @xinbi 公群 @gqdh 每日公群 @gong 供需 @abcd 客服 @xbkf

share link

@xbdb
also @akkkk

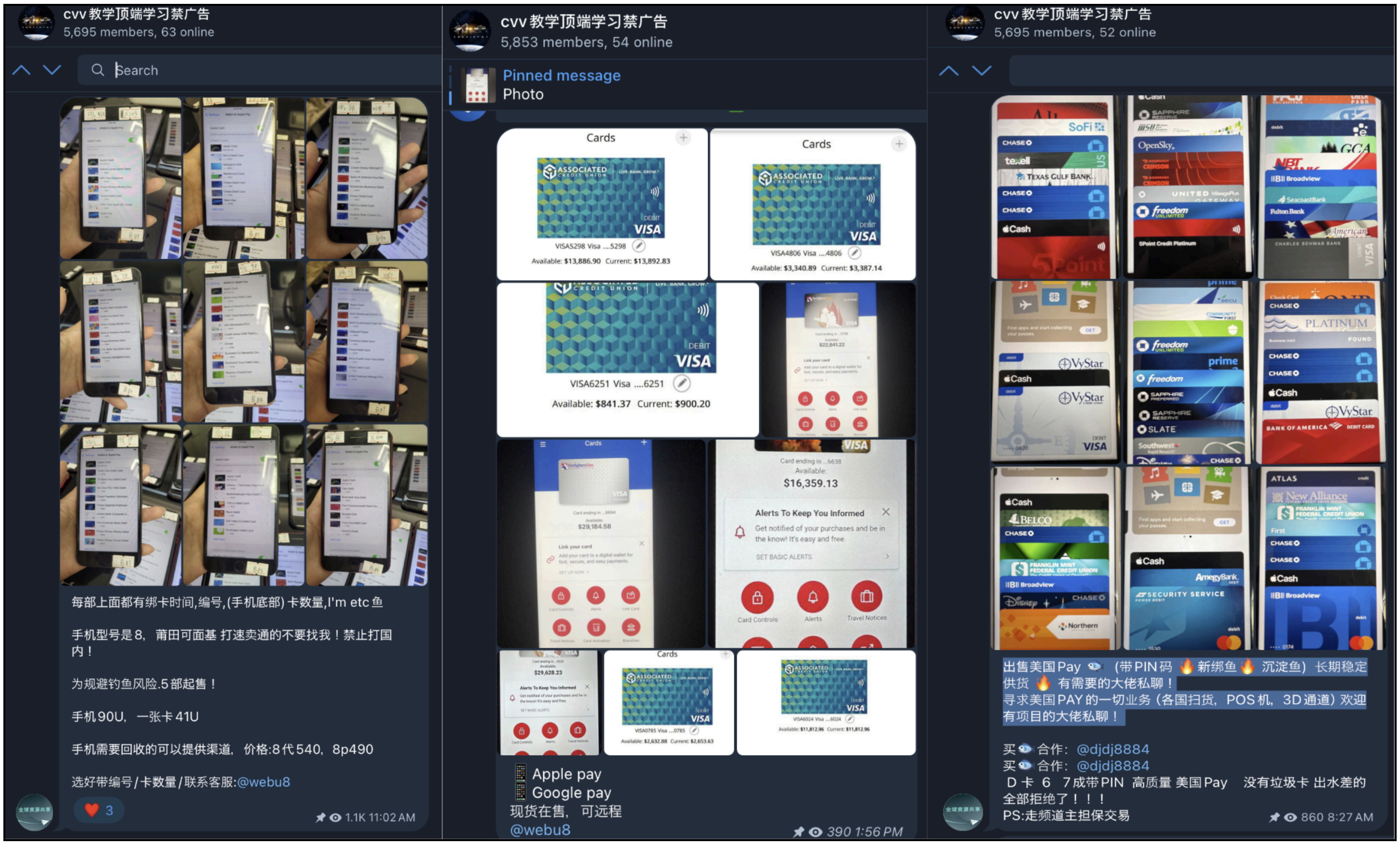
Figures 11 and 12: *(Left) Administrators of @daoshua are @webu8 and @xbdb0 (Source: Telegram); (Right) Xinbi Guarantee's Telegram channel's sharelink is @xbdb, which is very similar to the administrator of @daoshua00, whose moniker is @xbdb0; through engagement, @xbdb0 claimed to have connections with Xinbi Guarantee (Source: Telegram)*

The three images below, shown in **Figure 13**, showcase @webu8's advertisements on the Telegram channel @daoshua00.

The first image on the left shows multiple burner phones tagged with linked payment card credentials. Each phone is tagged with a card binding time (day and month the payment card was linked to the burner phone) and the quantity of compromised payment cards linked. The price of each phone is 90 USDT (approximately $90), and each linked card is 41 USDT (approximately $41); a minimum purchase of five burner mobile phones is required. If a burner phone contains ten linked compromised payment cards, the price of the phone is $500 USDT. The burner phone can be purchased in Putian City, Fujian Province, China. The threat actor used the Chinese text 莆田可面基 打速卖通的不要找我！禁止打国内!, which translates to: "Able to meet in Putian, please do not contact me if you use AliExpress! Domestic calls are prohibited!" Insikt Group assessed that such measures are to maintain anonymity and avoid detection by China's law enforcement agencies, and having in-person meetups would be more secure to build a strong and stable relationship among Chinese cybercriminals. @webu8 also provided a phone recycling service for Chinese-speaking syndicates, likely to load new compromised payment card credentials into existing burner phones. We note that in August 2023, law enforcement agencies in Singapore arrested ten Chinese-speaking syndicate members originating from Fujian, China, and seized assets worth $3 billion Singapore dollars ($2.33 billion USD). The members are linked to unlicensed money lending in China, scams, and remote online gambling operations in the Philippines. Insikt Group is unable to confirm whether @webu8 and @xbdb0 are linked to the same syndicate whose members were arrested in 2023.

The second image in the middle showcases @webu8 advertising stolen card credentials linked to an unspecified contactless payment system, with payment card values indicating available remaining credit. The threat actor claims these cards are compatible with Apple Pay and Google Pay, have ready stocks for sale, and can be used for ghost-tapping purposes.

The third image on the right showcases @djdj8884, another ghost-tapping seller, advertising US payment cards with PIN codes obtained from phishing campaigns. The threat actor is seeking to supply newly phished payment cards regularly to Chinese-speaking syndicates. The cards are advertised to be compatible with making payments to purchase physical goods over POS machines. The screenshot shows burner phones loaded with multiple cards, indicating that the buyer can load the payment card information, together with PIN codes, into their own burner phones.



每部上面都有绑卡时间,编号,(手机底部) 卡数量,I'm etc 鱼

手机型号是8，莆田可面基 打速卖通的不要找我！禁止打国内！

为规避钓鱼风险.5部起售！

手机90U，一张卡41U

手机需要回收的可以提供渠道，价格:8代540，8p490

选好带编号/卡数量/联系客服:@webu8

❤️ 3 1.1K 11:02 AM

Apple pay
Google pay
现货在售，可远程
@webu8

390 1:56 PM

出售美国Pay 🐟 （带PIN码 🔥 新绑鱼 🔥 沉淀鱼）长期稳定供货 🔥 有需要的大佬私聊！
寻求美国PAY的一切业务（各国扫货，POS机，3D通道）欢迎有项目的大佬私聊！

买 🐟 合作：@djdj8884
买 🐟 合作：@djdj8884
D卡 6 7成带PIN 高质量 美国Pay 没有垃圾卡 出水差的全部拒绝了！！！
PS:走频道主担保交易

860 8:27 AM

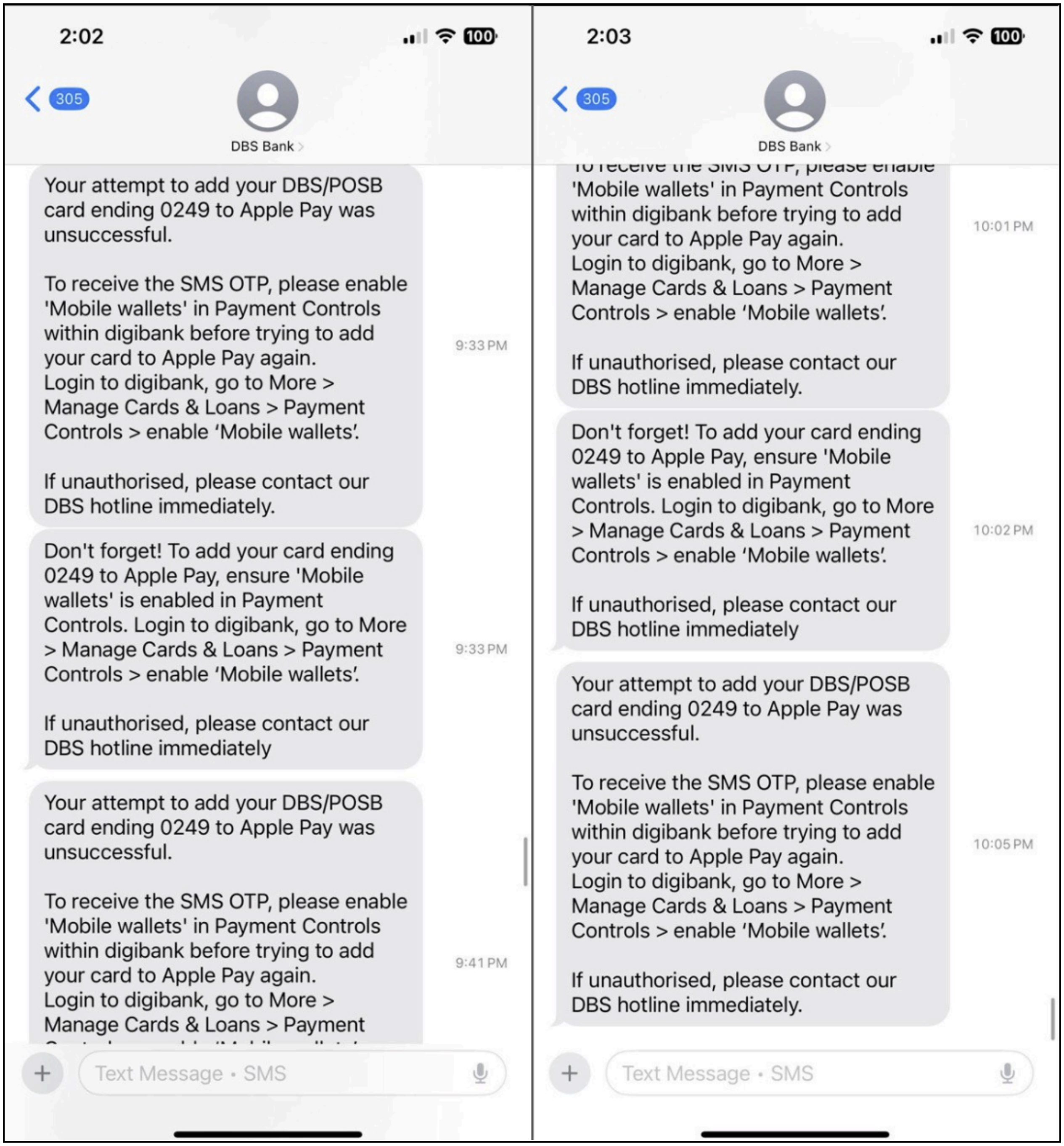
***Figure 13**: @webu8 advertising burner iPhones loaded with stolen payment card credentials; each mobile phone is tagged with a serial number, and all phones are either set to airplane mode or have no SIM cards inside (Source: Telegram)*

From these three images, we observed two business models used by ghost-tapping criminals:

1. @webu8 threat group's business model is to load compromised payment card credentials onto burner phones, getting syndicate members to deal in person with the buyer located in "Putian", a city in Fujian Province, China. For this business model, the buyer is getting burner phones that are already loaded successfully and ready for ghost-tapping campaigns.

2. @djdj8884 threat group's business model sells compromised payment card credentials in bulk, together with PIN codes to other Chinese-speaking syndicate members, where transactions can be conducted remotely. For this business model, the buyer is responsible for loading compromised payment card credentials into their own burner phones to prepare for future ghost-tapping campaigns. Insikt Group assessed that this business model requires more preparation time, as not all compromised cards can be loaded into a contactless payment system due to varying security measures employed by different banks.

We also obtained evidence through proprietary means that cybercriminals are automating the process of linking compromised card credentials to contactless payment systems on burner phones. The screenshot below shows automated attempts to add a compromised payment card belonging to DBS Bank to Apple Pay at intervals of every four to eight minutes. In this case, DBS Bank employs a security feature that requires an individual to log in to their mobile application to authorize the linking of their payment cards to a mobile wallet such as Apple Pay or Google Pay. Customers who wish to add their DBS card must first turn on the "Mobile wallets" toggle in Payment Controls within the DBS digibank app. To further protect users, this "Mobile wallets" feature will be automatically turned off if the card is not added to any mobile wallet within ten minutes. However, in the event that an individual's bank login details are compromised due to mobile malware or through social engineering techniques, this security feature will not be able to prevent cybercriminals from linking compromised payment cards to contactless payment systems.



Your attempt to add your DBS/POSB card ending 0249 to Apple Pay was unsuccessful.

To receive the SMS OTP, please enable 'Mobile wallets' in Payment Controls within digibank before trying to add your card to Apple Pay again.
Login to digibank, go to More > Manage Cards & Loans > Payment Controls > enable 'Mobile wallets'.

If unauthorised, please contact our DBS hotline immediately.

9:33 PM

Don't forget! To add your card ending 0249 to Apple Pay, ensure 'Mobile wallets' is enabled in Payment Controls. Login to digibank, go to More > Manage Cards & Loans > Payment Controls > enable 'Mobile wallets'.

If unauthorised, please contact our DBS hotline immediately

9:33 PM

Your attempt to add your DBS/POSB card ending 0249 to Apple Pay was unsuccessful.

To receive the SMS OTP, please enable 'Mobile wallets' in Payment Controls within digibank before trying to add your card to Apple Pay again.
Login to digibank, go to More > Manage Cards & Loans > Payment

9:41 PM

To receive the SMS OTP, please enable 'Mobile wallets' in Payment Controls within digibank before trying to add your card to Apple Pay again.
Login to digibank, go to More > Manage Cards & Loans > Payment Controls > enable 'Mobile wallets'.

If unauthorised, please contact our DBS hotline immediately.

10:01 PM

Don't forget! To add your card ending 0249 to Apple Pay, ensure 'Mobile wallets' is enabled in Payment Controls. Login to digibank, go to More > Manage Cards & Loans > Payment Controls > enable 'Mobile wallets'.

If unauthorised, please contact our DBS hotline immediately

10:02 PM

Your attempt to add your DBS/POSB card ending 0249 to Apple Pay was unsuccessful.

To receive the SMS OTP, please enable 'Mobile wallets' in Payment Controls within digibank before trying to add your card to Apple Pay again.
Login to digibank, go to More > Manage Cards & Loans > Payment Controls > enable 'Mobile wallets'.

If unauthorised, please contact our DBS hotline immediately.

10:05 PM

***Figure 14**: An example of automated attempts to add a compromised payment card belonging to DBS Bank to Apple Pay at intervals of four to eight minutes via SMS; this automation technique can likely be applied to any banking institution (Source: Recorded Future Proprietary Data)*

Engagement

Insikt Group engaged with @webu8 to find out more about ghost-tapping. The threat actor claimed that their ghost-tapping technique can be applied in any country and that the scheme involves a type of proprietary software capable of relaying payment card data to other mobile devices, which they develop and update regularly. The threat actor mentioned they would lend the proprietary software to us for free if we purchased compromised payment card credentials from them, and a member of their team would guide us on how to use it.

From this engagement, we learned that this threat group not only sells burner phones loaded with compromised payment card details, as shown in **Figure 13**, but also sells compromised payment card details directly to other Chinese syndicates through the use of proprietary software capable of relaying payment card information in real time. This criminal group orchestrating ghost-tapping schemes is unwilling to hire mules to conduct retail fraud using ghost-tapping methods by themselves and does not bear any risk of getting caught by law enforcement agencies while conducting retail fraud.

Chinese-speaking syndicates that purchase compromised payment card information, or burner phones loaded with compromised card information from this ghost-tapping threat group, are responsible for sending ghost-tapping mules to commit retail fraud or contactless NFC ATM withdrawal in person, where mules bear the greatest risk of being arrested by law enforcement agencies.

Due to the threat actor's request to meet in person to discuss more business details in Cambodia, we assess with high confidence that well-established Chinese-speaking syndicates operating in Southeast Asia have members physically located in Cambodia who could discuss terms and conditions further. We also interpret the request for a physical meetup as a method used by the threat actor to filter out less-prominent criminal gangs and as a desire to conduct business with more well-established syndicates on a much larger scale to maximize their profits.

According to Cleafy, the "SuperCard X" MaaS offering was created by a Chinese-speaking threat actor and shares similarities with the proprietary software @webu8 mentioned. According to Cleafy, the "Reader" application contains an embedded file that stores multiple "Answer To Reset" (ATR) messages. These messages, typically used to initiate and negotiate communication parameters between a smart card and an NFC reader, are reused to facilitate card emulation. When the "Reader" captures and relays a victim's card data, the corresponding ATR is transmitted via the command-and-control (C2) infrastructure to the "Tapper" device that is going to use this message to emulate a virtual card, effectively deceiving POS terminals or ATMs into recognizing it as a legitimate physical card. By leveraging ATRs, SuperCard X enables seamless, real-time relay attacks, allowing threat actors to bypass physical proximity constraints and carry out fraudulent transactions. Insikt Group is unable to confirm whether the SuperCard X platform application is the proprietary software used by @webu8 due to the existence of multiple ghost-tapping criminals advertising similar schemes on Huione Guarantee, Xinbi Guarantee, and Tudou Guarantee.

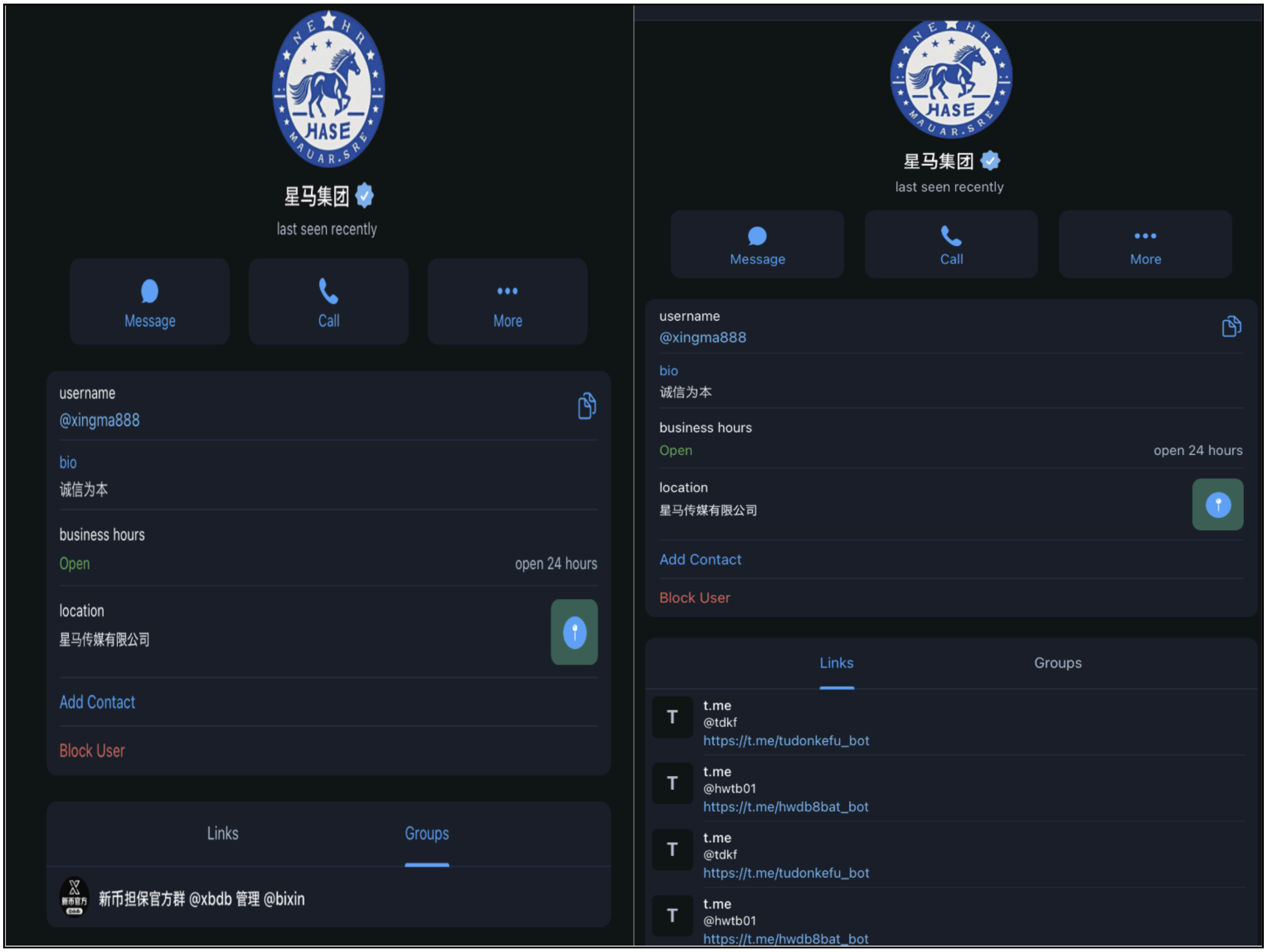
Cleafy also identified a SuperCard X campaign targeting Italy and found evidence that suggests custom builds tailored for specific affiliates or regional operations. This research corroborates @webu8's claim that their ghost-tapping attack vector could be conducted anywhere in the world and that such proprietary software could be loaned to non-Chinese-speaking syndicates.

Insikt Group also published a report titled "SuperCard X MaaS Expands Infrastructure, Likely Targeting High-Profile Organizations," which builds upon Cleafy's research on the SuperCard X campaign.

@xingma888: Reseller and Mule Controller

Background

On Xinbi Guarantee, we engaged with the threat actor "星马集团" (@xingma888; translates to "Singapore and Malaysian organization"), who is involved with laundering funds into physical goods and cashing out. Through our conversations, we identified that the threat actor is part of a Chinese-speaking ghost-tapping syndicate that operates in Singapore and Malaysia. This threat actor engagement sheds light on how Chinese-speaking syndicates operate and how platforms such as Huione Guarantee, Xinbi Guarantee, and Tudou Guarantee facilitate ghost-tapping campaigns and other forms of cybercrime.



username
@xingma888

bio
诚信为本

business hours
Open — open 24 hours

location
星马传媒有限公司

新币担保官方群 @xbdb 管理 @bixin

username
@xingma888

bio
诚信为本

business hours
Open — open 24 hours

location
星马传媒有限公司

t.me
@tdkf
https://t.me/tudonkefu_bot

t.me
@hwtb01
https://t.me/hwdb8bat_bot

t.me
@tdkf
https://t.me/tudonkefu_bot

t.me
@hwtb01
https://t.me/hwdb8bat_bot

***Figure 15:** @xingma888 is a member of Xinbi Guarantee and is open to using Xinbi, Huione, or Tudou Guarantee's escrow service to deal with other Chinese-speaking threat actors (Source: Recorded Future)*

Engagement

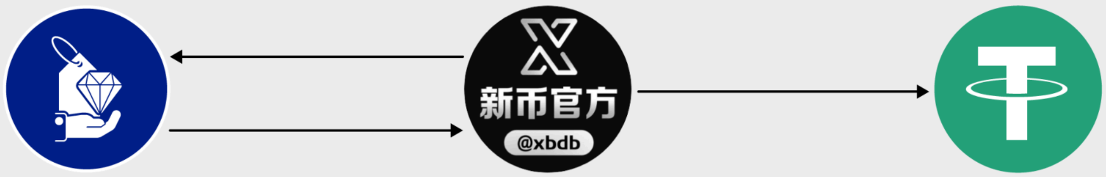
During an engagement, we learned that @xingma888 is able to supply a “motorcade” (车队) — mules for ghost-tapping campaigns to make in-person purchases at retail stores in Singapore and Malaysia. Threat actors requiring such services will have to specify what kind of physical goods they wish to obtain, and @xingma888 will quote the deposit amount required to mobilise the mules for the ghost-tapping campaign. The deposit amount must be paid in USDT to an escrow system belonging to either Huione, Tudou, or Xinbi Guarantee. In a manner similar to placing an order, the buyer has to provide a physical address for mules working for @xingma888 to deliver the physical goods. @xingma888 stated that after successfully delivering the goods, the buyer should take a video of the unboxing process and verify the authenticity of the items, then proceed to ask the customer service officer belonging to an escrow system of the buyer’s choice to release the amount of USDT to @xingma888.

Taking into account details of multiple threat engagements with different cybercriminals involved in ghost-tapping campaigns, as well as open-source articles reporting about syndicates funding transportation costs and air tickets for mules, Insikt Group assesses with a high level of confidence that @xingma888 funds the following:

- Burner phones loaded with stolen payment card credentials
- Transportation costs, such as airline tickets for mules
- Accommodation for mules
- USDT or cash to recruit and pay mules
- A money mule to launder USDT into fiat currency

Meanwhile, prospective buyers, which usually refers to Chinese syndicates, will be able to resell the physical goods bought via ghost-tapping campaigns for cash, successfully converting USDT into fiat currency through this cash-out method. In most cases, the prospective buyer will have to pay a greater amount of USDT to mule handlers such as @xingma888. We also assess that syndicates will likely need to recruit reseller mules to resell the physical goods for cash. Insikt Group has yet to factor in the cost of obtaining USDT in the first place, which is most likely obtained through illicit means involving cybercrime, illegal online gambling, and scams, where Southeast Asia is a hotbed for Chinese criminal gangs.

Figure 16 illustrates how a Telegram-based escrow system, such as Xinbi Guarantee, helps to facilitate and mediate transactions between Chinese-speaking syndicates and mule controllers, such as @xingma888, looking to work together, as well as an overview of the financial gains each party receives during the process.



Buyers will receive and resell physical goods such as mobile phones and luxury goods for cash, which will help them successfully launder USDT into cash. In most cases, the prospective buyer will have to pay a greater amount of USDT to mule handlers such as @xingma888.

Buyer has to deposit USDT based on agreed terms with @xingma888 into an escrow system such as Xinbi Guarantee. Upon confirmation of receipt of goods, the buyer will ask the escrow service to release the deposited USDT to @xingma888.

@xingma888 will receive USDT for each physical item delivered, which will have to be used to fund the recruitment of ghost-tapping, transportation, and money laundering mules; ghost-tapping criminals and burner phones loaded with compromised credit card credentials; air tickets; and accommodation for mules.

Figure 16: *Overview of mutual gains when syndicates work with mule controllers such as @xingma888 to cash out illicitly obtained USDT for fiat currency through ghost-tapping campaigns based on our threat actor engagement (Source: Recorded Future)*

Mitigations

For banks and payment providers:

- Banks should introduce security measures to prevent payment card phishing fraud, such as a security feature that requires the individual to log in to their own bank account to authorize the linking of their payment card to a mobile wallet. This feature should turn off automatically if the card is not added to any mobile wallet within a designated short time frame.
- Card issuers should consider alternatives to SMS- or email-based OTPs for device wallet authentication and activation. These may include automated or “manned” calls with customer service or push provisioning from the issuer’s official mobile application, which are less susceptible to phishing.
- In scenarios where SMS- or email-based OTPs are still used, card issuers should consider placing the OTP in the second half of messages and excluding it from preview text on mobile home screens, increasing the chance that a cardholder notices suspicious activity.
- Analyze device risk factors before allowing a payment card to be added to a digital wallet. Enforce stricter authentication when a card is being added from an unrecognized device or location.
- Flag transactions where the same payment card is used in geographically distant locations within an unrealistic timeframe.
- Analyze patterns where multiple cards are linked to the same device, particularly following known phishing incidents.
- Leverage machine learning models to recognize the characteristics of relayed payments and device behavior anomalies related to NFC relay fraud.
- Allow customers to verify high-risk transactions or digital wallet provisioning attempts via their banking app before finalizing them.

For consumers:

- Individuals should contact their respective banking institutions and block their access to their compromised payment cards as soon as they receive notifications of unauthorized use.

- Individuals should not download third-party mobile applications outside official App stores.
- Individuals should not add payment card information to any unknown or untrustworthy websites and should not share any OTPs or PINs with anyone. Changing their payment card PIN regularly and monitoring payment card transactions can help reduce the chance of payment card phishing.
- Individuals should be wary of scammers impersonating bank personnel and should contact the bank through their official banking hotline to obtain and clarify information regarding their own banking matters.

For law enforcement:

- Collaborate with payment networks, financial institutions, and digital platforms to identify and track emerging trends related to NFC relay fraud and payment card phishing.
- Support efforts to dismantle infrastructure used to distribute phishing kits and mobile malware used in payment credential theft schemes.

Outlook

Insikt Group believes that Chinese-speaking syndicates are pivoting toward using ghost-tapping as an attack vector to commit retail fraud and launder funds from goods purchased with compromised payment cards. We assess that ghost-tapping criminals can capitalize on data breaches belonging to banks and telecommunications firms to obtain PII and use social engineering techniques to steal payment card information via phishing. Data breaches of telecommunications companies involving databases belonging to customers may increase the risk of SIM swapping, where cybercriminals can potentially add, link, and authenticate payment card information remotely to burner phones.

Despite the shutdown of Huione Guarantee's operations on May 13, 2025, we observed cybercriminals quickly pivoting toward alternative Telegram-based escrow systems such as Xinbi Guarantee and Tudou Guarantee. These platforms continue to empower cybercriminals to conduct transactions and recruit mules for ghost-tapping operations. Due to these marketplaces being criminal sources and claiming to be a trusted platform, there remains the possibility of them ceasing operations, like Huione Guarantee, while events such as Telegram clamping down on channels linked to these two platforms can temporarily disrupt ghost-tapping campaigns. If these two marketplaces were to cease operations, Chinese-speaking syndicates would likely pivot to different platforms that have stronger operation security measures, which could result in less visibility for researchers and law enforcement agencies to monitor ghost-tapping-related intelligence.

Success in ghost-tapping campaigns will bring about more financial resources to both syndicates and cybercriminals. Ghost-tapping is likely going to expand globally, with threat actors offering custom-built tooling to tailor to non-Chinese speaking syndicates and regional operations. Conversely, if banks around the world introduce more stringent measures to prevent payment card phishing fraud in a manner similar to DBS's security feature, the overall success rate of linking compromised payment card credentials to any contactless payment system would be lowered.

Appendix A: Glossary of Terms

Chinese	Direct Translation	Definition
NFC远程刷卡	Remote NFC Swiping	Using ghost-tapping techniques to obtain physical goods
ATM无卡 取现车	Contactless ATM withdrawal crew	Mules are hired to withdraw cash from ATMs using contactless payment
招 NFC 无卡取现	Recruiting mules withdrawing cash using NFC methods	
实物	Physical goods	
车手	Driver	Mules to do ATM withdrawals or conduct ghost-tapping have to be conducted in person
车队	Motorcade	A group of mules hired by multiple syndicates to perform tasks on behalf of the syndicates who hired them
奢饰品	Luxury goods	Luxury goods
实物,黄金,手机, 奢饰品	Physical goods, gold, mobile phones, luxury items	
跑分;洗料	Runner; wash materials	Money laundering, converting stolen card information into physical goods, USDT, or cash
料	Material	Bank accounts, passwords, mobile phone numbers, and identity card numbers
一道	First-hand	Obtained directly from the source, usually referring to payment cards and databases
二道	Second-hand	Obtained directly from a first-hand seller, usually referring to payment cards and databases

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