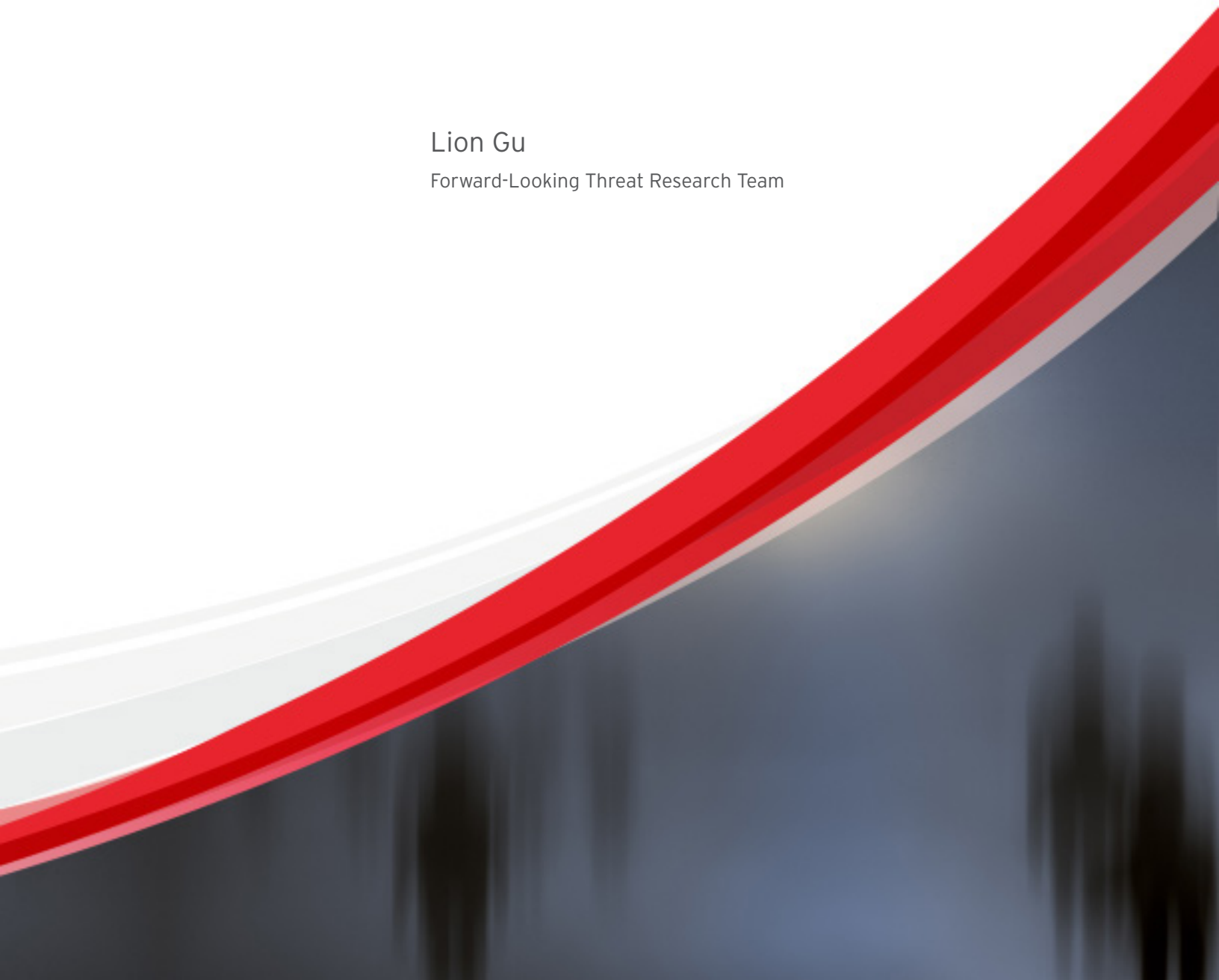
A Trend Micro Research Paper

Cybercriminal Underground Economy Series

The Mobile Cybercriminal Underground Market in China

Lion Gu

Forward-Looking Threat Research Team



Contents

Cybercriminal Underground Economy Series

Places in the Internet where cybercriminals converge to sell and buy different products and services exist. Instead of creating their own attack tools from scratch, they can instead purchase what they need from peers who offer competitive prices. Like any other market, the laws of supply and demand dictate prices and feature offerings. But what's more interesting to note is that recently, prices have been going down.

Over the years, we have been keeping tabs on major developments in the cybercriminal underground in an effort to stay true to our mission—to make the world safe for the exchange of digital information. Constant monitoring of cybercriminal activities for years has allowed us to gather intelligence to characterize the more advanced markets we have seen so far and come up with comprehensive lists of offerings in them.

In 2012, we published "Russian Underground 101," which showcased what the Russian cybercriminal underground market had to offer.[1] That same year, we worked with the University of California Institute of Global Conflict and Cooperation to publish "Investigating China's Online Underground Economy," which featured the Chinese cybercriminal underground.[2] Last year, we revisited the Chinese underground and published "Beyond Online Gaming: Revisiting the Chinese Underground Market."[3] We learned then that every country's underground market has distinct characteristics. So this year, we will add another market to our growing list, that of Brazil.

The barriers to launching cybercriminal operations lessened in number than ever. Toolkits are becoming more available and cheaper; some are even offered free of charge. Prices are lower and features are richer. Underground forums are thriving worldwide, particularly in Russia, China, and Brazil. These have become popular means to sell products and services to cybercriminals in the said countries. Cybercriminals are also making use of the Deep Web to sell products and services outside the indexed or searchable World Wide Web, making their online "shops" harder for law enforcement to find and take down.

All of these developments mean that the computing public is at risk of being victimized more than ever and must completely reconsider how big a part security should play in their everyday computing behaviors.

1 Max Goncharov. (2012). "Russian Underground 101." Last accessed February 19, 2014, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf.

2 Zhuge Jianwei, Gu Liang, and Duan Haixin. (July 2012). "Investigating China's Online Underground Economy." Last accessed February 19, 2014, http://igcc.ucsd.edu/publications/igcc-in-the-news/news_20120731.htm.

3 Lion Gu. (2013). "Beyond Online Gaming Cybercrime: Revisiting the Chinese Underground Market." Last accessed February 19, 2014, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-beyond-online-gaming-cybercrime.pdf.

Introduction

The mobile Web is significantly changing the world. More and more people are replacing their PCs with various mobile devices for both work and entertainment. This change in consumer behavior is affecting the cybercriminal underground economy, causing a so-called "mobile underground" to emerge.

This research paper provides a brief overview of some basic underground activities in the mobile space in China. It describes some of the available mobile underground products and services with their respective prices. Note that the products and services and related information featured in this paper were obtained from various sites and QQ chats.

Mobile Underground Offerings

Premium Service Numbers

Subscribing victims to unwanted premium SMS is a common malicious mobile app behavior. These apps, known as "premium service abusers," subscribe victims to premium mobile services that they may not even be interested in.

People who wish to subscribe to premium services send providers a text message to do so. They then receive a confirmation text message from the provider. To complete their subscription, users need to send a confirmation text message. But, as stated earlier, premium service abusers can also subscribe them to unwanted services. These malicious apps can reply via text message on users' behalf then delete confirmation text messages, leaving no trace of what happened. As a result, users are charged subscription fees that end up in the hands of malicious app developers.

Premium service numbers are critical components of the scam described above. Network carriers normally assign premium service numbers to qualified service providers. The service providers can then offer premium services to users. Premium service numbers are, however, sold underground to any interested buyer. Some malicious app developers buy premium service numbers from legitimate service providers and use these for nefarious purposes.

SMS Forwarders

Many carriers widely use SMS for authentication or verification purposes for services like site registration, password resetting, and online payment. Users who forget their passwords to certain sites, for instance, receive a text message via their registered mobile phone numbers from the site so they can access their accounts. They get a verification code that, when keyed in to the site, lets them change their passwords.

SMS forwarders are Trojans designed to steal authentication or verification codes sent via text messages for malicious purposes. At present, they only run on Android™ phones. They monitor text messages sent by certain phone numbers usually associated with online payment service providers and banks to intercept authentication or verification codes that they then forward to cybercriminals. Like premium service abusers, they also delete the text messages they intercept to hide traces of infection. If cybercriminals get hold of victims' usernames in certain sites, they can easily change passwords and take control of stolen accounts.

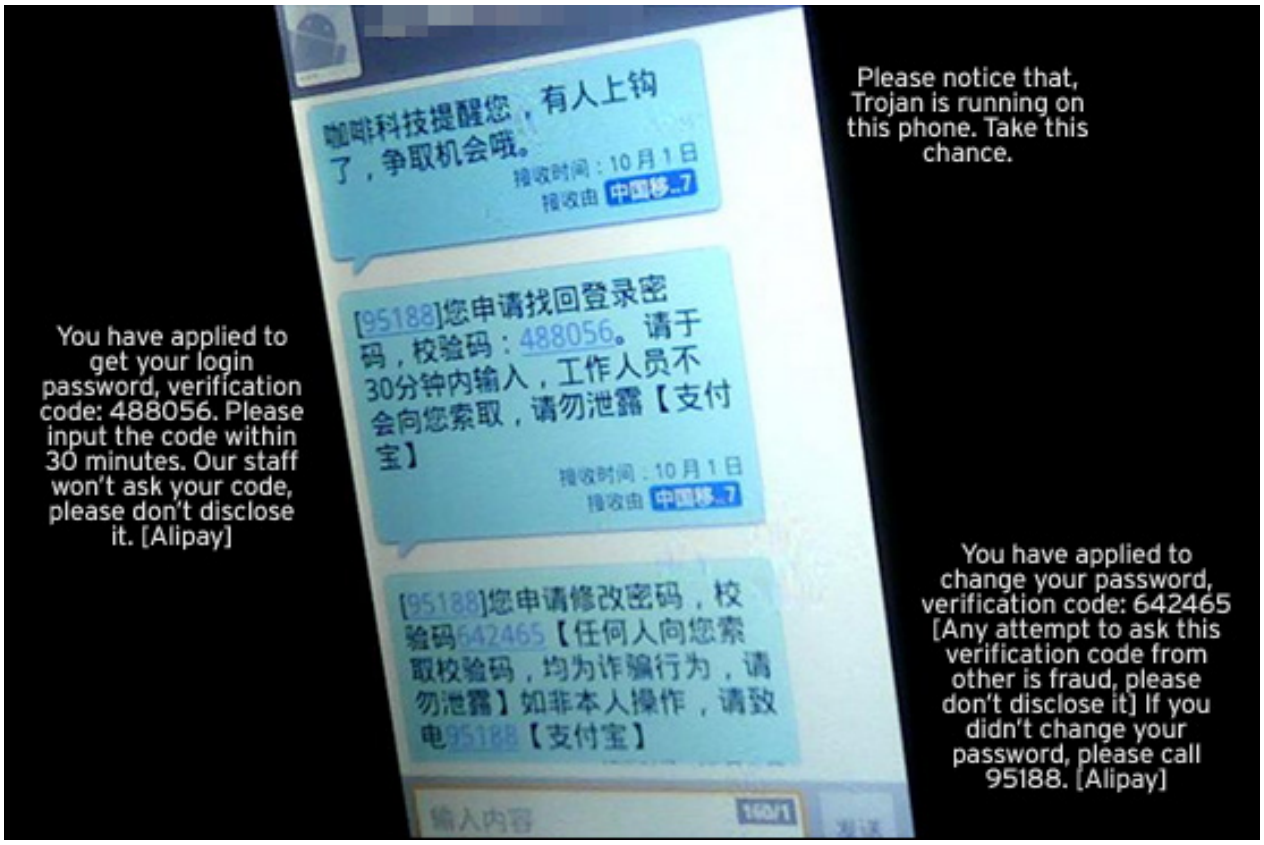


Figure 1: Sample online payment text messages SMS forwarders send to cybercriminals
(Note that the text message contains the verification code the user needs to reset his password.)

SMS Spamming Services and Devices

Spammers send unsolicited bulk text messages known as "SMS spam" to mobile phone users. The spam usually advertise products or services although more of these now come with phishing URLs.

Figure 2: Sample SMS spam with a phishing URL targeting ICBC customers

Cybercriminals use three common devices to send out spam, namely:

- **GSM modem:** A device that can send and receive text messages. It operates like a normal mobile phone does. It uses a SIM card to connect to a mobile network. A GSM modem can also be connected via a serial USB so it can be controlled by an application running on a computer. Some GSM modems have several slots (see Figures 3 and 4) that accept one SIM card each. As such, a GSM modem can simultaneously support several SIM cards. This type of GSM modem is also called a "GSM modem pool." A 16-slot GSM modem can send 9,600 text messages in one hour.

Figure 3: A GSM modem with 16 SIM card slots

Figure 4: An 8-slot GSM modem with SIM cards

- **Internet short message gateway:** A device that mobile network carriers provide to service providers to handle bulk-text-sending services. Note that the sending speed of this gateway is much higher than a GSM modem's. It can also be very easily abused in that it can make spam sending much easier for scammers and fraudsters.

- **SMS server:** A low-cost piece of radio frequency (RF) hardware (see Figures 5–8) that can send out software-defined radio (SDR) signals in GSM frequency ranges. It is especially useful for sending out SMS spam. When running, an SMS server announces itself as a base station by sending a high-power signal, which forces all nearby mobile phones to disconnect from the legitimate base stations of their network carriers and instead connect to the SMS server. The SMS server can then push out spam to the mobile phones. When finished, the SMS server disconnects from the mobile phones, which are then reconnected to their legitimate base stations. The spammer can use any sender number when texting. As such, they can send fraudulent or fake text messages using a known public or a legitimate bank's service number. Because an SMS server takes the place of a legal base station to hijack nearby mobile phone connections, it is also known as a "fake base station."

Figure 5: All-in-one SMS server package made up of a laptop, a GSM mobile phone, an SMS server box, an antenna, and a USB data cable sold underground for RMB 45,000 (~US$7,400)

Figure 6: Applications that run an SMS server are usually installed on an Ubuntu-based system; Ubuntu is a Debian-derived Linux distribution

* All RMB to US$ conversions were based on February 20, 2014 exchange rates.

Figure 7: Insides of an SMS server

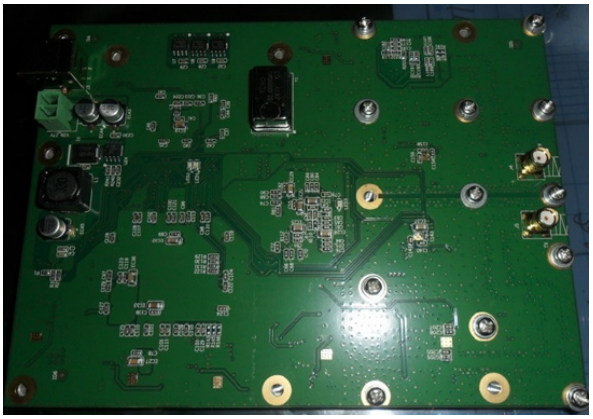


Figure 8: Motherboard of an SMS server that's quite different from a PC's

iMessage Spamming Services and Software

iMessage® is Apple's instant-messaging (IM) service on both iOS and OS X®. It allows iPhone®, iPad®, iPod touch®, and Mac® users to send text and group messages and other media files to fellow users without additional charges as long as they're Wi-Fi-connected.

iPhone users can link their phone numbers and Apple IDs to iMessage. Doing this lets them continue to receive instant messages from other Apple device users. As usual, the more popular a service gets, the more they become likely cybercrime targets. That is probably why iMessage spam are gaining notoriety (see Figure 9). Note, however, that only Apple device users can receive iMessage spam.

Figure 9: Sample iMessage spam that promotes a new iPhone game

Figure 10: Control panel of the iMessage spamming software

To effectively spam people, searching for phone numbers linked with Apple IDs is a crucial step. To do this, spammers usually send a test message to a phone number then checks if it was successfully sent. Each number that successfully received the test message becomes a spamming target (see Figure 11). iMessage spam are proving to be good threat vectors, as the iPhone was named one of the top 4 best-selling smartphones worldwide. Apple particularly quadrupled its share in the Chinese market even before it partnered with China Mobile.[4]

4 Chuck Jones. (December 11, 2013). *Forbes.* "Apple's iPhone 5s #1 Worldwide Smartphone and Quadruples Chinese Share." Last accessed February 4, 2014, http://www.forbes.com/sites/chuckjones/2013/12/11/apples-iphone-5s-1-worldwide-smartphone-and-quadruples-chinese-share/.

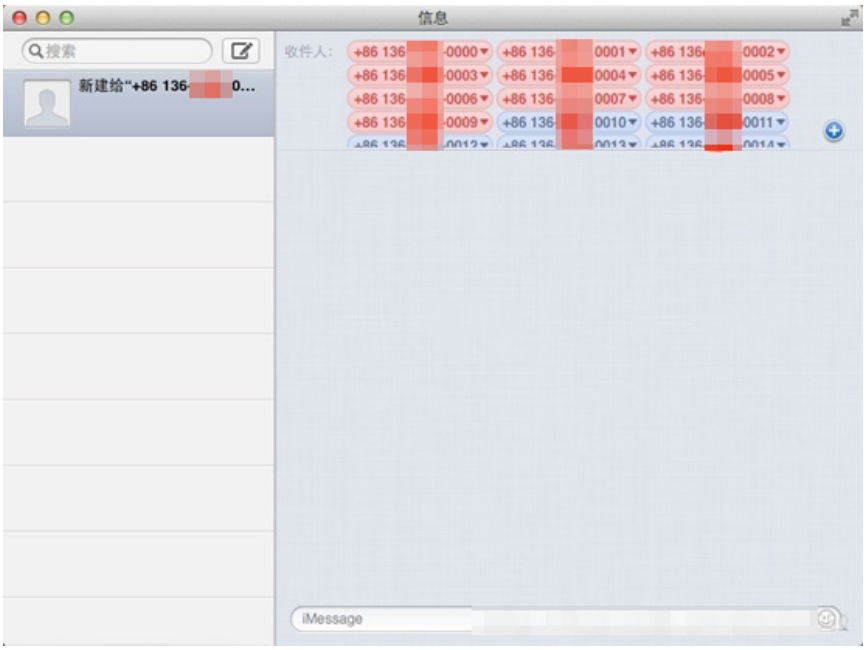


Figure 11: Set of phone numbers tested using the spamming software to see if they can be potential victims

Phone-Number-Scanning Services

The number of mobile subscribers has been exploding. The mobile technology has also been constantly improving. These are just two of the reasons why mobile network carriers now provide new mobile phone under 3G and 4G networks.

The speed by which mobile phone numbers are replaced and added to carriers' lists is making it hard for cybercriminals to keep up. Filtering out unused phone numbers from spamming lists is very important to SMS spammers and phone fraudsters because doing so allows them to save time and money. Scanning helps spammers know the current status of phone numbers, including whether their users are online or not, or if they are still actively used. Phone numbers that pass scanning are called "real numbers" and are targeted by spammers and telephone fraudsters.

To scan for so-called "real numbers," a mobile phone or a GSM modem is connected to a computer running a scanning application (see Figures 12 and 13). The application controls the connected mobile phone or GSM modem to check the status of phone numbers. Note that one scanning-software-controlled mobile phone can scan 400 phone numbers in one hour. This process, however, consumes a considerable amount of time. That is why query services to databases that store volumes of phone number statuses are popular underground.

Figure 12: Eight GSM mobile phones can be connected to each serial card, all of which can be controlled by phone-number-scanning software

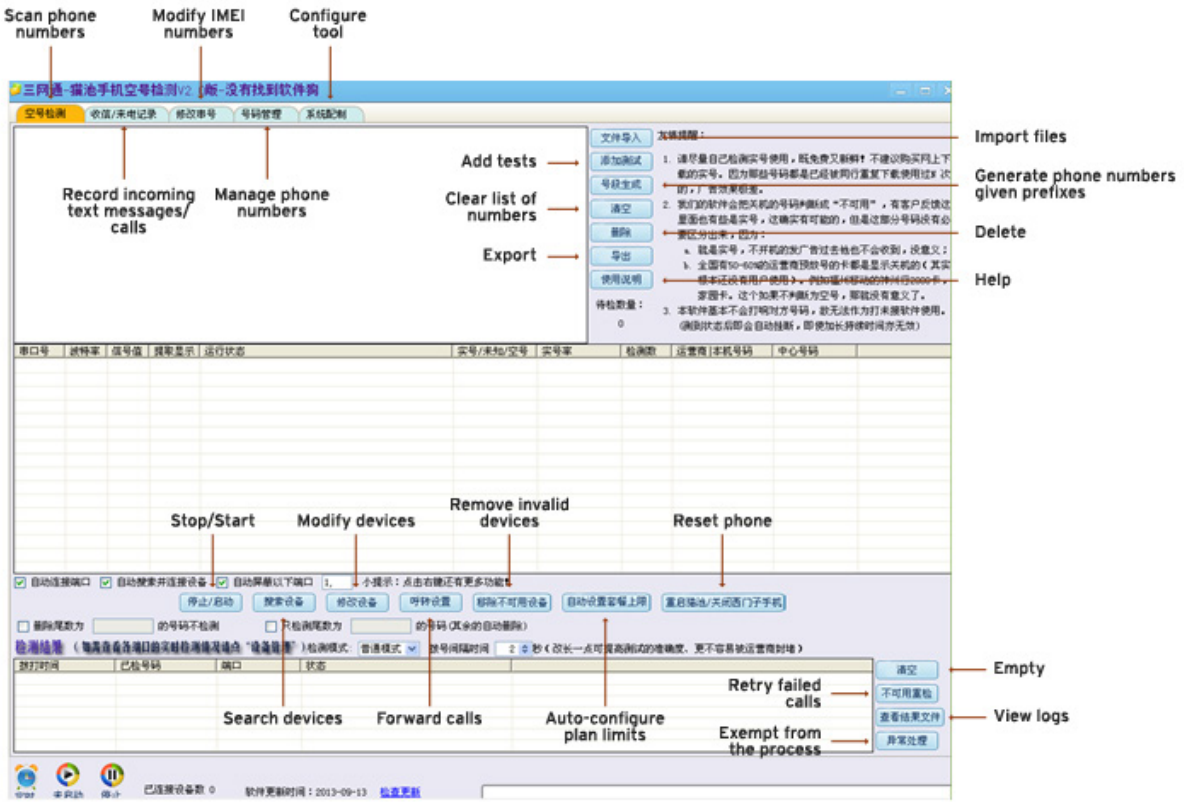


Figure 13: Sanwangtong scanning software's features include importing phone numbers, saving incoming text messages, modifying International Mobile Station Equipment Identity (IMEI) numbers, and checking SIM card balances

App-Rank-Boosting Services

Most smartphone users download apps from official app stores. All Apple device users, except those with jailbroken ones, can only download apps from the App Store℠. Most Android™ device users, meanwhile, can download either from Google Play™ or third-party app stores. Note that in China though, most Android device users download apps from third-party app stores. Regardless where users download apps, however, all app stores rank and recommend apps to customers. And no matter what ranking algorithm an app store adopts, download numbers and reviews always play a part in determining an app's ranking. Consequently, users consider an app's ranking when deciding whether or not they would download it.

App rank boosting increases an app's ranking in app stores. Cybercriminals usually boost an app's ranking by creating several dummy accounts to download and write good user reviews for it. This is especially true for Android apps in third-party app stores in China. Doing so is, however, costly.

Mobile Cybercriminal Wares Sold in the Chinese Underground Market

The following table shows the various products and services sold in the Chinese mobile underground market.

Cybercriminal Underground Wares Sold in China		
Product/Service	**Feature**	**Price**
Premium service numbers	Can be rented or bought by anyone; can subscribe all China Mobile users to premium services just by sending text messages; comes with detailed subscription reports from network carriers; 15% of the total subscription income goes to the network carrier and the remainder goes to renter or owner	Six-digit subscription number: RMB 220,000 (~US$36,000) per year
		Seven-digit subscription number: RMB 100,000 (~US$16,400) per year
		Eight-digit subscription number: RMB 50,000 (~US$8,200) per year
		Nine-digit subscription number: RMB 15,000 (~US$2,500) per year
SMS forwarder source code for Android	Intercepts SMS from certain phone numbers; removes intercepted SMS from phones; has a hidden app icon	RMB 3,000 (~US$500)

Cybercriminal Underground Wares Sold in China		
Internet short message gateway spamming service	5,000 text messages	RMB 300 (~US$50)
	10,000 text messages	RMB 400 (~US$65)
	20,000 text messages	RMB 700 (~US$115)
	50,000 text messages	RMB 1,500 (~US$250)
	100,000 text messages	RMB 2,800 (~US$460)
GSM modem	Supports 16 SIM cards; can be connected via USB	RMB 2,600 (~US$430)
SMS server	Works on the 885–915MHz frequency (uplink) and the 930–960MHz frequency (downlink); has a maximum output power of 20W (5 shifts) and a service range of 200–2,000 meters; can send 300 messages per minute and hijack a mobile phone in 5 seconds	RMB 45,000 (~US$7,400)
iMessage spamming service	1,000 text messages	RMB 100 (~US$16)
	1,000 multimedia messages	RMB 500 (~US$82)
iMessage spamming software	Can support text and multimedia message sending, scan multiple sets of phone numbers at one time, import phone numbers from text files, automatically switch Apple IDs, and be preconfigured and sent as a virtual image (saving the buyer time to configure the application); allows users to view task progress	RMB 30,000 (~US$4,900)
Real number querying service	100,000 numbers	RMB 100 (~US$16)
	1,000,000 numbers	RMB 500 (~US$82)
	3,000,000 numbers	RMB 1,000 (~US$160)

Cybercriminal Underground Wares Sold in China		
Phone number scanning software	Can support GSM modems and mobile phones, automatically hang up on scanning calls (so the user doesn't have to pay for test calls made), filter out inactive phone numbers and rescan them should they prove only temporarily inactive, change IMEI numbers, automatically refuse incoming calls, record incoming callers' numbers and text messages, and automatically generate phone numbers to scan	RMB 230 (~US$38)
Phone number scanning hardware package	Includes eight mobile phones, one Payment Card Industry (PCI) serial card, one data cable, and the scanning software	RMB 1,100 (~US$180)
App rank boosting in any third-party Android app store	10,000 downloads	RMB 40 (~US$7)
	60,000 downloads	RMB 230 (~US$38)
	90,000 downloads	RMB 340 (~US$56)
	120,000 downloads	RMB 450 (~US$74)
	150,000 downloads	RMB 550 (~US$90)
	180,000 downloads	RMB 650 (~US$106)

Cybercriminal Underground Wares Sold in China		
App rank boosting in Apple's App Store	Ranked among the top 5	iPhone app: RMB 60,000 (~US$9,800) iPad app: RMB 35,000 (~US$5,700)
	Ranked among the top 10	iPhone app: RMB 39,000 (~US$6,400) iPad app: RMB 25,000 (~US$4,100)
	Ranked among the top 15	iPhone app: RMB 30,000 (~US$4,900) iPad app: RMB 22,000 (~US$3,600)
	Ranked among the top 20	iPhone app: RMB 22,000 (~US$3,600) iPad app: RMB 20,000 (~US$3,300)
	Ranked among the top 25	iPhone app: RMB 21,000 (~US$3,400) iPad app: RMB 13,000 (~US$2,100)
	Ranked among the top 50	iPhone app: RMB 14,000 ~US$2,300) iPad app: RMB 8,000 (~US$1,300)
	Ranked among the top 75	iPhone app: RMB 10,000 (~US$1,600) iPad app: RMB 6,000 (~US$980)
	Ranked among the top 100	iPhone app: RMB 6,000 (~US$980) iPad app: RMB 4,400 (~US$720)
	Ranked among the top 200	iPhone app: RMB 2,850 (~US$470) iPad app: RMB 2,700 (~US$440)
User review in Apple's App Store	100 reviews	RMB 150 (~US$25)

Conclusion

This paper introduced several common types of mobile underground offerings in China. To understand the existing underground business model, it provides detailed information on various products and services sold, along with their features and prices.

As evidenced by the thriving mobile underground economy, cybercriminals have quickly adapted to technological developments, current trends, and changing user behaviors. As part of the security industry, we must pay attention to developments in the mobile underground. And we should exert effort to educate mobile users on the risks they face and help them improve their security posture so they can protect not just their mobile devices but also the information stored in them.

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit www.trendmicro.com.

TREND MICRO™

Securing Your Journey to the Cloud

225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.

Phone: +1.817.569,8900