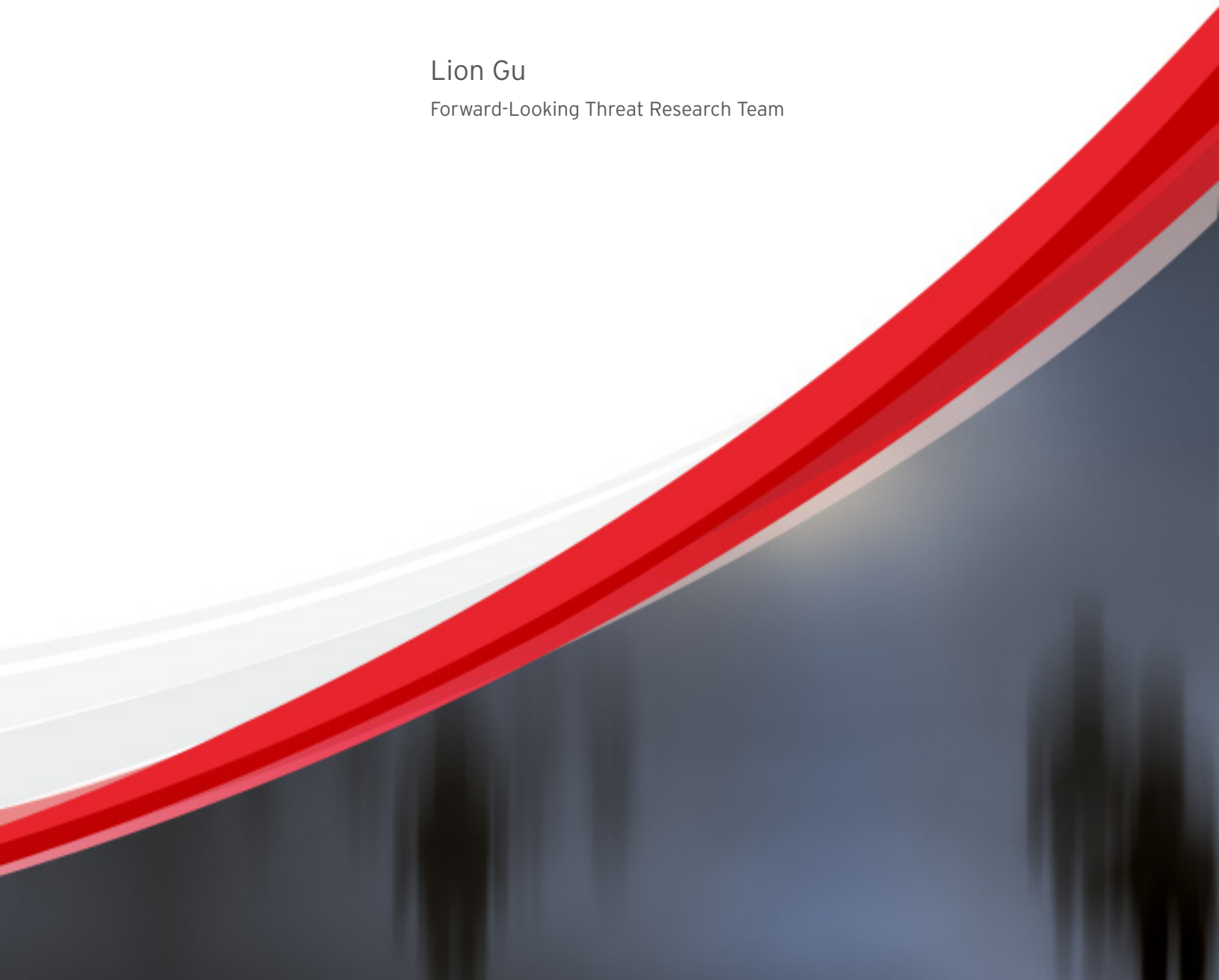
A Trend Micro Research Paper

Cybercriminal Underground Economy Series

The Chinese Underground in 2013

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 to 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 had distinct characteristics. So this year, we will add another market to our growing list, that of Brazil.

The barriers to launching cybercrime have decreased. 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.

Introduction

We have been continuously monitoring the Chinese underground market since 2011. And by the end of 2013, we have seen more than 1.4 million instant chat messages related to activities in the market from QQ™ Groups alone.

This research paper reviews these millions of messages, along with trends observed and product and service price updates seen in the Chinese underground market throughout 2013.

QQ Groups Abuse

Cybercriminals have been known to abuse popular Web services for malicious gains. We have seen services such as Dropbox and Evernote, for instance, abused for command-and-control (C&C) communication early this year.[4, 5] The cybercriminals in China are no different; they have abused popular instant-messaging (IM) app, QQ, as a communication tool.

QQ Groups—a feature of an IM service provided by Tencent—allows users to easily create multiple chat groups that can each accommodate up to 2,000 users.[6] Each group can have a unique number of users, name, and description. QQ Groups allows users to search for particular chat groups based on the number of users or keywords in group names and descriptions.

Figure 1: QQ Groups search results for the keyword, “DDoS”

Because of its excellent features and huge user base, QQ Groups has been a major target of underground market players. In fact, cybercriminals who use QQ to peddle crimeware even include certain underground jargon to help newbies find what they are looking for. The ads for underground products and services are always shorter than those found in dedicated underground forums or websites. Unlike the latter, however, the ads on QQ are more frequently updated.

Figure 2: QQ Groups chat showing two ads for DDoS services

By determining popular words used for underground products and services, one can identify which QQ Groups would be useful to monitor then review the activities of those with the biggest number of users.

A Statistical Look at the 2013 Chinese Underground Market

From March 2012 to December 2013, data gathered from monitoring almost 500 QQ Groups and reviewing 1.4 million messages helped to determine certain characteristics and developing trends in the Chinese underground economy.

In the last 10 months of 2013, the number of messages sent over the underground chat groups doubled from the same period in 2012. This indicates increased underground market activity.

Figure 3: 2012 and 2013 underground chat group activity comparison

Hourly statistics of the QQ Groups messages in 2013 indicate that their members were active from 8 to 10 P.M. This could mean that they only engaged in underground market trading part-time.

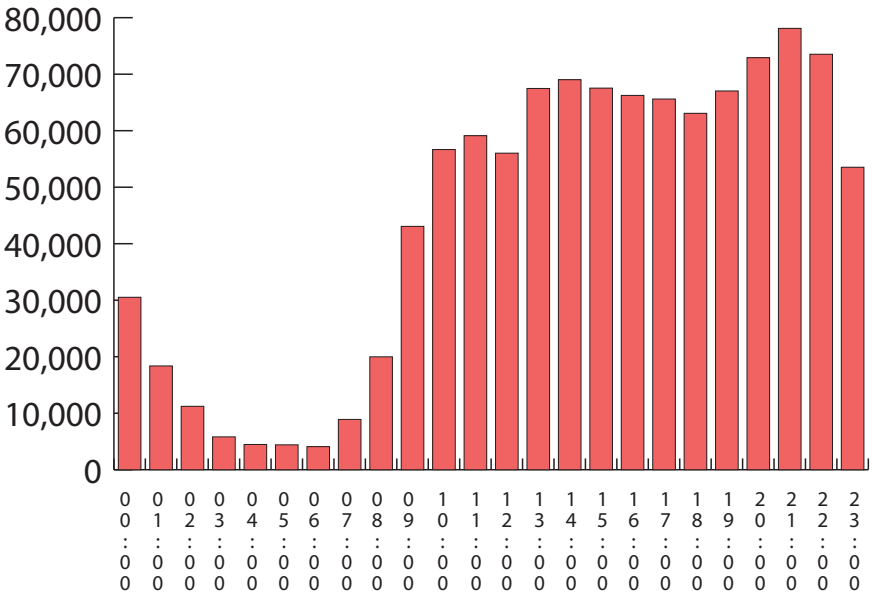


Figure 4: Number of underground chat messages per hour in 2013

The weekly statistics on the same groups further confirmed this theory, as more activity occurred on Sundays.

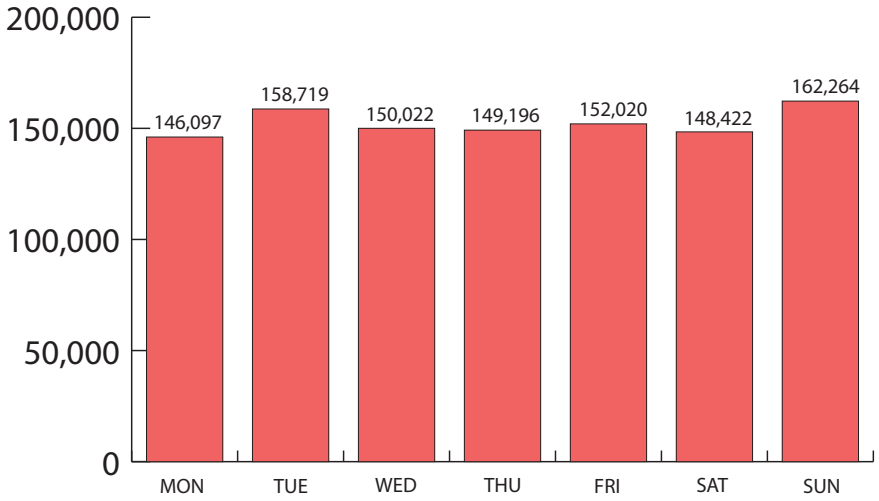


Figure 5: Number of underground chat messages per day in 2013

We created a new indicator—messages per group per day (MGD)—to measure the underground activity of each chat group monitored in 2012 and 2013. This shows the average number of messages sent by the members of each group per day. The 2012 MGD was 28.74 while that in 2013 was 62.56, twice the number in the previous year. This means that the underground chat groups were more active in 2013 than they were in 2012.

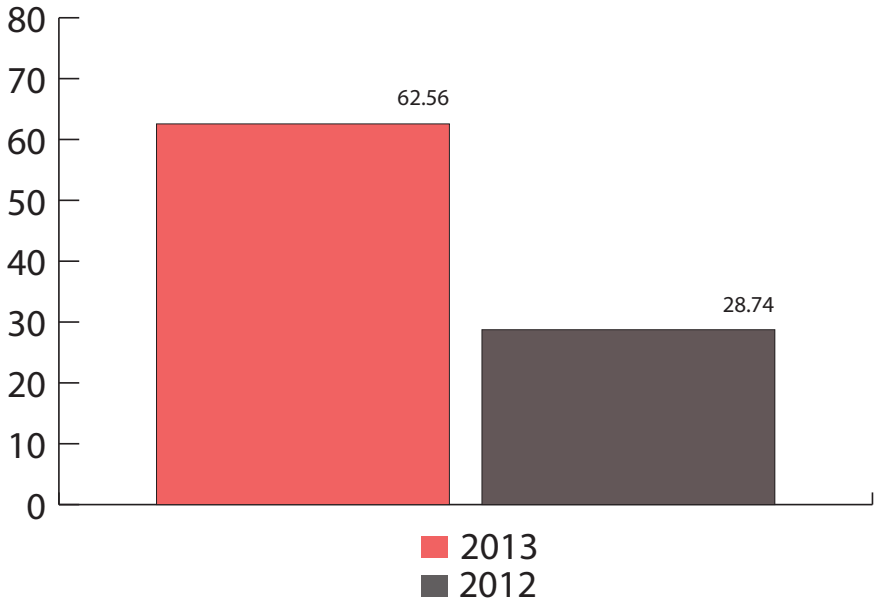


Figure 6: 2012 and 2013 MGD comparison

As with all online chat services, QQ Groups show the message senders' IDs and nicknames in logs, which allowed for the discovery of more information on their participants available on the Internet. For instance, the number of underground chat participants significantly increased from 2012 to 2013. Similar to the number of messages, the participant volume in the last 10 months of 2013 doubled compared with the same period in 2012.

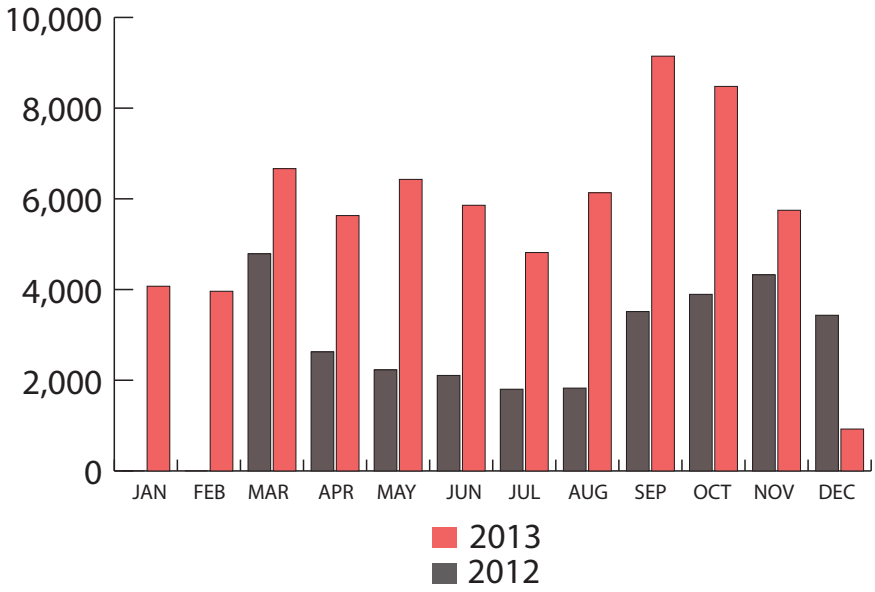


Figure 7: Number of underground chat participants in 2012 and 2013

We also developed another indicator to measure underground chat group activity in terms of participant volume—participant per group per day (PGD). This shows the average number of participants in each chat group per day. We discovered that the PGD in 2012 was only 5.13 while that in 2013 was 11.26, which means that more users became interested in the business of cybercrime.

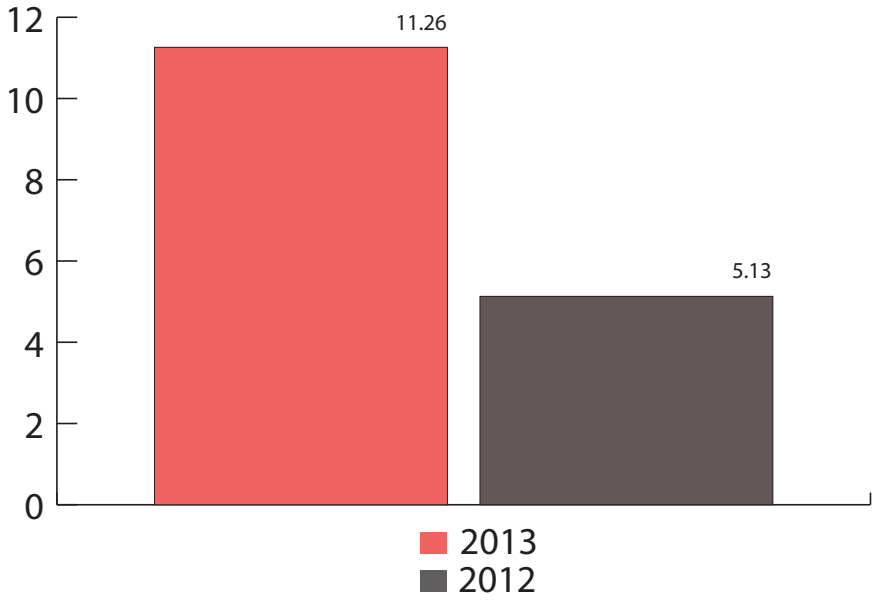


Figure 8: 2012 and 2013 PGD comparison

We also looked at the popularity of various products and services offered in the underground market. This could provide insight on the type of cybercrime the members of the underground chat groups were most interested in. The use of underground jargon actually helped determine how popular each kind of product or service was. The three most popular products/services in the Chinese underground market were compromised hosts, distributed denial-of-service (DDoS) attack services, and remote access tools/Trojans (RATs).

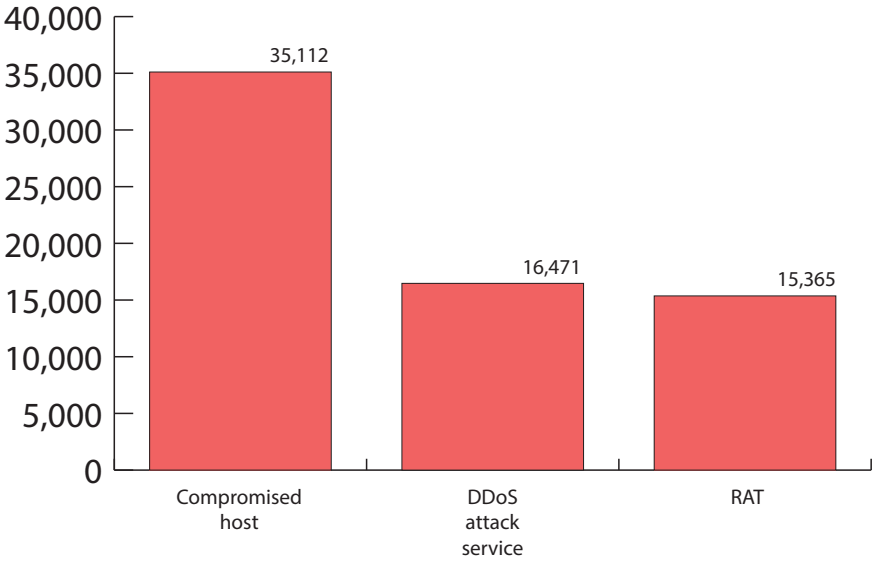


Figure 9: Most popular underground products/services in 2013

Compromised Hosts

Compromised hosts refer to servers that cybercriminals have gained command and control of without their owners' consent.[7] This means that they can operate the systems as local system administrators. Hosts typically have unique computing capabilities, amounts of storage space, network bandwidths, and IP addresses and contain sensitive data. Cybercriminals can abuse or misuse all of these for their own malicious purposes such as:

- **Use the compromised host as a malware or spam distributor.** Cybercriminals can infect a host with malware that can spread to systems and devices connected to it. They can also use it to distribute spam.[8]
- **Use several compromised hosts to launch DDoS attacks.** Cybercriminals can also command several hosts they have compromised to access a certain IP address or URL at the same time. The large amount of traffic these hosts would generate could bog down the site's server, causing a DDoS.[9]
- **Use a compromised host to run complex computing tasks.** An example of such abuse is using compromised hosts as Bitcoin miners.[10] This allows cybercriminals to mine Bitcoins without the need to increase their own systems' computing power, as mining the cryptocurrency eats up a lot of computing resource.

Cybercriminals typically compromise hosts via:

- **Launching drive-by download attacks.** Cybercriminals upload malware, usually RATs, to legitimate sites then trick users into visiting them with irresistible social engineering lures. Visiting the compromised sites then drop malware onto the users' systems. And when executed, the malware allows the cybercriminals to gain command and control of infected systems.[11]

- **Exploiting remote access.** Many Internet-connected systems are not properly configured in terms of security. As such, cybercriminals can easily gain command and control of them via Remote Desktop Connection.[12] Although this is a legitimate feature that helps IT administrators remotely access systems for troubleshooting and other purposes, systems that have been configured to run this feature on the default port—3389—but have weak passwords could easily be hacked. In fact, such systems known as "3389 hosts" are easy to find on the Internet.

DDoS Attack Services

DDoS attacks disrupt access to legitimate online services.[13] In such an attack, cybercriminals flood a site's server with too many service requests, causing service disruption. Two of the most popular types of DDoS attack services offered in the Chinese underground are:

- **SYN flooding:** SYN flooding attacks involve sending throngs of Transmission Control Protocol (TCP)/SYN packets often with forged sender addresses to target sites.[14] Each packet is handled like a connection request, causing the site's server to spawn a half-open connection by sending back a TCP/SYN-ACK packet while waiting for a response packet from the sender. However, because the sender address is forged, the server never gets a response, causing service disruption.

- **HTTP GET flooding:** Also known as "Challenge Collapsar (CC)" attack, it targets Web servers.[15] HTTP GET flooding is initiated by sending tons of HTTP GET requests to a target URL. Responding to Web page requests consumes Web server resources, much like querying databases and reading files from hard disks. Getting and responding to a lot of HTTP GET requests requires a lot of system resource, which renders websites inaccessible.

Cybercriminals who want to launch DDoS attacks can purchase DDoS kits from the Chinese underground. DDoS kits refer to tools that allow a remote user to control several systems to send a large amount of network packets to a target site. Apart from SYN and HTTP GET flooding use, DDoS kits can also be used for Internet Control Message Protocol (ICMP), User Datagram Protocol (UDP), ACK, and other kinds of flooding attacks.[16, 17, 18] Compromised systems—either compromised hosts or dedicated servers—that would send the packets to targets are also available underground.

Dedicated servers are only offered for rent. For the amount of time they are rented, the renter obtains all of the resources in it. Unlike compromised hosts, dedicated servers have better hardware and faster Internet connection. Dozens of dedicated servers are enough to launch an attack. To conceal the identity of dedicated servers, cybercriminals use spoofed IP addresses when sending out packets to the target.

Figure 10: DDoS kit portal

Cybercriminals usually send a flood of packets directly to the target IP address. Some, however, also send a flood of packets to the Domain Name System (DNS) server that hosts the target domain. If the DNS server is out of service, it cannot respond to any query for any of the domains it hosts, including the target domain. As such, many websites will suffer if an attack on a DNS server succeeds. Tools to attack DNS servers are new offerings underground.

RATs

RATs allow users to remotely access and control systems.[19] They have plenty of features to cover most system administration tasks. They were primarily designed to facilitate system administrators' work but are now being misused to take remote control of target systems because of their ability to evade detection.[20]

RATs are also flexible. Cybercriminals, for instance, can use a RAT to obtain a list of file names in the target system. They can then choose and compress a file of interest for the target system to send to them.

Chinese Underground Offerings in 2013

The three above-mentioned products/services appeared to be the most popular underground market offerings in China in 2013. Several other products and services are available to anyone interested in procuring them.

Chinese Underground Market Product Offerings		
Product	**Details**	**Price**
Botnet	Windows: • With 100 Windows XP bots • With 100 Windows Server 2003/2008 bots DDoS attack: • 100 bots • 300 bots • 800 bots • 2,000 bots	 US$8 US$48 US$95 US$208 US$386 US$596
Exploit kit	NB Exploit Pack	US$323
Fake post/comment/view/ follower	Baidu Tieba forum: • 100 new posts • 100 comments 10,000 Youku video views Sina Weibo blog: • 100 followers • 1,000 followers • 3,000 followers	 US$16–48 US$8–16 US$0.65 US$2 US$13 US$37
Fake site	QQ/Taobao/ICBC Bank Various online games Online game trading site	US$81 US$16–32 US$81–97
Scanned fake document	China/U.S./Canada passport	US$5
Serial key	Microsoft products: • Windows® 8 Pro • Windows Server 2012 R2 • Microsoft™ Office® 2013 Pro Other products: • Adobe® Photoshop® Creative Suite® 6 • AutoCAD® 2013	 US$0.65–3 US$0.81–2 US$0.81–6 US$0.81–3 US$3–11

Chinese Underground Market Product Offerings		
Product	**Details**	**Price**
Traffic	500 IP addresses per day 1,000 IP addresses per day 5,000 IP addresses per day 10,000 IP addresses per day 50,000 IP addresses per day 100,000 IP addresses per day 500,000 IP addresses per day	US$0.26 US$0.42 US$2 US$5 US$38 US$95 US$473
Trojan	QQ account stealer Taobao account stealer Yun Teng, a bank Trojan toolkit: • Bronze level • Silver level • Gold level • Platinum level • Diamond level	US$32 US$323 US$1,273 US$1,596 US$2,080 US$2,565 US$3,856

NOTE: The product prices in the table above are based on RMB to U.S. dollar exchange rates as of July 27, 2014.
SOURCES: 51traffic.com, bw520.com, QQ chat messages, taobao.com, tieba.baidu.com, www.07328.com, www.520banks.com, www.hangamei.com, www.wsddos.yulusa.com, youlong2013.com

Chinese Underground Market Service Offerings		
Service	**Details**	**Price**
Cracking	Encrypted .RAR, .ZIP, .DOC, .XLS, or .EXE file Software: • Dongle protection • Registration code • User number limit protection	US$45 US$807–12,919 US$161 US$242
Dedicated-/Bulletproof-server hosting	One-month with DDoS protection	US$81–775
DDoS attack	1GB packets: • SYN per day • HTTP GET per day 10GB SYN packets per day DNS server attack DDoS toolkit rental: • One month • Six months • One year • Lifetime	 US$16 US$73 US$161 US$323 US$81 US$161 US$258–323 US$452–484

Chinese Underground Market Service Offerings		
Service	**Details**	**Price**
Fake document rework		US$19
Hacking	Forum account: • Normal user • Subforum administrator • Forum administrator • VIP QQ account: • Password • Six-month chat log • One-year chat log Email account: • Personal • Corporate Sina/Weibo/Renren account	 US$81 US$161 US$323 30% of the official service fee US$48 US$81 US$129 US$48 US$81 US$48
Malware checking against security software	Various software	US$13–19
Programming	RAT toolkit Trojan	US$161 US$323–8,075
Proxy-server hosting	HTTP SOCKS proxy server: • With a single fixed IP address per month • With 800 IP addresses per month • With 9,000 IP addresses per month • With 32,000 IP addresses per month	 US$4 US$0.16 US$2 US$16
RAT toolkit rental	TYT/MBZ RAT per year RD RAT: • One month • One year	US$97 US$129 US$258
Spamming	1,000 email addresses 10,000 email addresses 20,000 email addresses 50,000 email addresses 100,000 email addresses	US$13 US$97 US$161 US$323 US$484
Trojan attack	One online game per day	US$29

Chinese Underground Market Service Offerings		
Service	**Details**	**Price**
VPN-server hosting	One month Three months One year	US$3 US$8–10 US$19–32

NOTE: The service prices in the table above are based on RMB to U.S. dollar exchange rates as of July 27, 2014.
SOURCES: 173.252.233.132, 17msge.com, blog.sina.com.cn, QQ chat messages, task.zhubajie.com, wodexiangzi.com, www.2sxvpn.com, www.360email.cn, www.49207.com, www.512727.com, www.51cxjilu.com, www.71n.net, www.gyddos.com, www.jx39.com, www.killdog.net, www.nc2c.com, www.rmd5.com, www.sinogemsoft.com, www.whenq.com

A Statistical Look at the Chinese Mobile Underground Market

Attacks against mobile phone users have been rapidly increasing, as evidenced by the fast-rising number of Android™ malware.[21] We took a look at the emerging mobile underground market in China as well in 2013.

For this paper, we monitored 11 mobile underground chat groups (included in the total—500) to determine the mobile MGD. We found that the mobile MGD was 61.3, which means that each of the mobile underground groups we monitored sent around 61 messages per day. This number was very close to the overall cybercriminal underground MGD in 2013. Compared with the 2012 MGD, the amount of mobile underground activity slightly increased in 2013.

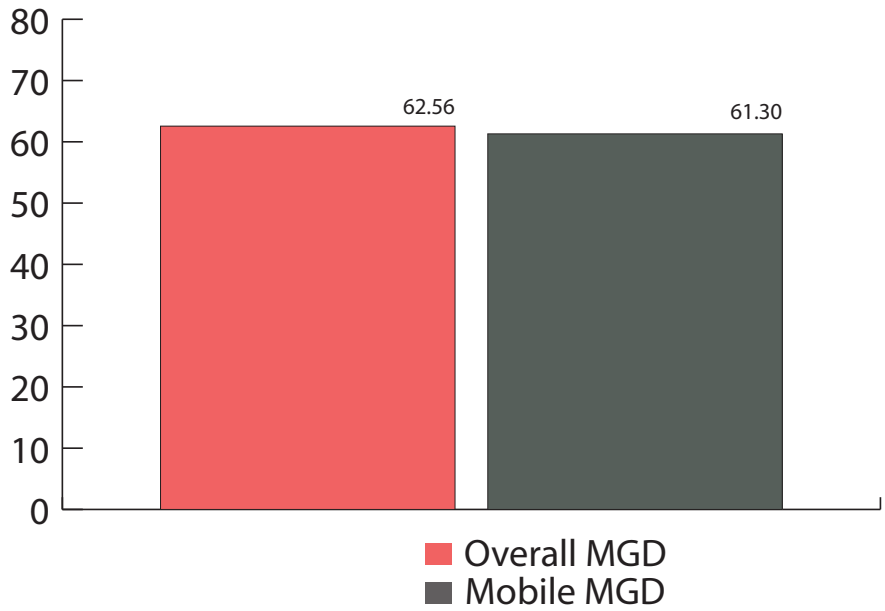


Figure 11: 2013 overall and mobile MGD comparison

We also determined the mobile PGD and found that it significantly increased from around 11 in 2012 to around 29 in 2013. This means that each mobile underground group in 2013 had around 29 participants per day, almost 2.5 times as many as in 2012. The mobile PGD was more than double the overall PGD in 2013 as well.

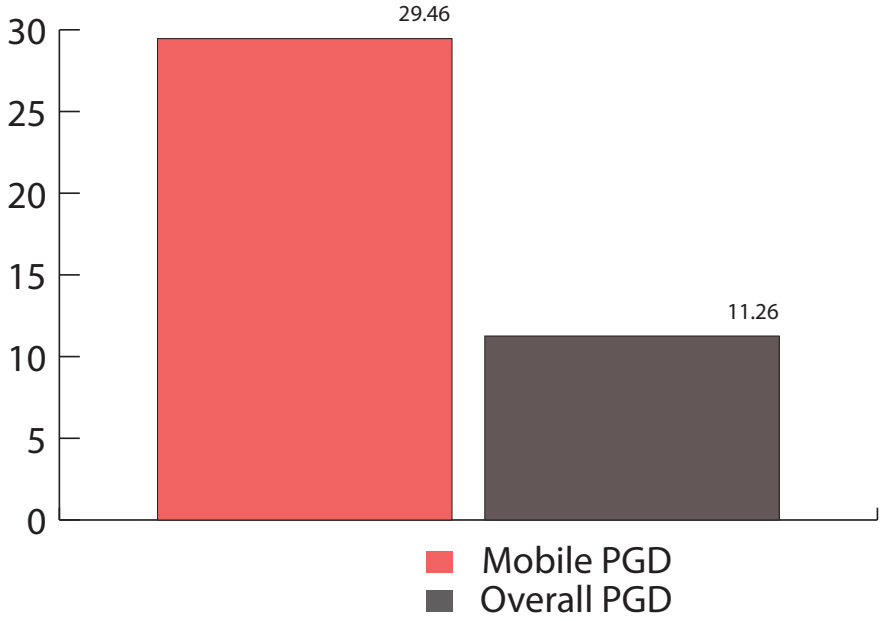


Figure 12: 2013 overall and mobile PGD comparison

We also determined which products/services were most in demand in the Chinese mobile underground market and found that these were spam Short Message Service (SMS) spamming services, SMS servers, and premium service numbers.

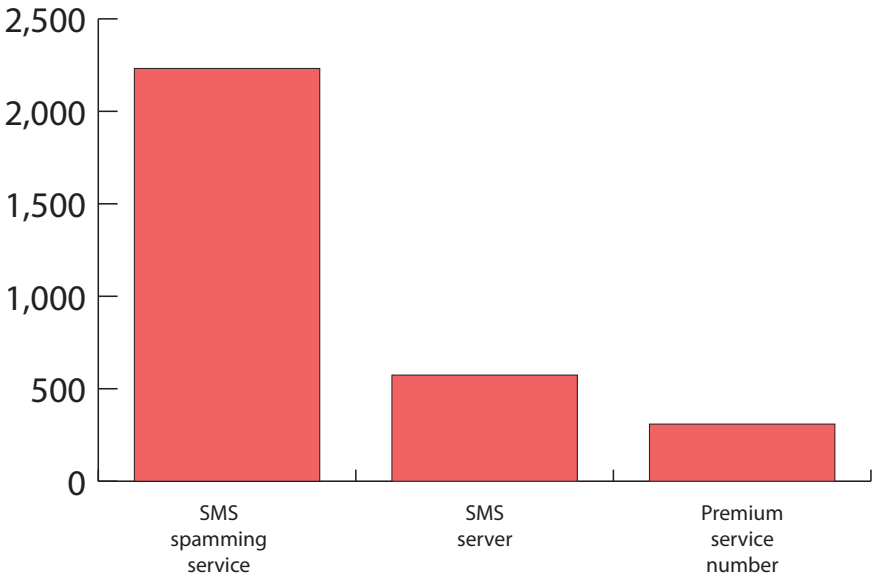


Figure 13: Most popular mobile underground products/services in 2013

For more details and pricing information on the most popular and other product/service offerings in the Chinese mobile underground market, read "The Mobile Cybercriminal Underground Market in China."[22]

Conclusion

This research paper featured an analysis of the Chinese underground market based on monitoring of QQ Groups in 2012 and 2013. Our findings revealed that the amount of underground activity in China doubled in 2013 compared with 2012—both with regard to number of participants and product and service offerings.

Compromised hosts, DDoS attack services, and RATs were the most-sought-after products/services in the Chinese underground market. The country also has an emerging mobile underground economy. SMS spamming services, SMS servers, and premium service numbers were the most-sought-after products/services in this space.

In sum, the Chinese underground market players are keeping pace with the developments in the security landscape. They no longer just peddle malicious wares to attack PC users but also to attack the rapidly growing mobile device market. This should serve as another reminder to all computer or any Internet-connected device to always be security-aware to live a threat-free digital life.

References

1. Max Goncharov. (2012). *Trend Micro Security Intelligence.* "Russian Underground 101." Last accessed July 27, 2014, http://www.trendmicro.com/cloudcontent/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf.

2. Zhuge Jianwei, Gu Liang, and Duan Haixin. (July 2012). *IGCC.* "Investigating China's Online Underground Economy." Last accessed July 21, 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 July 27, 2014, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-beyond-online-gaming-cybercrime.pdf.

4. Maersk Menrige. (June 25, 2014). *TrendLabs Security Intelligence Blog.* "PlugX RAT with "Time Bomb" Abuses Dropbox for Command-and-Control Settings." Last accessed July 21, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/plugx-rat-with-time-bomb-abuses-dropbox-for-command-and-control-settings/.

5. Nikko Tamaña. (March 27, 2014). *TrendLabs Security Intelligence Blog.* "Backdoor Uses Evernote as Command-and-Control Server." Last accessed July 21, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/backdoor-uses-evernote-as-command-and-control-server/.

6. Tencent. (2014). *QQ International.* "The Official Blog of QQ International." Last accessed July 21, 2014, http://blog.imqq.com/.

7. Wikimedia Foundation Inc. (July 24, 2014). *Wikipedia.* "Botnet." Last accessed July 25, 2014, http://en.wikipedia.org/wiki/Botnet.

8. Maria Manly. (April 24, 2014). *TrendLabs Security Intelligence Blog.* "AOL Mail Service Hacked, Compromised Emails Used to Send Spam." Last accessed July 25, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/aol-mail-service-hacked-compromised-emails-used-to-send-spam/.

9. Chris Huang. (April 16, 2013). *TrendLabs Security Intelligence Blog.* "Botnets Involved in Anonymous DDoS Attacks." Last accessed July 25, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/botnets-involved-in-anonymous-ddos-attacks/.

10. Karl Dominguez. (September 4, 2011). *TrendLabs Security Intelligence Blog.* "Bitcoin Mining Botnet Found with DDoS Capabilities." Last accessed July 25, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/bitcoin-mining-botnet-found-with-ddos-capabilities/.

11. Jonathan Leopando. (October 26, 2010). *TrendLabs Security Intelligence Blog.* "Firefox Zero-Day Found in Compromised Nobel Peace Prize Website." Last accessed July 25, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/firefox-zero-day-found-in-compromised-nobel-peace-prize-website/.

12. Microsoft. (2014). *Windows.* "Remote Desktop Connection." Last accessed July 25, 2014, http://windows.microsoft.com/en-us/windows7/products/features/remote-desktop-connection.

13. Trend Micro Incorporated. (2014). *Threat Encyclopedia.* "Distributed Denial of Service (DDoS)." Last accessed July 25, 2014, http://about-threats.trendmicro.com/us/definition/distributed-denial-of-service-ddos.

14. Wikimedia Foundation Inc. (December 28, 2013). *Wikipedia.* "SYN Flood." Last accessed July 25, 2014, http://en.wikipedia.org/wiki/SYN_flood.

15. Neustar Inc. (2014). *DDoSAttacks.biz.* "HTTP GET Flood DDoS Attack, aka HTTP Object Request Flood." Last accessed July 25, 2014, http://www.ddosattacks.biz/attacks/http-post-flood-ddos-attack-definition-mitigation/.

16. Wikimedia Foundation Inc. (July 26, 2014). *Wikipedia.* "Internet Control Message Protocol." Last accessed July 27, 2014, http://en.wikipedia.org/wiki/Internet_Control_Message_Protocol.

17. Wikimedia Foundation Inc. (July 4, 2014). *Wikipedia.* "User Datagram Protocol." Last accessed July 27, 2014, http://en.wikipedia.org/wiki/User_Datagram_Protocol.

18. Staminus Communications. (September 24, 2013). "Types of DDoS: ACK Flood." Last accessed July 27, 2014, https://wiki.staminus.net/index.php/Types_of_DDoS:ACK_Flood.

19. Trend Micro Incorporated. (2014). *Threat Encyclopedia.* "Remote Access Programs/Tools." Last accessed July 27, 2014, http://about-threats.trendmicro.com/us/definition/remote-access-programs-tools.

20. Rhena Inocencio. (May 26, 2014). *TrendLabs Security Intelligence Blog.* "The Blackshades RAT—Entry-Level Cybercrime." Last accessed July 27, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/the-blackshades-rat-entry-level-cybercrime/.

21. Trend Micro Incorporated. (2014). *Threat Encyclopedia.* "TrendLabs 2Q 2014 Security Roundup: Turning the Tables on Cyber Attacks." Last accessed August 12, 2014, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-turning-the-tables-on-cyber-attacks.pdf.

22. Lion Gu. (2014). *Trend Micro Security Intelligence.* "The Mobile Cybercriminal Underground Market in China." Last accessed July 27, 2014, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-mobile-cybercriminal-underground-market-in-china.pdf.

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.

Securing Your Journey to the Cloud

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

Phone: +1.817.569,8900