The Chinese Underground in 2013

Lion Gu
Forward-Looking Threat Research Team
Contents
Cybercriminal Underground Economy Series .................................................................1
Introduction.................................................................................................................2
QQ Groups Abuse ........................................................................................................2
A Statistical Look at the 2013 Chinese Underground Market ........................................3
Compromised Hosts .....................................................................................................8
DDoS Attack Services .................................................................................................9
RATs ..........................................................................................................................10
Chinese Underground Offerings in 2013 ...................................................................11
A Statistical Look at the Chinese Mobile Underground Market ......................................14
Conclusion ..................................................................................................................16
References ..................................................................................................................16

TREND MICRO LEGAL DISCLAIMER
The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.
Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.
Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an “as is” condition.
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. 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. 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”](image)
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.

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.

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

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.

![Bar chart showing comparison of underground chat group activity between 2012 and 2013.](image)

**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.

![Bar chart showing number of underground chat messages per hour in 2013.](image)

**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](image)

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](image)
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. 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.

- **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.

- **Use a compromised host to run complex computing tasks.** An example of such abuse is using compromised hosts as Bitcoin miners. 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.\(^\text{11}\)

- **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.\(^\text{12}\) 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.\(^\text{13}\) 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.\(^\text{14}\) 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.\(^\text{15}\) 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.\(^\text{16, 17}\).\(^\text{18}\) 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. 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.

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.

<table>
<thead>
<tr>
<th>Product</th>
<th>Details</th>
<th>Price</th>
</tr>
</thead>
</table>
| 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

<table>
<thead>
<tr>
<th>Product</th>
<th>Details</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Traffic</strong></td>
<td>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</td>
<td>US$0.26 US$0.42 US$2 US$5 US$38 US$95 US$473</td>
</tr>
<tr>
<td><strong>Trojan</strong></td>
<td>QQ account stealer Taobao account stealer Yun Teng, a bank Trojan toolkit:  • Bronze level  • Silver level  • Gold level  • Platinum level  • Diamond level</td>
<td>US$32 US$323 US$1,273 US$1,596 US$2,080 US$2,565 US$3,856</td>
</tr>
</tbody>
</table>


## Chinese Underground Market Service Offerings

<table>
<thead>
<tr>
<th>Service</th>
<th>Details</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cracking</strong></td>
<td>Encrypted .RAR, .ZIP, .DOC, .XLS, or .EXE file Software:  • Dongle protection  • Registration code  • User number limit protection</td>
<td>US$45 US$807‒12,919 US$161 US$242</td>
</tr>
<tr>
<td><strong>Dedicated-/Bulletproof-server hosting</strong></td>
<td>One-month with DDoS protection</td>
<td>US$81‒775</td>
</tr>
<tr>
<td><strong>DDoS attack</strong></td>
<td>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</td>
<td>US$16 US$73 US$161 US$323 US$81 US$161 US$258‒323 US$452‒484</td>
</tr>
<tr>
<td>Service</td>
<td>Details</td>
<td>Price</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>----------------------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Fake document rework</td>
<td></td>
<td>US$19</td>
</tr>
<tr>
<td>Hacking</td>
<td>Forum account:</td>
<td>US$81</td>
</tr>
<tr>
<td></td>
<td>• Normal user</td>
<td>US$161</td>
</tr>
<tr>
<td></td>
<td>• Subforum administrator</td>
<td>US$323</td>
</tr>
<tr>
<td></td>
<td>• Forum administrator</td>
<td>30% of the official service fee</td>
</tr>
<tr>
<td></td>
<td>• VIP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>QQ account:</td>
<td>US$48</td>
</tr>
<tr>
<td></td>
<td>• Password</td>
<td>US$81</td>
</tr>
<tr>
<td></td>
<td>• Six-month chat log</td>
<td>US$129</td>
</tr>
<tr>
<td></td>
<td>• One-year chat log</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Email account:</td>
<td>US$48</td>
</tr>
<tr>
<td></td>
<td>• Personal</td>
<td>US$81</td>
</tr>
<tr>
<td></td>
<td>• Corporate</td>
<td>US$129</td>
</tr>
<tr>
<td></td>
<td>Sina/Weibo/Renren account</td>
<td></td>
</tr>
<tr>
<td>Malware checking against</td>
<td>Various software</td>
<td>US$13–19</td>
</tr>
<tr>
<td>security software</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Programming</td>
<td>RAT toolkit</td>
<td>US$161</td>
</tr>
<tr>
<td></td>
<td>Trojan</td>
<td>US$323–8,075</td>
</tr>
<tr>
<td>Proxy-server hosting</td>
<td>HTTP SOCKS proxy server:</td>
<td>US$4</td>
</tr>
<tr>
<td></td>
<td>• With a single fixed IP address per month</td>
<td>US$0.16</td>
</tr>
<tr>
<td></td>
<td>• With 800 IP addresses per month</td>
<td>US$2</td>
</tr>
<tr>
<td></td>
<td>• With 9,000 IP addresses per month</td>
<td>US$16</td>
</tr>
<tr>
<td>RAT toolkit rental</td>
<td>TYT/MBZ RAT per year</td>
<td>US$97</td>
</tr>
<tr>
<td></td>
<td>RD RAT:</td>
<td>US$129</td>
</tr>
<tr>
<td></td>
<td>• One month</td>
<td>US$258</td>
</tr>
<tr>
<td></td>
<td>• One year</td>
<td></td>
</tr>
<tr>
<td>Spamming</td>
<td>1,000 email addresses</td>
<td>US$13</td>
</tr>
<tr>
<td></td>
<td>10,000 email addresses</td>
<td>US$97</td>
</tr>
<tr>
<td></td>
<td>20,000 email addresses</td>
<td>US$161</td>
</tr>
<tr>
<td></td>
<td>50,000 email addresses</td>
<td>US$323</td>
</tr>
<tr>
<td></td>
<td>100,000 email addresses</td>
<td>US$484</td>
</tr>
<tr>
<td>Trojan attack</td>
<td>One online game per day</td>
<td>US$29</td>
</tr>
</tbody>
</table>
### Chinese Underground Market Service Offerings

<table>
<thead>
<tr>
<th>Service</th>
<th>Details</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN-server hosting</td>
<td>One month</td>
<td>US$3</td>
</tr>
<tr>
<td></td>
<td>Three months</td>
<td>US$8‒10</td>
</tr>
<tr>
<td></td>
<td>One year</td>
<td>US$19‒32</td>
</tr>
</tbody>
</table>

**NOTE:** The service prices in the table above are based on RMB to U.S. dollar exchange rates as of July 27, 2014.


### 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.\(^2\) 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.

![Overall MGD vs Mobile MGD](image)

**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](image)

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](image)
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.”

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


