



CHINA:

# PAINTING THE THREAT LANDSCAPE

By Geok Meng Ong and Yichong Lin

**F**ew events today are changing the world's political and economic landscape quite like China's rapid rise among the great powers. In 2006, China's Gross Domestic Product (GDP) grew by 10.7 percent, the highest figure in 11 years; this occurred only one year after China overtook the United Kingdom as the world's fourth-largest economy. At this time of tremendous growth and change, China's Internet threat landscape is also changing rapidly. Why are we seeing this increase in malware coming from and moving into China?

### Rapid Internet growth

In 2007, 12 percent of this enormous nation—37 percent of all Internet users in Asia, or 137 million people—were online. Dr. Charles Zhang, chairman and CEO of Sohu.com, a Chinese Internet portal, offers his interpretation of what this means.<sup>1</sup> Chinese Internet users spend almost two billion hours every week online, he says, or more than 15 times longer than American Internet users. He attributes this phenomenon to the lack of a free press in conventional media in China. In September 2006, Chinese lawmakers passed a new ruling requiring all foreign news agencies to release information through the state-owned Xinhua News Agency.<sup>2</sup> China's Internet population skyrocketed at an effective growth rate of 509 percent during the last five years. In comparison, the world has seen a 200 percent and the United States a 121 percent effective growth rate during the same period.

### Booming local Internet apps

In the age of the Internet boom, there is a need to grow localized content, as the audience develops an appetite for more.

### Online gaming

A quarter of all Chinese Internet users are online game players; as of April 2007, 33 percent of players were between 19 and 22 years old. Online gaming addiction is burning across China like wildfire, so much so that the Chinese government introduced a unique "Game Fatigue Regulation" system: Each time an under-aged gamer plays for more than three hours in a day, he or she loses "experience points" in the game. Playing beyond five hours a day costs a gamer all the points. In today's 31-million-player gaming market, the business of online gaming has a new meaning.

### Virtual commodities

Real Money Trade (RMT), the concept of trading virtual gold or goods collected from computer games for real money, is rapidly catching on with online gamers. The popularity of online gaming in China creates a ready market for RMT, which industry observers estimated to be worth up to US\$900 million. A quick search of Chinese keywords "Gold" and "World of Warcraft" on China's number-one auction portal, Taobao.com, yields 32,891 finds; with "Power Leveling Service" and "World of Warcraft," we got 19,982 results.

The sellers include gaming workers or "gold farmers," who play online games day and night to harvest virtual currency, goods, or magic spells in "virtual sweatshops." Each gold farm can employ hundreds of young workers, each making up to US\$250 a month.<sup>3</sup> It is estimated that there are more than 100,000 such gamers in China supplying virtual commodities to both domestic and foreign demands.

---

*Online gaming addiction*

*is burning like wildfire,*

*so much so that the*

*Chinese government*

*introduced a unique*

*'Game Fatigue Regulation' system.*

---

<sup>1</sup> "China Surpasses U.S. in Internet Use." Forbes.com. [http://www.forbes.com/2006/03/31/china-internet-usage-cx\\_nwp\\_0403china.html](http://www.forbes.com/2006/03/31/china-internet-usage-cx_nwp_0403china.html)

<sup>2</sup> "The Administration of Release of News and Information in China by Foreign News Agencies," Xinhua. [http://news.xinhuanet.com/politics/2006-09/10/content\\_5072446.htm](http://news.xinhuanet.com/politics/2006-09/10/content_5072446.htm)

<sup>3</sup> "Ogre to Slay? Outsource It to Chinese." The New York Times. <http://www.nytimes.com/2005/12/09/technology/09gaming.html?ex=1291784400&en=a723d0f8592dff2e&ei=5090>

### Instant messaging

RMT is not limited only to online gaming. Instant messaging (IM) in China is more than what the name implies. Beyond instant messages, it has developed into a platform providing telephony service, entertainment, email, gaming, and remote assistance. To sell virtual amusements to Chinese Internet users, Tencent retails one virtual QQ coin for ¥1 (1 yuan, about US\$0.13) on the street. With few restrictions when initially introduced, the QQ "currency" has been traded for real currency in black markets, creating an avenue for money laundering and making the RMT of QQ accounts and currency profitable. Even online casinos and pornography sites trade QQ coins, raising an alarm with the Chinese authorities due to its wide abuse.

In a survey conducted by the Chinese media, 70 percent of users have had their QQ account stolen at some time.<sup>4</sup> Tencent, owner of the QQ network, recognizes these increasing threats and provides free security education and services on their Web site.<sup>5</sup>

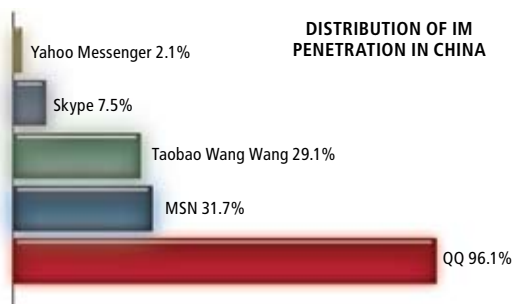


Figure 1: Tencent QQ dominated the Chinese Internet messaging market in 2007.<sup>6</sup>

### Anonymous payment modes

To widen the scope of money laundering and RMT, most people in China do not have a credit card or a personal computer to make online payments. Many Chinese gamers hang out at Internet cafés, and prepaid game cards are the preferred payment method not only at the cafes, but also in online stores and gaming centers. Without the need for registration, prepaid cards are virtually anonymous. In real-world cases, cyberthieves with stolen online bank accounts or credit numbers buy the prepaid cards and sell them online. Cybercriminals have also penetrated prepaid card networks to steal prepaid card numbers. The anonymity and wide use of prepaid cards increase the complexity for law enforcement agencies to track down rogue transactions and cybercrimes.

### Malware activities in China

We have seen how virtual commodities trading has become a multimillion-dollar business, and we have seen enterprising gold farmers making use of low-cost labor to increase their gains. It's no surprise that those with access to the technical know-how to achieve these goals in a bigger and faster way are using malware. As we have seen, the majority of malware originating from Chinese domains are password stealers. At first targeting the main platforms—QQ, World of Warcraft, Lineage—today password stealers cover every possible target of RMT.

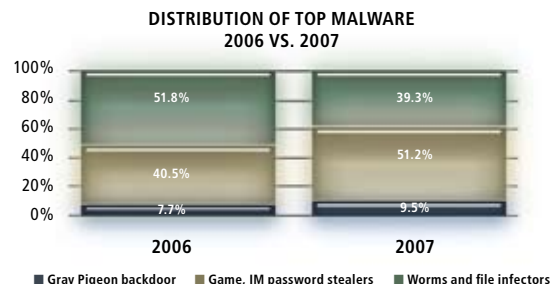


Figure 2: The last year has seen a big increase in password stealers in the Chinese market.

McAfee® Avert® Labs reported an increasing trend in game password-stealer threats in 2006 that peaked in October, and the trend is evidently continuing in 2007. From the earliest PWS-QQPass, PWS-WoW, and PWS-Lineage Trojans, we now see "cocktails" such as PWS-OnLineGames and PWS-MMORPG targeting multiple online games and communities. Multivector worms such as W32/Fujacks and Web exploits continue to increase the opportunities to commit crimes.

---

*Cybercriminals are not necessarily expert hackers. As in traditional sales channels, they follow a chain of supply and demand.*

---

4 "Tencent Introduces QQ Security Card," Sohu.com. <http://digi.it.sohu.com/20070906/n251998008.shtml>

5 "Tencent Safe," Tencent. <http://safe.qq.com/>

6 "QQ Extends Its Market Leadership in 2007," "Taobao Wangwang Catching Up With MSN Q1," iResearch. [http://www.iresearchgroup.com.cn/Consulting/instant\\_messenger/DetailNews.asp?id=65222](http://www.iresearchgroup.com.cn/Consulting/instant_messenger/DetailNews.asp?id=65222)

### Organized crime

With Chinese malware, we see a massive Internet community and RMT market supporting its growth; substantial profits provide the means for exploits to get better and bigger. China's Computer Emergency Response Team (CNCERT) noted, in its recent half-yearly report, an increase in Chinese Web sites used for phishing and the hosting of malicious code; the increase alone is greater than the overall figure for 2006.

In 2007, McAfee SiteAdvisor™ has found 0.2 percent of all Web sites registered in China to be hosting exploits; that's more than twice the global average. These sites include a good mix of .org.cn, .gov.cn, .com.cn, .net.cn, and other domains. Many of these may be legitimate sites that have been hijacked by criminals to host malicious code, allowing unaware users to risk infection while browsing their regular "clean" sites. What is more alarming is the wide use of zero-day exploits such as Exploit-AniFile.c. File-infecting worms such as W32/Fujacks and man-in-the-middle or address resolution protocol-poisoning threats such as NetSniff act as catalysts for wide propagation.

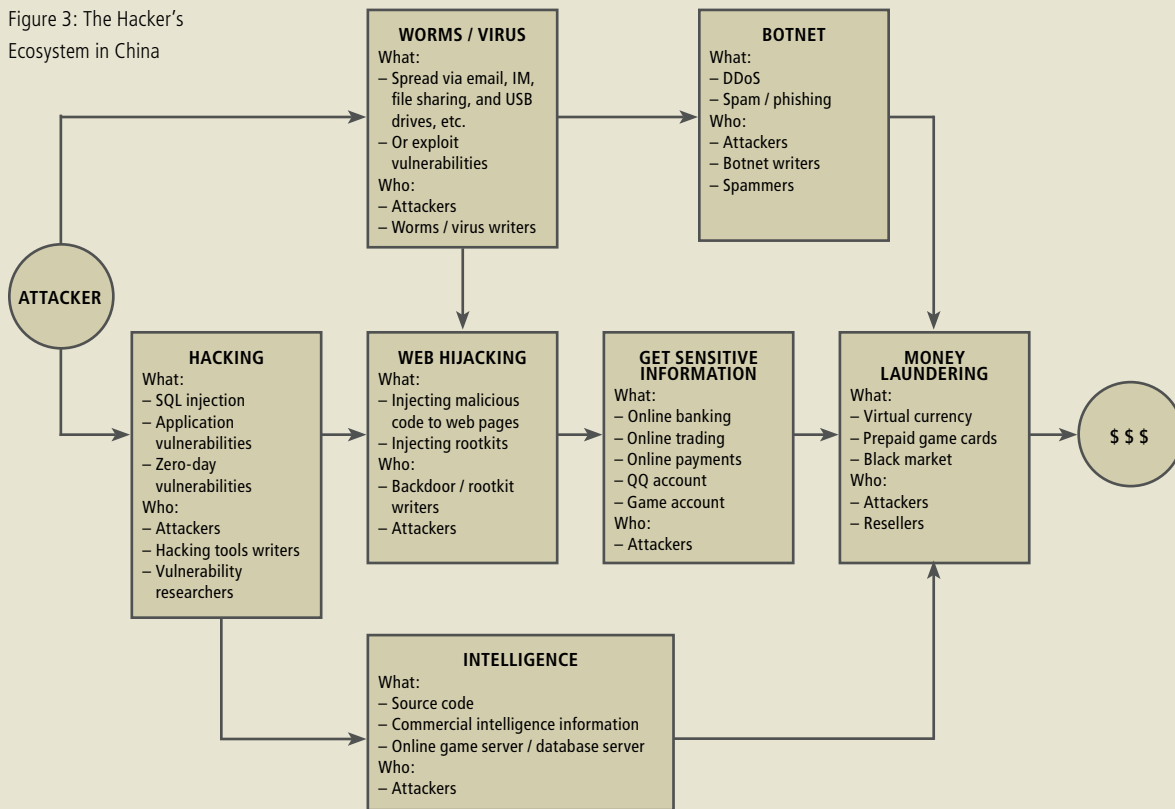
Cybercriminals are not necessarily expert hackers. As in traditional sales channels, they follow a chain of supply

and demand. In February 2007, Xinhua reported a group of 50 resellers in Zhejiang province helped sell stolen user accounts and virtual commodities from Li Jun (the W32/Fujacks author) and his accomplices. They were also reportedly part of a syndicate to perform phishing and release adware to commit fraud. None of the resellers were computer experts; one of them worked as a chef in a restaurant.

In an organized cybercrime chain, various tools and roles typically work hand in hand. Exploits target unpatched vulnerabilities to provide an entry for intruders, bots and backdoors provide command and control, and password stealers and spyware collect sensitive or profitable data.

BackDoor-AWQ.b, or Gray Pigeon backdoor as it is called by its creators, has been commercially marketed and sold as a "remote administration tool" on its Web site since 2003; it costs just ¥100 (US\$13) for an annual subscription. Users get updated versions with enhanced features such as rootkits, distributed command and control, keylogging, etc. The site was shut down by its owners in March 2007, following the arrests of the W32/Fujacks authors. Security analysts worry that this group could be moving its operations underground, and will be even harder to track.

Figure 3: The Hacker's Ecosystem in China



## Talent pool vs. unemployment

In Beijing alone, the number of university graduates reached an all-time high of nearly 200,000 in 2007. However, only 43 percent are expected to be employed. In rural regions, unemployment can be worse. In fact, many “gold farmers” came from rural and suburban China, working 12-hour shifts and making US\$250 a month, which is a pretty good wage in the poorest parts of the country.

Li Jun, 25, having been unsuccessful in securing a job after graduating from a computer school in 2005, desperate for money, and armed with malware-writing skills, has since authored and released W32/QPass.worm and W32/Lewor, in addition to the now infamous W32/Fujacks.worm. He sold the source code of W32/Fujacks to more than 120 buyers, making a profit of over US\$13,000 in a city where the per capita annual salary is around US\$3,000. There could easily be more young people like him. Hackbase.com is one of largest “hacker” training Web sites in China; they claim to have more than 10,000 members. At sister site hackerbase.net, they explicitly offer paid hacking services.

## Government policies

In September 2007, Li Jun was convicted by the Chinese court to four years in prison. Will that deter other malware authors from committing cybercrimes? During the trial, Li Jun’s lawyer presented an offer letter from an IT company in Hangzhou for the position of CTO. He claimed that there were ten other offers from various companies to pay Li Jun more than ¥1 million (US\$133,000) annual salary. In fact, the spread of worms in China has not declined following these arrests in early 2007. The fact that the W32/Fujacks source code was sold didn’t help.

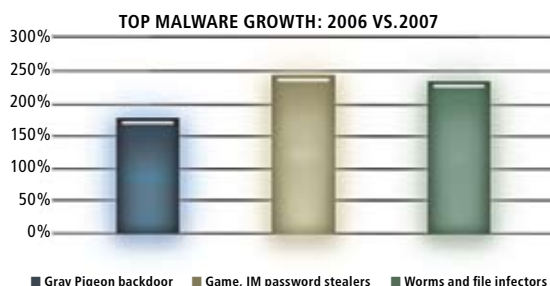


Figure 4: Password stealers are growing at a faster rate than other malware.

Have recent changes been too overwhelming in China? At least in Internet security, we can see that the rapid adoption of technology has been far quicker than government policies, corporations, and traditional culture can catch up.

ICBC, the largest state-owned commercial bank, reported e-banking transaction volume hitting ¥170 billion (US\$22.6 billion) in the first quarter of 2005 alone, up from only ¥15.4 billion (US\$2 billion) in 2000. In 2005, the China Banking Regulatory Commission (CBRC) revealed that

---

*Analysts reportedly said that the popularity of QQ currency has reached a point where it threatens the value of the yuan.*

---

policies passed in 2000 were not able to regulate the management and monitoring of the additional risks associated with Internet banking. New “E-banking Business and Relevant Security Evaluation” criteria were introduced by CBRC in 2006 to cover the new risks in the virtual world.<sup>7</sup>

Now that QQ currency has been available for five years, Chinese regulators have finally ordered restrictions on its circulation—after concerns of abuse and money laundering. Analysts reportedly said that the popularity of QQ currency has reached a point where it threatens the value of the yuan.

## What’s next?

We have seen how the Chinese threat landscape has been shaped by its unique local cultures, politics, and economics. Regulation and controls have been playing catch-up at a peak of China’s growth and changes. The popularity of the Internet, combined with widespread unemployment and a large talent pool, has created an environment that encourages malware writers. Current conditions have pushed these hackers to become cybercriminals going for the money.

---

*On the positive side, the recent conviction of cybercriminals such as Li Jun shows that Chinese lawmakers are taking cybercrime seriously.*

---

<sup>7</sup> Q&A with China Banking Regulatory Commission. <http://www.cbrc.gov.cn/chinese/home/jsp/docView.jsp?docID=2243>

On the positive side, the recent conviction of cybercriminals such as Li Jun shows that Chinese lawmakers are taking cybercrime seriously. The impact of local cyberthreats has also hastened the development of government policies and local applications to introduce new measures to deter cybercrimes. The only way to ensure the continual growth of this market is to develop the necessary security measures to protect its users.



Geok Meng Ong manages a team of security researchers in the Asia Pacific and Japan regions for McAfee Avert Labs.

By chance, he discovered the dark side of the cyberworld, which fuelled his passion for security research. In the spirit of Singaporean kiasu-ism,<sup>8</sup> he joined McAfee to master the zen of world-class security. A hands-on researcher himself, Ong focuses on malware heuristics and vulnerability research, and is often quoted in the media for his analysis of new malware trends and exploits that are prevalent in this region.



Yichong Lin is a security researcher at McAfee Avert Labs. He focuses on intrusion-detection technology and vulnerability research. Both

authors have studied the Chinese security market for many years.



<sup>8</sup> "The calculating obsession that inflicts people who believe that they must get their money/time/effort's worth (the greater the returns the better!)" Urban Dictionary. <http://www.urbandictionary.com/define.php?term=kiasuism>