An investigation into Chinese cybercrime and the underground economy in comparison with the West

SOCA
SERIOUS ORGANISED CRIME AGENCY

Michael Yip
School of Engineering and Computer Science
University of Southampton

UNIVERSITY OF Southampton
School of Electronics and Computer Science

Introduction

With 420 million Internet users, China has become the world's largest Internet population. Yet, the Internet penetration rate in China is only 31.6%, which means that the Chinese Internet population has the potential to triple in size in the foreseeable future. With cybercrimes transcending national boundaries, the security of the Internet in China is becoming increasingly significant to the global Internet.

Economic factors

By understanding the current state of the Chinese labour market, it is easy to understand why some have become cybercriminals.

- 94.9% of the Internet users in China have an average monthly income of less than 5,000 RMB (£473), which is less than the average weekly salary of £489 in the U.K. in 2009.
- The Chinese education system, just like in Russia, places strong emphasis on computing related subjects like Mathematics and Science, perhaps stemming from their common Communist preference for a polytechnic education system which stresses industriousness.

Framework of cybercrime

Not only do organised cybercrimes exist in China but also a sophisticated underground economy is flourishing rapidly. It has been estimated by Chinese security experts that the potential worth of the Chinese underground economy would soon reach 10billion RMB (US$1.48 billion). This is far larger than the figure reported in 2008 by Symantec who estimated the total amount of the advertised goods they observed was worth approximately US$276 million.

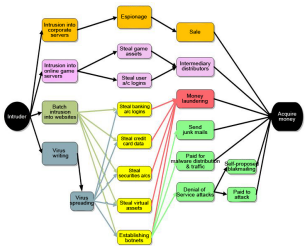


Figure 1 – Chinese underground economy "production chain"

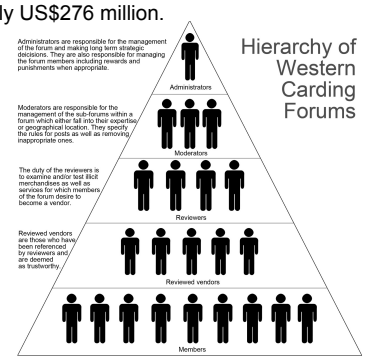
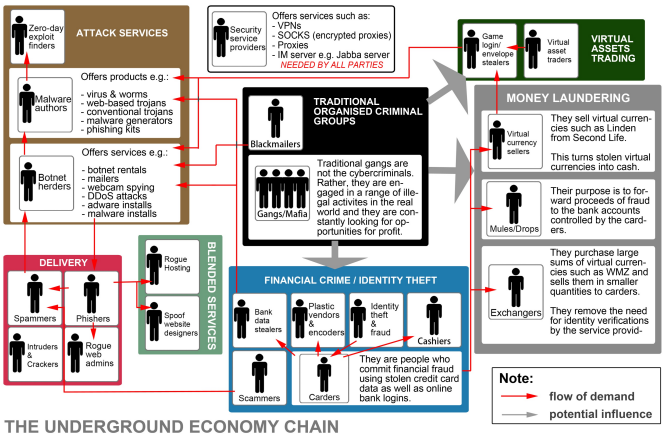


Figure 2 – the common hierarchical structure in Western carding forums



THE UNDERGROUND ECONOMY CHAIN

Figure 3 – a generalised mapping of the underground economy

Political factors – "hacktivism"

It is a popular belief in China that after suffering more than a century of national humiliation since the Opium War (1840), it is Communism which has brought the glory days back to China. Thus, the Chinese hacktivists are called the "Red hackers" (the *honkers)* and they are those empowered to protect their country from further political humiliation. Recently, the honkers launched cyber-attacks against Japan and by monitoring their discussion forums, several interesting observations were made including:

- The honkers showcasing their work like trophies (figure 5).
- Intervention from the Chinese government brought a stop to the attacks.
- Not all honkers agree on attacks such as website defacements.

Figure 5 – the honkers showcasing the defacement of a Japanese website. They hacked into servers and change the homepage to the one shown above which states a demand for an official apology from the Japanese government.

Chinese underground economy

While the Western cybercriminals prefer to use online forums which commonly have a hierarchical management structure (figure 2), the Chinese cybercriminals prefer to form networks of ephemeral relationships (figure 1) using more decentralised means such as *Baidu Tieba* (figure 6) and *QQ Instant Messenger*. Furthermore, the pricing of carding merchandises were found to be similarly priced in China and the West but services such as hacking and Denial-of-Service (DoS) attacks are not.

Carding: *the fraudulent use of third party credit card information for personal gain*

Figure 6 – the "visa" bar on *Baidu Tieba*, the most popular online discussion board for Chinese carding advertisements

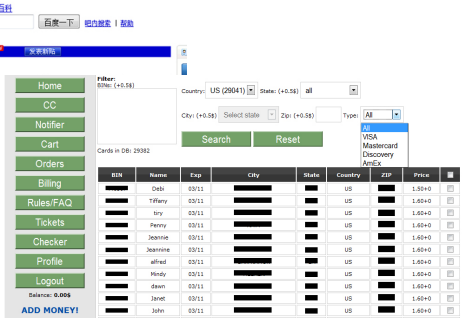


Figure 7 – Chinese carders were found to use foreign carding sites, which could explain the similar pricing of carding merchandises in China and the West

Conclusion

Like in the West, organised cybercrimes are flourishing in China. With a rapidly expanding Internet population, China is fast becoming a giant hub of cybercrime activities. Therefore, it is in the interest of Western cyber-security experts to increase their attention to China's cyber-security.

Acknowledgements

I would like to express my gratitude to Dr Craig Webber and the Serious Organised Crime Agency for the support throughout the project.