An Investigation into Chinese Cybercrime and the Applicability of Social Network Analysis

Michael Yip
School of Engineering and Computer Science
University of Southampton
Southampton SO17 1BJ
my2e09@ecs.soton.ac.uk

ABSTRACT
With the support from the UK's Serious Organised Crime Agency (SOCA), this paper presents the findings from a two-month comparison study between the underground economy in China and the West. Significant differences were found which are due to traditional boundaries of crime, such as cultural and language barriers. Lastly, Social Network Analysis (SNA) is proposed and discussed as a tool for future cybercrime research.

Categories and Subject Descriptors
K.4.2 [**Computers and Society**]: Abuse and crime involving computers

General Terms
Security, Human Factors, Theory

Keywords
Cybercrime, Organized Crime, Carding, Underground Economy, Social Network Analysis

1. INTRODUCTION
The last decade has seen fascinating transformation in the nature of cybercrime, from solely destructive to omnivorously profit seeking. With this transformation was the change in the ways in which cybercrimes are committed as cybercriminals become increasingly collaborative and organized. Individuals with different skill-sets join in ephemeral relationships to commit a common act and to reproduce their skills and knowledge [11]. This trend is relatively well researched in the West but very little is known about the Far East and especially China.

As China's internet presence continues to grow rapidly, the state of cybercrime in China can no longer be ignored. Therefore, a two month qualitative study on Chinese cybercrime was carried out with the support from U.K.'s Serious Organised Crime Agency (SOCA). The findings from this study were then compared with the workings of the Western underground economy. The results of this comparison study are presented in this paper and the application of Social Network Analysis (SNA) is proposed and discussed as a potential tool to study cybercrime in future research.

The remainder of this paper is as follows: section 2 presents some related work. Section 3 presents the characteristics of the current Western online black markets. Section 4 presents the characteristics of the Chinese underground economy and compared with that of the West. Section 5 presents a discussion of the results and Social Network Analysis (SNA) as a tool to study cybercrime in future research.

WebSci '11, June 14-17, 2011, Koblenz, Germany.

2. RELATED WORK
Related work falls into two categories: underground economy on Internet Relay Chat (IRC) and Chinese cybercrime.

Two previous studies have focused on the underground economy on the IRC channels. In their work, Thomas and Martin [9] present a concise introduction to the workings of the underground economy and the actors involved. The work of Franklin et al. [3] also focused on IRC channels but their work involved keeping track of the advertisements by capturing IRC logs over a 7 month period. Their analysis was focused on examining characteristics such as sensitive data types, credit card types and country of issuing banks.

With regards to Chinese cybercrime, the most closely related study is the work by Zhuge et al. [14] in which they examine the Chinese underground economy with a focus on virtual assets such as QQ accounts and equipments in online games. Their work involved a detailed analysis of the posts made on the largest bulletin board in China, post.baidu.com (now known as tieba.baidu.com or Baidu Tieba).

The study presented in this paper is unique from the above in that the focus is on the carding activities that occurs on the World Wide Web rather than IRC and that the underground economy in China and the West are treated as separate subjects of study.

3. WESTERN ONLINE BLACK MARKETS
While this study does not intend to eliminate the possibility of Chinese carders collaborating with Western carders, it was found that a substantial portion of Chinese carders operate differently from their Western counterparts.

There are two reasons for this. Firstly, due to the workings of the internet and the need to preserve anonymity, it is hard for a criminal to place trust on another online identity. This is problematic for those seeking to trade and profit from carding. As documented by von Lampe and Johansen, in the criminal world, one of the ways to reduce risk in the absence of trust is to test merchandises before a transaction is made. This increases the need for negotiation and the author believes this is where some of the Chinese carders hit the language barrier. Secondly, there is a cultural difference in the tools they use, such as payment and communication applications. This will be discussed in section 4.

Thus, the focus of this study is on understanding how the Chinese carders operate by drawing on SOCA's information on the

Western carders. This section presents infrastructure of the online carding markets in the West.

3.1 Online carding forums

Aside from the well researched IRC channels, it is observed by Peretti [5] and agreed by SOCA that most Western carding activities occur in closed membership forums. Members are usually "vouched" in through previous transactions with existing members or the quality of the "goods" they offer are tested.

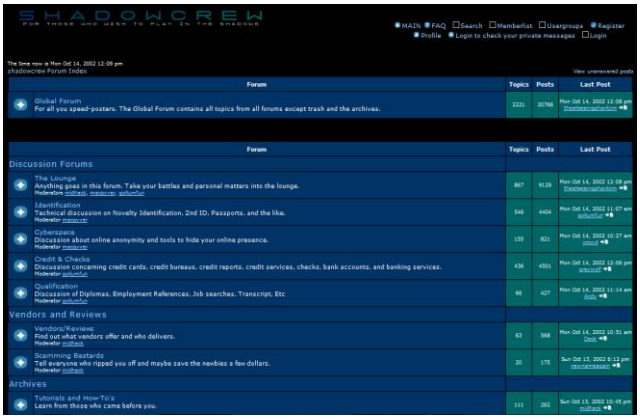

Figure 1: Shadowcrew, one of many carding forums shut down by the FBI and SOCA

Figure 1 is a screenshot of a carding forum called Shadowcrew which began operation in 2002. It provided an exchange platform for carders and hackers to trade goods and services with free membership. The contents were available in both English and Russian in order to increase geographical dispersion of its members so that the availability of cash-out and drop[1] locations would increase. Shadowcrew was shut down by the U.S. and international law enforcement agencies in Operation Firewall in 2004 [1,2].

Shadowcrew, like many other online carding forums, contained sub-forums to serve different purposes such as trading, how-to tutorials, disputes and rippers report. Members could also contact each other privately using the private messaging service.

3.2 General management hierarchy

Due to the ways online forums are structured, most Western carding markets have an inherently hierarchical management structure, as described in the Operation Firewall indictment [1]. Such a management hierarchy is shown in figure 2. The role of each actor is summarised below.

Administrators: they are responsible for the overall management of the forum and making long term strategic decisions. Such strategic decisions include protecting the forum from attacks by other similar carding forums, should they become involved in a "board war". Administrators are also responsible for managing the forum members including rewards and punishments when appropriate. In particular, they safeguard the forum by removing the "rippers", the members who have cheated money off others.

[1] Drop – an intermediary location at which carders could use as delivery address for physical goods bought with fraudulent cards. They are also used to refer to intermediary bank accounts used in money laundering.

Moderators: the moderators are responsible for the management of the sub-forums within a forum which either fall into their expertise or geographical location. They specify the rules for posts as well as removing inappropriate ones.

Reviewers: their duty is to test illicit merchandises and services from the members wanting to become a vendor. This is the key part of the trust mechanism in place as these few reviewers are endorsed by the majority as trustworthy and the trust on them propagates to the vendors they review, allowing quality assurance to take place and propagate as supply increases.

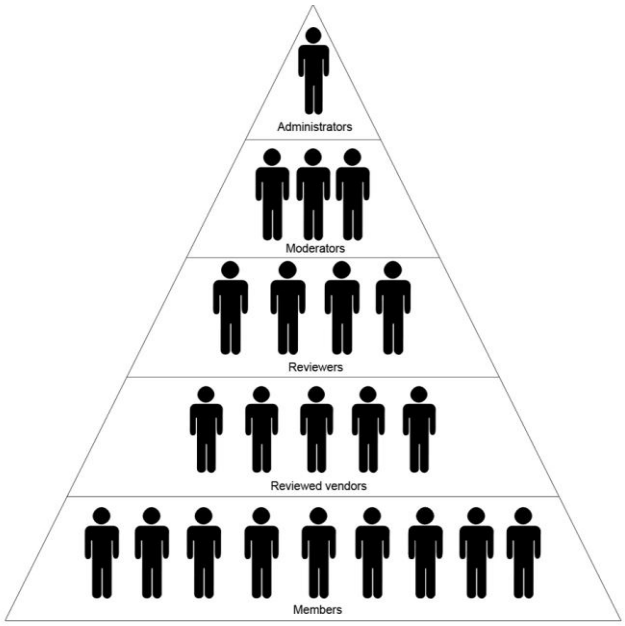

Figure 2: - a typical hierarchical chain of command in Western online carding forums

Reviewed vendors: they are those who have been referenced by the reviewers and are deemed as trustworthy. As reputation is crucial to their success and the only way the system can recognize these reviewed vendors is through their chosen username, these usernames become attached to their reputation. Thus, most members rarely change their usernames within a forum.

Members: normal members who are not reviewed vendors may also sell goods on carding forums but they most often sell at lower prices due to the lack of credibility. Those who buy from them bare the risk at their own discretion. The services offered by the members are generally similar to the ones listed by Thomas and Martin [9]. Many carders are members of various different forums.

This hierarchy is crucial as it puts in place a monitoring mechanism to defeat the rippers, thus allowing the carders to trade without needing to worry about being ripped.

4. CHINESE UNDERGROUND ECONOMY

To comprehensively compare Western and Chinese carding, this study focused on finding the ways in which the Chinese carders accomplish similar services offered by the Western online forums. In particular, this section presents how the Chinese carders advertise goods and services, the trust mechanism in place to avoid rippers, privacy to hold private negotiations and trading.

4.1 Advertising, trust and communication

The most essential element of carding is the need to advertise goods and services as well as a way to find these advertisements. In the Western carding forums, this is relatively trivial as forum posts are ordered chronologically and most forums offer a search engine for conducting keyword-based search for relevant posts. Furthermore, negotiations could take place using the forum's private messaging function or using ICQ[2]. There are two primary tools for Chinese carders to achieve these functions: Baidu Tieba[3] and QQ[4].

4.1.1 Baidu Tieba

As Zhuge et al. have noted, the Chinese cybercriminals do not use IRC but more prefer to use Baidu, China's largest search engine [14]. However, aside from searching, Baidu also offer various social networking services, most notably the Baidu Tieba.

Baidu Tieba is a publicly accessible and searchable message board system where specific boards (called "bar") can be freely created by a registered user under a specific title. Once the bar is created, it will be indexed by Baidu and the contents within these boards become easily searchable.

Users can choose whether to make a post on the board anonymously. If the user is registered, his username will be shown as the author. If the user is not registered, the first three range of his IP address is shown in the author's field. This means the anonymity of the users is preserved.

The lack of control of the Baidu Tieba, the permanent storage of posts, the preservation of anonymity and content search ability, makes Baidu Tieba the most convenient place for Chinese carders to advertise their goods and services as well as for those searching for specific services. The most popular boards used by the Chinese carders are: "visa", "master" and "cvv".

A typical sale advert is as shown in figure 3. The typical format of an advert on Baidu Tieba consists of a short message containing a brief description of the goods and services for sale or request (such as the country and types of credit cards) as well as leaving the QQ number for interested buyers to hold further negotiations in private conversations via QQ (see next section for a more detailed examination of QQ IM). This advertisement says that the seller has large quantities of credit card data from the US, UK, DE (Germany) and Japan.

Figure 3: a typical carding related advert on Baidu Tieba

One of the most fundamental functions offered by the closed membership forum is a tight control over rippers with reviewed vendors and monitoring by the administrators. The Chinese carders do not have such mechanism. Instead, rippers are posted and shamed on Baidu Tieba.

A typical report on rippers would consist of the QQ number of the ripper and some evidence as proof of ripping. Given the ease of searching for contents in posts on Baidu Tieba, the Chinese carders can avoid being ripped by performing a search for the QQ number of the carders they are interested in trading with, before entering any negotiations.

4.1.2 QQ

For private negotiations, the Chinese cybercriminals prefer to use Tencent's QQ Instant Messenger (IM) as it is the most popular instant messenger in China. However, QQ is more than just an instant messenger. QQ also offers a social networking service called QQ Group and its functionality is identical to that of an IRC channel. Unlike an IRC channel which is purely text based, multimedia content including text and images and webcam can be used on QQ groups. The QQ Groups found to be carding related are as follows:

Table 1: carding related QQ groups

QQ number	Group name	No. of members
60776008	国外 CVV 交易交流	138
9849627	PP,MB,CB,Card 交流 1	64
40702312	PP,MB,CB,Card 交流 2	84
85707782	内外料交易群	86
61981088	黑卡 CC	432
55807561	夜猫俱乐部	229
118731023	单身贵族	86
118731529	单身贵族（4）	149
31715092	财神到㊣EBAY/paypal 研究	199
57758881	黑 CARD 交流	55

Thus, the QQ messenger can be seen as the combination of ICQ and IRC and combined with the Baidu Tieba, it is evident that there is no need for the Chinese carders to mimic their Western counterparts and use closed membership forums, which are proven to be vulnerable to police undercover operations.

4.2 Trading

For Chinese carders, the most popular tool for trading is Taobao[5], China's biggest online trading platform equivalent to eBay in the West. Taobao is a popular place for Chinese cybercriminals because there are no admin charges for sellers and buyers have the power to review the purchased goods before instructing the payment system, Alipay, to forward the paid funds to the seller to complete the transaction.

5. DISCUSSION

There are two important implications from the results presented in this paper.

Firstly, the results show that there are aspects of profit-seeking cybercrime such as trading and negotiation, which can be constrained by traditional boundaries of crime such as location, culture and language barriers. Future research could focus on

[2] http://www.icq.com

[3] http://tieba.baidu.com

[4] http://www.qq.com

[5] Taobao – http://www.taobao.com

providing a quantitative analysis on such localized cybercrime, as well as an estimation of the volume and impact which can then be used to compare with the rest of the world.

Secondly, it is evident that social networking is a critical process for the profit seeking cybercriminals. Thus, there is a strong need for them to establish ties with others in the absence of trust. This is an area in which the author is looking to explore for his future research because the results presented in this paper only demonstrate the existence of a difference in cybercriminal *market* structure, not necessarily the structure of cybercriminal organizations behind the *"delivery"* of cybercrime.

Therefore, future research could include questions such as: "What are the structural patterns of interaction within the Western online carding forums and are they any different from those in China?", "Are there any hidden key players?" [12], "What are the constraints and opportunities provided by the different networks structures? For example: security/efficiency trade-off.", "How do individual-level characteristics interact with relational (network-level) characteristics?" [6] and "Is there a cultural or ethnic difference?".

To attempt at answering the above questions, McIllwain argues one should first realize that the least common denominator of organized crime is human relationships [4]. Social networking is inevitable for the provision of illicit goods and services as well as the protection, regulation and extortion of those engaged in the provision or consumption of these goods and services. This process of social networking occurs as part of a social system of organized crime, a system which explains the remarkable consistency of the process of organizing crime across time and space. Therefore, to understand organized cybercrime, researchers and analysts should focus on discovering the pattern of relationships (ties) and to understand why and how they occur. This can be achieved using Social Network Analysis (SNA), a theoretical and methodological paradigm for sophisticated examination of complex social structures and has long been suggested as a tool that could aid criminal intelligence proposed by Sparrow in 1991 [8]. The works by Xu and Chen provide some encouraging results in the use of SNA to study the dark web [13].

Social psychology will also play a vital role because as highlighted by Robbins, any network analysis risks an incomplete analysis if the social psychology of the target network is neglected [6]. That is, since the target network is a human social system, it is unreasonable to neglect the individual factors which influence the network structure, that is, the individual factors which are explanatory of network features.

6. ACKNOWLEDGMENTS

This research would not have been possible without the support from the Serious Organised Crime Agency (U.K.) who have expressed great interest throughout the entire duration of study and were very kind helping to ensure the accuracy of the findings. It must be clarified that all views and conclusions presented in this paper are those of the authors and should not be interpreted as representing official policies or endorsements of SOCA. All stolen data encountered during the course of this study have been reported to SOCA.

7. REFERENCES

[1] Department of Justice 2003. Operation Firewall Indictment. DOI= http://www.justice.gov/usao/nj/press/files/pdffiles/firewallindct1028.pdf#search=%22firewallindct1028.pdf%22.

[2] Fossi, M. et al. 2008. Symantec Report on the Underground Economy. Symantec. DOI= http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_underground_economy_report_11-2008-14525717.en-us.pdf.

[3] Franklin, J. & Paxson, V., 2007. An inquiry into the nature and causes of the wealth of internet miscreants. In *Proceedings of the 14th ACM conference on Computer and communications security*. New York, NY, USA: ACM, pp. 375-388. DOI= http://doi.acm.org/10.1145/1315245.1315292.

[4] McIllwain, J.S., 1999. Organized crime: A social network approach. *Crime, Law and Social Change*, 32(4), pp.301-323. DOI= http://dx.doi.org/10.1023/A:1008354713842.

[5] Peretti, K. 2008. Data Breaches: What the Underground World Of "Carding" Reveals. U.S. Department of Justice. DOI= http://www.chtlj.org/sites/default/files/media/articles/v025/v025.i2.Peretti.pdf.

[6] Robins, G., 2008. Understanding individual behaviors within covert networks: the interplay of individual qualities, psychological predispositions, and network effects. *Trends in Organized Crime*, 12(2), pp.166-187. DOI= http://www.springerlink.com/index/10.1007/s12117-008-9059-4.

[7] Smith, R., 2010. Identity theft and fraud. In Y. Jewkes & M. Yar, eds. *The Handbook of Internet Crime*. Devon: Willan Publishing, pp. 273-301.

[8] Sparrow, M., 1991. The application of network analysis to criminal intelligence: An assessment of the prospects. *Social Networks*, 13(3), pp.251-274. DOI= http://linkinghub.elsevier.com/retrieve/pii/037887339190008H.

[9] Thomas, R. & Martin, J., 2006. the underground economy : priceless. *The USENIX Magazine*, 31(6), pp.7-16. DOI= http://www.usenix.org/publications/login/2006-12/openpdfs/cymru.pdf.

[10] von Lampe, K. & Ole Johansen, P., 2004. Organized Crime and Trust: On the conceptualization and empirical relevance of trust in the context of criminal networks. *Global Crime*, 6(2), pp.159-184. DOI= http://www.informaworld.com/10.1080/17440570500096734

[11] Wall, D., 2008. Cybercrime: The Transformation of Crime in the Information Age, Malden: Polity Press.

[12] Xu, J. et al., 2004. Analyzing and Visualizing Criminal Network Dynamics: A Case Study. In H. Chen et al., eds. *Intelligence and Security Informatics*. Springer Berlin / Heidelberg, pp. 359-377. DOI= http://dx.doi.org/10.1007/978-3-540-25952-7_27.

[13] Xu, J. & Chen, H., 2008. The topology of dark networks. *Commun. ACM*, 51(10), pp.58-65. DOI= http://doi.acm.org/10.1145/1400181.1400198.

[14] Zhuge, J. et al., 2009. Studying Malicious Websites and the Underground Economy on the Chinese Web. In *Managing Information Risk and the Economics of Security*. Springer US, pp. 225-244.DOI= http://dx.doi.org/10.1007/978-0-387-09762-6_11.