Cards, Money and Two Hacking Forums

An Analysis of Online Money Laundering Schemes

Alexander Mikhaylov and Richard Frank
School of Criminology, Simon Fraser University
British Columbia, Canada
{amikhayl, rfrank} @sfu.ca

***Abstract*—The emergence of the internet as a global, borderless communication platform afforded a wide range of social and economic opportunities to people throughout the world. Criminals have exploited the ability to communicate instantaneously around the globe to facilitate cross-jurisdictional cyber-fraud and subsequently, online money laundering. Coordinating international fraud and money laundering schemes requires a medium of communication, such as online hacking and carding forums, where offenders meet to exchange information and to engage in their illegal business. For the study presented in this paper, publicly available online carding and hacking forums were downloaded and keywords of interest pertaining to online money laundering were extracted. This study undertakes an analysis of two large Russian-speaking hacking and carding forums by qualitatively analyzing and quantifying contexts of keyword usage. Findings indicate that cyber-fraudsters are primarily interested in cashing out digitally stolen funds and do so mainly by resorting to the services of money mules and virtual casinos.**

Keywords—hacking; carding; online forum; money laundering; virtual casino; money mule

I. Introduction

The ability to communicate instantaneously with vast numbers of other people located throughout the world has revolutionized our lives. However, the internet has also created new venues of victimization and exploitation of law-abiding internet users [1]. Security and intelligence agencies in the UK, the USA and Australia consider cybercrime one of the most critical threats today, putting it on the same level as global terrorism [2, 3, 4, 5]. The FBI also noted that cybercriminals are often linked with "offline" criminal activity, including traditional organized crime groups that hire hackers to enable global reach of their operations [4]. While ties may exist between "offline" organized crime and cybercriminals, this paper focuses on criminals who are organized but do not necessarily have the same structure as the traditional organized crime [6].

There is debate over whether cybercrime is organized crime in the traditional sense or merely an assortment of lone criminals who organize themselves as needed within the virtual environment [5, 6, 7]. As cybercriminal communities matured and the cybercrime market evolved, profit became the new motivator for cybercriminals, replacing mischief and the "pride of one-upmanship". Today organized cybercriminals appear to be primarily financially motivated and are thought to be responsible for the majority of cybercrimes [4, 7, 8]. Other authors have pointed to the lack of empirical data on whether the cybercrime market is indeed dominated by criminal organizations [4, 6, 7, 9]. Estimates of economic impacts of cybercrime vary between dozens of billions and up to $1 trillion globally, however as with any underground economy it is difficult to gauge the actual size and scale of cybercriminal enterprises [4, 10].

As with legitimate multinational companies, organized criminals consider international jurisdiction when deciding on where and how to do business. Developing economies with insufficient regulation serve to attract cybercriminal enterprises and act as a source of criminal transactions, as the police or the judiciary systems are not prepared to investigate and prosecute cybercrimes. Eastern Europe, and specifically Russia, are often mentioned in the literature in connection with organized crime and cybercrime alike [4, 5, 6, 7, 8, 9]. Russian-speaking cybercrime markets may make up to a third of the global market [10].The anonymity, speed and global reach of transactions afforded by online payments are utilized by criminals to a great advantage. Transmitting ill-gotten gains electronically is cheaper, while impersonal online accounts can hardly be controlled using know-your-customer techniques [1, 11, 12]. The purpose of this paper is to explore the abilities available to online criminals, and how online money laundering is perpetrated. This is done by first examining the current state of research in this area (Chapter II), then we outline how we collected discussions from online hacking forums (Chapter III) and analyzed it to gain insight into the money laundering process (Chapter IV). We then discuss our findings (Chapter V) and conclude the paper (Chapter VI).

II. Literature Review

Soudijn and Zegers conceptualized cyberspace as a virtual offender convergence setting where Internet is a place for socializing and exchanging information [13]. Online forums serve two functions: facilitating the exchange of information and acting as a marketplace [12, 13, 14, 15, 16, 17]. Holt analyzed online criminal forums that doubled as marketplaces for stolen data using a number of methods, such as qualitative analysis of the forum content to discern social organization of the market and an analysis of social and economic forces which shape such markets [14, 15]. Yip, Webber and Shadbolt investigated the role of trust within cybercrime markets and the social structure of carding/hacking forums [2].

Holt and Lampke considered what tools and resources are sold on cybercrime markets and how market forces influence relationships between market actors [18]. Holt et al. also analyzed the types of goods and services which are offered on

978-1-5090-2857-3/16 $31.00 © 2016 IEEE
DOI 10.1109/EISIC.2016.19

IEEE computer society

cybercrime markets and explored how trust and regulation mechanisms are implemented by market actors [16]. Motoyama et al. studied structural characteristics of 6 hacker forums and social dynamics of user interactions [17]. Several studies have taken a language-specific perspective before, as Russian-speaking offenders have consistently been implicated in cybercrime [14, 15, 16]. Motoyama et. al also sampled German-speaking hacking forums [17]. However, online communities that can be accessed from anywhere in the world have the potential to have widely varying "user bases", and according to Holt, Russian language online social networks dedicated to trading stolen credentials remain understudied [15]. This study is intended to contribute to a deeper understanding of language-specific differences that arise in online cybercrime markets.

III. Methods

A. Data Collection and Forum Selection

The data in the sample was obtained through software called the Open Discussion Forum Crawler (ODFC). For full details, see [19]. This study focuses on two exclusively Russian-speaking hacking and carding forums, which will be referred to as *Forum AC* and *Forum DM.* They were located through searches using a Russian-language search engine Yandex by entering queries such as "buy dumps CC" [7, 8]. Based on the subforum names, Forum AC hosts discussions on topics such as programming, exploits, and affiliate programs. An overview of Forum DM reveals topics such as digital currencies, money laundering, and illegal business. At the time Forum AC contained 1,530,404 posts and Forum DM contained 468,827 posts. As both forums were public, and the analysis was not focused on identifying the individual users but rather studying the larger community, no ethical concerns are created by accessing and analyzing them. However, to preserve the privacy of individual users, members are referred to as "user1", "user2", etc.

B. Search Queries and Quantitative Analysis

Keywords to be used as a search query were obtained by using OpenNLP functionality embedded within ODFC to produce a list of keywords of interest, for instance, "ATM", "account" and "bitcoin". OpenNLP allows for the extraction of the various types of words, nouns and verbs for example. For a detailed description of the process, see [19]. Since OpenNLP works in English, we analyzed some previously collected data for keywords in English, selecting a list of 21 keywords. These keywords were translated into Russian and where exact translation was impossible a close equivalent was used. Of the posts that contained the keywords, a convenience sample of 20 posts per keyword used, producing 420 posts per forum or 840 posts in total. Posts that could be described by multiple keywords were counted multiple times – once per keyword.

C. Relevance Criteria

When sampling a forum it is important to consider how the range of topics discussed may influence accuracy and relevance of the sample. For instance, Holt noted that 13% of the data in the sample was related to legitimate or "gray market" jobs in areas such as programming and web design which would not be relevant for this study [14]. The relevance criteria allow for the screening of posts in order to determine the most pertinent content. Three relevance criteria are established: 1) the post must contain a keyword; 2) the keyword is mentioned in the context of illegal activity; 3) "illegal activity" refers to a particular service, actor, method, tool, scheme or a business model that is connected to online money laundering. Posts which contained non-specific references to money laundering but did not describe illegal activity on part of forum members or their associates were considered irrelevant. These posts were primarily news and off-topic discussions.

IV. Analysis

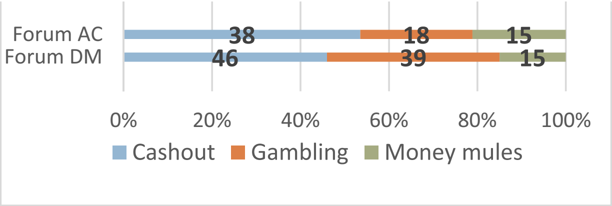

Figure 1. Relevant posts on Forum AC and Forum DM.

Out of a sample population of 420 posts on Forum AC, only 68 posts (16.1%, N=420) were found to be relevant. Among the 20 instances of search results per keyword the amount of relevant posts varied between 0 and 9 for both forums, with 3.2 relevant posts on average for Forum AC and 4.6 relevant posts on average for Forum DM per page of search results. Three broad categories of posts were identified – cashout, gambling, and money mules. A post belonging to more than one category was counted multiple times. Several minor categories such as scams, account sales, and carding were not consistent enough across forums to warrant a category of their own.

A. Cashout

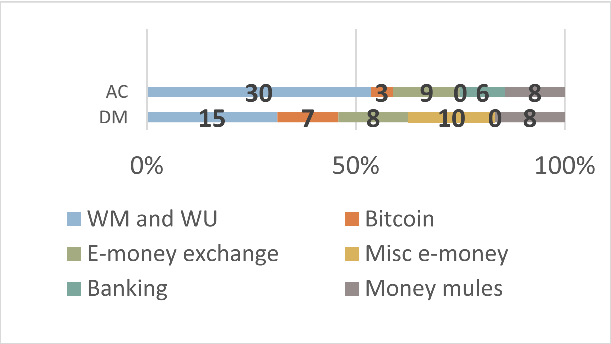

Figure 2. Prevalence of cashout discussions broken down by payment type. "WM and WU" refers to WebMoney and Western Union.

> "*More or less advanced guys register ATM [cards]+personal certificates in the necessary amounts and, being mindful of the limits, cash out 100k rubles per month from each card*" – user1

Cashout was a prominent topic on both Forum AC (38 posts, or 55.8% of all relevant posts, n=68), and Forum DM (46 posts, or 46.9%, n=98). Cybercriminals are interested in cashing out the stolen funds in order to integrate them within the financial system under their own name. Digital currencies that are being traded illegally are pre-laundered due to the fact they are processed by legitimate financial institutions [1]. Cashout services are typically offered on cybercrime markets, including by users who advertised their services as money mules [14, 15, 16, 18].

Converting digital currency into various forms of money by using online exchange services provides an advantage during the layering stage [1, 20]. However, several users have noted that due to cooperation and transparency practices of exchangers, proceeds of crime which were processed through exchange services remain "dirty" money. Exchanging currencies with cashing out as the end goal involved Western Union in 4 (5.8%, n=68) posts, WebMoney in 4 (5.8%) posts and Bitcoin in 1 (1.4%) post. The use of money mules is essential for cybercriminals, as money mules are recruited to withdraw the stolen money and transfer it back to the offender [13]. A minority of users also discussed using bank accounts registered to credentials of money mules to cash out the stolen money in 6 (8.8%) posts.

B. *Gambling*

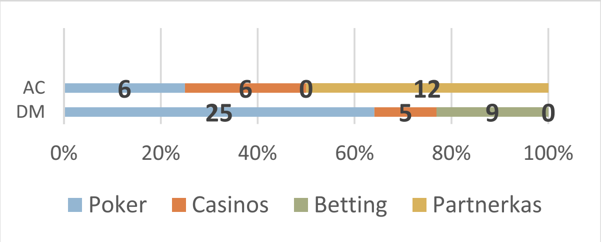

Figure 3. Prevalence of gambling mentions.

> "*An affiliate program from the 'Ramzes' casino – daily payments within 5 minutes. Almost all online casinos pay within 48 hours, however we will return your winnings in just 5 minutes.*" – user2

The second largest category of services and avenues for money laundering within the sample was connected to gambling in 18 (26.4%, n=68) posts on Forum AC and 39 (39.7%, n=98) posts on Forum DM. Forum AC users primarily discussed affiliate programs (or "partnerkas") for gambling, also mentioning gambling in the context of cashing out illicit funds but without referring specifically to the service they used. Online gambling is the perfect opportunity for money laundering. Lilley conducted an internet search and found 45,000 results pertaining to "virtual casino" in 2002 [21]. Today the exact same search produces 14,200,000 results. It is difficult to know how many virtual casinos exist and how much money exactly flows through them [21]. Online casino revenue was estimated to be $6 billion in 2002, and in 2016 it is expected to exceed $45 billion [21, 22].

Poker accounts were primarily used for cashing out the laundered money on Forum DM in 25 (25.5%, n=98) posts, while this method was less common on Forum AC in only 6 (8.8%, n=68) posts. Betting and bookmaking firms, such as William Hill, were not used within the Forum AC sample at all (0.0%, n=68), while it was the second preferred method of cashout on Forum DM in 9 (9.1%, n=98) posts. Gambling affiliate programs also went unused on Forum DM (0.0%, n=98), while they were the most common method on Forum AC in 12 (17.6%, n=68) posts.

C. *Money mules*

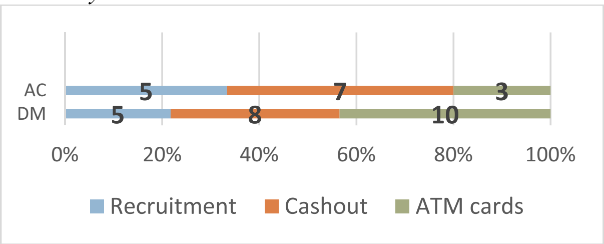

Figure 4. Prevalence of money mule discussions.

> "*Find a school kid or a college student on the street, promise him 100, 200 rubles for receiving a transfer for you. Send a SMS with the kid's name, he gets the transfer and gives it to you*" – user3

The post above serves as an illustrative example of how money mules are recruited and exploited by offenders. Soudijn and Zegers described a case where a classified ad in the Netherlands recruited people to wire sums of money to recipients in Russia, allowing the mules to keep 5% for themselves [13]. The prospect of easy money serves as a powerful lure for potential unwitting drops whose credentials criminals use to break the audit trail of the illicit funds. "100, 200 rubles" mentioned by *user3* would amount to approximately $3 and $6 (USD) at the time the post was made, what highlights the ease with which Russian-speaking fraudsters are able to recruit money mules without incurring significant losses themselves. Two other forum users suggested hiring homeless people and drug addicts as money mules. From a prevention and enforcement perspective, it poses a significant challenge because unwitting money mules are recruited precisely due to their lack of knowledge of the financial system or lack of concern about the source of the funds. Based on characteristics identified by forum users who offered advice on drop recruitment, schoolchildren, poor university students, drug addicts, homeless people and the elderly are some of the social groups that are ideal for money mule recruitment targeting.

V. Discussion

Cyber-fraudsters rely on e-money services to transfer and cash out their illicit funds. This is frequently accomplished by using online gambling outlets and/or money mules to serve as a layer of anonymity between the illicit funds' origin and the destination, i.e. the offender. Tropina noted no proof existed of online gambling outlets being connected to money laundering [1]. From the user quotes and analysis provided, it is a fair conclusion that online gambling is in fact being used by cyber-fraudsters to launder illicit funds. This study points to a need for further research on involvement of virtual casinos in online money laundering schemes.

Only a small fraction of posts were analyzed compared to the amount of total forum posts. For Forum AC, the study population (N=420) represented 1.2% of the 34,780 posts which contained the keywords used for sampling. For Forum DM, the study population (N=420) comprised 0.26% of the 158,348 posts with the keywords of interest. As a result, findings in this study are probably not representative. External validity of the results is also low owing to the fact only 2 forums were sampled, as well as the fact forum users likely reside within ex-USSR countries with similar legislation. Due to implementation of the relevance criteria, posts which did not specifically discuss elements of online money laundering were omitted from consideration.

VI. Conclusion

This study explored two large Russian-speaking carding and hacking forums in an attempt to reveal the means by which cyber-fraudsters perpetrate online money laundering. Using the Open Discussion Forum Crawler, forum content was downloaded and analyzed to locate relevant posts which discussed services, actors, methods, tools, schemes or business models implicated in online money laundering. Forum AC and Forum DM were similar in the range of topics discussed and their relative frequency of mentions. Cashout discussions dominated both forums with gambling/betting taking the second place, followed by money mule discussions. Cashing out electronic currencies was the primary topic of interest within the cashout subsample on both forums. Within the gambling subsample, online poker rooms and virtual casinos were the most frequently seen, along with betting/bookmaking and gambling affiliate programs.

Cashing and transferring money was primarily accomplished through WebMoney and Western Union on both forums, as well as Bitcoin, although the use of the cryptocurrency was relatively rare. As described in previous research on the topic of carding forums, money mules represent an essential element in online money laundering schemes. With respect to money mule recruitment, some authors provided anecdotal examples of methods used by cyber-fraudsters to recruit unwitting drops, however the exact recruitment target audience and methods were not discussed. The current study revealed that fraudsters were willing to exploit vulnerable social groups, such as the poor and the drug addicted, in order to further their money laundering objectives. Forum users also described schemes which involved using gambling/betting services to launder money. Betting and bookmaking firms, such as William Hill, as well as online poker rooms represented some of the services which offenders used to legitimize the proceeds of crime.

References

1) Tropina, T. (2014). Fighting money laundering in the age of online banking, virtual currencies and internet gambling. ERA Forum, 15(1), 69-84.

2) Yip, M., Webber, C., & Shadbolt, N. (2013). Trust among cybercriminals? Carding forums, uncertainty and implications for policing. Policing & Society, 23(4), 516-539. doi:10.1080/10439463.2013.780227

3) Wall, D. S., & Williams, M. L. (2013). Policing cybercrime: networked and social media technologies and the challenges for policing. Policing & Society, 23(4), 409-412. doi:10.1080/10439463.2013.780222

4) Kshetri, N. (2010). The global cybercrime industry: economic, institutional and strategic perspectives. London: Springer. Retrieved from http://troy.lib.sfu.ca/record=b5646829~S1a

5) Choo, K. (2008). Organised crime groups in cyberspace: a typology. Trends In Organized Crime, 11(3), 270-295. doi:10.1007/s12117-008-9038-9

6) Lusthaus, J. (2013). How organised is organised cybercrime?. Global Crime, 14(1), 52-60. doi:10.1080/17440572.2012.759508

7) McCusker, R. (2007). Transnational organised cyber crime: distinguishing threat from reality. Crime, Law & Social Change, 46(4/5), 257-273. doi:10.1007/s10611-007-9059-3

8) Hutchings, A. (2014). Crime from the keyboard: organised cybercrime, co-offending, initiation and knowledge transmission. Crime, Law & Social Change, 62(1), 1-20. doi:10.1007/s10611-014-9520-z

9) Broadhurst, R., Grabosky, P., Alazab, M., & Chon, S. (2014). Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime. International Journal Of Cyber Criminology, 8(1), 1-20.

10) Kuzmin, A. (2012). State and trends of Russian cybercrime in 2011. ICUMT. Retrieved from http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6459794

11) Levi, M., & Reuter, P. (2006). Money Laundering. Crime and Justice, 34(1), 289–375. http://doi.org/10.1086/501508

12) Filipkowski, W. (2008). Cyber Laundering: An Analysis of Typology and Techniques. International Journal Of Criminal Justice Sciences, 3(1), 15-27.

13) Soudijn, M., & Zegers, B. (2012). Cybercrime and virtual offender convergence settings. Trends In Organized Crime, 15(2/3), 111-129. doi:10.1007/s12117-012-9159-z

14) Holt, T. J. (2013). Examining the Forces Shaping Cybercrime Markets Online. Social Science Computer Review, 31(2), 165-177. doi: 10.1177/0894439312452998

15) Holt, T. J. (2013). Exploring the social organisation and structure of stolen data markets. Global Crime, 14(2/3), 155-174. doi:10.1080/17440572.2013.787925

16) Holt, T. J., Smirnova, O., Chua, Y. T., & Copes, H. (2015). Examining the risk reduction strategies of actors in online criminal markets. Global Crime, 16(2), 81-103. doi:10.1080/17440572.2015.1013211

17) Motoyama, M., McCoy, D., Levchenko, K., Savage, S. & Voelker, G. M. (2011). An Analysis of Underground Forums. Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference, 71-80. doi:10.1145/2068816.2068824

18) Holt, T. J., & Lampke, E. (2010). Exploring stolen data markets online: products and market forces. Criminal Justice Studies, 23(1), 33-50. doi:10.1080/14786011003634415

19) Macdonald, M., Frank, R., Mei, J., & Monk, B. (2015). Identifying Digital Threats in a Hacker Web Forum. Proceedings of the 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2015, 926-933, doi:10.1145/2808797.2808878

20) Financial Action Task Force (2010). Money Laundering Using New Payment Methods. Retrieved from http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf

21) Lilley, P. (2003). Dirty dealing: the untold truth about global money laundering, international crime and terrorism. London: Kogan Page Limited.

22) Statista (2016). Size of the online gambling market from 2009 to 2018 (in billion U.S. dollars). Retrieved from http://www.statista.com/statistics/270728/market-volume-of-online-gaming-worldwide/