The Digital Underground Economy: A Social Network Approach to Understanding Cybercrime

Michael Yip[1], Nigel Shadbolt[1], Thanassis Tiropanis[1], Craig Webber[2]
[1]Web Science Doctoral Training Centre
School of Electronics and Computer Science
University of Southampton
Southampton SO17 1BJ
{my2e09, nrs, tt2}@ecs.soton.ac.uk

[2]Web Science Doctoral Training Centre
School of Social Sciences
University of Southampton
Southampton SO17 1BJ
c.webber@soton.ac.uk

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
Emphasized in both the National Security Strategy [11] and the Cyber Security Strategy [3], cybercrime is now a Tier-One national threat to the United Kingdom, a threat which must be addressed as our lives become ever more embedded in the digital economy. Recent cybercrime statistics [14, 24] indicate that with hundreds of millions worth of damage, cybercrime remains one of the primary threats facing nations, corporations and ordinary people. The intriguing question then is how has cybercrime managed to evolve into such a persistent problem despite almost a decade of extensive research into cybersecurity?

The problem with the current cybersecurity practice is that it is too often perceived as a technological challenge. Rather, this project argues that cybersecurity should be embraced as a broader socio-technological phenomenon because humans are also central to the problem: they are both to protect *and* to defend against.

By focusing on technology alone, the effects of security become bounded by the pace of technological advance because at every incidence of technological change exists new unforeseen security vulnerabilities, which are new exploitable opportunities for the adversaries. Security practitioners are simply left playing a never-ending cat and mouse chase with their malicious counterparts.

What remains more consistent across time, space and domain but too often neglected is the people committing the crimes: their motivations and attitudes, their behaviour and also, the environments within which allow them to thrive [30]. By studying these, security practitioners can better assess the risks they face, anticipate rather than reacting to attacks and addressing the problem with the right tools. This is what this project aims to offer. More precisely, this project examines one of the most profound transformations of crime brought about by the Internet [1, 8, 22, 23, 31]: online criminal networking. The primary focus of this project is on profit driven cybercrime also know as carding[1]. The perpetrators are known as the carders [22].

In collaboration with the Serious Organised Crime Agency (SOCA), this project has been granted access to the archives of several online criminal social networks, better known as carding forums [8, 13, 23, 34]. These forums have previously been operating as online black markets for stolen data but have since been shut down by law enforcement agencies. They are fundamental to the emergence of the global digital underground economy we are witnessing today. Therefore, this project is presented with a unique opportunity of taking an inside look into the lives of the cybercriminals.

By using an interdisciplinary approach involving network science [7] and criminology, this project aims to tackle some overdue unanswered questions regarding the profit driven cybercriminals including: why and how they entered the trade, what are the patterns in their behaviour and how do they manage the threats from dishonest traders and law enforcement in an anonymous environment? We believe that gaining such insights will help security practitioners to better understand and anticipate cybercriminal activities.

2. DIGITAL UNDERGROUND ECONOMY
As argued by Wall [31], the empowering of an individual is one of the most profound transformations of crime brought about by the Internet. Furthermore, he argues that the cybercriminals are "lone offenders who exploit networked technology to carry out incredibly complex and far-reaching tasks that can be repeated countless times globally". Brenner [1] labels these empowered individuals, "cyber-entrepreneurs".

With the attraction of big money, more and more cybercriminals are entering the trade. However, since a wide range of skills is needed to become successful in this dark venture [21, 22, 28], the cybercriminals began collaborating with one another, trading goods and services that contributes to the crime [28] and some even venture as far as recruiting talents from universities [17]. As

[1] Carding: refers to the illicit use of third party credit card. The perpetrators are called carders.

Digital Futures '12, October 23 – 25, 2012, Aberdeen, UK.

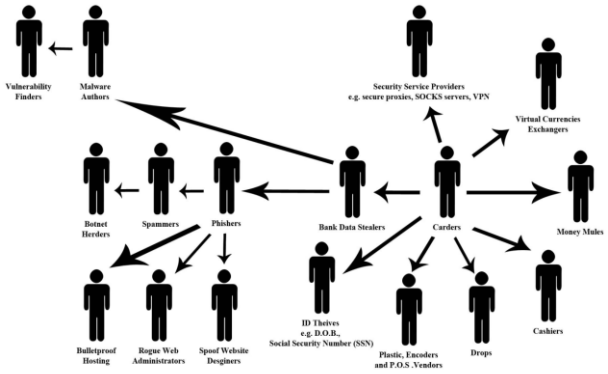

Figure 1. The Digital Underground Economy.

Moore et al [20] note, "[j]ust as in Adam Smith's pin factory, specialization has led to impressive productivity gains, even though the subject is now bank card PINs rather than metal ones". Therefore, a digital underground economy has gradually emerged over the last decade, as shown in figure 1.

To facilitate their need for networking, many criminal social networks [8, 13, 23, 28, 34] have been set up over the Internet, allowing the cybercriminals to network with one another from across the world, share techniques and values of crime, trade goods and services as well as forming collaborations. The Internet Relay Chat (IRC)[2] is one of the popular virtual venues for hackers and carders to network but as identified by Thomas and Martin [28] as well as Herley and Florencio [10], the dishonest traders or "rippers" are too prevalent on this open platform for serious criminal exchanges to occur. The more serious cybercriminals in fact reside within a much more tightly managed type of social networks known as carding forums, which are conventional online discussion forums used for the purpose of carding [13, 34]

It is argued in this project that it is this extensive networking that has given cybercriminals the ability to exploit opportunities which would not have been possible before [20, 26, 31] and which has turned cybercrime into such a persistent problem. Thus the aim of this project is to provide cybersecurity with a new understanding of the cybercriminals and their social networks by analysing carding forums using an analytical framework called social network analysis (SNA).

3. METHODOLOGY

Since criminal organisations are the aggregations of criminal relationships, it is argued by McIllwain [18] that the study of organised crime should focus on these "human relationships", otherwise known as "criminally exploitable ties" [29]. Such ties form the common denominator among the different manifestations of criminal organisations which in this case are the cybercriminal social networks. Therefore, a tool is needed to comprehensively study the "human relationships" embedded within these carding forums.

Sparrow [27] is one of the first scholars to propose the suitability of Social Network Analysis (SNA) as a tool for criminal investigation. He found that the crime investigators have long been studying criminal networks using simple techniques such as link analysis and he argues that aspects of graph theory such as network structure and centrality are particularly applicable to criminal network investigations. This is supported by Coles [6] who criticised the criminology field for failing to adopt SNA techniques and concepts for criminal network investigations. He believes that several concepts from SNA are particularly relevant to criminal networks: the Small-World problem first empirically demonstrated by Milgram [19], the concept of "weak ties" by Granovetter [9] and the concept of "brokerage" [2]. Chattoe and Hamill [5] critically appraised Coles' proposal by arguing that qualitative SNA must also be applied to allow non-egocentric data to compensate for the incomplete quantitative data. Lastly, Robins [25] highlights the importance of social psychology and he argues that any network analysis which neglects the social psychology of the subject network risks an incomplete analysis. That is, since the subject network is a human social system, both the individual and collective characteristics and behaviour must be studied as they have mutual effects on one another.

Therefore, in this project, an interdisciplinary approach is taken to studying the cybercriminals. Our approach consists of two main components: the use of network science [7] to study the social dynamics [4] of the carding forums and the use of criminology theories to ethnographically examine the cybercriminal subcultures, their motivations and their behaviour.

4. WORK DONE SO FAR AND FUTURE WORK

Through the use of network science, we have so far modelled the social interactions on the carding forums as network graphs [35]. We find that the social networks exhibit small world properties [32] and this empirically proves that carding forums enable cybercriminals to find each other more easily. Furthermore, we find that the social networks exhibit a non-linear preferential attachment as evident from a lognormal network degree distribution. These findings have important implications on network disruption strategies which are further discussed in [35].

Furthermore, we have undertaken a criminological study of the cybercriminals [33] in which we have revealed some previously unrecognised characteristics as well as removed some stereotypical preconceptions associated with the cybercriminals.

Future work includes examining the evolution of these social networks and to explore how relationships between cybercriminals could be predicted using publicly mineable data from existing carding forums. Also, more detailed ethnographic studies of these carding forums similar to that by Mann and Sutton [16], Jordan and Taylor [15] and Holt [12] will be carried out, drawing on theories from criminology and social psychology.

5. CONCLUSION

In this paper, we have argued that cybersecurity must be embraced as a socio-technological challenge and that new insights can be found by studying the cybercriminals: their motivations and attitudes, their behaviour and the environments within which allow them to thrive. In collaboration with the Serious Organised Crime Agency (SOCA), this project has been presented with a unique opportunity to take an inside look into their lives and their social networks. Using an interdisciplinary framework called Social Network Analysis (SNA) and drawing on theories from network science and criminology, this project aims to offer a comprehensive examination of the cybercriminals and their social networks. The findings from this project will allow security

[2] See: http://en.wikipedia.org/wiki/Internet_Relay_Chat

practitioners to better assess the risks they face and to take a more proactive approach towards protecting their assets.

6. ACKNOWLEDGMENTS

We thank the Serious Organised Crime Agency (SOCA) from the U.K. for their support throughout this project. This research was funded by the Research Councils UK Digital Economy Programme, Web Science Doctoral Training Centre, EP/G036926/1.

7. REFERENCES

[1] Brenner, S.W. 2002. Organized Cybercrime ? How Cyberspace May Affect the Structure of Criminal Relationships. *North Carolina Journal of Law & Technology*. 41, 1984 (2002), 1–50.

[2] Burt, R.S. et al. 1998. Personality correlates of structural holes. *Social Networks*. 20, 1 (Jan. 1998), 63–87.

[3] Cabinet Office U.K., 2011. *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World.*

[4] Carley, K. 2006. Destabilization of covert networks. *Computational & Mathematical Organization Theory*. 12, 1 (Apr. 2006), 51–66.

[5] Chattoe, E. and Hamill, H. 2005. It's Not Who You Know--It's What You Know About People You Don't Know That Counts: Extending the Analysis of Crime Groups as Social Networks. *British Journal of Criminology*. 45, 6 (Feb. 2005), 860–876.

[6] Coles, N. 2001. It's Not What You Know--It's Who You Know That Counts. Analysing Serious Crime Groups as Social Networks. *British Journal of Criminology*. 41, 4 (Sep. 2001), 580–594.

[7] Easley, D. and Kleinberg, J. 2010. *Networks, Crowds and Markets: Reasoning about a Highly Connected World*. Cambridge University Press.

[8] Glenny, M. 2011. *Darkmarket: Cyberthieves, Cybercops and You*. The Bodley Head.

[9] Granovetter, M. 1973. The Strength of Weak Ties. *The American Journal of Sociology*. 78, (1973), 1360–1380.

[10] Herley, C. and Florêncio, D. 2010. Nobody Sells Gold for the Price of Silver: Dishonesty, Uncertainty and the Underground Economy. *Economics of Information Security and Privacy*. (2010), 33–53.

[11] HM Goverment 2010. *The National Security Strategy*.

[12] Holt, T.J. 2007. subcultural evolution? examining the influence of on- and off-line experiences on deviant subcultures. *Deviant Behavior*. 28, 2 (Feb. 2007), 171–198.

[13] Holt, T.J. and Lampke, E. 2010. Exploring stolen data markets online: products and market forces. *Criminal Justice Studies*. 23, 1 (Mar. 2010), 33–50.

[14] IC3 2012. IC3 2011 Internet Crime Report. (2012).

[15] Jordan, T. and Taylor, P. 1998. A sociology of hackers. *The Sociological Review*. 46, 4 (1998), 757–780.

[16] Mann, D. and Sutton, M. 1998. >>NETCRIME: More Change in the Organization of Thieving. *British Journal of Criminology*. 38, 2 (1998), 201–229.

[17] McAfee Virtual Criminology Report: 2006. *http://www.sigma.com.pl/pliki/albums/userpics/10007/Virtual_Criminology_Report_2006.pdf*. Accessed: 2011-01-31.

[18] McIllwain, J.S. 1999. Organized crime: A social network approach. *Crime, Law and Social Change*. 32, 4 (1999), 301–323.

[19] Milgram, S. 1967. The Small-World Problem. *Psychology Today*. 1, 1 (1967), 60–67.

[20] Moore, T. et al. 2009. The Economics of Online Crime. *Journal of Economic Perspectives*.

[21] Panda Security 2011. *The Cyber Crime Black Market*.

[22] Peretti, K.K. 2008. Data Breaches: What the underground world of "carding" reveals. *Santa Clara Computer and High Technology Journal*. 25, (2008), 375–414.

[23] Poulsen, K. 2011. *Kingpin: How one hacker took over the billion-dollar cybercrime underground*. Crown Publishing.

[24] PwC 2012. UK Information Security Breaches Survey - Technical report. (2012).

[25] 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 (Nov. 2008), 166–187.

[26] Sandywell, B. 2010. On the globalisation of crime: the Internet and new criminality. *Handbook of Internet Crime*. Y. Jewkes and M. Yar, eds. Willan Publishing. 38–66.

[27] Sparrow, M. 1991. The application of network analysis to criminal intelligence: An assessment of the prospects. *Social Networks*. 13, 3 (Sep. 1991), 251–274.

[28] Thomas, R. and Martin, J. 2006. the underground economy : priceless. *The USENIX Magazine*. 31, 6 (2006), 7–16.

[29] von Lampe, K. 2003. Criminally Exploitable Ties: A Network Approach to Organized Crime. *Transnational Organized Crime: Myth, Power, and Profit*. Carolina Academic Press. 9–22.

[30] von Lampe, K. 2005. Making the second step before the first: Assessing organized crime. *Crime, Law and Social Change*. 42, 4 (2005), 227–259.

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

[32] Watts, D.J. and Strogatz, S.H. 1998. Collective dynamics of "small-world" networks. *Nature*. 393, 6684 (Jun. 1998), 440–442.

[33] Webber, C. and Yip, M. 2012. Drifting on and off-line: humanising the cyber criminal. *Future Directions in Crime and Deviancy: Proceedings of the York Deviancy Conference*. Routledge.

[34] Yip, M. 2011. An Investigation into Chinese Cybercrime and the Applicability of Social Network Analysis. *ACM Web Science Conference 2011, 14-17 June 2011, Koblenz, Germany*. (2011).

[35] Yip, M. et al. 2012. Structural analysis of online criminal social networks. *IEEE International Conference on Intelligence and Security Informatics (ISI) 2012* (Apr. 2012), 60–65.