Copyright © 2015 International Journal of Cyber Criminology (IJCC) – Publisher & Editor-in-Chief – K. Jaishankar ISSN: 0973-5089
July – December 2015. Vol. 9 (2): 173–184. DOI: 10.5281/zenodo.56210

This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited. This license does not permit commercial exploitation or the creation of derivative works without specific permission.

Cyber Criminal Networks and Money Mules: An Analysis of Low-Tech and High-Tech Fraud Attacks in the Netherlands

Rutger Leukfeldt[1]
The Netherlands Institute for the Study of Crime and Law Enforcement (NSCR)

Jurjen Jansen[2]
NHL University of Applied Sciences, The Netherlands

Abstract
This paper is about the money mules used by cyber criminals. Although money mules are not part of the core group of criminal networks, they play an important role within these networks. They are used to interrupt the trail to criminal networks. However, to date only a few cyber crime studies have focused on money mules. Based on case studies about cyber criminal groups, we expected differences between money mules used by low-tech as opposed to high-tech groups. We analyzed data from a fraud registration database of a Dutch bank to gain in-sight into the characteristics of money mules and how cyber criminal networks use them. Our analyses clearly show that there are indeed significant differences. Furthermore, the characteristics of money mules indicate what kind of criminal network is behind the attack. The results of our study can be used by law enforcement agencies to develop targeted investigation and prosecution strategies.

Keywords: Money Mules, Phishing, Malware, Cyber crime, Organized Crime.

Introduction
Money mules can be seen as a crucial part of the criminal network. They are of great importance for the core members of these networks because money mules are used to interrupt the trail that may lead law enforcement agencies to the top of the network. Money mules, for example, register bank accounts or businesses under their names, which are actually exploited by the criminal network.

Several studies acknowledge the important role of money mules in the diversion of money stolen by cyber criminals who are engaged in financial cyber crimes, such as carding[3] or phishing[4] attacks (Choo, 2008; Moore & Clayton, 2009; McCombie, 2011;

[1] Postdoc researcher, The Netherlands Institute for the Study of Crime and Law Enforcement (NSCR), De Boelelaan 1077a (entrance Buitenveldertselaan), 1081 HV Amsterdam, The Netherlands. Email: rleukfeldt@nscr.nl
[2] PhD Candidate, NHL University of Applied Sciences, Rengerslaan 10, P.O. Box 1080, 8900 CB Leeuwarden, The Netherlands. E-mail: j.jansen@nhl.nl
[3] Carding involves the fraudulent use of personal data taken from bank cards and credit cards (Peretti, 2008).

© 2015 International Journal of Cyber Criminology. All rights reserved. Under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) License

Aston et al., 2009; Soudijn & Zegers, 2012; Leukfeldt, 2014; Leukfeldt et al., 2016b, 2016c). Most of these studies, however, concentrate primarily on the core group of the criminal networks and only focus indirectly on money mules. Empirical studies into characteristics of internet money mules are lacking. Only Aston et al. and McCombie carried out some exploratory analyses of money mules used in Australian phishing attacks.

In order to fill this knowledge gap, this paper focuses on money mules who are used by cyber criminal groups that carry out attacks on financial institutions. To gain insight into this group of criminals, which we believe plays a vital role in the crime process; we analyzed unique data from a fraud registration system of a major Dutch bank. We obtained 600 fraud incidents from the period 2011-2013. Based on these data, this paper provides insight into the characteristics of money mules and the way in which this group is used by criminal networks to transfer money from victim bank accounts. More specifically, we present background characteristics, the socioeconomic status of money mules, and the value and number of transactions to money mules.

Review of Literature

The present study advances the work of Leukfeldt et al. (2016a, 2016b, 2016c). These studies provide insight into the composition, origin and growth, and criminal capabilities of criminal networks carrying out financial cyber crimes. Forty cyber criminal networks were analyzed in the Netherlands, Germany, UK and the US. The Dutch cases provided the authors with information about cyber criminal networks and their members largely as a result of investigative methods such as wiretaps, IP taps, observations, undercover policing and house searches. The authors reviewed the financial cyber crime cases systematically using an analytical framework. In the other three countries, the authors relied on interviews with case officers and public prosecutors involved in the criminal investigations against cyber criminal networks since no police files were available to them. This section briefly describes the main results of these three studies.

Criminal Capabilities

All networks that were analyzed by Leukfeldt et al. are involved in attacks on online banking. The crime scripts of the Dutch networks have many similarities. Step one is obtaining login credentials from victims. Cyber criminals use phishing e-mails, phishing websites and malware to intercept these credentials. However, in order to transfer money from the account of the victims, so-called 'one-time transaction authentication codes' are needed. Hence, step two is obtaining these codes. Various methods are used to obtain these codes. In some cases, the criminals posed as bank employees and made telephone calls to the victims. In other cases, malware adapted the transaction that victims made without them knowing or being able to see it. Step three is related to the topic of the present study, i.e., transferring money to money mule accounts. Money from victims' accounts is not transferred to the accounts of core members directly. Rather, in order to

[4] Phishing is the process that criminals use to find out users' personal information by posing as a trusted authority and using digital means such as e-mail (see, e.g., Lastdrager (2014) who analysed 113 definitions of phishing).

© 2015 International Journal of Cyber Criminology. All rights reserved. Under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) License

obscure the trail to the core members, money mule bank accounts are used.[5] Once money is transferred to the money mule account, the money is taken out in cash as fast as possible and via various links given to the core members.[6]

The networks from Germany, the UK and US predominantly have the same crime scripts as described above. However, there are some exceptions. Some networks, for example, attack financial institutions directly (by installing malware on their systems or by hacking databases with customer credentials), rather than the individual customer. There are also networks that buy user credentials on forums and do not need to take the first two steps of the crime script described above.

Differences regarding the crime scripts can be boiled down to the degree of technology used by the criminal networks. There are low-tech networks, keeping the use of Information Technology to a minimum. These networks use phishing e-mails and phishing websites to get login credentials. After that, criminals posing as bank employees phone the victims in order to obtain one-time security codes. On the other hand, there are high-tech networks using malware that requires no direct interaction with the victim. In one case, for example, the criminals infected a number of websites with outdated security. Once a user visited on of these websites, his or her computer became infected with malware automatically. Now the criminals have control over the victim's computer and are able to (manually or automatically) adjust or change online banking sessions.

Furthermore, the authors found that the criminal activities of the networks are not always restricted to financial cyber crimes. In more than half of the cases, members of the networks also perform other criminal activities. Although these secondary criminal activities often relate to financial crimes, other activities like human trafficking or drug trafficking were also observed.

The Structure of Networks

Within all Dutch cyber criminal networks, four hierarchical positions can be identified: core members, professional enablers, recruited enablers and money mules. Core members are those who initiate and coordinate the attacks; they are a rather fixed group and direct and manage the other members. The other positions in the network are more fluid. In the position under the core members, we find members who can provide services to the core members that are necessary to carry out attacks. Leukfeldt et al. identified two kinds of criminal service providers: professional enablers and recruited enablers. Professional enablers offer services to core members (and other criminals) on their own initiative (e.g. fake identity documents). Recruited enablers provide more straightforward services to core members, and are explicitly encouraged by them to do so (e.g. provide useful intelligence). Money mules can be found at the bottom of the hierarchical structure of the network. This group is used by core members or by enablers to interrupt the financial trail that could lead investigative authorities to the core members.

[5] These money mules were recruited by core members or by recruiters that worked for the core members. Potential mules – often young people – were recruited at schools or sport clubs, or on street corners. Some money mules state that everybody in their neighbourhood knew that you could make money fast by giving your debit card and security code to members of the criminal network.

[6] Although there are some networks experimenting with other ways of cashing their money, for example by buying Bitcoins, all networks in the analysis predominantly used money mules.

© 2015 International Journal of Cyber Criminology. All rights reserved. Under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) License

Unlike the Dutch cyber criminal networks, the structure of the networks analyzed in the other three countries seems more diverse, occasionally lacking core members, enablers or money mules. Sometimes core members execute all parts of the crime script themselves. They simply purchase the required services or information on a forum or through reliable partners. Although they are still dependent on others, they only need a limited number of enablers in order to carry out the crime scripts. An interesting finding from the studies conducted by Leukfeldt et al. is that no exceptional technical knowledge is required by criminals to execute low-tech or high-tech attacks. Their analysis shows that only one person with such expertise, who could be a core member or enabler, is needed to execute these cyber attacks.

Origin and Growth of Networks

In most cyber criminal networks, social ties seem to play an important role in the origin and growth of these networks. A majority of networks have emerged and grown because core members know each other from the (offline) criminal underworld. Both types of enablers and money mules are often recruited through social networks as well. However, forums also play a significant role in some networks, for instance for finding suitable partners in other countries. Furthermore, forums are a means for buying and selling criminal services and information. Numerous networks that are primarily based on social ties use forums to acquire specific knowledge or to buy tools. Moreover, Leukfeldt et al. demonstrate that core members with access to a forum can relatively quickly increase the criminal capabilities of their network compared to core members who do not have access. In sum, social contacts as well as forum access are used to expand criminal networks.

Money Mules used in Low-Tech and High-Tech Fraud Attacks

The analyses presented in Leukfeldt et al. (2016a, 2016b, 2016c) show that there are different types of origin and growth processes and that the criminal capabilities of networks are linked to these processes. These differences are illustrated by the cases studies of Soudijn and Zegers (2012) and Leukfeldt (2014). These case studies describe criminal networks engaged in intercepting login codes and transaction authentication codes of people using online banking systems. The crime script of the groups showed many similarities: the formation of a criminal group, capturing login details from victims, transferring funds to money mules' accounts and cashing money from these accounts to interrupt the digital money trail. There are, however, important differences between the identified groups. The main difference can be reduced to the degree of technology use. The first group carried out high-tech attacks, consisted of members from different countries who used online forums to meet and communicate, carried out attacks in multiple countries and recruited money mules using spam messages. The second group consisted of people living in the Netherlands who carried out low-tech attacks, who had meetings in the streets of Amsterdam, only attacked people within their own country, and recruited money mules through existing social networks in large cities in the Netherlands.

Differences between the networks can be explained based on the social opportunity structure perspective. According to this perspective, criminal networks emerge and grow on the basis of existing social networks and contacts (Kleemans & De Poot, 2008). In order to expand beyond this initial social network, contacts with outsiders have to be

© 2015 International Journal of Cyber Criminology. All rights reserved. Under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) License

made. This explains why some groups continue growing to become international specialists while others do not go beyond operating on a local level (see for example, Kleemans et al., 2002; Van de Bunt & Kleemans, 2007; Kruisbergen et al., 2012). The case studies of Soudijn and Zegers (2012) and Leukfeldt (2014) show that this distinction also holds for cyber criminal networks: low-tech local groups versus high-tech international specialists. Differences between these groups may also be reflected by the type of money mules that are used and the way in which these money mules are used. A group of international specialists that operate entirely online will have to recruit their money mules in a different way than local groups. The group in the Soudijn and Zegers case, for example, recruited unemployed people in another country using emails with job offers while the group in the Leukfeldt case used existing local social networks to recruit youngsters at schools and sports clubs. Because differences in the case studies could be reduced to the degree of technology use, we divide the money mules into two groups: money mules used in low-tech and high-tech attacks. Therefore, this paper provides insight into the characteristics of money mules and the way in which they are used by cyber criminal networks that carry out low-tech attacks and high-tech attacks.

Data and Methods

Data from the fraud registration database of a Dutch bank were used to gain insight in to money mule characteristics and the way in which this group is used by criminal networks to transfer money. This registration system contains information about online banking fraud and attempted fraud.

Attacks in the low-tech category (i.e., phishing) are attacks in which criminals limit their use of technology to sending e-mails and using fake bank websites to steal user credentials. In most of these cases, criminals also made telephone calls to bank customers to obtain these credentials. High-tech attacks (i.e., malware) are attacks in which the device (computer, mobile phone) that victims use to access their online bank accounts is infected with malicious software. Once the device is infected, criminals have control over this device. Criminals can then manipulate online banking sessions in an automated way.

In total, 600 fraud incidents were analyzed. Each incident is a fraud attack on one victim. A bank employee records each attack. The employee might have discovered the fraudulent transaction himself through the bank's fraud detection or via a customer who has noticed strange transfers from his or her account and contacts the bank's fraud desk. The employee then tries to find out what has happened and records his findings in the database. A record contains, for example, information about the way the attack was carried out, damages, accounts to which money is transferred to and relevant documents like victim statements and police reports. Cases were selected using the search field of the fraud database. The key words 'phishing' and 'malware' were used to retrieve the right cases. The researchers ruled out any false positives by manually checking whether or not the case was actually a phishing or malware case.

During April and May of 2014, we had access to a fraud registration database. We had access to all the recorded data from 2011, 2012 and 2013. Each year, hundreds of incidents are registered. Therefore, we opted for a representative sample. Our aim was to analyze 100 low-tech incidents and 100 high-tech incidents per year. Based on the total number of cases per year, a calculation was made to determine which cases should be selected. For example, if year x yielded 900 hits, every 9th case was selected. If the case chosen initially

© 2015 International Journal of Cyber Criminology. All rights reserved. Under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) License

was incorrect, e.g., not an online banking attack, the following case was selected. This also applies to cases that did not include any information.

The database contained information about the type of incident (low-tech or high-tech), characteristics of the transaction (damages, number of money mules, number and amount of transactions to money mules), background characteristics of money mules (gender, age, postal code, nationality), and type of money mule accounts (business or private). The data for each incident were exported to a Microsoft Excel work file. Thereafter, the socioeconomic status of the neighborhood that money mules live in was added. The socioeconomic status could be linked to the postal codes. The socioeconomic status are calculated by The Netherlands Institute for Social Research and are derived from the characteristics of the people who live there, namely the average income, the percentage of people with a low income, the percentage of people with a low level of education and the unemployment rate. The scores reflect the situation in 2010; more recent scores were not available. This resulted in a database with information of 600 fraud incidents. We used SPSS (a software package used for statistical analysis) to find out differences between money mules used in low-tech attacks (i.e., phishing) and high-tech attacks (i.e., malware).

Results

The results are based upon an analysis of 600 fraud incidents in which 1,005 fraudulent transactions were made from victim accounts to 967 money mules. However, information about transactions or background characteristics was not always available. Therefore, the total number of analyzed cases will not always add up to 600.

The following section shows the characteristics of the fraudulent transactions. The subsequent sections describe the characteristics of the money mules. In all instances, low-tech and high-tech attacks are compared with each other.

Characteristics of Transactions

Regarding the characteristics of transactions from victim accounts to money mules, each incident provided information about the total amount cyber criminals wanted to transfer, the number of money mules they used and the value of the transfers to individual money mules. Furthermore, we know whether the money was sent to money mules with a Dutch bank account or to someone outside the Netherlands. Each of these elements shows significant differences between the money mules that are used in low-tech compared to those used in high-tech attacks.

We know how many money mules were used for 579 incidents. In the other cases it was clear that criminals had access to the victims' accounts, but information about money mules was not available. A total of 1,005 transactions were made from victim accounts to the accounts of money mules. There is a significant difference ($p < .01$) between the number of money mules that are used in low-tech compared to high-tech attacks. Table 1 shows that in high-tech attacks usually one straw man is used per victim account. In contrast, low-tech attacks use between 2 and 5 mules per victim account in more than a quarter of attacks. In nearly 9 percent of the attacks 6 or more money mules are used. We even observed incidents in which 16, 17 or 39 money mules were used to plunder a single victim account.

© 2015 International Journal of Cyber Criminology. All rights reserved. Under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) License

Table 1. Number of money mules per type of incident (in %)

Number	Low-tech (n=286)	High-tech (n=293)	Total (n=579)
1	64.3	98.3	81.5
2-5	26.9	1.7	14.2
6+	8.7	0.0	4.3
Total	100.0	100.0	100.0

$p < .01$

More money mules are used per low-tech attack than per high-tech attack. Table 2 shows that the amount of money that criminals try to steal from online accounts of victims is also higher in low-tech attacks than in high-tech attacks ($p < .01$). The amount of money transferred in high-tech attacks more often falls within the lower loss categories: more than a quarter of the total loss per attack is below 1,000 euros and more than 80 percent is below 5,000 euros. Less than 10 percent fall into the category of 10,000 euros or more. In low-tech attacks nearly 30 percent fall into the highest categories. Almost 12 per cent of the attackers stole or tried to steal amounts over 25,000 euros.

Table 2. Amount of Money Transferred from Victim Account (in %)

Amount	Low-tech (n=288)	High-tech (n=291)	Total (n=579)
≤ 1,000	13.5	27.1	20.4
1,001 – 5,000	46.5	54.3	50.4
5,001 – 10,000	11.8	10.7	11.2
10,001 – 25,000	16.3	6.2	11.2
≥ 25,001	11.8	1.7	6.7
Total	100.0	100.0	100.0

$p < .01$

In many cases we could also determine the amount of money transferred to individual money mules. Table 3 provides an overview. There is a significant difference between the amounts transferred to money mules used in low-tech and high-tech attacks ($p < .01$). This is reflected particularly in the number of transactions below 1,000 euros in the high-tech category.

We then examined whether criminals use money mules with private or business accounts. There are significant differences between money mules used in low-tech and high-tech attacks ($p < .01$). Both groups primarily use money mules with private bank accounts. This percentage is highest for low-tech attacks (Table 4).

© 2015 International Journal of Cyber Criminology. All rights reserved. Under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) License

Table 3. Amount of Money Transferred to Individual Money Mules (in %)

Amount	Low-tech (n=556)	High-tech (n=216)	Total (n=772)
≤ 1,000	9.9	32.4	21.2
1,001 – 2,500	37.8	28.7	32.6
2,501 – 5,000	37.9	22.7	27.9
5,001 – 10,000	6.8	9.3	8.3
≥ 10,000	7.6	6.9	9.9
Total	100.0	100.0	100.0

$p < .01$

Table 4. Type of Money Mules Account (in %)

Type of account	Low-tech (n=582)	High-tech (n=176)	Total (n=758)
Private	82.1	61.4	77.3
Business	17.9	38.6	22.7
Total	100.0	100.0	100.0

$p < .01$

Finally, as Table 5 shows, it appears that primarily money mules with a Dutch bank account are used in low-tech attacks (nearly 90 percent), while in the majority of high-tech attacks foreign accounts are used (62.5 percent). These differences are significant. In over a quarter of the high-tech attacks, criminals used Eastern European bank accounts. For both low-tech and high-tech attacks, if foreign accounts are used they are usually limited to European countries.

Table 5: Country of Registration of Money Mules (in %)

Country	Low-tech (n=663)	High-tech (n=296)	Total (n=959)
Netherlands	88.8	37.5	73.0
Northern Europe	0.3	5.4	1.9
Eastern Europe	3.8	26.8	11.0
Southern Europe	2.0	11.4	5.0
Western Europe	1.9	11.4	4.9
Central Europe	1.9	11.4	4.9
India	0.1	1.6	0.6
Total	100.0	100.0	100.0

$p < .01$

© 2015 International Journal of Cyber Criminology. All rights reserved. Under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) License

Money Mule Characteristics

The fraud registration database only provides background information, such as gender, age and postal code, for money mules with Dutch bank accounts. However, background information was not available in all cases and not for all money mules. We know the gender of 336 money mules, and the age and socioeconomic status of 337. We did not find significant differences concerning age and socioeconomic status. Money mules are more likely to be male than female (63.5 percent in the low-tech attacks and 74.4 percent in high-tech attacks), which is similar to ordinary criminals.

There is a significant difference in the age of money mules that are used in low-tech and high-tech attacks ($p < .01$). Table 6 shows, that 56 percent of the money mules in low-tech attacks are part of the lowest two age classes compared to 29 per cent of the money mules used in high-tech attacks. In this latter group, a relatively large number of money mules are between 25 and 34 years old (38 percent).

Table 6. Money Mules per Age Category (in %)

Age	Low-tech (n=295)	High-tech (n=42)	Total (n=337)
≤ 17 years	14.2	2.4	12.8
18-24 years	44.4	26.2	42.1
25-34 years	16.3	38.1	19.0
35-44 years	12.9	16.7	13.4
45-54 years	9.2	4.8	8.6
55-64 years	1.4	9.5	2.4
≥ 65 years	1.7	2.4	1.8
Total	100.0	100.0	100.0

$p < .01$

Discussion and Conclusion

There are significant differences between money mules that are used in low-tech compared to high-tech attacks on online banking. Differences can be observed in the background characteristics of money mules and in the transactions made to money mule accounts. The largest number of significant differences was observed in the characteristics of transactions made from victim accounts to money mules. In low-tech attacks, larger amounts are stolen than in high-tech attacks, more money mules are used per attack and the amount of money transferred to individual money mules is higher. Furthermore, money mules in low-tech attacks are more likely to have a private account and are more likely to have an account with a Dutch bank. Fewer significant differences are found in the background characteristics of money mules. Only the age distribution differs significantly. Money mules who are used in low-tech attacks are more often part of the lowest two age categories (≤ 24 years), while money mules of high-tech groups are more often in the age group of 25-34 years.

We expected differences between money mules of low-tech and high-tech attacks based on research in to cyber criminal networks. Our analyses clearly show that there are indeed significant differences in the characteristics of money mules and the way they are

© 2015 International Journal of Cyber Criminology. All rights reserved. Under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) License

deployed in the different types of attacks. The analyses show, for example, that in the low-tech cases criminals steal larger amounts of money from victims than in the high-tech attacks. One possible explanation is that low-tech attacks are performed manually and high-tech attacks can be automated.[7] In low-tech attacks the attackers have to perform more actions to transfer money from victim accounts. First, criminals have to gain control of online bank accounts. After that, the criminals have to transfer money manually to money mules' accounts. In many cases, the criminals have to call the victims in order to get transaction authentication codes. All things considered, it takes a relatively large effort to gain control over an account. If criminals finally control an account, it pays off to transfer as much money as possible. In high-tech attacks both the initial infection of the device used for online banking and the actual money transfers to money mules can be done in an automated way. In this case, infecting as many machines as possible pays off. Due to a large number of infections, smaller amounts of money can be transferred. Smaller transfers are less likely to be noticed by victims and by the banks' fraud detection systems. Because of the sheer size of the automated attacks, these smaller amounts still add up to large sums of money.

Furthermore, a clear difference can be observed in the type of money mules that are used in the different types of attacks. In low-tech attacks money mules are usually younger and have a private bank account at a Dutch bank. In high-tech attacks there are more money mules with a foreign bank account, there is a relatively large group of money mules in the age category 25 to 34 years old and money mules are more likely to have a business account. This is in line with our expectations based on the social opportunities structures perspective: locally rooted networks that recruit money mules through their social networks versus internationally operating networks that recruit money mules digitally. The characteristics of money mules used in low-tech attacks fits into the picture that Leukfeldt (2014) paints of local cyber criminal networks that persuade young people to give their debit card and PIN number for a small fee through existing social networks such as schools and sport clubs. On the other hand, the characteristics of money mules used in high-tech attacks fits within the image that Soudijn and Zegers (2012) draw of an international network that recruits money mules through spam and job sites. People who apply for a job via the internet will usually not fall into the lowest or highest age categories (because they are too young or too old to work).

Differences between the modus operandi of local and international networks can perhaps also explain the differences in amounts of money that are sent to individual money mules. In low-tech attacks criminals transfer larger amounts of money to money mules than in high-tech attacks. This may be due to the extent to which criminals have control of their money mules. Local low-tech networks that use money mules who are recruited through social networks have relatively tight control over these men and women: they know who they are, by whom they were recruited and which school or sports club they go to. If a money mule makes a run with the money, then it is easier for the criminal network to trace him or her. Money mules that are used by high-tech networks and were recruited by electronic means in another country are more difficult to

[7]See, for example, the case studies of Soudijn and Zegers (2012) and Leukfeldt (2014) in which criminal networks are described that have a similar crime script but execute them differently due to technology use.

© 2015 International Journal of Cyber Criminology. All rights reserved. Under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) License

control. There has been no physical contact between the criminal group and money mules, and the geographical distance is large.

Our analyses confirmed that low-tech networks and high-tech networks not only have different criminal opportunities (e.g. degree of technology use, contacts with facilitators), but also use a different type of money mule and use them in a different way.

Limitations and Directions for Future Research

One limitation of our data is that we only know what type of attack was carried out: low-tech or high tech. We assume that low-tech attacks are only carried out by low-tech networks and high-tech attacks only by high-tech networks. Unfortunately, we do not know this for sure. It is possible that one network carries out both low-tech and high-tech attacks. More research into the type of attacks networks carry out is therefore essential. Our findings, however, are relevant for law enforcement agencies to further develop investigation and prosecution strategies. If victims and money mules are from the same country and relatively large amounts of money are transferred to individual money mules, the chances are high that it is a low-tech attack by a locally rooted network. This requires a different approach by law enforcement agencies than handling an international high-tech attack.

The analyses in this paper are based on data from a Dutch bank. It is a first attempt to gain more insight into money mules that are used by cyber criminal networks. This is important because not much empirical research into this important group of offenders has been done. However, additional research is needed to enrich the current findings. This can be done by doing the same type of analyses with other banks in the Netherlands and in other countries. Perhaps the banks' specific security policies or the investigation and prosecution strategies of law enforcement agencies affect the way money mules are recruited and used.

Further research can also be done using other research methods. Obvious methods are offender interviews and analyzing police investigations. These methods can be used to obtain a more complete picture of the recruitment process. If there is more knowledge about this process, intervention methods can be developed to frustrate the recruitment of this important link in the chain of online banking fraud.

References

Aston, M., McCombie, S., Reardon, B., & Watters, P. (2009). A Preliminary Profiling of Internet Money Mules: An Australian Perspective. Proceedings of the 2009 *Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing, IEEE* Computer Society: 482-487.

Bunt, H. G. Van de., & Kleemans, E. R. (2007). *Georganiseerde criminaliteit in Nederland, derde rapportage op basis van de Monitor Georganiseerde Criminaliteit.* [3rd report on organized crime in the Netherlands] Den Haag: WODC.

Choo, K. K. R. (2008). Organised crime groups in cyberspace: a typology. *Trends in Organised Crime*, *3*(11), 270-295.

Kleemans, E. R., & De Poot, C. J. (2008). Criminal careers in organized crime and social opportunity structure. *European Journal of Criminology, 5*(1) 69-98.

Kleemans, E. R., Berg, Van der, A. E. I. M., & Bunt, Van de, H. G. (1998). *Georganiseerde criminaliteit in Nederland. Rapportage op basis van de WODC monitor.*

© 2015 International Journal of Cyber Criminology. All rights reserved. Under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) License

[Organised crime in the Netherlands. Report based on the WODC monitor] Den Haag: WODC.

Kleemans, E. R., Brienen, M. E. I., & Bunt, Van de, H. G. (2002). *Georganiseerde criminaliteit in Nederland. Tweede rapportage op basis van de WODC-monitor.* [Organised crime in the Netherlands. Second report based on the WODC monitor] Den Haag: WODC.

Kruisbergen, E. W., Bunt, Van de, H. G., & Kleemans, E.R. (2012). *Georganiseerde criminaliteit in Nederland. Vierde rapportage op basis van de Monitor Georganiseerde Criminaliteit.* [Organized crime in the Netherlands, fourth report based on the Monitor Organized Crime], Den Haag: Boom Lemma Uitgevers.

Leukfeldt, E. R. (2014). Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization. *Cyberpsychology, Behavior, and Social Networking*, *17*(8), 551–555.

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2016a). Cyber criminal networks, social ties and online forums: Social ties versus digital ties within phishing and malware networks. *British Journal of Criminology*. DOI:10.1093/bjc/azw009

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2016b). From low-tech locals to high-tech specialists. A typology of phishing networks. *Crime, Law and Social Change*. (in press)

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2016c). Origin, growth and criminal capabilities of cyber criminal networks. An international empirical analysis. *Crime, Law and Social Change*. (in press)

McCombie, S. J. (2011) *Phishing the long line. Transnational cyber crime from Eastern Europe to Australia.* Unpublished PhD Thesis submitted to the Macquarie University.

Moore, T. & Clayton, R. (2007). Examining the impact of website take-down on phishing. *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit*. Pittsburgh, Pennsylvania, ACM: 1-13.

Soudijn, M. R. J., & Zegers, B. C. H. T. (2012). Cyber crime and virtual offender convergence settings. *Trends in Organized Crime*, *15*(2-3) 111-129.

© 2015 International Journal of Cyber Criminology. All rights reserved. Under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) License