A typology of cybercriminal networks: from low-tech all-rounders to high-tech specialists

Leukfeldt, E.R.; Stol, W.PH.; Kleemans, E.R.

published in
Crime, Law and Social Change
2017

DOI (link to publisher)
10.1007/s10611-016-9662-2

document version
Publisher's PDF, also known as Version of record

Crime Law Soc Change (2017) 67:21–37
DOI 10.1007/s10611-016-9662-2

A typology of cybercriminal networks: from low-tech all-rounders to high-tech specialists

E. Rutger Leukfeldt[1,2] · **Edward R. Kleemans**[3] · **Wouter P. Stol**[2]

Published online: 22 November 2016

Abstract Case studies show that there are at least two types of groups involved in phishing: low-tech all-rounders and high-tech specialists. However, empirical criminological research into cybercriminal networks is scarce. This article presents a taxonomy of cybercriminal phishing networks, based on analysis of 18 Dutch police investigations into phishing and banking malware networks. There appears to be greater variety than shown by previous studies. The analyzed networks cannot easily be divided into two sharply defined categories. However, characteristics such as technology use and offender-victim interaction can be used to construct a typology with four overlapping categories: from low-tech attacks with a high degree of direct offender-victim interaction to high-tech attacks without such interaction. Furthermore, clear differences can be distinguished between networks carrying out low-tech attacks and high-tech attacks. Low-tech networks, for example, make no victims in other countries and core members and facilitators generally operate from the same country. High-tech networks, on the contrary, have more international components. Finally, networks with specialists focusing on one type of crime are present in both low-tech and high-tech networks. These specialist networks have more often a local than an international focus.

Keywords Cybercrime · Phishing · Malware · Criminal networks · Theory · Organized crime

✉ E. Rutger Leukfeldt
RLeukfeldt@nscr.nl

[1] Netherlands Institute for the Study of Crime and Law Enforcement (NSCR), De Boelelaan 1077a, 1081 HV, Amsterdam, The Netherlands

[2] Open University of the Netherlands, Valkenburgerweg 177, 6401 DL, Heerlen, The Netherlands

[3] VU University Amsterdam, De Boelelaan 1105, 1081 HV, Amsterdam, The Netherlands

Introduction

'Warning! The security of your online bank account needs to be updated. Update today or your account will be blocked. Click here to go to our secure website directly.' Criminals use these kinds of e-mail messages to lure bank customers to phishing websites with only one goal: obtaining user credentials to clear out their bank accounts.

This article is a follow-up to the work of Soudijn and Zegers [20] and Leukfeldt [15]. These studies described phishing networks, based on police files, and showed that phishing networks can have totally different characteristics. The 'crime script' of the two different networks was quite similar: the formation of a criminal core group, contacting other capable criminal enablers, capturing login details from victims and transferring funds to money mule accounts. However, the origin, growth, and criminal opportunities of these networks – and thus the possibilities for crime prevention – were completely different. In the first group [20], technology played a major role: e.g. malware was used to steal user data, a forum functioned as offender convergence setting to meet new criminals, contacts between offenders were primarily online, and spam e-mails were used to recruit money mules. In the other case [15], social ties played an important role: e.g. e-mails and telephone calls were used to steal user data, other criminals were recruited through social contacts, and encounters took place on the streets of large cities.

These two case studies confirm what a priori one might expect: that cybercriminal groups are not all the same. However, empirical criminological research into cybercriminal networks is scarce (see for an overview e.g. [5, 6, 22]). Only a few case studies on a limited number of criminal groups exist. It is clear that more research into cybercriminal groups is required to map the range of possible compositions. This article takes a more comprehensive approach and analyzes all known phishing and banking malware cases in the Netherlands in the period 2004–2014. This gives more insight into the different types of criminal groups that are involved in these cybercrimes and may help to develop effective crime prevention methods.

This article uses a social opportunity structure perspective to study cybercriminal phishing and banking malware networks (see section 2 for a more detailed explanation). It elaborates upon the criminal capabilities of networks (e.g. modus operandi and the use of technology, secondary criminal activities, and international components) and the composition of networks (e.g. functions within networks). Section 3 describes data and research methods. Subsequently, the results of the study are presented regarding criminal capabilities of networks (section 4) and composition of networks (section 5). Section 6 contains a taxonomy of networks, whereas section 7 contains the main conclusions and discussion.

Social opportunity structure

The studies by Soudijn and Zegers [20] and Leukfeldt [15] show that there are at least two types of groups involved in phishing. As Leukfeldt [15] pointed out, an explanation for these differences can be found in the concept of social opportunity structure. Social opportunity structure plays a major role in organized crime networks. Social ties and networks provide access to criminal opportunities and their nature further determines the opportunity structure, which facilitates different types of crime (e.g. [9, 18, 19]). Social relationships, however, are highly clustered and therefore always limited in

certain ways (e.g. because of geographical or social barriers between countries, lack of access to different ethnic groups, or barriers between illicit networks and the licit world – see [7]: 179–180). In order to expand opportunities, it is necessary to establish relationships with 'outsiders' (persons outside someone's existing social network). Therefore, access to 'offender convergence settings' (cf. [3, 4]) and key figures that are able to arrange these new contacts determine the growth and criminal opportunities of a given network. Studies into traditional criminal networks showed that access to these important brokers causes some offenders to remain local, whereas other offenders became international players (e.g. [9]). The local offenders commit all sorts of crimes in their own region, but they have no contacts outside their region and have no expertise others depend on. A condition for evolving into an international player is having contacts with brokers who give access to new export markets, or who have capital or expertise.

The degree of access to key figures and (digital) offender convergence settings provides an explanation for the differences between the cases described in Soudijn and Zegers [20] and Leukfeldt [15]. In fact, a parallel of the distinction between local and international offenders can be observed. The second group had no access to digital offender convergence settings and was constrained to a local social cluster. Accomplices were recruited through local social contacts and were all living in the Netherlands. All the victims were Dutch too. They also committed all kinds of other crimes to earn easy money. Conversely, the offenders of the first group met each other at a digital forum. Specific criminal services could relatively easily be acquired through the forum: victims were targeted, and accomplices were recruited in foreign countries. It also seems that the criminals were specialized in phishing attacks, as no other criminal activities were described in this case. Offenders were able to recruit new members in other countries and attack victims in multiple countries.

The social opportunity structure perspective can be used to explain differences between the nature and capabilities of cybercriminal groups described above. The two case studies show that there are differences between the criminal capabilities of cybercriminal networks and the composition of networks. In this article, we analyze 18 cybercriminal networks and test if these differences hold or need to be nuanced. The data and variables used in this article to gain insight into these elements will be described in the next section.

Data and methods

Eighteen Dutch criminal investigations were analyzed in order to gain insight into the composition and the criminal capabilities of criminal networks. These police files provide unique knowledge about cybercriminal networks and their members due to the use of special investigative powers such as wiretaps (telephone and internet traffic), observation, undercover policing, and house searches.

Cybercriminal networks: a demarcation

This study is part of the Research Program Safety and Security of Online Banking. Therefore, this study only includes networks that carry out attacks on online banking. Briefly, this means phishing attacks and malware attacks. In the literature, different definitions of phishing are used (see, for example, Lastdrager [14] for an analysis of

113 definitions). The common thread is: Phishing is the process aimed at retrieving users' personal information by criminals who, by using digital means such as e-mail, pose as a trusted authority. User credentials can be intercepted in a more technical way, namely by using malicious software such as Trojans or spyware. This kind of malware could log keystrokes, screenshots, e-mail addresses, browsing habits, or personal information such as credit card numbers.

Case selection

In our analysis, only completed criminal investigations are used. In these cases, the public prosecutor has decided that enough evidence has been collected to prosecute the suspects successfully. This, however, does not mean that there has already been a court decision.

There is no central registration system in the Netherlands that allows for a quick overview of all criminal investigations into phishing networks. The selection of cases was, therefore, done by using the snowball method. Starting points were cybercrime and fraud teams on a national and (inter)regional level. Using existing contacts within the Dutch police and the Dutch Police Academy, team leaders and senior investigators of these teams were asked whether they knew any investigations into phishing networks. Subsequently, public prosecutors who deal with cybercrime and fraud cases were asked the same question. Furthermore, an online database in which (a limited number of) court documents are published, was used, and a media analysis was done to find news reports about phishing cases. During the file study, people involved in the criminal investigation were asked whether they knew any other phishing cases. In total, eighteen criminal investigations into phishing networks were obtained. The investigations ran between six months and three years and were carried out between 2004 and 2014.

Analytical framework

The criminal investigation files contained records of interrogations and information obtained through special investigative powers (e.g. transcripts of phone taps, internet traffic and other surveillance reports). Relevant information was systematically gathered from the investigation files using an analysis framework. The framework was based on the analytical framework used in the Dutch Organized Crime Monitor. This is a long-running research program on organized crime (see [9–13, 21]).

The analytical framework consists of a list of topics the researcher has to describe (rather than a closed questionnaire). The topics and questions of the framework include inter alia composition (hierarchy, fluid cooperation, important roles/functions, use of enablers) and criminal capabilities (modus operandi, use of technology, secondary criminal activities, working area of the network).

Interviews

The analyses of the criminal investigation were complemented by interviews with the public prosecutor, the police team leader, and senior detectives (e.g. financial or digital experts). The same analytical framework was used. The interviews were conducted because the information in the police files is aimed at providing evidence of criminal activity, meaning that other relevant information to this analysis is often lacking.

Hierarchy and secondary criminal activities, for example, are not always described. Respondents, however, were sometimes able to provide more insight into these topics.

Criminal opportunities

Modus operandi

All networks are engaged in attacks on online banking. The scripts of the crime networks have many similarities in common. The first step is to intercept login credentials from victims to gain access to their online bank accounts. However, that is not enough to transfer money from the account of victims. In order to do this, so-called 'one-time transaction authentication codes' are required. Obtaining these codes is, therefore, step 2. With these transaction authentication codes, transactions can be done from victim accounts to the accounts of money mules.[1] Once the money has been transferred successfully, it is cashed out and, via various links, given to core members. There are some networks experimenting with other ways of cashing. These, for example, buy goods using the account of victims or buy Bitcoins. However, all networks predominantly use bogus front accounts to cash out the money.

Although the scripts of all criminal networks are roughly similar, there are some important differences. These differences concern obtaining user credentials and transaction authentication codes. The extent of ICT-use and degree of contact between the criminals and the victims differ. The high-tech capability of offenders makes it possible to limit the direct contact with the victim, but there is variation within the networks studied regarding the extent to which criminal attackers actually reduce contact with the victim. At one end of the continuum, there are networks limiting the use of ICT to a minimum and where victims issue codes to the criminals. These networks use e-mails (and sometimes phishing sites) to get user credentials. Subsequently, victims are phoned by criminals posing as bank employees in order to elicit necessary transaction authentication codes. At the other side of the continuum, there are networks using advanced malware that requires no direct contact with the victim. These networks, for example, infect websites that have outdated security. Once someone visits this website, his or her computer becomes infected with malware. This malware gives criminals access to and control over the victim's computer and enables the attacker to adjust or change online banking sessions.

The differences between these two types of attacks relate to the extent of ICT use during the attack, as well as the degree to which criminals have direct contact with the victims. The crime scripts can, therefore, be divided into two main categories: low-tech attacks and high-tech attacks. Moreover, each category of attacks can be subdivided by the degree of interaction between offenders and victims (Fig. 1). As a result, 4 attack variants can be identified: low-tech attacks with a high degree of direct interaction between attacker and

[1] In cybercrime literature, the term 'money mule' is often used to describe these offenders (see Choo [2]; McCombie [17]; Aston et al. [1]; [15, 20]). In our opinion, 'money mule' is not entirely the right term as these offenders are not used to physically move money from one place to another, but instead solely to disguise the financial trail from victims' bank accounts leading back to the core members (see Leukfeldt et al. [16] for a more comprehensive description). As the term money mule is so widely used, we have chosen to use it in this article.

victim (10 cases), low-tech attacks with a low degree of direct interaction (5 cases), high-tech attacks with a low degree of interaction (4 cases) and high-tech attacks without interaction (1 case). Networks that are carrying out low-tech attacks sometimes use several types of attacks (both with a low degree of contact and a high degree of contact). The total number of type of attacks is, therefore, higher than the total number of networks. Below a brief description will be given for each category.

Type 1: Low-tech attacks with a high degree of victim-attacker interaction

The 10 networks executing low-tech attacks with a high degree of interaction between the criminals and victims all use phishing e-mails and websites. As a rule, victims receive an e-mail appearing to be sent by their bank. The e-mail refers to the security of online banking, and the victim is asked to take immediate action to ensure that his or her account remains secure. Sometimes the victim has to reply to the e-mail itself and sometimes via a link in the e-mail (which usually links to a 'secure section of the website of the bank'). In both cases, offenders obtain user credentials and other relevant information. Subsequently, the victim is contacted by a member of the criminal network by telephone. The caller poses as a bank employee. During the telephone conversation, the caller refers to the phishing e-mail. Besides, the caller is able to give the victim information only the bank is supposed to know. This provides confidence that the victims are actually talking to a bank employee. During the telephone call, victims are asked to give one-time security codes, 'to finalize the latest security updates'. Using these security codes, offenders are able to transfer money from the victim's bank account to money mule accounts.

Type 2: Low-tech attacks with a low degree of victim-attacker interaction

Seven networks also use phishing e-mails and websites to acquire user credentials and other victim information. However, the crime script of these groups does not require a telephone call. Just like in the first attack variant, victims receive a phishing e-mail containing a link to a phishing site. This website has an additional entry field in which a telephone number has to be entered. Once the victim logs on to this phishing site, the criminals have access to the online bank account, and they consequently know the victim's telephone number. The criminals request a new SIM card in the name of the victim. Once this has been approved by the telecom company, all communication to

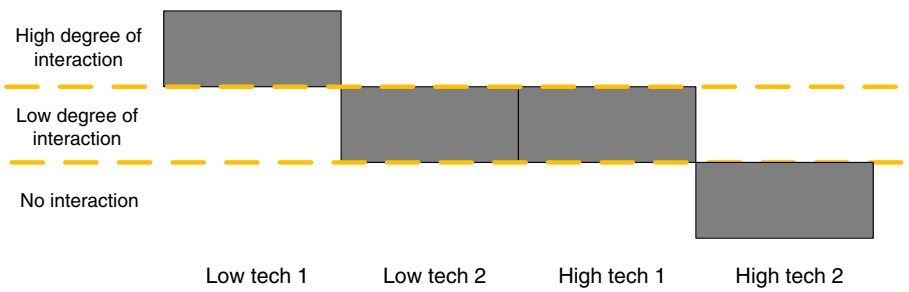

Fig. 1 Degree of technology use and contact between offender and victim

the phone number of the victim goes to the criminals. Transaction authentication codes sent to the mobile phone of the user are now received by the criminals, and can be used for transactions from the victim's bank account.

Type 3: High-tech attacks with a low degree of victim-attacker interaction

Networks using malware do not need to have direct interaction with victims to intercept user credentials and transaction authentication codes. The malware gives the criminal network control over the user's computer. As soon as this has been accomplished, transfers made by the victims can be manipulated. The most important part of this attack is infecting computers of potential victims with malware. 4 networks use a method installing malware when victims click on a link in an e-mail. Network 15, for example, first hacks into several databases of companies to obtain e-mail addresses. The group also hacks a hosting company to send large amounts of e-mail via the servers of that company (in at least one case over 250,000 e-mails). The e-mail appears to originate from a major utility company in the Netherlands. The e-mail states that the recipient is in arrears and that the utility company has tried to contact the victim several times without success. It also contains a link to the invoice that has not been paid. When the recipient clicks on the link in the e-mail, the computer is infected with a Trojan. This gives the criminals control over the browser of the victim. Information the victim enters can be adjusted without the victim noticing this. Criminals alter information that the victim enters when transferring money from his or her online bank account.

Type 4: High-tech attacks without victim-attacker interaction

Thus, high-tech attacks also require some degree of victim-attacker interaction; if users do not click on the link in the e-mail, their computers never become infected. Network 18, however, uses an attack method in which there is no victim-attacker interaction at all. This network infected a number of websites with outdated security. When someone visits this website, his or her computer is infected with malware automatically; the user does not need to perform any actions. When the victim uses his or her online bank account to transfer money, the malware alters the highest transaction. The amount is split in two: one part goes to the original beneficiary, whereas the other part goes to the account of a money mule. The victim has to approve the transaction, as usual and enter the transaction authentication codes. The victim does not suspect anything because the total amount is not changed, and the victim does not see anything abnormal on the screen. The malware ensures that the split payment is not visible in the transaction overview of the online bank account. The only way for the victim to find out that there has been a fraudulent transaction is by logging into their online account using a computer that has not been infected with malware.

Secondary criminal activities

The activities of the analyzed networks are not always limited to phishing or malware attacks. In 10 cases, it is clear that core members also perform other criminal activities. It seems to be a matter of ad hoc alliances: subgroups of core members working together on specific types of crime. Sometimes core members

collaborate with people outside the core group of the analyzed network. Most criminal activities relate to financial crimes.

Six networks, for example, also carry out fraud-related activities. Five of these are low-tech networks. Two of those networks are involved in attacks on payment transactions in which technology is not used at all. These groups use postal officials to intercept newly requested debit cards and official post from the bank containing PIN numbers and login details of online bank accounts. Other groups also engage in skimming or trading stolen goods. Some low-tech groups use their money mules for other purposes than transferring money alone. In the name of these money mules, for example, tax returns are requested or multiple telephone subscriptions are registered. The phones belonging to the subscriptions are resold, and the money mules are left with the subscription fees.

Four low-tech networks are also involved in drug trafficking. This varies from setting up a cocaine line into the Netherlands to the sale of different types of pills. Furthermore, three networks are involved in burglaries, muggings, and/or trading stolen goods. One network is involved in human trafficking.

One group performing malware attacks is also engaged in credit card fraud. On forums, they buy stolen credit card information. In the Netherlands, this information is used to buy goods and to travel. Another group performing malware attacks is also involved in phishing attacks aimed at Dutch webshops (to get access to their store credit and/or credit card credentials). The core member of this network also sells goods on online auction sites without delivering these goods.

International components

To determine how 'international' a network is, we looked at the countries from which the network members operated and from where the victims originated.

In 11 cases, the core members operate from the Netherlands and only use enablers and money mules that have been recruited in the Netherlands. All these networks carry out low-tech attacks. The 7 other networks have core members (2), professional enablers (5), recruited enablers (2) or money mules (2) operating outside of the Netherlands or having been recruited outside of the Netherlands. One of these networks performs low-tech attacks. This network uses a foreign professional facilitator to develop phishing websites. The other networks with core members from outside the Netherlands are engaged in high-tech attacks.

The two networks in which the core members come from countries other than the Netherlands, use a forum to recruit professional enablers. Whether the core members themselves have become acquainted with each other through this forum is unknown.

The 4 high-tech networks use professional enablers from outside the Netherlands to purchase malware, spam services, user credentials, or money laundering services. Core members use various forums on which such criminal services are offered.

Recruited enablers from outside the Netherlands provide services to 2 networks. One facilitator sets up a ring of money mules in England; and another facilitator helps money mules from Latvia to cross the border in Ireland. Two networks use money mules from countries other than the Netherlands. One network, which operates from Eastern Europe, recruits money mules in the Netherlands and Russia. Another network recruits money mules in Latvia and arranges buses to transport them to the Netherlands

and other countries where the network is active. Their goal is to open bank accounts, possibly with forged identity papers.

The low-tech networks are responsible for the majority of attacks on victims in the Netherlands. Twelve low-tech networks only attack customers of Dutch banks. One low-tech network also attacks people in Germany and the UK. One high-tech network only attacks customers of Dutch banks, whereas the other 4 high-tech networks also attack customers of banks in Germany, Belgium, UK, France, Swiss, and Spain.

Mapping the networks

Within all networks, there are dependency relationships and different functions. In addition to a more or less fixed group of core members, the composition of the networks changes regularly. In subgroups, core members carry out other criminal activities, individual core members commit crimes with criminals outside the network occasionally, new enablers are recruited when crime scripts change in response to new security measures, core members are constantly recruiting new enablers, and there is a constant flow of new money mules. Despite all these changes, four positions can be recognized within all networks: core members, professional enablers, recruited enablers, and money mules.

Core members are those members of the network initiating and coordinating attacks on online banking. Without the core members, the crimes in the investigations analyzed could not be committed, and they direct other members of the network. Within the group of core members, there can also be a hierarchy. For example, one core member who directs the other core members, and subgroups of core members with a specific set of tasks. However, such a hierarchy is not a necessary part of these enterprises.

Individuals providing services to the criminal network are in the layer below the core members. These services are necessary to execute the criminal activities. Some enablers play a more important role than others for the core members. Some services are simply rarer or more sought after. Hence, also within the group enablers, a distinction can be made between professional enablers and recruited enablers. The professional enablers provide certain services to the core members, e.g. falsifying identity documents or developing malware. These enablers are qualified 'professional' because they offer their services to the core members on their own initiative. They, for example, offer their services on online forums which are used by cybercriminals, or they are 'well known' criminal enablers in the offline criminal underworld. Recruited enablers also provide services to the core members, but they are encouraged or forced by the core members to do this. They have access to information that is of interest to the core members or they are able to provide 'simple' services; services that core members could also perform on their own or without which the crime script could still be executed. Examples include employees of call centers of banks, postal workers and employees of telecommunication companies. Similar to professional enablers, the recruited enablers provide services to the core members. The difference between the two groups is that the recruited enablers are less important for the execution of the crime script and are more easily replaceable than the professional enablers. Recruited enablers receive a small fee for the work and are only used by one particular network.

Money mules are the bottom layer of the networks. As a rule, these people are used by the core members or by enablers to interrupt the financial trail to the core members. In all networks, amounts of money were transferred from victims' online bank accounts to bank accounts of money mules.[2] The money was then cashed by the money mule, a facilitator, or a core member. This makes it impossible to follow the money trail.

In all networks, we can identify core members, enablers, and money mules. However, the number of people involved in the levels of the networks differs. Network 14, for example, is a relatively small network of three core members who carry out almost all criminal acts. The core members only use a professional facilitator to obtain fake identification documents. Conversely, network 1 consists of eight core members who use at least two professional enablers and 11 recruited enablers (regarding ICT support, fake identification documents, information from banking systems, and intercepting post from banks). Naturally, we only have information about the members that came up during the criminal investigation. It is quite conceivable that there are other members of the criminal network that never attract police attention.

Core members

In 11 cases, there is information about the core members, but in the other 7 cases, the investigation stopped before core members were actually identified and could be prosecuted. This section is based on the 11 networks for which we have information about core members.

The number of core members and their tasks differs for each network. The networks consist of between 1 and 8 core members. Typical for networks with multiple core members is that during the investigation these people jointly manage the criminal activities. From that perspective, there is a group of criminals who work together for an extended period. That does not mean that the individual core members do not cooperate with other criminals outside this network. Below an outline is given of the core members of two groups with a relatively large group of core members and a relatively small group of core members. Both cases include both phishing and malware networks.

Network 1 is a phishing network consisting of 8 core members. These core members know each other from the criminal underworld in Amsterdam and work together in loosely connected subgroups. There is not one specific leader controlling the other core members. According to police respondents, this group could also represent 2 or 3 smaller criminal partnerships that employ all kinds of criminal activities and only collaborate on specific types of crime. Core members discuss how to carry out phishing attacks and how to recruit the right people, but most of the core members also have their own specific tasks. There is, for example, one core member having a contact providing fake identification documents, one core member having a contact outside the Netherlands making phishing websites, three core members being responsible for cashing the illegally obtained money, and two other core members transferring money from victims' accounts to the accounts of money mules.

[2] Money from the victims' accounts can also be cashed in other ways. Criminals, for example, also buy goods or Bitcoins directly from the victims' accounts. However, all networks mainly used accounts of bogus men to get the money.

Network 6 is an international network performing malware attacks. This network consists of five core members. There is one core member who directs the other core members and who has contacts with professional enablers (providing malware, spam services, and other relevant services). The other core members have specific roles, for example, getting access to online bank accounts of infected bank customers, managing the European and Russian money mules, or recruiting new money mules.

There are also networks with a limited number of core members. Network 10 performs phishing attacks and consists of a stable core group of three persons. A man and a woman who are in a romantic relationship together are responsible for all the main criminal activities. The woman calls victims, tries to obtain transaction codes, and transfers money to accounts of money mules. The man recruits money mules and directs enablers that also recruit money mules for this network. He is also responsible for cashing the money from money mules accounts. Sometimes he cashes the money himself and sometimes the person who recruited the money mules is responsible for this. In addition, a long-time friend of the main recruiter who is a major supplier of money mules is also part of the group of core members.

Network 13 carries out malware attacks and has only one core member. This person is able to gain control over bank accounts by using malware. He meets enablers from other countries on forums (e.g. to buy specific malware or e-mail addresses), whereas he directs postal employees and money mules in the Netherlands.

Professional enablers

For 15 networks, it is clear that core members use services of professional enablers, or that the network itself consists of professional service providers. In 7 of these networks, the police investigation, however, is not directed at this group of suspects and provided little insight into this group of offenders. 3 networks do not use services of professional enablers at all. The networks that do use professional enablers, use them for ICT services such as malware writing or developing phishing sites (7 networks), supplying false identity documents (6 networks), recruitment of money mules (6 networks), cashing of money (4 networks) and money laundering (1 network). Below some examples of these services are described.

The IT services used by 7 networks include the development of phishing sites, supplying large amounts of e-mail addresses and manufacturing of malware. The core members of network 13 and 15 purchase malware through a forum. One of the core members of network 15 is the technical man of this network. He is responsible for technical aspects of the crime script, such as infecting computers with malware and encrypting communication. The network uses unique malware, which has most likely been developed by the technical man himself, but this core member also uses forums to look for new criminal tools. The core member of network 13 does not make the malware he uses in attacks himself but buys malware from a forum. Furthermore, internet taps show that he frequently visits forums where criminal enablers offer all kinds of services. He places several requests on these forums, for example, to send large amounts of e-mails. He also places a call in which he asks for a programmer who can solve a specific problem with a website of a bank.

The core members of network 6 also use malware to carry out their attacks. It is unclear whether the malware was purchased or self-developed. It is, however, clear that

the core members use a forum to come into contact with people who can translate texts of phishing mails and e-mails to recruit money mules. The texts are translated from Russian into English, German, and Dutch. Furthermore, one of the core members negotiates with a member of the forum who offers spamming services that can be used to send large amounts of e-mails.

Another service for which core members use enablers is forging identity papers. Five phishing networks and one malware network used enablers for this purpose. These forged documents are used by money mules to open multiple bank accounts, to collect large sums of money in bank offices (identification is required to withdraw large amounts of money), or to send money abroad using money transfers. In none of the networks it becomes clear who these enablers actually are.

Recruited enablers

Networks also regularly use recruited enablers. 14 of the 18 networks use this type of enablers. Examples are money mules recruiters (N = 14), cashers who ensure the money which has been withdrawn from the accounts of money mules gets to the core members (N = 9), bank employees who, for example, provide core members with information about potential victims (N = 2), postal employees who intercept post with newly requested logins to online bank accounts (N = 2), callers who telephone victims and try to obtain transaction codes (N = 2), and an employee of a telecommunications company who is able to swap SIM cards of telephones allowing transaction codes sent to victims' mobile phones to be redirected to the criminals (N = 1). Below some examples of money mules recruiters / cashers and bank employees will be presented.

14 networks use recruiters providing new money mules to the core members. Within 9 networks, money mules recruiters are also responsible for cashing the money. Money mules are essential to the core members because money from victim accounts is transferred to the money mules accounts. Without the bank account of money mules, the money would be transferred directly to the core members and they would be easily identified by the bank or the police. Recruiters often operate within the area in which they live and use their social network to recruit new money mules. In the case of network 8, for example, only young people in the city of The Hague are used. One of the core members of this network operates from Amsterdam. This core member is in contact with a network that is specialized in the recruitment of money mules and cashing the illegally obtained money. The group of recruiters and cashers in The Hague only recruit money mules in their own region. One of the money mules states: 'I already said that everybody in the Netherlands is doing this. Particularly young people. You can make easy money and many want to do that. Many young people or junkies who have nothing to lose.' This money mule was recruited on the streets of The Hague by someone he vaguely knew from his neighborhood. He came across this person every once in a while and was offered money multiple times to lend his bank card and PIN code. Another example of recruitment within one particular area is case 10. The network of recruiters employed by network 10 only recruited money mules within a particular ethnic community in a medium-sized town in the North-West of the Netherlands. These money mules received a fee for their services, so it was not difficult for recruiters to engage new money mules. New money mules even approached recruiters on their own initiative. Interrogations provide evidence that 'on the

street' everybody knew that the recruiter was involved in criminal activities in which easy money could be made.

The bank employees involved in the criminal activities are all in the immediate vicinity of core members. They are approached by core members or recruiters to deliver specific services. Some bank employees reported being put under pressure; others cooperated because they got financial compensation. The bank employees provide detailed information from bank systems that is used by the core members. The bank employees work in the call centers of several large banks. In order to work there, they need a 'Certificate of Good Conduct'. Furthermore, these employees usually have completed a relevant study (e.g. Financial Services). Through their work, these employees have access to customer data and are able to make changes in customers' accounts. Core members use these data, for example, to cherry pick wealthy customers, to convince customers they talk with a bank employee because they can provide information that only the bank knows, and to increase cashing limits of victims' accounts (so stolen money can be cashed more easily).

Money mules

17 networks use money mules. These people are used to break the money trail to core members. Money mules are recruited by core members themselves (4 networks), professional enablers (4 networks), and/or recruited enablers (14 networks). In most cases, money mules also offer their 'services' spontaneously to recruiters. This happens, for example, if a recruiter recruits long enough in one specific area. After some time, it becomes 'common knowledge' that easy money can be made by providing a debit card and security code. New money mules then approach recruiters or previously recruited money mules, and make clear that they also want to earn money.

Taxonomy

Section 4 and 5 provide evidence that networks have different characteristics. There are differences in the composition of networks (e.g. the number and type of enablers) and criminal capabilities (e.g. degree of technology use and interaction between offenders and victims). Additionally, international components can be recognized at different levels within the networks (at the level of core members, enablers, and victims). Finally, there are both specialists and generalists; networks carrying out one specific type of attack and networks performing a variety of criminal activities.

To provide insight into the relationship between the crime script, international components, and the degree of specialization of networks, we created a taxonomy of the networks. In Fig. 2, the 18 networks are plotted along an X-axis and Y-axis. The X-axis indicates the degree to which a network has international components. Each network has a score between 1 and 4 points. The network gets 1 point if both the core members and enablers only operate from the Netherlands, and if only victims are made in the Netherlands. If there are (also) core members or enablers involved operating from countries other than the Netherlands or if there are victims outside of the Netherlands, a network receives one extra point for each of these categories. In total, a network is able to get 4 points. The Y-axis represents the degree of technology use and the offender-

victim interaction. Again, networks can get a score between 1 and 4 points. Networks performing low-tech attacks with a high degree of offender-victim interaction get 4 points. 3 points are for networks performing low-tech attacks with a low degree of offender-victim interaction. Networks executing high-tech attacks with a low degree of offender-victim interaction receive 2 points and networks carrying out high-tech attacks without offender-victim interaction get 1 point. Finally, Fig. 2 shows whether networks consist of specialists who are engaged in one type of attack or that a network deployed all kinds of criminal activities. Specialist networks are grey in Fig. 2.

Figure 2 shows that the 18 networks cannot easily be divided into two sharply defined categories. However, there are clear differences between networks carrying out low-tech attacks and high-tech attacks. Low-tech networks, for example, make no victims in other countries and core members and enablers generally operate from the same country. The high-tech networks, on the contrary, have more international components. The 4 high-tech networks with the highest 'international' score consist of core members and/or enablers from different countries and get victims from several countries. The two high-tech networks with the lowest degree of international components carry out high-tech attacks in the Netherlands and operate from the Netherlands. Forums are used to recruit other suitable co-offenders in other countries (both core members or professional enablers).

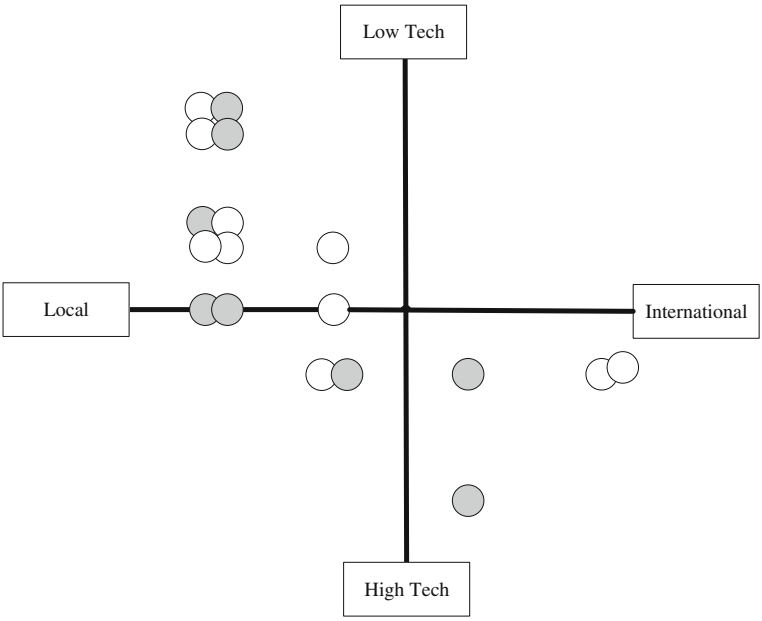

Fig. 2 Taxonomy of phishing and malware networks. The X-axis indicates the degree to which a network has international components (ranging from networks with all the members of the networks and victims operating from the same country to networks with members operating from different countries and victims in different countries). The Y-axis represents the degree of technology use and the offender-victim interaction (ranging from networks performing low-tech attacks with a high degree of offender-victim interaction to networks carrying out high-tech attacks without offender-victim interaction). Finally, specialist networks carrying out one type of attack are grey. For a more extensive explanation, see section 6

Furthermore, networks with specialists focusing on one type of crime can be seen in both low-tech and high-tech networks. These specialist networks have more often a local than an international focus.

Conclusion and discussion

Conclusion

There appears to be a greater variety of networks than the empirical studies of Soudijn and Zegers [20] and Leukfeldt [15] show. Networks cannot simply be classified into high-tech networks with specialists who perform international attacks versus low-tech networks of criminal all-rounders who perform local attacks: technology use, the degree of offender-victim interaction, and international components create a more variegated set of arrangements. The most obvious differences are related to the international capabilities of low-tech networks and high-tech networks. And apparently, high-tech networks are able to carry out their attacks with fewer core members and enablers.

The crime scripts of networks have much in common. First, getting hold of credentials and one-time transaction authentication codes of victims in order to gain control over online bank accounts. Second, making transactions from victim accounts to the accounts of money mules, cashing out the transferred money, and getting the money to the core members. However, there are differences in exactly how networks carry out their crime scripts. These differences are related to obtaining user credentials and transaction authentication codes. The extent of ICT use and degree of offender-victim interaction differ. The modus operandi of the networks can, therefore, be divided into four categories: low-tech attacks with a high degree of direct offender-victim interaction, low-tech attacks with a low degree of direct interaction, high-tech attacks with a low degree of interaction and high-tech attacks without interaction.

The networks in our analysis are fluid. Although the core members of the networks form a more or less consistent group of criminals, the general composition of networks changes frequently. Subgroups of core members execute secondary criminal activities, and individual core members work together with criminals from outside the criminal network to commit all kinds of crimes.

Within all networks, four roles can be distinguished: core members, professional enablers, recruited enablers, and money mules. Core members are those members initiating and coordinating attacks on online banking. They direct and/or control the members with other roles. Enablers provide necessary services for the execution of criminal activities. A distinction can be made between professional enablers (offering their services to all kinds of criminal networks) and enablers who are recruited by core members themselves. Money mules are used by the core members or enablers to interrupt the financial trail to the core members.

Discussion

Differences between the analyzed networks mainly boil down to technology use. The higher the degree of technology use, the less interaction between offenders and victims.

Thanks to technology use, high-tech networks are able to execute successful attacks without much interaction with victims. The degree of offender-victim interaction is important because the victim has the opportunity to notice the attack during these interactions. If there is no direct interaction at all, such as in the attacks by network 18, the possibilities for users to protect themselves are very limited.

It also appears that high-tech networks more often than low-tech networks operate internationally and consist of relatively few core members and enablers. For these networks, forums play an important role as digital offender convergence settings. On forums, core members are able to search and find other suitable co-offenders and/or purchase malware to carry out attacks. Forums enable a small group of core members to have a high impact. Some of our analyzed cases show that individual core members end up at criminal forums out of curiosity. On these forums, they connect with other members, ask all sorts of questions, and experiment with offered criminal tools and services. From core members of other networks, it is unknown how they ended up at the forums they used to search for co-offenders or criminal tools. This is an important topic for further research. Questions that need to be answered include what the exact role of forums is in the origin and growth of cybercriminal networks, how core members end up on a forum for the first time, and how new criminal alliances are forged.

Research limitations

The analysis of criminal investigations presented in this article provides a unique view of the different roles and functions within cybercriminal networks and the criminal capabilities of these networks. The methodology, however, also has some limitations.

First of all, our analyses are based on a limited number of criminal networks in the Netherlands. We were able to track down 18 criminal investigations. Our study shows that investigations provide a good picture of the different layers and roles within cybercriminal networks and the criminal capabilities of these networks. However, because of differences in priorities, capacity, and expertise in the area of cybercrime, the same sort of analysis in other countries might provide different insights. The methodology used in our study can also be applied in other countries to supplement our analysis.

Furthermore, only criminal investigations and interviews with persons who were involved in carrying out these investigations are used. We only have information about cybercriminal networks known to and investigated (successfully) by the police. There is no knowledge about networks that remain invisible for law enforcement. For a more extensive review of methodological questions concerning the use of police investigations, see [8]. Future research should also focus on criminal networks that are able to avoid police attention and should also use other methods than file analysis.

Finally, we only analyzed cybercriminal networks carrying out phishing and malware attacks on online banking. Whether criminal networks engaged in other forms of cybercrime, such as extorting businesses with ransomware or DDoS attacks, have the same characteristics is unknown. Future research should therefore also focus on criminal networks that commit other types of cybercrime.

References

1. 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.
2. Choo, K.K.R. (2008). Organised crime groups in cyberspace: aa typology. *Trends in Organized Crime, 3*(11), 270–295.
3. Felson, M. (2003). The process of co-offending. In M. J. Smith & D. B. Cornish (Eds.), *Theory for practice in situational crime prevention (volume 16)* (pp. 149–168). Devon: Willan Publishing.
4. Felson, M. (2006) *The ecosystem for organized crime* (HEUNI paper nr 26). Helsinki: HEUNI.
5. Grabosky, P. N. (2004). The global dimensions of cybercrime. *Global Crime, 6*(1), 146–157.
6. Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior, 35*(2014), 20–40.
7. Kleemans, E. R. (2007). Organized crime, transit crime, and racketeering. *Crime and Justice. A Review of Research, 35*, 163–215.
8. Kleemans, E. R. (2014). Organized Crime Research: Challenging Assumptions and Informing Policy. In J. Knutsson & E. Cockbain (Eds.), *Applied Police Research: Challenges and Opportunities. Crime Science Series*. Cullompton: Willan.
9. 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.
10. Kleemans, E. R., & Van de Bunt, H. G. (1999). The social embeddedness of organized crime. *Transnational Organized Crime, 5*(2), 19–36.
11. Kleemans, E.R., Van der Berg, A.E.I.M. & Van de Bunt, H.G. (1998). *Georganiseerde criminaliteit in Nederland. Rapportage op basis van de WODC monitor.* [Organized crime in the Netherlands] Den Haag: WODC.
12. Kleemans, E.R., Brienen, M.E.I., Van de Bunt, H.G., Kouwenberg, R.F., Paulides, G. and Barensen, J. (2002) *Georganiseerde criminaliteit in Nederland. Ttweede rapportage op basis van de WODC-monitor.* [Second report on organized crime in the Netherlands] Den Haag: WODC.
13. Kruisbergen, E.W., Van de Bunt, H.G., Kleemans, E.R. and Kouwenberg, R.F. (2012) *Georganiseerde criminaliteit in Nederland. Vierde rapportage op basis van de Monitor Georganiseerde Criminaliteit.* [Fourth report on organized crime in the Netherlands] Den Haag: Boom Lemma.
14. Lastdrager, E. E. H. (2014). Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Science, 3*(9), 1–6.
15. Leukfeldt, E.R. (2014). Cybercrime and social ties. Phishing in Amsterdam. *Trends in Organized Crime, 17*(4), 231–249.
16. Leukfeldt, E.R., Kleemans, E.R., and Stol, W.P. (2016) Cybercriminal Networks, Social Ties and Online Forums: Social Ties Versus Digital Ties within Phishing and Malware Networks *British Journal of Criminology* (accepted for publication / online first).
17. McCombie, S.J. (2011). *Phishing the long line. Transnational cybercrime from Eastern Europe to Australia*. (PhD-thesis). Sydney: Macquarie University
18. McGloin, J. M., & Kirk, D. S. (2010). An overview of social network analysis. *Journal of Criminal Justice Education, 21*(2), 169–181.
19. Scott, J., & Carrington, P. J. (2011). *The SAGE Handbook of Social Network Analysis*. London: SAGE Publications.
20. Soudijn, M. R. J., & Zegers, B. C. H. T. (2012). Cybercrime and virtual offender convergence settings. *Trends in Organized Crime, 15*(2–3), 111–129.
21. van de Bunt, H.G. and E.R. Kleemans (2007) *Georganiseerde criminaliteit in Nederland, derde rapportage op basis van de Monitor Georganiseerde Criminaliteit.* [3rd report on organised crime in the Netherlands] Den Haag: WODC.
22. Wall, D. S. (2007). *Cybercrime. The Transformation of Crime in the Information Age*. Cambridge: Polity Press.