Banking malware and the laundering of its profits

Custers, B.H.M.; Pool, R.L.D.; Cornelisse, R.

Banking malware and the laundering of its profits

Bart HM Custers
Leiden Law School, the Netherlands

Ronald LD Pool
WODC, the Netherlands

Remon Cornelisse
WODC, the Netherlands

Abstract
Banking malware is malicious software that aims to steal money from victims via manipulated bank transfers in online banking. This paper describes how the profits of banking malware are generated and subsequently laundered, with a particular focus on the use of bitcoins and other digital payment methods. Computers are infected with banking malware via phishing e-mails, in which people are persuaded in various ways to click on links or open attachments, or via exploit kits, programs that try to find weak spots in the security of computer systems. After infection, bank transfers of the online banking accounts of victims are manipulated via fake website screens (web injects). Behind the screens the amounts and beneficiaries of transactions are modified, emptying the victims' bank accounts. In the next step, the banking malware profits are laundered. In this paper we describe two models that are used in particular (next to more traditional money laundering methods). The first model involves the use of money mules and a quick cash-out. The second model focuses on direct spending via (A) direct purchases of products via online shopping, (B) direct purchases of Bitcoins via Bitcoin exchanges or (C) direct purchases of luxury goods. Bitcoins can be further laundered via so-called mixing services. All in all, these methods allow criminals to launder profits in relative anonymity and prevent seizure of the illegal profits.

Keywords
Banking Malware, Bitcoins, Cybercrime, Money Mules, Money Laundering.

Introduction

Despite a lot of research on money laundering of profits of traditional crime such as drug trafficking (Savona 2005; Schaap 1998), relatively little is known about the money laundering of cybercrime. Whereas in traditional crime the profits are often in cash, cybercrime profits are often generated in the form of electronic money (i.e., digital euros, dollars, etc. on online bank accounts). Furthermore, in the area of cybercrime, there exists valuable research on financial cybercrime, phishing and related areas, but most of it focuses on the victims of cybercrime (Anderson 2006; Choi 2008; Harrell and Langton 2013; Leukfeldt 2014; Leukfeldt 2015; Jansen and Leukfeldt 2016; Ngo and Paternoster 2011, Vishwanath et al.2011; Van Wilsem 2011), whereas research on the cybercriminals and their methods is limited. In this paper we try to add to existing knowledge and literature by focusing on the laundering

of cybercrime profits and the methods cybercriminals use for this. We focus specifically on the profits of banking malware, a type of financial cybercrime that uses malicious software (or 'malware' in short) that aims to steal money from victims via manipulated bank transfers in online banking.
Banking malware has been one of the most prominent threats in the area of cybercrime in recent years and cybercriminals generate large profits with banking malware (Europol, 2015a: 7). In July 2015, it was reported that a group of cybercriminals generated profits amounting to a hundred million euro with banking malware between 2005 and 2014 (Sandee 2015: 3). Although banks have taken several measures to address and mitigate this threat, their clients are still being attacked by cybercriminals on a daily basis.
Similar to other crimes in which criminals aim to make profits, in the case of banking malware and other types of financial cybercrime it is necessary to launder the generated profits. When the profits are not laundered, its origins can easily be traced and this may increase the likeliness that the cybercriminals will be caught. In the case of banking malware, it is electronic money that has to be laundered in order to conceal its illegal origins and prevent seizure of the profits.
In this paper we will provide an answer to the key question: "how are the profits of banking malware generated and subsequently laundered?" In answering this question, we will particularly focus on the role of bitcoins and other digital payment methods. For instance, Europol signals a shift from the use of more traditional payment methods towards digital payment methods, such as Bitcoin, that offer more anonymity (Europol 2015a: 30).
This paper is structured as follows. In the second section we describe the methodology used in our research. In the third section we describe what banking malware is and how it works. In the fourth section we identify two different models that are used for the laundering of banking malware profits, illustrated by a real police case in one of the police files we encountered in our research. In the fifth section the methods for laundering Bitcoins are described. The final section we provide conclusions.

Methodology

The key question of this paper was answered in a research project that was carried out by the authors when working for WODC, the Research Centre of the Ministry of Security and Justice in the Netherlands (Oerlemans et al. 2016). This research was requested by the Team High Tech Crime of the Dutch National Police, who wanted to have more background knowledge both on how profits of financial cybercrime are laundered and the roles of different actors involved in the money laundering processes.
The question in this paper was answered by applying various research methods. Apart from desk research – focusing on existing relevant literature on cybercrime, banking malware, bitcoins, virtual currencies and money laundering - a series of 20 interviews were conducted and a total of four police files with criminal cases were investigated. The research was carried out in 2016.
The desk research focused on an analysis of available literature and relevant media messages in order to collect background information on (the relations between) cybercrime, money laundering and digital payment methods. The literature was also used to validate results from the other research methods.
The interviews consisted of a series of twenty semi-structured interviews with (mainly Dutch) experts in the areas of cybercrime, money laundering and the use of digital payment methods. These experts are mainly active in law enforcement, banks and financial institutions and the digital payment services industry. Six interviewees are affiliated to the largest commercial banks in the Netherlands. One respondent works for the Dutch national bank. One person is employed at Bitonic, a bitcoin exchange based in the Netherlands. Nine interviewees are active in law enforcement, including one person from Europol, three persons from the public prosecution service, three persons from the national police (from the Team High Tech Crime) and two persons from the FIOD, the fiscal intelligence and investigation service of the Netherlands Tax and Customs Administration. Two interviewees are affiliated with Fox-IT, a private company focusing on cyber security. One interviewee is affiliated with Mollie, a private company specialized in online payment methods.

The list of questions used for the interviews consisted of three major topics. The first topic concerned cybercrime, particularly banking malware, with questions on how the respondents view banking malware, ways in which infection with malware takes place, current and near-future developments, and typologies of perpetrators. The second topic was on money laundering, particularly via cryptocurrencies, with questions on past, present and future constructions of money laundering, the payment methods used, the role of cryptocurrencies in the money laundering, and the role of online market places, money mules and other actors possible involved in money laundering. The third topic was on combating money laundering, with questions on proving intent, gathering evidence for money laundering, anti-money laundering measures, the prosecution of money laundering as a separate charge (apart from the cybercrime itself), measures envisioned or needed to better fight money laundering, and new anti-money laundering legislation.
Not all interviewees were asked the same set of questions. Rather, depending on the background and expertise of each interviewee, a subset of the list of interview questions was used in each interview. The interview results were used to generate knowledge on the use of digital payment methods in digital money laundering processes of the banking malware profits.
In cooperation with the Dutch National Police and the Public Prosecution Service, four police files concerning cybercrime and money laundering were investigated. The cases were selected because they involved banking malware and/or the use of Bitcoins. The information in the police files concerns information on digital money laundering methods and characteristics of actors involved. Three cases concerned banking malware, one case concerned ransomware. In all cases Bitcoins were used in the money laundering process and in some of the cases Webmoney, PayPal, Ukash, Vouchers, Western Union, MoneyGram and other digital payment methods were used. In one case, MegaServer, most of these digital payment methods were used. This case is described in Section 4.3.

Banking malware: how it works

A thorough understanding of the workings of banking malware is required in order to understand how the profits are generated. Cybercrime may be defined as 'criminal acts committed using electronic communications networks and information systems or against such networks and systems' (European Commission 2007: 2; Wall 2007)). This approach clearly distinguishes between tool cybercrimes (i.e., types of cybercrime that use electronic communication networks and information systems) and target cybercrimes (i.e., types of cybercrime that are targeted against electronic communication networks and information systems) (Koops 2014: 214; cf. Charney 1994; cf. Parker 1976: 17-22).
Target cybercrimes specifically focus on the integrity, confidentiality and availability of such networks and systems. The most obvious example is illegal access, often referred to as 'hacking' (Décary-Hétu and Dupont 2012; Dupont et al 2016). This is a criminal offense under Article 2 of the Council of Europe's Convention on Cybercrime (Council of Europe 2001). The illegal access may concern computers, but also Internet of Things devices (Atzoria et al. 2010). A variety of approaches may yield such unauthorized or illegal access. Examples include misleading or persuading victims to provide log-in details, crunching passwords with computer power or abusing software vulnerabilities (Bernaards et al. 2012: 29-34). Criminals may also use malicious software ('malware') to gain unauthorized access to computers from a distance. Creating and disseminating such malware is also a criminal offence according to the Convention on Cybercrime.[1]
Malware can have different functionalities. Examples include keylogging (recording all strikes on the keyboard), backdoors (remote access to computers via pre-programmed backdoors) and Remote Administration Tools (RATs) (Europol 2015a: 21-25) that can remotely control computer systems and can turn on and off functions like webcams and microphones from a distance. Computers infected with malware that are remotely controlled by other computers are part of so-called botnets (Bernaards et al. 2012; 45). These botnets may be useful for their computing power, for instance, to start DDoS attacks, crunch passwords, crack encryption or mine Bitcoins.

Tool cybercrimes focus on the facilitating role that the internet and computer systems may play. Deception and fraud are crimes that increasingly take place online (Clough 2010: 372-373). Online scams often concern phishing (Lastdrager 2014), a scam in which criminals try to obtain personal data in order to later abuse these data. According to our interviewees, phishing has been considerably professionalized in recent years (CSBN 2016: 45). Via fake e-mail messages, victims are requested to visit a copy of their online banking website to verify their account. After people have entered their name and account details, they are contacted by a (fake) bank employee and persuaded via 'social engineering' to disclose their PIN codes or to make specific payments.[2] Spear-phishing is another method, consisting of a targeted attack on an individual or company using personal data that is already known by the attackers (Bernaards et al. 2012: 58-59). Money laundering via digital or virtual currencies can also be considered a tool cybercrime, as computers and the internet are tools used to commit these crimes. Case law in the Netherlands shows that criminals committing these offences are often convicted for traditional theft.[3]

Next to malware via phishing e-mails, computers can also be infected with the use of so-called exploit kits. These are programs that try to find weak spots in the security of computer systems and then install the malware. This may happen when victims did not take adequate security measures, such as using passwords, firewalls and anti-virus software. Research has shown that, even though people take measures to protect themselves against online banking fraud, most victims are unaware of the scam that they fell victim to prior to the incident (Jansen and Leukfeldt 2016). People also report to have insufficient knowledge and skills regarding the safety and security of online banking and find it difficult to assess to what extent protective measures help them to safeguard against fraudulent attacks (Jansen and Leukfeldt 2016; Custers et al. 2014).
After a computer is infected with the banking malware, the malware starts doing what it was designed for. Usually this involves manipulating the bank transfers that the victim makes with his or her online banking account. The malware often makes use of so-called web injects, fake website screens that pretend to be a user's online banking environment. The malware may allow cybercriminals to manipulate the web browsers of their victims and show these fake screens, for instance, when the victims try to enter their online banking environment (Sandee 2015: 16-18). The malware recognizes the name of the bank or the URL the victim is searching for and guides the victim to the fake website that the cybercriminal has created (Bernaards et al. 2012: 43). The fake websites may be very hard to distinguish from the real websites for online banking. When the victim wants to transfer money to another account, behind the screens the amount and the beneficiary are modified.[4] This type of attack is also referred to as a man-in-the-browser-attack (Tajalizadehkoob 2013: 25). Sometimes waiting screens are used to keep the victim waiting while the transaction is prepared and executed. A typical business model for cybercriminals is to buy and disseminate the malware (which costs approximately 3.000 dollars) and then generate profits by emptying the bank accounts of victims (on average 722 dollar per victim), with total profits running into the hundreds of thousands of dollars to millions of dollars (Ilyin 2014).

Many banks have a two factor identification system that requires, apart from log-in details like a username and password, an authentication code. This may be, for instance, a code sent via a mobile phone text message or a code generated by a special device (often in combination with the credit or debit card). These codes can be intercepted by the criminals via malware (for instance, when mobile phones are also infected with the malware) or by directly contacting the victims (for instance, by opening a chat screen or another type of pop-up screen, or by calling them, pretending to be a bank employee) (Sandee 2015: 17-18). The trade in credit and debit cards with related codes is referred to as 'carding' (Peretti 2008).
A lot of banking malware has several different functionalities and is not only aimed at stealing log-in details of online banking accounts of victims. The malware, for instance, also tries to collect other personal data by attacks based on particular keywords like popular electronic communication services and payment services (Binsalleeh et al. 2010). Also, some malware offers the possibility for criminals

to install other malware on the infected computers to further exploit the victims. Fees are charged for this between criminals, generating profits not only from victims, but also from other criminals (Sandee 2015: 4-5).
Case studies show that there are at least two types of groups involved in cybercrime: low-tech all-rounders and high-tech specialists (Leukfeldt et al. 2016a). Although empirical criminological research into cybercriminal networks is scarce, there appears to be some variety in cybercriminal networks. Networks can further be characterized by clear differences in low-tech attacks and high-tech attacks. High-tech networks typically have more international components. The majority of networks fall into the high-tech, international category of networks. Most networks are not restricted to one type of cybercrime (Leukfeldt et al 2016b).
A typical example of a high-tech, international network is the Zeus network. The network was led by two individuals. One of them, a person calling himself Slavik, probably wrote the ZeuS malware (Sandee 2015: 6). Since 2006, the malware has gone through several revisions and evolutions in which functionalities were added (Sandee 2015). In recent years, the ZeuS malware has been very successful in executing fraudulent bank transfers in online banking environments (Falliere and Chien 2009). In 2014 the network had grown to an organization of over fifty people, who were not hierarchically organized and did not meet in person. Rather, the criminals worked online on the basis of tasks that were outsourced (Krebs 2015). The exploitation of the malware was outsourced to so-called bot herders, who manage the botnets mentioned above (Hogben et al. 2011: 15). Infecting computers was outsourced to other people. A lot of money was spent on so-called bullet proof hosting providers, to keep the servers from which the botnets were controlled out of sight and stable (Sandee 2015: 15). The criminals succeeded in exploiting victims all over the world. By establishing themselves in Eastern Russia, a working day started with attacking banks in Australia and ended with attacking banks in the United States (Krebs 2015). In this way, the cyber criminals generated profits of an estimated 100 million dollar between 2006 and 2014. In 2014, the FBI dismantled the botnet infrastructure in cooperation with private partners (FBI 2014). Slavik is still a fugitive.
There seems to be a trend in which the organizations exploiting banking malware are becoming more professional and people in these organizations have specialized roles within this malware economy (Bauer et al. 2008: 8; Hogben et al. 2011; De Graaf et al. 2012: 1; Soudijn and Zegers 2012). In 2016 in the Netherlands, there were several cases in which criminals were convicted for being part of an organized crime network that used banking malware for fraudulent transactions and subsequent money laundering.[5] In these cases criminals closely worked together, dividing amongst each other technical tasks (like developing the malware, infecting computers and creating an infrastructure) and financial tasks (like money laundering). According to Europol, it is likely that in the future there will be more loosely organized criminal networks in which individuals gather online on a temporary basis to cooperate and commit cybercrimes (Europol 2015b: 11).

Laundering banking malware profits

Once the cybercriminals have generated profits with banking malware, they will want to launder the profits, in order to conceal the illegal origins and to avoid confiscation. There are many definitions of money laundering (Unger 2006: 30-35; Van Koningsveld 2008; Gelemerova 2011: 59), but the essence is to avoid attention of police and justice organizations and tax authorities (Kleemans et al. 2002: 127). This can be done by avoiding policing technologies (Custers 2015).
In many situations, money laundering of criminal profits takes place with (combinations of) 'traditional' money laundering methods. These methods can be straightforward or more complex. A typical example of a straightforward money laundering method is to create a (long) series of transactions, including several currency exchanges, transfers to other countries and investments in real estate or other assets (Kruisbergen et al. 2012: 190-203; Soudijn and Akse 2012). Because of due diligence and anti-money laundering legislation in many countries, banks and financial institutions have to notify the authorities when transactions or actors are suspicious (Custers 2007). Typically, criminals split

transactions to smaller amounts to avoid suspicion and transfer money via countries with less strict rules and supervision (Kruisbergen and Soudijn 2015: 13). Another straightforward money laundering method is to spend the profits directly on products and services.

More complex money laundering methods include fictitious turnovers, fictitious gambling profits and loan-back constructions (Europol 2015c: 18). Fictitious turnover involves raising the turnover of legitimate companies with revenues that do not exist. In this way, legal profits are mixed with illegal profits. In a different version of this method, called trade based money laundering, the illegal profits are kept within a company for legal international transactions, such as buying products in one country and selling them in another country (FATF 2008: 1). Fictitious gambling profits can be created by suggesting that profits originate from gambling rather than crime. Although casinos are strictly regulated in many countries, online gambling is legal in many jurisdictions. By creating several online gambling accounts, criminals can transfer money between these accounts, concealing the origin of the profits. In loan-back constructions, criminals also create several accounts (sometimes on fake names or for family members) and then lend money to themselves. This can also obfuscate financial trails.

All these constructions, and combinations thereof, can also be used for laundering the profits of cybercrime. In many cases, criminals prefer to generate profits in cash or to quickly exchange their profits into cash, as using cash is the easiest to conceal the illegal origin of the profits (Europol 2015c: 9). In most types of traditional crime, this is not very difficult because the profits are already in cash, but the profits of banking malware are usually digital profits, i.e., digital euros, dollar, etc., in an online banking environment. Hence, the first step for cybercriminals to launder their profits is to transfer the money from this environment to where they want to have it. This may involve also other methods than the traditional money laundering methods described above. In this section, we will describe these methods. In the first and second subsection we describe two models for laundering the profits of banking malware that we could identify in our research, based on the available literature, the police files and the interviews. The first model involved the use of so-called money mules and a quick cash-out. The second model involves the direct spending of the profits in the online banking environment. In the third subsection we describe a real case from the police files in the Netherlands that illustrates how the money laundering works.

Money mules and cash-out

When cybercriminals gain access to the online bank accounts of their victims via banking malware, they can transfer money from the victim's account to another account. Usually, they do not transfer the money directly to their own bank account, as this would make them very easy to trace. Instead, the cybercriminals recruit so-called money mules.[6] These are people who are willing to provide their bank account for a fee (Aston et al. 2009). A typical fee is about 5 % of the total amount that is transferred (Europol 2015c: 41; UNODC 2014: 52). For instance, the recruiters may offer them a fee of 500 euro if they are willing to transfer 10.000 euro via their bank account. After the money is transferred from the victim's account to the money mule's account, the money mule usually withdraws the money from his account via an ATM. This is called the cash-out. In order to ensure the money mule does not steal the money, in many cases it is not the money mule but someone else who performs the cash-out. This person is also referred to as the casher.[7]

The money mule and the cash-out constitute the first stage of the money laundering process (see Figure 1). Usually the actions in this first stage are sufficient to constitute money laundering in terms of a criminal offence, as illegal profits are processed with the intention of concealing the illegal origin of the profits.

The second stage can consist of all kinds of combinations of money laundering methods to conceal the illegal origin of the profits, including the traditional money laundering methods described above. The money may be transferred to foreign bank accounts or, after the cash-out, it may be transmitted abroad via money transmitting services, spent on luxury goods or transferred abroad in cash. A typical method we encountered in the police files and literature is via money transfers with Western Union of MoneyGram (UNODC 2014: 20; Europol 2015c: 41).[8] Relatively often the money is transferred to

Eastern European countries, where local money mules collect the money, without knowledge of the illegal origin of the money (UNODC 2014: 20, 53-54; Krebs 2015: 22).[9] In practice, the first and second stage may be hard to distinguish. The second stage may consist of a long chain of transactions.

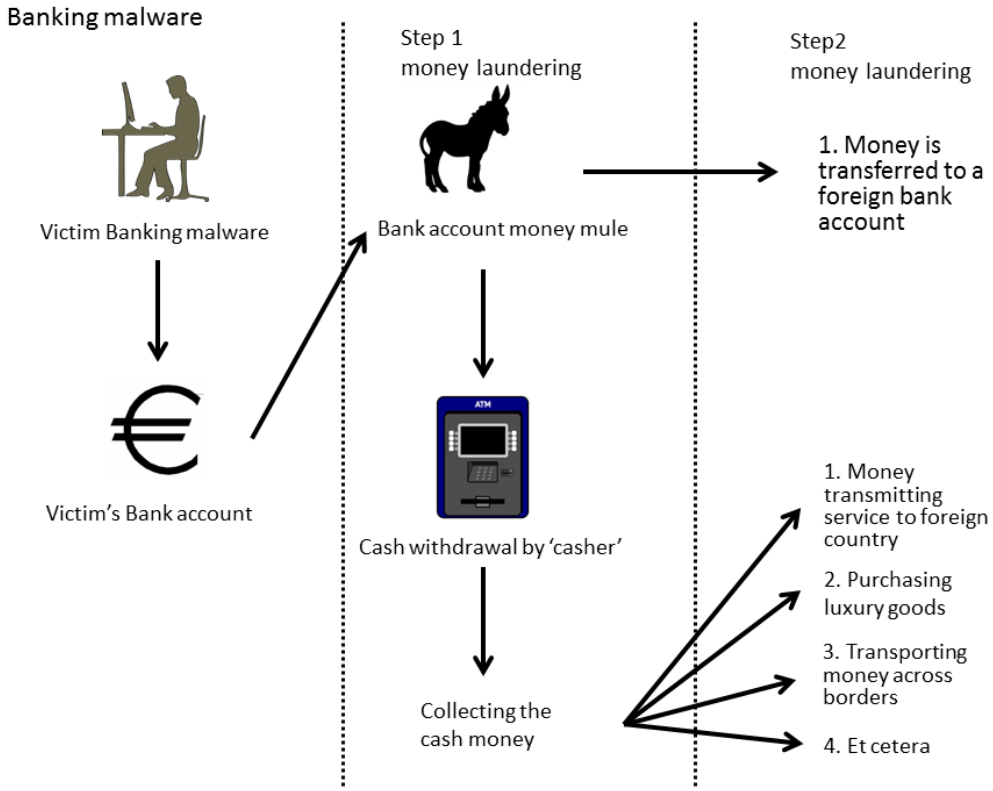

Figure 1: Model with money mules and cash-out.

On the basis of the case law and the literature we studied and the police files examined, transferring money from the victim's account to the account of a money mule is the most common approach to handle banking malware profits (UNODC 2014: 20).[10] However, this method has a significant drawback for cybercriminals: each bank has implemented maximum amounts for withdrawals each day (and sometimes also each week). Furthermore, the duration of the cash-out period is also maximized, since banks block accounts after victims report the crime to the police or to their bank. Banks have also implemented other detection methods to rapidly respond to money mules. In short, the amount of money that can be laundered with the help of one money mule is limited to a few hundred or a few thousand euro. Hence, for the money laundering of large amounts of illegal profits, many money mules need to be recruited. After the bank account of a money mule has been blocked, he is unable to open a new bank account. Banks usually also report the activities of money mules to the police and they may be convicted for money laundering. Reusing money mules may therefore be difficult for cybercriminals.

Cybercriminals partially address this by recruiting money mules abroad, delaying and complicating the detection of these money mules and the blocking of their accounts.[11] However, organizing large numbers of money mules in different countries requires a complex organization that may involve considerable costs for criminals.

Direct spending

The second model (see Figure 2) may appear in three versions: (A) direct purchases of products via online shopping, (B) direct purchases of Bitcoins via Bitcoin exchanges, or (C) direct purchases of luxury goods. These are discussed below:

(A) Instead of transferring the money from the victim's account to the account of a money mule, banking malware also allows for the option to order products (and sometimes services) via online shopping and pay for this from the victim's bank account. Obviously, when the products are delivered, the cybercriminals do not use their own address, as this would directly lead back to them. Money mules are recruited for this.[12] In some cases the police found large amounts of unopened parcels with game computers. Other products that are purchased include prepaid cards, gift cards and credit for mobile phones (see also the Mega Server case discussed below). In interviews it was indicated that parcels are often shipped to Eastern European countries. The products are sometimes resold for profit.

(B) In recent years, not only products are purchased in banking malware cases, but also Bitcoins are purchased via Bitcoin exchanges, for which payments are made directly from the victim's bank account.[13] The Bitcoins can be kept in a Bitcoin wallet that functions like a bank account from which cybercriminals can spend something from time to time. Further laundering of Bitcoins is explained in Section 5.

(C) When victims have large amounts of money on their accounts, cybercriminals can use this to directly purchase luxury goods, like cars. With the use of Remote Administration Tools (see Section 3), cybercriminals monitor the activity on the victim's computer. When the timing is right, a payment can be executed. This method is rather complicated and requires some timing and, according to our respondents, does not seem to be used often. This may change in the future, however.

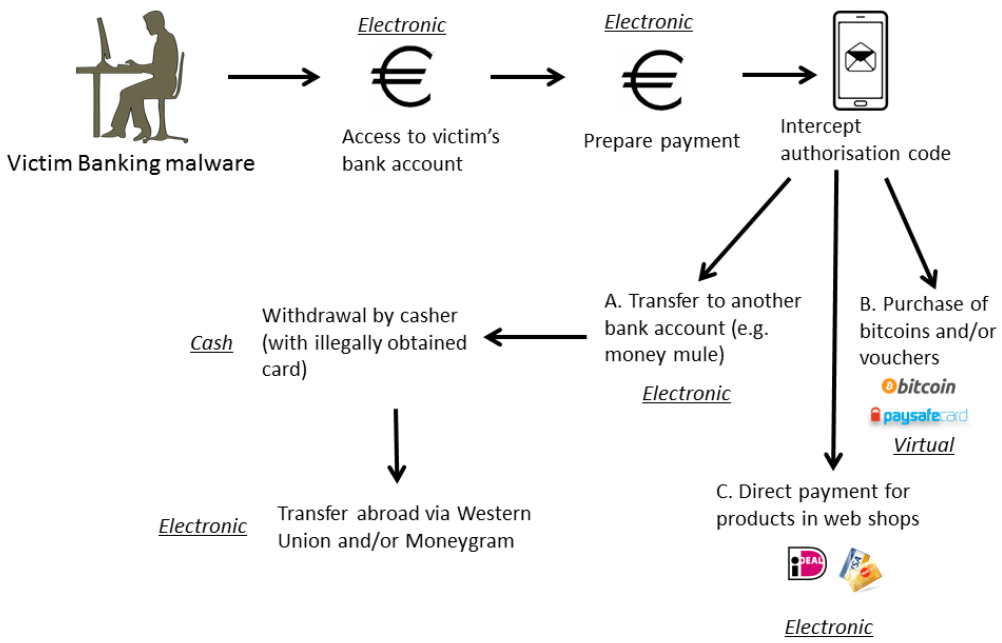

Figure 2: Model with direct spending of the profits.

In comparison with the first model, the second model allows more time for the criminals to cash out money, since it usually takes longer before the money mules are traced, as there are no bank account details available to trace them. Hence, it takes a bit longer before the money mules get caught, usually via the addresses where the purchases are delivered. The money mules can thus be used by the cybercriminal networks for a longer period of time and larger amounts of banking malware profits can be laundered per money mule (or, in other words, less money mules need to be recruited for laundering the same amount of money). The disadvantage for criminals of model 2A, however, is that it still depends on the use of money mules that need to be recruited. Another obvious disadvantage for criminals is that the profits are transformed into products rather than money. To the extent that the criminals do not consume the products themselves, they need to resell these items, which may be time-consuming and yield financial losses. The disadvantage of model 2C for criminals is that it is time-consuming and requires thorough timing. Model 2B does yield spendable money. The laundering of Bitcoins is discussed in more detail in the next section.

The mega server case

As indicated above, in most banking malware cases several money laundering methods are combined to conceal the illegal origin of the profits. To illustrate this, we describe a specific case, the Mega Server case, on banking malware in the Netherlands, for which the criminals were convicted by the court of Rotterdam in 2015.[14]

On 2 October 2015, four suspects were convicted by the court of Rotterdam for possessing and acquiring malware, committing computer trespass, theft, scams and money laundering. In the verdict, a detailed description is provided of their practices. The banking malware was disseminated via botnets in order to infect other computers. After infecting a computer, the malware ensured that the victims were shown fake screens, via web injects, that appeared to be the online banking environment the victim was used to. After the victims completed their log-in details on the fake screen, the cybercriminals obtained these personal details from the victims. Furthermore, mobile phones of victims were also infected with tailored malware, in order to intercept text messages the bank used to verify bank transfers.

After obtaining access to and control over the online banking accounts, the criminals transferred the money from the victim's accounts to the accounts of several money mules and cashers. Also, the cybercriminals used fake identity documents to open many bank accounts at various banks. The banking malware profits were withdrawn from these intermediate accounts via cash-outs from ATMs, according to model 1. Subsequently, the money was transferred abroad via Western Union. Also, the cybercriminals purchased Bitcoins and prepaid cards (like paysafecards) directly from the victim's accounts, according to model 2. Bitcoins with a total value of 13.000 euros were purchased. These actions were qualified as money laundering by the court. For an overview of the methods used, see Figure 3. The cybercriminals also used other money laundering methods. For instance, one of them created a fake company to receive the banking malware profits. Another applied for a credit card in the name of one of his victims. Yet another laundered some of the profits in a casino.

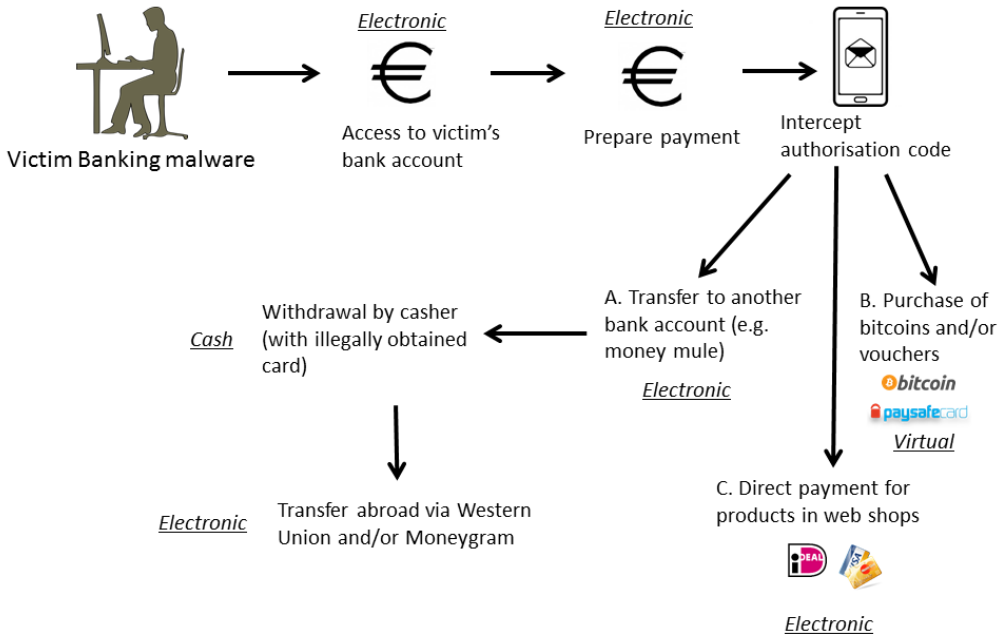

Figure 3: Money laundering methods in the Mega Server Case.

The court stated in its verdict that these are serious crimes, in which Dutch banks were coarsely attacked. This damaged, according to the court, the trust in the integrity of the electronic payment systems and it might have seriously disrupted social and economic infrastructures. On average, the cybercriminals were convicted for terms in prison of two years, of which six months were conditional. When applying these sanctions, the court took the relatively young age of the cybercriminals into account.

Laundering bitcoins

A description of what Bitcoins are and how the underlying blockchain technology works, is beyond the scope of this paper. However, in order to describe how money laundering of bitcoins works, we will briefly describe the functionality of Bitcoins. For the purposes of this paper, it is sufficient to consider Bitcoin transactions similar to transactions with other currencies. For instance, bitcoins can be exchanged for euros or dollar (or vice versa) similar to the way euros or dollars can be exchanged for pounds or yens. Exchanging bitcoins usually takes place via Bitcoin exchanges, online financial service providers that charge a small fee for each exchange. The major differences between bitcoins (and other virtual currencies) and euros, dollar, etc. (so-called fiat currencies) are that bitcoins are decentralized (i.e., not issued and supported by a national government) and that bitcoins have no offline, physical equivalent (i.e., no cash). As mentioned above, banking malware profits that are turned into bitcoins may simply be put in a Bitcoin wallet that serves as a savings account from which cybercriminals can spend from time to time.
Bitcoin wallets are anonymous to some extent, so this may conceal the illegal origin of the profits and prevent seizure. However, Bitcoins are based on blockchain technology that uses a public ledger in which all transactions can be consulted. As such, all transactions from one Bitcoin account can be linked to each other. For this reason, cybercriminals may create several Bitcoin accounts, to prevent linkability. When cybercriminals transfer bitcoins between their own accounts, this may indicate a link

between these accounts (Nakamoto 2008). Using advanced analysis of transaction data, pseudonyms may be clustered to several users (Meiklejohn et al. 2013; Ron and Shamir 2013). The next step is to establish real identities behind these pseudonyms. This can be done by employing different sources. For instance, when someone mentions his or her Bitcoin address on a website or forum, this may enable establishing a real identity (Meiklejohn et al. 2013; Reid and Harrigan 2013). Also, via payment details in online shopping information may be retrieved, for instance, shipping addresses and e-mail addresses. Reluctant cybercriminals will use anonymization software like Tor.[15] However, there are also methods to couple Bitcoin addresses to IP addresses that circumvent these anonymization techniques (Biryukov et al. 2014).

A typical way to conceal the illegal origin of Bitcoins is the use of so-called mixing services (also known as mixers, blenders or tumblers). These are online services that exchange Bitcoins for Bitcoins, against a fee. After a user has submitted the Bitcoins, the mixing service collects Bitcoins from different sources (or even mines completely new Bitcoins) and pays them back to the respective user on a different account.[16] A typical fee is 3 % (Möser et al. 2013: 4). Mixing services are usually only accessible via Tor to ensure anonymity of the service provider and its clients (Europol 2015a). As a result, it is often not clear in which jurisdiction the mixing services are established. From the police files and interviews it appeared that cybercriminals do not always use mixing services.

Conclusion

In this paper we answered the question: how are the profits of banking malware are generated and subsequently laundered? Banking malware is malicious software that aims to steal money from victims via manipulated bank transfers in online banking. Via spam people are persuaded to click links or open attachments. By doing so, they unknowingly install malicious software on their computers. This malware enables cybercriminals to gain illegal access to and control over online banking accounts of their victims. The malware uses web injects (i.e., fake screens that look like the online banking environment) in which victims complete their log-in details. Behind the screens the amounts and details of the beneficiaries are manipulated. This way the bank accounts of the victims are compromised. An average of over 700 dollars is extracted from each victim.

The profits are generated in the form of electronic money, that is subsequently laundered in order to conceal its illegal origin and to prevent seizure. We identified two models that are used to launder the banking malware profits. The first model focuses on money mules and a quick cash-out. The money is transferred from the victim's bank account to the money mule's bank account who subsequently withdraws the money via an ATM. Next, the money is often transferred abroad via money transfer services. The second model involves direct spending from the victim's bank account. This may involve direct purchases of products via online shopping, direct purchases of Bitcoins via Bitcoin exchanges, or direct purchases of luxury goods. When bitcoins are purchased they can be laundered further via mixing services that exchange bitcoins for bitcoins to further conceal the illegal origin of the banking malware profits. All in all, these methods allow criminals to launder profits in relative anonymity and prevent seizure of the illegally obtained electronic money.

The analysis of money laundering methods of banking malware profits presented in this paper provides new, unique insights in the ways cybercriminals act in order to be able to enjoy the profits of their cybercrimes. However, the methodology used in this research also has some limitations. First, the analysis is based on a limited number of interviews and cases. The number of cases investigated is constrained by the availability of cases. As a result of the limited material, we are unable to assess the prevalence of the described models and to which extent these findings can be applied to other contexts. As a result, the analysis remains at a descriptive, qualitative level. In the future, if significantly larger amounts of cases become available, quantitative analyses may become possible and perhaps even predictive models can be developed and hidden patterns disclosed.

Second, the focus on expert interviews and cases implies that the scope of this research is limited to forms of banking malware and money laundering known to and investigated by law enforcement.

There is no knowledge available (nor is it included in this research) about methods that remain invisible for law enforcement.
Third, this research specifically focused on the national context in the Netherlands. As such, the results are difficult to extrapolate the findings to cybercrime and cybercriminals in other countries. Although cybercrime typically is an international type of crime, in which cybercriminals make practical use of limitations caused by jurisdictions of law enforcement agencies, there may be differences in the ways cybercriminals and cybercriminal networks from different countries operate.
Future research should therefore also focus on cybercrime and cybercriminals in other countries. If more cases become available, quantitative research becomes possible. Furthermore, future research could also focus on the methods to fight cybercrime, particularly banking malware and money laundering of cybercrime profits. There already exists research on investigating cybercrime (Oerlemans 2017) and new technologies in policing (Custers and Vergouw 2015), but knowledge on the usefulness and effectiveness of these policing methods is limited. Finally, further research may also be needed on how to further empower people to safeguard themselves against cybercrime. From a customer perspective, awareness of fraudulent schemes and training in how to apply protective measures are critical in keeping online banking safe and secure (Jansen and Leukfeldt 2016; Kumaraguru et al 2010).

Notes

1. See Article 11 of the Convention on Cybercrime.
2. A typical case can be found in Dutch case law: Rb. The Hague, 15 July 2016, ECLI:NL:RBDHA:2016:7981.
3. See, for instance, Dutch case law: Rb. Rotterdam, 2 October 2015, ECLI:NL:RBROT:2015:7041, Rb. Zeeland, 29 June 2016, ECLI:NL:RBZWB:2016:3877 en Rb. Rotterdam, 20 July 2016, ECLI:NL:RBROT:2016:5814, Computerrecht 2016/175.
4. For examples, see Dutch case law: Rb. Zeeland, 29 June 2016, ECLI:NL:RBZWB:2016:3877 en Rb. Rotterdam, 20 July 2016, ECLI:NL:RBROT:2016:5814, Computerrecht 175 (2016).
5. Dutch case law: Rb. Zeeland, 29 June 2016, ECLI:NL:RBZWB:2016:3877 en Rb. Rotterdam, 20 July 2016, ECLI:NL:RBROT: 2016:5814, Computerrecht 2016/175.
6. Usually the recruiters are different people (i.e., not the cybercriminals themselves) who are specialized in and hired for this tasks. See Europol (2015a), p. 10 and examples in Dutch case law: Rb. Rotterdam, 2 October 2015, ECLI:NL:RBROT:2015:7041 and Rb. Zeeland, 29 June 2016, ECLI:NL:RBZWB:2016:3877.
7. See examples in Dutch case law: Rb. Rotterdam, 2 October 2015, ECLI:NL:RBROT:2015:7041 and Rb. Zeeland, 29 June 2016, ECLI:NL:RBZWB:2016:3877.
8. Dutch case law: Rb. Rotterdam, 2 October 2015, ECLI:NL:RBROT:2015:7041.
9. 'In nearly every case, the sequence of events is virtually the same: The organization's controller opens a malware-laced email attachment, and infects his or her PC with a Trojan that lets the attackers control the system from afar. The attackers then log in to the victim's bank accounts, check the account balances – and assuming there are funds to be plundered — add dozens of money mules to the victim organization's payroll. The money mules are then instructed to visit their banks and withdraw the fraudulent transfers in cash, and wire the money in smaller chunks via a combination of nearby MoneyGram and Western Union locations.' (Krebs 2015).
10. See also Dutch case law: Rb. Rotterdam, 2 October 2015, ECLI:NL:RBROT:2015:7041, Rb. Zeeland, 29 June 2016, ECLI:NL:RBZWB:2016:3877 and Rb. Rotterdam, 20 July 2016, ECLI:NL:RBROT:2016:5814, Computerrecht 175 (2016).
11. See examples in Dutch case law: Rb. Zeeland, 29 juni 2016, ECLI:NL:RBZWB:2016:3877 en Rb. Rotterdam, 20 juli 2016, ECLI:NL:RBROT:2016:5814, Computerrecht 175 (2016).
12. Strictly speaking, these are not money mules, as money mules provide their bank account, whereas these people (sometimes referred to as 'drops') provide their address.

13. See Dutch case law: Rb. Rotterdam, 2 October 2015, ECLI:NL:RBROT:2015:7038, Rb. Zeeland, 29 June 2016, ECLI:NL:RBZWB: 2016:3877 and Rb. Rotterdam, 20 July 2016, ECLI:NL:RBROT:2016:5814, Computerrecht 175 (2016).
14. Rb. Rotterdam, 2 October 2015, ECLI:NL:RBROT: 2015:7038.
15. https://www.torproject.org/
16. See, for instance, Deepdotweb, 'Introducing Grams Helix: Bitcoins Cleaner', 22 June 2014. www.deepdotweb.com/2014/06/22/introducing-grams-helix-bitcoins-cleaner.

References

Anderson KB (2006) Who are the victims of identity theft? The effect of demographics. *Journal of Public Policy & Marketing*, *25*(2), 160–171.

Aston M, McCombie S, Reardon B, and 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.

Atzoria L, Ierab A and Morabito G (2010) The internet of things: A survey, *Computer Networks: The International Journal of Computer and Telecommunications Networking,* 54, 2787-2805.

Bauer JM, Van Eeten MJG and Wu Y (2008) *ITU study on the financial aspects of network security: Malware and spam.* Genève: ITU.

Bernaards F, Monsma E and Zinn P (2012) *High tech crime: Criminaliteitsbeeldanalyse*, Driebergen: KLPD-DNR.

Binsalleeh H, Ormerod T, Boukhtouta A, Sinha P, Youssef A, Debbabi M and Wang L (2010) On the analysis of the ZeuS Botnet Crimeware, In *2010 Eighth Annual International Conference on Privacy, Security and Trust (PST)*, 31-38.

Biryukov, A, Khovratovich D and Pustagarov I (2014) Deanonymisation of clients in Bitcoin P2P network. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, ACM* (pp. 15-29). New York: ACM.

Charney, S (1994) Computer crime: Law enforcement's shift from a corporeal environment to the intangible, electronic world of cyberspace, *Federal Bar News*, *41*(7), 489.

Choi KS (2008) Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology*, *2*(1), 308–333.

Council of Europe (2001) *Convention on Cybercrime*, ETS 185, 23 November 2001.

Clough, J (2010) *Principles of cybercrime.* Cambridge: Cambridge University Press.

CSBN 6 (2016) *Cyber Security Beeld Nederland 6.* The Hague: Nationaal Cyber Security Centrum.

Custers, BHM (2007) Risk profiling of money laundering and terrorism funding: Practical problems of current information strategies. *Proceedings of the 9th International Conference on Enterprise Information Systems*. Portugal: Funchal.

Custers BHM, Van der Hof S and Schermer B (2014) Privacy Expectations of Social Media Users: The Role of Informed Consent in Privacy Policies, *Policy and Internet* 6(3): 268-295.

Custers BHM and Vergouw SJ (2015) Promising policing technologies: Experiences, obstacles and police needs regarding law enforcement technologies, *Computer law & security report* (31): 518-526.

Décary-Hétu D and Dupont B (2012) The social network of hackers. *Global Crime*, 13(3), 160–175.

Dupont B, Côté A, Savine C and Décary-Hétu D (2016) The ecology of trust among hackers. *Global Crime*, 17(2), 129–151.

De Graaf, D, Shosha AF and Gladyshev P (2012) EDOLAB: Shopping in the Cybercrime Underworld. *Research Paper*.

European Commission (2007) Towards a general policy on the fight against cyber crime. Communication from the commission to the European Parliament, the Council and the Committee of the Regions. COM (2007) 267. Brussels, 22 May 2007, p. 2.

Europol (2015a) *The internet organised crime threat assessment (iOCTA).* The Hague: Europol Police Office.

Europol (2015b) *The future of organised crime report 2015.* The Hague: Europol Police Office.

Europol (2015c) *Why is cash still king?,* The Hague: Europol Police Office.

Falliere N and Chien C (2009) *Zeus: King of the bots.* Symantec Security Response.

FATF (2008) *Best Practices on Trade Based Money Laundering*; Financial Action Task Force. Paris: FATF-OECD.

FBI (2014) *U.S. Leads Multi-National Action Against GameOver Zeus Botnet and Cryptolocker Ransomware, Charges Botnet Administrator*, FBI Press Release, 2 June 2014. See: www.fbi.gov/news/pressrel/press-releases/u.s.-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware-harges-botnet-administrator.

Gelemerova, L (2011) *The anti-money laundering system in the context of globalisation: A panopticon built on quicksand?*, Nijmegen: Wolf Legal Publishers.

Harrell E and Langton L (2013) *Victims of identity theft, 2012*. Washington DC: Bureau of Justice Statistics.

Hogben G, Plohmann D, Gerhards-Padilla E and Leder F (2011) Botnets: detection, measurement, disinfection & defence, European Union Agency for Network and Information Security (ENISA), Heraklion: ENISA.

Ilyin, Y (2014) Cybercrime Inc.: how profitable is the business. Moscow: Kaspersky Lab. https://blog.kaspersky.com/cybercrime-inc-how-profitable-is-the-business/15034/

Jansen J, Leukfeldt ER (2016) Phishing and Malware Attacks on Online Banking Customers in the Netherlands: A Qualitative Analysis of Factors Leading to Victimization. In: *International Journal of Cyber Criminology*, 2016. DOI 10.5281/zenodo.58523.

Kleemans ER, Brienen MEI, Van de Bunt, HG, Kouwenberg RF, Paulides G and Barensen J (2002) *Georganiseerde criminaliteit in Nederland: Tweede rapportage op basis van de WODC-monitor*. The Hague: Boom.

Koops, EJ (2014) Cybercriminaliteit. In Van der Hof S, Lodder AR and Zwenne GJ (eds.) Recht en computer, p. 213-241. Deventer: Kluwer.

Krebs, B (2015) Inside the $100M 'Business Club' Crime Gang, *Krebsonsecurity.com*, 5 August 2015:

Kruisbergen EW, Van de Bunt HG and Kleemans ER (2012). Georganiseerde criminaliteit in Nederland: Vierde rapportage op basis van de Monitor Georganiseerde Criminaliteit. The Hague: Boom Lemma uitgevers.

Kruisbergen, EW and Soudijn MRJ (2015) Wat is witwassen eigenlijk? Introductie tot theorie en praktijk, *Justitiële verkenningen*, *1* (2015), 10-23.

Kumaraguru P, Sheng S, Acquisti A, Cranor LF and Hong J (2010) Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology*, *10*(2), 7:1–7:31.

Lastdrager, EEH (2014). Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Science*, 3(9), 1–6.

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

Leukfeldt ER (2015) Comparing victims of phishing and malware attacks: Unraveling risk factors and possibilities for situational crime prevention. *International Journal of Advanced Studies in Computer Science and Engineering, 4*(5), 26–32.

Leukfeldt ER, Kleemans ER and Stol WP (2016a) A typology of cybercriminal networks: From low tech locals to high tech specialists. In: *Crime, Law and Social Change*, 2016. DOI 10.1007/s10611-016-9662-2

Leukfeldt ER, Kleemans ER and Stol WP (2016b) Origin, growth and criminal capabilities of cybercriminal networks. An international empirical analysis.. In: *Crime, Law and Social Change*, 2016, DOI 10.1007/s10611-016-9647-1.

Meiklejohn S, Pomarole M, Jordan G, Levchenko K, McCoy D, Voelker GM and Savageet S (2013) fistful of bitcoins: Characterising payments among men with no names, *Proceedings of the 2013 conference on Internet measurement conference*, *ACM (2013)*, 127-140;

Möser M, Böhme R and Breuker D (2013) An inquiry into money laundering tools in the bitcoin ecosystem, *Proceedings of the 2013 e Crime Researches Summit,* 1–14.
Nakamoto S. (2008) Bitcoin: A peer-to-peer electronic cash system. *Bitcoin.org.*
Ngo FT and Paternoster R (2011) Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology*, *5*(1), 773–793.
Oerlemans JJ, Custers BHM, Pool RLD and Cornelisse R (2016) Cybercrime en witwassen: bitcoins, online dienstverleners en andere witwasmethoden bij banking malware en ransomware. Meppel: Boom Criminologie.
Oerlemans JJ (2017) *Investigating cybercrime,* Leiden: Meijers Research Institute.
Parker DB (1976) *Crime by computer.* New York: Scribner.
Peretti, KK (2008) Data breaches: what the underground world of 'carding' reveals. *Santa Clara Computer and High Technology Law Journal*, 25(2), 345–414.
Reid F and Harrigan M (2013) An analysis of anonymity in the bitcoin system, S*ecurity and privacy in social networks*, 197-223.
Ron D and Shamir A (2013) Quantitative analysis of the full bitcoin transaction graph. *Financial cryptography and data security*, *7859*, 6-24.
Sandee M (2015) Game over Zeus: Background on the Badguys and Backends, Whitepaper for the U.S. Blackhat conference 2015.
Savona E (2005) *Responding to money laundering*, Amsterdam: Harwood Academic Publishers.
Schaap C (1998) *Fighting money laundering*, London: Kluwer Law International.
Soudijn MRJ and Akse T (2012). Witwassen: Criminaliteitsbeeldanalyse 2012. Driebergen: KLPD.
Soudijn MRJ and Zegers BCHT (2012) Cybercrime and virtual offender convergence settings. *Trends in organized Crime*, *15*(2), 114-115.
Tajalizadehkoob S (2013) *Online banking fraud mitigation.* Delft: TU Delft.
Unger B (2006) *The scale and impacts of money laundering.* Cheltenham: Edward Elgar.
UNODC (2014) Basic manual of the detection and investigation of the laundering of crime proceeds using virtual currencies. *United Nations Office on Drugs and Crime.*
Van Koningsveld TJ (2008) Witwassen: de fasen van het witwasproces getoetst, *Tijdschrift voor Onderneming en Financiering*, 4, p. 88-104.
Van Wilsem JA (2011) Bought it, but never got it: Assessing risk factors for online consumer fraud victimization. *European Sociologic Review, 29*(2),168–178.
Vishwanath A, Herath T, Chen R, Wang J. and Rao HR (2011) Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*, *51*(3), 576–586.
Wall, DS (2007) *Cybercrime. The Transformation of Crime in the Information Age*. Cambridge: Polity Press.