Summary

Cybercrime and money laundering
Bitcoins, payment service providers and other methods of laundering banking malware and ransomware profits

Background, research question and scope

Compared to money laundering in traditional offenses, like drug trafficking, relatively little is known about money laundering in cybercrime. The major difference is that, contrary to traditional offenses, in which criminals usually acquire money in cash, cybercrime profits increasingly appears to be made via new payment methods. With the growth of cybercrime in recent years, there is an urgency to gain insight into the money laundering process and the actors involved. This study focusses on the money laundering process and maps the actors involved in banking malware and ransomware. Banking malware, in short, is malicious software that is intended to steal money through online banking payments. Ransomware is malicious software that keeps a computer system (or all files on it) 'hostage' and demands a ransom payment to unlock the system. In recent years, a new form of ransomware has emerged. This so-called cryptoware encrypts files on a computer and demands a ransom payment, often by paying with the virtual currency Bitcoin to decrypt the files.

The key question of this research report is: *in what way and through which actors are profits of banking malware and ransomware laundered?* To answer this question, six sub-questions were formulated:

1 What is money laundering of banking malware and ransomware profits, and how can this kind of laundering be qualified in criminal law?
2 What are new payment methods, especially virtual currencies such as Bitcoin, and how do they work?
3 How and with the help of which actors is money laundered that is obtained
   a through banking malware?
   b through ransomware?
4 What are the characteristics of actors involved in the money laundering process?
5 Which information about the modus operandi of actors involved in the money laundering of banking malware and ransomware profits is available on the dark web?
6 What role do new payment methods, especially virtual currencies such as Bitcoin, have in the money laundering process of banking malware and ransomware?

Methodology

The research questions have been answered through use of the following methods: (1) desk research, (2) interviews, (3) police files analysis, (4) an 'experiment' with bitcoins and mixing services, and (5) a quantitative analysis of transaction data from Dutch banks, related to banking malware and phishing. The desk research has been conducted on the basis of an analysis of scientific literature, professional literature, and news articles with regard to money laundering, cybercrime and new payment methods. Semi-structured interviews were held with twenty experts in various relevant disciplines. The desk research and the interviews provided knowledge about the use of new payment methods and the digital laundering of cybercrime profits. In addition, four cases from the Dutch National High Tech Crime Unit were analysed with regard to cybercrime and money laundering. By means of an empirical test, in which bitcoins were purchased and submitted to a mixing service for processing, insight was gained into the world of online money laundering services. Finally, a quantitative analysis was conducted on transaction data from all large banks in the Netherlands. This data provided information on the characteristics of money mules involved in the money laundering process of banking malware.

Results and conclusions

Typically the profits of banking malware and ransomware are digital. In case of banking malware, criminals acquire electronic money and in case of ransomware the ransom is often paid with vouchers or (in case of cryptoware increasingly) with bitcoins. Laundering of the profits consists of concealing the criminal origin of the money. The legal typologies developed to prove deliberate money laundering, relate mainly to cash in drug offenses. Consequently, there is a lack of clarity as to when processing or possessing large sums of digital money can be seen as money laundering.

Many types of new payment methods can be used to launder cybercrime profits. A distinction can be made between electronic money and virtual money. Electronic money is the digital representation of real money (fiat money), i.e. national currencies, while virtual money is not endorsed by any government. Virtual money can be either centralised or decentralised, and may or may not be convertible to real money. Convertible, centralised virtual currencies includes credit on websites. Non-convertible centralised virtual currencies include money in online games and virtual worlds. Convertible, decentralised virtual currencies include cryptocurrencies. Bitcoin is by far the best-known cryptocurrency, with 90% of the total market value of all cryptocurrencies.

In this study various models of money laundering are identified and described. The research results show that banking malware and ransomware profits are laundered in several different ways.

Money mules are often, but not always, involved in the laundering of banking malware profits. The electronic money is transferred from the account of the online banking account of the victim to an online banking account of a money mule. Subsequently, the money mule performs a so-called cash-out of the money as soon as possible at an ATM. This method of money laundering can partly be explained by the preference of criminals to have cash. However, from the police file analysis and quantitative analysis it also became clear that goods, services or bitcoins are purchased directly via the account of victims of banking malware, using their financial data. Criminals typically use multiple online services in this process.

The ransom that is demanded after infection with ransomware is usually in the form of online vouchers or bitcoins. Vouchers are generally credited to an online account with an e-wallet service, after which the money can be laundered digitally. It is also possible to sell the vouchers or directly pay for an online service. Criminals tend to use a combination of money laundering methods. The origin of bitcoins can be disguised using a mixing service. Mixing services allow bitcoins to be swapped for other bitcoins in exchange for a fee. The bitcoins can then be used for purchases or converted to other currencies via Bitcoin Exchanges. Finally, there are also illegal online service providers who are prepared to exchange digital and virtual payment systems for a fee.

In these models, the following actors can be identified as part of the money laundering process: (1) banks, (2) money mules, (3) money transfer offices, (4) Payment Service Providers (5) e-commerce, (6) voucher services, (7) e-wallet services, (8) Bitcoin exchanges, (9) mixing services, and (10) bitcoin dealers. The characteristics of these actors are described in this report to identify which parties are likely to appear in police investigations. By using the transaction data with regard to phishing and banking malware, it has been possible to map the characteristics of money mules in the Netherlands. The picture that emerges from the analysis of the data sets, shows that money mules are mostly young adults between 18 and 22 years from relatively poor neighbourhoods who allow criminals to use their debit cards. While these young adults in the relatively poor areas of the three major Dutch cities (Amsterdam, Rotterdam and The Hague) are overrepresented, money mules come from all municipalities in the Netherlands. Furthermore, there is an overabundance of juveniles with an Eastern European nationality.

This study shows that criminals (still) often opt to use cash. This is probably because cash can be moved quickly and anonymously. As a result, cash remains the instrument of choice for them to enjoy the proceeds of crime, including those of cybercrime. The scale of laundering cash therefore appears much greater than money laundering using new payment methods – which is the focus of this study. Whether that will change in the future, strongly depends on the developments of new payment methods and measures taken by companies and institutions to address money laundering. Police agencies and the Public Prosecution Service should maintain and further develop their expertise to combat money laundering via new payment methods.

Based on this research, it is recommended to consider regulating the Dutch Bitcoin exchanges. Dutch Bitcoin exchanges have already voluntarily taken an extensive range of measures to combat money laundering. However, with regulation they would, for example, also be able to report to the FIU, the financial intelligence unit, which can contribute to the detection of money laundering with virtual currencies. The enforcement of anti-money laundering regulations will remain a challenge, given that online payment services can offer their services worldwide and thereby may be located in jurisdictions with less strict regulations or a lack of supervision and enforcement. Moreover, there are also other online payment services that allow digital and virtual payment methods to convert, which settle in jurisdictions with more lenient regulation or poor supervision. It remains necessary that payment service providers take technical measures to detect and block suspicious transactions. Other parties, including citizens, should adopt technical measures to address malicious software, such as monitoring network traffic (including phishing emails). Citizens and organizations would thereby have to maintain a good cyber strategy and make regular backups of systems. It is also important to raise awareness among computer users about cybercrime, in particular ransomware, by providing more information.