BRILL
NIJHOFF

EUROPEAN JOURNAL OF CRIME, CRIMINAL LAW AND CRIMINAL JUSTICE 28 (2020) 121-152

brill.com/eccl

Laundering the Profits of Ransomware

Money Laundering Methods for Vouchers and Cryptocurrencies

Bart Custers
Professor of Law and Data Science, eLaw, Center for Law and Digital Technologies, Leiden University, the Netherlands
b.h.m.custers@law.leidenuniv.nl

Jan-Jaap Oerlemans
Professor of Intelligence and Law, Willem Pompe Institute for Criminal Law and Criminology, Utrecht University, the Netherlands
j.j.oerlemans@uu.nl

Ronald Pool
Senior Legal Counsel, ICTRecht, Amsterdam, the Netherlands
mail@ronaldpool.nl

Abstract

Ransomware is malicious software (malware) that blocks access to someone's computer system or files on the system and subsequently demands a ransom to be paid for unlocking the computer or files. Ransomware is considered one of the main threats in cybercrime today. Cryptoware is a specific type of ransomware, which encrypts files on computer systems. The ransom is often demanded in bitcoins. Based on desk research, a series of interviews, and the investigation of several police files, this paper investigates the modi operandi in which cybercriminals use ransomware and cryptoware to make profits and how they launder these profits. Two models, based on the payment of the ransom via vouchers and via bitcoins respectively, are identified and described. These methods allow criminals to launder profits in relative anonymity and prevent the seizure of the illegally obtained money.

Keywords

ransomware – cryptoware – bitcoins – cybercrime – money mules – money laundering

1 Introduction

Every computer user is familiar with the frustrations that a system failure may cause. When a computer crashes, a user is no longer able to access his files. Something similar, but usually more difficult to solve, happens when someone becomes the victim of *ransomware* or *cryptoware*. Ransomware is malicious software (malware) 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, which is called cryptoware and encrypts files on a computer.[1,2] Most ransomwares make intensive use of file encryption and can therefore be considered cryptoware.[3] In Figure 1, an example is shown of a message that victims of ransomware may get displayed on their screen. The message contains an instruction on how to unlock the system or the files, which is via the payment of the ransom. The ransom is usually the equivalent of a few hundred euros or U.S. dollars per victim[4] and is increasingly demanded via the payment of Bitcoin.[5,6] Although most victims are not familiar with Bitcoin at all, may not own any bitcoins and may never have paid with Bitcoin, the instructions include a clear and detailed description of what victims need to do in order to regain access to their files. Although police agencies in many countries urge victims not to pay the ransom, it may not be very surprising that some victims are nevertheless inclined to pay the ransom, especially when they do not have a back-up of their files.

1 This implies that there also exists ransomware that is not cryptoware. Usually these types of ransomware are so-called 'screenlockers'. A typical example is WinLock, which blocked access to computers by showing pornographic images and then requesting a ransom to be paid.

2 Leyden, J. (2010) Russian cops cuff 10 ransomware Trojan suspects, *The Register*, 1 September 2010. www.theregister.co.uk/2010/09/01/ransomware_trojan_suspects_cuffed/; McMillian, R. (2012) Alleged ransomware gang investigated by Moscow police, *PC World*, 10 March 2012. www.pcworld.com/article/204577/article.html.

3 Gazet A. (2008) Comparative analysis of various ransomware virii, *Journal in Computer Virology*, 6(1), 77–90. doi:10.1007/s11416-008-0092-2, p. 77.

4 According to one source, the average ransom amount in 2017 was the equivalent of 544 USD, see O'Brien, D. (2017) Internet Security Threat Report Ransomware 2017, Mountain View, CA: Symantec. https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-ransomware-2017-en.pdf, p. 17. Note that someone can be a victim of ransomware more than once.

5 Bitcoin is spelled with a capital letter when referring to the protocol, software and community, and with a lower when referring to units of the currency.

6 Europol (2016) *The internet organised crime threat assessment* (*iOCTA*). The Hague: Europol Police Office. See also Europol (2019) *The internet organised crime threat assessment* (iOCTA). The Hague: Europol Police Office.

FIGURE 1 Example of a blocking screen demanding a ransom, after the computer system is infected with ransomware. This example concerns the cryptoware known as CTB Locker.

For such victims, the value of the files can be much higher than the ransom that is to be paid. Imagine, for instance, the encryption of family pictures, personal letters and financial documents. Some of these files may be invaluable for people. Research shows that, in the Netherlands, approximately 10% of the people who report being a victim of ransomware actually paid the ransom in order to regain access to their files.[7] It may be obvious that paying the ransom does not guarantee regaining access to the computer system and the files on it,[8] but neither is it pointless, as unlocking may be part of the business model of cybercriminals: if they would never give the keys after the ransom is paid, it may be expected that the number of victims who actually pay the ransom would rapidly decrease.[9] Meanwhile, cooperating police agencies and IT

7 CSBN (2015) *Cyber Security Beeld Nederland 2017*. The Hague: Nationaal Cyber Security Centrum, p. 12.

8 A number of ransomware families did not even work properly, so decryption was not even technologically possible.

9 Note that this assumes perfect information. This is why, for instance, the cybercriminals behind the Cryptolocker ransomware put significant effort into 'customer support' so that people would tell each other that paying would be effective.

security companies also provide decryption keys for some families of (sometimes poorly designed) ransomware.[10]

In case the ransom is not paid or the criminals do not provide a key to unlock the computer or files, computer users may lose their documents and pictures stored on the infected computer systems and storage devices after the infection with ransomware. Companies and government agencies may have to temporarily suspend their activities if the office computers and networks are blocked. Cryptoware can also infect virtual hard discs, external hard discs, USB keys, and back-up discs. Organisations that have not made back-ups of their files may suffer considerable damage after a ransomware infection.

The threat of ransomware developed rapidly in recent years. In 2014, the threat related to police ransomware without encryption.[11] In 2015, non-encrypting police ransomware still accounted for a significant proportion of ransomware cases,[12] but in 2016, police ransomware had mostly vanished, except for on mobile devices, superseded by a growing variety of cryptoware.[13] By 2017, the number of ransomware families exploded, their impact significantly overshadowing other malware threats such as banking Trojans.[14] Industry reported that ransomware damages had increased fifteen-fold over the previous two years.[15] Furthermore, ransomware attacks appear to be more targeted with greater damages.[16] For example, in May 2017, the WannaCry ransomware rapidly infected up to 300,000 victims in over 150 countries, including some parts of the UK National Health Service, Spanish telecommunications company Telefónica, and logistics company Fed-Ex.[17] The WannaCry attack created significant societal anxiety, but yielded limited financial success for the cybercriminals, with less than 1% of the victims paying the ransom.[18] Despite the fact that WannaCry was not financially successful, it was a ransomware attack that caused one of the highest financial losses, estimates ranging from

10 See, for instance, https://nomoreransom.org/en/index.html.
11 Europol (2014) *The internet organised crime threat assessment* (*iOCTA*). The Hague: Europol Police Office.
12 Europol (2015) *The internet organised crime threat assessment* (*iOCTA*). The Hague: Europol Police Office.
13 Europol (2016).
14 Europol (2017) *The internet organised crime threat assessment* (*iOCTA*). The Hague: Europol Police Office.
15 Europol (2018) *The internet organised crime threat assessment* (*iOCTA*). The Hague: Europol Police Office, p. 17.
16 Europol (2019) *The internet organised crime threat assessment* (*iOCTA*). The Hague: Europol Police Office, p. 15.
17 Europol (2017), p. 19.
18 Europol (2017), p. 20.

hundreds of millions up to four billion USD.[19] Perhaps the most damaging ransomware attack was NotPetya, causing an estimated 10 billion USD in total damages in 2017.[20]

The damage that ransomware attacks can cause, does not always reflect the size of the profit cybercriminals make, as the WannaCry attack illustrates. Nevertheless, cybercriminals can make large amounts of money via ransomware and cryptoware.[21] With CryptoWall 3, for instance, a total of 325 million USD was earned within a period of two months.[22] An analysis of 35 ransomware families (not including CryptoWall) showed that, from 2013 to mid-2017, the minimum worth of the market for ransom payments represents USD 12,768,536 (22,967.54 BTC).[23] For the Netherlands, the country which this research focused upon, a growth of ransomware, cryptoware in particular, is predicted.[24] Yet, so far, in the Netherlands, there is only *one* successful prosecution, in which the perpetrators were actually sentenced. In 2015, the authors of the 'CoinVault' and 'Bitcryptor' ransomware were arrested.[25] These cybercriminals, two brothers aged 18 and 22 at the time, netted each a 10,000 Euro profit.[26] They were sentenced to 240 hours of community service in 2018.[27]

---

19 Berr, J. (2017) WannaCry ransomware attack losses could rearch $4 billion, CBS News, May 16th 2017. https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/.

20 Greenberg, A. (2018) The Untold Story of NotPetya, the Most Devastating Cyberattack in History, Wired, 22 August 2018. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/#.

21 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/; Van Eeten, M., Bauer, J.M. (2008) Economics of malware: Security decisions, incentives and externalities. Tech. Rep. OECD STI Working Paper 2008/1, OECD, Paris. http://www.oecd.org/dataoecd/53/17/40722462.pdf; Anderson R., Barton, C., Böhme, R., Clayton, R., Eeten, M.J.G. van, Levi, M., Moore, T., Savage, S. (2013) Measuring the Cost of Cybercrime. In: Böhme R. (eds) The Economics of Information Security and Privacy. Springer, Berlin, Heidelberg.

22 Beek, C. (2016) Ransomware: an insight to financial gain, Santa Clara (CA): McAfee https://blogs.mcafee.com/mcafee-labs/ransomwareinsight-financial-gain/.

23 Paquet-Clouston, M., Haslhofer, B., & Dupont, B. (2018). Ransomware Payments in the Bitcoin Ecosystem, paper presented at the 17th Annual Workshop on the Economics of Information Security (WEIS), June 2018, Innsbruck, Austria. See *arXiv preprint arXiv:1804.04080.*

24 CSBN (2017) *Cyber Security Beeld Nederland 2017.* The Hague: Nationaal Cyber Security Centrum, p. 28.

25 Reuters (2015) Dutch arrest two in "CoinVault" computer blackmail case, 17 September 2015. https://www.reuters.com/article/netherlands-cybersecurity-ransomware-idUSL5N11N1Z220150917.

26 CSBN (2017), p. 28.

27 Court of Rotterdam, 26 July 2018, ECLI:NL:RBROT:2018:6152.

Despite substantial research on the money laundering of profits in relation to traditional crime such as drug trafficking,[28] 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. in 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,[29] whereas research on the cybercriminals themselves 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 made from ransomware and cryptoware.

As with other crimes in which criminals aim to make profits, in the case of ransomware and cryptoware and other types of financial cybercrime it is necessary for the cybercriminals to launder the generated profits before they can spend it. When the profits are not laundered, its origins can easily be traced and this may increase the likelihood that the cybercriminals will be caught. In the case of ransomware and cryptoware, it is virtual money (sometimes vouchers, but usually Bitcoins) that has to be laundered in order to conceal its illegal origins and prevent the seizure of the profits.

28 Savona E (2005) *Responding to money laundering*, Amsterdam: Harwood Academic Publishers; Schaap C (1998) *Fighting money laundering*, London: Kluwer Law International.

29 Anderson KB (2006) Who are the victims of identity theft? The effect of demographics. *Journal of Public Policy & Marketing*, *25*(2), 160–171; Choi KS (2008) Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology*, *2*(1), 308–333; Harrell E and Langton L (2013) *Victims of identity theft, 2012*. Washington DC: Bureau of Justice Statistics; 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; 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; 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; 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; 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.

In this paper, we will provide an answer to the key question: "how are the profits of ransomware and cryptoware 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. The reason for this is probably that cybercriminals assume that cryptocurrencies may offer more anonymity (which is not always a correct assumption).[30,31]

The research results presented in this paper can provide further guidance to law enforcement when addressing money laundering via cryptocurrencies.

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 ransomware and cryptoware are and how they work. In the fourth section, we identify two different models that are used for the laundering of profits made from ransomware, based on payment of the ransom via vouchers and via Bitcoins respectively. In the fifth section, we discuss the limitations of this research and in the sixth section we provide conclusions.

2 Methodology

This research was requested by the Team High Tech Crime of the Dutch National Police, who wanted to have more background knowledge on the manner in which profits of financial cybercrime are laundered and the roles of the different actors involved in the money laundering processes. This research focused on two major types of financial cybercrime, i.e., banking malware and ransomware.[32] The results on banking malware were published in another paper,[33] while this paper focuses on ransomware.[34]

30 Note that only a few cryptocurrencies are (seen as) anonymous. Monero and to a lesser extent Zcash are branded/regarded as anonymous, but for instance Bitcoin has some issues regarding absolute anonymity. Biryukov et al. 2014. It may even be disputable whether Bitcoins may offer a greater degree of anonymity than traditional payments, but this may be the case for other cryptocurrencies, such as Monero.

31 Europol (2017), p. 11.

32 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.

33 Custers, B.H.M., Pool, R.L.D., and Cornelisse, R. (2018) Banking malware and the laundering of its profits, *European Journal of Criminology*, p. 1–18, DOI: 10.1177/1477370818788007.

34 Note that the methodology used was the same for both types of cybercrime, resulting in some overlap in both papers.

The question in this paper was answered by applying various research methods. Apart from desk research – focusing on existing relevant literature and online sources – a series of 20 interviews were conducted and a total of four police files with criminal cases were investigated.

The desk research focused on an analysis of available literature and relevant news articles 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 20 semi-structured interviews with (primarily 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 cryptocurrency 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 High Tech Crime Team) 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 that focuses on cyber security. One interviewee is affiliated with Mollie, a private company specializing in online payment methods.

The list of questions used for the interviews consisted of three major topics. The first topic concerned cybercrime, particularly ransomware and cryptoware, with questions on how the respondents view ransomware and cryptoware, the ways in which infections with malware take place, current and near-future developments, and the typologies of perpetrators. The second topic was in relation to 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 money laundering, and the role of online market places, money mules and other actors possibly involved in money laundering. The third topic concerned 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 the digital money laundering processes of the profits made from ransomware and cryptoware.

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 cybercrime and the use of Bitcoins. The information in the police files concerns information relating to digital money laundering methods and the characteristics of the actors involved. Three cases concerned banking malware, and one case concerned ransomware.[35] In all of the 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, called 'MegaServer', most of these digital payment methods were used.[36]

3 Ransomware and Cryptoware: How they Work

A thorough understanding of the workings of ransomware and cryptoware is required in order to understand how profit is generated. Cybercrime may be defined as "criminal acts committed using electronic communications networks and information systems or against such networks and systems".[37] This approach clearly distinguishes between tool cybercrimes (i.e., types of cybercrime that use electronic communication networks and information systems as a means to an end) and target cybercrimes (i.e., types of cybercrime that are targeted against electronic communication networks and information systems).[38] Ransomware can be both, depending on the goals of the cybercriminals. In this section, basic terminology and background information is provided on how computers can get infected with ransomware and cryptoware,

35 No other cases of ransomware were available at the time of this research.

36 For more on this case, see Custers et al. 2018. See also Court of Rotterdam, 2 October 2015, ECLI:NL:RBROT:2015:7038 (in Dutch).

37 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; Wall, DS (2007) *Cybercrime. The Transformation of Crime in the Information Age*. Cambridge: Polity Press.

38 Cf. 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; Parker DB (1976) *Crime by computer.* New York: Scribner, p. 17–22.

the different types of ransomware and cryptoware and cybercriminals. Furthermore, in relation to money laundering, it is explained how money mules, cash-out, cryptocurrencies and online payment service providers work.

3.1 *Malware Infections*

Computers can get infected with ransomware and cryptoware in different ways. The most prevalent way of infection is via phishing, including e-mail phishing, phishing on social networks, or spear phishing. Usually, computer users are persuaded to click on a link to a falsified website or to open an infected attachment of the e-mail message. When the attachment is opened, the malware installs itself and starts doing what it is supposed to do. When a link to a website is clicked on, the malware may be installed behind the screen.[39]

Next to the distribution of malware through e-mail messages, computers are also 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 anti-virus software.[40] Research has shown that, even though people take measures to protect themselves against online banking fraud, most victims are unaware of the phishing that they fell victim to prior to the incident.[41] People also report to have insufficient knowledge and skills regarding the safety and security of online banking and find it difficult to assess the extent to which protective measures are able to help them safeguard against fraudulent attacks.[42] About one third of malware infections occur via exploit kits versus two thirds via e-mail messages.[43] For a more detailed description of how ransomware works, we refer to existing literature.[44]

3.2 *Types of Ransomware and Cryptoware*

Ransomware is aimed at locking out victims from accessing (parts of) their computers and, in the case of cryptoware, the encryption of several files or the

39 This is referred to as a 'drive-by-download'. Note that this attack vector usually requires old or non-updated software (such as the browser or a plugin) to work.

40 Note that cybercriminals usually spread the malware before the anti-virus software detects it, which is why updates of the anti-virus software is very important.

41 Jansen and Leukfeldt (2016).

42 Jansen and Leukfeldt (2016); 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.

43 Cyber Threat Alliance (2015) *Lucrative ransomware attacks. Analysis of the cryptowall version 3 threat*, 2015, http://cyberthreatalliance.org/cryptowall-report.pdf, p. 6.

44 Orman, H. (2016) Evil Offspring: Ransomware and Crypto Technology, IEEE Internet Computing, Vol. 20, Nr 5, Sept-Oct 2016, p. 89–94. DOI: 10.1109/MIC.2016.90.

entire storage drive. The simplest forms of ransomware aim to lock the computer screen (a 'screen locker') or a phone; a problem that is often solved by restarting a computer. More advanced are infections with cryptoware in which some files or the entire storage drive is strongly encrypted by the malware.[45] Additionally, shared network directories on infected computer systems can get infected with the ransomware. Computers that are infected with cryptoware may still allow for the possibility to visit certain websites in order to make the ransom payment.[46]

The most commonly reported ransomware families are Curve-Tor-Bitcoin Locker (CTBLocker), Cryptolocker, CryptoWall, Cerber, Crysis, Dharma, Locky and SamSam.[47] CTB stands for Curve-Tor-Bitcoin[48] and is cryptoware that is distributed via e-mail messages in which the sender poses as a financial institution with a fake payment form in the attachment.[49,50]

The ransom used to be one Bitcoin. Since 2015, CTB Locker was revised and the ransom was increased to three Bitcoins. A remarkable feature is that this new version offered victims the opportunity to select five files on their computer for free decryption. This was probably meant to convince victims that the payment of the ransom is actually worth the money. However, it may also be that this serves to find out which files are most valuable for the victims. By the end of 2017, the Romanian police arrested five suspects related to the CTB

45 Cryptoware usually uses asymmetric encryption. This means that the key used for the encryption of files is a different key than the one used for decrypting the files. For each victim a unique key is generated and the key that can be used for decryption is solely controlled by the cybercriminals. Beek (2015), p. 16. It is also possible to encrypt only the first 10% of important files, which also effectively locks a computer.

46 For instance, CTB Locker allows making a connection via the Tor network to a payment website in order to pay the ransom. Tor stands for 'The Onion Router', which is free software for anonymous communications in which the IP addresses of computer users are obscured and the network communications are encrypted. See Dingledine, R., Mathewson, N., and Syverson, P. (2004) *Tor: the second-generation onion router*, Washington DC: Naval Research Lab.

47 Europol (2018), p. 16; Paquet-Clouston et al. (2018).

48 Curve stands for a cryptographic method based on elliptic curves, Tor stands for 'The Onion Router', free software for anonymous communications, and Bitcoin stands for the payment method for the ransom. CTB Locker is also known as Critroni.

49 Klijnsma, Y. (2015) The state of ransomware in 2015' *Blog Fox-IT*, 7 September 2015 http://blog.fox-it.com/2015/09/07/the-state-of-ransomwarein-2015/.

50 For a technical description of this malware, see Computer Incident Response Center Luxembourg, *TR-33 Analysis – CTBLocker/Critroni* (www.circl.lu/pub/tr-33/#ctb-locker-commands-andstates). Beek (2015), p. 18, indicates that CTB Locker was also disseminated via IRC-chat, peer-to-peer networks and news groups.

Locker ransomware. New forms of ransomware threaten to also publicly disclose sensitive personal information from the computers of victims.[51]

CryptoLocker is cryptoware that is targeted at Microsoft Windows and it appeared for the first time in the fall of 2013. Dissemination occurs via infected e-mail attachments. Although the malware can be removed relatively easily, the files remain encrypted in a way that is hard to decipher. The ransom in 2016 was 400 USD that was to be paid via prepaid cash vouchers (for instance, via MoneyPak or Ukash) or a similar amount in Bitcoins.[52] An estimated 28 million USD was extorted from victims with CryptoLocker.[53] During an international operation conducted by criminal investigation agencies in 2014 a database with private keys was discovered and then placed online for victims to recover their files.[54]

CryptoWall is one of the most profitable examples of cryptoware. This family of ransomware first appeared in June 2014 and several versions were later discovered. The initial ransom was 500 USD, to be paid in Bitcoins. Version 3 yielded approximately 325 million USD in a period of two months, and distributed over hundreds of thousands of computers, most of them in North America.[55]

The average amount that victims of ransomware pay, strongly depends on the type of victim. For individuals, this amount is approximately 250 USD in 2019.[56] The average ransom that companies pay when they become victim of a ransomware attack has increased significantly over the past years, with rates of 7,000 USD in 2018 and 13,000 USD early 2019. After that, the ransom prices have even tripled, resulting in average ransom amounts of 41,000 USD in late 2019.[57] Since the exchange rates of Bitcoin are very volatile and have skyrocketed the last few years, it is hard to provide clearer statistics on the ransom amounts. What is clear though, is an emerging diversification, in which cybercriminals increase or decrease the ransom amounts according to what they expect

51 An example of this type of mailware is Chimera, see https://blog.botfrei.

52 The initial amount of Bitcoins was 2 Bitcoins, but was later lowered by 0.3 Bitcoins to compensate for the fluctuating exchange rate of Bitcoins. Blue 2013.

53 Blue, V. (2013) CryptoLocker's crimewave. A trail of millions in laundered Bitcoin, *ZDNet*, 22 December 2013.

54 Krebs, B (2014) New site recovers files locked by Cryptolocker ransomware, *Krebsonsecurity.com*, 18 August 2014.

55 Cyber Threat Alliance (2015), p. 5.

56 Simoiu, C., Gates, C., Bonneau, J., Goel, S. (2019) I was told to buy a software or lose my computer. I ignored it: a study of ransomware, *USENIX Symposium on Usable Privacy and Security* (*SOUPS*) 2019. August 11–13, 2019, Santa Clara, CA, USA.

57 https://www.bankinfosecurity.com/ransomware-average-ransom-payout-increases-to-41198-a-13333.

victims are able and willing to pay.[58] Since many companies prefer not to disclose being victimised by ransomware, fearing it may harm their reputation, it becomes increasingly difficult to monitor the ransom amounts.

3.3 *Types of Cybercriminals*

Case studies show that there are at least two types of groups involved in cybercrime: low-tech generalists and high-tech specialists.[59] Although empirical criminological research into cybercriminal networks is scarce, there appears to be some variety in cybercriminal networks. Networks can further be characterised by the clear differences between 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.[60]

There seems to be a trend in which the organisations exploiting malware are becoming more professional and people in these organisations have specialized roles within this malware economy.[61] From 2016 to 2018, there were several cases in the Netherlands in which criminals were convicted for being part of an organised crime network that used malware for fraudulent transactions and subsequent money laundering.[62] In these cases criminals closely worked together, dividing amongst each other technical tasks (such as developing the

58 Europol (2019) *The internet organised crime threat assessment* (*iOCTA*). The Hague: Europol Police Office, p. 15.

59 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.

60 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; Kruisbergen, EW, Leukfeldt, ER, kleemans, ER, Roks, RA, (2018), 'Organised crime and IT. Empirical results of the fifth round of the Dutch Organised Crime Monitor', The Hague: WODC, Cahiers 2018–08 (full text only available in Dutch).

61 Bauer JM, Van Eeten MJG and Wu Y (2008) *ITU study on the financial aspects of network security: Malware and spam.* Genève: ITU, p. 8; 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; De Graaf, D, Shosha AF and Gladyshev P (2012) EDOLAB: Shopping in the Cybercrime Underworld. *Research Paper*, p. 1; Soudijn MRJ and Zegers BCHT (2012) Cybercrime and virtual offender convergence settings. *Trends in organized Crime*, *15*(2), 114–115.

62 Court of Zeeland, 29 June 2016, ECLI:NL:RBZWB:2016:3877 and Court of Rotterdam Rotterdam, 20 July 2016, ECLI:NL:RBROT:2016:5814, annotated by J.J. Oerlemans, *Computerrecht* 2016, no. 5, p. 268–277. See also Court of Rotterdam, 30 May 2018, ECLI:NL:RBROT:2018:4291. See also: https://www.wodc.nl/onderzoeksdatabase/2437-monitor-georganiseerde-criminaliteit-(vijfde-ronde).aspx.

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 organised criminal networks in which individuals gather online on a temporary basis to cooperate and commit cybercrimes.[63]

3.4 *Money Mules and Cash-out*

In some varieties of the models identified and described in this paper, cybercriminals recruit so-called money mules.[64] These are people who are willing to provide their bank account for a fee.[65] A typical fee is about 5% of the total amount that is transferred.[66] For instance, the recruiters may offer them a fee of 500 euros if they are willing to transfer 10,000 euros 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 a person other than the money mule performs the cash-out. This person is also referred to as the casher.[67]

After the cash-out, the next steps may consist of a wide variety of combinations of money laundering methods in order to conceal the illegal origin of the profits, including traditional money laundering methods. The money may once again be put in other bank accounts and then transferred to foreign bank accounts or it may be transmitted abroad via money transmitting services, spent on luxury goods or transferred abroad in cash. A typical method we encountered in police files and literature is via money transfers with Western Union or MoneyGram.[68] Relatively often the money is transferred to Eastern

63 Europol (2015) *The future of organised crime report 2015.* The Hague: Europol Police Office, p. 11.

64 Usually the recruiters are different people (i.e., not the cybercriminals themselves) who are specialised in and hired for these tasks. See Europol (2015) *The internet organised crime threat assessment* (*iOCTA*). The Hague: Europol Police Office, p. 10, and examples in Dutch case law: Court of Rotterdam, 2 October 2015, ECLI:NL:RBROT:2015:7041 and Court of Zeeland, 29 June 2016, ECLI:NL:RBZWB:2016:3877.

65 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.

66 Europol (2015) *Why is cash still king?* The Hague: Europol Police Office, p. 41; 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*, p. 52.

67 See examples in Dutch case law: Court of Rotterdam, 2 October 2015, ECLI:NL:RBROT:2015:7041 and Court of Zeeland, 29 June 2016, ECLI:NL:RBZWB:2016:3877.

68 Europol (2015) *Why is cash still king?* The Hague: Europol Police Office, p. 41; UNODC (2014), p. 20.

European countries, where local money mules collect the money, without knowledge of the illegal origin of the money.[69,70]

A big disadvantage for cybercriminals is the limited amounts of money that money mules can cash-out. Usually, the bank accounts of money mules are identified by the authorities and banks within one week and closed down. Laundering 10,000 euros requires a few money mules, but this practice is hard to scale to laundering 100 million euros.

3.5 *Bitcoin and Other Cryptocurrencies*

A description of what Bitcoin is and how the underlying blockchain technology works is beyond the scope of this paper. However, in order to describe how bitcoin laundering 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 yen. Exchanging bitcoins usually takes place via so-called cryptocurrency exchanges, which are online financial service providers that charge a small fee for each exchange. Cryptocurrencies usually have no offline, physical equivalent (i.e., no cash).[71] As mentioned above, ransomware and cryptoware usually generate profits for cybercriminals in bitcoins, which can be stored in a Bitcoin wallet that serves as a savings account from which cybercriminals can spend from time to time.[72]

Bitcoin wallets are anonymous to some extent, so this may conceal the illegal origin of the profits and prevent seizure. The use of cryptocurrencies can (if done correctly) make it hard to identify who the criminals are. However,

---

69 UNODC (2014), p. 20, 53-54; Krebs, B (2015) Inside the $100M 'Business Club' Crime Gang, *Krebsonsecurity.com*, 5 August 2015, p. 22.

70 "In nearly every case, the sequence of events is virtually the same: The organisation'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 organisation'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 2015:22).

71 Images of physical bitcoins can be found online. Some are artist impressions, other are Casascius coins, physical metal coins created by Casascius IMike Caldwell). The private key for the bitcoin is embedded inside the physical coin on a card. Once opened and used, the coin loses its value (apart perhaps from being a collector's item).

72 For more on Bitcoins scams, see Vasek, M., and Moore, T. (2015) There's No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits of Virtual Currency Scams. In *Financial Cryptography and Data Security*, January 2015.

Bitcoins are based on blockchain technology that uses a public ledger in which every transaction can be viewed. As such, all transactions from one Bitcoin wallet can be linked to each other. For this reason, cybercriminals may create several Bitcoin wallets, to inhibit linkability. When cybercriminals transfer bitcoins between their own accounts, this may indicate a link between these accounts.[73] Using advanced analysis of transaction data, pseudonyms may be clustered to several users.[74,75] 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 an investigator to establish the cybercriminal's real identity.[76] Also, via payment details in online shopping information may be retrieved, for instance, shipping addresses and e-mail addresses. Reluctant cybercriminals may use anonymisation software like Tor.[77] However, there are methods proposed and developed to couple Bitcoin addresses to IP addresses that circumvent these anonymisation techniques.[78] These methods do not target the Tor network itself, but aim to disable Tor connections to the Bitcoin network of the client.

According to Europol, Bitcoin is the most frequently used cryptocurrency by criminals, believed to be a consequence of familiarity within the customer base. However, there has been a more pronounced shift towards more privacy-orientated currencies.[79] Typically, Monero is becoming more popular,[80] because it focuses on fungibility, privacy and decentralization. Contrary to Bitcoin, Monero uses an obfuscated public ledger, not accessible to outsiders. Although Monero was beyond the scope of our research, it obviously is possible

73 Nakamoto S. (2008) Bitcoin: A peer-to-peer electronic cash system. *Bitcoin.org*.

74 Dutch case law shows that the software tool 'ChainAnalysis' is often used. See Court of Rotterdam, 19 December 2017, ECLI:NL:RBROT:2017:10225 and Court of Midden-Nederland 24 January 2018, ECLI:NL:RBMNE:2018:234 and ECLI:NL:RBMNE:2018:235.

75 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; Ron D and Shamir A (2013) Quantitative analysis of the full bitcoin transaction graph. *Financial cryptography and data security*, *7859*, 6–24; Paquet-Clouston et al. (2018).

76 Reid F and Harrigan M (2013) An analysis of anonymity in the bitcoin system, S*ecurity and privacy in social networks*, 197–223; Meiklejohn et al. (2013); Paquet-Clouston et al. (2018).

77 https://www.torproject.org/.

78 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.

79 Europol (2019), p. 54.

80 Europol (2017), p. 1.

for cybercriminals to exchange Bitcoin to Monero and back to further conceal the origins of ransomware profits.

3.6 *Online Payment Service Providers*

Payment service providers facilitate payments on a large scale for online service providers, such as online stores. A payment service provider aggregates different payment methods and acts as an intermediary between a customer, an online store and a financial institution, such as a bank. In this way, an online store can offer many different payment methods with only one (technological) connection with a payment service provider. With these connections, payments become possible via, for instance, iDeal,[81] credit cards and PayPal, but also with virtual currencies like Bitcoin and vouchers like Paysafecards.[82] The payment service providers facilitate the payments between consumers, online stores and banks, but not (at least not as far as they are aware of) money laundering activities (apart from some criminal payment service providers). Typical examples of payment service providers are Adyen, Mollie, Neteller, PayPal, Paysafe Group, Skrill and WebMoney. Also, many regular banks offer these services, although they usually do not include exchanges to and from cryptocurrencies like Bitcoin.

Some payment service providers also allow users to hold a balance in a personal account, usually referred to as an e-wallet, online wallet or digital wallet. Such accounts are only accessible via the Internet. Contrary to a bitcoin wallet, such e-wallet can also contain other types of currencies, sometimes several currencies at the same time. Typical examples of e-wallet services are PayPal and WebMoney. With the help of an e-wallet service, payments can be made at connected online stores and transactions can be made to or from other users of the e-wallet service. When the online wallet is connected to a bank account, it is also possible to transfer money to and from the bank account. However, for many of these services, no bank account or credit card is required. Connecting an e-wallet to a bank account can be an additional verification method for the service provider and can be a source of information for criminal investigation authorities in the case that e-wallets are used for money laundering purposes.

81 iDeal is an e-commerce payment system widely used in the Netherlands, based on online banking.

82 Paysafecard is a prepaid online payment method based on vouchers with a 16-digit PIN code.

4 Laundering Ransomware Profits

Once the cybercriminals have generated profits with ransomware and cryptoware, 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,[83] but the essence of it is to transfer money and to avoid the attention of law enforcement and tax authorities. This can be achieved by avoiding policing technologies.[84]

In many situations, money laundering of cybercriminal 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 (including to and from cryptocurrencies such as Bitcoin to Monero to USD), transfers to other countries and investments in real estate or other assets. 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.[85] Typically, criminals split transactions to smaller amounts in order to avoid suspicion and transfer money via countries with less strict rules and supervision. 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.[86] 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.[87] Fictitious gambling profits can be created by suggesting that profits originated from gambling

83 Unger B (2006) *The scale and impacts of money laundering.* Cheltenham: Edward Elgar, p. 30–35; Gelemerova, L (2011) *The anti-money laundering system in the context of globalisation: A panopticon built on quicksand?*, Nijmegen: Wolf Legal Publishers, p. 59.

84 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.

85 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.

86 Europol (2015) *Why is cash still king?* The Hague: Europol Police Office, p. 18.

87 FATF (2008) *Best Practices on Trade Based Money Laundering*; Financial Action Task Force. Paris: FATF-OECD, p. 1.

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 using fake names or the names of family members) and then lend money to themselves. This can also obfuscate financial trails.

All of these methods, or combinations thereof, can also be used for laundering the profits of cybercrime. Organized crime groups tend to invest a great deal of energy in diversifying money laundering procedures, from primitive to very complex schemes.[88] 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.[89] In most types of traditional crime, this is not very difficult because the profits are already in cash, but the profits of ransomware and cryptoware are usually in the form of vouchers or cryptocurrencies. Bitcoin is most common here, but Monero is gaining popularity because it provides more anonymity via an obfuscated public ledger.[90] The advantages for cybercriminals of Monero's anonymity can Bitcoin's popularity can be combined via exchanging Bitcoin to Monero and back to Bitcoin again during the money laundering process.

The first step for cybercriminals to launder their profits is to transfer the money from the environment where the ransom payment was made to where they want to have it. This may also involve methods other 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 ransomware and cryptoware that we identified in our research, based on the available literature, the police files and the interviews conducted.

Our research shows basically two models for laundering the profits of ransomware. The first model is based on money laundering via vouchers, the second model is based on laundering of Bitcoins. Basically, the cybercriminal's choice of models depends on the way in which the ransom is demanded. In the past, several types of ransomware asked for payment via vouchers, but in recent years this has changed – currently, most types of ransomware request

88 Barone R. and Masciandaro D. (2011) Organized crime, money laundering and legal economy: theory and simulations, *European Journal of Law and Economics*, 32: (1), 115–142. https://doi.org/10.1007/s10657-010-9203-x, p. 119.

89 Europol (2015) *Why is cash still king?* The Hague: Europol Police Office, p. 9.

90 Europol (2018), p. 58 and Europol 2019, p. 54.

Bitcoin payments.[91] Other forms of payments, such as through an online banking transfer or in cash are rare. Payments via online banking can rather easily be traced. In principle the use of money mules could avoid a direct trace to the cybercriminals, similar to what is performed by banking malware (malicious software that aims to steal money from victims via manipulated bank transfers in online banking).[92] However, in the case of ransomware (and contrary to banking malware), the victim is immediately aware of his or her victimisation, even before any electronic money is transferred from the victim's bank account to the money mule's bank account. This leaves no time for money mules to quickly cash-out. The use of cash depends on geographic location, which would prevent world-wide profits and would also directly lead to the cybercriminals or their accomplices.

In the models presented in this section we distinguish two stages in the money laundering process. In practice, these stages may be hard to distinguish, but they are important from a legal perspective. The first stage consists of the very first step the cybercriminals take (i.e., the first transfer of the money) after the ransom has been paid. This first step is important to distinguish from any subsequent steps, as this qualifies as money laundering from a legal perspective, irrespective of any subsequent steps. Extracting money from victims via ransomware constitutes a cybercrime, but does not qualify as money laundering. Only after actions are taken to process or transfer the profits, this may legally constitute money laundering. In the second stage, further concealment of the criminal origin of the ransomware profits takes place. This may consist of (long chains of) different money laundering methods. This stage is important for criminal and financial investigative authorities to find out whether particular funds have an illegal origin (trace backwards in case the money is suspicious) and to find out where the criminal profits have gone (trace forwards in order to seize the criminal profits). All steps in the second stage are not really important for (further) qualifying the behaviour or actions as money laundering, but have practical importance, as these actions may complicate criminal investigations.

4.1 *Laundering Via Vouchers*

Cybercriminals can ask for payment of the ransom via vouchers. Vouchers can be purchased via different physical stores. A typical example of this is a Paysafecard (formerly Ukash). Other examples are gift cards for iTunes or

91 Europol (2017), p. 11; Cyber Threat Alliance (2015), p. 4.

92 Custers et al. (2018).

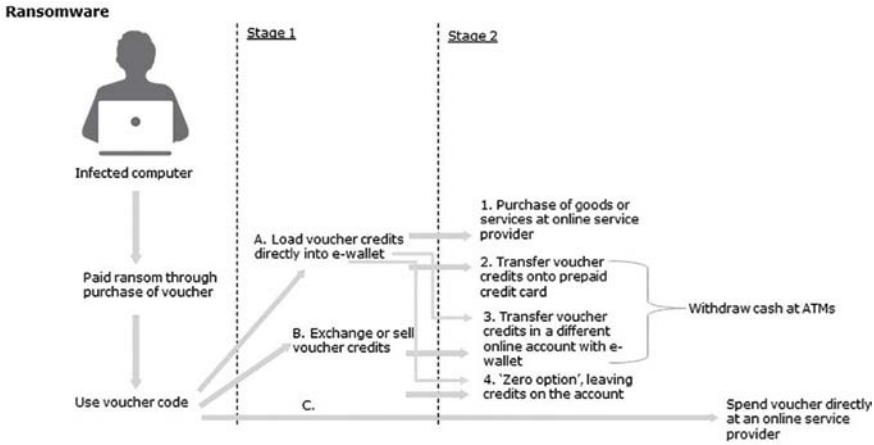

FIGURE 2 Model for the money laundering of ransomware and cryptoware profits via vouchers.

Amazon.[93,94] The model for the money laundering of ransomware and cryptoware profits via vouchers is shown in Figure 2.

The first stage deals with the process after a victim has paid the ransom via vouchers to the cybercriminals. Legally speaking, this already constitutes a money laundering activity and, therefore, entails criminal liability. The second stage deals with the further concealment or spending of the virtual money. In most cases, the vouchers are exchanged for cash via a cash-out.

4.1.1 Stage 1

After the ransom is received by payment through a voucher, the organisation behind the ransomware can choose from a variety of next steps. The interviews with financial crime investigators showed that two major approaches can be distinguished: (A) putting the value of the voucher into an e-wallet account, or (B) exchanging or selling the voucher. A third approach (C) is not transferring the voucher, but directly spending it at some online service provider or store.

When putting the voucher credits into an online account as in the approach in (A), several digital payment service providers can be used. Typical examples are Skrill and Neteller. In this way, it is possible to transform Paysafecard vouchers into e-wallet credits of online payment services. Our research of police files

93 Abrams, L. (2016) Decrypted: Alpha Ransomware accepts iTunes Gift Cards as Payment, BleepingComputer, 30 April 2016. https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-ransomware-2017-en.pdf.

94 Note that this type of payment is easily traceable compared to laundering using Bitcoins.

showed that suspects often use many different services for laundering cybercrime profits, in order to spread the money (in case it gets confiscated) and to further conceal the criminal origins of the money. Often, foreign online payment service providers and voucher systems are combined for this. In one police file, service providers such as PayPal and Western Union, Bitcoins, and vouchers were all used. Further concealment actions take place in the second stage (see below). Note that the authorities can request the details of transactions which involved a voucher from the issuing organisation. If this is successful, it can be revealed where a voucher was issued, which, in turn, can provide a clue in a criminal investigation. In case a money mule, face-to-face offline transfer or a fake identity was used, this lead may turn out to be a dead end.

The vouchers can also be exchanged or sold for its 'real money' value as in (B). Selling vouchers usually takes place on criminal online platforms. Our interviews showed that vouchers are sold via advertisements on the darkweb[95] in exchange for dollars or cryptocurrencies, such as Bitcoin. This is also a method to further conceal the origins of the money. On online platforms, it is possible to exchange Paysafecards for regular gift cards. Selling vouchers via an online service is also possible. Several legitimate services, such as Zeek,[96] offer the option to buy and sell vouchers in exchange for cash.

In some cases, such as in (C), vouchers are not transferred, exchanged, or sold, but used for direct spending. This is possible at online service providers or stores that accept such vouchers as a payment method. If the purchased products were delivered directly to the cybercriminals, it would be easy to trace them, for instance, via delivery addresses or order details. That is why this approach usually includes money mules as intermediaries, who deliver the products to the cybercriminals, sometimes via a chain of intermediaries. Direct spending can be either the final goal of the cybercriminals that want to purchase expensive luxury items or it can (still) be an intermediate stage, for temporary storage of the profits or another step in further concealing the origin of the profits.

4.1.2 Stage 2

In the second stage, the profits are further laundered by the subsequent concealment or the spending (or both) of the exchanged money. Our research of literature and police files showed a plethora of money laundering methods. Often a combination of methods is used. Here, we discuss four methods that

95 The deep web consists of websites on servers that are not indexed and, therefore, cannot be found by regular search engines like Google and Yahoo. The dark web is the part of the deep web that can only be accessed with special technologies, in this case via Tor.

96 www.zeek.me.

are often used in combination with other (more traditional) methods for money laundering.

A first method (A => 1) is the direct spending of a voucher at an online service provider or store, where they can be directly exchanged for products or services. In a recent case, this method was used to exchange the credits on a Paysafecard into mobile phone credit.[97] Similar to method (C) described above, direct spending can be either the final goal or an intermediate stage in the money laundering process. For instance, when accumulating money on mobile phone credits, it may be expected that this is not the final goal, but merely a temporary storage of the profits.

A second method (A => 2) is to transfer the voucher credits from an account with a connected e-wallet to prepaid credit cards. Many online payment service providers offer prepaid credit cards to easily spend money. There are also service providers that issue completely anonymous prepaid credit cards, sometimes with very high credit limits or no credit limits at all.[98] The prepaid cards can be used to withdraw cash at regular ATMs.

A third method (B => 3) is quite prevalent and includes transferring the voucher credits to an online account with a connected e-wallet. This e-wallet is then used to purchase products or services at online stores. In this way, the value of a voucher can be spent. However, the credits can also be converted into other currencies, for instance, into dollars or euros and then use a cash-out. Voucher credits can also be loaded from one e-wallet to another (A => 3).

A fourth method (B => 4) is the so-called zero option, i.e., doing nothing with the credits and leave them in the account as if it were a savings account. When the money is sufficiently laundered (i.e., when the illegal origin of the money is sufficiently concealed), the cybercriminal can start spending the money in the legal economy. Usually this is only the case after the money has been transferred many times from one payment service to another and exchanged from one payment method to another. Europol underlines that criminals can easily transfer money from one online payment service to another.[99] This can take place via online platforms or using several exchanges. Exchange services and online payment service providers can also be used to transfer money to PayPal or Western Union.[100] Another option to directly load the voucher credits into an e-wallet and then just leave the credits there (A => 4).

97 This accumulated to hundreds of thousands of euros in Skype credits.

98 UNODC (2014), p. 16.

99 Europol (2015) *The future of organised crime report 2015*. The Hague: Europol Police Office, p. 47.

100 UNODC (2014), p. 70.

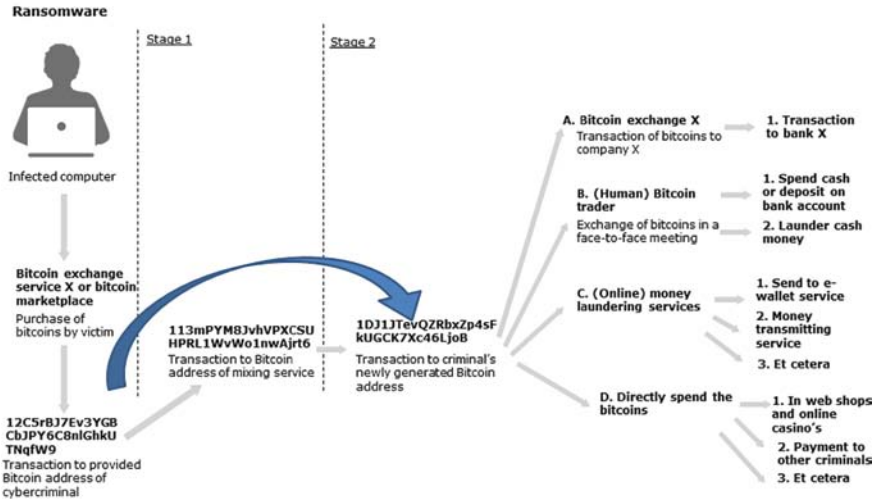

FIGURE 3 Model for the money laundering of ransomware and cryptoware profits via bitcoins.

4.2 *Laundering Via Bitcoins*

The current trend is to ask for payment of the ransom in Bitcoin rather than in vouchers. In the second model, cybercriminals ask for a transfer of bitcoins to other Bitcoin addresses or a series of Bitcoin addresses. After such a transfer, a cash-out may follow, but not always. This model consists of two stages and is shown in Figure 3. In the first stage, the origin of the money is concealed with the use of so-called mixing services, which are used to conceal the illegal origin of the Bitcoins. From a legal perspective, the use of mixing services is very likely already a concealment action that qualifies as money laundering. In some cases, the first stage is skipped. In the second stage, the Bitcoins are transferred to the Bitcoin addresses of one or more intermediaries, after which they end up with the cybercriminals for spending.

4.2.1 Stage 1

Before bitcoins are transferred to the Bitcoin address(es) of the cybercriminals, regardless of whether intermediaries are used, the criminals can choose to use so-called mixing services.[101,102] These are online services that exchange bitcoins for bitcoins, against a fee. The obvious goal is to make using bitcoins

101 Europol (2017), p. 63.

102 Mixing services are also referred to as tumbling services or blending services or, in short, mixers, tumblers and blenders.

more anonymous.[103] After a user has submitted the bitcoins, the mixing service collects bitcoins from different sources (or even mines completely new bitcoins)[104,105] and pays them back to the respective user on a different account.[106] A typical fee is 3%.[107] Mixing services are usually only accessible via Tor to ensure the anonymity of the service provider and its clients.[108] This also conceals the jurisdiction in which the service providers are located or in which they are offering their services. Recent case law in the Netherlands, suggests that cybercriminals indeed use mixing service to make Bitcoin transaction more anonymous.[109]

The way in which mixing services operate is successful because the origin of the bitcoins is concealed in such a way that the bitcoins cannot be traced from the victim to the cybercriminals and vice versa. It is likely that the use of mixing services for bitcoins with criminal origins qualifies as money laundering in most jurisdictions.[110] Via the payment of fees and the purpose of the service (i.e., the concealment of the origin of bitcoins obtained via cybercrime), intent can probably be proven.[111] Seizure of servers that host mixing services could be very valuable in criminal investigations, as the data stored on such servers

103 This may seem at odds with the concept of blockchain technology upon which cryptocurrencies are based. The essence of a blockchain is that it is a transparent ledger open to everyone. Hence, all Bitcoin transactions can be traced to the Bitcoin addresses of senders and receivers, including the amounts transferred and the number of Bitcoins on each account. The anonymity is in the (usually non-transparent) link between the Bitcoin address and the owner of the Bitcoin address.

104 Wegberg, R. van, Oerlemans, JJ, and Deventer, O van (2018) Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin, *Journal of Financial Crime*, Vol. 25 Issue 2, p. 419–435, https://doi.org/10.1108/JFC-11-2016-0067.

105 In fact, a whole chain of transactions is executed: Bitcoins are not exchanged on a one-to-one basis, but in a large pool of Bitcoins, hence the term mixing.

106 See, for instance, Deepdotweb, 'Introducing Grams Helix: Bitcoins Cleaner', 22 June 2014. www.deepdotweb.com/2014/06/22/introducing-grams-helix-bitcoins-cleaner.

107 Möser M, Böhme R and Breuker D (2013) An inquiry into money laundering tools in the bitcoin ecosystem, *Proceedings of the 2013 eCrime Researchers Summit*, 1–14, p. 4.

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

109 See Court of Noord-Holland. 10 March 2017, NL:RBNHO:2017:1940, Court of Midden-Nederland, 17 October 2017, ECLI:NL:RBMNE:2017:5716, Court of Midden-Nederland, 24 January 2018, ECLI:NL:RBMNE:2018:234 and Court of Midden-Nederland 10 April 2018, ECLI:NL:RBMNE:2018:1184.

110 See, e.g., FIU Netherlands 2017.

111 Mixing services like BitLaundry are very transparent about the purposes of the service they offer, see Möser et al. 2013, p. 3.

might reveal data that enables connecting bitcoin transactions, which may contribute to identifying the original senders.[112]

4.2.2 Stage 2

In stage two of this model, the bitcoins finally arrive in an account of the cybercriminals, usually via one or more intermediaries. In this stage, the cybercriminals further exchange the bitcoins or spend them.[113] Four types of further laundering and/or spending in this model are described here.

A first method (A) directly exchanges the bitcoins into electronic money via a cryptocurrency exchange for fiat currencies such as euros or dollars. When using the services of a cryptocurrency exchange, the Bitcoins are transferred to a specified Bitcoin address of the cryptocurrency exchange. Next, the same amount in euros or dollar, minus any fees, is transferred to an online banking account specified by the client. This process can be completed within one day.[114]

A second method (B) is the use of a (human) Bitcoin trader, for example by using a platform such as 'LocalBitcoin'.[115] These are people who are willing to exchange Bitcoins in a face-to-face meeting, for instance at a McDonald's or Starbucks. Our research of the police file and the interviews conducted show that such face-to-face meetings do take place between Bitcoin traders and their clients.[116] During such meetings, the Bitcoin trader accepts Bitcoins on the spot (both parties bring a laptop or other device to make the transfer) and hands over the agreed amount of fiat currency either in cash or by transfer to an online banking account of the client. In this model, the client is either one of the cybercriminals behind the ransomware or some intermediary. The fees for these transactions are relatively high, probably due to the risks and efforts involved for the Bitcoin traders.

A third method (C) is the use of online money laundering services. These are online criminal service providers (anonymous and via the dark web) that offer to launder the money. After transferring the Bitcoins to such a company,

112 Obviously, these services may have taken measures to regularly delete their logs.

113 Similar to the previous model with vouchers, the criminals can choose to keep the Bitcoins in their account as if it were a savings account. A disadvantage is that the exchange rate of Bitcoins may be very volatile and thus their total value may heavily fluctuate.

114 In case of large amounts of money, banks may block transfers or may further investigate them which may cause delays.

115 See also FIU Netherlands (2017), 'The bitcoin trader a facilitating role in the cash out of criminal proceeds', Anti Money Laundering Centre, De Bilt; Pauet-Clouston et al. (2018). For case law, see for example, Court of Rotterdam 19 December 2017, ECLI:NL:RBROT:2017:10225.

116 See also Kruisbergen et al. (2018).

a client can choose how he or she wants the money returned via legitimate online financial payment service providers like PayPal, Western Union and MoneyGram.

During our interviews, respondents mentioned the use of exchanging Bitcoins into virtual currencies like WebMoney.[117] Particularly cybercriminals from Eastern Europe would allegedly use WebMoney for services provided to each other (Europol 2016:16). The use of WebMoney did appear in the police files we investigated, but not in relation to ransomware. The interviews showed, however, that the use of WebMoney did appear in ransomware cases investigated by Europol. Europol suspects that WebMoney is used on a (much) larger scale than the statistics provided by national police agencies suggest.[118] During the interviews, it was also mentioned that prepaid cards are used relatively often. Other research confirms this.[119] It is also possible to have the value of the virtual currencies returned via a prepaid credit card which, in turn, can be used to cash-out at a regular ATM.

A fourth method (D) is to directly spend the bitcoins. Bitcoins can be spent in online casinos, on hosting services and during online shopping. Additionally, an increasing number of brick-and-mortar businesses, like pubs, restaurants and shops accept Bitcoin as a payment method. In this way, cybercriminals can easily spend their (laundered, anonymised) bitcoins on products and services. Obviously, money mules are often needed to conceal the link to the identity of the cybercriminals. An obvious choice (which also appeared in one of the police files investigated) is to spend Bitcoins when purchasing criminal products (such as guns or drugs) and services (such as the latest malware or hosting services) offered online by other criminals.[120] A Europol report on online payment methods in cybercrime cases states that 33% of the transactions between criminals is made in Bitcoin.[121] Some law enforcement agencies also report that street level drug dealers are converting to cryptocurrencies for payments.[122]

117 See also Odinot, G., Verhoeven, M.A., Pool, R.L.D. & Poot, C.J. de (2017). *Cybercrime, Organised Crime and Organised Cybercrime in the Netherlands. Empirical Findings and Implications for Law Enforcement*. Den Haag: WODC.

118 Europol (2016), p. 16.

119 Odinot et al. (2017).

120 This is also referred to as the Crime as a Service (CaaS) business model, Europol (2017), p. 58.

121 Europol (2016), p. 11

122 Europol (2017), p. 62.

5 Discussion

The implications of our findings are both theoretical and practical in nature. Section 5.1 discusses the theoretical implications and Section 5.2 discusses the practical implications. Section 5.3 discusses the limitations of this research.

5.1 *Theoretical Implications*

At a theoretical level, the generally accepted model for money laundering consists of three stages:[123]

- Placement: the illegal profits are placed into the financial system
- Layering: a sequence of sometimes complex financial transactions is created in order to conceal the illegal origins
- Integration: the illegal profits now seem legal and are invested in the legal economy

This traditional model of money laundering assumes that all three stages are passed before the money laundering is completed and the illegally obtained profits are finally part of the legal economy. However, when looking at the methods for money laundering in this paper, the goal of money laundering (enjoying the profits of crime) can also be achieved without going through all these three stages. Particularly the placement stage can often be skipped,[124] since the profits are already in the financial system, assuming cryptocurrencies are part of the financial system. If it is assumed that cryptocurrencies are not part of the financial system, then the three stages model is even more difficult to apply to cryptocurrency laundering. For instance, transferring bitcoins obtained via ransomware to different wallets is legally considered money laundering, but would not be covered by this traditional money laundering model, since all this is beyond the scope of the financial system.

The three stages model also suggests a clear final stage of the money laundering process. Our research results show that in the case of cryptocurrency laundering, there does not really need to be such a final stage. Sometimes cryptocurrencies or credits are simply stored somewhere online and used again when needed. The same could be argued of course with illegally obtained cash that is stored in someone's house, but spending large amounts of cash is more complicated that spending large amounts of cryptocurrencies, now that cryptocurrencies are more and more accepted everywhere.

123 Unger, B. (2007). *The scale and impacts of money laundering.* Cheltenham: Edward Elgar.

124 Tropina, T. (2014). Fighting money laundering in the age of online banking, virtual currencies and internet gambling. *ERA Forum*, 15(1), 69–84.

Altogether, we recommend to abandon the traditional three stages model for money laundering involving cryptocurrencies, because it does not aptly describe current practices of cryptocurrency laundering such as described in this paper. This traditional model never was in line with the legal perspective on money laundering anyway: in most countries only one of the three stages is already sufficient to qualify as money laundering.

5.2 *Practical Implications*

Practical implications of our research findings mostly relate to law enforcement and to the legislator. The amounts of money laundered via cryptocurrencies are still (very) small in comparison with money laundering via cash. As such, law enforcement should not redirect all its efforts to cryptocurrencies. However, not addressing this at all, may have as a result that cryptocurrencies become (even) more attractive for criminals. In order to better address cryptocurrency laundering, law enforcement should further familiarize itself with this topic. Law enforcement agencies in many countries increasingly have specialised departments dealing with cybercrime and also specialised departments dealing with money laundering. However, when dealing with cryptocurrency laundering, the expertise of both departments needs to be combined. In other words, further specialisation or combination of both expertises may be required.

Looking at our research results, it may be suggested that law enforcement can address cryptocurrency laundering better when not only looking at the beginning of the money laundering chains, i.e., the high profile ransomware cases that cause large damages and attract lots of media attention, but also at the middle parts and the ends of the laundering chains, where large amounts of money are processed. However, in the current situation it is quite hard to do this, because the legal frameworks do not always allow this.

A clear recommendation for the legislator, therefore, is to consider regulating Bitcoin exchanges.[125] In the European Union, the 5th Anti-Money laundering directive obliges EU member States to impose 'Know Your Customer' obligations and monitoring obligations for Bitcoin exchanges and wallet providers to combat money laundering.[126] EU Member States must implement the directive in their judicial framework. Most users need Bitcoin exchanges for transferring their cryptocurrencies to and from fiat currencies. Regulating these

125 Bitcoin exchanges is the regular term used for all cryptocurrency exchanges.

126 Directive 2018/843/EU of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, OJ L 15.

companies could include obligations to notify the national Financial Intelligence Units (FIU) in case of irregular or suspect transactions. A similar system already applies to regular banks and financial institutions, and puts supervisory authorities in a position to better monitor money laundering. Such a system would allow law enforcement better overview and insight in suspicious transactions. It may be useful both for guiding criminal investigations and collecting evidence.

When money laundering practices via cryptocurrencies keep increasing, and we think it is reasonable to expect this, it may also be recommended to further regulate cryptocurrencies, not necessarily by prohibiting them, which would be overregulation, but to bring cryptocurrencies within the scope of regular currencies and financial legislation. Cryptocurrencies currently are not considered money in most jurisdictions, which means they are not subjected to financial legislation, including anti money laundering legislation. Considering cryptocurrencies as money would also bring them further into scope of financial supervisory authorities, which means that not only law enforcement, but also other authorities would focus on these problems.

5.3 *Limitations*

The analysis of money laundering methods of ransomware and cryptoware 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 a significantly larger number of cases become available, quantitative analyses may become possible and perhaps even predictive models can be developed that uncover hidden patterns.

Second, the focus on expert interviews and cases implies that the scope of this research is limited to forms of ransomware, cryptoware and money laundering known to and investigated by law enforcement. The number of these cases is very limited. There is no knowledge available (nor is it included in this research) about money laundering methods that remain invisible to law enforcement, for instance, because particular crimes are not reported, are beyond their jurisdiction, or because some crimes take place on the dark web, which is not publicly or easily accessible for law enforcement officers. For this

reason, it may be helpful for law enforcement to not solely focus on cybercrimes, but also on suspicious money transfers (see next section).

Third, this research specifically focused on the national context in the Netherlands. As such, the results are difficult to extrapolate 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 the jurisdictions of law enforcement agencies, there may be differences in the ways cybercriminals and cybercriminal networks operate in different countries.

6 Conclusion

In this paper we answered the question: how are the profits of ransomware and cryptoware generated and subsequently laundered? Based on how the profits of ransomware are generated, i.e., in the form of vouchers or Bitcoin, we identified two models that are used to launder the ransomware and cryptoware profits (Figure 2 and Figure 3 respectively). When examining these models more closely, they consist of several different methods, including transferring, exchanging or spending the vouchers or cryptocurrencies. These methods can be used in combination with each other and/or in combination with traditional money laundering methods. From the perspective of cybercriminals, it is clear that cash is, in the end, often the most preferable option, because of its non-traceability and anonymity. However, the profits of several types of cybercrime do not come in cash. Particularly in ransomware, the profits come in the form of vouchers or cryptocurrencies, which often need some kind of processing in order to obfuscate their origin. Hence, the form in which ransomware profits are made, necessitate cybercriminals to rely, at least partially, on non-traditional methods of money laundering.

Furthermore, the use of cash is inefficient in a digitized, international context. Large amounts of cash cannot always be easily transferred across borders and exchanging large amounts of cash to different currencies can be costly and complicated. In essence, the problem with cash is that it is not efficient for dealing with large amounts of money, as large amounts of cash can attract unwanted attention and may easily rise suspicion.

As a result of the need to process cryptocurrency profits and the limitations of cash from the perspective of cybercriminals, money laundering via cryptocurrencies is increasing. It is to be expected that the use of the cryptocurrency laundering methods described in this paper will further increase in the near

future, especially if law enforcement is not adequately addressing these methods, something that seems to vary across jurisdictions.

Although our research focused on the laundering of ransomware profits, we think that our findings can also be useful when looking at laundering profits of other types of (cyber or non-cyber) crime. Our research focused on ransomware, because its profits being vouchers or cryptocurrencies necessitate laundering cryptocurrencies. However, cryptocurrencies can also be attractive for other criminals and, therefore, be used as a tool in (part of) a money laundering process. For instance, large amounts of profits made by organized drugs cartels require laundering and, in some stages, cryptocurrencies may be useful for criminals to process these profits, for instance, to transfer the money across borders or to obfuscate its illegal origins.

Furthermore, this research focused mostly on Bitcoin, but most of it applies to any cryptocurrency. The ways in which Bitcoin is used for money laundering described in this paper are in essence no different from situations in which Monero, ZCash, Dash, or any other cryptocurrency could be used for the same purposes. The most important differences are in the popularity of specific cryptocurrencies (are they accepted or not) and the level of anonymity they offer or seem to offer. We focused on Bitcoin in this research because of its popularity and relatively high levels of acceptances, but this dominant position of Bitcoin may be taken over by other cryptocurrencies in the future.

Future research should 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 ransomware and the money laundering of cybercrime profits. There already exists research on investigating cybercrime[127] and the use of new technologies in policing,[128] but knowledge on the usefulness and effectiveness of these policing methods is limited. Finally, further research may be needed on how to further empower people to safeguard themselves against cybercrime. From a user perspective, awareness of fraudulent schemes and training in how to apply protective measures are critical to be kept safe and secure from ransomware and cryptoware attacks.[129]

127 Oerlemans JJ (2017) *Investigating cybercrime*, Leiden: Meijers Research Institute. Amsterdam: Amsterdam University Press.

128 Custers and Vergouw (2015). Pool R.L.D & Custers B.H.M. (2017) The Police Hack Back: Legitimacy, Necessity and Privacy Implications of The Next Step in Fighting Cybercrime, *European journal of crime, criminal law and criminal justice* 25(2): 123–144.

129 Jansen and Leukfeldt (2016); 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.