On Locky Ransomware, Al Capone and Brexit

John MacRae[1,2] and Virginia N. L. Franqueira[2](✉)

[1] Department of Research and Impact, Ulster University,
Belfast BT37 0QB, UK
j.macrae@ulster.ac.uk

[2] Department of Electronics, Computing and Mathematics,
University of Derby, Derby DE22 1GB, UK
v.franqueira@derby.ac.uk
j.macrael@unimail.derby.ac.uk

Abstract. The highly crafted lines of code which constitute the Locky cryptolocker ransomware are there to see in plain text in an infected machine. Yet, this forensic evidence does not lead investigators to the identity of the extortionists nor to the destination of the ransom payments. Perpetrators of this ransomware remain unknown and unchallenged and so the ransomware cyber crimewave gathers pace. This paper examines what Locky is, how it works, and the mechanics of this malware to understand how ransom payments are made. The financial impact of Locky is found to be substantial. The paper describes methods for "following the money" to assess how effectively such a digital forensic trail can assist ransomware investigators. The legal instruments that are being established by the authorities as they attempt to shut down ransomware attacks and secure prosecutions are evaluated. The technical difficulty of following the money coupled with a lack of registration and disclosure legislation mean that investigators of this cybercrime are struggling to secure prosecutions and halt Locky.

Keywords: Locky · Ransomware · Cryptolocker · Bitcoin · Brexit
Digital forensics · Money laundering

1 Introduction

Ransomware is not new. In fact the first reported example of a ransomware attack dates back to around 1989 and masqueraded as AIDS education software [1]. Ransomware is the name given to a class of software programs that prevents users from accessing their computer resources until a ransom is paid. In the earliest instances of ransomware this meant a screen lock or installing password protection on user's files. More recently a particular class of ransomware has been discovered called cryptolockers which encrypts a user's files using the AES and RSA algorithms [2]. Locky is an instance of cryptolocker ransomware. The AES and RSA algorithms require keys for encryption and decryption. The private key for decryption is provided only on payment of the ransom. Most recent versions of cryptolocker ransomware are also able to self-propagate and delete or encrypt backup files [3]. This means that the standard defence against ransomware, that of restoring files from backup, may not be effective.

P. Matoušek and M. Schmiedecker (Eds.): ICDF2C 2017, LNICST 216, pp. 33–45, 2018.
https://doi.org/10.1007/978-3-319-73697-6_3

Additional tools to perpetuate the extortion have been observed such as countdown timers after which no ransom payments are accepted and ransom payments which increase with time. Ransom amounts have increased with the sophistication of ransomware so that amounts equivalent to thousands of dollars are now commonly demanded by the extortionists [4].

Section 2 of this paper is an overview of how Locky works. This is known as the Locky infection chain. Section 3 looks in detail at two steps within the infection chain; the spam email which initiates the Locky download, and the Tor page where Locky payments are made. These steps inform how any digital forensic investigation of Locky can be undertaken. Section 4 observes that the impact of Locky and ransomware in general is significant. The potential cost to society goes beyond financial so there is an urgent need to find the perpetrators and shut down attacks. Section 5 expands on the detail of the Tor payment page, noting that the ransom payments are in Bitcoin. Bitcoin is particularly attractive to ransomware perpetrators due to its anonymity. Section 6 evaluates what tools are presently available and their likely effectiveness against Bitcoin anonymity. Tools are one way of supporting investigators, legal instruments and cooperation between jurisdictions are another. Efforts to introduce legislation and information sharing within the EU is described in Sect. 7. Consideration is given to the consequences of Brexit for the UK's legislation and participation in these EU arrangements. In the concluding section the combined value of tools, legislation and cooperation arrangements are assessed against the backdrop of cryptocurrency money laundering techniques being increasingly used by ransomware cybercriminals. It is shown that virtual currency processors located beyond the reach of legislation and information sharing agreements remain an unsolved problem.

2 How Locky Works

A diagrammatic summary of the Locky infection chain is shown in Fig. 1 [5]. Locky is delivered as an email attachment, ostensibly an invoice for payment. The email itself could be spam email, or the victim's email address could have been collected as part of a preliminary phishing attack. The attachment is a Word document with an embedded macro function. The function can only execute if Word macros are enabled. In order to encourage the user to enable macros, distorted text is shown along with the message "*enable macro if data encoding is incorrect*". When the Word document is opened the macro downloads the Locky code which then encrypts files on the machine and simultaneously renames the filenames and changes the file extension to .locky. The first instances of Locky appeared early in 2016 and a number of variants have appeared since, namely bart, odin and thor. Bart simply moves the victim's files into a password protected zip archive and demands 3 Bitcoin for the password, unless the default language of the computer is Russian or Ukrainian in which case bart uninstalls itself. Emails with an odin malware payload have a slightly different subject line and append the extension .odin to the encrypted files. The thor variant of Locky was released in October 2016 [6] and is distributed using a javascript-based downloader and a DLL file. The DLL is executed using the rundll32.exe file. rundll32.exe is a normal windows executable which enables the thor variant of Locky to install itself stealthily [7].

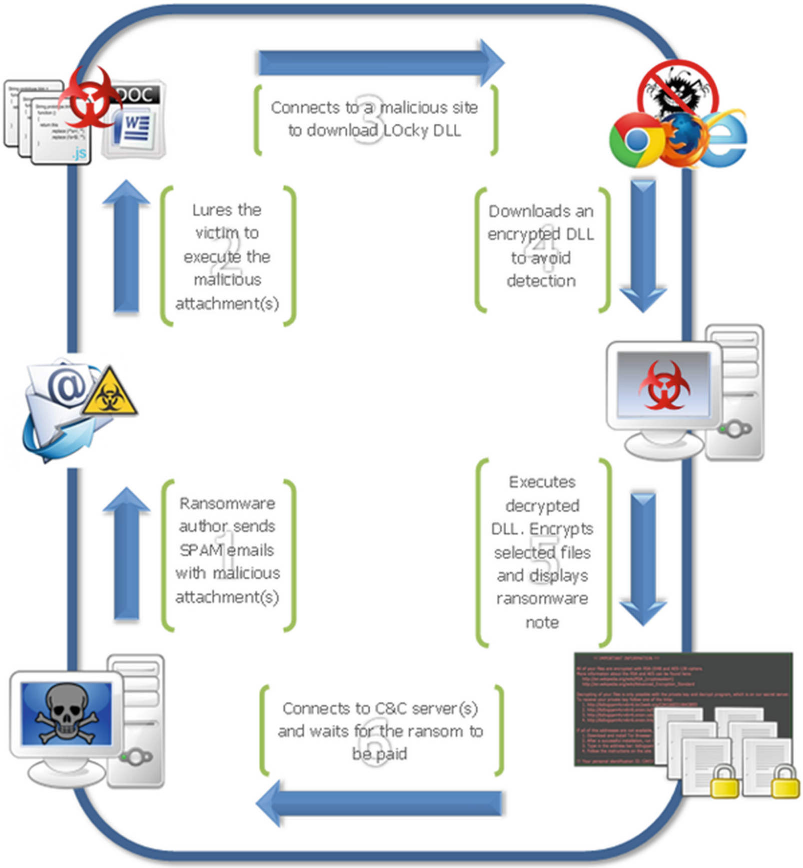
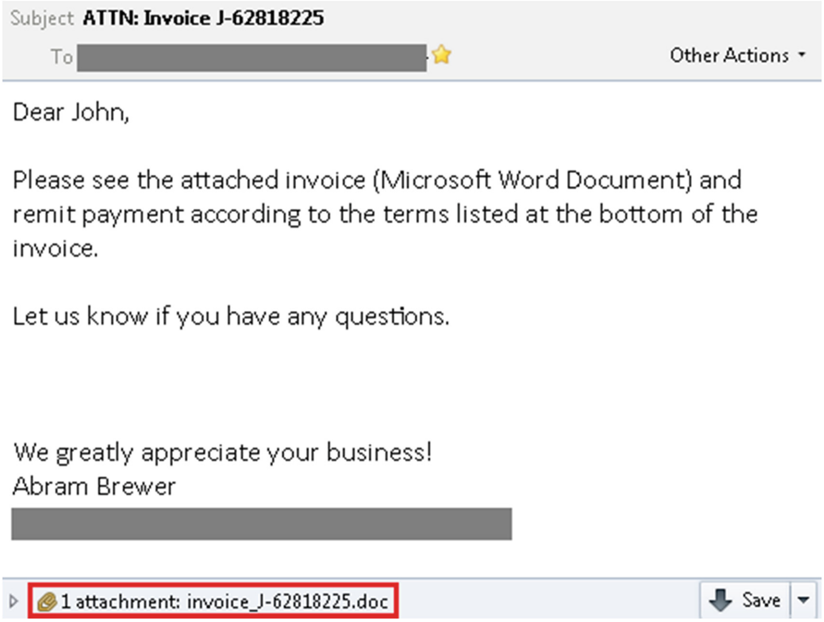

DOC
.js
Connects to a malicious site to download LOcky DLL
Lures the victim to execute the malicious attachment(s)
Downloads an encrypted DLL to avoid detection
Ransomware author sends SPAM emails with malicious attachment(s)
Executes decrypted DLL. Encrypts selected files and displays ransomware note
Connects to C&C server(s) and waits for the ransom to be paid

Fig. 1. The Locky infection chain [5]

3 Mechanics of the Locky Malware

The distribution and activation mechanism for Locky mirrors that of the dridex botnet and in fact may use a subnet of this botnet [8]. It is reported that this botnet has a database of 385 million email addresses so can generate significant amounts of spam targeted mainly at accounts departments of companies and enterprises rather than individuals. A typical Locky spam email is shown in Fig. 2 [9]. Note how the email masquerades as a payment invoice with a spurious purchase order reference in the subject line. The phraseology of the email is deliberately worded so that the invoice cannot readily be disregarded as fake unless the details are checked by opening the attachment.

The actual download code for Locky is obfuscated meaning that it is not directly visible within the Word macro. Instead a function CallByName is passed a string, the output of which is a visual basic script similar to that in Fig. 3 [9]. Note the section highlighted in red which shows the construction of the URL from which Locky is to be downloaded. For forensics investigators trying to find the download source of Locky, this is the start of the trail.



Subject **ATTN: Invoice J-62818225**

To [redacted]

Dear John,

Please see the attached invoice (Microsoft Word Document) and remit payment according to the terms listed at the bottom of the invoice.

Let us know if you have any questions.

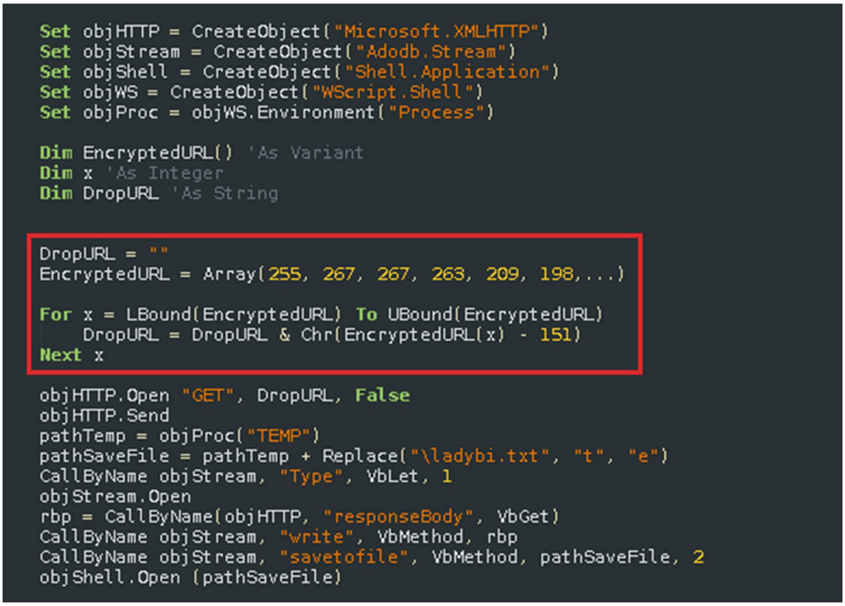
We greatly appreciate your business!
Abram Brewer
[redacted]

1 attachment: invoice_J-62818225.doc

Fig. 2. Sample email with which Locky has been associated [9] (Color figure online)

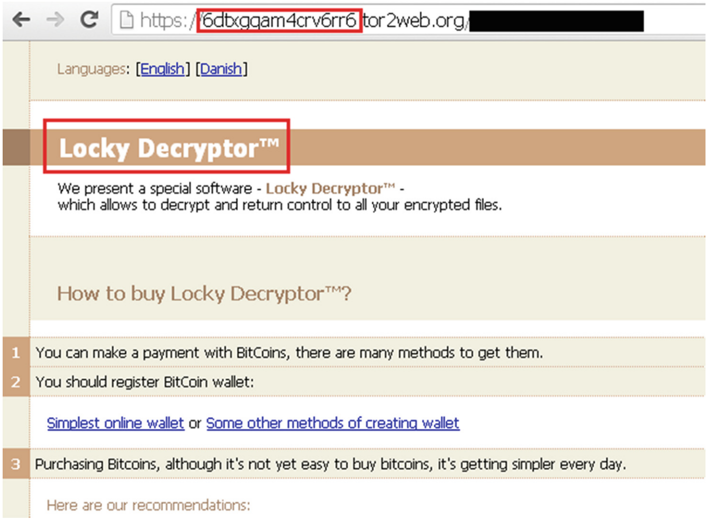
Once Locky is downloaded it renames itself svchost.exe so that it looks like a regular windows executable. The renamed process initiates a secondary process to delete backup files and prevent a system restore. Before file encryption can commence the ransomware must communicate with the command and control servers to report that a system has been infected and to obtain the RSA public key. A unique ID of the infected machine is generated and stored on the command and control server. However even this communication is encrypted so as to prevent ethical hackers observing the traffic. As of 2016, nine of the command and control servers were reported to be in Russia and therefore beyond EU law enforcement [9].

Locky can encrypt a wide range of file types – 164 according to Threat Intelligence Team [9] – which means that a very wide range of businesses can be impacted. The strength of the encryption algorithm is such that it is not possible to decrypt the affected files without the matching private key downloaded from the command and control servers. The servers provide the correct private key by cross referencing against the unique system ID provided when the infection process commenced. Figure 4 shows the ransomware payment page within the tor network [9]. Note the payment instructions in Bitcoin. This payment mechanism has substantial implications for forensic investigators whose task is to "follow the money". These implications are discussed throughout the remainder of this paper.



```
Set objHTTP = CreateObject("Microsoft.XMLHTTP")
Set objStream = CreateObject("Adodb.Stream")
Set objShell = CreateObject("Shell.Application")
Set objWS = CreateObject("WScript.Shell")
Set objProc = objWS.Environment("Process")

Dim EncryptedURL() 'As Variant
Dim x 'As Integer
Dim DropURL 'As String

DropURL = ""
EncryptedURL = Array(255, 267, 267, 263, 209, 198,...)

For x = LBound(EncryptedURL) To UBound(EncryptedURL)
    DropURL = DropURL & Chr(EncryptedURL(x) - 151)
Next x

objHTTP.Open "GET", DropURL, False
objHTTP.Send
pathTemp = objProc("TEMP")
pathSaveFile = pathTemp + Replace("\ladybi.txt", "t", "e")
CallByName objStream, "Type", VbLet, 1
objStream.Open
rbp = CallByName(objHTTP, "responseBody", VbGet)
CallByName objStream, "write", VbMethod, rbp
CallByName objStream, "savetofile", VbMethod, pathSaveFile, 2
objShell.Open (pathSaveFile)
```

Fig. 3. Visual basic script showing the Locky download code [9]



https://6dtxgqam4crv6rr6.tor2web.org/[redacted]

Languages: [English] [Danish]

Locky Decryptor™

We present a special software - Locky Decryptor™ -
which allows to decrypt and return control to all your encrypted files.

How to buy Locky Decryptor™?

1 You can make a payment with BitCoins, there are many methods to get them.

2 You should register BitCoin wallet:

Simplest online wallet or Some other methods of creating wallet

3 Purchasing Bitcoins, although it's not yet easy to buy bitcoins, it's getting simpler every day.

Here are our recommendations:

Fig. 4. Locky payment page within the Tor dark web [5]

4 Impact of Locky is Substantial

A Symantec report on ransomware published in 2016 [4] makes the point that it is impossible to measure how much money has been paid to ransomware extortionists. Anubis Networks detected 4500 infected machines between 16th and 18th February 2016 [10]. If every machine pays a decryption cost of 1 bitcoin, which is worth £800 in February 2017, then that adds up to £1.2 million per day. However that infection rate is a 2016 figure: since then more sophisticated versions of Locky have been released which encrypts backups and shared drives. Accordingly the cost of decryption has increased. FBI researchers have estimated that the revenue from ransomware collectively could be as high as a billion dollars annually [11].

However the revenue being collected by the extortionists is only part of the economic cost of Locky. The other part is the cost incurred by organisations that have their work disrupted. Hospitals have been a particular target for Locky. In February 2016 Hollywood Presbyterian Medical Centre in Los Angeles paid $17,000 to regain access to their patients data [12]. There were attacks on other US and Japanese hospitals [13]. Attacks on hospitals mean that patients medical records may be inaccessible leading to delays in administering treatments and medications. This has the consequence of putting lives at risk and exposing the hospital to fines and legal claims.

5 Ransomware and Cryptocurrency Have Become Either Side of the Same (Bit)Coin

For cyber criminals the most problematic aspect of the ransomware model has always been that of receiving payment in a way that did not lead to their detection. Early methods involved sending an SMS message to a premium account or use of an anonymous PO Box mailing address. Law enforcement soon learnt to stake out the PO Box until someone came along to pick up the payments. PayPal, Western Union, iTunes and gift cards have also been used as payment methods but they all suffer from limited anonymity; the money cannot be spent unless it ultimately goes through a conventional bank account or online retailer.

The scale and sophistication of ransomware attacks has accelerated in recent years. This is partly due to the spread of botnets that are distributing the Locky infection email. It is partly due to reorganisation within the crime gangs which have turned to offering cybercrime-as-a-service business models. Philadelphia [14] is an example of ransomware-as-a-service in which the ransomware attack and payment infrastructure is leased out, allowing criminals with no IT knowledge to take advantage of the ransomware extortion. However the success of ransomware is mostly to do with the technical sophistication of ransomware itself. This means efficient implementation of the public private key encryption so that infected computers cannot be decrypted without the private key. It means traffic between infected computers and the command and control computers (C&C) is encrypted so that the URL of the C&C computers cannot be traced, and it means virtually untraceable payments made in Bitcoin or another cryptocurrency.

Bitcoin is a peer-to-peer cryptocurrency in which transactions are recorded in a distributed ledger called blockchain. There is no central repository or single administrator. The information which is used to perform Bitcoin transactions is stored in a software application called a wallet. Bitcoin uses public key cryptography: the information contained in the wallet is essentially the public and private keys relating to a user's Bitcoin ownership. Blockchain contains the public key hashes of all Bitcoin transactions. Since there is no single administrator the entire blockchain must be distributed across the internet and these public key hashes are visible.

The connection between visible public key hashes and the private keys only takes place in whatever way the wallet is implemented. Increasingly the function of the wallet is provided by Bitcoin processors. Such processors can move money between the Bitcoin virtual currency and real bank accounts. They can take the form of ATMs or of online payment intermediaries similar to the services provided by MasterCard and VISA as used by merchants. Wallets are also implemented as smartphone applications that can be used to pay for goods and services directly. An example of the rich functionality that such smartphone wallets now provide can be seen in the CoinsBank wallet app [15].

6 Review of Tools for Bitcoin and Blockchain Deanonymisation

Strictly speaking, Bitcoin transactions are pseudonymous rather than anonymous. The public key hashes of the transactions are visible, but the link between the public keys and their owners is not visible or accessible. Deanonymisation is the process of using other sources of information to try to connect public key hashes to Bitcoin owners or to their bank accounts. This process uses a combination of traditional policing methods otherwise known as the classical forensic approach [16] and more recently dedicated tools such as BitIodine [17], BitCluster [18], Elliptic [19] and Chainalysis [20] all of which involve collection to some extent of open source forensics. The term open source forensics refers to information and potential evidence publically available from internet blogs, forums and social media.

The so-called classical approach is analogous to a blunt instrument in which a legal demand is served on Bitcoin processing businesses to reveal the owner or bank account of public key hashes of interest to investigators. As it is the purpose of Bitcoin processors to enable the transfer of money from Bitcoin to and from traditional currencies, these processors hold the link between the anonymous public key hashes and their owners. However the classical forensic method is fraught with difficulty. A particular problem is connecting a public key hash suspected to be associated with cyber criminality with a specific Bitcoin processor on which to serve the information demand. The Bitcoin processors may themselves be illegal and may be operating outside of the legal jurisdiction of the investigators such that they cannot be compelled to provide information. This problem is discussed in Sect. 7.

In contrast BitIodine could be described as a covert approach to Bitcoin forensics. This method, which relies on open source forensics, is described as trying to correlate Bitcoin transaction activity with Facebook account activity [15]. A more comprehensive description of BitIodine is that it consists, inter alia, of a set of “crawlers” which search the web for Bitcoin addresses which can be associated with real users. The types of domains that are searched include usernames on Bitcoin forums, details of known scammers and tagged data from blockchain.info, news sites and from social media.

Meiklejohn et al. [21] describe the application of BitIodine to a ransomware investigation. It is not stated in the paper if the destination of the ransom money was ultimately determined, but BitIodine was able to detect Bitcoin clusters belonging to the ransomware perpetrators and cross reference that to a reddit thread where victims had been posting addresses.

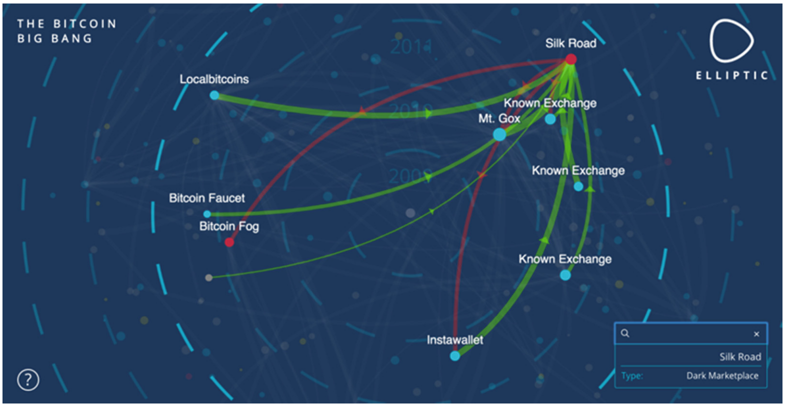
BitCluster is an open-source data mining tool which allows its users to group Bitcoin transactions by their participants. The goal of BitCluster according to [18] was to gather data on users of the Bitcoin network, and attempt to aggregate Bitcoin wallets which otherwise would seem to be anonymous and isolated from one another. BitCluster therefore enables investigators to detect significant payment patterns which could be linked to ransomware schemes. BitCluster is a way to link public key hashes to campaigns using the scale of transactions linked to the timing of spam attack. If the relevant public key hashes can be determined then investigators can follow-up with the classic forensics approach of demanding information from the Bitcoin processors. However BitCluster only works as long as the same public key hashes are used for ransom payments. The effectiveness of the tool is defeated if each new ransom payment uses a new public key hash.

Elliptic is a startup company founded in 2013. The Elliptic product is a data mining tool with similarities to BitCluster but with ongoing development and support commensurate with a commercial product [19]. Elliptic started life as a Bitcoin vault platform but found that Bitcoin forensics was of particular interest to financial institutions worried about the consequences of anti-money laundering regulations that would leave them exposed were they inadvertently be involved in processing of Bitcoins obtained as proceeds of crime. The technology underlying Elliptic is not described in the public domain. However according to a 2017 paper [15] it traces transactions through the blockchain, uncovers relationships between different entities and uses artificial intelligence techniques to enable mapping between public hash keys and their real owners. It is a logical step from Elliptic’s history as a Bitcoin vault, that is as a store of Bitcoin transaction, to analysing and visualising the transaction history.

A typical Elliptic screenshot is shown in Fig. 5 [19]. This visualisation indicates the relationships between the illegal marketplace “Silk Road” and other entities processing Bitcoins. Elliptic claims to provide forensics intelligence to ransomware investigators and thus facilitate the arrest of ransomware cybercriminals and assist financial institutions in refusing to process Bitcoins collected through ransomware attacks.

Chainalysis was formed in 2014 and has already signed an MoU with Europol [22] on the provision of technical services to spot connections between Bitcoin transactions and cyber criminals. The Chainalysis Reactor tool is specifically aimed at forensics investigation of virtual currency transactions.

There is little material in the public domain linking these data mining tools to successful prosecutions of cyber criminals. The most convincing is the application of the BitIodine tool to the Dread Pirate Roberts case described by Meiklejohn et al. [21].



Silk Road

Type: Dark Marketplace

Fig. 5. Elliptic screenshot showing Bitcoin trading relationships [19]

This might be due to the need to maintain confidentiality for prosecutions which have not yet come to court. Or it might be the case that cyber criminals have already learnt to outwit the data mining tools by changing transaction patterns: essentially money laundering within virtual currencies. For forensic investigators, these tools are unlikely to possess the specificity to withstand court scrutiny - if they provide any evidence at all - and at best may provide some complementary investigative direction.

7 Legal Instruments Facilitating Ransomware Digital Forensics

On the 30th November 2016 a federal court in the northern District of California authorised the tax authorities in the US, known as the Internal Revenue Service (IRS), to serve a "John Doe" summons [23] on the Bitcoin processor Coinbase Inc [24]. The purpose of the summons is to demand that Coinbase releases the names and financial trading history of owners of Bitcoin and other cryptocurrencies so that the IRS can collect any unpaid taxes. The John Doe summons is considered a brute force approach by the IRS yet is also an acknowledgement that the pseudonymous nature of cryptocurrencies means that it is otherwise difficult for the tax authorities to detect hidden wealth and potentially taxable capital gains. Note that the IRS have chosen the approach of forcing the cryptocurrency processor to disclose information rather than using other means - such as the data mining tools described above - to try to link the public key hashes that are visible on the bitcoin exchanges with their owners and bank accounts.

There is an interesting parallel with the notorious American prohibition-era gangster Al Capone. Despite Capone's involvement in a criminal syndicate that supplied illegal alcohol, he was eventually tried and convicted by the FBI on a charge of tax evasion. This was considered a novel strategy by the FBI in 1931. The suspicion of tax evasion is therefore being used to challenge the pseudo-anonymity of cryptocurrencies in a strategy which may provide information and lead prosecutors to the recipients of the proceeds of ransomware. The strategy relies on being able to link public key hashes with ransomware payments, and it relies on the relevant cryptocurrency processors operating within the jurisdiction covered by the US court summons.

The UK's first money laundering national risk assessment was published by UK Government in 2015 [25]. Although the report is concerned with money laundering in all its respects, it acknowledges the speed of trade, anonymity and cross border nature of virtual currency transactions. It assesses this threat as principally related to the activities of cyber criminals. The report concluded that there was a strong case for anti-money laundering legislation in order to create a hostile environment for illicit users of virtual currencies. Contemporaneously, legislation was being developed by the European Commission known as the 4th Money Laundering Directive (4MLD). The 4MLD was published on 20th May 2015 and was essentially implementing the recommendations of the international Financial Action Task Force dating back to 2012 [26]. The Commission proposed that 4MLD was implemented into the national legislation of EU member countries by 26 June 2017. 4MLD did not, at this stage, make any reference to disclosure requirements for virtual currencies.

In response to terrorist attacks across Europe during 2015, a number of European bodies, specifically the Justice and Home Affairs Council [27], the Economic and Financial Affairs Council [28] and the European Council [29] stressed the need to intensify the work within the EU on addressing terrorism and enhancing the provisions within 4MLD. This led, on 5th July 2016, to the Commission adopting an Action Plan [30] as amendments to 4MLD to tackle the abuse of the financial system for terrorist financing purposes. This document also brought forward to 1st January 2017 the date by which the 4MLD including these amendments was to be implemented in member states.

The effect of the amendments is to add virtual currencies and wallet providers as entities to whom the obligations of the 4MLD apply. These obligations are, inter alia, know-your-customer requirements, suspicious activity reporting, licensing and registration. The consequence of these additional obligations on virtual currency processors is that anonymous virtual currency ownership and trading will no longer be possible within EU-based entities. The 4MLD legislation will therefore increase the forensic material available to ransomware investigators. This information will have to be used alongside other sources of forensics, such as the data mining tools described above in Sect. 6, in order for investigators and cryptocurrency processors to identify and link ransomware payments with cryptocurrency transactions.

The European Commission's action plan of amendments to 4MLD states that the proposed objectives cannot be achieved by member states alone and can be better achieved at the European Union level: the lack of an effective anti-money laundering framework in one member state can have consequences across the other member states and undermine the disclosure and transparency aims of 4MLD. As well as the legislative momentum for 4MLD and its later amendments coming from the EU, the proposed information sharing mechanisms will be EU-wide under the proposal to establish and then interconnect national central registers which would hold information on virtual currency transactions.

Despite Brexit, the UK Government has given a commitment to implement the 4MLD in the UK as the Money Laundering and Transfer of Funds (Information on the Payer) Regulations 2017. As yet unanswered is the question of the UK's participation post Brexit in the information sharing aspects of 4MLD between EU Financial Intelligence Units. Information sharing is an important aspect in achieving the desired transparency on ownership of virtual currency. Also unanswered is the UK's ongoing participation, post Brexit, in the various European bodies from which legislative momentum is derived. Post Brexit, without participation in such European bodies, without the legislative momentum derived from European Commission proposals and without access to shared information, there is a risk that ransomware forensic investigators in the UK are substantially blindfolded compared with their European counterparts. There is a corresponding risk that outside of European frameworks of cooperation the UK could become a preferred destination for the cryptocurrency transactions of cybercriminals.

8 Conclusions

According to Cisco, the ability to demand payment in Bitcoin, a pseudonymous virtual currency not controlled by any country, was 'the birth of ransomware' and has led to a substantial increase in number of ransomware attacks since the currency's introduction in 2009. Since the source and control of ransomware involves botnets and servers invariably hidden in uncooperative jurisdictions, the best strategy for digital forensics investigators is to "follow the money" to see if recipients of the Bitcoin ransomware payments can be identified. Some research projects and corresponding tools were identified and examined.

The commercial tools especially make bold claims concerning the deanonymisation of Bitcoin public key hashes, but there is little in the public domain about how they work. There are no case studies with demonstrated convictions. The exception is Meiklejohn et al. [21] who describe in detail the algorithms and approaches designed into the BitIodine open source tool and demonstrate its effectiveness in several real world use cases. It can be inferred from the terminology used that the commercial tools use similar approaches with similar outcomes.

The best that might be said of the state of the art in Bitcoin forensics tools is that they can provide leads for investigators to follow alongside investigative processes. However since the tools are based on the data mining techniques of pattern matching and clustering, these algorithms can be defeated if the cyber criminals start to use multiple independent Bitcoin keys, each transaction being of a small Bitcoin amount. A further obfuscation technique the criminals use is to vary transaction patterns: the cryptocurrency version of money laundering. Clearly data mining tools are not a panacea for ransomware investigators, although it is worth keeping an eye on the capabilities of the commercial tools as a complement to traditional investigative processes.

In the US and Europe the experience of chasing Al Capone has not been forgotten and so the approach to increasing the forensics available to ransomware investigators is not on the crime itself, but via the financial crimes of tax evasion and money laundering. However enabling legislation in cooperating jurisdictions is not yet in place. In Europe the provisions within the 4th Anti-Money Laundering Directive were substantially amended following the terrorist attacks in Europe in 2015 to include disclosure and information sharing requirements on virtual currency processors. It is not clear how Brexit will affect the UK's long term participation in this information sharing, but it will be important for ransomware investigators that the UK continues to participate in the cooperation arrangements proposed by the EU. This desire was formally expressed in the UK Prime Minister's letter to the EU President on 29th March 2017 which triggered Article 50, that is, the UK intention to leave the European Union [31].

Regardless of Brexit or 4MLD, the legislation does not address the problem of illegal processors or those operating outside the frameworks of cooperation. For example, a close examination of the CoinsBank bitcoin processor described in Sect. 5 reveals that the website is operated by CB Exchange LP with an address in Edinburgh. The underlying financial services of CoinsBank are provided by XBIT Ltd which is registered and regulated in Belize. It is not yet clear if this structure will fall within the jurisdiction of the UK's 4MLD. Virtual currency processors resident and regulated outside the jurisdiction of 4MLD will continue to represent a formidable obstacle for ransomware forensic investigators.

References

1. Alina, S.: Ransomware's stranger-than-fiction origin story (2015). https://medium.com/un-hackable/the-bizarre-pre-internet-history-of-ransomware-bb480a652b4b-.z5qxcdeyy
2. Calderbank, M.: The RSA Cryptosystem: History, Algorithm, Primes. http://www.math.uchicago.edu/~may/VIGRE/VIGRE2007/REUPapers/FINALAPP/Calderbank.pdf
3. Trendmicro.co.uk: Ransomware - Definition - Trend Micro UK. http://www.trendmicro.co.uk/vinfo/uk/security/definition/ransomware
4. Symantec: ISTR2016 Ransomware Report. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ISTR2016_Ransomware_and_Businesses.pdf
5. Valdez, J.: Meet the latest member of the Locky family: odin. https://blog.gdatasoftware.com/2016/10/29245-meet-the-latest-member-of-the-locky-family-odin
6. State of Security: The Thor Variant of Locky Virus. https://www.tripwire.com/state-of-security/latest-security-news/thor-variant-locky-virus
7. It-b.co.uk: What is Thor. http://www.it-b.co.uk/blog/what-is-thor
8. Zorz, Z.: Dridex botnet alive and well, now also spreading ransomware - Help Net Security. Help Net Security. https://www.helpnetsecurity.com/2016/02/17/dridex-botnet-alive-and-well-now-also-spreading-ransomware/
9. Intelligence Threat Team: A closer look at the Locky ransomware. Blog.avast.com, https://blog.avast.com/a-closer-look-at-the-locky-ransomware
10. Blog.anubisnetworks.com: Locky ransomware, metrics and protection. http://blog.anubisnetworks.com/blog/locky-ransomware-metrics-and-protection
11. Griffin, D.: Cyber-extortion losses skyrocket, says FBI. CNNMoney. http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/
12. Yadron, D.: Los Angeles hospital paid $17,000 in bitcoin to ransomware hackers. The Guardian. https://www.theguardian.com/technology/2016/feb/17/los-angeles-hospital-hacked-ransom-bitcoin-hollywood-presbyterian-medical-center

13. Theregister.co.uk: FireEye warns ‘massive’ ransomware campaign hits US, Japan hospitals. http://www.theregister.co.uk/2016/08/18/fireeye_warns_massive_ransomware_campaign_hits_us_japan_hospitals/
14. Krebsonsecurity.com: Ransomware for Dummies: Anyone Can Do It — Krebs on Security. https://krebsonsecurity.com/2017/03/ransomware-for-dummies-anyone-can-do-it/
15. Coinsbank.com: CoinsBank - the bank of Blockchain future. https://coinsbank.com/wallet
16. InfoSec Resources: The End of Bitcoin Ransomware? http://resources.infosecinstitute.com/the-end-of-bitcoin-ransomware/#gref
17. Spagnuolo, M., Maggi, F., Zanero, S.: BitIodine: extracting intelligence from the Bitcoin network. In: Christin, N., Safavi-Naini, R. (eds.) FC 2014. LNCS, vol. 8437, pp. 457–468. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-662-45472-5_29
18. Bit-cluster.com: BitCluster. http://www.bit-cluster.com
19. Elliptic: Elliptic. https://www.elliptic.co/
20. chainalysis.com: Chainalysis - Blockchain analysis. Chainalysis. https://www.chainalysis.com/
21. Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G., Savage, S.: A fistful of Bitcoins. Commun. ACM **59**(4), 86–93 (2016)
22. Europol: Europol and Chainalysis Reinforce Their Cooperation in The Fight Against Cybercrime. https://www.europol.europa.eu/newsroom/news/europol-and-chainalysis-reinforce-their-cooperation-in-fight-against-cybercrime
23. Justice.gov: Court Authorizes Service of John Doe Summons Seeking the Identities of U.S. Taxpayers Who Have Used Virtual Currency. https://www.justice.gov/opa/pr/court-authorizes-service-john-doe-summons-seeking-identities-us-taxpayers-who-have-used-virtual-currency
24. Coinbase.com: Bitcoin & Ethereum Wallet - Coinbase. https://www.coinbase.com/?locale=en
25. UK Treasury: UK national risk assessment of money laundering and terrorist financing. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/468210/UK_NRA_October_2015_final_web.pdf
26. Fatf-gafi.org: Documents - Financial Action Task Force (FATF) (2017). http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html
27. Consilium.europa.eu: Economic and Financial Affairs Council configuration (Ecofin) - Consilium. http://www.consilium.europa.eu/en/council-eu/configurations/ecofin/. Accessed 15 Mar 2017
28. Consilium.europa.eu: Justice and Home Affairs Council configuration (JHA) - Consilium. http://www.consilium.europa.eu/en/council-eu/configurations/jha/
29. Consilium.europa.eu: The European Council - Consilium. http://www.consilium.europa.eu/en/european-council/
30. European Union: AML Directive. http://ec.europa.eu/justice/criminal/document/files/aml-directive_en.pdf
31. BBC News: Teresa May Article 50 letter. http://news.bbc.co.uk/1/shared/bsp/hi/pdfs/29_03_17_article50.pdf