Deviating from the cybercriminal script: Exploring tools of anonymity (mis)used by carders on cryptomarkets

Authors
Gert Jan van Hardeveld, Craig Webber & Kieron O'Hara

Abstract
This work presents an overview of some of the tools that cybercriminals employ in order to trade securely. It will look at the weaknesses of these tools and how the behaviour of cybercriminals will sometimes lead them to use tools in a non-optimal manner, creating opportunities for law enforcement to identify and apprehend them. The criminal domain this article focuses on is carding, the online trade in stolen payment card details and the consequent criminal misuse of such data. However, these findings could be applied more broadly, as many of the analysed tools are used across (cyber)criminal domains. This paper is a continuation of earlier work (van Hardeveld, Webber & O'Hara, 2016), in which a crime script analysis of 25 carding tutorials presented the tools that cybercriminals use to cash-out stolen payment card details while remaining anonymous. We use these tutorials and an analysis of the literature to identify how they can be used incorrectly and create a typology of potential behavioural and technological pitfalls in these tools. Finally, we conclude that finding pitfalls in the usage of tools by cybercriminals has the potential to increase the efficiency of disruption, interception and prevention approaches. However, in future work, interviews with law enforcement experts and convicted cybercriminals or still active users should be used to analyse the operational security of cybercriminals in more depth.

Introduction

Online marketplaces on which stolen credit card details are sold have been around since the early 2000s. Some of the first 'carding' forums were CarderPlanet and ShadowCrew, both of which were shut down in 2004 (Glenny, 2011). The shutting down of these and other forums has had the effect of making carders more conscious of their personal 'operational security' practices, encouraging them, for example, to move from using VPN services to the more secure Tor network when browsing carding forums (Thomas et al., 2015). The regular Web is still used for hosting carding forums and marketplaces. However, carders have been using the Tor network ever since the rise of Silk Road in 2011, the first cryptocurrency-fueled illicit marketplace that ran on the Tor network as a hidden service. Such 'cryptomarkets' on the Tor network can be recognised by the .onion suffix and are only accessible through the Tor network, which offers more anonymity than regular websites. Hidden services are more resilient against traffic analysis and thus harder to penetrate than the regular web.

Takedowns of online underground forums and cryptomarkets are often deemed an effective countermeasure by law enforcement and researchers (Afilipoaie & Shortis, 2015; Yip, Webber & Shadbolt, 2013; Motoyama et al., 2011), but it has also been argued to be an inefficient deterrent in the long term given that it has failed to reduce sales or markets' revenue (Décary Hétu & Giommoni, 2017;

Ladegaard, 2017). Soska and Christin (2015) have shown that the ecosystem stays equally strong after takedowns and conclude that complex and expensive international law enforcement operations may not be worth the resources invested in them. They therefore call for alternative solutions, with a stronger focus on prevention or on active intervention. Hutchings and Holt (2017) similarly found that tensions exist around such takedowns, arguing that they focus too much on high-value small volume crimes, but ignore small-value high-volume crimes. Law enforcement generally prioritises arresting major sellers, but carders who, for example, sell low quantities with various pseudonyms will be less likely to be apprehended. An example of how carders try to cash-out payment cards is by ordering computers, laptops, tablets or televisions (van Hardeveld, Webber & O'Hara, 2016). Other high value items often acquired by carders are airline tickets, car rentals and hotel accommodation (Europol, 2016).

According to Thomas et al. (2015), researchers need to reconsider the 'fire-fighting approach' and instead focus on the dependencies of the ecosystem. Hutchings and Holt (2017) provide a collation of current intervention and disruption methods of stolen data markets, demonstrating some elements of the ecosystem that could be addressed. However, they do not look at the modus operandi of individual users of such markets. In online underground communities this is known as 'operational security' or 'opsec', which merits further research, as carders can employ these skills, even when all marketplaces are taken down. Carders could still buy card details at different places on the web, such as carding shops, IRC channels or hacker forums (Benjamin et al., 2015). Van Hardeveld, Webber and O'Hara (2016) found which tools are often used by carders to obtain and cash-out stolen card details by analysing 25 tutorials focused on carding, found on a hidden service on Tor[1]. This paper is a continuation of that work.

Objective

We will continue our previous analysis of the advice given to carders in tutorials about what tools to use to protect themselves from exposure to law enforcement, look for the pitfalls in these tools and at how carders may use them incorrectly. We want to identify where pitfalls lie in the technology and in the behaviour of carders. By doing this, we create a better insight into the operational security of online criminals. This can lead to new insights for academia and help law enforcement in determining how to approach investigations, as we will expose potential weaknesses in the operational security of users of cryptomarkets.

Method

In previous work (van Hardeveld, Webber & O'Hara, 2016), we used a crime script analysis, which is a method that aims to describe the procedural aspects of a crime (Cornish, 1994). We deconstructed carding to identify some of the common processes users of an underground marketplace go through to obtain and cash-out stolen payment cards. We looked at 25 tutorials, found on a forum connected to a cryptomarket on the Tor network, which focused on different

[1] This marketplace went offline in April 2016.

aspects of the carding process to create the most commonly advised 'optimal' route, as can be seen in figure I.

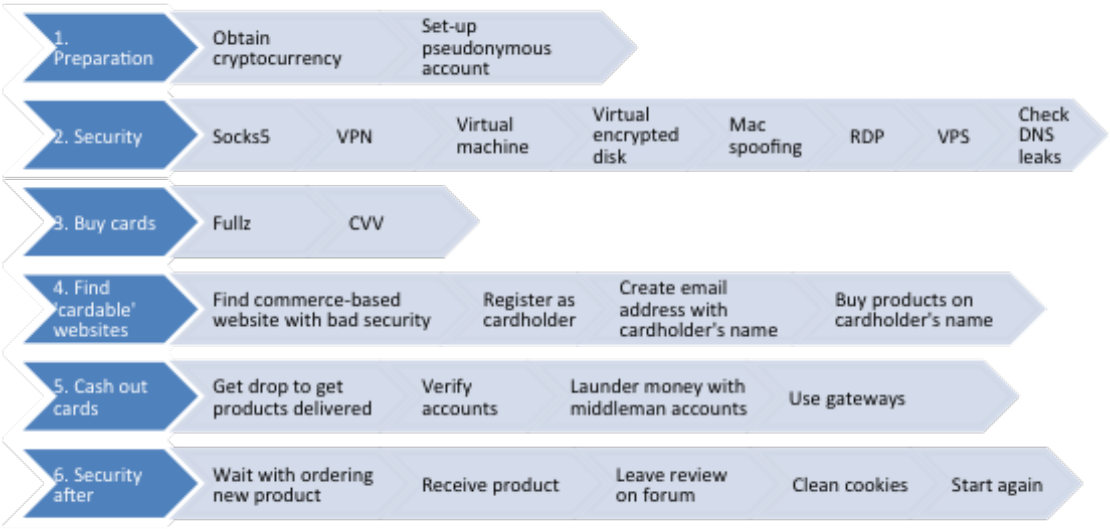

Figure I adopted from Van Hardeveld, Webber & O'Hara, 2016

The tutorials were posted for free between 2013 and 2015. We only analysed free tutorials, as buying tutorials contributes to the thriving of underground marketplaces, which is ethically questionable. The tutorials focus on different facets of carding: terminology, basics, laundering, delivering products and others. It is hard to determine when they were written, as they could have been offered before. One of the tutorials was, for example, a law enforcement agency's insight into carder's methods from around the time of ShadowCrew and CarderPlanet between 2001 and 2004. The rest of the tutorials content is more recent, as some, for example, focus on Bitcoin laundering. While the tutorials will not be generalisable to account for all kinds of behaviour by carders, this sample is relevant to analyse, as the tutorials were accessible for carders for free. They will therefore have played a part in the learning process of at least some of them, representing a form of social learning and initiation into the carding subculture (Holt, 2006). Insights into the operational security of carders can thus be obtained from this dataset.

In this paper, we will look at some of the most commonly discussed tools mentioned in these tutorials, the ones that have been mentioned in two or more tutorials. We will review the literature on these tools to analyse why they are used, what their technical pitfalls are and how carders can use them incorrectly. The tools can be categorised as *proxy-based services*, *financial services* and *offline*. Within these categories the following tools that were mentioned in tutorials will be discussed: virtual machines, VPNs, SOCKS proxies, Tor, RDP, MAC address changers, DNS, Bitcoin and drops. Paypal was mentioned in several tutorials, but an analysis of how this is misused by carders can be found in previous work (van Hardeveld, Webber & O'Hara, 2016). Finally, a typology of some of the behavioural and technological pitfalls in tools used by carders will be created,

which can be used, and elaborated on, by researchers and law enforcement agencies to understand how carders can be potentially identified in future research.

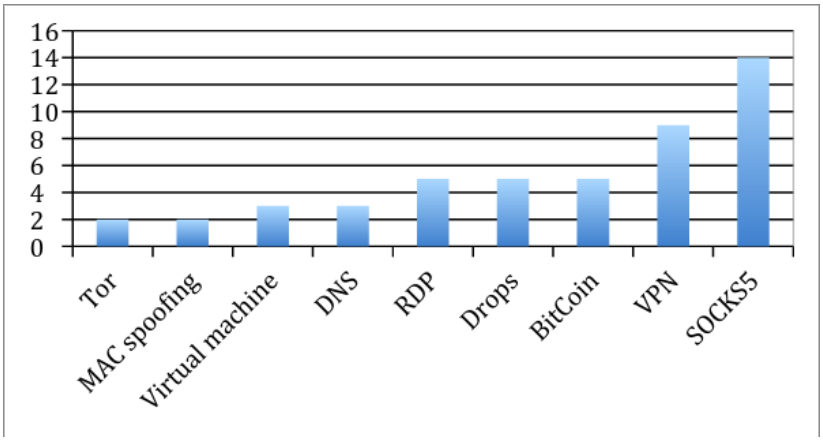

Figure II Number of mentions of tools in tutorials

An analysis of the literature will show how and why users of illicit online marketplaces use tools to stay secure while making profits from stolen card details. These tools can affect the investigatory process for law enforcement. We will look at what the technological pitfalls of these tools are from the perspective of carders and how the misuse of the tools can lead to opportunities for the investigatory process for law enforcement. We assume that carders will try to stay anonymous, while law enforcement will try to discover the real identity of carders[2]. Our aim is to explore the pitfalls in the various tools used by cybercriminals.

Proxy-based services

Virtual machines

It is recommended in three of the analysed carding tutorials to use a virtual machine (VM). VM software allows users to create multiple isolated virtual computers that run within a single physical computer. VMs can be run as part of a cloud environment, which leads to a wide variety of issues for law enforcement in their investigations (Healey, Angelopoulou & Evans, 2013). This makes them appealing for carders. According to some of the authors of tutorials, carders should work on virtual machines to have a safe and separate place from their personal computing in which they can do their carding business in order for them to be very hard to trace by law enforcement. Also, by using a virtual machine for carding and the 'normal' computer for regular browsing activity, the carder is less likely to leave traces of their real identity anywhere in a carding environment. Such behaviour also means that the chance that there is evidence left behind on the physical computer is minimal. Online criminals can thus commit their crimes on a virtual machine while deleting evidence on their physical computer. To investigate such crimes, forensic investigation needed to adopt new techniques. These are known as cloud forensics (Zawoad & Hasan, 2013).

[2] Although we are aware that this is not always the case.

Cloud forensics deal with different issues than traditional digital forensics. Dykstra & Sherman (2011) identified the acquisition of data as one of the main issues of cloud forensics. In a cloud environment, data does not have to be stored on the physical computer of the user, but will be located on various computers owned by the cloud provider. Data and log files will be co-located with data of other users (Healey, Angelopoulou & Evans, 2013) and are sometimes hard to retrace, as they can be located among many hosts in different data centres (Zawoad & Hasan, 2013). Another acquisition problem is that law enforcement needs a search warrant to access data on cloud provider's servers. This could be problematic when it is not located at one specific location or when the data of other users is stored on the same server, as looking at data on these servers can then violate their privacy. Cooperation of the cloud provider can help in such cases to figure out the best approach, as they generally have more evidence of what data belongs to a suspect (Zawoad & Hasan, 2013). When using a VM on a cloud service, it also acts as a proxy, as the user's actions appear to come from the VM which is on the network of the cloud provider. Cross-jurisdictional approaches are thus necessary if the data are stored at data centres in other countries.

VMs can also be run on user's local desktops. While using a VM on a local machine, it was also advised in one tutorial to use TrueCrypt on top. TrueCrypt is on-the-fly encryption software, which means that only the data needed by the user is accessible and that all data is encrypted from the onset (Balogun & Zhu, 2013). TrueCrypt can encrypt a VM and thus make it even harder for law enforcement to seize data from it. In the tutorial the argument for using TrueCrypt is made as it can help someone when law enforcement tries to raid a suspect's house. If virtual disk encryption is used, the suspect could simply pull the plug of the computer, making it impossible to enter the virtual machine without decrypting it first. The encrypted VM will appear to have random data in it, which could lead to plausible deniability of the suspect. Such incidents, in which data is encrypted, are often not prosecutable because of a lack of evidence (Balogun & Zhu, 2013). Because of this, law enforcement often tries to prevent a suspect of an online crime from closing or turning off their machine during an arrest, as this could lead to a loss of evidence. However, TrueCrypt is discontinued by its developers, which means that potential vulnerabilities will not be patched and that it is no longer available through the official website. Readers of the tutorials in which TrueCrypt is recommended might make the mistake of still trying to download the software. These download files could be infected with malware by malicious attackers who want to access their system. This could be, for example, used as a tactic by law enforcement to identify potential suspects.

VPN

Virtual Private Networks (VPNs) are among the most discussed topics in the analysed carding tutorials. A VPN is a private network that uses "public networks (such as the Internet) tunnelling protocols, and security procedures to tunnel data from one network to another" (Hawkins, Yen & Chou, 2000: p. 134). After simple proxies, VPNs are, together with Tor, the technologies most used by

cybercriminals to achieve anonymisation (Europol, 2016). A VPN makes it seem as if the user's traffic originates from the VPN host. Therefore, VPNs are also used to avoid government censorship and to access content from countries in which it is not blocked. In some tutorials it is recommended that a VPN should be used at all times when a user is browsing the Web while doing something related to carding, as it helps prevent leaving a user's IP address behind. Users of underground markets will sometimes even use several VPNs, proxies and the Tor browser at the same time to achieve strong security (Europol 2014). While this will obfuscate the path to a user's IP address, it will also slow down the traffic of the carder and thus reduce usability.

Usability can sometimes be an important concern for carders. More usability can lead to acceleration of business, but also to deficient operational security and increases in the chance of being arrested. Sundaresan et al. (2016) found that only 4.8% of merchant accounts on underground forums consistently use a VPN. The authors analysed Skype handles, as according to them Skype is often used by cybercriminals to communicate with one another. They used a vulnerability in Skype, which allowed for the collection of the IP addresses of merchants from underground forums. They then used databases of geolocation and online fraud prevention company MaxMind[3] to map the IP addresses by country, Internet Service Provider (ISP) and ISP type. ISP types distinguish between cellular, residential, business, government and others. According to the authors, some merchants that use mobile phones instead of machines that consistently use VPNs will care more about being available than about being secure. The majority of users, 95.2% according to the random subset of Sundaresan et al., lacks in operational security by not always using a VPN and will thus be at risk of revealing their IP address, which could be used to deanonymise them.

The results of the study of Sundaresan et al. will most likely not be found equally across all online criminals. The fact that carders in the analysed subset all shared their Skype handle is an indication that they value availability and usability over operational security, as they would otherwise not communicate via Skype but in more secure ways, such as PGP, which is a program used to encrypt and decrypt messages, files and disk partitions. Therefore, the subset chosen may not be representative for all kinds of online criminals. It is therefore still important to consider users who use VPNs, as they might make up a larger percentage than assumed by Sundaresan et al. The usage of VPNs will make users less prone to third party snooping on their real IP address. VPNs encrypt all the incoming and outgoing data sent over the computers connected to its network (Goncharov, 2012; Hawkins, Yen & Chou, 2000). However, there are still methods employed by law enforcement to identify users of these services that use it for illicit activity. Law enforcement have in the past used informants to operate VPNs and obtained VPN log files through court orders. Because of this it has been suggested that illicit users of VPNs are moving away from the services to Tor and botnet-enabled proxies, because they do not trust them anymore (Hutchings & Holt, 2017). This shows that an increased law enforcement focus on specific tools

[3] https://www.maxmind.com/en/home

could lead to an uptake of technically more complex tools. These unintended consequences are also seen in others areas of law enforcement such as sentencing policy (Webber, 2010; Grabosky, 1996).

VPN providers can be forced by law to store log files and to reveal the IP addresses of users of their service. While there are VPN providers advertising that they do not keep logs, arrests have still occurred after law enforcement seized one of their servers with a court order on which IP transfer logs were found (Crawford, 2014). According to Zawoad and Hasan (2013), log files are crucial to forensic investigations and can reveal the who, when, where, and why of incidents. The majority of popular VPN services of 2017 say that they do not store log files (Eddy, 2017). However, sometimes this is specified as logs of a user's browsing history, which does not mean that the provider will still have access to logs of timestamps, user names, payment details and so on. According to one of these popular VPN services, it is a myth that VPN providers do not log personal identifying information[4]. Most of the VPN providers log the source IP address of the user when he/she logs into the VPN. One of the providers that states not to record any log data argues it is able to do so because it is based in Panama, which has lenient data retention laws that allow a provider to refrain from logging.

SOCKS

In more than half of tutorials it is recommended to use a SOCKS proxy on top of a VPN. According to one tutorial, SOCKS proxies are often not publicly listed or well-known and will thus not be widely blacklisted by merchants and detected by fraud detection systems. This means that SOCKS proxies can generally be used to access all sorts of websites, whereas this may be harder with VPN services that are known to be used for criminal activity. To use a SOCKS proxy, a user enters the IP address and port number of the proxy, which can be found in proxy directories online, into a configuration screen of the browser (Roberts et al., 2010). SOCKS proxies are sometimes offered per city and can thus make it seem as if a user is from that city, as the IP address will be located there. These characteristics can be used to trick fraud detection systems, which may not notice a deviation from regular payment patterns, as the cardholder is impersonated and it thus seems as if payments are being done from the same location.

SOCKS proxies often run on the machines of users without their knowledge when they are part of a botnet. An attacker would install a tool on compromised machines that can open chosen ports, port 8975 for SOCKS, turning it into a SOCKS proxy (Kaspersky Lab, 2016a). A network of such compromised machines can be used for spam distribution (Göbel, Holz & Trinius, 2009). In this way spam server blacklists can be circumvented (Ianelli & Hackworth, 2007), as the IP addresses of the compromised machines most likely do not appear on blacklists yet. According to Roberts et al. (2010), a problem for users of SOCKS proxies is that it is impossible to find out who runs it. They could, for example, be

[4] https://www.goldenfrog.com/blog/myths-about-vpn-logging-and-anonymity

run by a government, which would allow analysis of who is using the proxy and what they are looking at. Trusting the wrong SOCKS proxy provider could thus endanger fraudsters.

RDP

Remote desktop protocols (RDPs), or remote desktop connections, were mentioned in one in five of the analysed tutorials. They are used by carders to access someone else's computer and to thus make it seem as if the carding-related activity is being done from that computer. It has a similar effect to using a proxy, making the user's activities appear to come from the address of the remote machine. RDP is recommended in one tutorial as an alternative to a SOCKS proxy, as the accessed computer can also be based in the area of the cardholder. Remote desktop connections to legitimate computing resources are offered by legitimate companies, just as is the case with VPNs. However, remote desktop connections to hacked computers are also offered on underground marketplaces. In such a case, the owner of the computer will still have access to the computer, but carders will use them at the same time as proxies for carding activity.

Goncharov (2015) found that online criminals scan such hacked computers for online vendor accounts (such as Amazon & eBay credentials for example), payment systems (such as PayPal) and gaming sites amongst other things. The found credentials can then be sold on underground forums and be abused for fraud purposes. Furthermore, marketplaces have sprung up, purely focusing on the purchase of hacked RDP servers. One of these marketplaces[5] offered over 70.000 hacked servers from all over the world that can be accessed with RDP, for six dollars per server (Kasperky Lab, 2016a). However, the hacked computer's IP addresses used by online criminals were later leaked (Kaspersky Lab, 2016b). This could steer law enforcement into the right direction, as they then can find out which computers connected to the compromised RDP, to identify the IP addresses of online criminals and consequently locate them. Fully trusting a RDP can thus be a behavioural mistake, as data leaks on marketplaces may lead to the apprehension of the users using RDPs for illicit online activity.

DNS leaks

It is recommended in three tutorials to do a Domain Name System (DNS) leak test, to test whether the traffic of a user of proxies or anonymity services is completely routed through the service's servers. DNS translates domain names, such as example.com, to IP addresses. ISPs will provide a DNS server for customers to use, and these servers will commonly log addresses which users have looked up. If an operating system still uses the default DNS servers ascribed to a user by an ISP even when a proxy is in place, analysis of the DNS logs can be used to determine the browsing activity of the user (Crawford, 2015). There are tools[6] available to check whether one's DNS is leaking, which were recommended in some tutorials. If a user finds out that not all of the traffic goes through the

[5] http://xdedic.biz

[6] For example https://www.dnsleaktest.com/

proxy, he/she might obtain another proxy and do a DNS leak test again, until all traffic routes through the proxy. Not doing such a test could lead to a failure in spotting wrong configurations, leading to traffic not routing through proxies and making it easier for law enforcement to trace a carder.

MAC address spoofing

MAC spoofing is mentioned in two tutorials. Media Access Control (MAC) addresses are unique identifiers assigned to devices, such as a computer or smartphone, on a network and are used to identify these devices. MAC addresses are often printed on the hardware of the devices (Pandey & Saini, 2012). There are however methods to change the MAC address on a device. This is commonly referred to as MAC spoofing (Gupta et al., 2009). Since MAC addresses are only visible to devices in the same network, they are of little use or relevance in the online world. However, mobile devices share MAC addresses with public WiFi access points, even if they do not connect to the access point. Logs of when a MAC address was seen by a particular access point can be used to infer information such as location, but can also be correlated with CCTV to identify an individual (Minch, 2015). It is thus recommended to users in two tutorials to use tools that can spoof MAC addresses. Some anonymity-focused operating systems popular among online criminals, such as TAILS[7], offer tools for MAC spoofing. The analysed tutorials do not specify why one would spoof a MAC address, which could indicate that it is not seen as a very important step and might be ignored by some users. However, failing to spoof could lead to a carder's identity becoming known.

Tor

Tor was, surprisingly, only mentioned in two of the twenty-five tutorials. However, the tutorials were all distributed on a hidden service only accessible through Tor, with the exception of applications such as Tor2Web[8], which implies that carders who accessed the tutorials through the hidden service will already be using the network. Tor uses onion routing, which is an anonymity technology that fragments the links between client and server in various steps by sending a message through various random relays. Before data is sent through the Tor network of random relays, a layer of encryption is added for every relay in the route, which are removed per step, 'peeled off', hence the onion metaphor, leading to an unencrypted plaintext message at the point of arrival (Reed, Syverson & Goldschlag, 1998). An exit node, the last relay in the chain before the receiver of the message, can thus observe the content of messages if they are not encrypted by the user, but will not see the source of the message (Li et al., 2013). The technical workings of Tor are visualised in the graph below.

[7] https://tails.boum.org

[8] https://tor2web.org; Tor2web makes hidden services, i.e. sites with a .onion suffix, available through regular Web browsers.

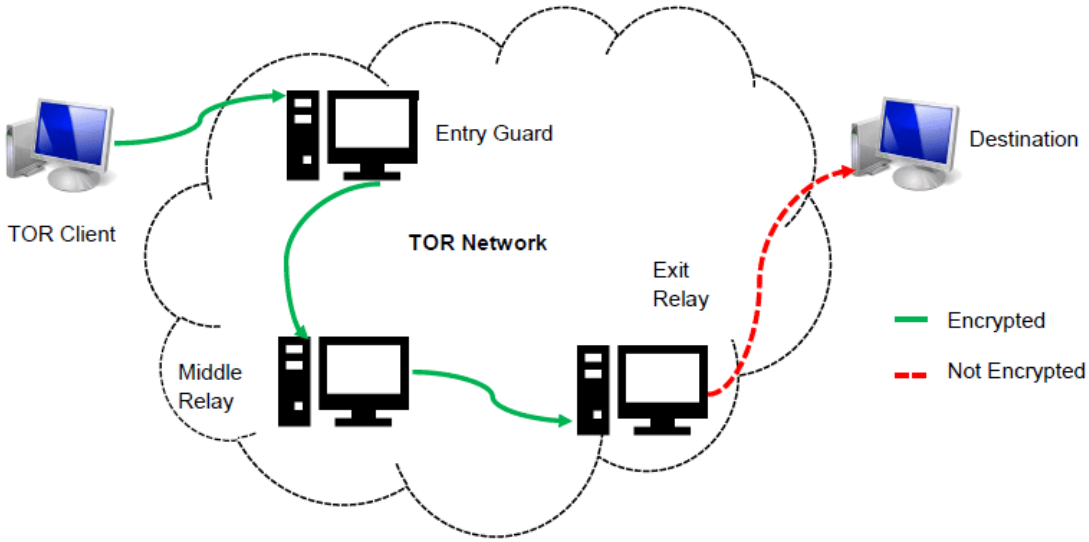

Figure III[9]

Tor can be used as a browser that can access normal top level domains (.com, .co.uk, .nl etc.), but also offers 'hidden services', or .onion pages, which are only accessible through the Tor network. They do not reveal the IP-addresses of the creator of the hidden service (Dingledine, Matthewson & Syverson, 2004). Research has shown that almost sixty percent of known hidden services focus on the trade in drugs and weapons, counterfeit products, stolen credit cards and otherwise hacked accounts (Spitters, Verbruggen & van Staalduinen, 2014). More niche crime areas on hidden services range from illegal wildlife trafficking (INTERPOL, 2017) to mobile malware (Kaspersky Lab & INTERPOL, 2017). Because of the increased anonymity Tor offers over regular Web browsing, it has become a popular and indispensable tool for online criminals.

Lewman (2016) has argued that a hidden service is just a single machine connected to the Internet and that there will thus still be opportunities for investigative and technical approaches to deanonymise traffic and users. Law enforcement operations, such as the arrest of the creator of the first Silk Road marketplace (USA vs. Ross William Ulbricht, 2013), 'Operation Onymous' (Afilipoaie & Shortis, 2015) and 'Operation Bayonet' (van Wegberg et al., 2017), show that opportunities for arrests still exist and that users of Tor's hidden services are at least not all fully anonymous. Biryukov, Pustogarov and Weinmann (2013) have, for example, shown that an attacker can correlate IP addresses to hidden services after taking over one or more guard nodes, which are extra nodes in the Tor network that the hidden service trusts and selects for users to reach its service through. Guard nodes were introduced to stop attackers from finding out the IP address, as the attacker would then never own the node next to hidden service (Øverlier & Syverson, 2006), but with the method of Biryukov, Pustogarov and Weinmann (2013) the attacker takes over exactly that node. Other vulnerabilities on Tor have been exploited by law enforcement and researchers. An interesting example of this is when the FBI subpoenaed Carnegie Mellon University researchers for information that could

[9] http://www.dataforensics.org/tor-browser-forensics/

lead to the IP address of a hidden service user they were after[10].

Other anonymisation services or 'darknets' similar to Tor have been available for many years, such as I2P[11] and Freenet[12], but have not enjoyed the same popularity as Tor. More recently, OpenBazaar[13], a peer to peer software that connects buyers directly to sellers, has been developed. More decentralised or distributed initiatives could, from a technical point of view, make it increasingly hard to discover the real identity of illicit users. However, vulnerabilities in software have been used by law enforcement for identification. Vulnerabilities in Tor have led to the identification and subsequent arrests of hidden service users who enabled JavaScript in their Tor browser[14]. Some websites will not work without JavaScript enabled, but it thus also has been exploited to uncover user's IP and MAC addresses. This is again a trade-off between usability and security, which will be acted on depending on the community's recommendations and preferences of individual users.

Financial services

Bitcoin and mixing services

The cryptocurrency Bitcoin is mentioned in five tutorials. Carders' two main uses of Bitcoin, and other cryptocurrencies, are to pay for stolen cards and to obfuscate the money trail from cardholder to carder. Bitcoin is a pseudonymous system that aims to provide more privacy than fully identified payments through banks. Bitcoin was created to establish direct financial transactions without the intervention of a third party. It also solves the problem of double-spending, which is the spending of the same bitcoins multiple times, with the introduction of the blockchain. The blockchain is a distributed public ledger of all bitcoin transactions ever made and serves as a database that checks on double-spending with user's verified signatures (Nakamoto, 2008). A public database of transactions seems to defeat the purpose of privacy enhancement, but the only identifying information is some seemingly random numbers (Hobson, 2013), which include the public key of the payer and payee, amount of bitcoins being sent and timestamps. This represents the flow of bitcoins between users over time, but users can generate a new public-private key-pair, which in public-key cryptography are used to encrypt and decrypt messages, for every new transaction to enhance their privacy (Reid & Harrigan, 2013) or use bitcoin mixers to obfuscate the money trail.

The private keys required to authorise Bitcoin transactions are stored in a wallet file. A wallet file can hold the private keys for many different addresses. Users can have endless numbers of addresses and wallets. Whilst they can use these to

[10] https://motherboard.vice.com/read/carnegie-mellon-university-attacked-tor-was-subpoenaed-by-feds
[11] https://geti2p.net/
[12] https://freenetproject.org/
[13] https://www.openbazaar.org/
[14] https://blog.torproject.org/blog/hidden-services-current-events-and-freedom-hosting

transfer their bitcoins from one to the other to obfuscate the money trail and create stronger privacy, network analysis can still - in some cases - infer information about the path, as all bitcoin transactions are logged in the blockchain (UK Government Office for Science, 2016). While associating addresses with real life identities is still very challenging, network analysis can be a threat for nefarious Bitcoin users. Mixing services try to further complicate the process for parties that want to retrace the origins of bitcoins. In such a service, bitcoins are sent to the mixing service, which sends the same amount of random coins from other users, minus a fee, back to 'mix' the bitcoins and in this way makes the link between sender and recipient harder to trace. As long as the mixing service keeps the information of whose coins it mixed private, it will be basically impossible for an external observer to find out the identities of people behind addresses (Moser, Böhme, & Breuker, 2013). The danger of sending bitcoins to mixers for users is that there is a chance that the service is a scam, which means they could lose all the coins they have sent. However, cryptographically secure mixing methods, such as CoinShuffle (Ruffing, Moreno-Sanchez & Kate, 2014), have been proposed to reduce the need for trust in a mixing provider.

Because of the public nature of the blockchain, many researchers and commercial entities have explored possibilities of tracing bitcoins across users. Tools such as BitCluster[15], Chainalysis[16] and Elliptic[17] analyse the blockchain to group Bitcoin transactions together that are seemingly related and find the origins of payments. Biryukov, Khovratovich and Pustogarov (2014) have shown how to deanonymise a significant fraction of Bitcoin users and in this way linking user's pseudonyms to their IP addresses. Reid and Harrigan (2013) suggest that a user directory can be partly built by associating Bitcoin users and their public keys with offline information. Stores that accept Bitcoin, exchanges will namely store identifying information on users, such as e-mail addresses, bank account details, IP addresses and so on. The authors also build a tool to analyse the laundering process and notice how funds are quickly transferred through public-keys, which shows an attempt of laundering. While this is circumstantial evidence, it can lead to a centralised (mixing) service that could have more information on the user. Newer alternative cryptocurrencies (altcoins), such as Monero, try to complicate traceability problem by employing different cryptographic methods that group transactions together.

Most users acquire bitcoins through exchanges with bank transfers. Also for converting bitcoins back to traditional currencies, exchanges are used. However, using exchanges can lead to operational risks (Hayashi, Moore & Sullivan, 2015). Moore and Christin (2013) found that approximately 45% of exchanges close down, often after a security breach in which bitcoins are stolen by hackers, such as recently with Hong Kong-based exchange Bitfinex from which bitcoins

[15] https://www.bit-cluster.com/
[16] https://www.chainalysis.com
[17] https://www.elliptic.co/

amounting to $65 million[18] were stolen. There is often no guarantee that users of exchanges get their money back after such breaches. According to Meiklejohn et al. (2013), the fact that law enforcement agencies can subpoena exchanges, in combination with researchers' ability to track bitcoins through the blockchain, make Bitcoin an unappealing option for large scale money laundering, as this might lead to the identity of illicit users. Still, laundering money from stolen payment cards to bitcoins or alternative cryptocurrencies is recommended in some carding tutorials (van Hardeveld, Webber & O'Hara, 2016), as bitcoins could be bought with the cardholder's personal details, making identification at the exchange impossible. Users can also avoid exchanges by using services that connect people willing to trade cryptocurrencies in person and exchange it for cash[19]. Still, the public nature of the Blockchain can be a risk for carders, if they do not obfuscate their transactions properly and leave a trace to centralised services to which they have given personal information.

Offline

Drops and postal services

Drops are mentioned in 20% of tutorials. They are (empty) houses, post boxes or other places that are used for the delivery of illicit goods. Carders use them for extra security when they want to obtain physical goods with stolen card details. This shows that there is an important offline element to cybercrime, which sometimes can even be local if people work together in the same areas (Lusthaus & Varese, 2017). However, it is often stressed in carding tutorials that a drop address cannot have any links to the carder's life and sometimes it is even recommended to set-up schemes in which the carder hires someone to pick-up packages from the drop and deliver to his/her real address (van Hardeveld, Webber & O'Hara, 2016). This is the case, as it will then be harder for law enforcement to trace packages to the carder. Such intermediaries are also known as 'packet mules' (Europol, 2016). Carders do not only ship illegally obtained products to their homes. Hutchings and Holt (2015) also found that plastics, which are empty cards on which stolen data can be loaded to then be used in stores and at ATMs, are sent by post. The drug trade on Tor is even more dependent on drop addresses and the postal system than carding, as it cannot be done purely digitally. As drugs are often sent internationally, they have to go through customs, who may use sniffer dogs and check odd-shaped packages. This is why drug sellers mimic traditional post and use special concealment techniques (van Hout & Bingham, 2013).

Using postal services creates a risk. Laziness and complacency might lead sellers to not properly conceal drugs (Martin, 2013). The same can occur with the usage of drops for carders, as this can be seen as an extra unnecessary hassle to them. Even if a drop is used, police surveillance could be in place at the drop. Therefore, there are many risks in this part of the process that can lead to interception of the illicit goods, or even to the real identity of the buyer. Impatience to get products delivered or laziness to properly arrange for a safe

[18] http://www.bbc.co.uk/news/business-36962254

[19] Such as https://localbitcoins.com/ and https://localmonero.co/

drop can thus lead to the apprehension of cybercriminals. The problem with empty houses is that activity around these can cause suspicion in a neighbourhood and lead to neighbours calling the police. Places with access to postal boxes are also risky, as they may employ CCTV. Therefore, it is hard to know whether drops are trustworthy and they may be hard to get and access. A better insight into the usage of drops and the postal system by buyers and sellers could thus lead to new chances for law enforcement.

Typology of potential pitfalls for carders

From our analysis it can be concluded that there are various overlapping pitfalls in carders' usage of tools, which could lead back to their real identities. Therefore, below, we list the pitfalls identified from the analysed tools. The pitfalls carders can be prone to can be put into two categories: behavioural and technical.

Behavioural	- Result-focussed - Overconfidence, laziness and forgetfulness - Trusting the wrong tool providers - Trusting the wrong people - Transcending online-offline boundaries - Inadequate obfuscation
Technical	- Vulnerabilities in tools

Figure IV Classes of pitfalls

Discussion

Behavioural pitfalls make up the majority of potential mistakes by carders that have been identified in the literature. These have been subdivided in *result-focussed*; *overconfidence, laziness and forgetfulness*; *trusting the wrong tool providers*; *trusting the wrong people*; *transcending online-offline boundaries* and *inadequate obfuscation*. Furthermore, one technical pitfall was identified: *vulnerabilities in tools*.

Result-focussed

Being too *result-focussed* has been identified as a behavioural pitfall, because carders may employ fewer security measures when they want to obtain a quick profit. Sundaresan et al. (2016) have already shown that only 4.8% of merchants on underground forums use a VPN. PGP has not been mentioned in any tutorials, but its usage can also be ascribed to this potential pitfall. According to Cox (2016), many users strengthen their operational security by encrypting their personal communication with PGP, as staff members of marketplaces often recommend this and provide guidance how to use it. Still, as Soska and Christin (2015) measured in January 2015, employment of PGP has not reached a 100%. PGP is time-consuming and perhaps complex for some non-technical users, which can explain these numbers. When marketplaces are seized by law enforcement agencies, however, they will often have access to all the public and

private messages, which could reveal identifying information about users, should they fail to encrypt their messages. In response to such events, some marketplaces started automatically encrypting all messages of users[20], so that unencrypted sensitive information is never accidentally sent to others. In recent infiltration operations, law enforcement managed to 'turn off' this automated encryption of a marketplace on Tor by altering the source code, allowing them to collect personal information of users, who thought their messages were still encrypted[21].

Overconfidence, laziness and forgetfulness

Closely related to *result-focussed* is *overconfidence, laziness and forgetfulness*. The result from both behavioural pitfalls is the same: adoption of fewer secure tools or methods. In the case of *overconfidence, laziness and forgetfulness* the carder will be aware of various available tools to stay secure, but not use them all. He/she will fail to see, or simply forget, the necessity of them and decide the time and effort spent establishing them outweighs the potential benefit. Not using bitcoin mixers, DNS leak tests and/or drops are such commonly ignored methods. The purpose of these tools is to ensure that the paths to users' real identity is obfuscated. When a carder does not employ these methods, and encounters no adverse effects, the added effort will not appear beneficial. Sunstein (1997) has referred to such behaviour as systematic overconfidence in risk judgements. Some users believe that low-probability risks are more likely to materialise for others than for themselves. In prospect theory (Kahneman & Tversky, 1979) this is explained by the finding that people are limited in their comprehension and evaluation of extreme probabilities. Such events are thus deemed unlikely or ignored altogether. These theories will be used to analyse overconfidence, laziness and forgetfulness of cybercriminal decision-making in future work. By doing so, some of the problems of crime script analysis can be overcome, especially in the conception of the criminal as an overly rational calculator (Ekblom and Gill 2016; Wortley 2002; Cornish and Clarke 2003).

Trusting the wrong tool providers

Proxy-based tools are based on technical mechanisms that strengthen the privacy of a user. These tools are intended to protect people's privacy and will be used for both legitimate and illicit purposes, which is why technologies such as Tor are often described as a double-edged sword (Chertoff, 2017; Jardine, 2015). However, there is still uncertainty for illicit users of some of these tools, such as VPN services as they can cooperate with law enforcement or even be run by them. This difficulty in determining the safety of certain tools by miscreants can be used as a deterrent by law enforcement. Tool providers may also have to abide by enforced data sharing laws. While they might advertise they do not share info with third parties, they may still be legally required to when served with a warrant. A failure to identify which tool providers cooperate with law enforcement can be seen as a behavioural pitfall. The fact that this is often not

[20] https://www.deepdotweb.com/2014/01/23/interview-with-outlaw-market-admin/

[21] See http://politiepcvh42eav.onion.link/hansafaq.html

public information will complicate decision-making for carders on which tools to trust.

Trusting the wrong people
To deliver products to drops or buyer's real addresses, a buyer and a seller need to exchange personal information, such as a (drop) address, in messages. A potential behavioural pitfall for miscreants is that they trust the wrong people, send them personal information and do business with them. Because of the nature of the anonymous environment, users may fail to identify that other users are scammers or undercover law enforcement (Décary-Hétu & Leppänen, 2016; Lusthaus, 2012). For example, once a drop address has been sent to an undercover agent, they can surveil the place and identify the individual that picks up the delivered packages. Also, money or packet 'mules' may know the real identity of buyers and sellers and could give up this information to law enforcement.

Transcending online-offline boundaries
While carders may have flawless online security, they may still encounter pitfalls when they move into the real-world realm. For example, as discussed earlier, mobile devices' MAC addresses are shared with public WiFi access points, which is data that, with the proper correlation, can be used to apprehend criminals. According to Aldridge & Askew (2017), the key risk of detection for users of cryptomarkets by law enforcement is found in offline activities, such as packaging and delivering. Another example is that when large amounts of cryptocurrencies are converted to fiat currency, banks or law enforcement agencies may be alerted, even if a carder took steps to obfuscate the trail from the illegal product sales to his/her own bank account. A lack of legitimate source of income could be seen as an indicative sign for money laundering, after which specialised units may start an investigation into the funds.

Lacking obfuscation
Not using the right, or enough, tools to make sure the path from illegal activity to the individual user is obfuscated is a behavioural pitfall that can lead to the apprehension of carders. Bitcoin mixing services might not have enough customers to mix properly (Meiklejohn et al., 2013). Furthermore, 'know-your-customer' regulations demand cryptocurrency exchanges to verify the identities of customers (UK Government Office for Science, 2016). This can help law enforcement in detecting illicit users. If carders use proxy-based services which do not encrypt and/or store log files, law enforcement can obtain information about the carder by issuing a warrant. This pitfall is similar to *trusting the wrong tool providers*, but the difference here is that carders themselves can also leave traces to their identity by not being sufficiently cautious with regard to where their information is stored, such as at centralised Bitcoin exchanges.

Vulnerabilities in tools
Vulnerabilities in tools can be exploited by law enforcement agencies to expose, for example, IP addresses of users or hidden services. While it may seem that such technological pitfalls cannot be avoided by criminal actors, this is not

always the case. In the case of the previously discussed example of the JavaScript vulnerability in the Tor browser used to identify some users of hidden services, only the users that enabled JavaScript in the browser were identified. This is also the case for the usage of discontinued software, as developers will not continue to patch vulnerabilities anymore and its usage is thus a potential pitfall.

Conclusion and future work

In this study we have explored how carders use tools to stay anonymous in the process of obtaining and cashing out stolen payment card data and what the potential pitfalls are in using these tools. We have identified six types of potential behavioural pitfalls and one technical one. These can be used by researchers and law enforcement to understand and explore further how carders, and possibly other cybercriminals too, can potentially make mistakes and how these could lead to their apprehension.

The success of carders, and users of underground markets more generally, partly depends on their correct uptake, and continued use, of tools such as those discussed in this paper. Therefore, future research should focus more on the operational security of individual users of underground markets. This would complement research looking at the workings of marketplaces. Behavioural analyses of the ways in which users of online illicit markets take up, use and misuse tools is needed to better understand what countermeasures to take. Such research can give law enforcement insights into common missteps in decision-making processes of online criminals, leading to better informed investigations. It is also important to bear in mind the fact that carders will deviate from the commonly perceived optimal norms established in tutorials and forum discussions (van Hardeveld, Webber & O'Hara, 2016). Some studies have already looked at under what conditions online drug vendors are willing to take risk, such as trade internationally (Décary-Hétu, Paquet-Clouston & Aldridge, 2016) and what the risk-reducing strategies are of actors on stolen data markets (Holt et al., 2015). Researchers' focus should lie more strongly on how and why deviations from the optimal usage of tools occur. Contingencies that lead to pragmatic decisions will occur and can in future work be explored with concepts from, for example, behavioural economics such as fast and slow thinking (Kahneman, 2011) and overconfidence in risk judgements (Sunstein, 1997), amongst others.

A cooperation between researchers and law enforcement agencies can "improve the quality and quantity" of such research that can help in understanding illicit market actors, suggests Holt (2017: p. 4). Such collaboration might be hard to establish though, as law enforcement agencies might not be able to share information related to ongoing investigations and prosecutions, he argues. It may be more feasible to interview law enforcement experts. Also, in future work, active and convicted users of such marketplaces could also be interviewed to obtain first-hand information on the usage of tools. Tool providers can also be given questionnaires or be interviewed to obtain a proper overview of how tools are used by cybercriminals. Only with a proper understanding of how users of underground marketplaces use tools that facilitate their trade, keep them

anonymous and out of hand of law enforcement, can adequate methods for disruption, interception and prevention be designed.

It must be noted, as this work is based on an analysis of 25 freely available tutorials, that more pitfalls may be discovered in future research when a different dataset is used. However, this typology should be treated as an initial exploration of the pitfalls carders, and possibly other online criminals, encounter and can serve as a basis for future cybercrime research, which explores the possible ways in which cybercriminals can be identified.

Acknowledgements
We would like to thank Costel Ion and Dominic Hobson for their helpful insights and comments. Also, we are grateful to TNO for providing access to their tool, the 'Dark Web Monitor', which has helped in collecting data which would otherwise not have been accessible to us.

Funding
This work was supported by the EPSRC, grant number EP/G036926/1. The Digital Economy Theme is a Research Councils UK cross council initiative led by EPSRC and contributed to by AHRC, ESRC, and MRC. Kieron O'Hara was partly supported by EPSRC project SOCIAM, grant number EP/J017728/2. Opinions, findings and conclusions in this article are not necessarily held by the sponsor.

References
Afilipoaie, A., & Shortis, P. (2015). Operation Onymous: International law enforcement agencies target the Dark Net in November 2014. *Global Drug Policy Observatory*. Retrieved from https://www.swansea.ac.uk/media/GDPO%20SA%20Onymous.pdf.

Aldridge, J., & Askew, R. (2017). Delivery dilemmas: How drug cryptomarket users identify and seek to reduce their risk of detection by law enforcement. *International Journal of Drug Policy*, *41*, 101–109.

Balogun, A., & Zhu, S. (2013). Privacy Impacts of Data Encryption on the Efficiency of Digital Forensics Technology. *International Journal of Advanced Computer Science and Applications*, *4*(5), 36–40.

Benjamin, V., Li, W., Holt, T., & Chen, H. (2015). Exploring Threats and Vulnerabilities in Hacker Web: Forums , IRC and Carding Shops. In *Proceedings of IEEE International Conference on Intelligence and Security Informatics (ISI)*, 85–90.

Biryukov, A., Pustogarov, I., & Weinmann, R. (2013). Trawling for Tor Hidden Services: Detection, Measurement, Deanonymization. In Proceedings of *IEEE Symposium on Security and Privacy*, 80–94.

Biryukov, A., Khovratovich, D., & Pustogarov, I. (2014). Deanonymisation of clients in Bitcoin P2P network. In *Proceedings of the ACM SIGSAC Conference on*

Computer and Communications Security, 15–29.

Chertoff, M. (2017). A public policy perspective of the Dark Web. *Journal of Cyber Policy*, *2*(1), 26–38.

Cornish, D. (1994). The procedural analysis of offending and its relevance for situatinoal crim eprevention. In R.V. Clarke, *Crime Prevention Studies*, Volume 3, Monesy, NY: Criminal Justice Press, 151-196.

Cornish, D. B., & Clarke, R. V. (2003). Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. In M. Smith & D. B. Cornish (eds.), *Crime Prevention Studies: Vol. 16. Theory for practice in situational crime prevention*. Monsey: Criminal Justice Press, 41-96.

Cox, J. (2016). Staying in the shadows: the use of bitcoin and encryption in cryptomarkets. In EMCDDA project group (Eds.), *The internet and drug markets*, 41-47. Publications office of the European Union: Luxembourg.

Crawford, D. (2014). EarthVPN user arrested after cops find logs. Retrieved from https://www.bestvpn.com/blog/8383/earthvpn-user-arrested-cops-find-logs/.

Crawford, D. (2015). A complete guide to IP leaks. Retrieved from https://www.bestvpn.com/blog/31750/a-complete-guide-to-ip-leaks/.

Décary-Hétu, D., & Leppänen, A. (2016). Criminals and signals: An assessment of criminal performance in the carding underworld. *Security Journal*, *29*(3), 442–460.

Décary-Hétu, D., Paquet-Clouston, M., & Aldridge, J. (2016). Going international? Risk taking by cryptomarket drug vendors. *International Journal of Drug Policy*, *35*, 69–76.

Décary-Hétu, D., & Giommoni, L. (2017). Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous. *Crime, Law and Social Change*, *67*(1), 55–75.

Dingledine, R., Mathewson, N., & Syverson, P. (2004). Tor: The second-generation onion router. *Proceedings of the 13th Conference on USENIX Security Symposium*.

Dykstra, J., & Sherman, A. T. (2011). Understanding Issues in Cloud Forensics: Two Hypothetical Case Studies. *Journal of Network Forensics*, *3*(1), 19–31.

Eddy, M. (2017). The Best VPN Services of 2017. Available at http://uk.pcmag.com/software/138/guide/the-best-vpn-services-of-2017.

Ekblom, P. and Gill, M. (2016). 'Rewriting the Script: Cross-Disciplinary Exploration and Conceptual Consolidation of the Procedural Analysis of Crime'. *European Journal on Criminal Policy and Research, 22*(2), 319-339.

Europol. (2014). *The Internet Organised Crime Threat Assessment (iOCTA)*. Retrieved from https://www.europol.europa.eu/sites/default/files/publications/europol_iocta_web.pdf.

Europol. (2016). The Internet Organised Crime Threat Assessment. Retrieved from https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2016.

Glenny, M. (2011). Darkmarket: Cyberthieves, cybercops and you. London: The Bodley Head.

Göbel, J., Holz, T., & Trinius, P. (2009). Towards Proactive Spam Filtering. In U. Flegel & D. Bruschi (eds), *Detection of Intrusions and Malware and Vulnerability Assessment*, 38–47. Como, Italy: Springer.

Goncharov, M. (2012). Russian Underground 101. Cupertino, CA: Trend Micro Incorperated.

Goncharov, M. (2015). Russian Underground 2.0. Cupertina, CA: Trend Micro Incorperated.

Grabosky, P.N. (1996). Uninted Consequences of Crime Prevention. In R. Homel and J. Clarke (eds), *Crime Prevention Studies*, *5*, 25-56.

Hardeveld, G. J. van, Webber, C., & O'Hara, K. (2016). Discovering credit card fraud methods in online tutorials. In *Proceedings of the Workshop on Online safety, trust and fraud prevention. ACM Web Science Conference*, 1-5.

Hayashi, F., Moore, T., & Sullivan, R. J. (2015). The Economics of Retail Payments Security. In *Fifth International Payments Policy Conference: The Puzzle of Payments Security, Federal Reserve Bank of Kansas City*, 1–60.

Hawkins, S., Yen, D. C., & Chou, D. C. (2000). Awareness and challenges of Internet security. *Information Management & Computer Security*, *8*(3), 131–143.

Healey, N. J., Angelopoulou, O., & Evans, D. (2013). A discussion on the recovery of data from a virtual machine. In *Proceedings of the 4th International Conference on Emerging Intelligent Data and Web Technologies*, 603–606.

Hobson, D. (2013). What is Bitcoin? *XRDS: Crossroads, The ACM Magazine for Students*, *20*(1), 40–44.

Holt, T. (2006). Subcultural evolution? Examining the influence of on- and off-line experiences on deviant subcultures, *Deviant Behaviour, 28 (2)*, 171-198.

Holt, T. J., Smirnova, O., Chua, Y. T., & Copes, H. (2015). Examining the risk

reduction strategies of actors in online criminal markets. *Global Crime*, *16*(2), 81–103.

Holt, T. J. (2017). Identifying gaps in the research literature on illicit markets online. *Global Crime*, *18*(1), 1–10.

Hutchings, A., & Holt, T. J. (2015). A Crime Script Analysis of the Online Stolen Data Market. *British Journal of Criminology*, *55*(3), 596–614.

Hutchings, A., & Holt, T. J. (2017). The online stolen data market: disruption and intervention approaches. *Global Crime*, *18*(1), 11-30.

Ianelli, N., & Hackworth, A. (2007). Botnets as a Vehicle for Online Crime. *The International Journal of Forensic Computer Science*, *1*, 19–39.

INTERPOL (2017). Illegal Wildlife Trade in the Darknet. Retrieved from https://www.interpol.int/News-and-media/News/2017/N2017-080.

Jardine, E. (2015). The Dark Web Dilemma: Tor, Anonymity and Online Policing, (21). Global Commission on Internet Governance paper series no. 21. Retrieved from: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2667711.

Kahneman, D., & Tversky, A. (1979). Prospect Theory: An Analysis of Decision under Risk. *Econometrica*, *47*(2), 263–292.

Kaspersky Lab. (2016a). The xDdedic Marketplace.
Retrieved from
https://securelist.com/files/2016/06/xDedic_marketplace_ENG.pdf.

Kaspersky Lab. (2016b). The Tip of the Iceberg. An Unexpected Turn in the xDedic story. Retrieved from https://securelist.com/blog/research/75120/the-tip-of-the-iceberg-an-unexpected-turn-in-the-xdedic-story/.

Kaspersky Lab & INTERPOL. (2017). Mobile Malware Evolution 2016. Retrieved from https://securelist.com/files/2017/02/Mobile_report_2016.pdf.

Ladegaard, I. (2017). We Know Where You Are, What You Are Doing and We Will Catch You. Testing Deterrence Theory in Digital Drug Markets. *British Journal of Criminology*, 1–20. Retrieved from http://doi.org/10.1093/bjc/azx021

Lewman, A. (2016). Tor and links with cryptomarkets. In EMCDDA project group (Eds.), *The internet and drug markets*, 33-39. Publications office of the European Union: Luxembourg.

Li, B., Erdin, E., Gunes, M. H., Bebis, G., & Shipley, T. (2013). An overview of anonymity technology usage. *Computer Communications*, *36*(12), 1269–1283.

Lusthaus, J. (2012). Trust in the world of cybercrime. *Global Crime*, *13*(2), 71–94.

Lusthaus, J. & Varese, F. (2017). Offline and Local: The Hidden Face of Cybercrime. *Policing: A Journal of Policy and Practice*, 1–11. Retrieved from http://doi.org/10.1093/police/pax042.

Martin, J. (2013). Lost on the Silk Road: Online drug distribution and the "cryptomarket." *Criminology and Criminal Justice*, *14*(3), 351–367.

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., & Savage, S. (2013). A fistful of Bitcoins: Characterizing payments among men with no names. In *Proceedings of the Internet Measurement Conference*, 127–140.

Minch, R.P. (2015). Location Privacy in the Era of the Internet of Things and Big Data Analytics. In *proceedings of the 48th Hawaii International Conference on System Sciences*, 1521-1530.

Moore, T., & Christin, N. (2013). Beware the middleman: Empirical analysis of Bitcoin-exchange risk. *Financial Cryptography and Data Security, Lecture Notes in Computer Science*, *7859*, 25–33.

Moser, M., Böhme, R., & Breuker, D. (2013). An inquiry into money laundering tools in the Bitcoin ecosystem. In *Proceedings of the eight Symposium on Electronic Crime Research*, 1-17.

Motoyama, M., McCoy, D., Levchenko, K., Savage, S., & Voelker, G. M. (2011). An Analysis Of Underground Forums. In *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement*, 71-79.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf.

Øverlier, L., & Syverson, P. (2006). Locating Hidden Services. *In Proceedings of the IEEE Symposium on Security and Privacy*, 100–114.

Pandey, A., & Saini, J. R. (2012). Counter Measures to Combat Misuses of MAC Address Spoofing Techniques. *Int. J. Advanced Networking and Applications*, *3*(5), 1358–1361.

Reed, M. G., Syverson, P. F., & Goldschlag, D. M. (1998). Anonymous connections and onion routing. *IEEE Journal on Selected Areas in Communications*, *16*(4), 482–494.

Reid, F., & Harrigan, M. (2013). An Analysis of Anonymity in the Bitcoin System. In Y. Altshuler, Y. Elovici, A. B. Cremers, N. Aharony, & A. Pentland (Eds.), *Security and Privacy in Social Networks* (pp. 197–223). New York, USA: Springer.

Roberts, H., Zucherman, E., York, J., Faris, R., & Palfrey, J. (2010). *2010 Circumvention Tool Usage Report*. Retrieved from

https://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/2010_Circumvention_Tool_Usage_Report.pdf.

Ruffing, T., Moreno-Sanchez, P., & Kate, A. (2014). CoinShuffle : Practical Decentralized Coin Mixing for Bitcoin. In *19th European Symposium on Research in Computer Security (ESORICS'14)*, *LNCS 8713*.

Soska, K., & Christin, N. (2015). Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem. In *Proceedings of 24th USENIX Security Symposium*, 33–48.

Spitters, M., Verbruggen, S., & Staalduinen, M. van. (2014). Towards a Comprehensive Insight into the Thematic Organization of the Tor Hidden Services. *IEEE Joint Intelligence and Security Informatics Conference*, 220–223.

Sundaresan, S., McCoy, D., Afroz, S., & Paxson, V. (2016). Profiling Underground Merchants Based on Network Behavior. In *Proceedings of the eleventh Symposium on Electronic Crime Research*.

Sunstein, C.R. (1997). Behavioural Analysis of Law. *University of Chicago Law Review*, 64, 1175-1197.

Thomas, K., Yuxing, D., Huang, D., Holt, T. J., Kruegel, C., Mccoy, D., Bursztein, E.,Grier, C., Savage, S. & Vigna, G. (2015). Framing Dependencies Introduced by Underground Commoditization. In *Proceedings of the Workshop on the Economics of Information Security*, 1–24.

UK Government Office for Science. (2016). *Distributed Ledger Technology: beyond block chain*. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf.

United States of America vs. Ross William Ulbricht (2013). Retrieved from https://www.scribd.com/document/312698658/Ulbricht-Criminal-Complaint.

Van Hout, M. C., & Bingham, T. (2013). "Silk Road", the virtual drug marketplace: a single case study of user experiences. *The International Journal on Drug Policy*, *24*(5), 385–91.

Webber, C. (2010). *Psychology and Crime*. London: Sage Publications.

Wegberg, R. van, Verburgh, T., Berg, J. van den, & Staalduinen, M. van (2017). Alphabay Exit, Hansa-Down: Dream On? Examining the Effects of Operation Bayonet on Dream Market. Retrieved from https://www.tno.nl/media/10032/17-9099-factsheetbrochure-dws-05.pdf.

Wortley, R. (2001). A Classification of Techniques for Controlling Situational Precipitators of Crime. *Security Journal*, *14*(4): 63-82.

Yip, M., Webber, C., & Shadbolt, N. (2013). Trust among cybercriminals? Carding forums, uncertainty and implications for policing. *Policing and Society: An International Journal of Research and Policy*, *23*(4), 1–39.

Zawoad, S., & Hasan, R. (2013). Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems. Retrieved from https://arxiv.org/pdf/1302.6312.pdf.