Australian
National
University

KIC Korean Institute
of Criminology

MALWARE TRENDS ON ‘DARKNET’ CRYPTO-MARKETS RESEARCH REVIEW

ANU Cybercrime
Observatory

School of Regulation
& Global Governance

ANU College of
Asia & the Pacific

Malware Trends on ‘Darknet’ Crypto-markets: Research Review

Report of the Australian National University Cybercrime Observatory for the
Korean Institute of Criminology

2018

The Australian National University Cybercrime Observatory, Canberra, Australia

URL - http://regnet.anu.edu.au/research/centres/cybercrime-observatory

Director
Professor Roderic Broadhurst
Email address: roderic.broadhurst@anu.edu.au

Researchers
David Lord
Donald Maxim
Bianca Sabol
Hannah Woodford-Smith
Ho Chung
Corey Johnston
Bryan Matamoros-Marcias

Interns
Matthew Ball
Kelly Bugler
Samara Carroll
Rahil Vora

Laboratory Co-ordinator
Harshit Trivedi

Associates
Professor Peter Grabosky
Dr. Lennon Chang
Dr. Steve Chon
Dr. Russell Smith
Dr. Khoi-Nguyen Tran
Dr. Gregor Urbas

Cite: Broadhurst, Roderic, David Lord, Donald Maxim, Hannah Woodford-Smith, Corey Johnston, Ho Woon Chung, Samara Carroll, Harshit Trivedi, and Bianca Sabol. 2018. *Malware trends on darknet crypto-markets: research review*, Australian National University, Cybercrime Observatory, Canberra; DOI:10.13140/RG.2.2.36312.60168

Acknowledgements

We thank Emeritus Professor Peter Grabosky, Australian National University, and Mr Julian Slater, OA, APM Visiting Fellow Australian National University Cybercrime Observatory. We also thank Bryan Matamoros-Marcias, Ashley Rogge and Sean Field (Special Counsel, Maddocks) for their assistance in finalising the report for publication. The support of the School of Regulation and Global Governance in hosting the ANU Cybercrime Observatory is greatly appreciated.

We especially thank Dr Seong-Jin Yeon, Director of the International Strategic Research Center of the Korean Institute of Criminology, as well as Dr. Jea Hyen Soung, Dr. Hyun-wook Chun, Ms Goeun Han-Baudin and Ms Claire Sujung An also of the International Strategic Research Center for their assistance in producing this review.

Foreword

It is with my great pleasure to present the *Malware Trends on 'Darknet' Crypto-markets: Research in Review*, the second joint-research project conducted by the Korean Institute of Criminology and the Australian National University Cybercrime Observatory. On behalf of KIC, I would like to fully acknowledge the significant efforts by Professor Roderic Broadhurst as well as all of the other adept researchers of the ANU Cybercrime Observatory.

Since malware and malware based criminal services are becoming principal products in the dark markets, this interdisciplinary research on the online illicit crypto-markets or darknets, and cryptocurrencies is timely and significant in our efforts to fight against cybercrime. Since the trade of malware and its criminal services are more clandestine in nature compared to drug trafficking, these crimes are more difficult to apprehend and analyze. Hence, it is crucial to discover these crime trends through research so that effective criminal policies can be established. In this regard, this joint research project of KIC and ANU Cybercrime Observatory signifies the importance of establishing platforms for global countermeasures against illicit crypto-markets or darknets.

Again, I would like to congratulate the accomplishment of this publication for it symbolizes the successful partnership between KIC and ANU Cybercrime Observatory. I hope to witness further cooperation between the two institutes within the diverse fields of criminology and criminal justice.

Zin-Hwan KIM
President
Korean Institute of Criminology

Preface

It is a pleasure for me to introduce this volume, the latest product from a longstanding partnership of Korean and Australian criminologists. I recall more than three decades ago having attended a meeting at the Australian Institute of Criminology in Canberra in honour of the then Attorney-General of Korea, who was considering the establishment of a national criminological institute for his country. The birth of the Korean Institute of Criminology (KIC) soon thereafter was an occasion of great significance. Over the ensuing years, the KIC has made significant contributions to criminological research and training, and we in Australia have been pleased to engage with our Korean colleagues in a variety of activities. These include, among many others, the establishment of the Virtual Forum Against Cybercrime, and the KIC workshop on cybercrime at the 2005 United Nations Congress on the Prevention of Crime and the Treatment of Offenders.

The establishment of the ANU Cybercrime Observatory under the guiding hand of Professor Roderic Broadhurst has led to further collaboration, including a report on cyberterrorism, and the present volume on illicit markets and cryptocurrency.

As we move further into the digital age, we are becoming increasingly enveloped by the Internet of Things. Electronic criminal opportunities increase by the hour, and timely research on the prevention and control of cybercrime becomes even more crucial. It is my hope that this report receives the widespread readership that it deserves, and that the Korean-Australian criminological partnership continues to thrive.

Peter Grabosky
Professor Emeritus
Australian National University

Summary

This is an overview of current trends in online illicit crypto-markets or darknets, including the key role of virtual cryptocurrencies in their operation. Our approach is cross disciplinary and the focus is on the different kinds of digital products that are found in these online 'dark markets'. Primary data collected from The Onion Router (Tor), that allows anonymous encrypted communication between websites, enabled a description of short-term trends in the different malware products available in underground or 'darknet' crypto-markets.

A growing research literature on the operation of these crypto-markets has focused on the illicit drug trade, which dominates the product list of many darknet markets (e.g. Barratt 2012; Broséus, Rhumorbarbe, Mireault et al., 2016; Décary-Hétu, Paquet-Clouston & Aldridge, 2016; Broséus, Rhumorbabe, Morelato, Staehli & Rossy 2017; Martin & Christin, 2016; Martin, 2014). We explore these markets in particular, by observing the trade in malware, stolen credentials, forged documents and 'crime-as-a-service' products. These crime-ware markets offer many common hacking and social engineering tools (e.g. key loggers, ransomware, Trojans etc.) as well as hacking services and forged documents (e.g. passports, customs documents, driver's licences, etc.). We have drawn on a broad range of sources including, but not limited to, government documents, web/blog posts, academic articles, LEAs, law reports, tech websites, darknet markets, and online and other news sources.

We observed the increasing interaction (informally or *en passant*) between cybercriminals and state or quasi-state cybersecurity actors, often in pursuit of offensive cyber operations. This has increased the value and the sophistication of malware available to criminals, such as zero-day exploits for mobile phones. Illicit markets for malware, forged documents and criminal services also indicate the likely scale and scope of cybercrime. This entails the use the technology to reach millions of potential victims, and products that are designed to compromise computers and networks. Opportunities for online criminal activities continue to grow as more and more commerce and social activity takes place online in an ever increasingly interconnected world.

Recent monographs by Sanger (2018) *The Perfect Weapon* and Maurer (2018) *Cyber Mercenaries*, outline the dangers of offensive cyber operations and the role of non-state actors or cyber proxies in the development and execution of offensive cyber operations as projections of state power. These innovations signal a fundamental realignment of traditional Weberian models of the state and its perceived monopoly over legitimate violence as engagement in cyber space requires relationships with cybercriminals. States have often resorted to criminal proxies in pursuit of 'reasons of state' however, the interdependence of the Internet enables a myriad of unintended consequences that may unleash hazards regardless of friend or foe, increasing fear and opportunities for sabotage. For example, according to a recent United States federal court indictment[1] officers of the Russian GRU (Main Intelligence Directorate of the General Staff of the armed services of the Russian Federation) engaged in a series of operations that involved the staged release of documents stolen through computer intrusions in order to influence the US presidential elections in 2016. The approximately US$95,000 funds needed for the operation were laundered via a web of cryptocurrency transactions and bitcoin mining to pay for the various costs involved such as purchasing cryptocurrencies, VPN, costs of third party transactions and identity obfuscation.

[1] US District Court of Columbia, (July 13, 2018), United States vs Victor Borisovich Netyshko and 10 others, http://cdn.cnn.com/cnn/2018/images/07/13/gru.indictment.pdf.

By December 2017, the Internet had reached over half of the world’s 7.6 billion population (4.156 billion or 54.4 %). Access has grown rapidly from just under 15% in 2000 (14.6% or 360 million) to 30% of the world’s population in 2010. About 95% of the global population live in an area now covered by a mobile wireless cellular network – allowing some of the least developed and remotest parts of the globe to leapfrog to modern information communication (ICT) technologies and the world-wide web. Disparity remains however, because Internet adoption rates are about 40% in developing countries and 15% for the least developed countries, compared to 81% t for the developed countries (International Telecommunication Union, 2016; see http://www.internetworldstats.com/stats.htm). This digital divide also has another important dimension – the gap between those digital devices that are secure and those that are insecure. The disparity in security reflects the significant presence of older insecure (and pirate) software and hardware, as well as the costs of newer technologies. The digital security divide enables criminal opportunities via the low cost of many widely available cybercrime tools that ‘attack’ older ‘legacy’ computer software and hardware.

As e-commerce markets have developed along with the growth of the Internet, so did deep-web illicit markets that copied E-Bay, Amazon and, other open online markets methods and practices. Well known examples include *Silk Road*, where illicit drugs, stolen credential, child exploitation and hacker (malware-as-a-service) services were sold. These adapted open web online market formats in the crypto-markets created by the application of Tor. Crypto-markets simply mimic well-established e-commerce practices, such as providing vendor rankings, escrow services and quality assurance practices that enhance trust and efficiency. The Silk Road model became the template for online crypto-markets in general. The number of general and niche crypto-markets has since grown, with many improving their security and resilience to threats from law enforcement operations and competitors. The addition of cryptocurrencies, such as Bitcoin, further assisted the rapid development of these underground services by adding another layer of anonymity for market administrators. These operators derive fees from hosting vendor sites and escrow services for vendors and customers.

Crypto-markets and cryptocurrency

A striking feature of these underground markets is their product diversity, volatility and typically ephemeral existence. The dependence of these markets on cryptocurrency once appeared to drive the value of cryptocurrencies, so essential for business on the dark net. However, e-currencies and cryptocurrencies, especially Bitcoin, have in the past few years evolved a value driven less by illicit crypto-markets and more akin to a volatile speculative commodity or asset. The rapid rise and falls in the value of Bitcoin, for example have also seen a rise in criminal activity focused on the theft or the manipulation of Bitcoin (Bitcoin minting or mining) and other block-chain technologies.

The cryptocurrency Bitcoin was allegedly first conceived by the mysterious Satoshi Nakamoto (2008) whose 2008 *Bitcoin White Paper* solved the risk of the so-called ‘double spend’ problem in digital ledgers. The key to Bitcoin’s success, however, is a continually growing list of data blocks, secured cryptographically, known as the blockchain. Bitcoin’s blockchain is a decentralised, transactional database which serves multiple roles. It is a distributed ledger, keeping a digital record of every Bitcoin transaction since inception, while it is also involved in the creation of new Bitcoins by computing a complex Elliptic Curve Digital Signature Algorithm (Rosic, 2016).

Overall confidence in the prudential integrity of Bitcoin and other cryptocurrencies has also declined, in the face of a surge of initial coin offerings that have been found to be scams and frauds. Cryptocurrencies can also be a vector for money laundering and the blockchain processes have been misused to hide child pornography and malware (Interpol 2015; UNICEF 2015). Matzutt et al. (2017) analysed more than 1,600 files embedded in the blockchain, and discovered 99% of the files contained text or images including a small proportion that contained references to Child Exploitation Material (CEM), copyright law breaches, sensitive or private content, and malware. However, standard cryptocurrency software does not contain the decoding tools required to reconstruct the content hidden in the blockchain, and thus access is a demanding and complex process (el33th4xor, 2018; Sward et al. 2017)[2].

In May 2018, the United States Federal Bureau of Investigations began an investigation into possible manipulation of the exchange value of cryptocurrency (notably Bitcoin and Ether) via possible collusion among major players (i.e. the risk of monopoly or oligarchic conduct in under-regulated markets). Some of the methods under scrutiny are 'spoofing' (cancelled orders) and 'wash trading' deceptive activities found in other markets (Robinson and Schoenburg, 2018). A series of high value thefts from cryptocurrency exchanges operating in South Korea (Youbit, Coinrail), Japan (Coincheck), Italy (BitGrail) and India (Coinsecure) have also undermined confidence in cryptocurrencies (Reuter 2018; Lam, Lee and Robertson, 2018).

Chapter 4 examines the extent that cryptocurrencies are subject to regulation around the world. While in most countries cryptocurrencies are legal and subject to varying degrees of regulation by a national or central bank, a significant number have made its use illegal (e.g. Iceland, Algeria, Bolivia, Ecuador, South Africa). There are also some countries that have conflicting documentation about the legality of digital currencies, or indications that policy will be changed in the near future (e.g. People's Republic of China, Republic of Korea, Russia, Egypt and Egypt). The overall trend, however, appears to be in favour of further regulation. Although particular cryptocurrency may come and go, it is also clear that the underlying technology of the 'block-chain' will prevail and evolve as a potentially efficient online currency. Uncertainty prevails given the extent and form of regulation likely to be implemented in key Bitcoin source jurisdictions. Georgia, the United States of America and China produce the vast majority of Bitcoins (Patel, 2017). Chinese miners are estimated to produce approximately 60% of all new bitcoins and include the largest commercial mining pools (i.e. F2Pool, AntPool, BTCC, and BW, see: https://blockchain.info/pools)[3].

Numerous criminal actors and enterprises now engage in 'crime-ware' creation and distribution, combining malware tools, social engineering, phishing, and identity theft with organisational efficiency to target vulnerable users, services and businesses. The extent that crypto-markets are controlled by mafia like groups is uncertain; however, there is little doubt that some cybercriminal activities require highly sophisticated technical and organisational skills. It remains for future research to explore and unravel the diversity of criminal organisation and networks encountered in the deep web. Vendor or seller's 'handles' or aliases appear to be relatively stable over time, acting as a product or market brand, by contrast vendor PGP encryption keys change more frequently, allowing some tracking of vendor behaviour across markets and time.

Hacker markets

This review provides a broad picture of the trends in illicit crypto-markets and a window into the tradecraft and modus operandi of one resilient market in particular (Dream Market). We focus specifically on 'malware-

[2] We thank Matthew Ball for providing additional relevant sources and techniques for revealing suspect data contained in blockchains.

[3] Australia has a minor role in mining operations, and the Bitcoin Group estimates 2% of their mining capabilities comes from Australia (Bitcoin Group Australia. (n.d). *Securing the Future of the Bitcoin Blockchain*. Available at: http://www.bitcoingroup.com.au/bitcoin-mining/).

as-a-service' or crime-ware markets – which amplify the scale and scope of cybercrime. These markets are growing in both size and complexity as a 2014 Rand study observed (Ablon, et. al., 2014: ix):

> *The hacker market — once a varied landscape of discrete, ad hoc networks of individuals initially motivated by little more than ego and notoriety — has emerged as a playground of financially driven, highly organised, and sophisticated groups…Black and grey markets for hacking tools, hacking services, and the fruits of hacking are gaining widespread attention as more attacks and attack mechanisms are linked in one way or another to such markets.*

The emergence and rapid development of crypto-markets has acted as an amplifier or multiplier of criminal enterprise and is a challenge to law enforcement around the world. Innovative and collaborative methods to suppress these markets are needed (Australian Cybersecurity Centre 2015). The difficulty of tracing offenders and collecting relevant digital evidence has been exacerbated by the cross-jurisdictional nature of most cybercrime. This has undermined conventional investigative approaches and the effectiveness of deterrence. In turn the low risk of arrest or interdiction has created the impression that offenders are immune from prosecution and sanction. Furthermore, the lucrative potential of these darknet markets have attracted high interest from organised crime groups, especially those engaged in illicit drug distribution.

A study of a large number of known cybercrime cases found that up to 80% of cybercrime could be the result of some form of organised activity. Half the cybercrime groups in the sample comprised six or more people (most of whom where much older [35 years of age or older] than thought and a quarter of them had only been in operation for less than 6 months (McGuire 2012). The size or the duration of the cybercrime group did not relate to the scale of the criminal activities because small groups could also have a substantial, if short term, impact on many potential victims. This study also suggested that traditional organised crime groups are extending their activities to the digital world alongside newer, looser types of crime networks. Crime groups show various levels of organisation, depending on whether their activity is purely aimed at online targets, uses online tools to enable crimes in the 'real' world, or combine online and offline targets. Recent qualitative studies of the morphology of groups or networks involved in cybercrime noted that 'terrestrial' or conventional crime groups have begun to harness digital technology in furtherance of criminal objectives (Broadhurst, et al. 2014; Europol 207).

Controversy remains about the sufficiency of the empirical evidence to ascertain if cybercrime is now dominated by organised or mafia-like crime groups and what form or structure such groups may take (Lusthaus, 2013). Although cybercrime has become the domain of organised groups and the days of the lone hacker are past, "…little is yet known about the preferred structures and longevity of groups, how trust is assured, and the relationship with other forms of crime" (Broadhurst, et al. 2014:4). There is also confusion over crimes that require a high degree of organisation and activities undertaken by organised crime groups (traditional, hybrid or online) in cyber space (Leukfeldt, Lavorgna, and Kleemans, 2017). A Europol (2017:14) assessment however, noted a significant increase in the number of known international organised crime groups observed since 2013 and "… the emergence of smaller criminal networks, especially in criminal markets that are highly dependent on the internet as part of their modus operandi or business".

Dream Market

Europol estimated that as of January 2017, the Tor network comprised at least 1.7 million users, and over 60,000 unique sites many classified as related to illicit activity (Europol 2017:22). Given this scale we tracked one large deep web crypto-market - *Dream Market*, which has been in operation since 2013 and is currently the largest known general or omnibus crypto-market. Dream Market on any day could have as many as

100,000 illicit products on sale – most of which are illicit drugs but also include a significant digital or malware product list. About 1,800 unique vendors or sellers are thought to be active on Dream Market. A summary of the products available on Dream Market on April 14, 2018 shows that 51.1% were illicit drugs and paraphernalia, digital products such as malware and stolen credentials comprised 41.6%, and services (3.6%) or 'other' (3.2%) made up remainder of the types of products on sale. However, compared to *Alpha Bay*, Dream Market is a relatively modest operation. Alpha Bay was one of the largest known crypto-markets prior to its demise in July 2017 with over 369,000 products on offer and involving 40,000 vendors, and over 200,000 customers. At the time of its takedown by 'Operation Bayonet' an international police operation, there were over 250,000 listings for illegal drugs and toxic chemicals on Alpha Bay, and over 100,000 listings for stolen and fraudulent identification documents and access devices, counterfeit goods, malware and other computer hacking tools, firearms and fraudulent services (US DOJ, 2017).

The analysis of Dream Market identified anomalous online trends in the availability and costs of malware or crime-ware, and the forged or fake documents segments of this market. On average, nearly 12,000 unique digital products were on sale at any one time on Dream Market over the data collection period. Compromised bank accounts and credit cards accounted for the majority of digital products (71.6%), followed by common hacking tool kits such as Zeus, Spyeye, phishing kits and tutorials that teach hacking skills. Stolen credentials were often sold as bundles of multiple accounts, and prices varied depending on the face value of the compromised credit card. Less commonly available were specific malware products such as keyloggers, ransomware and DDoS kits, as well as various Trojans, and exploits (see Table A).

Malware/digital product types	**% Unique Listings**	**Average $AU**
Account (compromised)	42.4	$47
Credit Cards	29.2	$45
Hacking Tools	10.3	$7
Documents (passports, etc.)	6.7	$747
Vulnerability/Exploits	0.94	$7
Keylogger	0.73	$4
Ransomware	0.73	$64
Botnet/DDOS	0.72	$29
Trojan/Virus	0.65	$27
All	100.00	_

Table A. Summary: digital products & average prices found on Dream Market (September 2017-April 2018)

Generally, the cost of these digital tools was low but the data obtained may also be traded as a commodity. However, as we note in detail below a few high value digital products were identified in the ransomware, Trojan/viruses and vulnerability/exploit listings. For example, a high value custom-developed version of ransomware, 'Ransomware-ALM4 Locker', became briefly available at AU$3,848. This was sixty times the average price for stock ransomware kits and attracted high interest due to its relative novelty. The high values attached to fake documents or identities illustrates the importance of 'document fraud' as one of the key engines of organised crime, along with money laundering and the online illicit trade, which in turn is likely to disrupt established criminal markets and their traditional distribution models over the next few years (Europol 2017: 11).

We also explored the products available on 0day.today a well-known forum and 'grey' market for malware, especially zero day exploits. The forum operates both an open and private or registered website, the latter providing opportunities to purchase potentially lucrative exploits. We observed sales exceeding AU$5,000 for exploits for the popular Apple iOS, privilege elevation tools for iCloud and exploits for Windows 2010.

Some commentators have suggested revising bug bounty programs and incentives from legitimate companies to shift transactions and talent away from these illicit markets into legitimate business operations. Other measures focus on disruption including, more radically, flooding dark net markets with fake products. Other measures include: posting unfavourable comments about the product and services supplied by darknet vendors; the launch of distributed denial of service (DDoS) attacks that disable or limit access to that market by customers; and undercover operations that set up a fake vendor service as a means of harvesting information and/or discrediting the overall operation (for example by means of an 'exit scam') of the darknet market. Such measures are already widely used by online market competitors, and account for the relatively short shelf life of some markets but also for the improved security and resilience of markets such as Dream Market.

This review first provides a short summary of the definitions of cybercrime, then outlines the criminological theories that address offender motivations, the role of crime networks and the measures used to suppress crime. Next, the primary data drawn from Tor sites are described in detail. We also explore the overlap between crypto-markets and cryptocurrencies. The high-degree of volatility in the value of cryptocurrency, rapid changes in the e-cash/currency eco-system, and the disruptive impact of block-chain technology have added complexity to the analysis of crypto-markets. Regulatory responses to these developments are evolving and are briefly described. A brief overview of state or quasi-state sponsored use of malware then follows. We conclude by discussing the challenges of interpreting the intelligence value of the data captured from underground malware markets.

Online malware and crime services thrive in the omnibus and niche darknet markets. Unlike the darknet drug markets where tangible, if stealthily packaged, products are delivered via vulnerable postal or courier services, digital products offer no routine opportunities for interdiction. In the analysis of prices and product availability, we infer that omnibus markets also operate as advertising platforms for more expensive and/or niche products. If so, monitoring these markets may offer some predictive value in anticipating the kinds of malware and their harms and the likely victims or vulnerabilities targeted. A better understanding of these malware 'bazaars' also may provide more effective ways of disrupting these markets and their multiplier effect, and may help focus or prioritize harm reduction efforts.

Contents

Chapter 1: Introduction

In 2016, Europol published its annual threat assessment on organised crime, which estimated that for the first time, cybercrime had surpassed traditional forms of crime in scope, volume and cost (Europol, 2016). Estimations for the global cost of cybercrime vary greatly. Conservative estimations report the cost of cybercrime increasing from approximately US$345 billion - $445 billion (0.62% of Global GDP) in 2014 to US$445 billion - $600 billion (0.8% of Global GDP) in 2017[4] (Lewis, 2018, p. 6). More liberal estimates place the cost of cybercrime at US$3 trillion in 2015 with predictions of US$6 trillion by 2021 (Paganini, 2016), whereas other projections suggest costs could reach US$2 trillion by 2019 (Morgan, 2017). Demand for cybersecurity products and services are also expected to increase from $75 billion in 2015 to $175 billion in 2020 for security countermeasures while the insurance industry is projected to grow from $2.5 billion to $7.5 billion in 2020 (Morgan 2017).

Fraud and the costs of other economic crimes have always been difficult to estimate (even in the pre-Internet age and the offline world). Although police records and survey data show substantial increases in on line fraud Levi (2017), and others have questioned the basis for these huge crime-cost estimates. Levi noted the complexity of making such estimates[5], the overall lack of the relevant statistical data for volume online fraud and the extent that online crime is transformative of criminal organisation and the effectiveness of the criminal justice response. Nevertheless, the flood of online fraud and crime cases requires a significant societal and policing response promoting cyberfraud prevention, resilience, and general 'reassurance' policing (Levi 2017:18).

This rise in cybercrime has been mirrored in illicit marketplaces. During the period 2014 – 2017, the Global Drug Survey (2017) found that participants who had used drugs in the past year obtained via the darknet had increased by 70%, albeit from a low but growing base of about 4.5% of all estimated sources. Not only are recognised online illicit markets growing in popularity, but the darknet is also establishing domains to buy and sell new technologies such as malware. Many cybersecurity companies consider the increase in occurrences of Internet crime to be a consequence of the availability and access to such software (Symantec, 2010; Trend Micro, 2011; Trend Micro, 2011a; Damballa, 2011). However, there is limited research that assesses the availability of new tools and methods available to criminals on both the 'surfaceweb' (or the open or clearnet) and 'deepweb' (darknet). Holt and Bossler (2014) made a similar observation of the scarcity of research conducted on the topic of online markets relating to malicious software, although since then, there has been a surge of publications about these crypto-markets. This report investigates the evolution of criminal activity on the darknet by assessing the overall availability and likely risks of malware sold or made available on the world-wide web – principally on crypto-markets found on the darknet.

As the literature shows, cybercrime is not actually "new crime" but has origins in traditional criminal activities including ransom/kidnapping, fraud, and drug trafficking. Importantly, cyberspace has provided a proliferation of new 'technology-enabled' opportunities to engage in traditional crimes, especially in terms

[4] This value is based on the sum of estimations from the loss of intellectual property and business confidential information; online fraud and financial crimes; financial manipulation that uses stolen business information; opportunity costs, including disruption in production or services, and reduced trust for online activities; the cost of securing networks, buying cyber insurance and paying for recovery from cyberattacks, and; reputational damage and liability risk for the hacked company and its brand including temporary damage to stock value (Lewis, 2018, p. 6).

[5] Levi (2017: 13) notes: "Efforts at cost estimation will always be provisional, not least because the exploitation of vulnerabilities and collateral damage may take years (if ever) to emerge: the 'tail' of costs from a data breach, for example, may depend on the organisation of crimes, the responses of victims and third parties".

of the tools used, the scale of and reach to potential victims, and the detached anonymous nature of the criminal activities (removing key obstacles in the psychology of crime and the choices made by offenders). Grabosky, Smith and Dempsey (2001) underlined that the more opportunities for crime a situation presents, particularly in the case of cybercrime, more crime would occur. In brief, the Internet affords many more ways for crime to reach mass, as well as specific victims, anonymously, and therefore crime prevention focused on vulnerable targets (potential victims) may afford the best means of reducing harm.

In the current environment both cryptocurrencies and purchases of malware or other software vulnerabilities on the darknet have become two of the most problematic trends in cyberspace (Greenberg, 2017; Dinham, 2018). Kaspersky Labs (2016) found that 25% of Internet users have spent money to fix a problem caused by malware, averaging US$121 per incident (Kaspersky, 2016). Similarly, the most frequently referenced cryptocurrency ‘Bitcoin’, also widely used in darknet markets gained increasing value, reached an all-time high of US$19,783.21 on 17 December 2017 (Higgins, 2017) before falling steadily to current values of US$6,476 as of 4 July 4 2018 (see https://www.coindesk.com/price/). These trends indicate that products of cyberspace, such as Bitcoins and malware, are becoming increasingly profitable and accordingly, a more attractive domain for offenders to exploit.

Of significant concern is the global nature of these crimes. Cybercrimes like the WannaCry and Petya ransomware attacks, indiscriminately exploited individuals, businesses and governments around the world with little regard for political or geographic boundaries. The transnational nature of the cyber domain combined with weak international controls, the relatively limited scope of the Council of Europe’s Cybercrime Convention, and the patchwork of mutual legal assistance treaties, allow offenders to engage in criminal activities with the advantage of plausible deniability and anonymity. This cross-border nature of cybercrime is frequently exploited by cybercriminals operating from within ‘safe havens’ – countries where limited action is undertaken by law enforcement against malicious online behaviour. This environment highlights the principal need for cross-national and international responses to combat cybercrime (Broadhurst & Chang, 2013).

Developing effective universal conventions or bilateral mutual legal assistance arrangements that can address these transnational law enforcement challenges has thus far proven to be highly complicated. While significant progress has been made in fostering international co-operation (for example 56 states are now parties to the Convention on Cybercrime), a number of states, notably Russia and China, have been reluctant. Without an international system of enforcement, we are unlikely to see significant steps toward a unified attempt to combat cybercrime.

Definitions

Malware

Malicious software or 'malware' describes computer code that is capable of compromising computer systems. The history of malware goes back as far as 1946, when computer scientist John von Neumann presented a paper on the "Theory and Organisation of Complicated Automata" at the University of Illinois. Neumann applied the idea of biological viruses and their self-replication to the computer. He presented the idea of "self-reproducing automata" within the entity of the then new "computing machines". Thus, the first type of malware was invented, the humble computer virus (Von Neumann, 1966).[6]

Even early networks such as the Advanced Research Projects Agency Network (ARPANET) established by the United States Department of Defense during the Cold War in the 1970s suffered from outbreaks of malware. With the rise in popularity and growing ubiquity of computers, malware has begun to appear more frequently and exponential growth has followed (see **Figure 1)**.

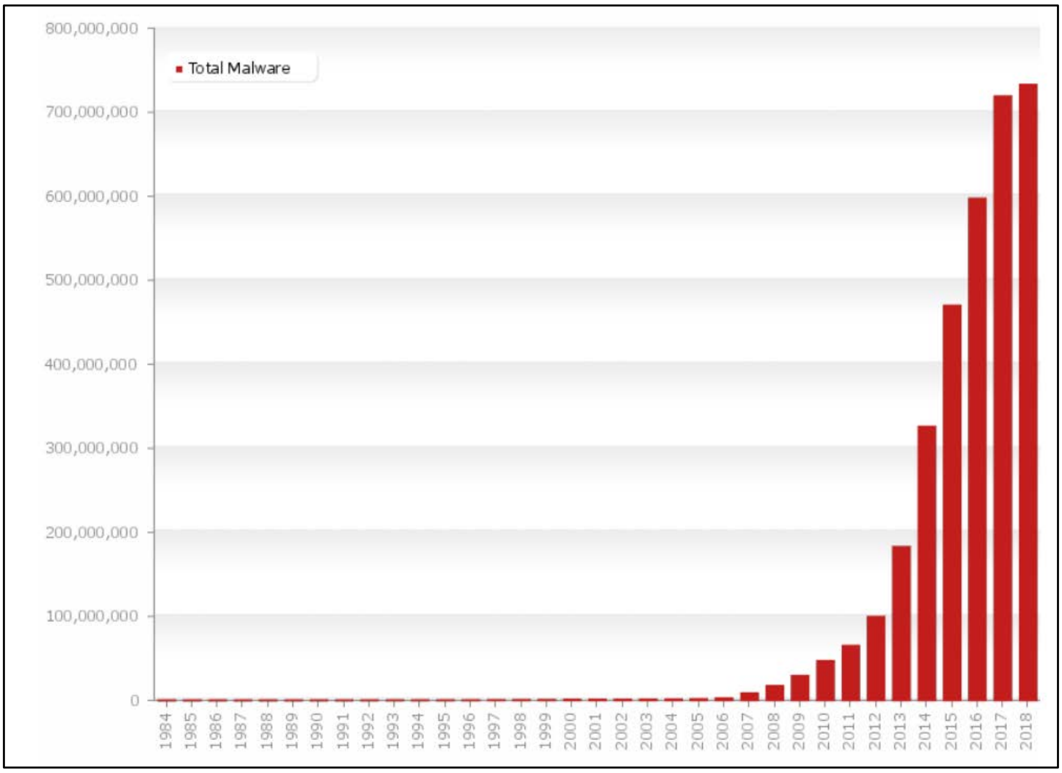


Figure 1 - Total Malware, AV-TEST (AV-TEST, 2018)

The term 'hacker' is now synonymous with malware. A 'hacker' was originally descriptive of a person motivated by technological curiosity and ingenuity. In the very early years of the Internet, hackers were mainly involved in "playing with systems and making them do what they were never intended to do" (Denning, 1990), and could be better described as a hobbyist community.

Starting in the mid-1980s onward, instances of computer based criminal activity became more common, resulting in a growing concern from law enforcement authorities and the general public. Elements of this

[6] For a brief history of the emergence of malware markets and service see: Roderic Broadhurst (May 16, 2017), 'What the underground market for ransomware looks like', *The Conversation*: https://theconversation.com/what-the-underground-market-for-ransomware-looks-like-77703

early hacker culture still exist today, persisting in online forums and encrypted messaging systems. In 2018, cybercrime is noticeably more varied than in the past.

Early outbreaks of malware may have alarmed users by causing computers to behave in unexpected ways. However, as malware developed, more insidious outcomes were observed. Malware which started appearing in the 1990s presented much more of a threat. Modern malware is often used to steal confidential information such as bank account details, logins, passwords and other personal data. However, malware can also be used to delete, corrupt or access private files, delete system calls, and create backdoors in the infected system for remote control of victim's computer by a third-party. Recently identified as an increasing threat is malware that hijacks a system's resources to mine cryptocurrency unbeknown to its user.

Many hacks, malware compromises, or breaches of computer systems involve the exploitation of vulnerabilities in computer software or hardware. Vulnerabilities within computer systems enable the injection of malicious code which can result in compromises, third-party control, or disruptions of the computer system (Yamaguchi, et al., 2014). Malware takes many forms including viruses, worms, Trojans, rootkits, adware, and spyware. Verizon's 2016 Data Breach Investigation Report notes a common challenge: "99% of malware hashes are seen for only 58 seconds or less. In fact, most malware was seen only once" (Verizon, 2016).

This creates difficulty for signature based security solutions as attackers may only use malware once before modifying or obfuscating the source code. Because entirely new strains of malware take more resources to develop, it is more likely that attackers are reusing and obfuscating already available code. This also reflects how quickly hackers are modifying malware source code to evade detection (Kidron, 2017; Verizon, 2016).

While the malware of 1970s – 1980s targeted a variety of operating systems and networks, most today are written to exploit vulnerabilities in commonly used software. Cybersecurity company Offensive Security (2018a) provides records of exploits reported within different operating systems. As seen in **Figure 2**, Windows exploits remain the most common.

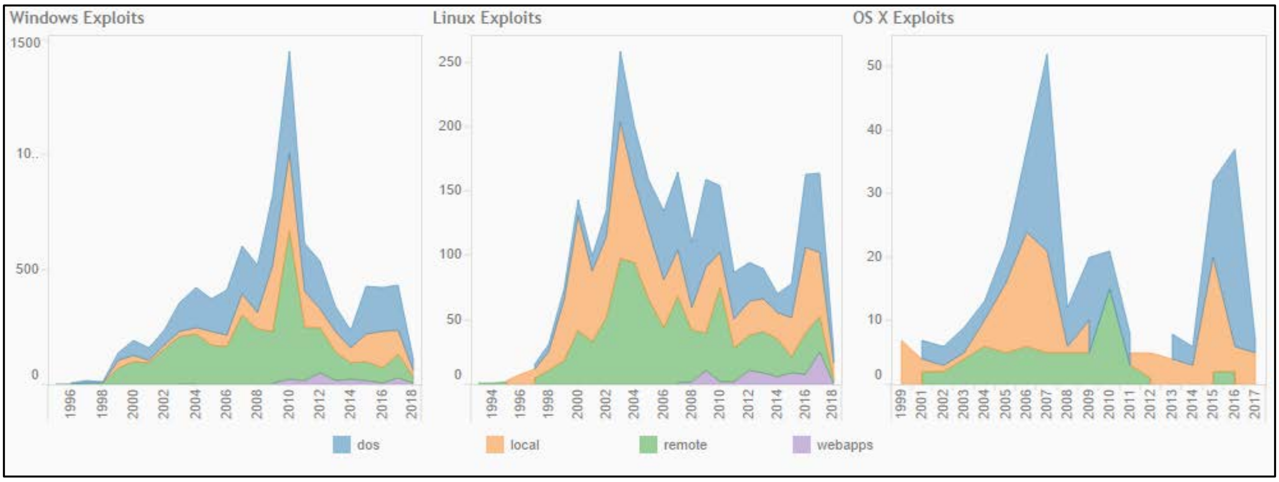


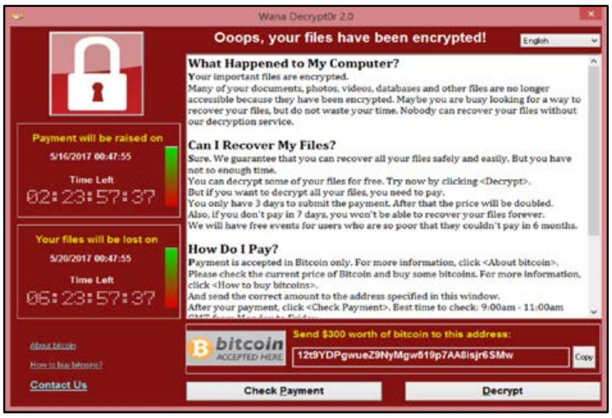
Figure 2 - Exploits by Operating System (Offensive Security, 2018a)

WannaCry(pt)

The WannaCry (also known as WannaCry(pt)) worm was a global scale ransomware attack which occurred between 12 and 15 May 2017, affecting more than 300,000 Windows computers in over

150 countries. The infected computers were held to ransom for a sum of US$300 in Bitcoin which was threatened to increase if demands were not met within a specified time. Notable victims of the attack were the United Kingdom's National Health Service (NHS), Spain's Telefonica, FedEx and Deutsche Bahn. The countries affected the most were Russia, Ukraine, India and Taiwan (Jones & Bradshaw, 2017). The initial attack was short lived due to the discovery of the kill switch by Marcus Hutchins, a 22-year-old web security researcher with the company MalwareTech (MalwareTech, 2017). Although subsequent versions of WannaCry lack the inbuilt kill switch, they have not spread to the same extent due to network and vulnerability patching. They still, however, remain a significant threat.

The original WannaCry ransomware attack has been attributed to the DPRK's Lazarus group, as it used the same tools seen in the Sony Pictures and Bangladeshi Bank hacks in 2014 and 2016 respectively (Symantec, 2017b). However, it must be remembered that attack vectors and tools are not exclusive to groups or individuals and can therefore be used to create a false flag, making the process of correct attribution difficult.



What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Figure 3 - The WannaCry(pt) Ransom Demand (GReAT, 2017)

WannaCry spread through the use of two infection vectors, the EternalBlue and DoublePulsar exploits in Windows' Server Message Block protocol which were stolen from the National Security Agency's (NSA) Equation Group by the criminal organisation (that may be linked to Russian intelligence services) known as the Shadow Brokers. Because of the breach, there has been considerable debate surrounding the hoarding of harmful exploits by security agencies, as they have proven to be dangerous to the general public.

The EternalBlue exploit vector was patched by Microsoft on 14 March 2017, on all affected operating systems for all of their Operating Systems (Burgess, 2017). The Shadow Broker group released the exploits on the 14 April, 2017, among a series of other stolen tools. However, many preventable infections still occurred due to system and network owners not downloading and installing the new patch (ACSC, 2017).

The NSA theft by the Shadow Brokers heralds a new and very worrying trend. Not only has there been a dramatic increase in ransomware campaigns that impact organisations (ACSC, 2017), cybercriminals (and less advanced Nation States) may target national security agencies and private cyber weapons developers in a bid to steal more sophisticated weapons in order to bypass technology development hurdles (Thomson, 2017). The NSA theft proves that even the best hackers are not impervious to attacks. If, or when, more sophisticated cyberattack vectors find their way into the wild it is very likely that cybercriminals will capitalise on these vulnerabilities before they are patched.

A Multi-layered Web: Surfaceweb, Deepweb and Darkweb

Many computer users are aware of the different layers of the Internet. However, what is commonly misconstrued or unknown are the differences between each layer and especially between the deepweb and the darkweb. It is therefore important to understand each specific networked layer and the different opportunities for the crimes these layers enhance (see **Figure 4)**. Many users are familiar with the ‘open Internet’, or what is referred to as the ‘surfaceweb’ or ‘clearnet’.

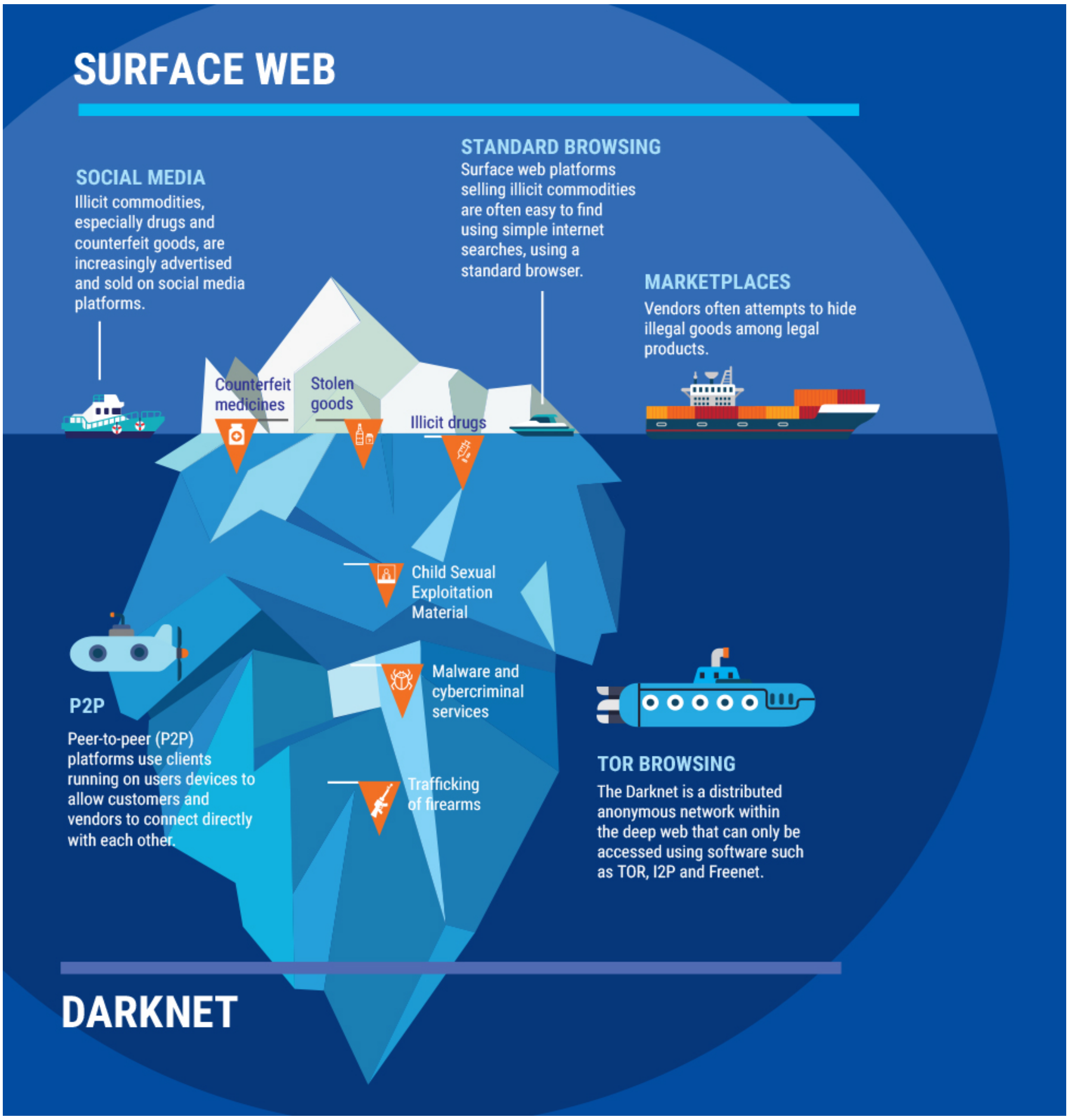

SURFACE WEB
SOCIAL MEDIA
Illicit commodities, especially drugs and counterfeit goods, are increasingly advertised and sold on social media platforms.
STANDARD BROWSING
Surface web platforms selling illicit commodities are often easy to find using simple internet searches, using a standard browser.
MARKETPLACES
Vendors often attempts to hide illegal goods among legal products.
Counterfeit medicines
Stolen goods
Illicit drugs
Child Sexual Exploitation Material
Malware and cybercriminal services
Trafficking of firearms
P2P
Peer-to-peer (P2P) platforms use clients running on users devices to allow customers and vendors to connect directly with each other.
TOR BROWSING
The Darknet is a distributed anonymous network within the deep web that can only be accessed using software such as TOR, I2P and Freenet.
DARKNET

Figure 4 - The Layers of the Internet (Europol, 2017 p.23)

Surfaceweb

The Internet is, in its simplest form, a global system of computer networks (which has now expanded to include other connected devices, such as mobile phones and tablets) and encompasses all layers of the web. From this overarching domain, there are two distinct layers: the surfaceweb (or the clearnet) and the deepweb. As Michael Chertoff (2017, p. 26) asserts, “the [surfaceweb] is what the average user thinks of as ‘the [I]nternet’. [It] is a collection of websites indexed by search engines like Google, Yahoo, and Bing that can be easily accessed through standard browsers and [I]nternet protocols. This may seem like a vast quantity of information, but the [surfaceweb] is just the tip of the iceberg.” The surfaceweb includes all freely available information that does not require a separate application base to access the data.

Deepweb

Forming the main body of the iceberg is the deepweb. This is the second layer of the web that is defined by the requirement of a separate interface to access the data because it is not indexed (Chertoff, 2017; Gehl, 2014). Many researchers have acknowledged the greater size of the deepweb compared to the surfaceweb, with Kristin Finklea (2017) estimating that the deepweb is approximately 4,000 – 5,000 times larger. The deepweb includes domains that Internet users access daily such as Facebook, Twitter, Snapchat, government resources, and academic information.

Darkweb

Distinctions between the deepweb and darkweb (or darknet) are often nuanced with differences rarely made explicit. This is due primarily to the interconnected nature of the deepweb and darkweb; the latter is best understood as the intentionally (or cryptographically) hidden content of the deepweb. The darkweb is a "distinct network supporting cryptographically hidden sites" that operates in the deepweb (Moore & Rid, 2016, p. 15; McCormick, 2013). Although this description suggests complex or nefarious processes, it is a domain that can be used for licit activities. The size of the darkweb, relative to the deepweb remains unknown, however Chertoff (2017) estimates that the darkweb only accounts for less than 0.01% of the sites on the Internet.

Darknet markets

One of the most common types of cryptographically hidden sites are darknet markets, or crypto-markets. Due to the enhanced ability to preserve anonymity via encryption, the darknet plays host to a significant proportion of illicit commercial and organisational activities such as illegal commodity trades, child exploitation, bids for contract killings, and terrorist/organised criminal communication or recruitment (McCormick, 2013; Viney, 2017; Broséus, Rhumorbarbe, Morelato, Staehil, & Rossy, 2017; Broadhurst, Woodford-Smith, Maxim et al., 2017). These marketplaces have raised the profile of the deepweb and are largely responsible for the often-misconstrued nefarious nature of the second layer of the Internet. These darknet marketplaces are predominantly devoted to the sale of illicit goods and commodities, and are defined by their use of advanced encryption software that protects an individual's identity within the marketplace (Broseus, Rhumorbarbe, Mireaultm Ouellette, Crispino & Decary-Hetu, 2016).

Darknet trends in malware product listings and sales are one means of identifying shifts in the availability of a particular variant of malware, either by observing changes in price or the number of specific malware products listed. Therefore, the monitoring of malware products offered within darknet marketplaces offers a method for tracking trends in potential victimisation.

Darknet markets are subject to regular attacks and disruption from law enforcement (e.g. Operation Bayonet, see page 35) or rival marketplaces ('"Mr. Nice Guy" Market Paid For Recent Attacks On Other Markets, Was Preparing To Exit Scam,' 2017). Law enforcement agencies (LEAs), such as in Operation Bayonet, take over the administration of the marketplace, gathering intelligence on its users and shut the site once they have collected enough information to begin the prosecution process (Europol, 2017).

Competing marketplaces have also been reported to be hostile to each other. In June, 2015 the TheRealDeal and Agora darknet markets (as well as their mirrors) faced a two week DDoS campaign which severely impacted their operations. One of the site owners under attack, the ironically named Mr. Nice Guy, bargained with the blackmailer, *ddosforsale*, to bring down seven rival markets. This was done for the purpose of displacing the users of the rival sites so that Mr. Nice Guy could execute an exit scam and give the attacker a share of the profit as payment ("Darknet Hidden Services Facing Large Scale DDoS Attacks", 2017). As a result of the activities by LEAs, competing darknet marketplaces, as well as extortionists and scams, it is a regular occurrence for both vendors and customers in the darknet to lose market presence ("Who is Attacking the Darknet Black Markets to Bring it Down?", 2017).

Although the operation of darknet markets is volatile, with frequent entry and exit, some crypto markets continue to offer services of high quality. Typical products offered within darknet markets can include: drugs, pharmaceuticals, identity documents, counterfeit goods, weapons and contraband. For example, Dream Market recently added fentanyl to the following as “forbidden products and services”:

- Assassinations or any other services which constitute doing harm to another
- Weapons of mass destruction: chemical, biological, explosives, etc
- Weapons
- Poisons
- Child pornography
- Live action snuff/hurt/murder audio/video/images

Darknet marketplaces operate on the same model as eBay, with three main actors: vendors and buyers (both participants of the Marketplace), and market administrators. Buyers can leave reviews, message vendors and even dispute transactions. Vendors conversely adopt a seller role within the marketplace. Administrators typically receive 5% – 10% cut of each sale, providing the web-platform, escrow services and supervision over the market’s operation.

Historically, market platforms have closed due to: high profile shut downs by law enforcement, exit scams where platform owners have run off with the money being held by the site (in escrow and/or in buyers’ and sellers’ accounts), and by voluntary exit. Market lifespan has been shown to be typically less than 12 months (Gwern, 2018).

Specifically, anonymous marketplaces are usually implemented as hidden services in The Onion Router (Tor) network, an overlay network providing anonymity to its users. The Tor network reroutes a user’s connection through multiple anonymous servers (onion routers), masking the original IP address of the user. Anonymity of both administrators and participants is ensured by the use of different technologies: electronic payments are carried out through the use of the virtual cryptocurrencies (Bitcoin is the most popular), Tor is used for network communication, and the Pretty Good Privacy (PGP) cryptosystem is often used to exchange emails (for more information on the PGP cryptosystem, see section: “Security of Marketplaces: PGP”).

Scraping the darknet for analysis of products is not new. Archives such as the darknet Market Archives (2013 – 2015) generated by Gwern (pseudonym) have provided researchers with a ‘treasure trove’ of information on darknet marketplaces, with the Gwern archives reportedly leading to 312 arrests by law enforcement (Gwern, 2018).

Accessing the Darknet

As noted above, the darknet is a small subsection of what is known as the ‘Deepweb’ that is accessed through the use of identity obfuscating browsers such as The Onion Router (Tor), Freenet and I2P. The Privacy Enhancing Technology (PET) utilised by these browsers owes its origins to the United States Naval Research Laboratory and DARPA (The Onion Router, n.d.). PET and the darknet were initially developed for the purpose of protecting online US intelligence communications from foreign surveillance (Smith, 2013), but were later repurposed and released by the The Tor Project in 2002 to create a platform that individuals could use to avoid monitoring by governments and corporations (Huang & Bashir, 2016). Due to the strong encryptions and the plethora of identity masking techniques readily available, the darknet has been adopted by cybercriminals to advertise and distribute their products (Egan, 2018).

Accessing the darkweb is a trivial task that can be accomplished by anyone that can download and install an Onion browser such as Tor or I2P (Bradley, 2018). However, simply installing the Onion browsers does not ensure anonymity on the darknet. A user's ISP and government are aware of when they use services such as Tor, although may not necessarily know what content the user is browsing (Bischoff, 2017b). Further steps are required to increase a user's anonymity while using the darknet. There are a plethora of different methods that can be employed to decrease the risk of detection. Below is a non-exhaustive list of the techniques used to increase a user's anonymity on the darknet.

Web browsers

Tor is the most popular browser used to access the darknet and allows users to access domains with the '.onion' suffix. It is easy to install and mimics many of the conveniences that modern browsers such as Firefox, Internet Explorer and Google Chrome employ. Tor comes preloaded with numerous hard-coded security and encryption enhancements that obfuscate IP addresses and therefore gives its users a higher degree of anonymity (Patterson, 2016). These security features scramble the user's IP address while using the darknet which makes individual identification difficult, but not impossible (Patterson, 2016).

I2P is the second most popular darknet browser and allows users to access its own brand of hidden sites known as 'eepsites' (sic) (Bischoff, 2017b). It is similar to Tor as it provides users with IP obfuscating abilities and allow users to access hidden websites on the darknet. However, I2P's primary design is to function as a "network within the Internet", confining traffic to itself and effectively operating as a 'true darknet' (Holden, n.d.). I2P boasts of being a more reliable service due to it using packet based routing instead of Tor's circuit based routing – meaning it is able to move around any network congestion and service interruptions in a similar manner to the surface nets of IP routing (Holden, n.d.).

Freenet is the third most popular darknet browser. It is more similar to I2P's functionality than to Tor's, but offers many unique features. Like I2P, Freenet is a self-contained network within the darknet that is unable to access the surface web (Bischoff, 2017b). Furthermore, the Freenet browser is only able to access content uploaded to its peer-to-peer distributed data store (Bischoff, 2017b). Unlike Tor and I2P, Freenet does not require a server to host content and operates like the surface web cloud. This means that when something is uploaded to Freenet, it remains online even if the uploader ceases to use the program (Bischoff, 2017b). Finally, the browser allows users two ways to connect. The open net function allows users to automatically connect to peers and sites on the Freenet network. The 'darknet' function allows for users to choose who they connect to and to specify the user's friends. This creates a closed group that only authorised users can access (Bischoff, 2017b).

Virtual Private Networks

Virtual Private Networks (VPNs) are regularly used by Tor users to add a further level of identity protection. VPNs allow users to encrypt all network traffic and route it through a designated server (Bischoff, 2017b; "Combining Tor With A VPN", n.d.) effectively creating a fake geolocation entry point to the Internet. There are two methods of using a VPN while browsing Tor: VPN before accessing Tor, and VPN after accessing Tor. Both methods mask the user's location and identity in some manner, but have their own pros and cons.

When a user engages their VPN before launching Tor, they are using Tor over VPN. Tor over VPN is the most common method of accessing the darknet using identity obfuscating technology (Bischoff, 2017b). The user's IP only sees the encrypted VPN network traffic. This means that they are unaware of any use of Tor by the user on their network ("Combining Tor With A VPN", n.d.). Many Tor users subscribe to encrypted VPNs that do not log any of the traffic and pay for them using cryptocurrency to ensure their anonymity (Bischoff, 2017b; “Combining Tor With A VPN”, n.d.). Tor over VPN does not however protect users from malicious exit nodes that may decrypt the user’s Internet traffic, steal personal details or inject malicious code (Bischoff, 2017a; “Combining Tor With A VPN”, n.d.).

When users access Tor and then use a VPN, they are using VPN over Tor. This method is less popular than Tor over VPN and does not allow access to hidden services websites, such as those with the .onion suffix (“Combining Tor With A VPN Continued”, n.d.). This limited accessibility is due to the VPN being the accessing agent instead of Tor. This means that all of the Tor traffic is channelled through the VPN (“Combining Tor With A VPN Continued”, n.d.). Although VPN over Tor has limited accessibility, it does have its own advantages. It allows a user to stay anonymous to their VPN (as long they have used a clandestine method of payment, such as cryptocurrency), and enables access to websites that have otherwise blocked Tor. When users pass through an exit node, their information remains safe and encrypted due to the VPN’s masking features (“Combining Tor With A VPN Continued”, n.d.).

Virtual Boxes

TAILS

The Amnesic Incognito Live System (TAILS) is based on Debian (a free OS designed for anonymity while using Tor) to create a ‘Virtual Box’ or ‘Virtual Machine’ using PGP encryption. TAILS was made infamous by Edward Snowden when he leaked secrets from the US National Security Agency (NSA) to the media before making his escape from the US (Palmer, 2016). The use of TAILS has proven to be a major hurdle for law enforcement as it makes identification of cybercriminals and terrorists far more difficult (Palmer, 2016; Sayer, 2014).

TAILS comes preloaded with a modified Tor browser as well as a suite of identity obfuscation and protection features including PGP for encryption (Condliffe, 2014). It is designed to launch from a USB or DVD drive (on any operating system) so as not to write any information to the local drive of the device used, thereby leaving no digital footprint (Finley, 2014).

Whonix

Whonix is designed for maximum security and secrecy and, like TAILS, it is built upon a Debian OS (Whonix, n.d.). Unlike Tails however, it is designed to be installed and run on a computer through a Virtual Machine on top of commercial off-the-shelf OS’s including Windows, MacOS, Ubuntu and Qubes (Chris, 2014). The program creates two sub-operating systems, called ‘Gateway’ and ‘Workstation’, on the user’s computer to provide a substantial layer of protection both from malware and for the user’s identity via IP address leaks (Whonix, n.d.).

The key to Whonix’s heightened anonymity is the unique way in which it operates. Whonix as a whole is made of two sub-operating systems. Internet surfing, document viewing, or any other styles of anonymous work are done exclusively through the ‘Workstation’ component, which is more akin to a standard OS (Whonix, n.d.). Meanwhile, the sole purpose of the ‘Gateway’ component is to act as a ‘middle-man’ between the Internet and the Workstation. All traffic from the Workstation is routed through the Gateway, which then accesses the Internet through Tor (Whonix, n.d.). Essentially, this means that if the Gateway were to become compromised in some way, the Workstation is still protected.

The challenge for law enforcement lies in the model described above – there is no clear pathway to meaningfully identifying the Whonix Workstation, because it is so well protected through the use of Tor, a middle-man Gateway and, optionally, a VPN. However, the fact that Whonix is often run within a host operating system presents a key weakness. If the host OS, particularly Windows or macOS, can be compromised, then the use of Whonix can be easily monitored through the use of data-stealing malware such as a keylogger. As such, most darknet users who value anonymity above all else will use a host operating system outside of the ‘big two’, such as Ubuntu or, more commonly in the case of Whonix, Qubes.

Marketplace Security

Marketplaces have evolved since the beginnings of *Silk Road* and *Agora*. No longer a single page website with minimal security, marketplaces employ a range of defences, including:

- Alternative Links
- CAPTCHAs
- DDoS Protection
- PGP Communication

Alternative links

Providing alternative links to access, darknet markets are able to maintain ‘up-time’ and continue operation by distributing the load of user activity. By hosting alternative links darknet markets can also limit the disruptive effect DDoS attacks represent – ironically these tools are also products listed within marketplaces. Between September 2017 and February 2018 Dream Market increased their number of alternative links from four to more than ten. Alternative links often change over time in an attempt to mitigate sustained DDoS attack – these changes to the .onion address of marketplaces is often reported by market administrators as a change to the URL can be a sign of a phishing attempt by law enforcement, disruption by criminal competitors or other 3rd parties.

CAPTCHA Protection

Most market virtual sites enact CAPTCHA protection to mitigate the effect of bot and other automated browser activity. By successfully resolving the CAPTCHA challenge, a user is able to access and explore the marketplace. **Figure 5** shows an example of a generic CAPTCHA challenge.

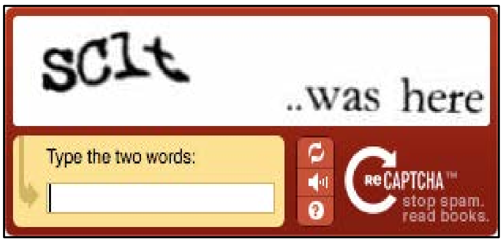


Figure 5 - Example of a CAPTCHA Challenge (Wikimedia Commons, 2016)

Often, market sites enact an initial CAPTCHA to protect the login landing page and a second CAPTCHA to protect the login procedure. CAPTCHAs are often implemented alongside DDoS protection for enhanced protection. The largest operational darknet market at the time of study, Dream Market, requires completion of a CAPTCHA where four alphanumeric digits are outlined within a box surrounded by an additional three or four digits.

DDoS Protection

Darknet markets have enacted their own forms of DDoS protection. These range from the use of proprietary services such as ‘CloudFlare’ (developed/enacted by 0day.today) through to custom ‘auto lock-outs’ in response to suspicious activity. Large scale DDoS attacks against darknet markets frequently occur, although seldom at the scale other sites have experienced, as in the case of Github.

Github DDoS Attack: The Biggest Attack to Date

According to research by Verisign/Merril Research (2018) a third of all downtime incidents are attributed to DDoS attacks. Recently Github, an open source developer platform, survived the largest recorded

DDoS attack of 1.35 terabits per second of traffic (Verisign, 2018). A digital system assessed the scale of the DDoS and within 10 minutes assistance from a mitigation service, Akamai Prolexic, was deployed. All Github traffic was sent to Prolexic 'scrubbing' centres to identify and block malicious traffic (Wired, 2018).

The result was minimal, with intermittent outages suffered for the duration of the DDoS.
Luckily, Github had previously modelled their traffic capacity for the event as Josh Shaul (vice president of web security at Akamai) stated: "I would have been certain that we could handle 1.3 Tbps, but at the same time we never had a terabit and a half come in all at once" (Wired, 2018).

By flagging suspicious browser behaviour, a system administrator has the ability to 'lock out' users or forcefully impose CAPTCHA challenges to limit the extent of suspicious behaviour. Darknet markets vary in their DDoS protection abilities. Below is an Example of DDoS protection measures reported by Olympus Market:

> *Once we receive a heavy rain of DDoS attacks, in rare cases where our dedicated servers will not be able to mitigate the attacks (it should but it still might happen,) we will run a script that will switch hostnames automatically every certain period of time and will post the new hostnames to our subreddit and to all official communication channels for our customers* (Olympus Market, 2018).

PGP Communication

PGP (Pretty Good Privacy) is an encryption protocol that implements cryptographic privacy and authentication with the goal of maintaining secure data communications. To do this, PGP generates a public private key pair. A public PGP key is used to encrypt any communication with the owner of the public key. A private PGP key is then used by the owner to decrypt any communication sent to the owner of the public key. This process is outlined in Figure 6.

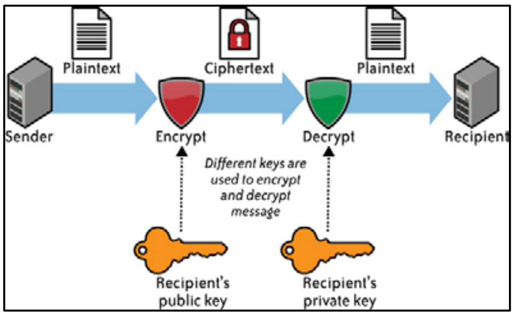


Figure 6 - Example of PGP Encrypted Messaging (Wikimedia Commons, 2017)

This exchange prevents any communication received or intercepted from being deciphered by anyone besides the owner of the Private PGP Key. Within darknet markets this allows vendors to advertise their Public PGP Key to enable correspondence.

Chapter 2: Cybercrime and Criminological Theory

Despite the rapid proliferation of cyber-enabled criminality, the criminological literature remains uncertain about the extent to which cybercrime facilitates the commission of traditional crimes, and whether it is a major driver of a new wave of criminality. Many cybercrimes, in targeting computers or using computers as technological enablers of mass scams and social engineering, require a high degree of organisation combined with specialist technical and monetisation functions. However, the extent that cybercrime is driven by organised crime groups (traditional or project based, i.e. short lived networks of criminal actors) is less clear, and the presence of state or semi-state criminal actors adds further complexity (see above).

Many cybercrimes resemble offline criminal activities and some are unique or at least novel forms of cybercrime. Criminal activity on the Internet is wide-ranging and can include an assortment of offenses such as illegal interception, copyright violation, stalking, money laundering, extortion, fraud and resource theft involving the illegal use of computers (Broadhurst & Choo, 2011). In short, two forms of novel crime have emerged with the digital revolution: technology enabled crime (spam, fraud etc.) and computers as the targets of crime (computer trespass, theft of data, etc.). Grabosky (2001, pp. 243– 244) summarises this leap from the real world to cybercrime aptly:

> *"Computer crimes are driven by time-honoured motivations, the most obvious of which are greed, lust, power, revenge, adventure, and the desire to taste 'Forbidden fruit.' None of the above motivations is new. The element of novelty resides in the unprecedented capacity of technology to facilitate acting on these motivations."*

Due to the variety of criminal acts committed on the Internet, there has been much debate on whether established traditional theories are adequate in analysing online crime, or if there is need for the development of newer, cyber-specific theories.

Contemporary theories about cybercrime draw on conventional crime theory, adapting "old wine in new bottles" (Grabosky, 2001). Many traditional crimes are readily facilitated by digital technology and can be seen as the "old wine" in the "new bottle" that is cyberspace. The contemporary theories briefly explored here include Rational Choice Theory and other related approaches that focus on the role of offender decision-making such as: Routine Activity Theory, Displacement Theory, Deterrence Theory, Social Learning Theory, and Techniques of Neutralisation or "drift".

New cybercrime specific theories have emerged in an attempt to more accurately describe online offending. These theories are largely built upon established theories and have been applied to cyberspace in novel ways, such as Jaishankar (2008) building his Space Transition Theory's on anonymity and online deviance by drawing on Akers' (1998) Social Learning Theory (Holt et al., 2018). The new cyber specific theory explored in this section is Digital Drift.

"New Wine in Old Bottles" – 2016 Bangladesh Bank Hack

With the advent of network-technologies and the subsequent dependence upon them, bank robberies can be conducted with the safety and assurance of distance (the perpetrator does not even need to be in the same country). Moreover, masks need not be the only thing preserving a criminal's identity, as the anonymity provided by cyberspace through 'virtual private networks' and geolocation anonymiser technology decreases the ability for law enforcement to achieve identifications and arrests.

The reward, or target, has also increased substantially. In February 2016, unidentified hackers managed to steal US$81 million from Bangladesh's central bank. According to Reuters, "the hackers sent fraudulent messages, ostensibly from the central bank in Dhaka, on the SWIFT system, to the New York Federal reserve seeking to transfer nearly US$1 billion from Bangladesh Bank's account there" (Finn, 2016, n.p). Though most of the requests were denied, US$81 million was transferred to a bank in the Philippines, where it was then dispersed through casinos (Gopalakrishnan & Mogato, 2016).

Cyberspace in this instance created an opportunity to commit this theft by exploiting flaws in the bank's computer systems. Similar hacks were also carried out against the US Federal Reserve and Qatar National Bank. For more information regarding these cyberattacks, see:

- **Finn, T. (2016, April 28).** Qatar National Bank investigating alleged data hack. *Reuters.* Retrieved from http://www.reuters.com/article/us-qatar-ntl-bank-idUSKCN0XO22S
- **Lange, J., & Volz, D. (2016, June 1).** Exclusive: Fed records show dozens of cybersecurity breaches. *Reuters.* Retrieved from http://www.reuters.com/article/us-usa-fed-cyber-idUSKCN0YN4AM

Rational Choice Theory

Rational Choice theory is based on the idea that criminals will consider and evaluate their decisions before they commit a crime. Criminals are regarded as rational calculators of risk unless subject to pathology or defects of reason. The decision to commit crime is heavily influenced by the time required to commit the offence, the relevant abilities of the offender, and the information available to them. Where offenders have 'limited' capacities, their reasoning about the decision to commit or not commit the crime is similarly limited (NSW DAGJ, 2011b). As per the theory, crime will occur if the offender decides that the benefits of committing the crime will outweigh the benefits of not doing so. This reasoning (perhaps not necessarily sound) assists the offender in determining the risks of being detected against the expected pay-out.

Rational Choice Theory is useful for understanding the motivations of cybercriminals and counters them with deterrence policies. Competent cybercriminals are capable of planning a rational, low-risk/high pay-out crime. Their rationale may draw on the plethora of attack vectors (amplified by the Internet of Things (IoT)) and methods to disguise their identity. This makes it difficult for LEAs to attribute an attack to an individual or group, and it is therefore attractive for criminals to choose victims in the cyberspace over conventional targets.

This theory analyses the methodology of a crime through the offender's perspective (their decision making and how the offender uses the environment to commit the crime) and can provide a defensive framework based on deterrence (e.g. effective network security that will improve the likelihood of an offender being caught) and increasing the certainty of arrest.

Deterrence Theory, drawing on the notion that criminals are rational actors, stresses that punishment must be certain, severe and swift in order to prevent crime from taking place. That is, to a rational offender, the threat of the punishment must exceed the attractiveness of the crime (AIC, 2004). When implementing cyber laws and policy, the central tenets of certainty, severity and swiftness are often unable to be realised.

The process of investigation and attribution of a cyber-offence to an offender(s) is the most significant impediment to applying Deterrence Theory. According to Hui, Kim, & Wang (2017), the identification of cybercriminals is more time consuming and complex than conventional crime. This is largely due to the trans-national nature of cybercrime, the myriad of identity obfuscation techniques available to criminals and the sheer volume of offences. As a result, many countries – the United States of America, Azerbaijan, Lithuania and Slovakia – have reserved the right in the Convention on Cybercrime to only investigate and criminalise activities which cause serious harm (Hui, Kim, & Wang, 2017). To further complicate investigations, countries, such as Russia, refuse to punish domestic cybercriminal activities that target entities outside of their own borders (Holt et al, 2018). As a result, cybercriminals operating from non-signatories' countries or parties to the Convention on Cybercrime can enjoy a degree of immunity from prosecution – such 'safe havens' attract offenders.

Routine Activity Theory

Routine Activity theory (Cohen and Felson, 1979) is widely used to analyse various forms of criminal behaviour. It was originally designed for real-world criminal activity, such as street crime, but has proven to be highly useful when analysing cybercrime (Grabosky, 2001). The theory states that crime will occur when the following four (originally three) conditions are met: There exists 1) an accessible and attractive target, 2) the absence of a capable guardian, 3) the presence of a motivated offender, and 4) the resources (skills, networks, etc.) required to commit the crime (Cohen & Felson, 1979; Ekblom & Tilley, 2000).

The target in cybercrime is any computer or computer network that can be accessed or compromised by an offender. The acronyms VIVA (Value, Inertia, Visibility and Access) and CRAVED (Concealable, Removable, Available, Valuable, Enjoyable and Disposable) are used to conceptualise a suitable target (Felson, & Clarke, 1998). The VIVA descriptor in cybercrime can be any data that is accessible and of potential value to the offender if copied or stolen. The CRAVED descriptor outlines what data is worth targeting by the offender.

Capable guardians are also present in the online world and include (but are not limited to): network administrators, forum moderators, users, peers, and CERT's. Capable guardians also include automated protocols including firewalls, virtual private networks, anti-virus and anti-intrusion software, and ID authentication and access management systems (Leukfeldt & Yar, 2016).

Finally, the resources required to commit the crime are as varied in the cyber domain as they are in the real-world. Resources that are paramount to a sophisticated hacker's ability are creativity, curiosity, intelligence, and problem solving abilities (Steinmetz, 2016). Additional resources required by hackers can also include a reliable internet connection, access to hacking hardware and ('weaponised') software as well as the associated coding skill. Other incidentals include resources of money and time.

Motivated offenders in the online environment are abundant and are increasing at an exponential rate. Offenders can range from fraudsters and swindlers, hackers, insider threats, pirates, stalkers, state actors, terrorists and 'trolls'. There are numerous suitable, accessible, and poorly protected targets depending on the offender's abilities and resources, including: proprietary data, personal information, online payment and purchasing services, and computer systems themselves. These can be compromised and disrupted by unauthorised intrusions (Leukfeldt & Yar, 2016).

Displacement Theory

Displacement Theory argues that crime prevention activities actually have a transference effect whereby crime is shifted elsewhere rather than substantially eradicated as intended. The five main ways crime is displaced are: 1) geographical displacement, 2) temporal displacement, 3) target displacement, 4) tactical displacement, and 5) the crime type displacement (Bowers & Johnson, 2003).

The Internet, specifically darknet markets, exhibits displacement. As terrestrial illicit markets are shut down, marketplaces migrate to the darknet. In turn, darknet markets are routinely shut down by LEAs which see a number of vendors simply open up shop on another forum or market under the same 'handle' or name. Crime prevention efforts in the darknet merely shift the site and vehicle for the criminal market to operate. Police take-downs of crypto-markets, such as Operation Onymous (2014) and more recently Operation Bayonet (2017), ensnare many of the key criminal actors, but many of the drug vendors in these defunct markets are displaced, join other markets or create new ones.

Social Learning Theory

Akers' (1998) Social Learning Theory has been frequently applied to both online and offline offending. Ackers argues that an individual may become deviant through learning the behaviours and norms of delinquent peers (Akers, 1998). This dynamic social learning process is reinforced through differential association as "individuals are exposed to deviant definitions, models, reinforcement based on their differences in association patterns" (Holt, Bossler, & May, 2012). This effectively means that the more an individual, particularly a criminal, participates in deviant acts with other criminals, the stronger the reinforcement of criminal behaviour will be.

Social Learning Theory is readily applicable to online offending and can be used to understand how individuals become deviant online. This is due to the fact that there is a significant amount of technical learning that must happen for an individual to become a cybercriminal (Skinner & Fream, 1997, p. 498). This technical learning process would likely lead potential cybercriminals to interact with deviant peers in order to adopt these skills and therefore reinforce their deviant behaviour (Holt et al., 2012). This is particularly apparent with the hacker subculture where associations with veteran hackers are sought after by novices. These relationships are formed through imitation style hacking activities enacted by novice hackers that mimic the actions of more experienced hackers. As the novice participates more in the hacker subculture, their actions are socially reinforced, deepening their deviant behaviour (Holt, 2018).

Akers' Social Learning Theory is complemented by Jaishankar's (2008) Space Transition Theory – it attempts to explain via an emphasis on the anonymity of the online environment as to why some individuals are often only deviant online and then sometimes limited to their engagement with certain groups. The theory itself however, has been largely untested (Holt et al., 2018).

Techniques of Neutralisation and Drift

Sykes and Matza's (1957) Techniques of Neutralisation provide a framework for exploring why individuals and groups engage in deviant activity online. The theory focuses on how deviants process and rationalise the decision to conduct criminal or delinquent activities. It assumes that most people uphold beliefs that are generally consistent with societal values but that they may also engage in criminal behaviour. Neutralisation techniques are used by criminals and delinquents prior to committing the act in order to justify their behaviour and avoid conflict with their general belief systems (Matza, 1964). It is this process which allows for criminals to 'drift' between criminal and non-criminal acts without accepting a criminal identity (Matza, 1964), a notion recently adapted by Goldsmith and Brewer (2015). The five basic techniques developed by Sykes and Matza (1957) are as follows:

1. Denial of responsibility
2. Denial of an injury
3. Denial of a victim
4. Condemnation of the condemners
5. Appeal to higher loyalties

Hackers use these neutralisation techniques or reasons to justify their actions. Importantly, these neutralisation techniques precede the event, releasing the offender from their criminal or deviant activities and are not post-event excuses. Many hackers deny or minimize the injury caused to their victim or the seriousness of the event, arguing that their computer exploits do not cause real harm to the individual or their computers. Alternatively, they may attack computer systems or users that are dishonest or exploitative, rationalizing that they are not victims to begin with. Hackers have also blamed their victims for their poor computer skills and security, and may also appeal to higher loyalties such as "internet freedom", state espionage, or political ideologies. Techniques of neutralisation thus serve to preserve the moral integrity of the cybercriminal who may still need to justify their (exceptional) deviation from societal norms and expectations (Gordon & Ma, 2003; Chua & Holt, 2016; Holt et al., 2018).

Digital Drift Theory

Goldsmith and Brewer's (2015) Digital Drift Theory modifies Matza's (1964) "drift theory" and juvenile delinquency when applied to the digital environment. Digital Drift Theory builds on the idea that an individual is able to limit their engagement with particular delinquent online associations or networks, because the "drifting offender" has a high degree of anonymity and independence from their peers (in contrast to real offline gangs). Online delinquents can be drawn into criminal activities through attractive content or activities (i.e. activism, free media, hacking techniques, or leaked information) which exposes them to criminal behaviours and justifications that make the drift possible. Delinquents, however are also able to drift out of criminal actions simply by no longer associating with deviant groups (Matza, 1964), and this occurs in the online realm as it does in the offline world. Drift Theory provides a framework for how individuals can move between online offending and non-offending and can be integrated with other theories including Akers' (1998) Social Learning Theory and Sykes and Matza's (1957) Techniques of Neutralisation to provide a broader analytical approach to online offending. Adaptations of conventional criminological theory to explain criminal behaviour in digital eco-systems are not fully developed given the complexity of the cyber world and its potential in affording criminal opportunities. The role of state or semi-state actors, as well as potentially powerful non-state actors (i.e. organised crime and violent extremists) in the enhancement (and suppression) of cybercrime, evokes conflicting perspectives and is yet to be fully considered. A broader approach than the social-psychological orientation of crime causation theories may be helpful in addressing the connection between individual drivers of crime and the social transformations of criminal opportunities driven by technology.

In the next section, a description of the data collected from darknet websites offering illicit products is provided. Darknet markets, such as Dream Market, are criminal enterprises that share with offline crime groups the primary goal of financial rewards, and the creation of a trusted market that achieves the perfect blend of secrecy and efficiency.

Chapter 3: Darknet Research Findings

Methodology – Reconnaissance and Data Collection

Web forums and marketplaces are avenues where computer security enthusiasts can share or purchase ideas, vulnerabilities or code. While increased sharing and collaboration has the potential to strengthen our defences, many collaborations observed on the darknet or deepweb are criminal collaborations or activities. To access the deepweb, a specialised browser called The Onion Router' (Tor) is used (see pages 8 – 9). This browser ensures traffic is anonymous through obfuscation of the user's physical IP (Internet Protocol) address. Privacy may also be further enhanced via the use of a VPN (see pages 9 – 10).

Prior to data collection, reconnaissance of marketplaces for malware and exploits was conducted to identify patterns of transaction and sites of interest using open source information services. These open source information services included: DeepDotWeb, Torch, DuckDuckGo, Reddit and others. Marketplaces spanning the continuum of 'white hat' to 'black hat' were examined, including: Dream Market (currently the largest and longest surviving darknet market), 0day.today (a prominent 'Grey' market), bug bounty programs and deepweb forums.

The process of data collection included:

- Product listings and vendor 'handles' or aliases from Dream Market, September 2017 – April 2018
- Malware and exploit listing from 0day.today for the 'private' category, January – May 2018
- Malware and exploit listings from 0day.today for the 'restricted 0day' category, February – May 2018.

The process of data exfiltration for product listings from marketplaces raises several challenges due to the defences enacted by marketplace owners. These challenges are well known and may be difficult to overcome. For efficiency, a targeted and scalable approach to darknet market exfiltration reduced the time spent in the data capture phase, as typical data collection may have involved many hours of computer processing time.

A Targeted and Scalable Approach to Darknet Market Exfiltration

Crawling exercises have typically relied upon a single user account for site indexing. In this report, a new targeted and scalable approach utilising several login sessions simultaneously to reduce time spent indexing was created drawing on suggestions made by Gwern (2018), based on his attempts through 2013 – 2015 to capture data from crypto-markets on Tor. Different IP addresses were assigned to each 'spider' to ensure the bypass of DDoS protection and additional spiders were used during indexing to reduce the time taken to complete the data capture process. This data capture process can be divided into three phases, as seen in **Figure 7**, which are 'indexing', 'extraction and storage'; and 'analysis'.

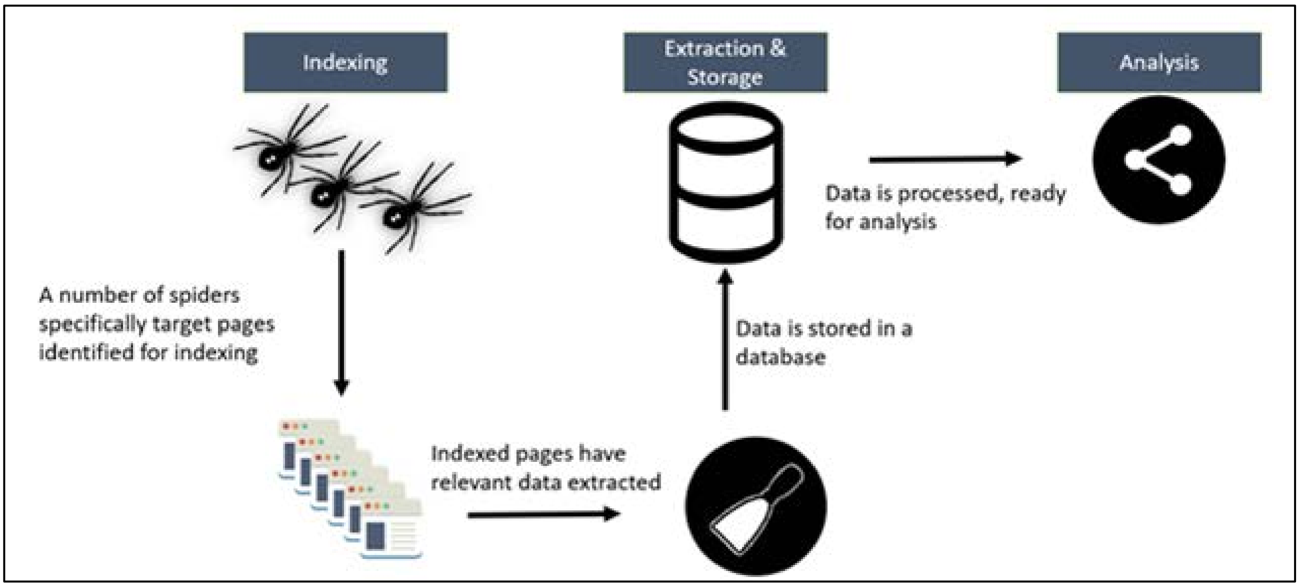
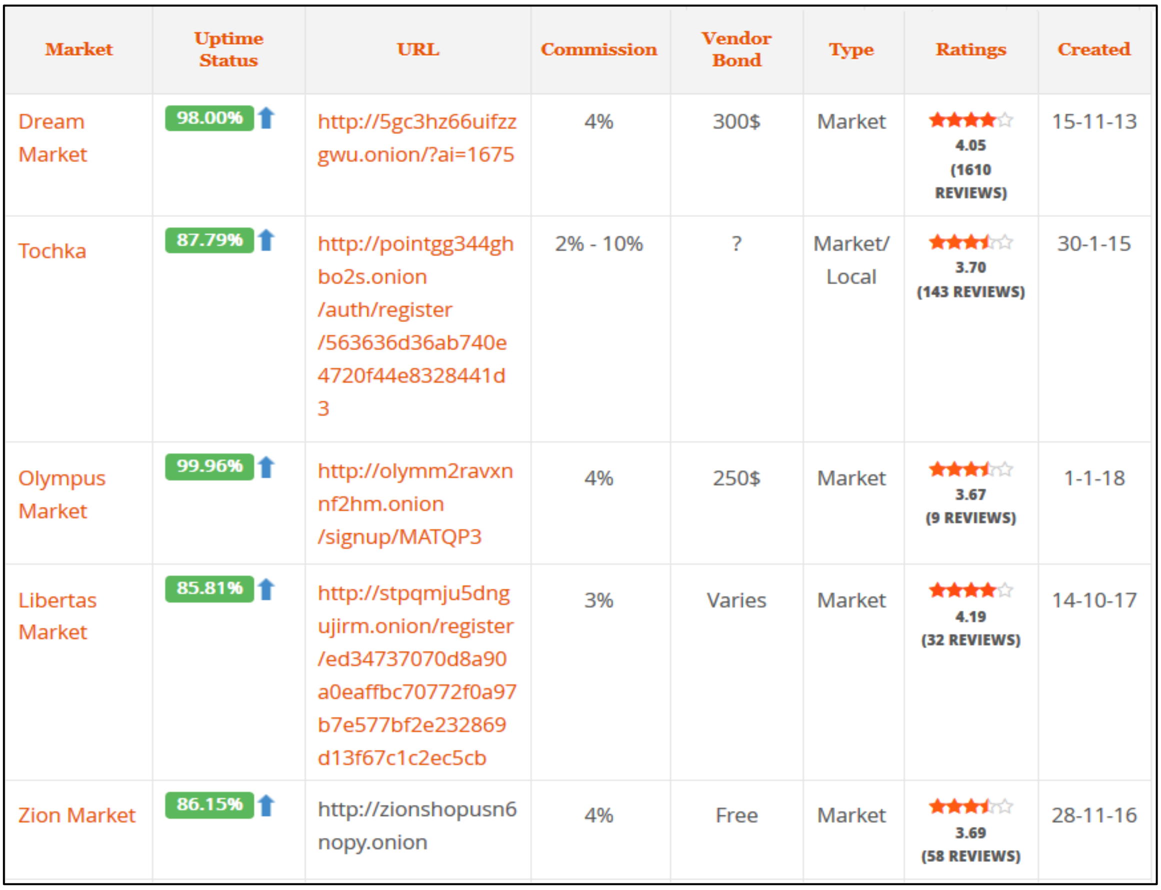

Indexing
Extraction & Storage
Analysis
Data is processed, ready for analysis
A number of spiders specifically target pages identified for indexing
Data is stored in a database
Indexed pages have relevant data extracted

Figure 7 - Logical workflow of the data exfiltration process

Indexing

Indexing of marketplaces was subject to darknet market availability, often termed 'uptime'. DeepDotWeb, a site that "gathers information and educates the public on everything related to the darknet" (DeepDotWeb, 2018) provides a comparison of different darknet markets' percentage uptime status, as seen in **Figure 8**. When a darknet market undergoes site maintenance, experiences a DDoS attack or the Tor exit node was slow, the indexing process becomes more time-consuming and, in some instances, inoperable. The overall accuracy of this data collection process was usually high and is reported below (see **Table 2**).



Market	Uptime Status	URL	Commission	Vendor Bond	Type	Ratings	Created
Dream Market	98.00% ⬆	http://5gc3hz66uifzzgwu.onion/?ai=1675	4%	300$	Market	★★★★☆ 4.05 (1610 REVIEWS)	15-11-13
Tochka	87.79% ⬆	http://pointgg344ghbo2s.onion/auth/register/563636d36ab740e4720f44e8328441d3	2% - 10%	?	Market/ Local	★★★½☆ 3.70 (143 REVIEWS)	30-1-15
Olympus Market	99.96% ⬆	http://olymm2ravxnnf2hm.onion/signup/MATQP3	4%	250$	Market	★★★½☆ 3.67 (9 REVIEWS)	1-1-18
Libertas Market	85.81% ⬆	http://stpqmju5dngujirm.onion/register/ed34737070d8a90a0eaffbc70772f0a97b7e577bf2e232869d13f67c1c2ec5cb	3%	Varies	Market	★★★★☆ 4.19 (32 REVIEWS)	14-10-17
Zion Market	86.15% ⬆	http://zionshopusn6nopy.onion	4%	Free	Market	★★★½☆ 3.69 (58 REVIEWS)	28-11-16

Figure 8 - Uptime of Darknet Markets (DeepDotWeb, 2018)

Extraction and Storage

Once indexing was completed, data extraction and storage was undertaken. Storage of product listings was maintained within a centralised database for ease of analysis. Embedded images were excluded from the data capture process to both prevent researcher exposure to illegal or offensive material, and to comply with ethical standards.

Analysis

To attribute product listings with the category of malware identified, linguistic analysis of the text string was executed via Python scripting. This required the formulation of word lists to effectively match listings to each category. It should be noted that these word lists are indicative of products only. Linguistic analysis may misclassify or overlook products and can incur Type I and Type II errors, false positives and false negatives.

Categories were established for determining the product sub-type within each product listed: Account, Botnet/DDos, Credit card, Documents, Hacking Tools, Keylogger, Phishing, Ransomware, Trojan/Virus, Tutorial and Vulnerability. For each of these categories, wordlists were formulated to categorise products found on Dream Market (see **Table 1**).:

Table 1 - Categories and their Respective Wordlists

Account	["account", "address", "bruteforce", "brute force", "username"]
Botnet/DDoS	["botnet", "booter","ddos", "denial of service"]
Credit card	["creditcard", "carding", "ccv", "fullz", "skimmer", "credit", "cvv", "fulls", "mastercard", "how to card", "credit card"]
Documents	["Identity documents", "documents", "passport", "document", "drivers license", "driving license", "credit card statement", "electricity bill"]
Hacking Tools	["sqli", "sql injection", "megapack", "hacking tool", "rootkit", "antidetect", "anti detect", "hack attack", "hack tool", "backdoor", "crypter", "blacklist", "black list", "wifi hack", "zeus", "spyeye", "spoofer", "penetration testing", "RATS", "Password", "account stealer", "hackpack"]
Keylogger	["keylogger", "key logger", "keystroke", "key stroke"]
Phishing	["phishing", "email", "spam", "phish"]
Ransomware	["ransomware", "ransom ware", "bitcoin ransom"]
Trojan/Virus	["trojan", "virus"]
Tutorial	["how to hack", "how to crack", "hacking tutorial", "hacking bible", "doxing tutorial", "penetration testing", "fraud guide", "hackers handbook", "hacking-ebook", "hacking ebook", "hack tutorial", "metasploit tutorial"]
Vulnerability	["vulnerability", "exploit", "code signing", "windows shell"]

Validation of Data Capture

In order to check the outcome and accuracy of each crawling attempt, the following steps were taken:

1. Record the total number of products listed within the market before crawling.
2. Total the number of product listing gathered by each spider at the end of crawling.
3. If these values (from a, b) coincide, we are reasonably sure of the completeness of our crawling. For a recording of accuracy = (b / a) * 100.

Over a six- month capture period, the average number of listings captured in the exfiltration process was 96.4% (note for September 1 and September 8 2017 data capture accuracy was unable to be verified). Malware listings remained stable, and variations in the number of *unique products* were not significant across the 16 data capture cycles. Descriptive statistics reported a mean of 7,534, and median of 7,128 products, with a minimum of 6,232 and maximum of 8,986 products.

*Table 2 - Basic Category Listings of All Products on Dream Market**

Product Type	Apr-14	Apr-04	Mar-28	Mar-21	Mar-18	Mar-12	Mar-08	Feb-24	Feb-09
Drugs	61926	59165	60052	58229	57580	56417	55006	53954	48263
Drug Paraphernalia	209	206	189	179	177	178	182	143	171
Digital goods	50113	49315	52698	52637	51751	50558	48769	47155	43204
Services	4341	4263	4150	4146	4157	4128	4089	3975	3336
Other	3841	3169	5351	5334	3111	5299	5219	5260	4983
All	120430	116118	122440	120525	116776	116580	113265	110487	99957
# Listings	**119844**	**105659**	**112280**	**111681**	**108246**	**116539**	**99645**	**95788**	**98919**
% Listings Captured	99.51%	90.99%	91.70%	92.66%	92.70%	99.96%	87.98%	86.70%	98.96%

*Note: Present here is a shortened version. For the full version, see Appendix 1.

Darknet Market Listings

The data exfiltration of Dream Market demonstrates the accessibility and low-cost for exploits and malware. Easily attainable malicious tools present a cybercriminal with plentiful opportunity to establish a revenue stream via committing numerous criminal acts. As noted previously, the number of unique product listings matching wordlists for malware remained relatively stable over the period of data collection. As seen in **Table 3**, average prices for each category of malware appeared stable with no major overall shifts observed. Fluctuations were noted within categories and 'anomalous' findings will be discussed – refer to each category average pricing graph. This table also shows the average number of listings, price and price rank across the six-month data exfiltration period for each category.

Table 3 - Average Number of Products and Prices for Different Malware Categories

Category	Average # Listings	% Listings	Average Price	Price Rank
Account (compromised)	5062.4	42.4	$47	3
Credit Card	3480.7	29.2	$45	4
Hacking Tools	1229.7	10.3	$7	9
Documents (passports, etc.)	801.6	6.7	$747	1
Phishing	497.6	4.2	$25	7
Tutorials	406.4	3.4	$6	10
Vulnerability/Exploits	112.0	0.94	$7	8
Keylogger	86.6	0.73	$4	11
Ransomware	87.2	0.73	$64	2
Botnet/DDOS	85.6	0.72	$29	5
Trojan/Virus	77.9	0.65	$27	6
Total	11927.8	100.00		

Due to their direct use in acts of fraud and other illicit monetary activities, it is not surprising that product listings for Credit Cards and compromised Accounts are the most prevalent listings, representing 72% of malware listings when combined.

Documents, including driver's licenses and passports, are the most expensive malware-related product listed based on average price. The expertise and tools required to produce these unique articles (e.g. a passport for a specific country) ensures that vendors can demand a high price due to the quality required for documents to pass verification.

Ransomware is the second most expensive malware related product also based on average price. However, individual prices vary greatly, indicating likely variations in quality. The cheapest product listings here were hacking tools ($7), tutorials ($6), vulnerability/exploits ($7), and keyloggers ($4). On examining listings within these categories, it is apparent that open source (free) versions of these are readily available.[7] Furthermore, these listings tended to come within a package of exploits or exploit toolkits. Recently, research conducted by Allodi (2018) in a Russian marketplace revealed a trend of packaged exploits becoming cheaper over time.

The 6 month observation of Dream Market demonstrates that openly accessible darknet markets tend to focus on products that are easily employable as a revenue stream or of unique value. Furthermore, this monitoring of darknet markets is invaluable to assist in the identification of cyberattack trends.

Anomalous 'Spikes' in Average Pricing

Anomalies were noted over the six-month period for the average pricing of the categories: ransomware, Trojan/viruses and vulnerability/exploits. On analysis, it was revealed that highly valuable listings persisted within the anomalous data points inflating the average price. However, these anomalous findings should not be ignored as an inflation of average price indicates that highly valuable malware sporadically persist within darknet markets. Each of the following categories exhibited anomalous average pricings and will be further examined: ransomware, Trojan/viruses and vulnerability/exploits.

Ransomware

No overall market shift within the category of ransomware was observed over the six month period. However, sporadic listings for highly priced ransomware did appear. For example, compare a typical listing for ransomware such as Philadelphia Ransomware (AU$19) and Ultimate Blackmail Bitcoin Ransomware (AU$13) with Ransomware-ALM4 Locker (AU$3,848).

This price differentiation depicts 'levels' of ransomware quality. That is, highly effective and sophisticated Ransomware will demand a higher price. Carbon Black (2017) research found that ransomware prices greater than $1,000 are either custom-developed, possess a unique code, or have been seldom employed in the wild (Carbon Black, 2017). Therefore, the 'anomalous' spikes in ransomware average prices depicted in these results indicate the presence of highly sophisticated malware.

For ransomware authors, successful creation and distribution of ransomware offerings appear to be fruitful, with some earning more than double the salary of legitimate software developers. Furthermore, ransomware sellers are increasingly specialising in one specific area of the supply chain, further contributing to the boom and lucrative development of ransomware (Carbon Black, 2017).

Trojan/Virus

Typical listings for Trojan/virus include the following common and inexpensive malware programs:

- Android Trojan Info Stealer [Fake Netflix] (AU$3.1)
- BTC wallet Alipboard Changer Virus 2018 (AU$5.2)
- Trojan Horse Creator Program Blackshades Full (AU$3.1)

[7] For example, the Windows XP SP3 MS11-006 exploit is freely available with an included tutorial at: "https://www.hacking-tutorial.com/hacking-tutorial/hacking-windows-xp-sp3-via-ms11-006-windows-shell-graphvulnerability/"

However, a sporadic ‘spike’ was observed on 15 November 2017 indexing and was associated with a single product listing for a Trojan capable of compromising ‘cash’ machines: “ATM MALWARE ATM VIRUS ATM JACKPOT WINCOR! (AUD$6,610)”. A Trojan capable of compromising certain ATMs understandably has high value but possesses a limited shelf or user lifespan. Nevertheless, they are heavily promoted as high income streams for cybercriminals.

Vulnerabilities/Exploits

Typical listings for common exploits and vulnerabilities are among the cheaper malware products and include:

- [Exploit Kit] Bleeding Life (2.0) (AU$1.1)
- 2018 Bank of America Business Account Exploit (AU$10.4)
- By Passing UAC Without Code Signing Hack With Src (AU$3.1)

Although these tools provide a range of capabilities, they often rely on older vulnerabilities that a victim may or may not be patched against in legacy or in current software. However sporadic ‘spikes’ were again observed on 1 September 2017 and 28 March 2018. Our analysis showed that these spikes were associated with the following updated exploits:

- Bestbuy Exploit - Updated (AU$631)
- SSENSE Exploit - Updated (AU$631)
- Walmart Exploit - Updated (AU$631)
- Expedia Exploit - Updated (AU$631)

For example, The Shadow Brokers advertised the NSA exploits on Dream Market in January 2017 at US$7,500 per exploit. No transactions were recorded on Dream Market; however, buyers may have been sceptical of authenticity due to no additional details provided within the listings (Lawrence et al. 2017). This demonstrates that cybercriminals may elect to advertise their ‘wares’ and ‘shop around’ for the best deal possible.

The ‘anomalous’ spikes in average price for the categories discussed above indicates the presence of highly sought after malware for sale within the market. These types of malware typically offer functions or innovations that have been unseen or utilise zero day exploits. As a result, marketplaces can facilitate the monitoring of harmful malware and act as an ‘Early Warning System’ for imminent waves of cyberattack. However, low level malware products are common and can saturate the market.

In the next section the average listings and prices for all the main digital products are described and illustrate the short-term trends over a six month capture period that also show the presence of atypical prices and numbers of product listings.

Malware and Crime-ware Products on Dream Market

The following section describes the different kinds of malware and other digital products available on crypto-markets such as Dream Market. The function, price (average price and trends) and desirability of each major type of malware is compared and examples of products advertised are illustrated.

Accounts

Accounts represent a large proportion of malware listings and include logins/passwords for various websites and 'hacked' accounts. Software and tools to hack specific providers such as Gmail, Facebook, Skype are also observed in this category. Here, accounts may also refer to credentials used for login to various sites, typically in the form of usernames and passwords. Figures 9 and 10 describe the recent trends for account product listing and average price.

Accounts are popular listings on darknet markets as buyers reduce their risk of detection and the investment of time and resources when trying to compromise the accounts themselves. These accounts can then be used for data mining personally identifiable information and digital content. It can also be used as a false flag type attack vector to conduct further cybercriminal activity, such as a spam or malware campaign, while reducing the overall threat of detection. The average product price was $41.

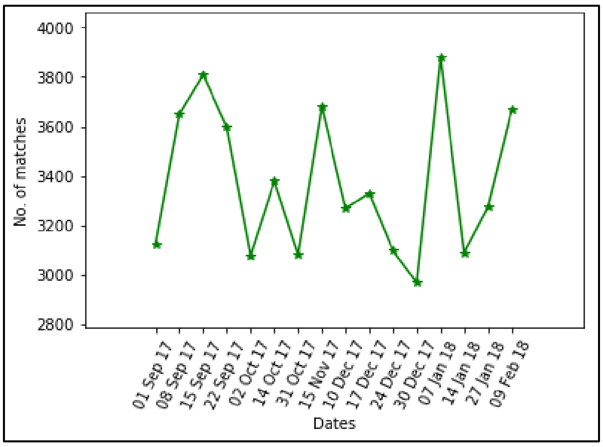


Figure 9 - Trends in Unique Product Listings for Accounts

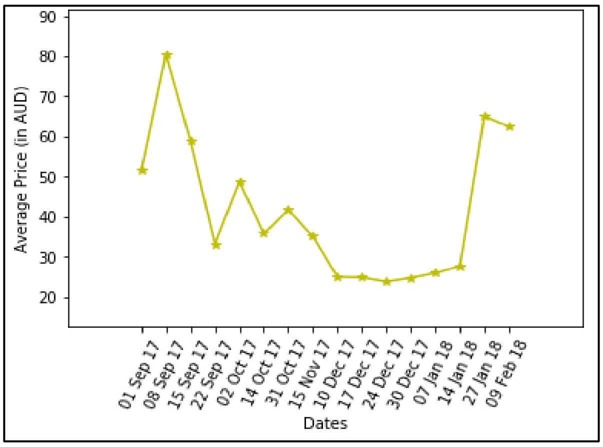


Figure 10 - Average Pricing $AU of Unique Product Listings for Accounts

DDoS and Botnet Services

DDoS (Distributed Denial of Service) and botnet services can be bought or rented including software to 'Build Your Own Botnet'. DDoS attacks are instances where a server is bombarded by more web traffic than it can process, resulting in restricted service. A botnet is a collection of 'zombie' computers that are controlled by

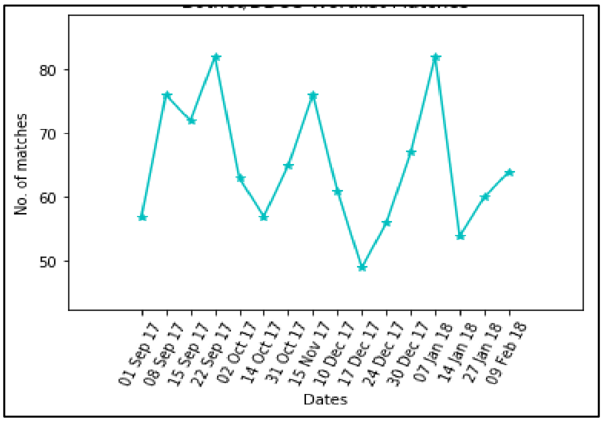


Figure 11 - Trends in Unique Product Listings for Botnet and DDoS Services

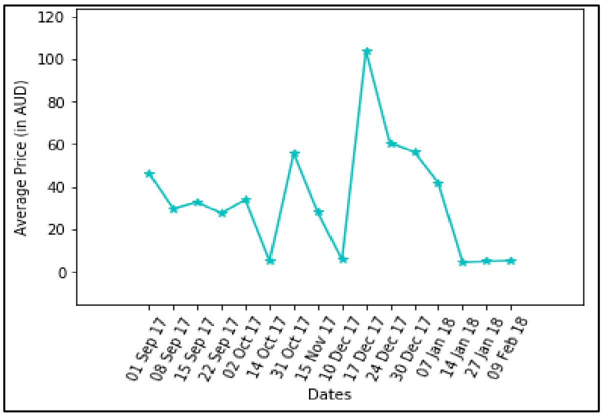


Figure 12 – Average Pricing $AU of Unique Product Listings for Botnet and DDoS Services

a single entity (Symantec, 2018). Botnets are commonly used to enable DDoS attacks, but can also be used for other purposes (e.g. cryptocurrency mining). See Figures 11 and 12 for average price trends over time.

The uses of a Botnet service are varied. They can be used to create a DDoS attack or used as a malware delivery system, such as the Andromeda Botnet (Europol, December 2017) or various crypto-jackers (Ścibor, 2018). They can also be used to mine personally identifiable information. Botnets are often difficult to attribute due to their complex nature and are even more so when a third party is involved, as with Botnet rentals. The average product price was $34.

Credit Card Credentials

Credit card credentials or carding services are readily available with many different types and countries advertised. Packaged deals often offer a discount. Vendors often advertise the success rate of their 'Carding' and give examples of utilising 'Fullz' for illicit purposes. Here, carding is the term used to denote the illicit process of utilising stolen bank cards and personal information (Peretti, 2008, p. 380). Fullz refers to a collection of information that includes all available details (e.g. number, personal information) of a victim (Holt & Lampke, 2010, p. 40). Figure 13 and 14 describes the recent trends for account product listing and average price.

Stolen credit cards details are primarily used for fraud and related activities. A seller is able to gain a profit from the sale itself with reduced risk of detection from a financial institution or law enforcement agency. Conversely, the buyer is able to launder money from a victim's account (e.g. purchasing cryptocurrency) with minimal risk of detection or attribution. The average product price was $34.

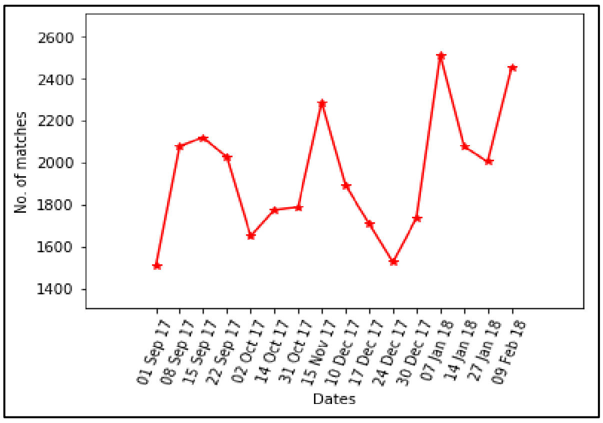


Figure 13 - Trends in Unique Product Listings for Credit Card Credentials

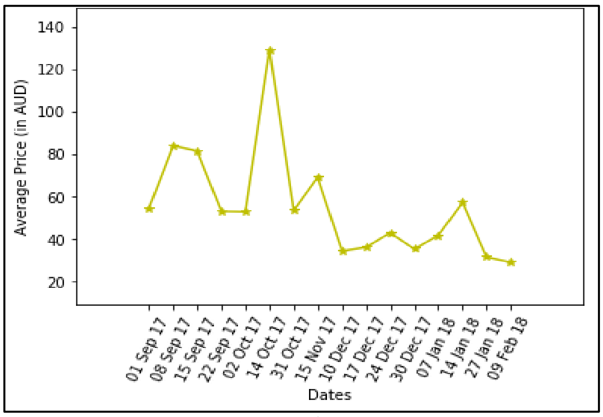


Figure 14 - Average Pricing of Unique Product Listings for Credit Card Credentials

Documents

Documents relating to identity (e.g. passport, driver's license, bank statements, etc.) are frequently made available on dark markets. Physical identity documents, digital scans and templates of legitimate documents are observed. 'Documents' - stolen or fraudulently produced documents in physical or digital form can be utilised in a range of criminal activities. Figures 15 and 16 describe the recent trends for account product listing and average price.

Stolen or forged documents can be used for the purposes of identity theft and fraud. Moreover, criminals use stolen or forged documents to avoid detection and to create false flags for illicit activities. This type of product is popular amongst sellers as information is usually easy to obtain from poorly defended computer systems. The average product price was $956.[8]

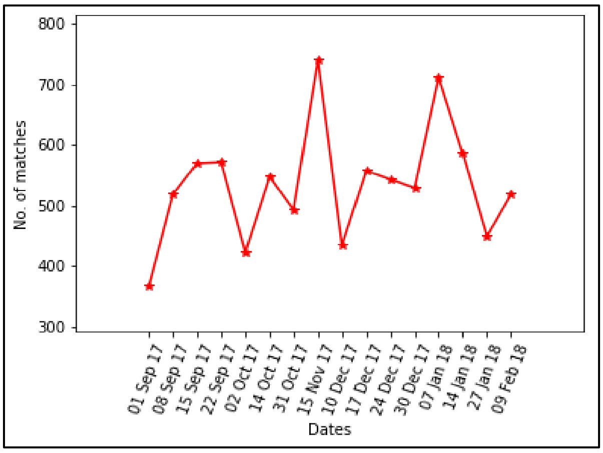


Figure 15 - Trends in Unique Product Listings for Documents

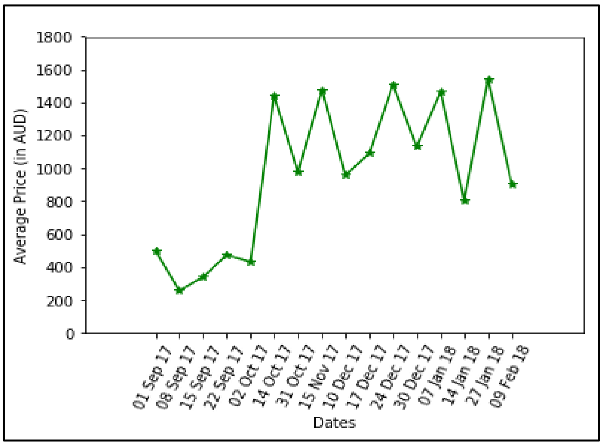


Figure 16 - Average Pricing of Unique Product Listings for Documents

Hacking Tools

Hacking tools relate to forms of software specifically built to perform malicious activity (for example, SQLi, RATs, hacking packs). Within this category are a range of tools frequently identified by law enforcement for use in criminal activity. This category encompasses a number of different forms of malware. These tools can be used to enable remote access or penetration testing, and are commonly offered with 'packs' – such as Zeus and Spyeye. Zeus is a type of Trojan malware that establishes a backdoor into affected Windows computers, and is capable of collecting passwords through keyloggers. Figures 17 and 18 describes the recent trends for account product listing and average price.

Hacking tools are desirable to a number of cybercriminals, ranging from low-skill script kiddies to more able hackers. These tools are often coupled with exploits that bypass a systems capable guardian, including firewalls and users, in order to infect as many systems as possible. The average product price was $7.

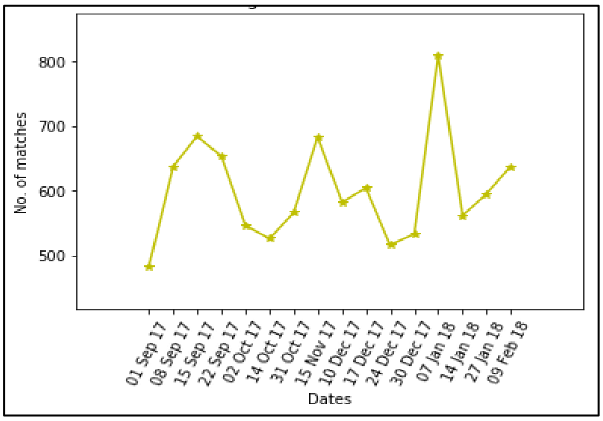


Figure 17 - Trends in Unique Product Listings for Hacking Tools

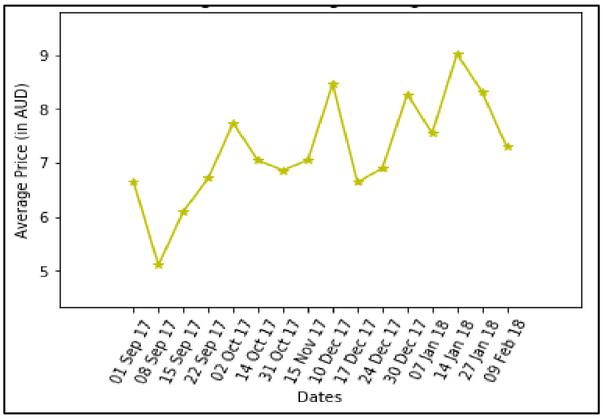


Figure 18 - Average Pricing of Unique Product Listings for Hacking Tools

[8] Note this sum differs from $747 reported in summary table 3 because it accounts for the average of unique listings rather than the average sum for all listings.

Keyloggers

Keyloggers are frequently advertised, and are often packaged with other malicious software. They are a form of malware that records the keyboard activity (keystrokes) of compromised systems, thus obtaining access to key passwords and information. Figures 19 and 20 describe the recent trends for account product listing and average price.

Keyloggers are covert malware that can avoid detection and are able to record keyboard activities on compromised systems. Stolen passwords and data can then be used for deeper system infiltration. By stealing passwords and data, attackers can effectively bypass a capable guardian by appearing to be a legitimate user. The average product price was $4.

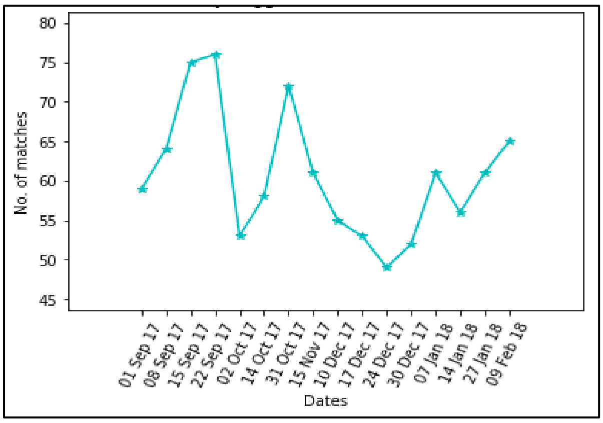


Figure 19 - Trends in Unique Product Listings for Keyloggers

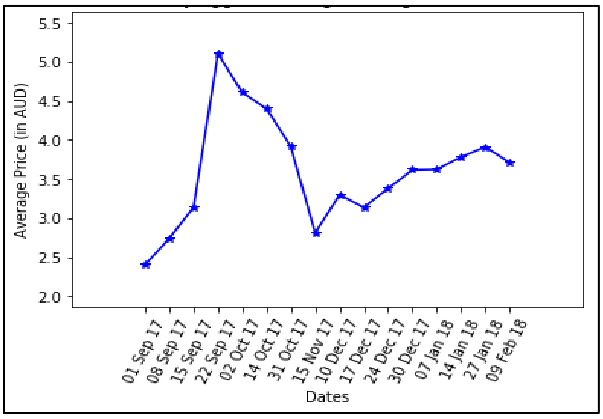


Figure 20 - Average Pricing of Unique Product Listings for Keyloggers

Phishing

Phishing tools are common, with templates for various pages. Often pre-packaged with customisable tools to carry out Phishing campaigns. 'Phishing' is the process of sending false emails to obtain personal information and passwords. Figures 21 and 22 describe the recent trends for account product listing and average price.

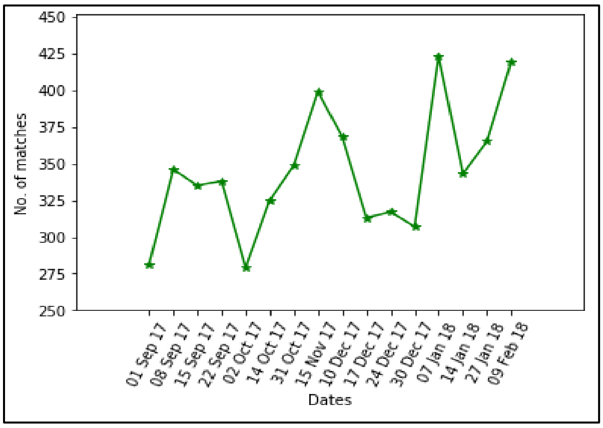


Figure 21 - Trends in Unique Product Listings for Phishing

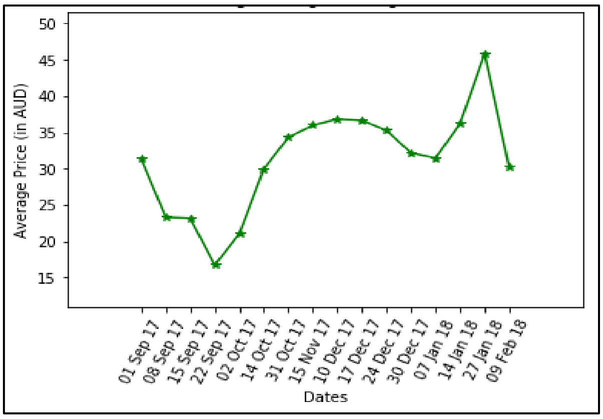


Figure 22 - Average Pricing of Unique Product Listings for Phishing

Phishing is a form of Social Engineering and does not necessarily need a high level of technical knowledge to execute. It relies on exploiting user vulnerabilities and trust in order to gain personally identifiable information or deeper system access. Phishing tools are often desirable as they come pre-packaged or sold with email databases and, therefore, make the act of phishing relatively simple. The average price was $31.

Ransomware

Ransomware is widely advertised with ready-made or customisable distributions. Customisable distributions can be tailored for specific email addresses or adjustable ransom payment. Ransomware specifically refers to a type of malware program that is used to extort financial funds from victims (often various forms of cryptocurrency). This malware will often encrypt important files and reduce the functionality of computer systems until the ransom is paid. Figures 23 and 24 describe the recent trends for account product listing and average price.

Ransomware has been sought after due to the direct pay out available. The payments are often made in ‘difficult to trace’ cryptocurrencies, such as Monero. This helps avoid the attribution of the attacker as they are able to easily launder their funds. These payments are usually equal to the price of having a computer fixed by professionals and as a result the ransom is often paid. Due to these attacks being overt, they draw a high degree of attention by LEA’s and the cybersecurity industries (See Wannacry, page 5). As such, using ransomware to extort payments from victims carries a moderate risk depending on the severity of the attack and the sophistication of ‘identity hiding’ techniques used. The average price was $74.

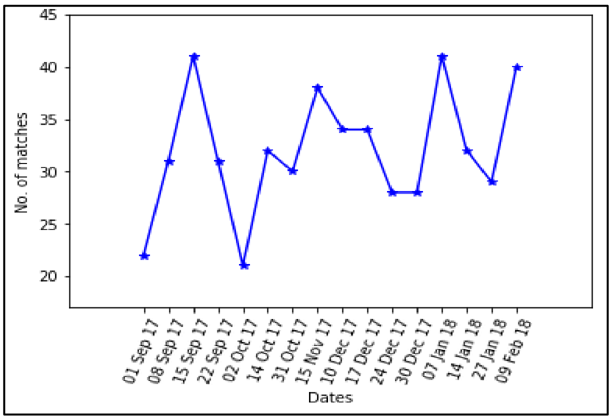


Figure 23 - Trends in Unique Product Listings for Ransomware

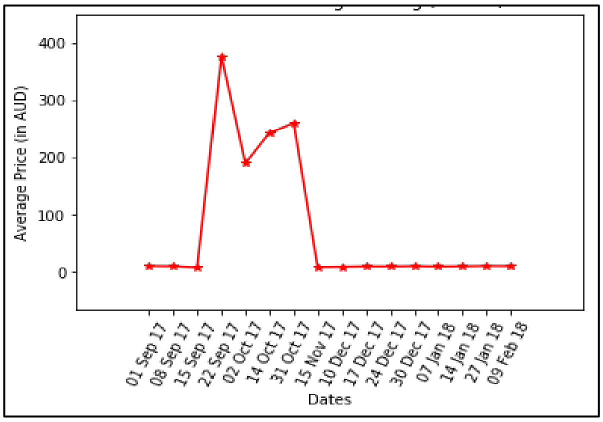


Figure 24 - Average Pricing of Unique Product Listings for Ransomware

Trojans and Viruses

Trojan and virus software along with detailed implementation instructions are common, often packaged with ‘builder’ software and tools. A ‘Trojan’ is a form of malware that impacts the operation of computer systems and steals important data (e.g. through tools such as keyloggers). Further, a Trojan can make the system vulnerable to the establishment of backdoors and remote access. A ‘virus’ is a form of malware that requires 'user activation' to obtain access to computer systems. Once installed, viruses can manipulate processes and infringe upon system functionality. Figures 25 and 26 (next page) describe the recent trends for account product listing and average price.

Trojans, like their historical namesake, are desirable because they are designed to bypass a computer or networks capable guardian and create a backdoor for attackers or to deliver a payload such as a virus. These are desirable by attackers as they can be difficult to detect, and due to their ubiquity, difficult to attribute. Because of this, attackers are not deterred from using these forms of attack. The average price was $24.

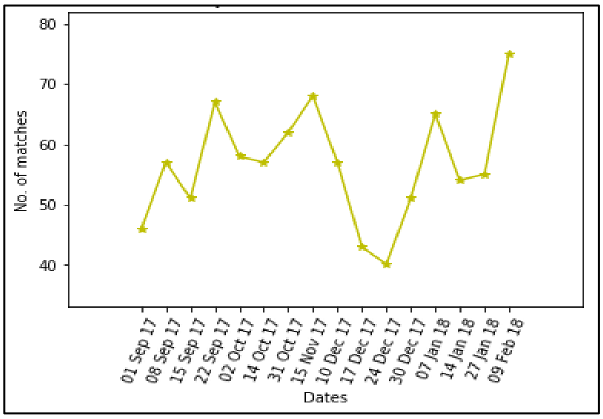


Figure 25 - Trends in Unique Product Listings for Trojans and Viruses

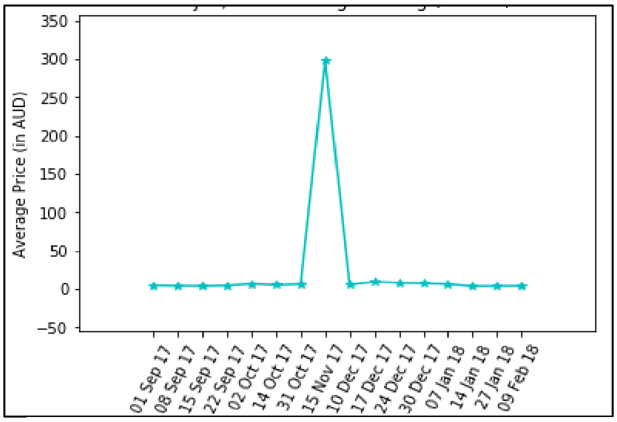


Figure 26 - Average Pricing of Unique Product Listings for Trojans and Viruses

Tutorials

Tutorials are common, and are often packaged in PDF files which include detailed teachings on many cybersecurity and hacking related topics. A tutorial as used here defines a set of instructions that depict particular hacking skills and methods. These are often found on websites where individuals can self-teach hacking. Figures 27 and 28 describe the recent trends for account product listing and average price.

Quality tutorials are highly desirable products by 'black', 'grey' and 'white hat' hackers. This is due to the wealth of information that can be provided for both offensive and defensive purposes. These tutorials also form part of the dynamic learning process in Social Learning Theory as not only are potential 'black' and 'grey hats' exposed to hacking culture, they are also given new definitions and models to base their behaviour on. The reinforcement component is satisfied where hackers use the lessons within tutorials in their own cyberattacks. The average price was $6.

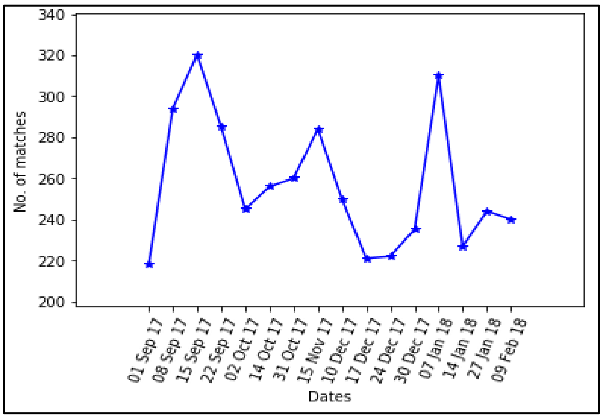


Figure 27 - Trends in Unique Product Listings for Tutorials

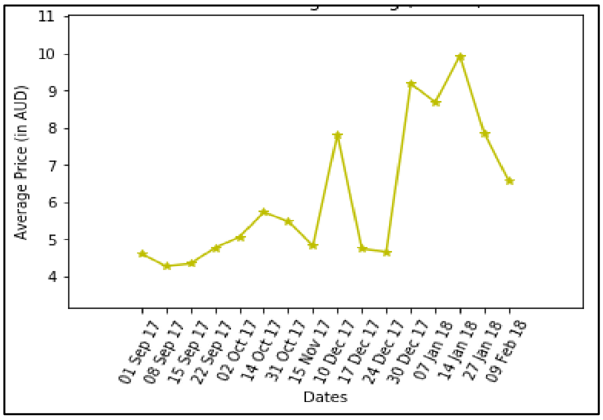


Figure 28 - Average Pricing of Unique Product Listings for Tutorials

Vulnerabilities and Exploits

Vulnerabilities and exploits are advertised with varying levels of sophistication and are often accompanied with detailed instructions. Within a computer system, a vulnerability is a security or software weakness that can be exploited by cybercriminals for malicious purposes, such as obtaining unauthorised access into a system (ACSC, 2017). Figures 29 and 30 describe the recent trends for account product listing and average price.

Vulnerabilities and Exploits are some of the most highly sought after items, especially if they are from new products (i.e. zero day exploits). These exploits, particularly newer ones, can be unknown to security vendors and, therefore, their use can be undetectable (See Spectre and Meltdown, see page 33). Because of this, attackers are able to use these exploits undeterred as there is little risk of being caught. The average price was $7.

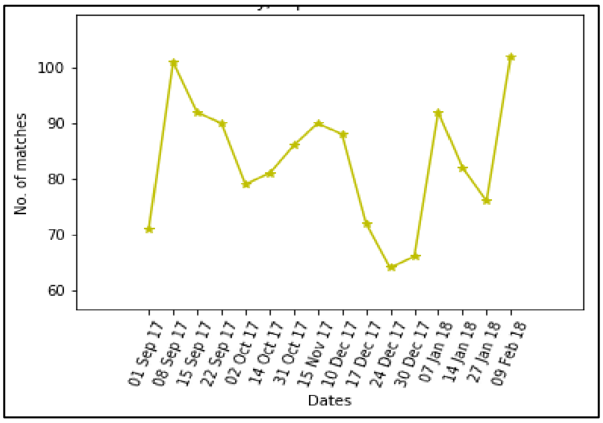


Figure 29 - Trends in Unique Product Listings for Vulnerabilities and Exploits

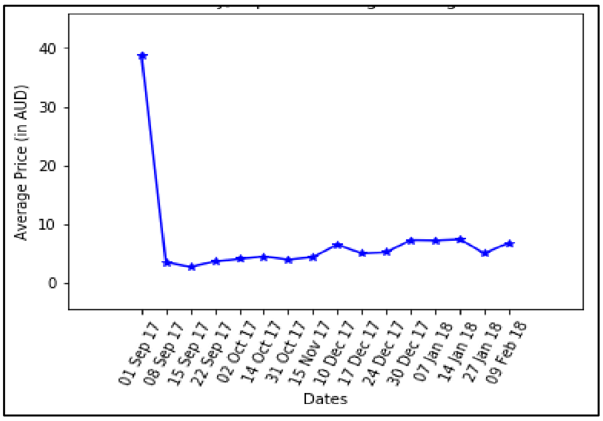


Figure 30 - Average Pricing of Unique Product Listings for Vulnerabilities and Exploits

In the following section specialised or niche markets for the sale of malware, especially zero-day exploits are described. Here we observe the relevant forum listings and price fluctuations associated with the so called 'grey' market and forum as well as the challenges the 'bug arms race' presents.

Marketplaces for Malware: Clearnet, Darknet and Closed Forums

The current landscape of online security may be viewed via a continuum encompassing 'white hat' and 'black hat' services. These range from proactive hackers engaging in bug bounty programs and cybersecurity research, to criminal actors involved in darknet marketplaces and services that occupy the deepest corners of the Internet. Bug bounty programs are cash incentives offered to cybersecurity researchers for identifying and reporting code and system errors in API's direct to the software producer or to the wider public. These often termed 'white hat' hackers engage in 'ethical' hacking and may be solicited by companies to engage in penetration testing, or offered a reward for notifying them of bugs and vulnerabilities found in their software. These ethical hackers may receive merchandise or monetary reimbursement for their efforts and operate in the open or clearnet. The incentives, or bounties, can range from as little as US$25 and up to US$100,000. However, some programs do not offer any remuneration for bug reporting and will only give an acknowledgement on their website or public forum.

The Internet services company, Netscape, is credited with introducing the first bug bounty program in 1995. Numerous bug bounty programs have since developed and usually entail specific rules set by the requesting company. These rules are generally in line with basic security and privacy policies and may carry penalties if not adhered to. Increasingly, many computer software companies have followed suit and introduced bug bounty programs to incentivise ethical hackers and now large corporations such as Facebook and Google use bug bounty programs to enhance the cybersecurity of their products. More recently, online firms have provided a platform for companies and organisations to access a large network of crowdsourced cybersecurity researchers. These third-party providers, such as HackerOne, Bugcrowd and Zerodium, offer a place where companies and organisations can connect with thousands of registered security researchers rather than implementing their own bug bounty programs (Schulz, 2014).

The concept of the bug bounty program has been widely adopted among computer software companies and the information technology industry. Bug bounty incentives are also being gradually implemented into financial services and other e-commerce industries, such as tourism. Vulnerabilities in publicly available software have contributed to a large number of cybersecurity incidents across the globe. Hence, patching these vulnerabilities are a priority given their potential for exploitation by malicious actors.

According to Bugcrowd's 2017 'State of Bug Bounty Report', there has been a rapid increase in new bug bounty programs compared to 2016 (Bugcrowd, 2017). Similarly, there has been an increase in the number of valid or actionable vulnerabilities submitted as well as the number of cybersecurity researchers. Following this trend, there has also been a steady rise in the average pay out for bug reporting (Bugcrowd, 2017). Generally, the highest bounties are awarded to bugs found within IoT devices, particularly within the automotive industry.[9]

There are many ways cybersecurity researchers can develop their skills, however cybersecurity competitions have grown significantly in popularity and innovation. These contests provide an environment for cybersecurity researchers to gain hands-on experience and test their skills against some of the best hackers in the world. Starting in 1993, DEFCON is now one of the largest hacking conventions in the world, as well as the longest running. DEFCON's signature event is their Capture the Flag competition, where each team must simultaneously defend their own services, while attempting to penetrate their opponent's (Childers et al., 2010). Since its inception, DEFCON has inspired dozens of other cybersecurity competitions across the globe (Childers et al., 2010).

Responsible Disclosure

Although the effectiveness of bug bounty programs has been recognised across industries, security researchers face the complex and fraught issue of disclosure when notifying companies and the public of software vulnerabilities (Mitra & Ransbotham, 2015). Bug bounties are based on the premise that security researchers will comply with the framework stipulated by the company or third-party, such as Bugcrowd. Through the incentivisation of identifying and sharing bugs, a form of capable guardianship is created (i.e. ability to stop or deter intrusions – see routine activity theory). However, the difficulty in negotiating a vulnerability disclosure is particularly apparent with companies that have not implemented a bug bounty program. The current extent of the commercialisation of vulnerabilities is also related to different methods of disclosing information about vulnerabilities. When security researchers elect to divulge a vulnerability, they have two disclosure options – responsible or full disclosure.

The responsible, or limited disclosure model requires that a security researcher refrain from disclosing the vulnerability to the public until it has been patched. This model aims to stall the circulation of attacks by first notifying the vendor or third-party organisation, such as the Software Engineering Institute, who in-turn inform the vendor (Mitra & Ransbotham, 2015). This allows time for the vendor to issue a patch before public notification. In turn, attackers and other security professionals are also made aware of the vulnerability at

[9] The amounts paid by bug bounties primarily depend on the popularity and security strength of the affected software or system, as well as the quality of the submitted exploit (full or partial chain, supported versions/systems/architectures, reliability, bypassed exploit mitigations, default vs. non-default component, process continuation, etc.).

the time of public notification. Cyberattackers may nonetheless discover vulnerabilities (and, therefore, exploit them) prior to the patch or indeed disclosure of the ‘bug’.

Full disclosure, however, occurs when security researchers, (potential) attackers and vendors are notified about a vulnerability simultaneously. The vulnerability is uncovered and directly disclosed through public forums and arguably “provides incentives to vendors to create better quality software” (Mitra & Ransbotham, 2015, p. 566). It may further be argued that this method of disclosure places the advantage with the attackers who are able to exploit the vulnerability before a patch is dispensed (Mitra & Ransbotham, 2015).

Where security researchers fail to disclose appropriately, or where a company’s standards of disclosure have not been adhered, lawsuits have been initiated against individuals who expose software vulnerabilities. This punitive approach also acts to deter security researchers, who are dissuaded from engaging in finding vulnerabilities, even where companies have implemented bug bounty programs (Whittaker, 2018).

While some security researchers disclose vulnerabilities for monetary incentive or accolades, others may wish to report and publish vulnerabilities for academic progression and cryptographic development. However, a review of some cases suggests that ambiguity and trust between security researchers disclosing software vulnerabilities and businesses protecting their intellectual property and integrity are common (Lynch, 2015). Lawsuits however, are not only reserved for individuals disregarding disclosure standards, but can be targeted at companies who do not inform the public in a timely manner, or issue sufficient patches to address the vulnerability. For example, Intel was sued in several US states for allegations of this nature (Kanji, 2018). Australia’s newly enacted data-breach disclosure rules should also stimulate attention to program or system vulnerabilities and encourage corporations and others who hold data to take active steps to prevent such breaches and to act promptly to repair or recover such data losses.[10]

Spectre and Meltdown

Spectre and Meltdown are legacy zero day vulnerabilities discovered in late 2017. There are three variations of these vulnerabilities: the first two are grouped together and are known as Spectre (CVE-2017-5753 & CVE-2017-5715) and the third is Meltdown (CVE-2017-5754) (Fruhlinger, 2018; Higgins, 2018). These vulnerabilities are present in nearly every computer that possesses a microchip manufactured in the last 20 years (Fruhlinger, 2018).

Unlike most computer vulnerabilities, Meltdown and Spectre are not found in the software but rather in the hardware of the microprocessors (Ford, 2018). This means that there is no readily available or easily distributable software patch (Ford, 2018). The stop-gap efforts distributed by vendors to patch the security flaw have also had the negative effect of slowing down CPUs by approximately 10% to 30% (Hruska, 2018; Higgins, 2018).

[10] Amendments to the Australian Privacy Act 1988 to introduce a Notifiable Data Breach scheme with the *Privacy Amendment (Notifiable Data Breaches) Act* 2017 with effect from February 2018 provides significant penalties for failure disclose and rectify data breaches, including those that arise from exploits and vulnerabilities.

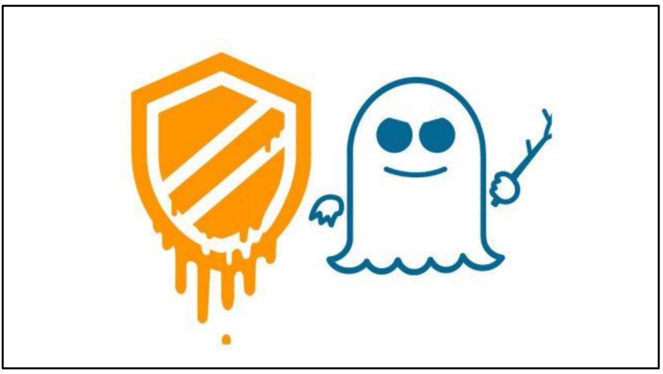


Figure 31 - The logos of the Meltdown and Spectre exploits (Hruska, 2018)

The Meltdown vulnerability received its name because it "melts security boundaries which are normally enforced by the hardware". It is able to "break the most fundamental isolation between user applications and the operating system" and can allow malware to access all the kernel memory on the device. It applies to personal computers and cloud infrastructure that use Intel processors (Graz University of Technology, 2018).

The Spectre vulnerability received its name based on the "root cause, speculative execution" and also from the extreme difficulty in fixing it, meaning that "it will haunt us for quite some time" (Graz University of Technology, 2018). It differs from Meltdown as it "tricks other applications into accessing arbitrary locations in their memory" (Graz University of Technology, 2018). When applied, an attacker is able to read the kernel memory and potentially sensitive system memory, including passwords, encryption keys and emails (Higgins, 2018). Spectre can be applied to all systems using Intel, AMD and ARM processors (Graz University of Technology, 2018).

Due to the nature of the vulnerabilities, Meltdown and Spectre are currently impossible to detect as they do not leave any traces in a computer's log files. Because of this, it is unknown if these vulnerabilities have been exploited in the wild (Graz University of Technology, 2018; Higgins, 2018). Meltdown and Spectre are particularly worrying as it is likely that these vulnerabilities are not unique (Higgins, 2018). It is far more likely that there will be more legacy zero day vulnerabilities discovered and exploited in the future that can pose an equally large risk to computer security.

Booter Services

Booter or stresser services may be found on open source websites and offer DDoS attacks for a small fee (Hutchings & Clayton, 2016). Masked as legitimate services offering stress testing for personal or professional purposes, booter services fall within the 'grey area' of cybersecurity. DDoS attacks overload a system, usually executed by a network of 'zombie', or robot, computers called a 'botnet' (Symantec, 2018).

Constructing and controlling a botnet is a technical and time-consuming endeavour, hence booter services operate through different technology that employ amplification and reflection techniques that enhance the impact of DDoS.

> "*—small request packets are sent to a third-party computer, which returns (reflects) a much larger response, often 10 to 20 times the size. However, the source of the requests is forged so that the responses go to the victim. By using many reflectors in parallel the booter service can overwhelm many victims simultaneously using just a single server to generate the request packets*" (Hutchings & Clayton, 2016, p. 1163).

Websites that offer booter services plausibly justify their enterprise through claiming the legitimacy of their stress testing practices. However, Douglas *et al.*, (2017) argue that these services are illegitimate and morally unjustified.

Marketplaces for Malware: Darknet Markets

Open Marketplaces

There are many marketplaces and vendors operating in Tor and similar environments. The exact number of such markets is unknown although Reddit, DeepDotWeb and other index and interest sites provide some lists of active market places; between 35 and 45 darknets are routinely listed on DeepDotWeb. The following darknet marketplaces were visited and data samples of product listings extracted and compared to Dream Market:

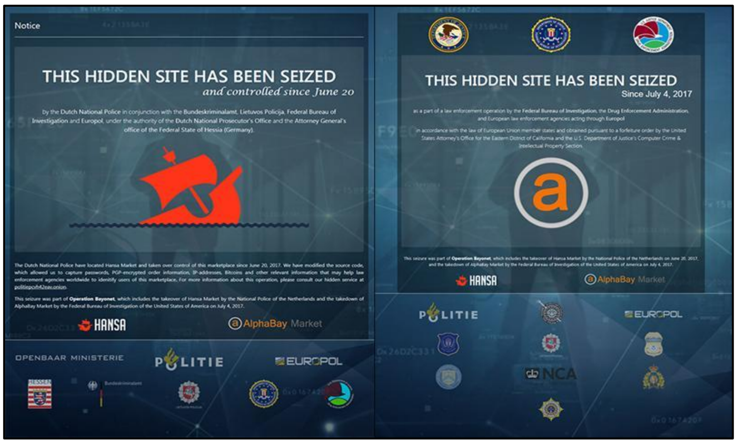
- Wall St Market
- Trade Route
- Tochka
- Aero
- Libertas
- Zion
- RSClub
- Berlusconi

During our data capture, Trade Route, Aero, and Libertas were shut down, whilst Zion experienced intermittent disruption. These smaller markets tended to focus on a fewer products or products not usually for sale on larger omnibus markets such as Dream Market. For example, RSClub offered firearm products typically prohibited on many markets. A number of non-English marketplaces were identified as operating (for example, the Portuguese Mercado Negro). However, for this research the scope was limited to English marketplaces. A substantial proportion of known malware are reportedly produced by Russian hackers and therefore the investigation of Russian malware markets (for example, WayAway, Hydra, and Rutor) may shed light on the rapid presence of innovative malware on the darknet. A recent paper by Allodi (2018) explored the operation of a prominent Russian darknet market where the trading of the most active attack tools reported by the security industry occurred (Allodi, 2018).

Response to Darknet Marketplaces: Operation Bayonet[11]

Operation Bayonet was an international law enforcement operation conducted in 2017 to seize the administration of AlphaBay. The operation was headed by the United States and involved the cooperation and efforts of law enforcement agencies (LEAs) in Thailand, the Netherlands, Lithuania, Canada, the United Kingdom, and France. The operation also included the European law enforcement agency Europol. This operation was conducted in conjunction with a Dutch police operation to seize control of the second most popular market, Hansa (US DOJ, 2017). AlphaBay and Hansa were under the control of LEAs for several months before they were taken offline (Europol, 2017).

[11] Details of the operation and its alleged founder and administrator are summarised in a forfeiture complaint in the US District Court against Alexandre Cazes (aka "Alph02"), available at https://www.justice.gov/opa/press-release/file/982821/download



Notice

THIS HIDDEN SITE HAS BEEN SEIZED
and controlled since June 20

by the Dutch National Police in conjunction with the Bundeskriminalamt, Lietuvos Policija, Federal Bureau of Investigation and Europol, under the authority of the Dutch National Prosecutor's Office and the Attorney General's office of the Federal State of Hessia (Germany).

The Dutch National Police have located Hansa Market and taken over control of this marketplace since June 20, 2017. We have modified the source code, which allowed us to capture passwords, PGP-encrypted order information, IP-addresses, Bitcoins and other relevant information that may help law enforcement agencies worldwide to identify users of this marketplace. For more information about this operation, please consult our hidden service at politiepcvh42eav.onion.

This seizure was part of **Operation Bayonet**, which includes the takeover of Hansa Market by the National Police of the Netherlands and the takedown of AlphaBay Market by the Federal Bureau of Investigation of the United States of America on July 4, 2017.

THIS HIDDEN SITE HAS BEEN SEIZED
Since July 4, 2017

as a part of a law enforcement operation by the Federal Bureau of Investigation, the Drug Enforcement Administration, and European law enforcement agencies acting through Europol

in accordance with the law of European Union member states and obtained pursuant to a forfeiture order by the United States Attorney's Office for the Eastern District of California and the U.S. Department of Justice's Computer Crime & Intellectual Property Section.

This seizure was part of **Operation Bayonet**, which includes the takeover of Hansa Market by the National Police of the Netherlands on June 20, 2017, and the takedown of AlphaBay Market by the Federal Bureau of Investigation of the United States of America on July 4, 2017.

Figure 32 - Hansa and Alphabay seizure messages (Europol, 2017)

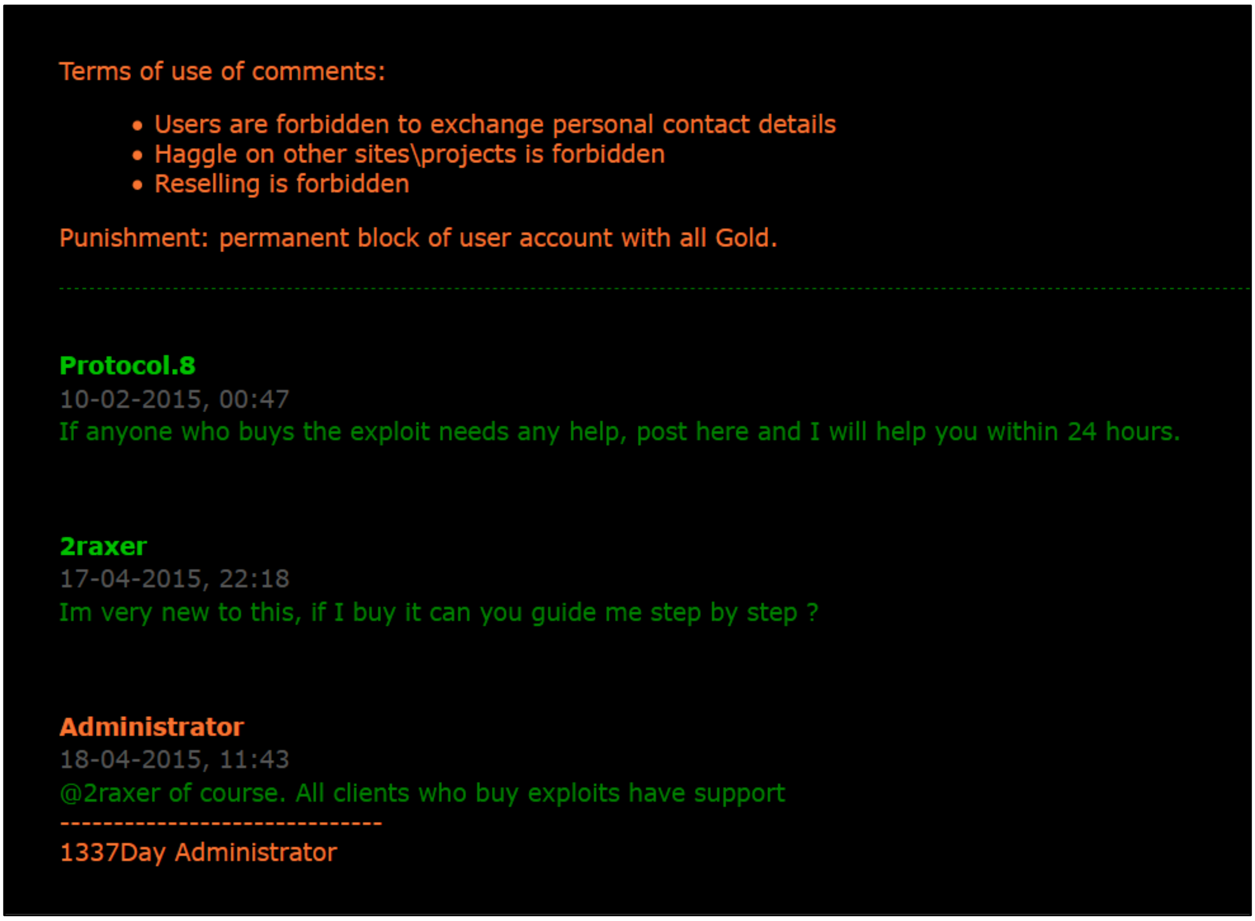
Prior to its takedown, AlphaBay claimed that it serviced over 200 000 users and 40 000 vendors. At the time of its takedown there were over 250 000 listings for illicit chemicals and narcotics. Furthermore, there were also over 100 000 listings for stolen and fraudulent identification documents and access devices, counterfeit goods, malware and other computer hacking tools, firearms and fraudulent services (US DOJ). When AlphaBay was shut by US authorities, Hansa recorded an eight times increase in the number of new users (Greenberg, 2017).

The successful operation created chaos on the darknet with many of Alphabay's clients and vendors displaced to Hansa. Unknown to the users of Hansa*,* the Dutch authorities had already taken over the administration of the market and had been gathering intelligence (including billing details, addresses and messages) on its users, which had been passed on to Europol (Europol, 2017). It is anticipated that many successful prosecutions will follow due to the massive trove of intelligence that the Dutch authorities obtained from the many vendors and user fleeing from AlphaBay to Hansa (Greenberg, 2017).

Marketplaces for Malware: Closed Forums

Closed malware forums are the most elusive markets to observe. Their existence can be partly attributed to the displacement effect of LEA operations in more open markets, including traditional darknet markets. These closed malware forums are where writers of malware can advertise products and buyers can interact with vendors, unlike large darknet marketplaces where 'one-off' transactions are observed (Chon, 2016). These online communities often have strict pre-conditions for registration and operate on referral only basis with significant proof of 'worthiness' for membership. To establish a connection to these forums requires knowledge of relevant onion address which also often change. Furthermore, closed forums also feature many of the safeguards regular marketplaces enact, such as CAPTCHAs, DDoS Protection and PGP Communication (Chon, 2016). Most interactions within these closed forums are publicly viewable to all members, however Private Messages (referred to as "PMs") between members are commonplace. PMs either occur via the forum site or are undertaken via the use of a third-party encrypted messaging systems. Encrypted messaging schemes have also been adopted by darknet marketplaces in the form of PGP (Pretty Good Privacy) Messaging (see above "Security of Marketplaces: PGP"). As privacy and anonymity is paramount to users of these forums, discussions often take place via third-party encrypted messaging systems and are not observable.

Within these forums listings for malware are sporadic, but both prices and performance were usually questioned by potential buyers with discounts offered as way to attract customers (Holt, 2015). When a member posts information about a products availability, other users will often ask about the malware's success rate of infection and exfiltration, as illustrated in Figure 33 overleaf.



Terms of use of comments:

- Users are forbidden to exchange personal contact details
- Haggle on other sites\projects is forbidden
- Reselling is forbidden

Punishment: permanent block of user account with all Gold.

Protocol.8
10-02-2015, 00:47
If anyone who buys the exploit needs any help, post here and I will help you within 24 hours.

2raxer
17-04-2015, 22:18
Im very new to this, if I buy it can you guide me step by step ?

Administrator
18-04-2015, 11:43
@2raxer of course. All clients who buy exploits have support

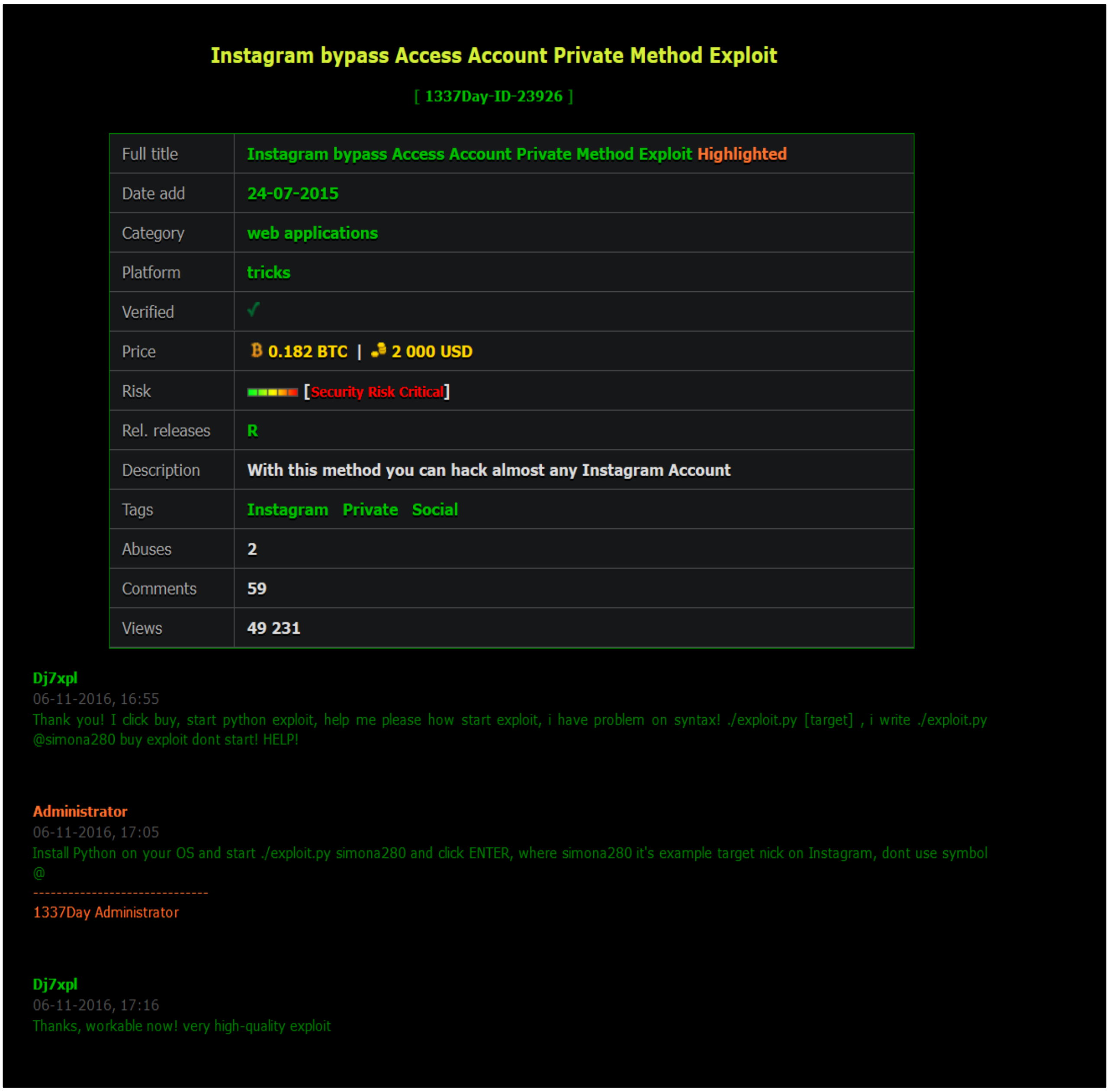
1337Day Administrator

Figure 33 - A junior member of a malware forum asks for guidance (Source: https://0day.today/exploit/description/23252)

Noobs and L33ts

A clearly delineated separation between professionals and non-professionals is observed within online forums, primarily related to experience (Chon, 2016). Vendors operating within online forums are typically identified as L33ts (skilled operators) with buyers as noobs (less experienced, often termed 'script kiddies'). So called 'black' and 'grey' hackers may use the markets and related forums to enhance reputations or monetise new or upgraded products.[12] The transaction of malware between the two entities provides an opportunity for a 'noob' to carry out sophisticated operations and further enhance their skills (See Social Learning Theory and Digital Drift on pages **16 – 17)**. Furthermore, assistance is often sought by buyers to successfully operate malware products, as shown in **Figure 34.**

[12] Black Hat hackers, like Grey and White Hats, possess advanced technological skill and hacking or malware writing expertise that are used to bypass security protocols to gain access to a computer or network (Symantec, n.d). However, Black Hats differ due to the criminality of their actions. They trespass on computers and networks with malicious intent often as a means of earning income (Kaspersky, n.d.). Black Hats can range in skill from the novice script kiddies to advanced hackers who write their own malware (Symantec, n.d.). They can also operate independently as lone wolves or as part of a criminal organisation (Kaspersky, n.d.).



Instagram bypass Access Account Private Method Exploit

[1337Day-ID-23926]

Full title	Instagram bypass Access Account Private Method Exploit Highlighted
Date add	24-07-2015
Category	web applications
Platform	tricks
Verified	✓
Price	฿ 0.182 BTC | 2 000 USD
Risk	[Security Risk Critical]
Rel. releases	R
Description	With this method you can hack almost any Instagram Account
Tags	Instagram Private Social
Abuses	2
Comments	59
Views	49 231

Dj7xpl
06-11-2016, 16:55
Thank you! I click buy, start python exploit, help me please how start exploit, i have problem on syntax! ./exploit.py [target] , i write ./exploit.py @simona280 buy exploit dont start! HELP!

Administrator
06-11-2016, 17:05
Install Python on your OS and start ./exploit.py simona280 and click ENTER, where simona280 it's example target nick on Instagram, dont use symbol @

1337Day Administrator

Dj7xpl
06-11-2016, 17:16
Thanks, workable now! very high-quality exploit

Figure 34 - A buyer asks for assistance (Inj3t0r, 2018)

The activity of vendors providing guidance on the operation of malware products clearly aligns with a deviant learning process (per Chon, 2016, Sutherland 1956[13]). Online forums not only provide a platform where sophisticated malware can be exchanged, but criminal behaviours encouraged and supported. Hence within forums, reputation dynamics play a large factor in trust between members. Reputation being the judgment of trust of an individual's worthiness based on their characteristics and past behaviour.

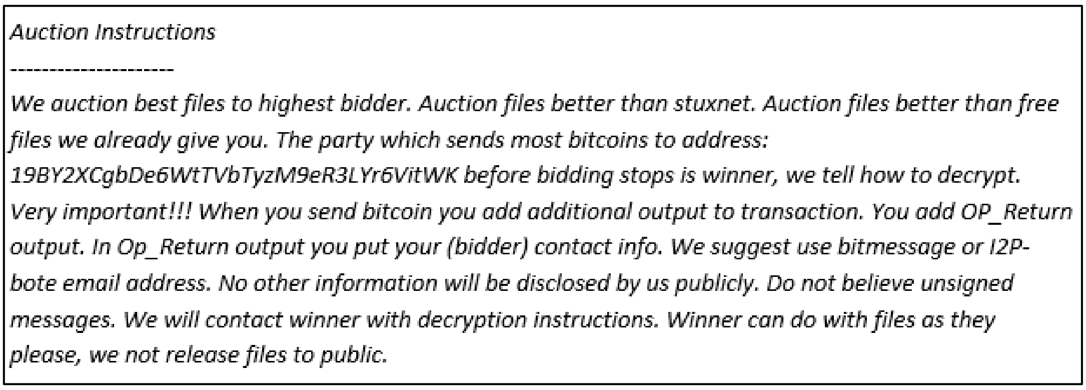
Décary-Hétu and Dupont (2012) attempted to quantify reputation using statistical methods and found that there was a relationship between specific attributes of web forum site members and their perceived reputation. Décary-Hétu and Dupont (2012) found that forum members preferred to deal with members that that had longer histories, a higher number of forum posts and that were more active.

[13] Sutherland studied the provenance of criminal behaviour, suggesting that every criminal was once a beginner before becoming an individual with significant expertise and skill, stating "… an inclination to steal is not a sufficient explanation of the genesis of the professional thief … [they] must be appreciated by professional thieves (Sutherland, 1956, p. 212)".

Reputation not only provides a means of identifying reliable members but can also influence and drive behaviour. Points for reputation could also be earned and gifted between members with the collection of reputation further encouraging participation. Other methods for reputational validation have also been identified within forums. In a study by Holt (2013), a third-party escrow exchange was established for members to verify the legitimacy of products. A standard procedure in many legal online markets (e.g. eBay). The third-party escrow service only releases funds after the product provided by the vendor was confirmed to be genuine. Holt (2013) suggests that online reputation played a role in subsequent interactions with members preferring to engage with members with a greater positive reputation.

The Shadow Brokers Case Example – Auctioning Zero Days

An example of malicious actors attempting to monetise zero day exploits is The Shadow Brokers. In August 2016, The Shadow Brokers announced the auction of hacking tools leaked from the National Security Agency (NSA), including several zero-day exploits. See Figure 35.



Auction Instructions

We auction best files to highest bidder. Auction files better than stuxnet. Auction files better than free files we already give you. The party which sends most bitcoins to address: 19BY2XCgbDe6WtTVbTyzM9eR3LYr6VitWK before bidding stops is winner, we tell how to decrypt. Very important!!! When you send bitcoin you add additional output to transaction. You add OP_Return output. In Op_Return output you put your (bidder) contact info. We suggest use bitmessage or I2P-bote email address. No other information will be disclosed by us publicly. Do not believe unsigned messages. We will contact winner with decryption instructions. Winner can do with files as they please, we not release files to public.

Figure 35 - Auction of NSA Exploit by The Shadow Brokers (Wired, 2016)

The encrypted file "eqgrp-auction-file.tar.xz" containing all items auctioned was a collection of tools primarily for compromising Linux/Unix based environments, including the zero day exploit: EternalBlue. In May 2017, the WannaCry ransomware attack used an EternalBlue attack on Server Message Blocks (SMB) to spread with EternalBlue also used to help carry out the Petya cyberattack in June, 2017.

This open auction by The Shadow Brokers was unprecedented. No doubt the group responsible for WannaCry and Petya identified the potential to use such exploits. The exploits collated by The Shadow Brokers have even been published on the open source code sharing platform GitHub.[14]

Grey Hat Hackers & Markets

Grey markets represent a medium between illicit markets and bug bounty programs where perhaps the most attractive exploits and vulnerabilities reside. Grey Hats typically aim to identify zero-day vulnerabilities for the purpose of selling them to security industry companies, governments, LEA's, intelligence agencies or militaries (Zetter, 2016). These hackers are not malicious but may 'drift' and use the exploits they have found. However, their actions are illegal because they often do not receive permission from the owners of the targeted product prior to conducting their "test" attacks (Symantec, n.d.). Grey Hats can operate independently or they can be part of defence contractors, or boutique firms that specialise in the brokerage of zero-days such as Vupen and Zerodium (Zetter, 2016).[15]

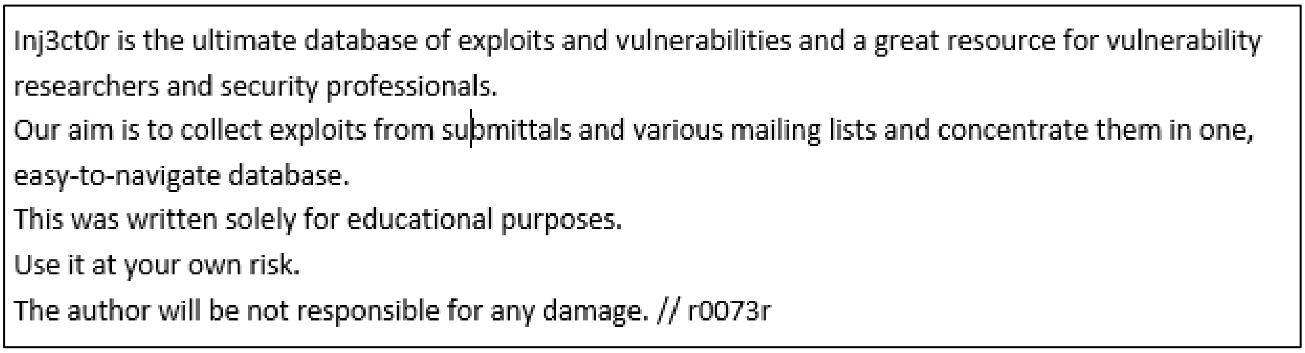
[14] https://github.com/ElevenPaths/Eternalblue-Doublepulsar-Metasploit

[15] See Appendix 3 for Zerodium bug bounty details

0day.today Marketplace

An example of a long standing and actively updated 'grey market' for exploits and vulnerabilities is 0day.today, run by The Inj3ctor Team. Formed in 2003, The Inj3ctor Team has self-identified as a hacktivist group with multinational ties to Chinese hackers as well as Russia, Turkey and other countries. 0day.today provides a platform where exploits and vulnerabilities are collected via submittals and various mailing lists and collated in a searchable database. The site features a prominent disclaimer about any improper use of exploits disseminated via the site, as shown in Figure 36.

Since December 2008 the group has managed 0day.today with payment methods evolving from traditional digital money transfer (e.g. Liberty Reserve, WebMoney) to cryptocurrencies such as Bitcoin, LiteCoin and others. By 10 October 2016, the Bitcoin address associated with 0day.today had exceeded 800 BTC, roughly US$6 million as of 18 March 2018 (ElevenPaths, 2016).



Inj3ct0r is the ultimate database of exploits and vulnerabilities and a great resource for vulnerability researchers and security professionals.
Our aim is to collect exploits from submittals and various mailing lists and concentrate them in one, easy-to-navigate database.
This was written solely for educational purposes.
Use it at your own risk.
The author will be not responsible for any damage. // r0073r

Figure 36- 0day.today Disclaimer (Inj3ct0r, 2018a)

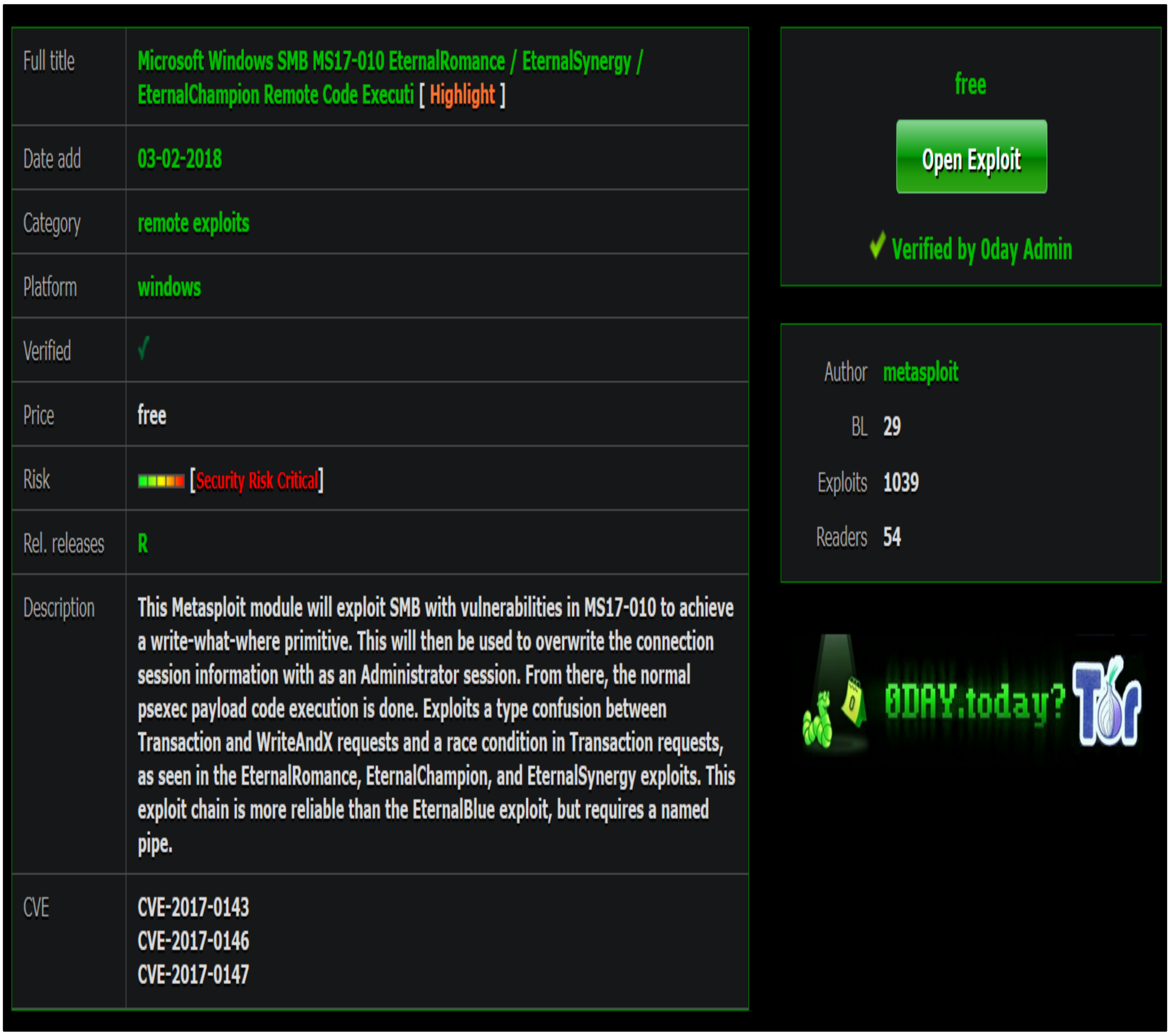
Free Exploits

Many of the exploits featured within 0day.today are free due to the collated natured of exploits listed from various data feeds. For example, exploits reported by Offensive Security (a cybersecurity research company) are found within 0day.today, as shown in Figure 37 (next page).

Paid-For Listings

The two paid-for exploit categories within 0day.today are the "private" and "0-day restricted" sections of the site. Table 4 provides an excerpt of exploits listed within this "private" category which represent a higher level of sophistication than free exploits and thus demand a higher price.

Collation of private listings from 0day.today was completed via simple data collection on 26 February 2018 that identified 37 exploits. These were analysed and a weak to moderate positive correlation between the price and publication date of exploit was found (Pearson's R value is R^2=0.225). This weak to moderate positive relationship indicates that as exploits age, their value decreases. In a recent paper, Allodi (2018) found similar findings where baseline prices for exploits varied widely by software vendor, but exploits lost value as they aged.



Full title	Microsoft Windows SMB MS17-010 EternalRomance / EternalSynergy / EternalChampion Remote Code Executi [Highlight]
Date add	03-02-2018
Category	remote exploits
Platform	windows
Verified	✓
Price	free
Risk	[Security Risk Critical]
Rel. releases	R
Description	This Metasploit module will exploit SMB with vulnerabilities in MS17-010 to achieve a write-what-where primitive. This will then be used to overwrite the connection session information with as an Administrator session. From there, the normal psexec payload code execution is done. Exploits a type confusion between Transaction and WriteAndX requests and a race condition in Transaction requests, as seen in the EternalRomance, EternalChampion, and EternalSynergy exploits. This exploit chain is more reliable than the EternalBlue exploit, but requires a named pipe.
CVE	CVE-2017-0143 CVE-2017-0146 CVE-2017-0147

free

Open Exploit

✓ Verified by 0day Admin

Author	metasploit
BL	29
Exploits	1039
Readers	54

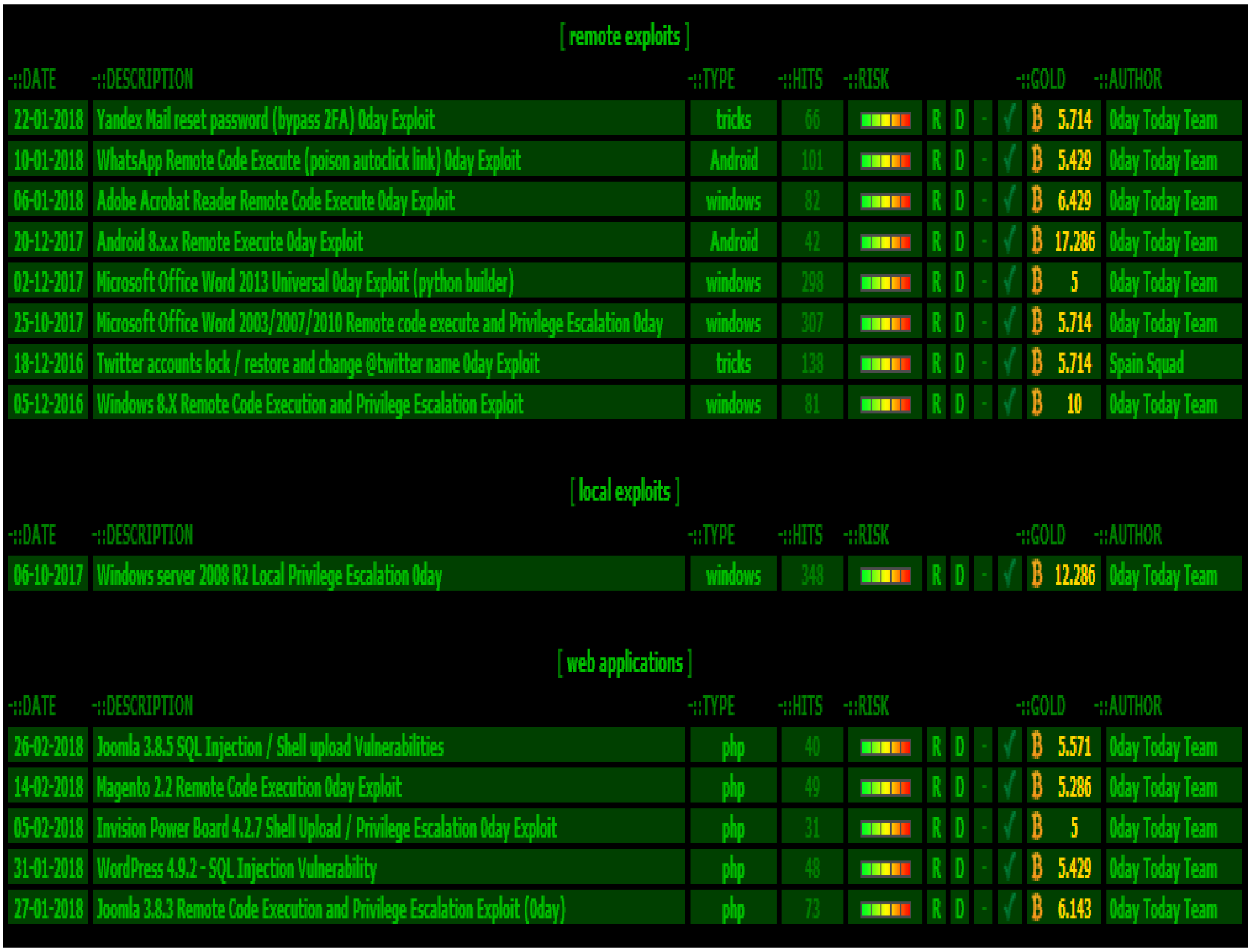
Figure 37 - 0day.today Listing fir MS17-010 Exploit (a.k.a. ExternalBlue) (Inj3ct0r, 2018b)

Table 4 – Data Collected from 0day.today on 26/2/2018 (ANU Cybercrime Observatory)

Date	Description	Price USD	Author
18/10/2017	Microsoft Office Word 2003+2007+2010 Universal 0day Exploit	3800	0day Today Team
24/10/2017	INTERMEDIA CONSEIL - Remote Code Execution Exploit	150	mr.oz1337
15/11/2017	Apple iOS 11.1.1 kernel DoS Exploit	5000	muxbear
11/12/2017	iCloud reset mail Account Authentication Elevation Of Privilege 0day Exploit	4500	0day Today Team
22/01/2018	Instagram info disclosure (email + phone) 0day Exploit	1400	HXO1
4/02/2018	Coinhive – Monero JavaScript Mining Information Disclosure (SecretKey) Vulnerability	1200	ogcrypto

'Restricted zero-day' Listings Analysis

Further featured within this 'grey market' (0day.today) is a "Restricted zero-day" section, requiring significant commitment to the site to access – either monetary (1,000 'Gold' – US$1,000 commitment) or previous exploit sales. Figure 38 is a screenshot of a typical list of remote and web exploits. Within this section true zero day exploits are advertised, attracting a hefty price tag. In an attempt to maintain zero-day status these exploits are also removed from advertisement once bought.



[remote exploits]

-::DATE	-::DESCRIPTION	-::TYPE	-::HITS	-::RISK					-::GOLD	-::AUTHOR
22-01-2018	Yandex Mail reset password (bypass 2FA) 0day Exploit	tricks	66	🟩🟩🟨🟧🟥	R	D	-	√	₿ 5.714	0day Today Team
10-01-2018	WhatsApp Remote Code Execute (poison autoclick link) 0day Exploit	Android	101	🟩🟩🟨🟧🟥	R	D	-	√	₿ 5.429	0day Today Team
06-01-2018	Adobe Acrobat Reader Remote Code Execute 0day Exploit	windows	82	🟩🟩🟨🟧🟥	R	D	-	√	₿ 6.429	0day Today Team
20-12-2017	Android 8.x.x Remote Execute 0day Exploit	Android	42	🟩🟩🟨🟧🟥	R	D	-	√	₿ 17.286	0day Today Team
02-12-2017	Microsoft Office Word 2013 Universal 0day Exploit (python builder)	windows	298	🟩🟩🟨🟧🟥	R	D	-	√	₿ 5	0day Today Team
25-10-2017	Microsoft Office Word 2003/2007/2010 Remote code execute and Privilege Escalation 0day	windows	307	🟩🟩🟨🟧🟥	R	D	-	√	₿ 5.714	0day Today Team
18-12-2016	Twitter accounts lock / restore and change @twitter name 0day Exploit	tricks	138	🟩🟩🟨🟧🟥	R	D	-	√	₿ 5.714	Spain Squad
05-12-2016	Windows 8.X Remote Code Execution and Privilege Escalation Exploit	windows	81	🟩🟩🟨🟧🟥	R	D	-	√	₿ 10	0day Today Team

[local exploits]

-::DATE	-::DESCRIPTION	-::TYPE	-::HITS	-::RISK					-::GOLD	-::AUTHOR
06-10-2017	Windows server 2008 R2 Local Privilege Escalation 0day	windows	348	🟩🟩🟨🟧🟥	R	D	-	√	₿ 12.286	0day Today Team

[web applications]

-::DATE	-::DESCRIPTION	-::TYPE	-::HITS	-::RISK					-::GOLD	-::AUTHOR
26-02-2018	Joomla 3.8.5 SQL Injection / Shell upload Vulnerabilities	php	40	🟩🟩🟨🟧🟥	R	D	-	√	₿ 5.571	0day Today Team
14-02-2018	Magento 2.2 Remote Code Execution 0day Exploit	php	49	🟩🟩🟨🟧🟥	R	D	-	√	₿ 5.286	0day Today Team
05-02-2018	Invision Power Board 4.2.7 Shell Upload / Privilege Escalation 0day Exploit	php	31	🟩🟩🟨🟧🟥	R	D	-	√	₿ 5	0day Today Team
31-01-2018	WordPress 4.9.2 - SQL Injection Vulnerability	php	48	🟩🟩🟨🟧🟥	R	D	-	√	₿ 5.429	0day Today Team
27-01-2018	Joomla 3.8.3 Remote Code Execution and Privilege Escalation Exploit (0day)	php	73	🟩🟩🟨🟧🟥	R	D	-	√	₿ 6.143	0day Today Team

Figure 38 - Screenshot of 0day.today's 'Restricted zero-day' Section on March 30, 2018

Hackers and Bug Bounties

'White hat' hackers, unlike their 'black' and 'grey' counterparts, are highly skilled and use their hacking expertise to improve security legally. They are also referred to as 'ethical hackers' and are generally employed by companies to find security flaws and holes through their hacking, and supervise or support bug bounty program (Symantec, n.d). 'White hats' are supposed to be the Internet's 'good guys' (Zetter, 2016). The proliferation of bug bounty programs and online marketplaces, both open and deepweb, delineates money as the primary motivating factor for the transaction of malware and exploits. Once acquired, these tools have the ability to be adapted and employed by a third-party to devastating effect, evidenced by WannaCry and Petya.

Companies 'Waking Up' to Bug Bounties

BugCrowd tracks bug bounty programs offered by companies and also lists incentives for the disclosure of exploits. Of the 427 companies listed by BugCrowd (as of March 2018), only 195 (46%) offer a reward in the form of money or 'swag' – slang for company merchandise. Furthermore, Bugcrowd (2017) found an increase of 77% in the availability of new bug bounty programs compared to 2016 (Bugcrowd, 2017). This indicates that many companies are becoming attuned to the issue of cybersecurity. However, reports of researchers receiving no reward, and in some cases legal action, for revealing a dangerous exploit undermines positive relationship with hackers.

In 2002, Hewlett-Packard threatened SnoSoft (a vulnerability research company) with legal action after one of its members, pseudonym 'Phased', posted an exploit for a serious and unpatched exploit within Hewlett-Packard's Tru64 operating system. SnoSoft received a letter from Hewlett-Packard warning that Snosoft "could be fined up to US$500,000" and its principals imprisoned for up to five years over its actions (The Registar, 2002). More recently in 2017, a vulnerability researcher was left with no reward after disclosing multiple vulnerabilities to ride sharing company, Uber, through a partnered bug bounty program with HackerOne. Uber had advertised a US$500 minimum guaranteed pay out for security vulnerabilities within the Uber app or information asset. The researcher, Gregory Perry, disclosed several vulnerabilities within Uber's architecture and recorded all correspondence with Uber and HackerOne to retrieve the minimum pay out. Perry took to an online blog to describe his correspondence with Uber and HackerOne. In this blog, Perry comes to a conclusion that "HackerOne does not honour their minimum bug bounty guarantee, and will not 'go to bat' for you if you have a dispute with one of their well-placed vendors such as Uber" (Perry, 2017).

An Ethical Question for Vulnerability Researchers

Selling a vulnerability can pose ethical questions and difficulty from the perspective of a researcher for guaranteed pay out. Certainly Perry (2017) and other malware researchers must ask themselves the question "why not just legitimately sell the exploit on any one of a number of commercial exploit brokerage auction services?" They could readily rationalise any of their actions, whether to sell the exploit legally or illegally, by employing any of the Techniques of Neutralisation (see page 16).

The duality that vulnerabilities represent ensures that bug bounty researchers must give away valuable information without knowing a guaranteed monetary reward, certainly "the same information that allows more widespread exploitation of vulnerabilities is required to correct those vulnerabilities" (Stisa Granick, 2017). On top of this, during the process of disclosure another entity could announce the vulnerability, and make the discovery worthless (Miller, 2007).

Bug Bounty and Cryptocurrency Convergence

A recent innovation in bug bounty marketplaces is Bounty0x, a blockchain based bug bounty platform where users can manage bounty programs, and bounty hunters can receive payment for completing bounty tasks (Bounty0x, 2018). Other adoptions include Hacken, advertised as the first custom-tailored decentralised token for cybersecurity professionals. With Hacken, customers are able to acquire penetration testing services and vulnerability assessments. Findings are time stamped and published to the blockchain-based HackenProof Vulnerabilities and Countermeasures Certificate, uniquely issued for each project (Hacken, 2018).

Report by HackerOne and Stack Overflow Survey

A report published by HackerOne (2018), a clearing house for vulnerabilities and a bug bounty platform for business and cybersecurity researchers, found that nearly 25% of hackers have not reported a vulnerability due to the company offering insufficient channels to disclose. Therefore, this may discourage those who to seek payment for their work on a bug bounty program, and encourage illicit trade or private transactions (The 2018 Hacker Report, 2018).

As we noted above in our discussion of criminological theory, motives vary, although financial gain and 'easy' money apply to the operation of criminal enterprise. HackerOne (2018) also found that money remains a top driver for discovering vulnerabilities. With pay outs of up to US$1.5 million it is not surprising that hacking has become a significant source of income for some hackers. HackerOne (2018) found that a quarter of hackers rely on bounties for at least 50% of their annual income. However, they also found that hackers are, above all, motivated by the opportunity to learn tips and techniques. Nearly 58% of the hacker survey respondents reported to be self-taught with less than 5% having learnt hacking skills in a classroom environment. With countless open source platforms offering opportunities to learn skills, there is no shortage of learning material.

In another survey conducted by Stack Overflow (2018) assessing software developers' approaches to security, respondents reported a range of 'ethical grey' practices while producing code. Respondents were also unsure how they would report ethical problems with varied perspectives about who is ultimately responsible for unethical code. However, Stack Overflow (2018) discovered very few developers reported they would write unethical code or thought that they have any obligation to consider the ethical implications of a using vulnerable or deceptive programs and code.

Discussion

The profitability of a harmful exploit offer could be a determining factor in the likelihood of malicious adaptation. Hackers across the white – black spectrum would seek to monetise their reward for identifying an exploit, especially in cases where significant time and effort has been invested by the hacker to uncover the exploit such as a zero-day. Large bug bounties and the opportunity to sell exploits anonymously via cryptocurrencies have led to significant investment by 'good' and 'bad' hackers alike, akin to a 'gold rush' in the identification and misuse of these 'tools' of cybercrime.

The low risk that selling malware presents, as opposed to the transaction of a physical product, coupled with an anonymous payment system (cryptocurrencies), means markets for malware are here to stay. Verizon's 2016 Data Breach Investigations Report found that 89% of breaches had a financial or espionage motive (Verizon, 2016). Allodi (2018) also found that exploits that are more expensive to acquire have lower odds of exploitation than 'cheaper' exploits. However, the generalisation that the transaction of malware within markets is driven simply by financial gain may be overly simplistic. Certainly, the idea of the 'Hacker's Ego' has deep foundations and persists in the form of an elaborate game of 'one-upmanship' within hacker communities (Holt, 2018).

'White' vs. 'Black' Profitability

The ease with which malicious actors can obtain dangerous malware and the number of vulnerable targets facilitates the establishment of a reliable revenue stream. So that "there is a greater economic incentive to attack than to defend and we have a perfect storm: a growing and under-defended attack surface and adversaries economically incentivised to attack it" (BugCrowd, 2017).

When directly comparing the profitability of either disclosing a harmful vulnerability to a bug bounty program with a sale on the darknet, hackers may elect to sell their discovery to the highest bidder. A RAND (2014) study found that "value can come from a vulnerability's uniqueness (e.g., if it is the only vulnerability found in a specific product) or the need and timeline of the customer" (RAND, 2014). Therefore, a hacker may elect to 'shop around' for the best deal when attempting to sell vulnerability information via gauging interest from the spectrum of ‘white’ to ‘black’ marketplaces. A complication for the sale of vulnerability information is that market values are unstable and fluctuate (Miller, 2007; RAND, 2014).

Chapter 4: Cryptocurrencies and Regulation

Cybercrime, Cryptocurrencies and the Internet

Within the cybercrime literature, and cybersecurity field more broadly, there is a tendency to conflate already ambiguously defined words such as 'cyber' and 'terrorism' or 'cyber' and 'crime.' Michael Stohl and Peter Grabosky (2003, p. 8) suggest that this tendency toward amalgamation "is hardly a guarantor of conceptual rigor" and only contributes to further confusion regarding cyberspace and the emerging real world trends within that domain. Further, the rate at which cybercrime techniques and the extent of 'cyberspace' are evolving increases the complexity of the phenomenon. In this section, we adopt current basic definitions of virtual currencies and the darknet.

Virtual methods of payment emerged in the 1950s following the introduction of the first credit cards and their comparatively primitive bank to bank transfer methods (Wolters, 2000). Since then, a range of payment methods using cyberspace have been developed, such as PayPal and prepaid debit cards. More recently, wholly virtual monetary mediums that use computer code to enable a decentralised transaction were created, the most commonly known of which is Bitcoin (for a more expansive list on Altcoins, see pages 48 – 49).

Electronic money

As there are a range of electronic financial systems and payment methods, it is necessary to distinguish between electronic money, virtual currencies and cryptocurrencies. Gina Pieters (2017, p. 20) in distinguishing between these methods contends that, "electronic money is a broad term for any money, currency, or asset not held in physical form" that "digitally represents many sovereign currencies, such as the US dollar." Thus, the original online payment types, including credit cards and PayPal, utilise standard sovereign currencies to make purchases and are directly transferable to physical cash.

Virtual currencies

Virtual currencies are a subset of electronic money, representing a payment method that is distinct from electronic money because it has no tangible, real-world, counterpart except for the physical goods one can purchase using the payment system (He *et al.*, 2016). Examples of this type of virtual payment are Internet or mobile coupons that allow the holder to make purchases for goods, but they cannot be exchanged for physical cash.

Cryptocurrencies

Cryptocurrencies, such as Bitcoin, are a further subset of virtual currencies. Such currencies occur where transactions through encryption that conceals the identity of the payer and the payee resulting in a higher degree of anonymity than is found in the 'open' or 'clear' web (Holt, et. al. 2017). Though Bitcoin is currently the most commonly recognised, other types of cryptocurrencies are gaining increasing traction and popularity due to advances in encryption technology. Monero, for example, is not a derivative of Bitcoin and instead uses a completely different algorithm to decentralise transactions. It uses the CryptoNight proof-of-work hash algorithm that enables each unit of the currency to be substituted by another unit (Monero, 2015). This avoids issues of blacklisting and currency refusal after a Bitcoin unit is associated with undesired activity (Monero, 2015). It therefore helps to obfuscate associated illicit activities and therefore avoid detection by LEA's.

It is the latter form of digital payment that has been most amenable to criminal activities in cyberspace. In the past governments around the world have been largely unsuccessful in preventing cryptocurrencies from becoming a recognised payment system (Greenberg, 2014). Currently there appears to be no universal agreement on whether cryptocurrencies can be a legitimate form of payment. In fact, significant debate remains over whether the online mediums of exchange, are just that (mediums of exchange), or whether they constitute a hybrid currency (somewhere between a payment system and commodity), or perhaps something of even lesser worth: “a quirky little project hallucinated by a cryptic computer programmer who was disillusioned with the post-financial-crisis world” going by the name of Satoshi Nakamoto (Kelly, 2015, p. 2). Most agree with the former assessments, believing that cryptocurrencies do have real value. An assessment that is supported by Bitcoin’s emergence on the Stock Exchange, and its growing status as a digital asset (Eha, 2017), albeit a volatile commodity or exchange.

Cryptocurrencies are very useful as a means of transaction between criminal entities. This is due primarily to the strength of the economic system itself created by anonymity and durability against attack; and the speed by which it operates—all but erasing the need for an intermediate party. Cryptocurrencies require no personal information in their acquisition and use, which ensures that identities of parties involved can remain encrypted throughout the entirety of any transaction or exchange (Lee, Long, Marcellus, Steiner & Handler, 2015). The database upon which cryptocurrencies rely also ensures the durability of the payment system as it is distributed across a potentially infinite array of computers. As such, if a hacker managed to compromise a computer containing the database, the organisation is largely immune to absolute failure or collapse from a cyberattack (Kelly, 2015; Long et. al, 2015; Bitcoin, n.d).

Moreover, given that cryptocurrencies by nature are ‘peer-to-peer’, the intermediate party is not required in the same sense a bank is needed for physical payments. Instead, the payment between buyer and seller is direct and immediate since they need not be verified, cleared or delivered (Kelly, 2015; Lee et. al, 2015; Tu & Meredith, 2015). The peer-to-peer nature is ensured through ‘blockchain technology’, which in its simplest form is “a chronological database of transactions recorded by a network of computers” whereby “each block contains information about a certain number of transactions, a reference to the preceding block in the block chain” (see Figure 36 next page) (Wright & De Filippi, 2015, p. 6). As a copy of the blockchain is then stored on each computer it is located on, and acts as a decentralised network that does not rely on a single entity to clear or verify transactions.

This system is in a sense a self-insurance system. Bitcoin miners are used to maintain the blockchain process by solving an algorithm that indicates the individual block is associated with those before it, a process known as proof-of-work. Once a miner solves the algorithm they are rewarded with Bitcoins, thereby continuing the process and preserving the integrity and strength of the blockchain. By incentivising the legitimisation (or verification) process through rewarding the miners with Bitcoins, the distribution (and the benefits of this process) are perpetuated, as well as the functioning or running, of the network itself. However, cryptocurrencies, and Bitcoin more specifically, are highly volatile currencies relative to fiat currencies.

Bitcoin is, at present, the most successful cryptocurrency (Katsiampa, 2017). However, Bitcoins are highly volatile and experience substantial fluctuations in value (Glaser, Zimmerman, Haferhorn, Weber & Siering, 2014). Bitcoin is therefore primarily used as an asset in licit domains, rather than a currency (despite its frequent mention as such) (Baek & Elbeck, 2015). However, on darknet markets Bitcoins are used as an effective facilitator of transactions (Kethineni, Cao & Dodge, 2017).

As described by Bitcoin (n.d), the cryptocurrency's "myriad potential, purposes and applications are yet to be decided." The ambiguity surrounding definitions and payment methods and their impact is a result of the nature of this emerging technology. The absence of a settled regulatory approach and indecision among governments about how to effectively prevent misuse of cryptocurrencies, suggest that its facilitation of criminal activities will continue and grow.

In the next section, we briefly discuss the emergence of numerous competitors to Bitcoin as improvements in blockchain technology advances. The imposition of regulatory constraints designed to minimise criminal misuse and/or tax the perceived asset qualities cryptocurrencies.

Alternative Cryptocurrencies

Alternatives to Bitcoin (termed 'Alt-Coins') have 'bandwagoned' on the pioneering success the virtual currency has achieved. Alt-Coins such as Monero and Bitcoin Cash have been identified as additional trading commodities within darknet marketplaces. Figure 39 indicates the rise of Alt-Coins in the development of cryptocurrency and their impact on Bitcoins declining dominance.

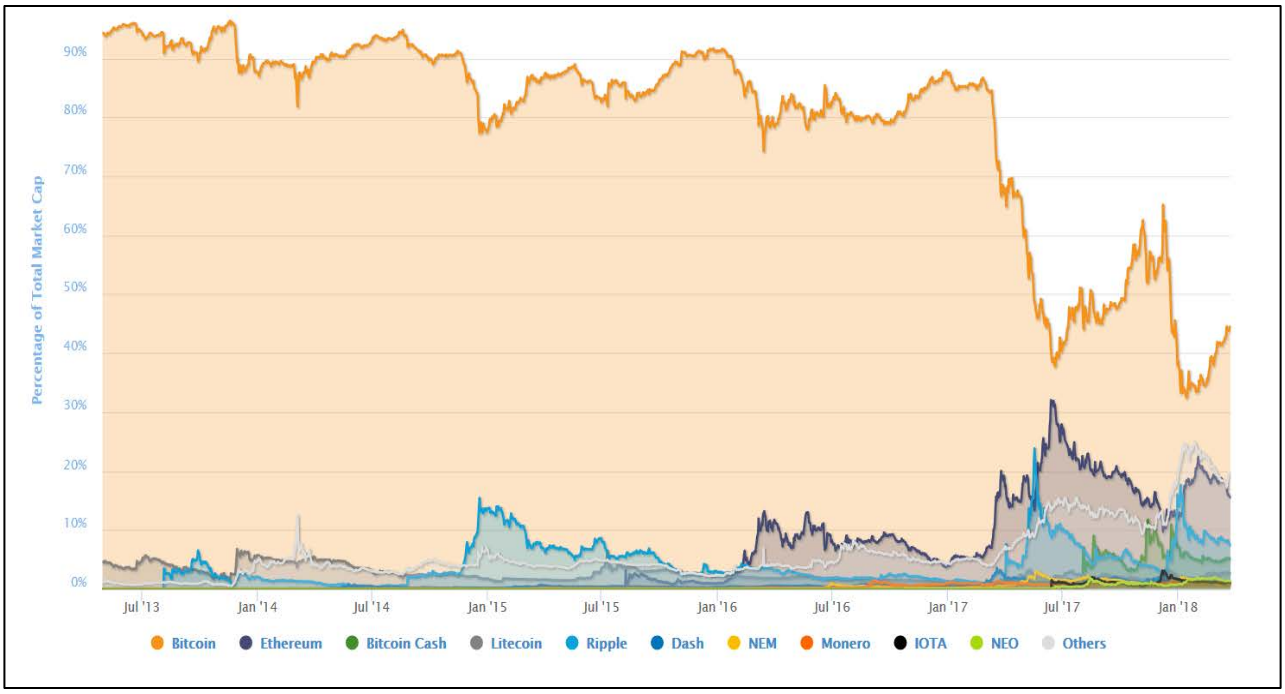


Figure 39 - Percentage of Total Market Capitalisation (Dominance), 2013 to Present (CoinMarketCap, 2018)

Cryptocurrency: Criminal Cases and Legislative Regulation

Cryptocurrency facilitates online criminal activity. While it is far from the technology's sole use, criminal activity and cryptocurrency are closely related. Consequently, there have been numerous arrests related to the use of cryptocurrency, and activities associated with it. However, because most jurisdictions apply different rules about the use and implementation of this technology, it is difficult to establish a global response or 'direction' for the uniform regulation of cryptocurrencies.

Arrests involving the prosecution of an individual for cryptocurrency use are generally limited to a small number of countries, most of which share the characteristic of having outright banned the use of the technology. Elsewhere, it is more common for individuals to be prosecuted based upon what they use cryptocurrency to buy (drugs, weapons, services, etc.), not for simply using the technology. For obvious reasons, these two 'branches' under which an individual can be prosecuted should remain separate; in the latter, cryptocurrency is largely irrelevant as a result of the accused is being charged with what they *bought* or *sold* – they arguably would have been accused of the same crime regardless of the currency which was used.

As of February 2018, there are no data on the number of reported criminal proceedings which involve the illegal use of cryptocurrency. There are two reasons for why this could be happening: 1) courts are not publicly releasing the details of proceedings; or 2) cases are being settled outside of court, and are thus never published. However, despite the lack of case law, the arrests of individuals associated with cryptocurrency are frequently reported in the media. One of the largest arrests occurred in May 2017, when it was reported that Bolivian authorities had arrested 60 people for "distributing Bitcoin-related pamphlets" and carrying out "training activities" related to cryptocurrency (Memoria, 2017). Likewise, in February 2018, Tokyo police arrested four Vietnamese individuals for illegally selling an account they opened on a cryptocurrency exchange – the account was allegedly used to receive criminal funds, and to launder money (The Japan Times, 2018). Many similar arrests have occurred in recent months, typically as a result of the theft of cryptocurrency, or the illegal use of it for laundering or receiving criminal profits. However, as stated above, arrests and criminal cases resulting from the mere use of cryptocurrency occur far less frequently.

Cryptocurrency: Bitcoin and the Altcoins

Bitcoin (BTC)

Figure 40 - The Bitcoin Logo (Coinbase, n.d.)

Bitcoin, is the world's first cryptocurrency and decentralised digital currency. Bitcoin was released as open-source software on 3 January 2009 by an unknown author under the pseudonym of Satoshi Nakamoto. It is traded through a peer-to-peer network, between users directly, and therefore does not require an intermediary. It is stored in a 'Bitcoin wallet' that has both a public and private key that act as a bank account and password for transactions. The transactions are verified through the use of nodes and are recorded in a publicly available shared ledger system called a blockchain. To acquire Bitcoins, you either need to purchase them at an exchange with real-world currency or through the energy intensive process of 'mining' the blockchain (Miller, 2017). The maximum supply (the highest amount that can be in circulation) of Bitcoins is 21 million units, which is expected to be hit by mid-2020 (Ron & Shamir, 2013). The highest recorded price of Bitcoin was US$19,783.21 on the December 15, 2017 (Higgins, 2017).

Altcoins

The popularity of Bitcoin has led to over 1,300 spinoff variants known as 'Altcoins'[16] (CryptoNews, 2017). Many of these coins are likely scams or 'pump-and-dump' schemes as they are very simple and offer very limited information about their developers (CryptoNews, 2017). With so many variants of Bitcoin in circulation,[17] below are a selection of Altcoins that have been proven to be legitimate and popular.

[16] Altcoin is the compound of the words 'Alternative' and 'Coin'.

[17] There was a 'boom' of new alt-coins in late 2017 when Bitcoin's value surged.

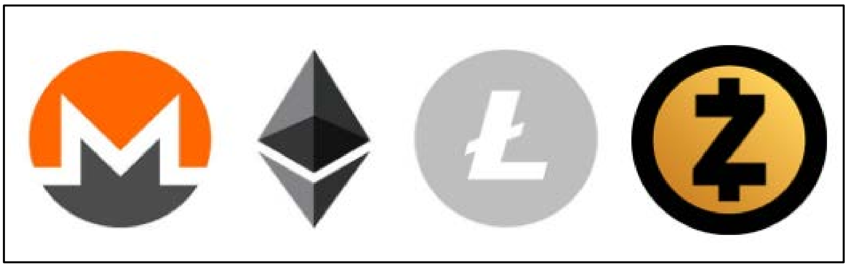


Figure 41 - Altcoin logos (Coinbase, n.d.). From left to right, Monero, Ethereum, Litecoin and Zcash

Litecoin (LTC) – Litecoin is often referred to as the 'silver to Bitcoin's gold' (Bajpai, 2017). It was launched on the 7 October 2011 by Charlie Lee, a former Google employee. It uses similar technology and is nearly identical to Bitcoin and other Altcoins. It differs from Bitcoin because it has a near zero payment cost and transactions are processed approximately four times faster than Bitcoin. Litecoin also differs from Bitcoin through its use of 'scrypt' as its proof-of-work algorithm (Bajpai, 2017). Litecoin has a maximum supply of 84 million units. At publication, the highest recorded price of Litecoin was US$375.26 (Coindesk, n.d. a).

Zcash (ZEC) – Zcash is an Altcoin produced by the Zerocoin project designed to improve the anonymity of Bitcoin users. It was launched on the 28th of October, 2016 by Zooko Wilcox-O'Hearn. It has several similarities to Bitcoin, including the payments being published on a shared ledger system. However, unlike Bitcoin, users have the option to use the privacy feature to conceal the sender, recipient and transaction. It is a selective disclosure process that allows a user to prove payment for auditing purposes. Zcash has a maximum supply of 21 million units. At publication, the highest recorded price of Zcash was US$876.31 on January 8, 2018 (Coindesk, n.d. b).

Monero (XMR) – Monero, launched on the 18 April 2014, is a cryptocurrency that has recently become the favoured currency of dark markets (such as the now closed Alphabay) and criminal organisations (including the Shadow Brokers). This is largely due to its focus on privacy, decentralisation and scalability. Unlike Bitcoin, it operates through the use of 'ring signatures' that mix the spender's address with a group of others which make it far more difficult to establish transaction links and ledgers. The currency also hides the transaction amount and destination. Monero has a maximum supply of 18.3 million units. At publication, the highest recorded price of Monero was US$494.16 on 7 January 2018 (Coindesk, n.d. c).

Ethereum (ETH) – Ethereum was launched on the 30 July 2015. It uses similar technology to Bitcoin's blockchain and wallet functions but has modulised them to suit a variety of client applications beyond money. The monetary unit is a token known as Ether, which can be traded similarly to all other cryptocurrencies. Ethereum users are able to create programs of similar functionality and power to a '1999 smartphone'. The support extends to "new rules of ownership, alternative transaction formats or different was to transfer state" (Hertig, n.d.). At publication, the highest recorded price of Ethereum was US$1,389.18 on 15 January 2018 (Coindesk, n.d. d).

Cryptocurrency Legislation

When assessing the legal status of cryptocurrency throughout the world, there are two primary questions to consider with regard to any given country. Is the purchase, use and sale of cryptocurrency specifically prohibited? In a vast majority of countries, the general use of cryptocurrency for *legitimate* purposes is either expressly or implicitly legal. Second: is the purchase of cryptocurrency, and the exchanges from which they are bought, regulated by the country's Government or Central Bank? Most countries, in one way or another, regulate cryptocurrency. However, whether or not a country regulates cryptocurrency is not directly related to its likely legal status – cryptocurrency can be expressly legal in a country whilst also being heavily regulated.

Figure 40 shows the legality of cryptocurrency throughout the world. Countries are divided into one of four categories depending on the stance of their government or legislature towards digital currencies. ‘Legal’ means that either legislation has been passed, or official government documentation has been released, which indicate that the use of cryptocurrency is legal. ‘Fluctuating/Subject to change’ refers to a country which has either released conflicting documentation about the legality of digital currencies, or has made an official statement which indicates policy will be changed in the near future. ‘Illegal’ refers to a country which has expressly outlawed the use of cryptocurrency in either legislation, or in an official statement. Where there is no documentation on the legality of cryptocurrency, or its status is completely uncertain, a country is categorised as ‘No Official Documentation or Legislation’.

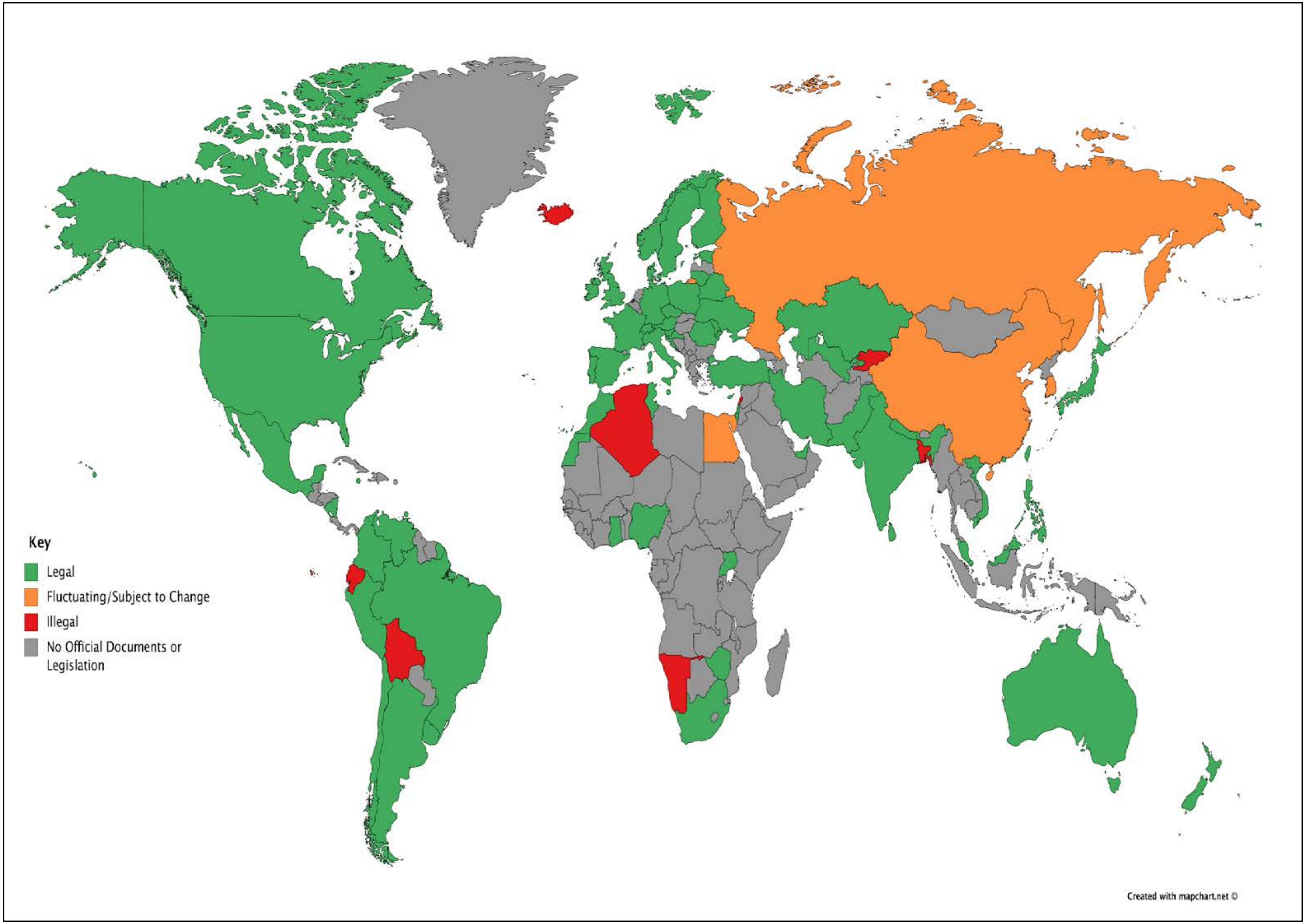

Key
🟩 Legal
🟧 Fluctuating/Subject to Change
🟥 Illegal
⬜ No Official Documents or Legislation
Created with mapchart.net ©

Figure 42 - Legality of Cryptocurrency in different state jurisdictions (May 2018)

North America

The North American response to the recent surge in cryptocurrency has been mostly uniform. All North American countries have either expressly stated the legality of cryptocurrency trading within them (such as the USA, Canada and Mexico), or lack any official statement or legislation to outlaw cryptocurrency, leaving its trade implicitly legal. There is currently no country in North America which considers the trade or distribution of cryptocurrency as illegal. All major countries regulate cryptocurrency in some way.

United States

Due to the lack of legislation, the use of cryptocurrency in the US is considered legal. However, the way in which cryptocurrency is regulated in the US serves to somewhat convolute the straightforward nature of its legal status. At a federal level, the Internal Revenue Service (IRS) considers cryptocurrency as 'property', not currency, and is legally entitled to tax profits made from investment in Bitcoin or other cryptocurrencies. In November 2017, a US court ruled that Coinbase, one of the largest cryptocurrency exchanges in the world, had to turn over 14,000 accounts for analysis by the IRS, where individuals could be taxed anywhere from 0% through to 39.6% depending upon the length of time that the cryptocurrency had been owned, and the overall income of the individual (O'Brien, 2017). Interestingly, some US states are attempting to legislate in a seemingly opposite direction. On 8 January 2018, a state legislator in Vermont proposed a bill which would allow certain firms to be classified as a 'digital currency limited liability company', which would, amongst other things, be required to pay US$0.01 in taxes per unit of digital currency it creates, trades or transfers, and would be exempt from other usually applicable taxes (Higgins, 2018). The bill has yet to be enacted, but it does represent an interesting shift in attitude towards the usefulness of cryptocurrency in certain states.

Canada

Although no legislation in Canada expressly states that cryptocurrency is legal, the official Government of Canada website specifically states an individual "may … buy and sell digital currency on open exchanges, called digital currency or cryptocurrency exchanges" (Government of Canada, 2018). The same site also refers to an individual's ability to buy goods and services on the Internet using digital currency. Consistent with this approach cryptocurrency is regulated in a very similar fashion to the US. All purchases made using cryptocurrency are subject to GST/HST, and any profits made from its use as a commodity are subject to Income Tax (Government of Canada, 2018).

Mexico

While no legislation specifically states that the use of cryptocurrency is legal, recent actions by the Mexican government make it almost certain that individuals who use cryptocurrency will not be prosecuted. This comes in the form of a bill passed unanimously in late-December 2017 which will allow for Fintech (Financial Technology) and cryptocurrency exchanges to operate *officially and legally* within Mexico, provided certain criteria are met. As such, it can be summarised that cryptocurrency is, by default, legal in Mexico as a result of the clear legality of the financial exchanges which deal with them.

South America

The response to cryptocurrency in South America has, similar to its northern counterpart, been mostly uniform. Most countries within the continent have either expressly or impliedly referred to cryptocurrency as being legal. However, there are two notable exceptions: Bolivia and Ecuador, both of which have prohibited Bitcoin and cryptocurrency.

Bolivia

General cryptocurrency and its derivatives, such as Bitcoin, have been expressly outlawed in Bolivia since May 2014 (Economía Bolivia, 2014). Unusually, when compared to other countries where cryptocurrency is also outlawed, the Bolivian authorities also followed through with the arrests of individuals found to be advocating digital currencies, with the belief that the sole purpose of cryptocurrency is to trick and defraud the Bolivian people in a type of 'pyramid scheme' (Cuen, 2017). Board Resolution 044/2014 issued by the Central Bank of Bolivia outlawed any form of currency which does not fall in the 'scope' of the national payment system. Bitcoin is explicitly mentioned in the resolution as being one of the currencies falling outside of the 'scope', resulting in its prohibition.

Brazil

Although Brazilian legislators have acknowledged the use of cryptocurrency within Brazil, no regulation existed as of March 2018. Brazil does not recognise cryptocurrency as a form of currency, nor a 'financial asset' (Goldstein, 2018). This perspective is derived from the Brazilian constitution, which only recognises 'foreign currencies' distributed by another country's government (Revoredo, 2017). Nonetheless, despite the lack of recognition, cryptocurrencies remain unregulated, and implicitly legal to use.

Ecuador

Ecuador has also expressly banned the use of existing cryptocurrency, albeit for a very different reason compared to equivalent countries. Almost identically to Bolivia, Bitcoin and cryptocurrencies were banned in July 2014: any Bitcoin businesses became illegal to operate, and any cryptocurrency in an individual's possession became subject to seizure at the hand of the government. However, within the same document, a new government sanctioned cryptocurrency was established. It became known as *Dinero Electrónico* (translating literally into 'Electronic Money'), which is still operating.

Europe

As at March 2018, no country in Europe has expressly banned the use of cryptocurrency. Considering the continent's size, there are a vast number of different ways in which countries have dealt with the rise in popularity of cryptocurrency, particularly over the last two years.

France

In January 2018, Finance Minister Bruno Le Maire ordered a proposal for new rules for cryptocurrency, with concerns surrounding its use in tax evasion, and the overall risk to French citizens (Hamill, 2018). In February 2018 French stock market regulator, the *Autorité des Marchés Financiers*, released a statement stating that cryptocurrencies should be regulated as financial 'derivatives.' Such labelling will mean that cryptocurrency trading platforms would require specific authorisation to trade, and any form of the technology would be barred from being advertised online. It remains to be seen whether this will set a precedent for the cryptocurrency market in Europe.

Russia

Russia's position on cryptocurrency appears significantly more uncertain than other countries in Europe. In 2016, the Russian Government was considering taking a hardline stance to Bitcoin by jailing individuals in possession of the cryptocurrency for up to seven years (CCN, 2016). In 2018, however, President Vladimir Putin publicly backed the use of blockchain technology in Russia during the near future (Bourgi, 2018). Similarly, positive attitudes to cryptocurrencies were evidenced by Putin's 'Minister of Internet', who created his own business specifically for mining Bitcoin (Liao, 2017). Based on these examples of acceptance at the political elite level in Russia, it is likely that cryptocurrency is legal in Russia, but may be regulated at some stage depending on the country's adoption of the currency.

United Kingdom

Any form of cryptocurrency is currently considered legal to use in the United Kingdom. However, like the US, monetary profit made from its purchase are subject to capital gains tax (UKcryptocurrency, 2018). At present, cryptocurrency is largely unregulated in the UK; however, there has been recent interest expressed by Prime Minister Theresa May to improve regulation. The UK Treasury has also started to investigate Bitcoin and cryptocurrency, making the future of cryptocurrency regulation in the UK uncertain.

Africa

Information on cryptocurrency policy in African states is generally lacking. Of the countries where a stance is known, there is little uniformity in the way they have dealt with the legality and regulation of the technology.

Algeria

The status of cryptocurrency in Algeria is clear: it was expressly banned by legislation signed into law on 27 December 2017. The law states: "The purchase, sale, use and possession of the so-called virtual currency is prohibited. The virtual currency is the one used by Internet users through the web. It is characterised by the lack of physical support such as coins, tickets, payments by check or credit card." (Official Newspaper of the Democratic and Popular Algerian Republic, 2017). Unlike some other countries which have banned cryptocurrency on the basis it is not issued by a government, Algeria has banned it because it has no physical equivalent in coins, notes or otherwise. Such a stance leaves no room for interpretation that could lead to the legal use of virtual currency.

South Africa

The Reserve Bank of South Africa has stated that there is "no legal status or regulatory framework" for the use of cryptocurrency (VDMA, n.d.); as such, its use may be considered legal. However, despite the lack of framework, and as a result of its status as an 'asset' (as opposed to legal tender) virtual currencies are taxed in South Africa depending on profits made from their use, similarly to the stance taken by the United Kingdom (Dlamini, 2017).

Asia and Oceania

The Asian region, especially the north-east, has recently experienced the most change in terms of cryptocurrency policy. Since the end of 2017, China and South Korea have drastically changed their stance on cryptocurrency, leading to the infamous crash of Bitcoin in January 2018 to just 35% of its price in November and December 2017. However, other regions of Asia and Oceania have experienced more stability, and a vast majority of them recognise cryptocurrency as legal to use.

Australia

Although Australia lacks legislation specifically dealing with the legality of cryptocurrency, actions by the Taxation Office and the Reserve Bank have clearly indicated that the use of the technology is legal. For example, until July 2017, the cryptocurrencies was double-taxed – it was subject to both capital gains tax, and the Goods and Services Tax (GST). However, as of July 2017, digital currencies are no longer subject to GST when they are purchased, as is the case in with other currencies (Australian Taxation Office, 2017). The Australian government has also introduced the licensing of digital currency exchanges in order to ensure they comply with existing anti-money laundering and counter-terrorist funding law. In addition, the Australian

Securities and Investment Commission (ASIC) has sought to regulate cryptocurrencies and distributed ledger technology as a financial product under the *Corporations Act 2001*[18].

China

In recent years, economic development of cryptocurrencies has allowed many individuals to ascend the economic ladder. However, China, as one of the largest Bitcoin trading countries, has pledged to bring a halt to these activities because they disturb social security and are thought to provide breeding grounds for criminality. Investments in digital currencies are thought not lead to an increase in the collective wealth in any given country, but to lead to the accumulation of personal wealth, if successful. This idea undermines a key tenet of communism because it encourages private ownership, and further widens the gap between the rich and the poor. Because Internet accessibility determines all transactions and investments of virtual currency, the Chinese Government seeks also to close grey activities that evade the Great Firewall by further tightening Internet censorship.

The world's second largest economy is now on a trajectory to ban Bitcoin. Nevertheless, cryptocurrency exchanges are not dead in China. Prohibitions of ICOs (Initial Coin Offerings) in 2017 and the "clean-ups" of VPNs showed China's attempt to eliminate all cryptocurrency exchanges in 2017 were unsuccessful. Additionally, these prohibitions did not have a significant effect on the Bitcoin surge in December 2017 when it reached nearly US$20,000 per Bitcoin. The prohibition encouraged Chinese investors to move their trading activities offshore to neighbouring countries, such as Hong Kong, Singapore, and Japan. Unable to adequately control cryptocurrency trading, Chinese authorities have subsequently focused upon domestic investors who attempt to, or already have, shifted their trading offshore.

China's tougher stance on cryptocurrency has undoubtedly discouraged local investments and ICOs. Since the beginning of 2018 about US$340 million has evaporated from the global cryptocurrency market. Speculation surrounded China's tougher regulations, and whether its response had led to such volatility. A report issued by the PBOC stated cryptocurrency trading the Chinese currency Renminbi (RMB) went from 90% of the global value to less than 1% ever since the ban of ICOs. However, despite the prohibition policy, Chinese platforms such as Baidu and Alibaba are currently exploring opportunities to become involved in cryptocurrency trade.

It is not clear whether China's regulations on cryptocurrency will protect their economy and national security; nonetheless, unintended side effects of their policies are evident. In February 2018, the National Internet Finance Association of China issued a notice warning of fake ICO white papers for sale on the Alibaba owned online shop platform *Taobao*. As such, China's new hard-line policy has simply resulted in opportunities for fraudulent activity on various marketplaces, particularly involving ICOs and Bitcoin information. Despite China's hostility towards Bitcoin, the PBOC has a positive attitude towards blockchain technology, but want it used by China's own cryptocurrency, as opposed to Bitcoin. China's anti-cryptocurrency policies are designed to discourage fraudulent behaviours, particularly money laundering, capital flight and tax evasion. China's attempt to regulate crypto-markets has proven difficult and has brought further volatility, as was seen in late 2017 (for a detailed timeline of events see Appendix 2). Given that some sources claim that the Chinese Yuan is estimated to make up perhaps 80% or more of all Bitcoin trading, with perhaps over 70% of Bitcoins located in China (Patel 2017; Woo 2017).

[18] For further details ASIC 'Initial Coin Offerings and Crypto-Currency', INFO225, May, 2018; see https://asic.gov.au/regulatory-resources/digital-transformation/initial-coin-offerings-and-rypto-currency/

South Korea

Despite the extensive media coverage of cryptocurrency policy changes in South Korea, the purchase, and trading of, cryptocurrency in South Korea remains legal. In January 2018, South Korean policymakers announced new legislation that would prevent Bitcoin and cryptocurrency trading where the name on the bank account, and the name on the digital currency wallet, were inconsistent – the legislation was enacted on 30 January (Reuters, 2018). At the time, it was speculated the move was the first in a series of regulatory controls which would eventually lead to a ban of cryptocurrency in the country. However, South Korea's finance minister, Kim Dong-yeon, stated that there were no plans to shut down virtual currency trading (Kim & Kim, 2018) as this could devastate the market and South Korea role as leading a trading 'hub'. Nonetheless, despite its 'legal' status, how stringently South Korea will regulate the technology in the future remains uncertain Kim & Park, 2018). Although anonymity remains a key problem for legislators there is a shift towards a unified regulatory approach based on the proposed G-20 model and compliance with Financial Action Task Force anti-money laundering practices (CNN, July 7 2018).

Chapter 5: State Actors and Cybercrime

State Actors Stockpiling Cyber Weapons

Uncovered exploits are potentially the most profitable when sold to malicious state actors – especially when the exploit provides a significant competitive advantage. State actors such as the Democratic People's Republic of Korea (DPRK) are known to seek zero-day compromises or exploits and fashion a range of custom made 'cyber-arms' by training and deploying cyber warriors. Zero-day forums and markets provide state actors with easy access to the latest exploits on offer and in turn encourage these markets with high rewards.

In a report published by RAND (2017) a government's approach to the use of vulnerabilities depends largely on whether the focus is on defence or offensive use. Defensively: "if one's adversaries also know about the vulnerability, then publicly disclosing the flaw would help strengthen one's own defence by compelling the affected vendor to implement a patch." Offensively: "publicly disclosing a vulnerability that isn't known by one's adversaries gives them the upper hand, because the adversary could then protect against any attack using that vulnerability, while still keeping an inventory of vulnerabilities of which only it is aware of in reserve." (Ablon and Bogart RAND 2017:np)" The RAND report suggests that the greatest defence and offensive capabilities for a state actor comes from a government stockpiling exploits, whilst also keeping track of an adversary's known stockpile (RAND, 2017, iii). The downside is that the users of vulnerable computers are exposed to risk while the exploit is stored for potential offensive cyber warfare.

Cybercriminal Activities of the Democratic People's Republic of Korea (DPRK)

The South Korean Defence White Paper (2014) noted that North Korea had about 6,000 'cyber warfare troops' (Ministry of National Defence – Republic of Korea, 2014). These cyber soldiers are used in the clandestine Reconnaissance General Bureau (RGB) and by the military's General Staff Department (GSD). Prospective candidates are selected from schools across the country and trained in cyber operations at the Pyongyang University of Automation and other colleges and universities (Denning, 2018).

The Worldwide Threat Assessment (2018) published by the U.S. intelligence community reports "Pyongyang probably has a number of techniques and tools it can use to achieve a range of offensive effects with little or no warning, including distributed denial of service attacks, data deletion, and deployment of ransomware" (Coats, 2018).

Lim Jong In, head of the department of cyber defence at Korea University in Seoul and a former special adviser to South Korea's president reports that "North Korea kills two birds with one stone by hacking: It shores up its security posture and generates hard currency," Lim says, "For hackers it offers a fast track to a better life at home" (Kim, 2018). DPRK has been known to typically employ attacks used by others in the past, falling short on creatively producing new attacks (Sheridan, 2018). Reports suggest that North Korea will continue to seek economic advantage within the converging space of cryptocurrencies and cybersecurity (Denning, 2018).

History of Cybercriminal Activities Perpetrated by the DPRK

Since the 1970s, the DPRK has engaged in the illicit economy as a means of producing income. These actions have included counterfeit currency and pharmaceuticals, drug production and smuggling, and extensive money laundering (Chestnut, 2007, p. 83; Cordesman, 2016, p. 15). The DPRK is also reported to have been involved in endangered species trafficking, human trafficking and arms dealing (Chestnut, 2007, p. 83; Broadhurst, Gordon and McFarlane 2012, p 151; Cordesman, 2016, p. 24). Although the DPRK strictly adheres to the isolationist concept of *juche* (self-reliance and economic self-sufficiency), it is clear that the transfer of these illicit materials has largely been facilitated by DPRK connections with a variety of international organised crime syndicates and third-party countries (Cordesman, 2016, pp. 15 – 16; Lim, 2008, pp. 31, 34). More recently, this criminal activity has also been used as a means of mitigating the impact of international sanctions. The implementation of various United Nations sanctions on the DPRK since 2006 (to prevent DPRK nuclear activity) is thought to have increased this illicit activity and the DPRK reliance on obtaining 'hard currency through illegal measures' (Berger, 2016, p. 15; see also Wertz, 2013, pp. 72 – 73; United Nations, 2017).

Given this history, the relatively recent inclusion of cybercrime within the DPRK illicit economy is unsurprising. Flatgard (2017) suggests that this has developed into a US$1 billion industry for the impoverished country. As an isolationist state, the DPRK does not allow Internet access to its citizens, reserving the right to a select few government bodies (Cordesman, 2016, p. 26). Instead, the country relies on an Intranet structure that effectively air-gapped it from the outside world (Cordesman, 2016, p. 27). Although this has reduced the potential risk of 'hackbacks' against the DPRK, it has increased the reliance of the DPRK on external technology sources. Siers (2014, p. 2) describes China as the DPRK's key "'cyber enabler and sponsor'". This is evident through the training DPRK hackers are reported to receive when sent to China and the alleged location and operation of particular DPRK cyber units (including the alleged '"Unit 121'") within China (Cordesman, 2016, p. 26; Osborne, 2014). Although the cyber capacity within the DPRK itself is relatively low in comparison to states such as South Korea and the United States, it is evident that the cybercrime industry in (or on the behalf of) the DPRK is likely to continue to grow as its techniques and technologies mature (Osborne, 2014). Indeed, many scholars have suggested that a number of recent cyber hacks and thefts conducted by groups are believed to be associated with the DPRK (Wagstaff & Smith, 2017).

DPRK Cyber-Thefts

The attribution of cyberattacks can be a highly "'nuanced process'" (Rid & Buchanan, 2015, p. 6). In the aftermath of a cyberattack, difficulties arise in the process of locating the likely source of the attack, and the potential international ramifications of identifying those responsible. According to the United States Computer Emergency Readiness Team (US CERT) (2017), a number of hacking groups allegedly associated with the DPRK (collectively referred to as *Hidden Cobra*) have partaken in recent cyberattacks.

The groups responsible include Lazarus and the Guardians of Peace (US CERT, 2017). Although the connection between Lazarus and the Guardians of Peace remains ambiguous, many scholars use the names interchangeably when discussing cases (Kaplan, 2016; Sharp, 2017; Whyte, 2016). Research conducted by Kaspersky (2017b, p. 3) has identified an additional group, Bluenoroff, as a subgroup of Lazarus. Although Lazarus is reported to have been operational since 2009, Bluenoroff is a relatively recent addition.

Both Kaspersky (2017b, p. 3) and Symantec (2016) report that Bluenoroff have used similar coding and hacking methods to Lazarus to conduct financially motivated attacks, thus indicating the connection between the two. Both of these groups have been implicated in a variety of cyber intrusions across a variety of countries and industries (Kaspersky, 2017a). Lazarus has been attributed to the 2014 Sony Pictures Entertainment hack and the recent 2016 Bangladesh Bank Hack see pages 13 – 14 (Kaspersky, 2017a). Bluenoroff has also been implicated in a number of attacks across a diverse range of countries, most notably the 2017 attacks on a number of Polish banks (CSO, 2017; Kaspersky, 2017b; Symantec, 2017a). Further, Lazarus and Bluenoroff are also strongly suspected to be involved in the hack of the Banco del Austro in Ecuador, the hack of Far Eastern International Bank in Taiwan, and the attempted hack of the Tien Phong Bank in Vietnam (Finkle, 2017; Symantec, 2016, 2017a). Recent research has also implied a coding link between Lazarus and the 2017 WannaCry ransomware attack see page 5 (Symantec, 2017b). The 2014 Sony hack is perhaps the most politically significant case, given that it drew initial international attention to the group.

DPRK: 2014 Sony Pictures Entertainment Hack

The Guardians of Peace and Lazarus attracted international attention in November 2014 following a damaging cyberattack against Sony Pictures Entertainment (Kaplan, 2016, p. 268). At the time, Sony had been preparing to release the controversial film *The Interview* that depicted a plot to assassinate current DPRK leader, Kim Jong-un (Sharp, 2017, p. 911). Following a series of earlier threats, the Guardians of Peace publically released over '"one hundred terabytes of data'" containing confidential information pertaining to various Sony employees and projects of the film (Kaplan, 2016, p. 268). Sony responded to this attack by delaying the release of the film, and eventually only screening it in select areas (Sharp, 2017, p. 913; Whyte, 2016, p. 99). Although investigations into the hack (e.g. 'Operation Blockbuster' conducted by Novetta) have directly attributed the attack to the Guardians of Peace and Lazarus, the extent of DPRK involvement is unclear and unconfirmed (Novetta, n.d.; Sharp, 2017, p. 913; Whyte, 2016, p. 99). The fact that both the Guardians of Peace and Lazarus are located outside of the DPRK has further complicated this attempted attribution (Flatgard, 2017).

Youbit Hack (2017)

During April and December of 2017, a South Korean online currency exchange Youbit (formally known as Yapizon) was hacked (Caster, 2017). Although the company was able to recover from the April attack, the December attack was particularly damaging. In the December hack, Youbit lost a total of 4,000 Bitcoin; equating to "'17 percent of its assets"' when a hot wallet was compromised, subsequently leading to the bankruptcy of the company (BBC, 2017; Caster, 2017, n.p.). Reuters (2017) suggest that online currency corporations are increasingly at risk of being targeted by cyberattacks, given their immense value. Although the attribution of this attack has not yet been confirmed, it is suggested Bluenoroff is responsible given the use of code similar to that utilised by Lazarus (Caster, 2017; Wagstaff & Smith, 2017).

The DPRK has an extensive history of transnational illicit activity (Cordesman, 2016, pp. 15, 24). The international expansion of this activity in the past provides a strong indication that a similar case could occur within the DPRK cyber activity (Siers, 2014, p. 7). The recent activity of cyber groups suspected to be associated with the DPRK (e.g. the Hidden Cobra) demonstrates that these groups possess an unprecedented capacity to launch highly damaging attacks that can be both financially and politically motivated. These have been shown to incur immense political and financial consequences on an international level. Given the global success of cyberattacks conducted by the Guardians of Peace, Lazarus, and Bluenoroff, it is not unfounded to suggest that these attacks will continue for the foreseeable future (Kaspersky, 2017b). The full extent of the connection between these groups (e.g. false flag, red herring) and the DPRK is yet to be seen.

Unlike physical products, such as drugs, criminal activity associated with malware is difficult for governments to prevent. In the case of drugs, governments can seize shipments at the border, perform controlled deliveries and track illicit articles. However, due to the non-terrestrial nature of the malware, governments are at a significant disadvantage in preventing criminal activity. Many operations to combat the illicit Dark Web involve undercover operations and rely upon significant investigative work (Van Wegberg et al., 2017).

Chapter 6: Conclusion

Research on cybercrime has relied on limited ethnographic or empirical studies of digital environments and traditional media reporting of specific cases. Studies conducted by Europol and the Organisation for Economic Cooperation and Development have provided some statistical data about the rise of cybercrime amplified by the crypto-market's facilitation of illicit trade. Relatively little is known about the socio-economic behaviour and the form of groups and networks on darknet markets, these platforms enable individual criminal entrepreneurs to offer Crime-as-a-Service (CaaS) and to "operate their own criminal business without the need for the infrastructures maintained by 'traditional' OCGs [organised crime groups]" (Europol 2017: 11). Europol's (2017: 56) most recent assessment of the organised crime threat, however, observed:

> *Technology is a key component of most, if not all, criminal activities carried out by organised crime groups in the EU and has afforded organised crime with an unprecedented degree of flexibility….it is also a key enabler of criminal activity and plays a role in all types of criminality. The impact of technology on crime, however, extends beyond the internet and involves all kinds of technical innovation such as advances in drone technology, automated logistics, and advanced printing technologies.*

Research on the darknet has found that the most common commodity sold is illicit drugs as we found in this research. The illicit drug market typically involves organised crime groups throughout the supply chain and critically in the protection of those markets and contracts. According to Kruithof, Aldridge, Decary-Hetu, et. al. (2016) drugs accounted for 57% of all products and services offered on the darknet markets they surveyed. Thus, much of the literature on crypto-markets concerns the illicit drug trade. However, we observe a substantial market in malware as well as crime-as-a -service, including special markets for fake credentials and documents such as passports. Research has also previously examined the characteristics of buyers and sellers; linguistic analysis of the terminology and text found on darknet markets; distribution networks; and trends more closely associated with drug use in particular (such as which products are commonly sold) (Martin & Christin, 2016; Martin, 2014; Lavorna & Sergi, 2016).

For example, in their attempt at a geographical analysis of drug trafficking on the darknet, Broséus, Rhumorbabe, Morelato, Staehli and Rossy (2017) collected data from the now defunct crypto-market 'Evolution'. They found that the availability of licit and illicit drugs, was affected by the vendor's alleged country of origin or from where the product was shipped. Broséus et al., (2017, p. 89) argued that:

> *… spatial specificity can be due to different factors affecting countries differently, such as geographic isolation, stringent border controls, relaxed laws in regards to illicit goods, high prices of goods, strict control of Internet access, proximity to producing countries, domestic productions of goods and relative availability of illicit goods*.

These variations reflect the broader drivers of transnational crime and explain why Broséus et al., (2017) found that in Australia and the US, the flow of illicit drugs was primarily within rather than across jurisdiction. The authors reason that this may be due to the perceived stringency of law enforcement and border control, which impact on a crypto-markets vendor's appetite for risk when shipping illicit products across international borders (Broséus et al., 2017).

A recent Europol intelligence assessment (Europol 2017) noted the rapid shift to darknet markets, despite their inherent instability. The emergence of peer-to-peer crypto-markets, such as Open Bazaar, that avoid the risks of being hosted in a specific location may be the next evolution in darknet markets.

> *New decentralised markets are likely to overcome the weakness and vulnerability of being hosted in a specific location. These localised Dark markets cut out intermediaries, cater to sellers and buyers in their own language allowing them to interact directly. Transactions on local platforms enable sellers and buyers to avoid international mail systems by arranging the local collection of illegal goods.* (Europol 2017: 53).

Previous research on crypto-markets has focused on how buyers and vendors manage security and achieve efficiency at reaching consumers of contraband. Thus, how these parties manage risk, motivations, branding, harm reduction, social capital based on trust, and the liminality or ambiguity of transactions have been addressed (Barratt 2012; Broséus, Rhumorbarbe, Mireault et al., 2016; Décary-Hétu, Paquet-Clouston & Aldridge, 2016; Tzanetakis, Kamphausen, Werse, & von Laufenberg, 2016; van Hout, & Bingham, 2013). However, much remains unknown and few qualitative or ethnographic studies of substance are available. Crime-ware markets are more simple and elusive than illicit products because the need to ensure a stealthy delivery is not required. Fine and Hancock (2016, p. 4) note we “must carefully consider this new frontier of field [labour]: How do we identify our subjects? What counts as data when we are following links, posts, and threads? Indeed, sitting at our computer, are we even ‘in the field?’”. Ferguson (2017) highlights that the digital environment offers both opportunities for safer observational methods through “lurking” techniques whereby researchers do not engage or alter the behaviour of those observed. However, there are also a number of problems associated with digital ethnography such as gaining access and entry that require time and prior knowledge, as well as ethical and privacy considerations. Ethical concerns about causing harm, restrict our interactions or ‘lurking’ on darknet markets limit the extent that we can observe vendors and market administrators. Many darknet markets and vendors require new ‘handles’ or vendors to trade in contraband, including offering similar products for sale before being able to fully participate in the market.

Despite the growing body of literature on darknet crypto-markets and cryptocurrencies and the proliferation of digital ethnography, the speed of change as well as the inherent volatility requires continuous attention to up-date data and monitor trends. Some limited historical data about darknet markets has been publically provided by Gwern (a pseudonym) whose inside knowledge of the Evolution crypto-market provides rare insight to organisation and tradecraft. Gwern’s (2015) databases described darknet markets and calculated their longevity between 2011 and 2015. Though essential for establishing long-term trends in the darknet, Gwern’s data is out of date. Since 2015, Bitcoin and other cryptocurrencies have increased in both their value and volume. The proliferation of new or recycled crypto-markets and the displacement of old ones has also occurred at pace since 2015. Media, darknet forums as well as (surfaceweb) specialist websites and indexes provide supplementary information. The reliability of these sources, however, is mostly unknown, and the data or analysis available from these sources may be unreliable (designed for advertising or obfuscation purposes). In order to minimise these problems, we captured data from a large general crypto-market – Dream Market. This enables us to monitor trends and describe in detail the types of products sold.

This review has provided an overview of developments in malware and illicit online crypto markets, and the policy responses globally. We noted that the number of malware listings observed over the eight-month study period remained relatively stable. However, the number of unique malware product listings and their values did vary across the period depending on the type of crime-ware on sale. Compromised accounts, credit card details, personal documents as well as hacking tools, keyloggers, phishing scams, ransomware, Trojan viruses, tutorials for hackers, vulnerabilities and exploits were prevalent among the services provided on the darknet market.

The markets and sites researched for this report provide an indication of the overall malware and exploit market landscape. Many transactions may occur privately between third parties with limited traceability and verification. More sophisticated zero day exploits are hard to come by – yet periodically appear on darknet markets, priced similarly or above the value of vulnerabilities offered by legitimate bug bounty programs. The lower rewards offered to security experts for disclosing via a bug bounty program could be a determining factor in whether an exploit is utilised in a malicious context.

Market activity is unlikely to stop in the near future with criminal profits likely to continue to play an increasing role in the cybercrime scenario. A recent study found “strong evidence of the correlation between market activity and exploit deployment" with the "time between vulnerability disclosure and appearance of exploit [sic] shortening" (Allodi, 2018, n.p). Reports by the Australian Cybersecurity Centre and other security agencies have also noted the link between malware markets and the cybercrimes reported to CERT’s and law enforcement. Our data does not allow us to fully explore this link, but this report has substantiated the importance of monitoring malware and exploit markets in the hope that they provide some warning about the risk of harmful cyber-attacks.

Further, this review found the services offered on online illicit markets appeared in line with other criminological research that suggests there is a spectrum of motivated individuals engaging in darknet markets from ‘white hat’ (ethical hackers), to ‘grey hat’ (actors that may violate laws or what is considered to be ethical, but that do not have malicious intent), and finally to the most nefarious actors ‘black hats’ (those individuals or groups deliberately engaging in illegal online activities).

The widespread incidence of malware distribution on darknet markets requires a broad-based and transnational prevention effort. Malware has become one of the most common threats faced by Internet users accompanied by a ‘booming’ crime-ware and exploit market (Kaspersky Lab, 2016). Fortinet Global (2017) reported that 90% of enterprises experience exploits of vulnerabilities more than three years old and 60% for vulnerabilities more than a decade old, indicating there is sizable window of opportunity for cybercriminals to exploit. The digital divide as we noted earlier, is expressed not in terms of access to cyberspace but in terms of insecurity. In spite of our own findings, and those of cybersecurity research organisations, the global cryptocurrency legislation is diverse and evolving, with the most rapid responses and changes to regulations being implemented across Asia, particularly in South Korea, Japan and China.

In response to the challenges, LEAs are compelled to adapt more rapidly than ever. A priority must be to increase the potency of deterrence. This will depend to a significant degree on the extent of mutual legal assistance given the cross-border nature of cybercrimes. Mandating standards and guidelines for built-in cybersecurity of new products written into the code level before release, combined with the promotion of crime prevention and cyber-safety awareness, must be central to the public-private partnerships needed to suppress cybercrime. The massive reach of the Internet inevitably enhances opportunities for cybercrime but it also offers the means to identify and counter threats, large and small, through effective forms of online community style policing that have proven effective in addressing violence in the non-virtual world.

Finding the balance between a secure yet open Internet is essential if the creative benefits provided by online resources are not lost. The steps already taken to secure the benefits of the new communication technologies through cross national mutual legal assistance, national cybersecurity strategies and community policing suggest how the impacts of cybercrime may be reduced.

Finally, "the recognition of a sense of 'shared fate' in cyberspace" should, "…quicken the development of multilateral responses and the capability for transnational crime control" (Broadhurst & Chang, 2013, p. 21). International cooperative measures will be key in the prevention of cybercrime because collaboration offers the best means to counter the problem of attribution (the identification of the cybercriminal).
identity obfuscation (such as VPNs) and the "plausible deniability" available to criminals, non-state and quasi-state actors active in cyberspace are barriers to attribution. Improving the targeting and forensic capacities of law enforcement will help disrupt, prosecute and deter offenders including in countries where the activity may not be criminalised or the state lacks the necessary capacity or will to suppress cybercrime directed abroad. Recognising this 'shared fate' and the prevalence of malware as crime as a service on darknet markets, the relative ease of acquisition and the low financial cost reinforces a need for continued monitoring and exploration. Research is also needed on the most effective means of suppressing cybercrime via better digital trace technologies and enhancing prevention strategies including 'target harden' and 'crime proof' design standards and practices. Partnership between governments, industry and academia will be crucial in responding to the opportunities for cybercrime in a period of uncertainty and disruption driven by rapid social and economic change.

References

English References

Ablon, Lillian and Timothy Bogart, Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits. Santa Monica, CA: RAND Corporation, 2017. https://www.rand.org/pubs/research_reports/RR1751.html..

Ablon, Lillian, Martin C. Libicki, & Andrea A. Golay, 2014. *Markets for Cybercrime Tools and Stolen Data Hackers' Bazaar*. Retrieved from the RAND website https://www.rand.org/content/dam/rand/pubs/research.../RAND_RR610.sum.pdf

Akers, R. L. (1998). *Social learning and social structure: a general theory of crime and deviance.* Boston, MA: Northeastern University Press.

Aliens, C. (2017, July 20). A Globally Coordinated Operation Just Took Down Alphabay and Hansa. *DeepDotWeb.* Retrieved from https://www.deepdotweb.com

Allodi, L. (2018). Economic Factors of Vulnerability Trade and Exploitation. Retrieved from https://arxiv.org/pdf/1708.04866.pdf

Australian Broadcasting Corporation. (2017, July 21). AlphaBay: Global authorities shut down dark net market 10 times the size of 2013's Silk Road. *Australian Broadcasting Corporation.* Retrieved from http://www.abc.net.au/news/

Australian Broadcasting Corporation. (2018, February 8). Infraud: Australian among 36 arrested in global cybercrime ring that stole $677 million*. Australian Broadcasting Corporation.* Retrieved from http://www.abc.net.au/news/

Australian Cyber Security Centre. (2017, June 29). Update on the initial infection vector of the Petya ransomware campaign. *The Australian Cyber Security Centre*. Retrieved from https://www.acsc.gov.au/news/petya-ransomware-campaign-impacting-organisations-globally.html.

The Australian Cyber Security Centre (2015). ASCC Threat Report 2015. Retrieved from https://www.acsc.gov.au/publications/ACSC_CERT_Cyber_Security_Survey_2015.pdf

Australian Taxation Office. (2017, December 21). *Tax treatment of crypto-currencies in Australia – specifically bitcoin.* Retrieved from https://www.ato.gov.au/General/Gen/Tax-treatment-of-crypto-currencies-in-Australia---specifically-bitcoin/

AV-TEST. (2018). Malware Statistics and Report. Retrieved from https://www.av-test.org/en/statistics/malware/

Baek C., & Elbeck M. (2015). Bitcoins as an investment or speculative vehicle? A first look. *Applied Economics Letters, 22*(1), 30 – 34, DOI: 10.1080/13504851.2014.916379

Bajpai, P. (2017, December 7). The 6 Most Important Cryptocurrencies Other Than Bitcoin. *Investopedia*. Retrieved from https://www.investopedia.com

BBC. (2015, January 2). China blocks virtual private network use. *BBC*. Retrieved from http://www.bbc.com

Berger, A. (2016). From Paper to Practice: The Significance of New UN Sanctions on North Korea. *Arms Control Today, 46*(4), 8 – 15. Retrieved from https://search-proquest-com.virtual.anu.edu.au/docview/1786538683?accountid=8330

Bitcoin. (n.d.). FAQ. *Bitcoin.* Retrieved from https://www.bitcoin.com/faq

Bischoff, P. (2017a, August 30). Warning: Darknet Markets Bitcoin mixing tutorial is a phishing scam. *Comparitech*. Retrieved from https://www.comparitech.com

Bischoff, P. (2017b, December 19). Step by step guide to safely accessing the darknet and deep web. *Comparitech*. Retrieved from https://www.comparitech.com

Bitcoin. (n.d.). FAQ. *Bitcoin.* Retrieved from https://www.bitcoin.com/faq

Blockchain. (2017, July 19). *Ingenious Minds Consultants*. Retrieved from http://www.ingminds.com/wp-content/uploads/2017/07/how-blockchain-works.png

Bloomberg News. (2013, December 5). China bans financial companies from Bitcoin transactions. Retrieved from https://www.bloomberg.com

Bloomberg News. (2017, July 10). China tells carriers to block access to personal VPNs by February. Retrieved from https://www.bloomberg.com

Bloomberg News. (2017, July 11). What China's VPN ban means for Internet users: Quick take Q&A. Retrieved from https://www.bloomberg.com

Borak, M. (2018, February 5). The final crackdown? China moves to completely ban and block cryptocurrency trading at home and abroad. *Technode.* Retrieved from http://technode.com

Bounty0x. (2018). Rewarding the Token Economy. Retrieved from https://bounty0x.io/

Bourgi, S. (2018, February 25). Vladimir Putin: Russia Must Enter the Race for Blockchain Adoption. *Hacked*. Retrieved from https://hacked.com

Bowers, K. J. & Johnson, S. D. (2003). Measuring the Geographical Displacement and Diffusion of Benefit Effects of Crime Prevention Activity. *Journal of Quantitative Criminology, 19* (3), 27 5– 301.

Bradley, S. (2018, Jan 25). How to use TOR. *Tech Advisor*. Retrieved from https://www.techadvisor.co.uk

British Broadcasting Corporation. (2017, December 19). Bitcoin exchange Youbit shuts after second hack attack. *BBC News*. Retrieved from http://www.bbc.com

British Broadcasting Corporation. (2018, February 7). Dozens charged for Infraud cyber-crime site. *British Broadcasting Corporation.* Retrieved from http://www.bbc.com

Roderic Broadhurst (May 16, 2017), 'What the underground market for ransomware looks like', *The Conversation*: https://theconversation.com

Broadhurst, R., P. Grabosky, M. Alazab, and S. Chon 2014, 'Organizations and Cybercrime: An Analysis of the Nature of Groups engaged in Cyber Crime', *International Journal of Cyber Criminology*, Vol. 8 [1]: 1 – 20.

Broadhurst, R & Chang, (2013). *Cybercrime in Asia: trends and challenges*, in Liu, J., Hebenton, B., Jou, S. (ed.), *Handbook of Asian Criminology*, Springer Science + Business Media, New York, pp. 49 – 63.

Broadhurst, R., Woodford-Smith H., Maxim, D., Sabol, B., Orlando, S., Chapman-Schmidt, Alazab, M. (2017, June 30). Cyber Terrorism: Research Report of the Australian National University Cybercrime Observatory for the Korean Institute of Criminology. *Social Science Research Network*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2984101

Broadhurst, R.G., Gordon, A. and J. McFarlane, 2012, 'Transnational and Organised Crime in the Indo-Asia Pacific', in F. Allum and S. Gilmour [Eds.], *Handbook of Transnational Organised Crime*, Routledge: London, pp. 143 – 156.

Broadhurst, R., & Choo, K. R. (2011). Cybercrime and On-Line Safety in Cyberspace. In C. Smith, S. Zhang, & R. Barbaret (Ed.), *International Handbook of Criminology* (pp.153 – 165). New York, United States of America: Routledge. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171559

Broséus, J., Rhumorbarbe, D., Morelato, M., Staehil, L., & Rossy, Q. (2017). A geographical analysis of trafficking on a popular darknet market. *Forensic Science International,* 277, 88 – 102. DOI: 10.1016/j.forsciint.2017.05.021

Broséus, J., Rhumorbarbe, D., Mireault, C., Ouellette, V., Crispino, F., Décary-Hétu, D. (2016). "Studying Illicit Drug Trafficking on Darknet Markets: Structure and Organisation From a Canadian Perspective." Forensic Science International. 264: 7 – 14.

BugCrowd (2017). 2017 State Of Bug Bounty Report. Retrieved from https://pages.bugcrowd.com/hubfs/Bugcrowd-2017-State-of-Bug-Bounty-Report.pdf

Burgess, M. (2017, June 28). Everything you need to know about EternalBlue - the NSA exploit linked to Petya. *Wired.* Retrieved from http://www.wired.co.uk

Carbon Black. (2017, Oct). The Ransomware Economy. Retrieved from https://www.carbonblack.com/wp-content/uploads/2017/10/Carbon-Black-Ransomware-Economy-Report-101117.pdf

Carr, K. (2014). An argument against using general deterrence as a factor in criminal sentencing. Cumberland Law Review, 44(2), 249 – 281. ISSN: 0360-8298

Caster, A. (2017, December 19). After Second Hack This Year, South Korean Exchange Youbit Closes Down. *Bitcoin Magazine*. Retrieved from https://bitcoinmagazine.com

Cheng, R. (2016, November 9). China passes long-awaited cyber security law. *Forbes.* Retrieved from https://www.forbes.com

CCN (2016, March 10). A 7-Yr Prison Term for Bitcoin Use, Says Russian Finance Ministry. *CCN*. Retrieved from https://www.ccn.com

Chertoff, M. (2017). A public policy perspective of the Dark Web. *Journal of Cyber Policy*, *2*(1), 26 – 38, DOI: 10.1080/23738871.1298643

Chestnut, S. (2007). Illicit Activity and Proliferation: North Korean Smuggling Networks. *International Security, 32*(1), 80 – 11. Retrieved from https://www.mitpressjournals.org

Chohan, U. (2017, September 24). Assessing the differences in Bitcoin and other cryptocurrency legality across national jurisdictions. *Social Science Research Network*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3042248\

Chon, S. (2016, June). *Cybercrime Precursors: Towards A Model Of Offender Resources* (Doctors thesis, The Australian National University, Canberra). Retrieved from https://openresearch-repository.anu.edu.au/bitstream/1885/107344/1/Chon,%20K%20H%20(Steve)%20Thesis%202016.pdf

Chris. (2014, June 13). Simple Whonix Installation Tutorial. *DeepDotWeb*. Retrieved from https://www.deepdotweb.com/2014/06/13/simple-whonix-installation-tutorial/

Chua, Y. T., & Holt, T. J. (2016). A cross-national examination for the techniques of neutralization to account for hacking behaviours. *Victims & Offenders, 11*(4), 534-555.

Coats, D. (2018, Feb 13). The Worldwide Threat Assessment. Retrieved from https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf

Cohen, L. E. & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activities Approach. *American Sociological Review, 44*(4), 588 – 608.

Coindesk (n.d. a). *[Litecoin] Cryptocurrency Market Capitalizations.* Retrieved 23 February, 2018, from https://coinmarketcap.com/currencies/litecoin/

Coindesk (n.d. b). *[Zcash] Cryptocurrency Market Capitalizations.* Retrieved 23 February, 2018, from https://coinmarketcap.com/currencies/zcash/

Coindesk (n.d. c). *[Monero] Cryptocurrency Market Capitalizations.* Retrieved 23 February, 2018, from https://coinmarketcap.com/currencies/monero/

Coindesk (n.d. d). *[Ethereum] Cryptocurrency Market Capitalizations.* Retrieved 23 February, 2018, from https://coinmarketcap.com/currencies/ethereum/

CoinMarketCap. (2018). Cryptocurrency Market Capitalizations: Percentage of Total Market Capitalization - Dominance. Retrieved from https://coinmarketcap.com/charts/

CNN (July 7 2018). South Korea to Loosen Crypto Rules in Cooperation With G20 Directive, available at https://www.ccn.com/south-korea-to-loosen-crypto-rules-in-cooperation-with-g20-directive/

Combining Tor With A VPN. (n.d.). Retrieved 20 December, 2017, from https://www.deepdotweb.com/jolly-rogers-security-guide-for-beginners/combining-tor-with-a-vpn/

Combining Tor With A VPN Continued. (n.d.). Retrieved 20 December, 2017, from https://www.deepdotweb.com/jolly-rogers-security-guide-for-beginners/combining-tor-with-a-vpn-continued/

Condliffe, J. (2014, April 14). Try The Super-Secure USB Drive OS That Edward Snowden Insists On Using. *Gizmodo*. Retrieved from https://www.gizmodo.com.au

Connection Tor - > VPN For Windows Users. (n.d.). Retrieved 02 February, 2018, from https://www.deepdotweb.com/jolly-rogers-security-guide-for-beginners/connecting-tor-vpn-for-windows-users/

Cordesman, A. H. (2016). *Korean Special, Asymmetric, and Paramilitary Forces.* Retrieved from https://csis-prod.s3.amazonaws.com/s3fs-public/publication/160809_Korean_Special_Asymmetric_Paramilitary_Forces.pdf

CryptoNews Room, (2017, Dec 20). How Many Alt-Coins are there? *Just Crypto News*. Retrieved from https://www.justcryptonews.com

CSO. (2017). *Kaspersky Lab reveals 'direct link' between banking heist hackers and North Korea.* Retrieved January 17, 2018, from https://www.csoonline.com/article/3187548/security/kaspersky-lab-reveals-direct-link-between-banking-heist-hackers-and-north-korea.html

Cuen, L. (2017, May 30). Bolivia Arrests Cryptocurrency Advocates, Calls Bitcoin A 'Pyramid Scheme'. *International Business Times*. Retrieved from http://www.ibtimes.com

Darknet Hidden Services Facing Large Scale DDoS Attacks. (2017). *Darkowl*. Retrieved from https://www.darkowl.com/blog/2017/darknet-hidden-services-facing-large-scale-ddos-attacks

Décary-Hétu, D. & Dupont (2012). The social network of hackers. Retrieved from https://www.tandfonline.com/doi/abs/10.1080/17440572.2012.702523

Décary-Hétu, D. & Giommoni, L. (February 2017). Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous. *Crime, Law and Social Change*, *67*, 55 – 75. doi: https://doi.org/10.1007/s10611-016-9644-4

Décary-hétu, D., & Leppänen, A. (2016). Criminals and signals: An assessment of criminal performance in the carding underworld. *Security Journal, 29*(3), 442 – 460. Retrieved from http://dx.doi.org.virtual.anu.edu.au/10.1057/sj.2013.39

DeepDotWeb. (2018). Dark Net Markets Comparison Chart. Retrieved from https://www.deepdotweb.com/dark-net-market-comparison-chart/

Denning, D. (2018, Feb 20). North Korea's growing criminal cyberthreat. *The Conversation*. Retrieved from https://theconversation.com

Denning, D. (1990). Concerning Hackers Who Break into Computer System. Retrieved from http://www-bcf.usc.edu/~hantran/3pov.html

Dinham. P. (2018, March 9). Steep rise in malware threats to Mac: report. *ITWire*. Retrieved from https://www.itwire.com

Dlamini, S. (2017, October 8). You're liable for tax on Bitcoin gains. *Personal Finance*. Retrieved from https://www.iol.co.za

Douglas, D. (2017). Booters: can anything justify distributed denial-of-service (DDoS) attacks for hire? Retrieved from https://pdfs.semanticscholar.org/73ff/c167ee36dec4978be1ac3955a1860cddf2db.pdf?_ga=2.261453582.209022998.1522320513-1330729790.1522320513

Economía Bolivia (2014, June 18). Utilización de dinero electrónico en Bolivia crece a pasos agigantados. *Economía Bolivia.* Retrieved from http://www.economiabolivia.net

el33th4xor (Sirer, Emin). (2018, March 21). But "receiving" data requires having the decoder that can reconstitute the original content from the specific encoding in the chain. And regular cryptocurrency software lacks such a decoder. [Twitter Post]. Retrieved from: https://twitter.com/el33th4xor/status/976541888110002178

Egan, M. (2018, Jan 10). What is the Dark Web? What is the Deep Web? How to Access the Dark Web. *Tech Advisor*. Retrieved from https://www.techadvisor.co.uk

Eha, B. P. (2017). Can Bitcoin's First Felon Help Make Cryptocurrency a Trillion-Dollar Market? *Fortune.* Retrieved from http://fortune.com

Ekblom, P., & Tilley, N. (2000). Going Going Equipped, *The British Journal of Criminology*, *40*(3), pp. 376–398, retrieved from https://doi.org/10.1093/bjc/40.3.376

ElevenPaths. (2016). Analysis Of The Inj3ct0r Team. Retrieved from https://www.elevenpaths.com/investigation-report-on-the-inj3ct0r-team-cyber-identity/index.html

Europol. (2016, September 27). The Relentless Growth of Cybercrime. *Europol Press Release*. Retrieved from https://www.europol.europa.eu

Europol, European Police Office, (2017). European Union serious and organised crime threat assessment, *Europol.* Retrieved from https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017

Europol, (2017, July 20). Massive Blow To Criminal Dark Web Activities After Globally Coordinated Operation. *Europol*. Retrieved from https://www.europol.europa.eu

Europol, (2017, December 4). Andromeda Botnet Dismantled In International Cyber Operation. *Europol*. Retrieved from https://www.europol.europa.eu

European Parliamentary Research Service. (2014, April 11). Bitcoin: Market, economics and regulation. Retrieved from http://www.europarl.europa.eu/RegData/bibliotheque/briefing/2014/140793/LDM_BRI(2014)140793_REV1_EN.pdf)

Faber, J. (2018, January 17). Chinese giant Alibaba launches a cryptocurrency mining platform despite government regulations. *Crypto Crimson*. Retrieved from https://cryptocrimson.com

Felson, M. & Clarke, R. V. (1998). Opportunity makes the thief: Practical theory for crime prevention. *Police Research Series Paper 98.* London: Home Office Research, Development and Statistics Directorate

Financial Consumer Agency of Canada (2018). *Digital currency*. Retrieved from the Government of Canada website https://www.canada.ca/en/financial-consumer-agency/services/payment/digital-currency.html

Finkey, K. (2014, April 14). Out In The Open: Inside The Operating System Edward Snowden Used To Evade The NSA. *Wired*. Retrieved from https://www.wired.com

Finkle, J. (2017, October 17). North Korea likely behind Taiwan SWIFT cyber heist: BAE. *Reuters.* Retrieved from https://www.reuters.com

Finklea, K. (2017, March 10). Dark Web. *Congressional Research Service CRS Report.* Retrieved from https://fas.org/sgp/crs/misc/R44101.pdf

Finley, K. (2014, April 14). Out In The Open: Inside The Operating System Edward Snowden Used To Evade The NSA. *Wired.* Retrieved from https://www.wired.com

Finn, T. (2016, April 28). Qatar National Bank investigating alleged data hack. *Reuters.* Retrieved from http://www.reuters.com

Flatgard, B. (2017). *Cyber crime: North Korea's billion-dollar soft spot.* Retrieved from the Lowy Institute website https://www.lowyinstitute.org/the-interpreter/cyber-crime-north-korea-s-billion-dollar-soft-spot-0

Fortinet. (2017). Threat Landscape Report Q2 2017. Retrieved from the Fortinet website https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/Fortinet-Threat-Report-Q2-2017.pdf

Friis-Jensen, E,. (2014, April 10). The History of Bug Bounty Programs. Retrieved from https://blog.cobalt.io/the-history-of-bug-bounty-programs-50def4dcaab3

Fruhlinger, J. (2018, January 15). Spectre and Meltdown explained: What they are, how they work, what's at risk. *CSO Online*. Retrieved from https://www.csoonline.com

Fox-Brewster, T. (2017, July 20). How The Cops Took Down An Alleged $23 Million Dark Web Drug Kingpin. *Forbes*. Retrieved from https://www.forbes.com

Gao, C. (2018, January 11). Apple to transfer Chinese iCloud operation to a Chinese state-owned company. *The Diplomat*. Retrieved from https://thediplomat.com

Gehl, R. W. (2014). Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network. *New Media & Society, 18*(7), 1219 – 1235. DOI: 10.1177/1461444814554900

Glaser, F., Zimmermann, K., Haferkorn, M., Weber, M., & Siering, M. (2014). Bitcoin - asset or currency? Revealing users' hidden intentions. *Twenty Second European Conference on Information Systems*. Retrieved from https://pdfs.semanticscholar.org/3c7d/998b88bf48c88cf693625d2852706e7cb8e4.pdf

Godwin, A. (2017, September 21). China's crackdown on cryptocurrency trading—a sign of things to come. *The Diplomat*. Retrieved from https://thediplomat.com

Goh, B. and Kelly, J. (2017, September 4). Bitcoin exchange BTC China says to stop trading, sparking further slide. *Reuters*. Retrieved from https://www.reuters.com

Goldsmith, A., & Brewer, R. (2015). Digital drift and the criminal interaction order. *Theoretical Criminology*, *19*, 112 – 130.

Goldstein, S. (2018, January 14). Brazilian Regulator: Cryptocurrency is Not a Financial Asset. *Finance Magnates.* Retrieved from https://www.financemagnates.com

Gopalakrishnan, R., & Mogato, M. (2016, May 19). Bangladesh Bank official's computer was hacked to carry out $81 million heist: diplomat. *Reuters*. Retrieved from https://www.reuters.com

Gordon, S., & Ma, Q. (2003). *Convergence of Virus Writers and Hackers: Factor or Fantasy*. Cupertino, CA: Symantec Security White Paper.

Grabosky, P. N. (2001). Virtual criminality: Old wine in new bottles? *Social & Legal Studies*, *10*(2), 243 – 249.

Grabosky, P., & Stohl, M. (2003). Cyberterrorism. *Australian Law Reform Commission – Reform Journal, 82*, 8 – 13. Retrieved from http://classic.austlii.edu.au/au/journals/ALRCRefJl/2003/3.html

Graz University of Technology (2018). *Spectre and Meltdown*. Retrieved February 26, 2018, from https://meltdownattack.com/

GReAT, (2017, May 12). The Wannacry(pt) Ransom Demand [Online Image]. *Secure List.* Retrieved from https://securelist.com

Greenberg, A. (2014, June 17). How to Anonymize Everything you do Online. *Wired.* Retrieved from https://www.wired.com

Greenberg, A. (2017, July 20). Global Police Spring A Trap On Thousands Of Dark Web Users. *Wired.* Retrieved from https://www.wired.com

Greenberg, A. (2018, February 7). Feds take down a half-billion dollar cybercrime forum after 7 years online. *Wired.* Retrieved from https://www.wired.com

Gwern, B. (2018). Darknet Market Archives (2013 – 2015). Retrieved from https://www.gwern.net/DNM-archives

HackerOne. (2018). *The 2018 Hacker Report.* Retrieved from the Hacker one website https://www.hackerone.com/sites/default/files/2018-01/2018_Hacker_Report_0.pdf

Hacken. (2018). *The first custom-tailored decentralized token for cybersecurity professionals*. Retrieved from https://hacken.io/

Hamill, J. (2018, January 15). France declares war on the cryptocurrencies Bitcoin, Ethereum, Litecoin and Ripple – could tough new stance lead to a ban?. *Metro*. Retrieved from http://metro.co.uk

He, D., Habermeier, K. F., Leckow, R. B., Haksar, V., Almeida, Y., Kashima, M., Kyriakos-Saad, N., Oura, H., Sedik, T. S., Stetsenko, N., & Verdugo Yepes, C. V. (2016). *Virtual Currencies and Beyond: Initial*

Considerations. Retrieved from http://www.imf.org/en/publications/staff-discussion-notes/issues/2016/12/31/virtual-curre

Hertig, A. (n.d.). How Ethereum Works. *Coindesk*. Retrieved on November 25, 2017 from https://www.coindesk.com

Higgins, S. (2017, December 29). From $900 to $20,000: Bitcoin's Historic 2017 Price Run Revisited. *Coindesk*. Retrieved from https://www.coindesk.com

Higgins, K. J. (2018, January 8). Meltdown, Spectre Likely Just Scratch the Surface of Microprocessor Vulnerabilities. *Dark Reading*. Retrieved from https://www.darkreading.com

Holden, E. (n.d.). ***An Introduction to Tor vs I2P.*** Retrieved from the IVPN website: https://www.ivpn.net/privacy-guides/an-introduction-to-tor-vs-i2p

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2015). *Cybercrime and Digital Forensics: An Introduction*. Oxon: Routledge.

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2018). *Cybercrime and Digital Forensics: An Introduction* (2nd Ed.). Oxon: Routledge.

Holt, T., Bossler, A., & May, D. C., (2012). Low Self-Control, Deviant Peer Associations, and Juvenile Cyberdeviance. *American Journal of Criminal Justice*, *37* (3), 378-396. doi: 10.1007/s12103-011-9117-3

Holt, Thomas J., Adam Bossler. (2014). "Cybercrime." Oxford Handbooks Online. doi: 10.1093/oxfordhb/9780199935383.013.002

Holt, T., Lampke, E. (2010). Exploring stolen data markets online: products and market forces. *Criminal Justice Studies, 23*(1), pp. 33 – 50

Holt, T. J. (2017). Identifying gaps in the research literature on illicit markets on-line. *Global Crime, 18*(1), 1–10. DOI: 10.1080/17440572.2016.1235821

Holt, T. J. (2013). Examining the forces shaping cybercrime markets online. *Social Science Computer Review, 31* (2), pages 165-177.

Hruska, J. (2018, February 28). Recent Intel CPUs Take Performance Hit With Spectre, Meltdown Patches. *Extreme Tech*. Retrieved from https://www.extremetech.com

Huang, H. & Bashir, M., (2016, December 27). The onion router: Understanding a privacy enhancing technology community. *Proceedings of the Association for Information Science and Technology*, *53* (1), 1-10. doi: 10.1002/pra2.2016.14505301034

Hutchins, A, Clayton, R., (2016). *Exploring the Provision of Online Booter Services*. Retrieved from https://www.tandfonline.com/doi/abs/10.1080/01639625.2016.1169829?journalCode=udbh20

Hui, K., Kim, S. H., Wang, Q. (2017). Cybercrime Deterrence And International Legislation: Evidence From Distributed Denial Of Service Attacks. *MIS Quarterly, 41* (2), 497 – 523

Hurlburt, G. (2017). Shining Light on the Dark Web. *Computer, 50*(4), 100 – 105. Retrieved from http://ieeexplore.ieee.org/Xplore/home.jsp

Inj3ct0r. (2018a). Official Statement of the 0day.today 1337day Team. Retrieved from https://0day.today/agree

Inj3ct0r. (2018b). 0day.today Listing For Remote Exploits. Retrieved from https://0day.today/exploit/description/29702

INTERPOL. (2015) *Cyber Research Identifies Malware Threat to Virtual Currencies*. Retrieved from https://www.interpol.int/News-and-media/News/2015/N2015-033

IT News (2016, May 9). SWIFT technicians blamed for Bangladesh bank vulnerabilities. *IT News*. Retrieved from https://www.itnews.com.au

Jaishankar, K. (2008). Space transition theory of cyber crimes. In F. Schmalleger & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 283 – 301). Upper Saddle River, NJ: Prentice Hall.

Japan Times, The. (2018). Tokyo police arrest four Vietnamese over illegal sale of cryptocurrency account. *The Japan Times*. Retrieved from https://www.japantimes.co.jp

Jones, S., & Bradshaw, T. (2017, May 14). Global alert to prepare for fresh cyber attacks. *Financial Times*. Retrieved from https://www.ft.com

Kaplan, F. (2016). *Dark Territory.* New York: Simon and Schuster.

Kaspersky Lab. (2017a). *Chasing Lazarus: A Hunt for the Infamous Hackers to Prevent Large Bank Robberies.* Retrieved from Kaspersky Lab website https://www.kaspersky.com/about/press-releases/2017_chasing-lazarus-a-hunt-for-the-infamous-hackers-to-prevent-large-bank-robberies

Kaspersky Lab. (2017b). *Lazarus under the hood*. Retrieved from Kaspersky Lab website https://securelist.com/files/2017/04/Lazarus_Under_The_Hood_PDF_final.pdf

Kaspersky Lab. (2016). 'All the Gear but No Idea': Our Devices Are Catching Viruses but We Don't Know Why. Retrieved from Kaspersky Lab website https://www.kaspersky.com/about/press-releases/2016_all-the-gear-but-no-idea-our-devices-are-catching-viruses-but-we-do-not-know-why

Kaspersky Lab. (n.d.). What is a Black-Hat hacker? Retrieved from Kaspersky Lab website https://www.kaspersky.com.au/resource-center/threats/black-hat-hacker

Katsiampa, P. (2017). Volatility estimation for Bitcoin: A comparison of GARCH models. *ResearchGate.* Retrieved from https://www.researchgate.net/publication/317723547_Volatility_estimation_for_Bitcoin_A_comparison_of_GARCH_models

Kelly, J. (2015, July 23). Betting on blockchain: firms seek fortune in bitcoin's plumbing. *Reuters.* Retrieved from http://www.reuters.com

Kethineni, S., Cao, Y., & Dodge, C. (2017). Use of Bitcoin in Darknet Markets: Examining Facilitative Factors on Bitcoin-Related Crimes. *ResearchGate.* DOI: 10.1007/s12103-017-9394-6

Kidron, M. (2017, December). *Blasted from the past: why you can't ignore old vulnerabilities*. Retrieved from https://www.sciencedirect.com/science/article/pii/S1361372317301094

Kim, D. & Kim, C. (2018, January 31). South Korea says no plans to ban cryptocurrency exchanges, uncovers $600 million illegal trades. *Reuters*. Retrieved from https://www.reuters.com

Kim, S. (2018, Feb 8). Inside North Korea's Hacker Army. *Bloomberg* News. Retrieved from https://www.bloomberg.com

Kim, D., & Park, J. (2018, February 27). South Korea keeps investors guessing on cryptocurrency regulation. *Reuters*. Retrieved from https://www.reuters.com

Lam, E., Jiyuen Lee, J., & Robertson, J. (June 10, 2018). Cryptocurrencies Lose $42 Billion After South Korean Bourse Hack. *Bloomberg News*. Retrieved from https://www.bloomberg.com

Lange, J., & Volz, D. (2016, June 1). Exclusive: Fed records show dozens of cybersecurity breaches. *Reuters.* Retrieved from http://www.reuters.com

Lavorgna, A., and A. Sergi, 2016, Serious, therefore Organised? A Critique of the Emerging "Cyber-Organised Crime" Rhetoric in the United Kingdom. *International Journal of Cyber Criminology*, 10:170 – 187.

Lawrence, H., Hughes, A., Tonic, R. Zou, C. (2017). *D-miner: A Framework for Mining, Searching,Visualizing, and Alerting on Darknet Events*. Retrieved from http://www.cs.ucf.edu/~czou/research/D-miner-CNS2017.pdf

Leathern, R. (2018, January 31). New ads policy: Improving integrity and security of financial product and services ads. *Facebook Business.* Retrieved from https://www.facebook.com

Lee, J., Long, A., McRae, M., Steiner, J., Handler, S. G. (2015). Bitcoin Basics: a Primer on Virtual Currencies. *Business Law International, 16*(1), 21 – 48. Retrieved from https://search-proquest-com.virtual.anu.edu.au/docview/1687833680/fulltextPDF/F7BA9813370244BBPQ/1?accountid=8330

Leukfeldt, E. R., Lavorgna, A., and Kleemans, E. R. (2017). Organised cybercrime or cybercrime that is organized? An assessment of the conceptualisation of financial cybercrime as organized crime. *European Journal on Criminal Policy and Research*, *23*(3), 287– 300.

Leukfeldt, E. R., & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior, 37*(3). doi: https://doi-org.virtual.anu.edu.au/10.1080/01639625.2015.1012409

Levi, M. (2017). Assessing the trends, scale and nature of economic cybercrimes: overview and issues. *Crime, Law and Social Change*, *67*(1), 3– 20.

Lewis, J. (2018). *Economic Impact of Cybercrime – No Slowing Down.* Retrieved from the Centre for Strategic and International Studies website: https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf?kab1HywrewRzH17N9wuE24soo1IdhuHd&utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21&utm_medium=email&utm_term=0_7623d157be-bb9303ae70-1940938

Leyden, J. (2002, August 2). HP withdraws DMCA threat: Wiser counsel prevails. *The Register*. Retrieved from https://www.theregister.co.uk

Li, C. (2017, September 15). In China's Hinterlands, workers mine Bitcoin for a digital fortune. *New York Times*. Retrieved from https://www.nytimes.com

Liao, S. (2017, October 31). Inside Russia's love-hate relationship with Bitcoin. *The Verge.* Retrieved from https://www.theverge.com

Lim, T. (2008). North Korea's Shady Transnational Business Activities and Their Future Prospects. *North Korean Review, 4*(2), 31– 48. doi: 0002006583;10.3172/NKR.4.2.31

Lynch, S. (2015, October 16). Full disclosure: Infosec industry still fighting over vulnerability reporting [Web log post]. Retrieved from https://umbrella.cisco.com/blog/2015/10/16/full-disclosure-infosec-industry-still-fighting

Lynch, S. N. (2018, February 8). U.S. shuts down cyber crime ring launched by Ukrainian. *Reuters*. Retrieved from https://www.reuters.com

Lusthaus, J. (2013). How organized is organized cyber crime? *Global Crime*, 14(1), 52–60. doi:10.1080/17440572.2012.759508.

MalwareTech. (2017, May 13). How to Accidentally Stop a Glock Cyber Attacks. *MalwareTech*. Retrieved from https://www.malwaretech.com

Marshall, A. (2018, January 30). Facebook bans cryptocurrency, ICO ads because of 'deceptive promotional practices'. *Coin Telegraph.* Retrieved from https://cointelegraph.com

Matzutt, R, Hiller, J, Henze, M, Ziegeldorf, J, Müllman, D, Hohlfeld, O, Wehrle, K. (2017). A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin*, In Proceedings of the 22nd International Conference on Financial Cryptography and Data Security (FC).* Springer.

Matza, D. (1964). *Delinquency And Drift*. University of California, CA: John Wiley & Sons, Inc.

Maurer, Tim (2018). *Cyber Mercenaries: The State, Hackers and Power*. Cambridge University Press.

McCarthy, K. (2017, July 11). Russia, China vow to kill off VPNs, Tor browser. *The Register*. Retrieved from https://www.theregister.co.uk

McCormick, T. (2013, September 12). The Darknet: A Short History. *Foreign Policy*. Retrieved from http://foreignpolicy.com

McGuire, M. (2012). *Organised Crime in the Digital Age*. London: John Grieve Centre for Policing and Security.

McMillan, R. (2014, March 3). The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster. *Wired.* Retrieved from https://www.wired.com

Mezher, T., El Khatib, S,. Sooriyaarachchi, TM,. (2015). Cyberattacks on Critical Infrastructure and Potential Sustainable Development Impacts. Int. J. Cyber Warf. Terror. 5, 3 (July 2015), 1– 18. DOI=http://dx.doi.org/10.4018/IJCWT.2015070101

Memoria, F. (2017, May 30). Bolivian Authorities Arrest 60 Bitcoiners, Reiterate Virtual Currencies as Illegal Pyramid Schemes. *CryptoCoinsNews*. Retrieved from https://www.ccn.com

Miller, C. (2007, May 6). *The Legitimate Vulnerability Market Inside the Secretive World of 0-day Exploit Sales*. Retrieved from the Independent Security Evaluators website http://www.econinfosec.org/archive/weis2007/papers/29.pdf

Miller, D. (2017, November 3). Bitcoin explained: The digital currency making millionaires. *ABC News*. Retrieved from http://www.abc.net.au

Ministry of National Defence – Republic of Korea. (2014). *2014 Defence White Paper*. Retrieved from http://www.mnd.go.kr/user/mnd/upload/pblictn/PBLICTNEBOOK_201506120206080360.pdf

Mitra, S. & Ransbotham, S. (2015). Information disclosure and the diffusion of information security attacks. *Information Systems Research*, *26*(3), 565– 584. DOI: 10.1287/isre.2015.0587

Mizrahi, A. (2018, February 5). China to block access to international cryptocurrency exchanges. *Bitcoin News*. Retrieved from https://news.bitcoin.com

Morgan, S. (2016, January 17). Cyber Crime Costs Projected to Reach $2 Trillion by 2019. *Forbes*. Retrieved from https://www.forbes.com

Nakamoto, Satoshi. (2008). *The Bitcoin Whitepaper*. Retrieved from the Bitcoin website https://bitcoin.org/bitcoin.pdf

Ngo, D. (2018, January 12). China's search engine giant Baidu launches blockchain open platform. *Coin Journal*. Retrieved from https://coinjournal.net

Monero. (2015). Monero. *Monero.* Retrieved from http://monero.org/

Moore, D., & Rid, T. (2016). Cryptopolitik and the Darknet. *Survival: Global Politics and Strategy, 58*(1), 7–38. DOI: 10.1080/00396338.2016.1142085

Morgan, S. (2016, January 17). Cyber Crime Costs Projected To Reach $2 Trillion by 2019. *Forbes*. Retrieved from https://www.forbes.com

"Mr. Nice Guy" Market Paid For Recent Attacks On Other Markets, Was Preparing To Exit Scam, (2017, May 31). *Darknet Markets*. Retrieved from https://darknetmarkets.org

New South Wales Department of Attorney General and Justice. (2011a). Routine activity theory crime prevention. Sydney, Australia: Author. Retrieved from http://www.crimeprevention.nsw.gov.au/Documents/routine_activity_factsheet_nov2014.pdf

New South Wales Department of Attorney General and Justice. (2011b). Rational choice crime prevention. Sydney, Australia: Author. Retrieved from http://www.crimeprevention.nsw.gov.au/Documents/rational_choice_factsheet_nov2014.pdf

Newman, L. (2017, April 8). The attack on global privacy leaves few places to turn. *Wired*. Retrieved from https://www.wired.com

Newman, L. H. (2018, January 3). Github Survived The Biggest DDoS Attack Ever Recorded. *Wired*. Retrieved from https://www.wired.com

Ngo, D. (2018, January 12). China's search engine giant Baidu launches blockchain open platform. *Coin Journal*. Retrieved from https://coinjournal.net

Novetta. (n.d.). *Operation Blockbuster: Unraveling the Long Threat of the Sony Attack*. Retrieved from https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf

O'Brien, S. (2017, December 7). While you're tallying your bitcoin gains, don't forget the taxman. *CNBC*. Retrieved from https://www.cnbc.com

Offensive Security. (2018a). Exploit Database Statistics. Retrieved from https://www.exploit-db.com/exploit-database-statistics/

Offensive Security. (2018b). Exploit Database. Retrieved from https://www.exploit-db.com/exploits/43970/

Official Newspaper of the Democratic and Popular Algerian Republic. (2017, December 27). *Official Journal of the Algerian Republic No. 76.* Retrieved from https://www.mfdgi.gov.dz/images/pdf/lois_de_finances/LF2018F.pdf

Olympus Market. (2018). Announcement: Olympus Market – We know you've been waiting for long. Retrieved from https://www.reddit.com/r/OlympusDNM/comments/7reg09/announcment_olympus_market_we_know_youve_been/

Osborne, C. (2014). North Korea cyber warfare capabilities exposed. *ZDNet.* Retrieved from http://www.zdnet.com

Oyedele, A. (2017, January 19). One country dominates the global Bitcoin market. *Business Insider*. Retrieved from https://www.businessinsider.com.au

Paganini, P. (2016, August 28). Global cost of cybercrime will grow from $3 trillion in 2015 to $6 trillion annually by 2021. *Security Affairs*. Retrieved from http://securityaffairs.co

Palmer, D. (2016, July 10). NSA labels Linux Journal readers and Tor and Tails users as extremists. *Digital Trends*. Retrieved from https://www.digitaltrends.com

Panda, A. (2013, December 6). People's Bank of China issues a regulatory notice on Bitcoin. *The Diplomat*. Retrieved from https://thediplomat.com

Parker, E. (2017, December 11). Can China contain Bitcoin? *Technology Review*. Retrieved from https://www.technologyreview.com

Patterson, D. (2016, July 11). How to safely access and navigate the Dark Web. *TechRepublic*. Retrieved from https://www.techrepublic.com

Perper, R. (2018, February 6). China is moving to eliminate all cryptocurrency trading with a ban on foreign exchanges. *Business Insider*. Retrieved from https://www.businessinsider.com.au

Peretti, K. K. (2009). Data Breaches: What the Underground World of "Carding" Reveals. *Santa Clara Computer and High - Technology Law Journal, 25*(2), 375– 413. Retrieved from https://search-proquest-com.virtual.anu.edu.au/

P**erry, G. (2017, Dec 24)**. How I Got Paid $0 From the Uber Security Bug Bounty. *Medium*. Retrieved from https://medium.com

Pieters, G. C. (2016). The Potential Impact of Decentralized Virtual Currency on Monetary Policy. *Globalization and Monetary Policy Institute 2016 Annual Report*. Federal Reserve Bank of Dallas: Dallas. Retrieved from https://poseidon01.ssrn.com/delivery.php?ID=436070084067080000126095019065123098100075028006087054119098104100087070077081082022097027039000046111005102103124122088107076042057047080049026103111065075066088091004081083008087125030065122127000074088114082064087121010093106066086121075067077092105&EXT=pdf

Patel, H. (2017). Three Countries With the Largest Number of Bitcoin Miners [Web Log Post]. Retrieved from https://blog.iqoption.com/en/three-countries-with-the-largest-number-of-bitcoin-miners/

Popper, N. & Ruiz, R. R. (2017, July 20). 2 Leading Online Black Markets Are Shut Down by Authorities. *The New York Times.* Retrieved from https://www.nytimes.com

Privacy Living. (2016, February 12). DARKNET, DARK WEB & THE TOR BROWSER. *Privacy Living.* Retrieved from https://privacyliving.com

RAND – **Research ANd Development (2014).** Markets for Cybercrime Tools and Stolen Data. Retrieved from https://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf

Rapoza, K. (2017, November 2). Cryptocurrency exchanges officially dead in China. *Forbes*. Retrieved from https://www.forbes.com

Reddit. (2016). *Visualisation of darknet market lifespans*. Retrieved from http://i.imgur.com/DLq1fDp.png

Reiff, N. (2018, January 17). Alibaba launches cryptocurrency mining platform. *Investopedia*. Retrieved from https://www.investopedia.com

Reuters Staff. (2017, September 4). ICO crackdown may just be the start: China is reportedly planning tighter cryptocurrency rules. *CNBC*. Retrieved from https://www.cnbc.com

Reuters Staff. (2017, December 19). South Korean cryptocurrency exchange to file for bankruptcy after hacking. *Reuters*. Retrieved from https://www.reuters.com

Reuters Staff. (2018, June 11). Bitcoin tumbles as hackers hit South Korean exchange Coinrail. *Reuters.* Retrieved from https://www.reuters.com

Reuters Staff. (2017, September 15). China is shutting down all of Beijing's Bitcoin and cryptocurrency exchanges. *Fortune*. Retrieved from http://fortune.com

Reuters. (2017, October 18). Xi says China will continue to open its economy, deepen financial reforms. Reuters. Retrieved from https://www.reuters.com

Reuters. (2018, January 22). South Korea to ban cryptocurrency traders from using anonymous bank accounts. *CNBC.* Retrieved from https://www.cnbc.com

Revoredo, T. (2017, November 6). Legal "Status" of Cryptocurrencies in Brazil. *Medium.* Retrieved from https://medium.com

Rid, T., & Buchanan, B. (2015). Attributing Cyber Attacks. *Journal of Strategic Studies, 38*(1-2), 4 – 37. doi: 10.1080/01402390.2014.977382

Robinson, M., & Schoenberg, T. (2018, May 24). U.S. Launches Criminal Probe into Bitcoin Price Manipulation. *Bloomberg News*. Retrieved from https://www.bloomberg.com

Ron, D., & Shamir, A. (2013). Quantitative Analysis of the Full Bitcoin Transaction Graph. *Financial Cryptography and Data Security, 7859*, 6 – 24. doi: https://doi.org/10.1007/978-3-642-39884-1_2

Rosic, Ameer. (2016). *What is Blockchain Technology?*, available at: https://blockgeeks.com/guides/what-is-blockchain-technology/

Sanger, David (2018). *The Perfect Weapon: War, Sabotage and Fear in the Cyber Age*. Penguin Random House, N.Y.

Sayer, P. (2014, December 30). Tor, TrueCrypt, Tails topped the NSA's 'most wanted' list in 2012. *PCWorld.* Retrieved from https://www.pcworld.idg.com.au

Ścibor, A. (2018, March 3). Cryptojacking: Smominru botnet infected already half a million servers, Windows. *AVLab*. Retrieved from https://avlab.pl

Sheridan, K. (2018, March 23). Looking Back and Thinking Ahead on Cyberwar, Nation-State Attacks. *Dark Reading.* Retrieved from https://www.darkreading.com

Sharma, R. (2018, January 4). China may curb electricity for Bitcoin miners: Will prices tank? *Investopedia*. Retrieved from https://www.investopedia.com

Sharp, T. (2017). Theorizing cyber coercion: The 2014 North Korean operation against Sony. *Journal of Strategic Studies, 40*(7), 898– 926. doi: 10.1080/01402390.2017.1307741

Siers, R. (2014). North Korea: The Cyber Wild Card. *Journal of Law & Cyber Warfare, 4*(1), 1– 12. Retrieved from http://heinonline.org.virtual.anu.edu.au

Skinner, W. F., & Fream, A. M. (1997). A social learning theory analysis of computer crime among college students. *Journal of Research in Crime and Deliquency*, *34*, 495-518.

Smith, G. (2013, July 18). Meet Tor, The Military-Made Privacy Network That Counts Edward Snowden As A Fan. *Huffington Post*. Retrieved from http://www.huffingtonpost.com.au

South China Morning Post. (2018, January 4). China plans to deter Bitcoin miners by curbing electricity use. *South China Morning Post*. Retrieved from http://www.scmp.com

Stack Overflow (2018). Developer Survey Results 2018. Retrieved from https://insights.stackoverflow.com/survey/2018

Stackpole, B. (2018, March 15). What to do when Botnets Go Berserk. *Symantec* Retrieved from https://www.symantec.com

Steinmetz, K. F. (2016). *Hacked: A Radical Approach To Hacker Culture And Crime*. New York, NY: New York University Press.

Sterling, B. (2016, August 19). The Shadow Brokers Manifesto. *Wired*. Retrieved from https://www.wired.com

Stisa Granick, J. (2017). *Legal Risks of Vulnerability Disclosure*. Retrieved from http://www.blackhat.com/presentations/win-usa-04/bh-win-04-granick.pdf

Suberg, W. (2018, January 16). China's Alibaba launches crypto mining platform despite restrictions, says local sources. *Coin Telegraph*. Retrieved from https://cointelegraph.com

Sutherland, E. H. (1956). The professional thief. University of Chicago Press.

Sward, A., Vecna, I., & Stonedahl, F. (2018). Data Insertion in Bitcoin's Blockchain. *Ledger*, 3.

Sykes, G.M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review*, *22* (6), 664– 670.

Symantec. (2016). SWIFT attackers' malware linked to more financial attacks [Web Log Post]. Retrieved from https://www.symantec.com

Symantec. (2017a). Attackers target dozens of global banks with new malware [Web Log Post]. Retrieved from https://www.symantec.com

Symantec. (2017b). *WannaCry: Ransomware attacks show strong links to Lazarus group* [Web Log Post]. Retrieved from https://www.symantec.com

Symantec Employee. (n.d.). What is the Difference Between Black, White and Grey Hat Hackers? Retrieved from https://us.norton.com/internetsecurity-emerging-threats-what-is-the-difference-between-black-white-and-grey-hat-hackers.html

Szoldra, P. (2013, August 21). Hacker reveals How Devastating a Cyberattack on the Stock Market Could Be. *Business Insider: Australia.* Retrieved from https://www.businessinsider.com.au

The Economist. (2018, January 4). China's great firewall is rising. *The Economist.* Retrieved from https://www.economist.com

The Global Drug Survey. (2017, May 24). Global Drug Survey: Global Overview and Highlights. Retrieved from https://www.globaldrugsurvey.com/wp-content/themes/globaldrugsurvey/results/GDS2017_key-findings-report_final.pdf

The Indian Express. (2017, September 15). Chinese Bitcoin exchange announces it is ending trading. *The Indian Express.* Retrieved from http://indianexpress.com

The Onion Router. (n.d.). *Inception*. Retrieved from https://www.torproject.org/about/torusers.html.en

The Sydney Morning Herald, (2018, January 16). China set to escalate its cryotocurrency crackdown. *The Sydney Morning Herald*. Retrieved from http://www.smh.com.au

Thomson, I. (2017, June 29). Shadow Brokers hike prices for stolen NSA exploits, threat to out ex-Uncle Sam Hacker. *The Register*. Retrieved from https://www.theregister.co.uk

Tiezzi, S. (2016, January 22). More over, Bitcoin: China wants to issue its own digital currency. *The Diplomat*. Retrieved from https://thediplomat.com

Tu, K. V., & Meredith, M. W. (2015). Rethinking Virtual Currency Regulation in the Bitcoin Age. *Washington Law Review, 19*(1), 271– 347. Retrieved from https://digital.law.washington.edu/dspace-law/bitstream/handle/1773.1/1442/90WLR0271.pdf?sequence=1&isAllowed=y

UKcryptocurrency (n.d.). Is Bitcoin Legal in the UK? Retrieved from https://ukcryptocurrency.com/

United Nations. (2017). *Resolutions.* Retrieved January 12, 2018, from https://www.un.org/sc/suborg/en/sanctions/1718/resolutions

United Nations Children's Fund (UNICEF). (2017). The State of the World's Children 2017, Children in a Digital World, Available at: https://www.unicef.org/sowc2017/

United States Computer Emergency Readiness Team. (2017). *Hidden Cobra – North Korea's DDoS Botnet Infrastructure.* Washington, United States: Author. Retrieved from https://www.us-cert.gov/ncas/alerts/TA17-164A

United States Department of Justice. (2017, July 20). *AlphaBay, the Largest Online 'Dark Market,' Shut Down.* Washington, United States of America: Author. Retrieved from https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down

United States Department of Justice. (2017). *Infraud superseding*. Nevada, United States: United States Department of Justice.

United States Department of Justice. (2018). *Thirty-six Defendants Indicted for Alleged Roles in Transnational Criminal Organisation Responsible for More than $530 Million in Losses from Cybercrimes*. Retrieved 26 February, 2018, from https://www.justice.gov/opa/pr/thirty-six-defendants-indicted-alleged-roles-transnational-criminal-organization-responsible

Varshney, N. (2016, January 20). People's Bank of China plans to launch its own digital currency. *Coin Telegraph*. Retrieved from https://cointelegraph.com

Verizon. (2016). *2016 Data Breach Investigations Report.* Retrieved from http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf

Verisign/Merril Research. (2018). *Q4 2017 DDoS Trends Report.* Retrieved from https://www.verisign.com/en_US/security-services/ddos-protection/cyber-security-resources/index.xhtml

VDMA. (n.d). *The Legal Regulation of Bitcoin*. Retrieved from http://www.vdma.co.za/legal-regulation-bitcoin/

Viney, S. (2017, July 21). What is the darknet, and how will it shape the future of the digital age? *ABC News*. Retrieved from http://www.abc.net.au

Van Wegberg, W. Verburgh, T. Van Den Berg, J. Van Staalduinen, M. (2017, August). *Alphabay Exit, Hansa-Down: Dream On?* Retrieved from the Dark Web Solutions website https://www.tno.nl/media/10032/17-9099-factsheetbrochure-dws-05.pdf

Von Neumann J. (1966). *Theory of Self-Replicating Automata*. Retrieved from http://cba.mit.edu/events/03.11.ASE/docs/VonNeumann.pdf

Wagner, J. (2017, June 1). China's Cybersecurity Law: What you need to know. *The Diplomat*. Retrieved from https://thediplomat.com

Wagstaff, J., & Smith, J. (2017). Multi-stage cyber attacks net North Korea millions in virtual currencies: researchers*. Reuters.* Retrieved from https://www.reuters.com

Wertz, D. (2013). The Evolution of Financial Sanctions on North Korea. *North Korean Review, 9*(2), 69– 82. doi: 10.3172/NKR.9.2.69

Whittaker, Z. (2018, February 19). Lawsuits threaten infosec research — just when we need it most. *ZDNet*. Retrieved from http://www.zdnet.com

Wikimedia Commons. (2016). CAPTCHA. Retrieved from https://upload.wikimedia.org/wikipedia/commons/4/49/Captchacat.png

Wikimedia Commons. (2017). Image of general encryption process. Retrieved from https://commons.wikimedia.org/wiki/File:Encryption3.jpg

Who is Attacking the Darknet Black Markets to Bring it Down? (2017, November 24). *Darknet Markets.* Retrieved from https://darknetmarkets.co/who-is-attacking-the-darknet-black-markets-to-bring-it-down/

Whonix. (n.d.). *About*. Retrieved 30 December, 2018 from https://www.whonix.org/wiki/About

Whyte, C. (2016). Ending cyber coercion: Computer network attack, exploitation and the case of North Korea. *Comparative Strategy, 35*(2), 93– 102. doi: 10.1080/0145933.2016.1176453

Willy, W. (2017, January 17). Estimating China's Real Bitcoin Trading Volumes. *Coindesk.* Retrieved from https://www.coindesk.com

Wolters, T. (2000). 'Carry Your Credit in Your Pocket': The Early History of the Credit Card at Bank of America and Chase Manhattan. *Enterprise & Society*, *1*(2), 315– 354.

Worthington, A., & McDonald, A. (2017, July 25). AFP hunts Australian dark net users after sites taken down. *Australian Broadcasting Corporation.* Retrieved from http://www.abc.net.au/news/

Wright, A., & De Filippi, P. (2015, January). Decentralised Blockchain technology and the rise of the lex cryptographia. *ResearchGate*. DOI: 10.2139/ssrn.2580664

Yamaguchi, F., Golde, N., Arp, D., & Rieck, K., 2014. Modeling and discovering vulnerabilities with code property graphs. Retrieved from https://www.computer.org/csdl/proceedings/sp/2014/4686/00/4686a590.pdf

Yang, S., Larson, C. and H., P. (2017, July 10). China tells carriers to block access to personal VPNs by February. *Bloomberg.* Retrieved from https://www.bloomberg.com

Ye, J. (2017, January 23). China tightens Great Firewall by declaring unauthorised VPN services illegal. *South China Morning Post*. Retrieved from http://www.scmp.com

Young, J. (2016, August 25). Baidu stops all Bitcoin-related advertising. *Coin Telegraph.* Retrieved from https://cointelegraph.com

Yu, X. (2018, February 5). China to stamp out cryptocurrency trading completely with ban on foreign platforms. *South China Morning Post*. Retrieved from http://www.scmp.com

Zerodium. (2018). *ZERODIUM Payouts*. Retrieved from https://www.zerodium.com/program.html

Zetter, K. (2016, April 13). Hacker Lexicon: What Are White Hat, Gray Hat, And Black Hat Hackers? *Wired*. Retrieved from https://www.wired.com

Zulkarnine, A. T., Frank, R., Monk, B., Mitchell, J., & Davies, G. (2016). Surfacing Collaborated Networks in Dark Web to Find Illicit and Criminal Content. *2016 IEEE*

Chinese References

百度百科. (2013, December 6). 关于防范比特币风险的通知. *Baidu*. Retrieved from http://www.baike.com

A notice issued by the PBOC on preventing Bitcoin's risks.

陈果静. (2017, September 22). 央行正在酝酿发行法定数字货币. *China Daily*. Retrieved from http://caijing.chinadaily.com.cn

PBOC is preparing to issue its own digital currency.

李国辉. (2018, February 4). 监管加码！中国将取缔、处置境内外虚拟货币交易平台网站. T*he Paper*. Retrieved from http://www.thepaper.cn

China is tightening its control over cryptocurrency online trading platforms both onshore and offshore.

新浪网. (2018, January 16). 腾讯加码区块链项目 已悄然注册"以太锁"商标. *Sina*. Retrieved from http://tech.sina.com.cn

Tencent has put forward its blockchain project and has registered the trademark "Ether Lock."

腾讯证券. (2018, January 16). 阿里巴巴挖矿平台悄然上线 知情人称将与电商结合. *Tencent Stock*. Retrieved from http://stock.qq.com

Alibaba has allegedly launched its own mining platform. An anonymous source claimed the company is planning to integrate the service with e-commerce.

王全浩. (2018, February 13). 写白皮书网上叫价3600， 可虚构海外背景. *Beijing News*. Retrieved from http://www.bjnews.com.cn
Fake ICO white papers with a forged overseas credibility are now available for RMB $3600 on Alibaba owned online shopping platform Taobao.

中华人民共和国工业和信息化部. (2017, January 22). 工业和信息化部关于清理规范互联网网络接入服务市场的通知. *Ministry of Industry and Information Technology*. Retrieved from http://www.miit.gov.cn/n1146295/n1652858/n1652930/n3757020/c5471946/content.html
A notice issued by the Ministry of Industry and Information Technology on cleaning up and regulating the Internet access service market.

中华人民共和国工业和信息化部. (2017, September 1). 互联网域名管理办法. *Ministry of Industry and Information Technology*. Retrieved from http://www.miit.gov.cn/n1146295/n1146557/n1146624/c5778555/content.html
A notice issued by the Ministry of Industry and Information Technology on regulating Internet domain names.

中国人民银行. (2016. January 20). 中国人民银行数字货币研讨会在京召开. *People's Bank of China*. Retrieved from http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/3008070/index.html
A statement of a PBOC's meeting about cryptocurrencies took that place in Beijing

中国人民银行. (2017, September 4). 中国人民银行 中央网信办 工业和信息化部 工商总局 银监会 证监会 保监会关于防范代币发行融资风险的公告. *People's Bank of China*. Retrieved from http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/3374222/index.html
A notice issued by PBOC, Office for the Central Leading Group for Cyberspace Affairs, the Ministry of Industry and Information Technology, State Administration for Industry and Commerce, China Banking Regulatory Commission, China Securities Regulatory Commission and China Insurance Regulatory Commission on preventing the financial risks of Initial Coin Offerings (ICOs).

Appendix 1

Basic Category Listings of Products on Dream Market.

Product Type	Apr-14	Apr-04	Mar-28	Mar-21	Mar-18	Mar-12	Mar-08	Feb-24	Feb-09	Jan-27	Jan-14	Jan-07	Dec-30	Dec-24	Dec-17	Dec-10	Nov-15	Oct-31	Oct-14	Oct-02
Drugs	61926	59165	60052	58229	57580	56417	55006	53954	48263	48076	45061	46299	43016	43220	46453	46539	47530	52119	53226	48042
Drug Paraphernalia	209	206	189	179	177	178	182	143	171	165	160	144	135	163	157	286	293	315	334	345
Digital goods	50113	49315	52698	52637	51751	50558	48769	47155	43204	44134	42637	43984	43273	34832	35110	44221	41619	41769	41678	42074
Services	4341	4263	4150	4146	4157	4128	4089	3975	3336	3732	2862	4448	4080	3969	3820	3622	4171	3629	3834	3392
Other	3841	3169	5351	5334	3111	5299	5219	5260	4983	5190	4906	5302	4906	3280	3192	3109	3423	2890	3083	2290
All	120430	116118	122440	120525	116776	116580	113265	110487	99957	101297	95626	100177	95410	85464	88732	97777	97036	100722	102155	96143
# Listings Captured	119844	105659	112280	111681	108246	116539	99645	95788	98919	92821	92587	96976	89512	82054	81154	94378	93922	100650	101642	93057
% Listings Captured	99.51%	90.99%	91.70%	92.66%	92.70%	99.96%	87.98%	86.70%	98.96%	91.63%	96.80%	96.80%	93.80%	96.00%	91.50%	96.50%	96.80%	99.90%	99.50%	96.80%

Appendix 2

A Timeline of Cryptocurrency Regulations in the Peoples Republic of China

2013 December 5: The People's Bank of China (PBOC) issued a "Bitcoin Regulatory Notice" 《关于防范比特币风险的通知》stressing the illegality of Bitcoin.

2014 January: PBOC set up its own cryptocurrency research team.

2015 January: The Chinese government blocked three major VPN providers in China: Astrill, StrongVPN and Golden Frog. Numerous popular VPN services are censored as well, such as Facebook, Google and Twitter.

2016: January 20: The PBOC convenes a meeting in Beijing to discuss opportunities ifor developing a local digital currency.

August 25: China's largest online search engine Baidu ceased all Bitcoin-related advertisements.

November 7: The Chinese government enacted the new Cybersecurity Law to come into effect in 2017. The law requires network operators to cooperate with Chinese crime or security investigators and allow full access to data and unspecified "technical support" to the authorities upon request. The law imposes mandatory testing and certification of computer equipment for critical sector network operators. In addition, the law requires business information and data on Chinese citizens gathered within China to be kept on domestic servers and not transferred abroad without permission. It also includes a ban on the export of any economic, technological, or scientific data that would pose a threat to national security or the public interest.

2017: January 22: The Chinese government issued a notice《关于清理规范互联网网络接入服务市场的通知》that would make the use of VPNs illegal in China. A cyber "clean up" operation commenced immediately until March 31, 2018.

April: Tencent announced the company's progress in developing a new blockchain "Ether Lock" and "Ethernet Lock".

June 1: Cybersecurity Law comes into effect.

July 10: The Chinese government ordered a total ban of unauthorised VPN starting from February 2018.

July 28: Apple Inc. complied with the Chinese government order to remove VPNs from its Chinese iOS AppStore

September 1: The Ministry of Industry and Information Technology issued a notice "Internet Domain Operation Methods"《互联网域名管理办法》stating websites operating in China must register to a Chinese domain name (.cn)

September 4: The People's Bank of China (PBOC) issued a notice that terminated the practice of initial coin offerings (ICOs).

September 15: The PRC government ordered the closure of all Beijing-based cryptocurrency exchanges.

September 30: One of China's biggest Bitcoin exchanges, the Shanghai-based BTCChina ceased trading.

2018 January 3: PBOC outlined a plan to restrict the activity of Bitcoin miners.

January 12: Baidu launches its own blockchain-as-a-service (BaaS) platform.

January 16: Alibaba has allegedly launched a cryptocurrency mining platform named "P2P Nodes".

January 30: Facebook prohibited all cryptocurrency and ICO-related advertisements.

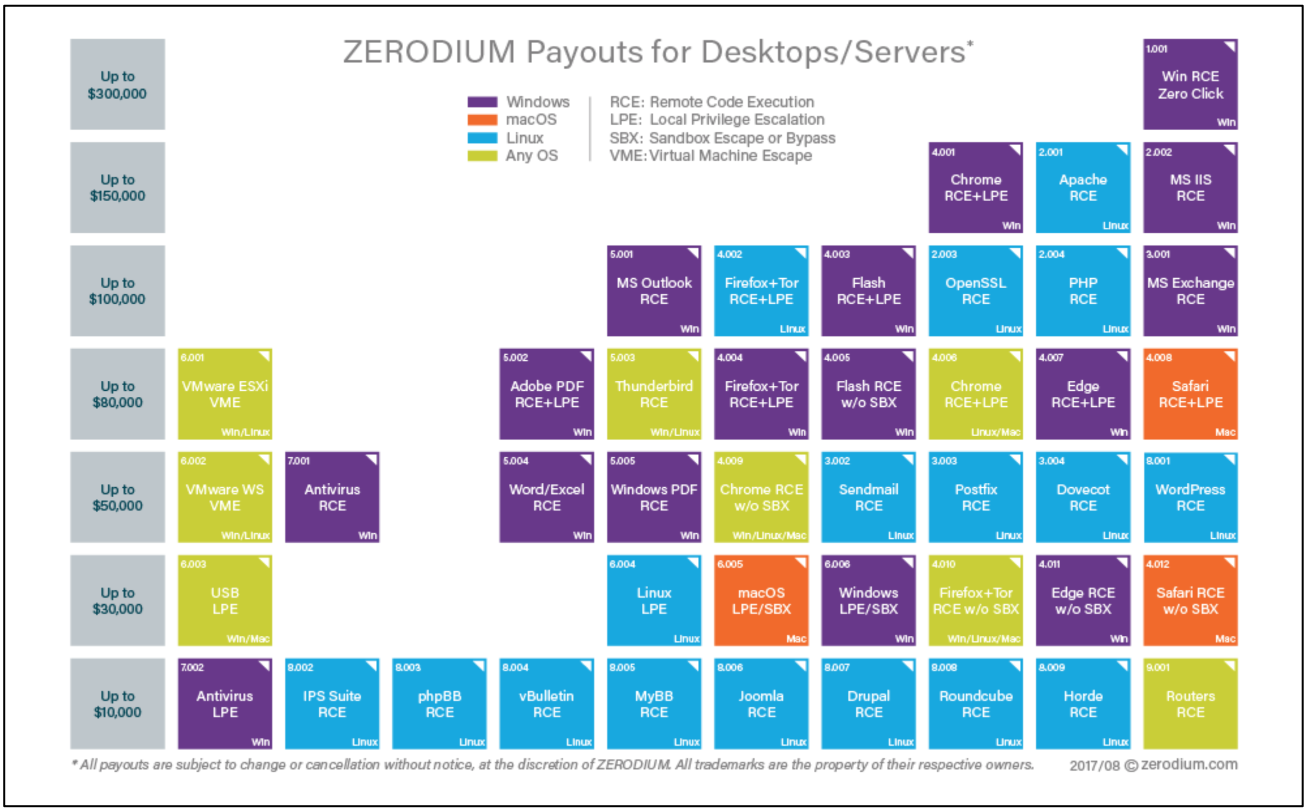
February: Apple announced that it transferred its iCloud operations in China to its Chinese partner, Guizhou-Cloud Big Data Industry Co. Ltd (GCBD) from February 28 onwards.

February 4: PBOC announced China will actively crackdown both onshore and offshore cryptocurrency-related trading platforms.

Appendix 3

Zerodium Bug Bounties

Zerodium Payouts for Desktops/Servers (Zerodium, 2018)



ZERODIUM Payouts for Desktops/Servers*

🟪 Windows
🟧 macOS
🟦 Linux
🟨 Any OS

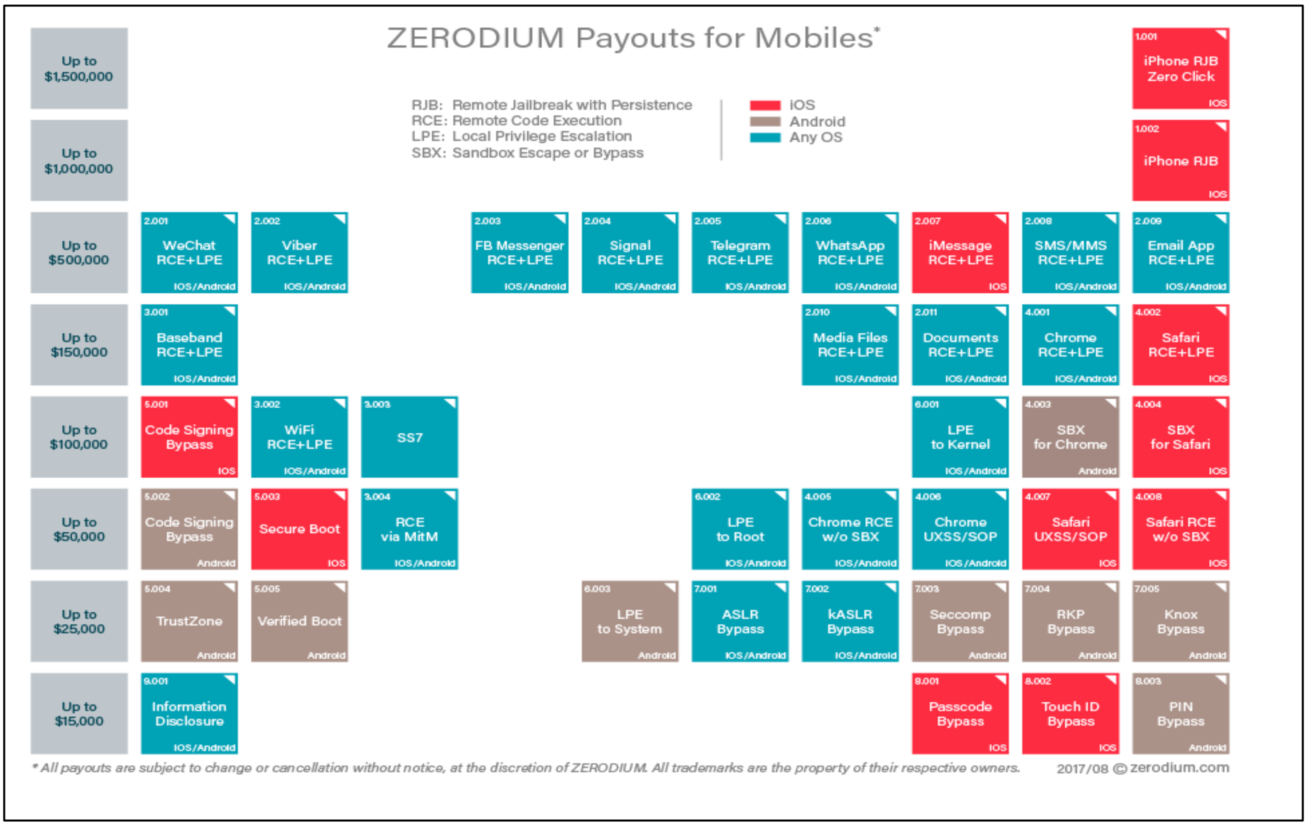
RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass
VME: Virtual Machine Escape

Up to $300,000										1.001 Win RCE Zero Click Win
Up to $150,000								4.001 Chrome RCE+LPE Win	2.001 Apache RCE Linux	2.002 MS IIS RCE Win
Up to $100,000					5.001 MS Outlook RCE Win	4.002 Firefox+Tor RCE+LPE Linux	4.003 Flash RCE+LPE Win	2.003 OpenSSL RCE Linux	2.004 PHP RCE Linux	3.001 MS Exchange RCE Win
Up to $80,000	6.001 VMware ESXi VME Win/Linux			5.002 Adobe PDF RCE+LPE Win	5.003 Thunderbird RCE Win/Linux	4.004 Firefox+Tor RCE+LPE Win	4.005 Flash RCE w/o SBX Win	4.006 Chrome RCE+LPE Linux/Mac	4.007 Edge RCE+LPE Win	4.008 Safari RCE+LPE Mac
Up to $50,000	6.002 VMware WS VME Win/Linux	7.001 Antivirus RCE Win		5.004 Word/Excel RCE Win	5.005 Windows PDF RCE Win	4.009 Chrome RCE w/o SBX Win/Linux/Mac	3.002 Sendmail RCE Linux	3.003 Postfix RCE Linux	3.004 Dovecot RCE Linux	8.001 WordPress RCE Linux
Up to $30,000	6.003 USB LPE Win/Mac				6.004 Linux LPE Linux	6.005 macOS LPE/SBX Mac	6.006 Windows LPE/SBX Win	4.010 Firefox+Tor RCE w/o SBX Win/Linux/Mac	4.011 Edge RCE w/o SBX Win	4.012 Safari RCE w/o SBX Mac
Up to $10,000	7.002 Antivirus LPE Win	8.002 IPS Suite RCE Linux	8.003 phpBB RCE Linux	8.004 vBulletin RCE Linux	8.005 MyBB RCE Linux	8.006 Joomla RCE Linux	8.007 Drupal RCE Linux	8.008 Roundcube RCE Linux	8.009 Horde RCE Linux	9.001 Routers RCE

* *All payouts are subject to change or cancellation without notice, at the discretion of ZERODIUM. All trademarks are the property of their respective owners.*

2017/08 © zerodium.com

Zerodium Payouts for Mobiles (Zerodium, 2018)



ZERODIUM Payouts for Mobiles*

RJB: Remote Jailbreak with Persistence
RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass

🟥 iOS
▨ Android
🟦 Any OS

Up to $1,500,000										1.001 iPhone RJB Zero Click IOS
Up to $1,000,000										1.002 iPhone RJB IOS
Up to $500,000	2.001 WeChat RCE+LPE IOS/Android	2.002 Viber RCE+LPE IOS/Android		2.003 FB Messenger RCE+LPE IOS/Android	2.004 Signal RCE+LPE IOS/Android	2.005 Telegram RCE+LPE IOS/Android	2.006 WhatsApp RCE+LPE IOS/Android	2.007 iMessage RCE+LPE IOS	2.008 SMS/MMS RCE+LPE IOS/Android	2.009 Email App RCE+LPE IOS/Android
Up to $150,000	3.001 Baseband RCE+LPE IOS/Android						2.010 Media Files RCE+LPE IOS/Android	2.011 Documents RCE+LPE IOS/Android	4.001 Chrome RCE+LPE IOS/Android	4.002 Safari RCE+LPE IOS
Up to $100,000	5.001 Code Signing Bypass IOS	3.002 WiFi RCE+LPE IOS/Android	3.003 SS7					6.001 LPE to Kernel IOS/Android	4.003 SBX for Chrome Android	4.004 SBX for Safari IOS
Up to $50,000	5.002 Code Signing Bypass Android	5.003 Secure Boot IOS	3.004 RCE via MitM IOS/Android			6.002 LPE to Root IOS/Android	4.005 Chrome RCE w/o SBX IOS/Android	4.006 Chrome UXSS/SOP IOS/Android	4.007 Safari UXSS/SOP IOS	4.008 Safari RCE w/o SBX IOS
Up to $25,000	5.004 TrustZone Android	5.005 Verified Boot Android			6.003 LPE to System Android	7.001 ASLR Bypass IOS/Android	7.002 kASLR Bypass IOS/Android	7.003 Seccomp Bypass Android	7.004 RKP Bypass Android	7.005 Knox Bypass Android
Up to $15,000	9.001 Information Disclosure IOS/Android							8.001 Passcode Bypass IOS	8.002 Touch ID Bypass IOS	8.003 PIN Bypass Android

*All payouts are subject to change or cancellation without notice, at the discretion of ZERODIUM. All trademarks are the property of their respective owners.

2017/08 © zerodium.com